780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 9, Issue 2

AvengerCon:

PURSUING CYBER EXCELLENCE ONE CON AT A TIME

PRAETORIANS

780th MI BDE

"STRENGTH AND HONOR"

Col. Matthew Lennox
Commander
Command Sgt. Maj. Ronald Krause
Command Sergeant Major

780th MILITARY INTELLIGENCE BRIGADE (CYBER), Fort George G. Meade, Maryland, publishes The BYTE as an official command information publication, authorized under the provisions of AR 360-1, to serve its Soldiers, Civilians, and Families.

Opinions expressed herein do not necessarily represent those of 780th MI BDE or the Department of the Army.

All photographs published in The BYTE were taken by 780th MI BDE Soldiers, Army Civilians, or their Family members, unless otherwise stated.

Send articles, story ideas, photographs, and inquiries to the 780th MI Brigade (Cyber) Public Affairs Officer (PAO) and The BYTE Editor, Steven Stover at steven.p.stover.civ@mail.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.

On the Cover
AvengerCon V logo

THIS ISSUE OF THE BYTE magazine is focused on AvengerCon, a free security event held every fall to benefit the hackers of the U.S. Cyber Command community and is supported by the 780th Military Intelligence Brigade (Cyber). AvengerCon features presentations, hacker villages, training workshops, and much more.

According to Capt. Skyler Onken, AvengerCon is an effort from within the ranks. Recently completing its fifth iteration, the idea for the training event came after Onken and Capt. Stephen Rogacki had attended a DefCon and saw how difficult it was for the Army to send people to hacker conferences.

“But they are really valuable in two ways, one, obviously the educational training benefit, two, really getting a feel for the community, because hacking and cyber is more than just a skillset or a profession, it really is a community,” said Onken.

Also, in this issue of the BYTE, The Task Force Echo transition between the Army National Guard’s 124th Cyber Protection Battalion and the 123rd CPB; the activation of B Company, 915th Cyber Warfare Battalion; and two cyber Soldiers join the prestigious Sergeant Audie Murphy Club.

Origins of AvengerCon

By Capt. Skyler Onken, 780th Military Intelligence Brigade (Cyber)

IN 2015, CAPT. STEVE ROGACKI and I were enjoying lunch at an overcrowded Las Vegas Johnny Rockets when the idea for AvengerCon was born. The 780th Military Intelligence Brigade (Cyber) had selected a small cohort to attend DEFCON 23 with the express purpose of returning to the force with lessons learned. Both Steve and I had previously attended hacker conferences and had been involved in the hacking community as hobbyists. As a result, we understood that the value of such events was not only in the presentations, but the exposure and immersion in the hacker culture. Unfortunately, costs and policy make it impossible to regularly send a large contingent of Soldiers. The only other plausible solution was to have the Army run its own DEFCON style conference.

The mission of the yet to be named event was to provide a bridge between the rigid and disciplined Army culture and the erratic and rebellious hacker culture. Hopefully, the Army could reconcile notions of incompatibility between being a hacker and a Soldier by engaging and exposing new cyber Soldiers to the hacker culture. Steve and I knew that for an event like this to be successful, it had to be designed and ran by the Soldiers themselves.

About a month later, the Commander of 781st MI Battalion (Cyber), Lt. Col. Justin Considine, challenged the junior officers to take ownership and initiative in the development of an Army cyber culture. Steve and I saw this as an opportunity to get command buy-in on the execution of this Army-style DEFCON; however, organizing a conference in a short amount of time is a daunting task. I enlisted the support of Sgt. 1st Class Craig Seiler, a cyber capabilities developer, and the other members of A Company (Avengers), 781 MI Battalion. Hunter Hutcheson, Company Commander, and Col. Matthew Lennox, then the Team Lead of 61 National Mission Team, provided their support for the event as a Company level training. This is how the name AvengerCon was born. A reference to the Alpha Company Avengers.

The first year of AvengerCon was as makeshift as it comes. The event took place in the R&E Symposium with about 100 attendees from throughout the Battalion. It consisted of snacks, some lock picks scattered on a table, and a plethora of speakers. There were both classified and unclassified talks provided by Soldiers of all ranks. The most notable presentation was the keynote by Bruce Potter, a legend in the hacker world. Having such high-profile keynotes would become a trademark of AvengerCon and maintain the emphasis on bridging Army and hacker culture.

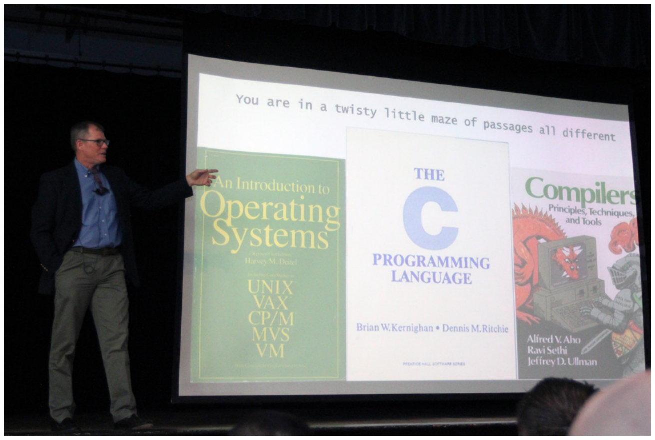
AvengerCon has evolved and grown each year since the first. Key personnel like Capt. Andreas Kellas, Maj. Neil Milchak and numerous others joined in the cause. The venue has changed to accommodate the growth, but the spirit and elements remain the same. Each year the AvengerCon team must overcome numerous challenges to make the event a success. No matter the work or challenges, AvengerCon has become a tradition which has accomplished much of what was envisioned in 2015. Hopefully it will continue to provide a bridge that shapes the culture of Army cyber. ■

AvengerCon V: Flexibility in a COVID Environment

SINCE 2016, PRAETORIANS FROM 780th MI BDE (Cyber) have worked to bring the U.S. Cyber Command community and the Department of Defense, the largest and fastest growing unclassified cyber training venue in the U.S. military, AvengerCon. From its inception, this conference has increased in participation, year after year – bringing some of the greatest minds in the cyber-hacking community to share time, talent and invaluable treasures. However, after the turn of calendar year 2020, no one expected to face the changes and challenges of a global health crisis. Early 2020 and for months afterward, organizations worldwide stalled, stuttered and even shut down, as no one had branches or sequels to counter this pandemic. The AvengerCon senior planners had to make a decision on whether to hold an annually-expected event and had to consider how to maintain the vision and intent through an alternate plan. This team of pioneers embraced this challenge and ran with the changes. They did not use COVID-19 as an "excuse" but rather as a planning factor in order to continue providing the highest level of training to all members within the cyber community.

With regards to cyberspace, the battlefield is always evolving. The world and especially, its technologies are progressing. Can you remember what businesses were like before the internet? Before the world wide web, and "zeroes and ones" (that was only 25 years ago), a commercial company would open its doors, put advertisements in the local paper, and hoped people bought what was being advertised. Today, organizations can now reach out to entities across the globe to make a sell. According to the James Clark School of Engineering, hackers are attacking computers with internet access every 37 seconds [1]. Thus placing a demand on cyber-security to constantly change and improve as quickly as one can identify a vulnerability or a patch. Operating systems and networks are updating, seemingly, on a weekly basis while we often neglect to update our human systems and habits. 780th MI BDE (Cyber) had to "update" and demonstrate resiliency in dealing with the public distress, embracing the restrictions to daily life and the uncertainty of what will come. Toward the end of AvengerCon IV (2019), the planning team, (consisting of U.S. Army Captains Skyler Onken, Andreas Kellas, Richard Shmel, Alex Farmer, Mathew Boston, and Jiung Kim, Chief Warrant Officer 2 Justin Helphenstine, Sgt. 1st Class Craig Seiler, Cpl. Andrew Fricke and Maj. Neil Milchak), had already started thinking about an "in-person" AvengerCon V. They were already planning how to improve the conference, how to implement changes, and integrate more effective ways to communicate to a technologically astute community.

The irony of working in a dynamic cyber-environment, is that Soldiers should also be able to adjust and modernize their courses of action based on our surroundings. No matter the cause or conflict, Soldiers have to remain agile and adaptive: able to change directions, left or right at a moment's notice, while also able to adjust to the problem set. As progressive as the cyber environment can be, so should our Soldiers be.



Although the pandemic has been disastrous and uncertain, COVID-19 was definitely a forcing function which caused us to change how we have communicated, conducted meetings and even trained our Soldiers. It forced Praetorians to operate with more flexibility; identifying other means to bring people together safely. The AvengerCon planners had to adjust the execution of this highly interactive conference, to bring the brigade, its first virtual AvengerCon. This was by no means a service of less quality confined by restrictions. Developers such as Fricke had to develop a secure AvengerCon website that filtered out individuals with authorized access, while Schmel developed a Capture the Flag training in a virtual village capable of hosting over 100 participants. Others like Boston and Seiler helped develop an infrastructure to assist over 1300 registrants. Although this global pandemic changed the face of how we conduct training and face-to-face interaction, the AvengerCon planners demonstrated their ability to be agile and adaptive. Their determination to remain in the fight enabled them to execute one of the largest cyber training conferences in the Army, all the while remaining completely in a cyber-environment, due to the COVID backdrop.

Reference:

[1] Cukier, Michel.A.James Clark: School of Engineering. "Study: Hackers Attack Every 39 Seconds" 9 February 2019.

The Necessity of Community to AvengerCon and the Army

By Capt. Andreas Kellas, Cyber Solutions Development Detachment-Meade, 781st Military Intelligence Battalion (Cyber)

IN 1997, AN ESSAY TITLED "The Cathedral and the Bazaar" caused a cultural shift in the way software was discussed. The essay was a rallying point for the open source community; in it, the author compared two models of software development: the old-school, top-down "cathedral" model where software is developed by a few experts in a very controlled and planned manner, and new style bottom-up "bazaar" model that had recently been adopted by some open source enthusiasts, where wide community engagement and participation was prioritized. The followers of the bazaar model held the maxim that "given enough eyeballs, all bugs are shallow", and called for the normalization of community-driven software development. The Linux kernel was held as one example of the success of the bazaar model, and the essay is credited with influencing the decisions to open-source other influential projects, like the Netscape browser.

In the U.S. Army, our decision making process looks more like the cathedral model of software development – and for good reason. Battlefield planning requires meticulous attention to detail and prompt care for deadlines. Just imagine the disaster that awaits trying to plan a movement to contact by community input, only to have the operation held up because the volunteer maintainers were not available to approve a merge request!

But every now and then, the opportunity presents itself for wider community-driven planning and participation, and the results are exhilarating. In the past five years of planning and executing AvengerCon, we've accidentally stumbled into learning the same core principles that drive successful open-source community software projects. We've learned that it's counter-productive to try to plan and execute a full AvengerCon event from top to bottom by ourselves – we just aren't imaginative, creative, or exciting enough to do that. Instead, all we need to do is build a venue and open up the doors to the larger community to bring enthusiasm and life to the event. The real heroes of AvengerCon are the volunteers who choose to present their knowledge, teach workshops, manage villages, engage with other attendees, or participate in any of the myriad of other ways.

Planning AvengerCon this way is a nauseating experience – every year, it feels like we're flying by the seats of our pants, and pulling everything together at the last second. It's anxiety inducing, and we constantly feel the weight of not wanting to let down the community. But what keeps us grounded is knowing that as long as we're able to pull off the bare-minimum – that is, that we're able to get a group of motivated hackers into a room to talk about their ideas and teach others how to grow – then we're going to be okay. Everything else that happens at AvengerCon is awesome, and it all makes the event better. But if that all crashed and burned, at the end of the day as long as we're providing a venue for a community of hackers to come together to share their knowledge and enthusiasm with the rest of the Army and Joint Cyber communities, we're succeeding.

I've had the pleasure of watching this first-hand over the years of being involved in AvengerCon. The very first AvengerCon was held in a classified auditorium with about 100 attendees, primarily from within the 781st MI BN. I was a newly arrived lieutenant in the unit, and I didn't yet know the conference founders (but thanks to the inviting culture of AvengerCon, they let me take the stage as a new presenter to speak). The entire experience was incredible, hearing the thoughts and projects of technical experts from across the battalion. When the event came back the following year, it was easy to reach out to the organizers to become a volunteer to help plan it. We made the decision that year to bring AvengerCon into the unclassified venue of McGill Training Center on Fort Meade in order to have broader reach and to be able to incorporate more community events, like Capture the Flag competitions. At AvengerCon III, we realized that we could do more to teach members of our community new skills, so we added a second day to AvengerCon in order to host workshops in topics like software reverse engineering and PowerShell scripting. By this point, AvengerCon had grown so much that we had more than 300 attendees and the key note presentation was given by Chris Eagle, a leader in the information security industry.

By this point, AvengerCon had established itself as its own cultural staple in the community of the unit. It was also at this point that Skyler Onken, the founder and lead organizer of AvengerCon so far, moved to Georgia to continue his Army career. He looked at me and effectively said, "Don't mess this up while I'm gone" – and that was scary. But the work was easy, precisely because of the large community that had grown around AvengerCon that kept it going. For AvengerCon IV, we teamed up with the U.S. Cyber Command J9 Capability Discover office, which partners with the non-profit Maryland Innovation and Security Institute (MISI), allowing us to use the DreamPort facility and expand into an event that saw over 700 people attend, with even more engagement from joint service and government agency partners.

The global coronavirus pandemic raised a lot of questions and challenges for AvengerCon V. When we began planning in the spring of 2020, we were completely unsure of when it would be safe to have a physical event with potentially more than 1,000 attendees. We were hesitant to go all-in on a virtual event if we didn't have to, because we thought we might lose the community engagement that makes AvengerCon so special. However, we also didn't want to fall into the trap of postponing AvengerCon indefinitely until a physical event could safely be planned. By July 2020, we made the decision to execute AvengerCon V virtually in order to give ourselves enough time to properly make the transition. And once again, it was the community that saw us through to success – except this time, the community was a bit bigger. Because of the virtual format, we had unprecedented levels of participation from the 782d MI BN, Cyber Protection Brigade, and the 915th Cyber Warfare Battalion, as well as from units and organizations beyond both Fort Meade and Fort Gordon. So while the load was heavier to put on a virtual AvengerCon, there were even more hands to share it with – in total, more than 1,300 registrants.

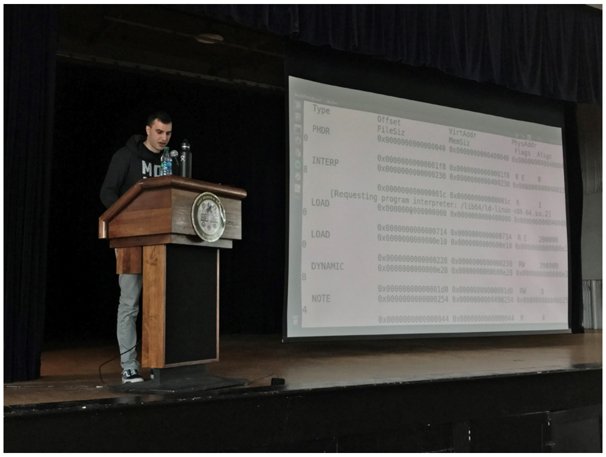
I don't know where AvengerCon is going to go next, but I do know that as long as the community is still excited about it, it's going to keep succeeding. But the importance of AvengerCon's success isn't just to put on an enjoyable experience for attendees for a couple of days; instead, the success of the event has implications for national and global security.

In my closing remarks at the end of AvengerCon V, I recounted the story about the young captains named Patton and Eisenhower who were stationed at Camp Meade in 1920, exactly 100 years before AvengerCon V. Camp Meade was very different from the Fort Meade that it would become – back then, it was the home of the Army's fledgling Tank Corps returned from World War I. At the time, the Tank Corps was organized as a part of the Infantry branch, and tanks were written into Army doctrine as such. The tanks of the era were slow and plodding, and were employed in a line in front of the infantry. The lines of tanks and infantry would advance together slowly, with the tanks leading first to clear out any enemy enforced positions so the infantry could clean up what was left. However, Patton and Eisenhower envisioned something more for the new technology. They imagined a Tank Corps that was separate from the infantry, and composed of fast-moving maneuverable vehicles that could quickly mass fires against an enemy flank to create a weak points to punch through. They spent the summer of 1920 disassembling their tanks and putting them back together, and pushing the vehicles to their limits for the sake of learning and understanding, and discussing new design ideas with engineers. They each wrote articles that were published in the Infantry Journal calling for an independent Tank Corps. However, the establishment of Army generals did not agree with their ideas, and effectively silenced them by instructing them to never again publish ideas that were contrary to "solid infantry doctrine." It wasn't until two decades later in World War II that Sherman tanks were used in precisely the manner that Eisenhower and Patton had proposed.

A similar story can be told about the creation of the Army Air Corps, which eventually grew into the U.S. Air Force. The first imagined uses of airplanes in the Army were for reconnaissance and surveillance, so the Army Signal Corps maintained the air units. Young aviators worked hard to re-imagine what air power could be by combining their domain experiences with policy suggestions. These aviators were people like Hap Arnold, who learned how to fly from the Wright brothers as a second lieutenant before going on to command the Army Air Forces during World War II, and Billy Mitchell, who believed so strongly in an independent Air Force that his vocal attacks on leaders who disagreed with him led to his court martial. Arnold and Mitchell were advocates for using airplanes to drop bombs and dominate the air. In fact, Mitchell even predicted, in 1924, that a future war with Japan would result in an air attack on Pearl Harbor.

Communities did not exist for these Soldiers to bring together their technical knowledge and ideas for the future of warfare. It's so important to have a community of our own as we try to understand how changing technology should best be organized in our national defense efforts. We need to be able to share our ideas, however unorthodox, to build excitement, learn from each other, and propose better ways of conducting business – and inspire the next generations to learn and have novel ideas of their own. We don't have two decades to wait to validate our ideas (and hopefully no courts martial are forthcoming in the meantime), so it's imperative that we build a place for these discussions now. AvengerCon is one such bazaar for these ideas, and we hope that it continues to have positive effects on the culture of our cyber forces as we grow into the mature organizations that we need to be. We can't do that without the community, but thankfully the community is very strong so far.

**Note that any references to the essay "The Cathedral and the Bazaar" by Eric S. Raymond are used for the discussion of the culture of open source software, and are not endorsements of the personal views expressed by Eric Raymond outside of the essay.*



FORT GEORGE G. MEADE, Md. – 1st Lt. Andreas Kellas doing a live demo.

What Happened in the Cyber Policy Simulation at AvengerCon V?

By Midshipman 3rd Class (sophomore) Elisse Gibbens, United States Naval Academy

AVENGERCON V WAS BUZZING with keynote speakers, events and villages alike this past November. One such village was the Cyber Policy Simulation supported by the Naval Academy Women in Cybersecurity and Computing (WiCC) club.

The cyber policy simulation involved multiple teams of students role-playing as members of assigned government agencies in response to a nationwide cyber attack. Overall, there were over forty students participating, the majority of whom were Midshipmen from the United States Naval Academy (USNA).

In addition to USNA, students from the University of Pennsylvania, New York University, University of Michigan, and Georgetown University participated. The "teams" or agencies they role-played were the National Security Agency, U.S. Cyber Command, Department of Defense, Department of State, Department of Homeland Security, Department of Treasury, Department of Justice, and Department of Commerce.

Last year, teams usually came from nearby universities where the cost of travel was easy to manage. However, "with the recent shift to a virtual forum in light of the global pandemic, we had to completely reassess how to construct the simulation," said MIDN 2/C Chase Lee, a key member of my staff. "We initiated a distinct approach by expanding the collaborative effort and engagement among students. In order to do so, we sought input from a wider audience to include undergraduate students from civilian universities nationwide, heretofore it had been limited to the Baltimore-Washington area."

The table-top simulation was made possible by the USNA faculty, staff, and other officers who volunteered their time to mentor teams and better facilitate real-world actions.

This event didn't start with me. The very idea of it was created by then MIDN 1/C Lani Davis and MIDN 1/C Grace Lawrence, two successful midshipmen who went on to join the fleet. According to now Ensign Davis, "We saw there was a gap in understanding for students on how an actual cyber attack could play out in the United States."

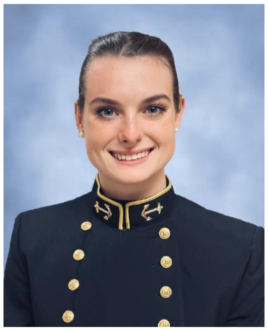
"In class", she continued, "we learn about many different types of attacks and some of the documents that would govern the U.S.' response. Despite reading documents and knowing definitions, we realized that many students don't understand how that coordinated response to a cyber attack would look like in the real world. We wanted to explore a way for students to understand how agencies could coordinate and how different powers could actually be applied together to combat a cyber attack." Ensign Lawrence added that "the goal was not to design a competition but start a conversation. And to explore how people with different backgrounds approach cyber because it is so multifaceted."

Back in 2019, after participating in the first edition of this simulation, I was amazed. I had never been given the opportunity to see how cyber affected all portions of the government, or how the U.S. would and should react in a crisis. A few months later when the application was sent out to join the newly minted staff for Avengercon V, I signed up immediately, as the secretary. It turned out, however, by May 2020, I was the only brave soul to forge ahead with this exciting leadership opportunity. That's when it became my project and mine alone. I was given the final notes and told good luck! It was terrifying. I had just finished plebe cyber and barely understood what a cyber attack looked like.

For the next three months of the summer leading into my youngster (sophomore) year, I poured myself into research. What was a tabletop simulation? Why do companies need these trainings? What would I make the simulation plot about? I thought I should quit and give it up to a senior or junior cyber major more than once. I was too inexperienced; I'd embarrass myself and USNA. But then I kept going back to that saying from plebe summer, drilled into my head tighter than a screw: "If not me then who?" It wouldn't stop replaying itself, and I knew I would regret every second of it if I gave up this project. So, after months of nail biting and research, I built my team. In July I had: an American University graduate student I'd met through one of the previous mentors at the first simulation; three seniors; and two juniors at USNA. Their majors ranged from political science to computer science and cyber operations. I wanted a diverse team that could give me several perspectives on one topic.

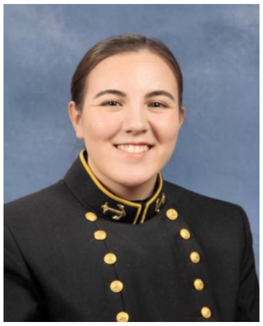
Then came the work. It was slow building at first, and we were completely unprepared. It took several meetings with a personal mentor of mine, Greg Glaros, a USNA grad I had met at a networking event, to figure out how I was going to lead this team. The biggest and most looming question was: what was my mission statement? That wasn't answered for a long time. My team was floating, and we kept scrapping ideas and trajectories (mostly due to my lack of executive leadership). It was September, we had less than three months, I was a sophomore who had never led before and I was scared. What if I failed?

Finally, I had my mission statement and we had our trajectory. "The point of this exercise [was] to teach college students how the government works together to fend off a cyber attack, what a cyber attack can look like off screen, and how foreign relations can often play an important role in cybersecurity." From then on, things got easier. We were able to connect with

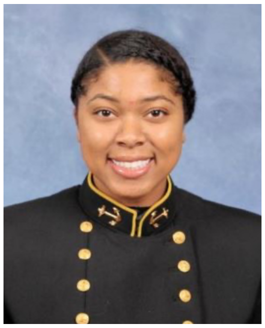


3/C Elisse Gibbens

2/C Chase Lee

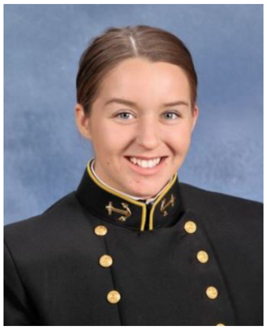


2/C Brigitta Szepesi



1/C Sierra Swanda

1/C Christian Moreno



1/C Kate Asaro

1/C Alexander Douglas

several industry professionals and faculty at USNA who were indispensable.

The plot, centered around the COVID pandemic, involved a fictitious field-level attack on ventilators that had been bought in bulk from a foreign country. These machines malfunctioned, causing chaos and panic across the U.S. The teams were instructed to perform a myriad of tasks to mitigate the situation. This included investigating the source of this attack by using information that was either solely given to a few teams, to simulate how true intel would flow during a cyber attack, or announced to all of them at once. The team leaders were also in charge of proposing how each team would use their real-world responsibilities to ease the chaos and trace back the source of this attack.

The participants formally met twice during the three-hour-long event in a "national security council (NSC) meeting" where each team proposed a "who-done-it" and explained how they would help the situation. In addition to this task, each group had a responsibility to handle public relations. They were fed articles in real time about how the U.S. was reacting, along with information that news outlets were gathering and tweets from fictitious world leaders commenting on the situation. One of my staff members was in charge of writing real-time reports based on the information each team gave at the council meetings.

"I really liked that the press releases were related to our responses. I also liked the simulation being relevant to what we are actually experiencing," commented a participant during the feedback portion of the event.

The participants not only had to handle the situation with care but needed to understand there would be consequences to their actions. Several foreign countries and actors were fictitiously involved, and based on the responses given, would react differently in a "choose your own adventure" style. For example, if the participants had chosen to be hostile towards Canada when it was revealed the ventilators originated from there, then the manufacturers at the imagined site would not have provided valuable information. However, they chose to be diplomatic, which appeased the suppliers and led the simulation further down the plot.

The staff of the simulation were praised for their "hard work, leadership, and creativity" by several of the faculty present from different schools.

One student remarked that "having the mentor there to help give a perspective on what our team should be doing definitely helped since almost none of us had any experience."

Having mentors in this simulation made it different from other table-top trainings. Having industry professionals at the ready allows our participants to make mistakes. They can ask questions, receive real time answers and have confidence in the applicability of those answers. ENS Davis emphasized this in the first edition of the simulation. “I think it’s a very unique feature of the simulation that not many other policy simulations are able to do. It was something that Grace [ENS Lawrence] and I really thought was important because it's one thing to read a document, but another thing to understand how it could be applied to a situation or if there could be a better alternative that we didn't know about. Mentors are a key feature that I think really helps make the simulations more realistic.”

This event did not come without challenges though. Due to the COVID-19 pandemic, the conference was held on a virtual platform via Discord. However, on the day of the event after several hours of prepping the channel and allocating Zoom calls for backup just in case, both plans A and B failed. For half an hour, my staff and I were handling distress calls from participants due to confusion over how to access the event and why they weren’t getting updates. It was incredibly hectic, and the simulation was finally boiled down to the basics: ten Google Meets and emails to send out the information. What was at first a logistics nightmare soon turned into a blessing. The majority of the participants, including those of us on the staff, were unfamiliar with the Discord environment and could more easily navigate this new trajectory. A few hiccups persisted nonetheless, such as when I accidentally sent out the wrong injects. That incident narrowly escaped revealing the final plot a mere third of the way through the event.

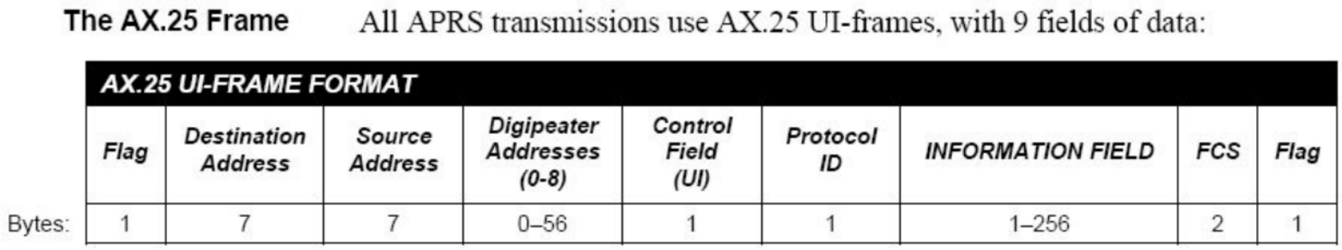
We have changed several things from the first edition of the simulation, some that I plan to continue into next year. We’re continuing with the NSC format, but I will be adding more staff members to play active roles within the plot. I want this to feel as real as possible. The simulation will also be modelled after a hybrid simulation, instead of a simple tabletop, extending the event from three hours to two days.

I’m proud to say that I worked with incredibly talented people to make this event possible. Collectively, we had very little knowledge on how to run this thing or where to even start. My role was simply to manage people and make sure it got done, and I could not have done this without them. Going into this next year I plan to increase the number of people on my staff and provide more leadership opportunities.

Staff members included: Midshipman 1st Class Sierra Swanda; Midshipman 1st Class Alexander Douglas; Midshipman 1st Class Christian Moreno; Midshipman 2nd Class Brigitta Szepesi; Midshipman 2nd Class Chase Lee; Midshipman 3rd Class Elisse Gibbens; and Austen Brennan, a graduate student of American University. Midshipman 1st Class Kate Asaro also provided staff support. ■

An Introduction to the Automatic Packet Reporting System

By Sgt. Evan Natter, B Company, 781st Military Intelligence Battalion (Cyber)



The AX.25 Frame All APRS transmissions use AX.25 UI-frames, with 9 fields of data:

AX.25 UI-FRAME FORMAT

	Flag	*Destination Address*	*Source Address*	*Digipeater Addresses (0-8)*	*Control Field (UI)*	*Protocol ID*	*INFORMATION FIELD*	*FCS*	*Flag*
Bytes:	1	7	7	0–56	1	1	1–256	2	1

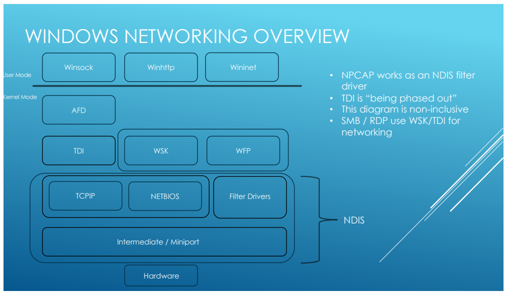
IMAGINE TRYING TO KEEP TRACK OF YOUR TEAM for hours spread out over a large area without a reliable cell phone signal. This can pose a real challenge in most situations but there is a simple solution. The automatic packet reporting system more commonly known as APRS is a protocol used in amateur radio. APRS is a digital protocol that uses special packets transmitted over the airwaves to send both positional data as well as short text messages. This flexible protocol can easily establish a digital lane of communication that can quickly be expanded in the number of users and range of coverage. Bob Bruninga, whose call sign was WB4APR, developed the radio protocol in the 1980s while he was a researcher at the U.S. Naval Academy. APRS uses digital packets transmitted over analog airwaves. APRS is normally run on the two-meter band on 144.39MHz but is also commonly seen on the thirty-meter band. It could run on any frequency that permits data transfer. APRS has been used to track search and rescue teams in the field, trucks out on the highways, track radio-controlled aircraft, weather balloons and amateur radio enthusiasts to help find each other. APRS can be utilized from a cellphone connected to the audio interface of a radio, can be built into a radio, or even work on a standalone single purpose-made beacon. The APRS protocol uses a digital technology called AX.25 UI frames.

AX.25 is a layer two link local protocol similar in concept to UDP. When AX.25 is implemented for use with APRS there is no layer three protocol in use. One of the greatest advantages of the APRS protocol is its' expandability. These digital packets can be funneled onto the internet via what is known as an IGATE. An IGATE is a piece of software that can be run in a listen only mode where it will just push APRS packets to the internet or in a two way mode where it will also transmit message packets out to try and get them to their intended users. From the internet, you can view the positional data for any call sign that is passing its data over the network. The range can also be extended over airwaves using a digipeater. A digipeater takes in digital signals then retransmits them from a higher altitude and commonly at higher power as well to extend the range of the signal. With a digipeater or a chain of them all tuned to the same frequency, it is easy to get a signal to travel well over a hundred miles. The final real advantage of APRS is how flexible it is, APRS can be found built into radios or run from a cell phone through a low-cost handheld radio. APRS is far from perfect in terms of security. APRS has no confidentiality, there is an FCC ban on encryption on the amateur radio bands meaning anyone can listen to your positional data. There is also no authentication on APRS all you need to connect as a specific user at most is a hash of a call sign. It is a system of trust that everyone is using their own call sign to identify themselves. Despite all this APRS is a solid protocol for tracking people and equipment, while the protocol is old and has all the old security holes the protocol is very flexible and easily expanded. ■

Techniques for Covert Communications in Windows

By 1st Lt. John Geenty III, Cyber Solutions Development – Georgia, 782d Military Intelligence Battalion (Cyber)

MICROSOFT HAS TAKEN GREAT MEASURES to ensure the security of their systems for their customers, however, hackers continue to evolve and find ways to subvert their defensive techniques. Microsoft has devoted a lot of its attention – when it comes to security – to the kerneland anti-virus. Examples of kernel mitigations include driver signing and kernel patch protection. With these defensive mechanisms, hackers have found creative and innovative ways to attack and persist on windows devices. To persist on devices, generally, the attacker needs to include a mechanism that will allow them to survive a reboot, load extra higher equity payloads, and a way to communicate with the listening post (LP). In my opinion, the most interesting of these are the last two: Loading payloads and communications. The easiest solution here is to survey the surrounding limits of the target device and build their tool to mimic the traffic. This, however, requires you to have more in depth knowledge of not just the target, but the surrounding network as well. Not only that, but it almost forces the developer to have to build a separate solution for every targeted attack. The goal instead should be to focus on building a mechanism that would be more extensible, lives deep inside of the device. A worthwhile approach to this would be to reverse engineer a component of windows software – the TCP/IP stack in the kernel for example – and change a small portion of the code or data without disrupting existing functionality. A nice approach to this would be to overwrite a function pointer or utilize a concept called "hotpatching" – which refers to patching the prologue of a function to short jump, then long jump to malicious code, then back to the next instruction in the prologue. The problem with overwriting function pointers is Control Flow Guard (CFG) both in user mode and the kernel will prevent the call to malicious code from happening. In this case, hot-patching with a proper locking mechanism – described and implemented[1] – should be able to subvert that defense. For the techniques described in this paper, it is assumed that the attacker has obtained arbitrary kernel code execution on a target. This paper builds off an existing idea to exfiltrate data from the kernel to a remote location via the TCP/IP stack and will look at a possibility of backdooring windows services. These payloads would be best suited for an in-memory stage-1 implant that does not persist and survive reboots. Thus, the purpose is to communicate in a covert manner, protect the persistent payload, and provide the ability to silently delete itself


WINDOWS NETWORKING OVERVIEW

- NPCAP works as an NDIS filter driver
- TDI is "being phased out"
- This diagram is non-inclusive
- SMB / RDP use WSK/TDI for networking

Figure 1: Windows Networking Stack.

Building a mechanism that essentially backdoors the TCP/IP stack enables the attacker to possibly subvert firewalls and – depending on the exact implementation – blend in automatically by abusing existing connections. In windows, there is an old mechanism that allows kernel mode drivers to interface with the networking stack called the Transport Driver Interface (TDI). TDI lives above the implementation of the transport and IP algorithms in the windows networking stack and the windows firewall. A security researcher, Sean Dillion, came up with a novel technique that enables an attacker to steal credentials and other vital data from the target. The technique – called SassyKitdi – uses fake TDI objects to gain access to the networking stack, then just sends the data from there to an LP. This achieves the goal of subverting communication and not introducing anomalous traffic into the networking, however, it does not subvert firewalls. This is since the attacker is using TDI, and it sits above the firewall implementation in the networking stack. In figure 1, TDI is adjacent to its replacement – Winsock Kernel – however it does not sit below the Network Driver Interface Specification (NDIS) layer which contains filter drivers, which is where the windows firewall sits. To bypass firewall detection mechanisms that attacker could build a custom TCP/IP stack as a protocol driver, however, this is not feasible for a stage-1 payload. To do that, requires a lot more time and effort from the attacker and a lot more code and data as well. Generally, building windows implants and communication mechanisms, the lower in the network stack the attacker aims to hook into, the more time and effort it takes. There's no one reason for this, but in the deep dark internals in the bottom of the stack there are a lot more components in the lower layers which requires a lot more research into the intricacies of the specific sub-system. There are many options at this point, each of which deserve their own paper, but a few examples are protocol drivers and miniport drivers that conform to the latest NDIS documentation.

Figure 2 graphically describes how to use this mechanism to build a stage- 1 in-memory loader. Once kernel execution is obtained, the payload proceeds to initialize all TDI objects and then beacons back to the LP. At this point, the remote attacker has their choice of operations: Check if alive, burn off, or load payload. The choice of payload can a kernel mode payload – typically a rootkit – or can be a user mode payload. The former holds more equity and risk because of additional mitigations that must be bypassed in the kernel. On the other hand, the latter will be your best guarantee to remain persistent on the target. The main problem the attacker will have to deal with is migrating from kernel mode to user mode. For jumping to user mode execution, a double Asynchronous Procedure Call (APC) – described in figure 3 – is a method to migrate from kernel mode to user mode. At this point persistence is achieved and the attacker can confirm this by checking that the implant was successfully loaded via their LP, then issue the burn-off command for the kernel mode payload.

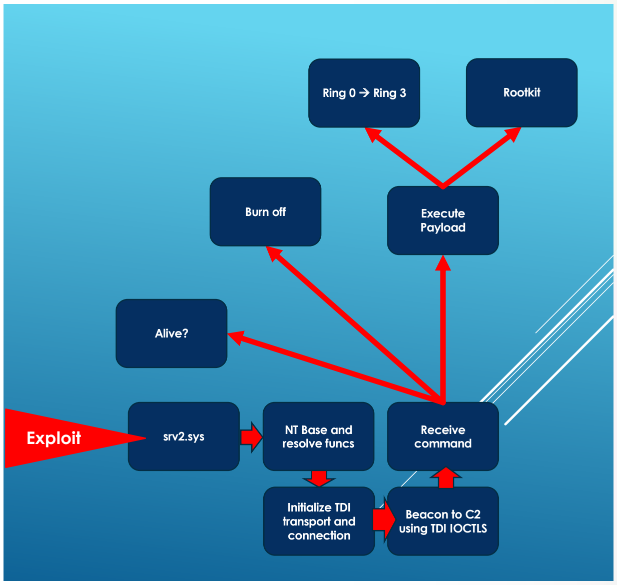
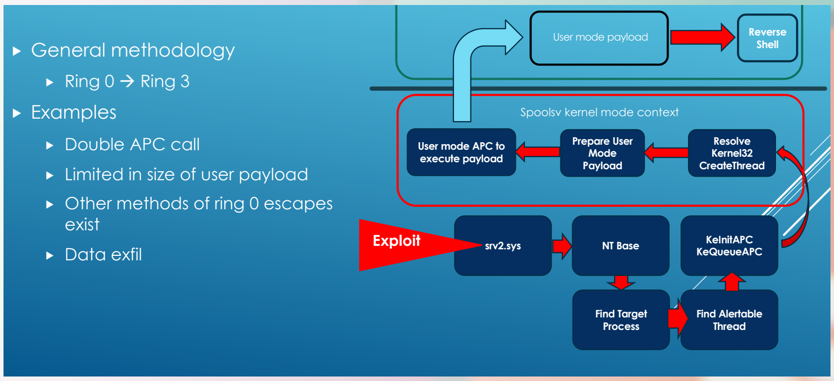

Ring 0 → Ring 3
Rootkit
Burn off
Execute Payload
Alive?
Exploit
srv2.sys
NT Base and resolve funcs
Receive command
Initialize TDI transport and connection
Beacon to C2 using TDI IOCTLS

Figure 2: Loading a secondary payload.

To improve on the current communication mechanism, the attacker could work to blend in with the traffic coming to and from the target. This would include using a technique built by Bill Demirkapi that hooks into existing connections and utilizes those connections as a communications medium. This can be accomplished by first searching for objects that represent existing connections, instead of creating a fake object. It would drastically increase the payload size but would definitely a viable option for a stage-2 communication mechanism. If the attacker wanted to blend in more with the environment, they could also choose to utilize windows services such as Server Message Block (SMB). A technique loosely described in a talk by both Joe Desimone and Gabriel Landau of Endgame[2], talks about overwriting the srvnet!SrvNetWskAcceptEvent function and hook all SMB requests made to the device. This would potentially blend in well in enterprise environments that use file shares, however, defenders could catch this by perform deep packet inspection. Note that for the defender to be successful, it also requires they know what to look for. More research is needed in this area, but definitely a viable approach.



- General methodology
  - Ring 0 → Ring 3
- Examples
  - Double APC call
  - Limited in size of user payload
  - Other methods of ring 0 escapes exist
  - Data exfil

User mode payload
Reverse Shell
Spoolsv kernel mode context
User mode APC to execute payload
Prepare User Mode Payload
Resolve Kernel32 CreateThread
Exploit
srv2.sys
NT Base
KeInitAPC KeQueueAPC
Find Target Process
Find Alertable Thread

Figure 3: Double APC Ring 0 escape.

This paper mostly built off existing approaches to covert communications mechanisms and presented two approaches for attackers to take. The general premise of covert communications is to find a service or component in the targeted device that is used often by the target and offers the potential ability to load secondary payloads. The latter is the most important because often it is easier to obtain command execution on a target and the quickest. Loading secondary payloads makes the attacker far more dangerous because now they can survive reboots, or even potentially destroy the box completely via loading a destructive payload.

References:

- [1] *https://zerosum0x0.blogspot.com/2019/11/fixing-remote-windows-kernel-payloads-meltdown.html.*

- [2] *https://github.com/AlfredoAbarca/Blackhat2018/blob/master/us-18-Desimone-Kernel-Mode- Threats-and-Practical-Defenses.pdf*

Transforming Operational Technology Underpinning Critical Infrastructure and Platforms Across All Domains into Our Most Secure Enclaves

By Maj. Brent Stone, Ph.D. Army Cyber Technical Warfare Center, and Dr. Ken Tindell, CTO Canis Automotive Labs

YOU'RE LIKELY READING THESE WORDS thanks to the same class of technology they were written with: information technology (IT). IT is the internet, smartphones, point of sales at stores, and more. Just as ubiquitous but easily overlooked is operational technology (OT). Passenger vehicles, microwave ovens, medical devices, and power grids are a few examples of OT [1], [2]. The fundamental objectives and engineering of IT and OT are orthogonal. IT is flexible, generalized, and capricious. OT is inflexible, specialized, and consistent. An anecdotal contrast of IT and OT may intuitively introduce their stark differences: it's inconvenient but acceptable to wait a while for a WiFi hotspot connection or streaming video; conversely, arbitrary delays for airbag deployment or aileron adjustments would cost lives and millions of dollars.

For decades, OT industries and their customers have consistently operated with the assumption that air-gapped isolation from IT eliminates the need for cybersecurity controls. The success of Stuxnet to destroy centrifuges, DARPA researchers' remote control of a stock passenger vehicle using its cellular connection, and the poisoning of a Florida city's water supply by an internet-based attack are a few of many examples that OT airgaps are disappearing and insufficient [3]–[5]. Figure 1: BSIDPS—Two Parts of CIA Triad

Despite the current wholesale lack of security throughout OT industries, it turns out the unique engineering features of OT technology inadvertently creates the potential for verifiably complete security at the physical and data link layers. Production tested and low maintenance retrofit solutions already exist to exploit this potential [6]–[11]. With the exception of confidentiality, the result is an OT security posture that is objectively superior to what is possible with IT. If these solutions were applied broadly, critical infrastructure and other OT would be transformed from the world's most vulnerable enclaves to the most secure.

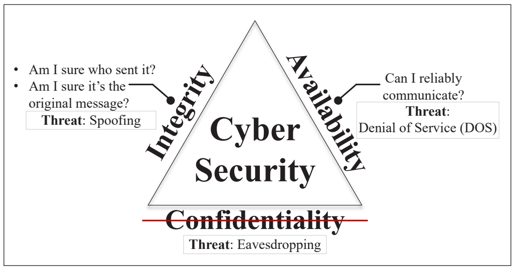


Figure 1: BSIDPS—Two Parts of CIA Triad.

Bit Smashing (BS) Intrusion Detection/ Prevention Systems (IDPS): BSIDPS

The potential for robust operational technology (OT) security is enabled by the following engineering trends:

1. Physical and logical bus network topology makes covert communication difficult or impossible
2. A static set of agents with manually assigned and unique IDs make spoofing obvious
3. Messages are only accepted if no bus errors occur and they match integrity checks like a cyclic redundancy check (CRC).
4. Protocol controllers that repeatedly fail to transmit may assume there is a local fault and enter a fail silent state.
5. OT devices and protocols are designed to operate in real-time where actions and state are routinely managed at the individual bit level.

The combination of trends 1 and 2 leads to each OT network agent knowing their ID and able to observe when another agent uses that ID. Any kind of central controller or gateway will also be able to immediately identify when an unassigned ID is used. Trends 3 through 5 creates the potential for agents observing their ID being spoofed to interrupt the message before it is accepted by other agents. This interruption may also cause the malign agent to go into a fail state that cannot transmit. A term for this real-time interruption at the physical and data link layer is bit smashing (BS)

An example of bit smashing (BS) using digital waveforms is presented in Figure 2. An attacker A attempts to send a payload 0xA. The defender applies extra voltage to the bus at bit time 4, overwriting the attacker's transmission. Other nodes on the bus are unaware anything other than 0xB was transmitted

BSIDPS in Practice: Automotive Controller Area Network (CAN) OT

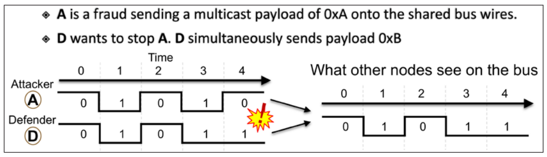

A is a fraud sending a multicast payload of 0xA onto the shared bus wires.
D wants to stop A. D simultaneously sends payload 0xB
Time
0
1
2
3
4
Attacker
A
0
1
0
1
0
Defender
D
0
1
0
1
1
What other nodes see on the bus
0
1
2
3
4
0
1
0
1
1

Figure 2: Bit Smashing Example.

The Controller Area Network (CAN) protocol as it is used in the automotive industry is the focus of the rest of this article to maintain concise and actionable discussion. However, the security concepts and their benefits apply to other industries and protocols. For example, the CAN protocol is used across several OT industries including robotics, medical devices, and transportation for sea, land, and aerospace [12]–[14].

A brief introduction to Automotive CAN

Ground vehicles depend on electronic control units (ECUs) that communicate with each other. For example, an engine management ECU may coordinate with a gearbox ECU to control throttle and gear changes. CAN is a preferred protocol for this kind of automotive communication. When a company named Bosch designed CAN over 30-years ago, few had heard of the internet or considered the possibility of an Internet of Things (IoT). Now fleets of commercial vehicles attach internet-connected telematics devices to the CAN bus to monitor operations. Offering in-vehicle WiFi and internet-enabled perks like remote unlock are common upgrades in personal vehicles. IT and OT interconnection throughout the automotive manufacturing, rental, and repair supply chains are also becoming commonplace.

The format of a CAN frame is shown in Figure 3. The protocol efficiently determines which agent has priority on the bus by allowing bit smashing (BS) during an arbitration phase. Whichever agent's ID contains the more dominant bits at earlier bit times will BS other IDs. Agents observe if their ID is overwritten on the bus and yield to the dominant ID. Whichever agent wins arbitration continues to send a few control bits, a payload, CRC, and finally waits for at least one other agent to broadcast a dominant ACK bit. At any time during the frame's transmission, any agent can send multiple dominant bits onto the bus to signal an error, cause all agents to drop the in-progress message, and reset the bus for a new arbitration phase.

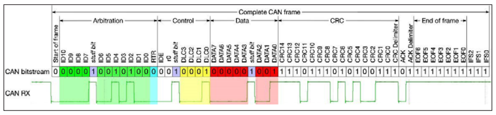


Figure 3: The Controller Area Network (CAN) Frame Format and Example Data [15], [16].

Fielded BSIDPS solutions for Automotive CAN

OT BSIDPS represents a final but robust security measure that compliments defense-in-depth. Ideally, other mechanisms will prevent direct access to a bus and protect supply chain attacks that hijack legitimate firmware reprogramming at the manufacturer, fleet, and repair facilities. Should other measures fail, BSIDPS will preserve physical and data link layer integrity and availability.

Integrity means that receivers can be sure the sender of a message is authentic and spoofing is prevented. Cryptographic methods are used in IT to provide authentication using shared secrets. There are practical weaknesses to this approach with OT. For example, a compromised ECUs will know to the shared secret or may not have the computational resources to implement cryptography. Cryptography is also unlikely to be backward compatible, creating the requirement for cost-prohibitive replacement of entire networks and supply chains.

Availability means that a compromised ECU cannot disrupt the bus and cause the vehicle to fail to operate. One simple and effective attack is to flood the CAN bus with messages. This causes bus bandwidth to be consumed and for legitimate messages to be delayed which is a catastrophic failure for real-time safety-critical networks. A Bus-Off attack is another denial-of-service (DOS) method. It involves an attacker waiting until a targeted ECU begins transmitting. They then bit smash the frame to cause an error. The attacker continues destroying messages when the target attempts to retransmit. This causes the target to assume they are faulty and enter into a fail silent state that cannot transmit. If that target was a critical ECU, the rest of the vehicle may shut down or go into a restricted operation mode. Passenger car manufacturers may call this degraded state a 'limp home mode.' There are network layer or above methods that can mitigate DOS at the physical and data link layers.

The NXP TJA115x and Canis Mercury (CAN-HG)

Two commercial solutions exist to achieve backward compatible BSIDPS security in existing and new CAN networks. The simpler and less complete approach is the TJA115x secure CAN transceiver created by NXP [6]. The TJA115x implements anti-spoofing by independently filtering inbound IDs observed on the bus and outbound IDs attempted to be used by the attached CAN controller. This behavior is analogous to an access control list on a firewall. To mitigate DOS attempts by an attached compromised controller, the chip uses a 'leaky bucket' that effectively rate-limits its transmission frequency.

The more robust and complete solution is the backward compatible CAN-HG protocol created by Canis Automotive Labs and their Mercury chip which implements it [7]. Like the TJA115x, the Mercury chip is physically and logically positioned between the data link and physical layers. Figure 4 demonstrates the man-in-the-middle positioning to achieve BSIDPS.

CAN-HG also uses a central BSIDPS ECU that monitors regular and CAN-HG traffic to identify and prevent illegitimate traffic. Automotive CAN networks typically use gateways that could contain this central supervisor. This central BSIDPS accounts for attacks, like a DOS, that aren't spoofing legitimate network IDs. For example, a central BSIDPS can broadcast a 'cease' command to a particular bus guardian for a compromised ECU. When the 'cease' is received, the bus guardian prevents the transceiver from sending additional frames. This state effectively disconnects the compromised ECU from the bus.

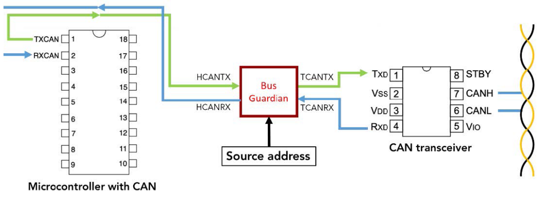


Figure 4: CAN-HG Implementation Between a CAN Controller, Transceiver, and Bus.

Other attacks can be detected and prevented as well. For example, several protocols like J1939 for heavy-duty vehicles extend CAN. The J1939 standard includes long messages sent using the J1939 and J1921 transport protocols that include a sequence number in each CAN frame. There are known attacks that can send the wrong sequence numbers to cause a common flaw in a J1939 software stack to overwrite memory. The flaw causes the chip to execute malware in the J1939 message. The BSIDPS can detect this type of attack, bit smash the attack, and logically disconnect the compromised ECU.

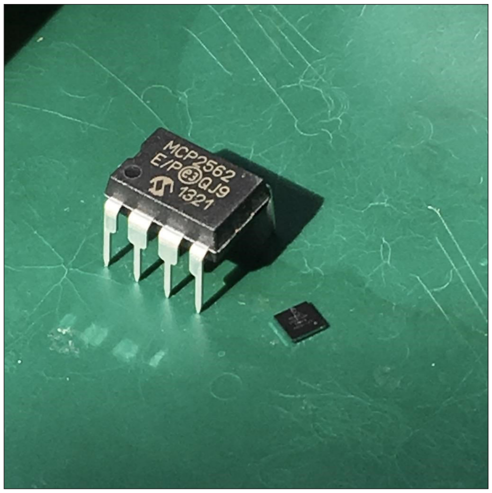


Figure 5: CAN Transceiver and Mercury Chip.

Summary

Bit smashing intrusion detection/prevention systems (BSIDPS) are an effective way to transform operational technology (OT) from an enterprise's most high-risk enclaves to its most secure. Because the approach is backward compatible with in-use systems, BSIDPS may be fielded gradually to meet cost and touch labor constraints. For example, implementing BSIDPS only at ECUs connected to information technology (IT) systems will likely achieve a robust security posture. In passenger vehicles, these ECUs include the internet-connected infotainment system and telematics units. BSIDPS can also be manufactured to conform to existing protocol chip form factors soldered onto in-use printed circuit boards (PCBs). By briefly turning off the OT platform to replace the plain protocol controller and transceiver with a BSIDPS, operational interruptions and cost can be minimized.

References:

1. A. Hahn, “Operational Technology and Information Technology in Industrial Control Systems,” in Cyber-security of SCADA and Other Industrial Control Systems, E. J. M. Colbert and A. Kott, Eds. Springer International Publishing, 2016, pp. 51–68.
2. H. Thomas, “What's the Difference Between OT, ICS, SCADA and DCS?,” *securicon.com/*, 2019. .
3. N. Falliere, L. O. Murchu, and E. Chien, “W32. stuxnet dossier,” Symantec Secur. Response, vol. 14, no. February, pp. 1–69, 2011.
4. C. Miller and C. Valasek, “Car Hacking: For Poories a.k.a. Car Hacking Too: Electric Boogaloo,” 2014. Accessed: Apr. 10, 2017. [Online]. Available: *http://illmatics.com/car_hacking_poories.pdf*.
5. SANS, “SANS NewsBites,” SANS.org, vol. XXII, no. 11, p. 1, 2021.
6. NXP Semiconductors, “NXP TJA115x Secure CAN Transceiver Family,” Eindhoven, Netherlands, 2020. [Online]. Available: *https://www.nxp.com/products/interfaces/can-transceivers/secure-can-transceivers*:SECURE-CAN.
7. A. Rajnák and K. Tindell, “MERCURY: The First Implementation of CAN-HG,” Canis Automotive Labs, 2020. .
8. T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, “A Method of Preventing Unauthorized Data Transmission in Controller Area Network,” 2012 IEEE 75th Veh. Technol. Conf. (VTC Spring), pp. 1–5, 2012, doi: 10.1109/VETECS.2012.6240294.
9. H. Giannopoulos, A. M. Wyglinski, and J. Chapman, “Securing Vehicular Controller Area Networks: An Approach to Active Bus-Level Countermeasures,” IEEE Veh. Technol. Mag., vol. 12, no. 4, pp. 60–68, Dec. 2017, doi: 10.1109/MVT.2017.2647814.
10. H. Giannopoulos, “Controller Area Network Frame Override,” US 2019 / 0098047 A1, 2019.
11. K. Tindell, “CANHack Git Repo,” Github.com, 2021. *https://github.com/kentindell/canhack* (accessed Feb. 11, 2021).
12. ISO/TC 22/SC 31, “ISO 16845-1:2016 - Road vehicles -- Controller area network (CAN) conformance test plan -- Part 1: Data link layer and physical signalling,” ISO. p. 126, 2106, Accessed: Sep. 18, 2017. [Online]. Available: *https://www.iso.org/standard/59166.html*.
13. M. Farsi, K. Ratcliff, and M. Barbosa, “An overview of controller area network,” Comput. Control Eng. J., vol. 10, no. 3, pp. 113–120, 1999, doi: 10.1049/cce:19990304.
14. National Instruments, “Controller Area Network (CAN) Overview,” ni.com, 2014. *http://www.ni.com/white-paper/2732/en/* (accessed Jul. 10, 2018).
15. K. Tindell, “Introducing the CANHack toolkit,” Github.io, 2020. *https://kentindell.github.io/2020/01/20/canhack-toolkit/* (accessed Feb. 11, 2021).
16. ISO/TC 22/SC 31, “ISO 11898-1:2015: Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signaling,” ISO 11898-1:2015. p. 65, 2015, Accessed: Jan. 01, 2017. [Online]. Available: *https://www.iso.org/standard/63648.html*.

The Right Tool for the Job – Information Management at Brigade and Below

By Capt. Stephen Willson, Analytic Support Officer, 1st Cyber Battalion, Cyber Protection Brigade

AT BRIGADE AND BELOW LEVELS across the Army, many processes require information management. The Army heavily relies on the Microsoft Office suite of products to support these daily processes. Word, Excel, and PowerPoint provide flexibility to accomplish a wide range of tasks; however, they are generic data manipulation tools combining both data storage and presentation and limiting programmatic interaction. When using these tools to process information, leaders supply external administrative guidance to specify how the data should be stored and presented. These products allow flexible data entry but that often leads to inconsistencies when aggregating information from multiple elements. Using these tools to manage routine processes takes a significant amount of time, is prone to human error, and may not provide a commander clear information for decision-making.

In this article, I will present a data centric tool approach where a reusable custom tool is designed and developed to provide leaders with relevant and useful information.

Current Process

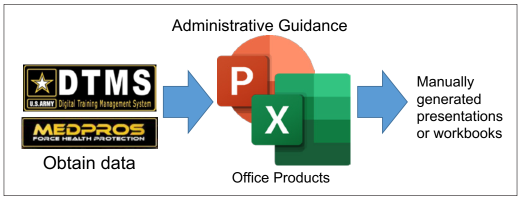


Figure 1: Current Process.

Many personnel across the Army work to streamline routine processes and develop solutions that often deal with Excel or PowerPoint coupled with guidance such as a standard operating procedure or a 'how to' guide. Subordinate units manually extract data from an authoritative data source (examples include DTMS for training statistics or MEDPROS for health information) and fill out an Excel workbook or update PowerPoint slides. Most units ask similar questions same questions of the data; questions such as "how many personnel are compliant with mandatory training," "what is the distribution of physical fitness levels as measured by the ACFT," and "what is the status of an award or evaluation." Data presented to leaders is extracted from an Army authoritative data source and then reformatted to match unit guidance. The process of generating the presented data is manually executed and often takes a considerable amount of time to compile.

To answer a common question such as the distribution of ACFT scores, the unit extracts data from the Army's Digital Training Management System to an Excel file to calculate statistics of scores based on the request. DTMS does not provide useful or configurable ways of visualizing stored data. This limitation requires the unit to manually generate reports for leadership.

Process Limitations

The main limitation to these processes is the time it takes to extract data, appropriately format the data, and then generate the data visualization. This time is not significant if only done a few times, but when this process is a part of regular status updates with visualizations, subordinate units are unable to keep up with requests. These requirements lead to long work hours or inaccurate data presentations. Another issue is human error. Extracting information from a system and then manually formatting the data may introduce accidental inaccuracies. The unit must always check to ensure that the standard process was executed. When an inaccurate Excel workbook or PowerPoint slide is presented, leaders lose clarity of the situation and may question other data presented by the unit. This lack of situational understanding by leadership contributes to frustration from both the subordinate and higher units when they cannot focus on what is truly important to their mission. A final issue is the inability to quickly present complex visualizations. Plotting ACFT scores by age is trivial, but more complex presentations are often done manually and result in a tedious process that is not easy or quick to repeat. Showing higher units the 'easy' graphs provides some value, but more complex graphs may be required to clearly convey situational understanding.

Proposed Process

Units across the Army have access to computers that at a minimum run the Microsoft Office suite of tools as well as a web-browser. Custom web pages can be created to support routine processes. Web browsers allow a unit to enter information and then present it in a custom command directed way. With this process, the unit maintains full control of the structure of the presentation and command guidance can be captured within the processing logic of the web page to ensure that the information displayed answers the commander's questions. Data should be stored in a structured format such as JavaScript Object Notation (JSON). Structured data can be sent from a subordinate unit to higher echelons and then aggregated and displayed in a pre-formatted way.

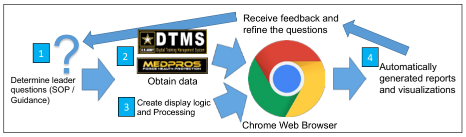

1
Determine leader questions (SOP / Guidance)
2
DTMS
MEDPROS
Obtain data
3
Create display logic and Processing
Chrome Web Browser
Receive feedback and refine the questions
4
Automatically generated reports and visualizations

Figure 2: Proposed Process.

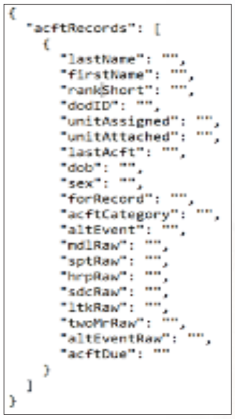
The proposed step by step process is:

1. Determine leader questions
2. Obtain data (format and fields)
3. Create display logic and processing (HTML file)
4. Automatically generate reports and visualizations, receive feedback, and refine the process (go to step 1)

Application of the Process – ACFT Tracking

1. Determine leader questions

The Army Combat Fitness Test is a six-event physical fitness assessment that all Soldiers are required to take unless medically exempt. For this physical assessment, leaders commonly ask about ACFT failures, high scores, and observed trends. Additionally, leaders may ask about ACFT scores by sex, plotted by age per event. This question generates 12 individual plots of data. While generating these data plots is manually possible, it is time consuming and tedious. Additionally, this information is more valuable when an organization aggregates its data from subordinate units.



```
{
  "acftRecords": [
    {
      "lastName": "",
      "firstName": "",
      "rankShort": "",
      "dodID": "",
      "unitAssigned": "",
      "unitAttached": "",
      "lastAcft": "",
      "dob": "",
      "sex": "",
      "forRecord": "",
      "acftCategory": "",
      "altEvent": "",
      "mdlRaw": "",
      "sptRaw": "",
      "hrpRaw": "",
      "sdcRaw": "",
      "ltkRaw": "",
      "twoMrRaw": "",
      "altEventRaw": "",
      "acftDue": ""
    }
  ]
}
```

Figure 3: ACFT JSON Data Structure

2. Obtain data

Army units are required to store ACFT data in DTMS. This information can be extracted to an Excel file with common columns. The Once exported, the individual records may be extracted to consist of the fields in Figure 3. In the browser-based tool, the data is stored in a JavaScript Object Notation (JSON) format. The JSON format provides a quick way to parse and manipulate the data to allow for programmatic interaction.

3. Create display logic and processing

To support ACFT tracking, a web browser based HTML file was created, "ACFT Tracker." The code is available on DISA DevForce (https://gitlab.devforce.disa.mil/cpb/admin-tools/acft-tracker). The 'index.html' file may be copied to a local workstation and used to capture and process ACFT results. This capability allows a user to import DTMS data and then display summary statistics or a summary plot of the data. This capability can be run from an internet connected computer or hosted on an internal SharePoint page to allow a unit to maintain control of the information presentation. This capability may be hosted on a web-server for mass distribution.

4. Automatically generate reports and visualizations

When using a web-page information processing capability the information is presented in a repeatable, highly structured format. The presentation can be tailored to the leader's specification, but unless modified data will always be presented in the same way. This benefit allows a subordinate unit to 'get it right once' and then use that presentation format. Once the data is presented, leaders may have ways to improve the visualization and these improvements may lead to new questions being asked. These enhancements can be captured and added as a capability for the display tool. This iterative process ensures that the subordinate unit receives feedback and responds to leader guidance. It also creates a dialogue between subordinate leaders as to what information is important and the meaning of that information.

Summary

Army units have the ability to significantly improve the quality of their reports while at the same time reducing the time spent summarizing data to provide situational understanding to leaders. The critical step is codifying the process and establishing a responsive venue for leaders to provide feedback. Leadership must provide the context for what is important to direct unit reporting. With a feedback loop between leader questions and data presentation, the unit can capture the guidance and repeatedly answer emerging questions quickly as new data is generated. To enable this process, subordinate units must get the data into a format that can be used by aggregation tools. With this process implemented subordinate units can focus on training and interpreting training results, not generating visualizations of training results.

Note: Special thanks to Chief Warrant Officer 3 Jakob Kaivo for his work on the WRWG JQR Data Entry Tool.

SUNBURST: Domain Generating Algorithm/ Domain Name Service Analysis

By Sgt. 1st Class Paul W. Murphy, Maj. Robert T. Qi, Capt. Eric J. Lu, Cyber Protection Brigade

THIS IS A TECHNICAL WHITE PAPER intended for consumption by cyber warfare professionals. The analysis reflected in this white paper would not have been possible without the Persistent Cyber Training Environment (PCTE). The analysis presented herein describes how analysts may identify how SUNBURST uses domain generated algorithms (DGA) as a domain name service (DNS) technique to target a victim SolarWinds host. Specifically, DNS requests with an encoded subdomain for avsvmcloud[.]com can be decoded to indicate whether the malicious cyber actor (MCA) was actively targeting a victim SolarWinds host at the time the DNS request was sent. Due to the differences in DGA DNS requests during SUNBURST's different modes, an analyst may determine which mode SUNBURST was in based on DNS logs.

While in passive mode, SUNBURST DGA generates the subdomain portion of the DNS request using a uniquely generated GUID + the victim's domain. While in active mode, SUNBURST's DGA generates the subdomain portion of the DNS request using the GUID + 3-byte timestamp + a 2-byte bitmap indicating status of several security software on the victim host. Moreover, SUNBURST embeds a 1-bit flag in the 3-byte timestamp to notify the MCA that SUNBURST is ready to begin HTTPS C2. If DNS response logs are available, a CNAME response to the victim SolarWinds host can corroborate this indicator. If response logs are not available, we can, at a minimum, identify whether the MCA has attempted to initiate HTTPS C2 for hands-on operation on the victim SolarWinds host.

To summarize, there are currently four known DNS-based indicators which can be used to identify whether the MCA actively attempted to initiate an HTTPS C2 connection with an infected SolarWinds host. All indicators require DNS response logs for detection.

- A DNS response containing a CNAME record after a DNS request is made for avsvmcloud[.]com.
- A DNS response containing an A record in the block of IPs that match "NetBios with CNAME flag set to True" after a DNS request is made for avsvmcloud[.]com.
- A DNS request for avsvmcloud[.]com contains 2-bytes at the end of the DGA consisting of a bitmask indicating existence of AV and security software status instead of an encoded domain name.
- A DNS request for avsvmcloud[.]com with the least-significant-bit the timestamp set to 1 (true).

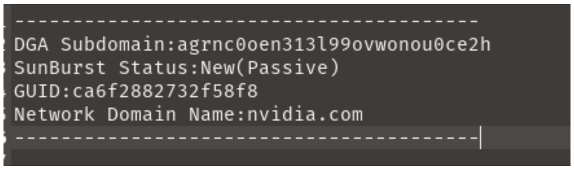
The presence of any of these indicators strongly suggests an attempt to establish an active HTTPS C2 connection.

SUNBURST Operational States

The SUNBURST backdoor possesses three operational states within its configuration file which is controlled by the key "ReportWatcherRetry." The DGA DNS requests sent out by SUNBURST are modified depending on its operational state. SUNBURST operates differently under each of the three states.

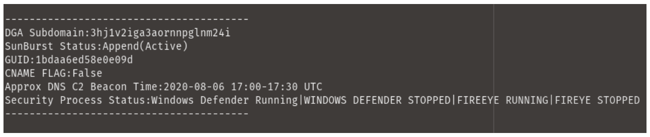
- NEW: Passive mode, also known as the initial state. SUNBURST sends encoded DGA DNS request to avsvmcloud consisting of "GUID + domain". The MCA likely monitored these queries to select targets to conduct follow on operations. ReportWatcherRetry value = 4
- APPEND: Active mode. Resolution of CNAME has likely occurred to final C2 HTTPS server if SUNBURST receives an order to set a "CNAME ready flag" to True. Otherwise, SUNBURST continues to send DGA DNS queries to the C2 coordinator consisting of a GUID + timestamp and a list of interesting processes (AV and security software status). ReportWatcherRetry value = 5
- TRUNCATE: Deactivated, no longer performs network activity and exits immediately after execution. ReportWatcherRetry value = 3

  Examples of decoded DGA DNS requests while in NEW and APPEND operational statuses are presented in figures 1 and 2 below.



```
--------------------------------------
DGA Subdomain:agrnc0oen313l99ovwonou0ce2h
SunBurst Status:New(Passive)
GUID:ca6f2882732f58f8
Network Domain Name:nvidia.com
--------------------------------------
```

Figure 1: Decoded SUNBURST DGA DNS requests while in the "NEW" status, consists of GUID + Domain.



```
----------------------------------------
DGA Subdomain:3hj1v2iga3aornnpglnm24i
SunBurst Status:Append(Active)
GUID:1bdaa6ed58e0e09d
CNAME FLAG:False
Approx DNS C2 Beacon Time:2020-08-06 17:00-17:30 UTC
Security Process Status:Windows Defender Running|WINDOWS DEFENDER STOPPED|FIREEYE RUNNING|FIREYE STOPPED
----------------------------------------
```

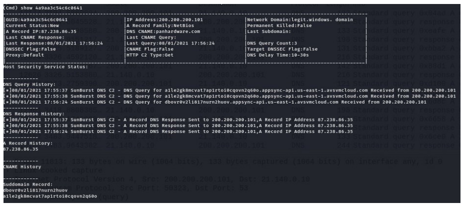
Figure 2: Decoded SUNBURST DGA DNS requests while in "APPEND" status, consists of GUID + timestamp + interesting processes.

Switching Operational States

It is possible for the SUNBURST backdoor to switch between operational states. Since the MCA has full control of the DNS response, it has the ability to send an A record response of its choosing to modify the backdoor's behavior and the state in which it is running. Therefore, checking the configuration file for the key "ReportWatcherRetry", which the SUNBURST backdoor uses to track the current operational status, may not be sufficient to tell if the backdoor was historically active. Instead, checking the CNAME responses and DNS A record IP address responses over time is the preferred method for providing fidelity on whether the MCA conducted follow on activities.

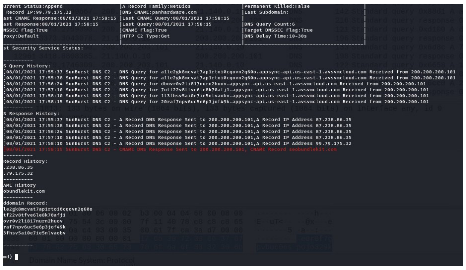
Cyber Threat Emulation

The PCTE allows cyber operators to fully simulate SUNBURST in its different operational states, utilizing both the DNS and HTTPS backdoor with full functionality. Without PCTE, the analysis that follows would not have been possible. Figures 3 through 6 below illustrate simulation results.



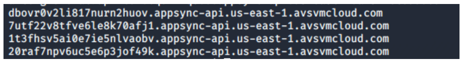
```
(Cmd) show 4a9aa3c54c6c0641
------------------------------------------------------------------------------------------------------------
|GUID:4a9aa3c54c6c0641                 |IP Address:200.200.200.101            |Network Domain:legit.windows. domain  |
|Current Status:New                    |A Record Family:NetBios               |Permanent Killed:False                |
|A Record IP:87.238.86.35              |DNS CNAME:panhardware.com             |Last Subdomain:                       |
|Last CNAME Response:                  |Last CNAME Query:                     |                                      |
|Last Response:08/01/2021 17:56:24     |Last Query:08/01/2021 17:56:24        |DNS Query Count:3                     |
|DNSSEC Flag:False                     |CNAME Flag:False                      |Target DNSSEC Flag:False              |
|Proxy:Default                         |HTTP C2 Type:Get                      |DNS Delay Time:10-30s                 |
|______________________________________|______________________________________|______________________________________|
Host Security Service Status:

----------
DNS Query History:
[*]08/01/2021 17:55:37 SunBurst DNS C2 - DNS Query for a1le2gk8mcvat7ap1rtoi0cqovn2q60o.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
[*]08/01/2021 17:55:38 SunBurst DNS C2 - DNS Query for a1le2gk8mcvat7ap1rtoi0cqovn2q60o.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
[*]08/01/2021 17:56:24 SunBurst DNS C2 - DNS Query for dbovr0v2li817nurn2huov.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
----------
DNS Response History:
[*]08/01/2021 17:55:37 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
[*]08/01/2021 17:55:38 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
[*]08/01/2021 17:56:24 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
----------
A Record History:
87.238.86.35

----------
CNAME History

----------
Suddomain Record:
dbovr0v2li817nurn2huov
a1le2gk8mcvat7ap1rtoi0cqovn2q60o
```

Figure 3: Victim SolarWinds host checking in with its DGA DNA requests; the Cyber Threat Emulator (CTE) operator has set the next A record response to transition SUNBURST into APPEND status.



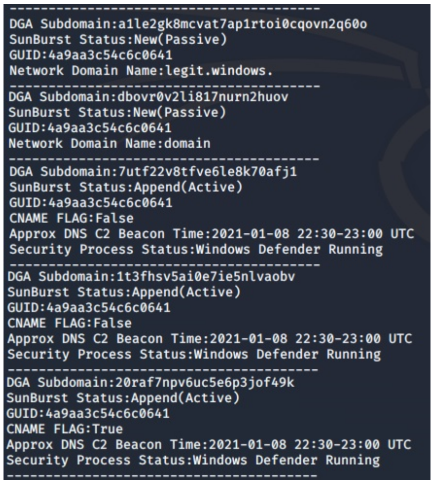
```
urrent Status:Append                  |A Record Family:NetBios               |Permanent Killed:False                |
 Record IP:99.79.175.32               |DNS CNAME:panhardware.com             |Last Subdomain:                       |
ast CNAME Response:08/01/2021 17:58:15 |Last CNAME Query:08/01/2021 17:58:15  |                                      |
ast Response:08/01/2021 17:58:15      |Last Query:08/01/2021 17:58:15        |DNS Query Count:6                     |
NSSEC Flag:True                       |CNAME Flag:True                       |Target DNSSEC Flag:True               |
roxy:Default                          |HTTP C2 Type:Get                      |DNS Delay Time:10-30s                 |
______________________________________|______________________________________|______________________________________|
st Security Service Status:

----------
S Query History:
]08/01/2021 17:55:37 SunBurst DNS C2 - DNS Query for a1le2gk8mcvat7ap1rtoi0cqovn2q60o.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
]08/01/2021 17:55:38 SunBurst DNS C2 - DNS Query for a1le2gk8mcvat7ap1rtoi0cqovn2q60o.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
]08/01/2021 17:56:24 SunBurst DNS C2 - DNS Query for dbovr0v2li817nurn2huov.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
]08/01/2021 17:57:10 SunBurst DNS C2 - DNS Query for 7utf22v8tfve6le8k70afj1.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
]08/01/2021 17:58:10 SunBurst DNS C2 - DNS Query for 1t3fhsv5ai0e7ie5nlvaobv.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
]08/01/2021 17:58:15 SunBurst DNS C2 - DNS Query for 20raf7npv6uc5e6p3jof49k.appsync-api.us-east-1.avsvmcloud.com Received from 200.200.200.101
----------
S Response History:
]08/01/2021 17:55:37 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
]08/01/2021 17:55:38 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
]08/01/2021 17:56:24 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
]08/01/2021 17:57:10 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 87.238.86.35
]08/01/2021 17:58:10 SunBurst DNS C2 - A Record DNS Response Sent to 200.200.200.101,A Record IP Address 99.79.175.32
]08/01/2021 17:58:15 SunBurst DNS C2 - CNAME DNS Response Sent to 200.200.200.101, CNAME Record seobundlekit.com
----------
Record History:
.238.86.35
.79.175.32
----------
AME History
obundlekit.com
----------
ddomain Record:
le2gk8mcvat7ap1rtoi0cqovn2q60o
tf22v8tfve6le8k70afj1
ovr0v2li817nurn2huov
raf7npv6uc5e6p3jof49k
3fhsv5ai0e7ie5nlvaobv
----------

md) ▋
```

Figure 4: Victim SolarWinds Host in the APPEND status; CNAME has been set and returned to tell SUNBURST to initiate follow on HTTPS C2 to the identified domain.



```
dbovr0v2li817nurn2huov.appsync-api.us-east-1.avsvmcloud.com
7utf22v8tfve6le8k70afj1.appsync-api.us-east-1.avsvmcloud.com
1t3fhsv5ai0e7ie5nlvaobv.appsync-api.us-east-1.avsvmcloud.com
20raf7npv6uc5e6p3jof49k.appsync-api.us-east-1.avsvmcloud.com
```

Figure 5: All DGA DNS requests sent to the C2 coordinator from "NEW" state to the "APPEND" state as aggregated from Cyber Threat Emulation session illustrated in figures 3 and 4.



```
----------------------------------------
DGA Subdomain:a1le2gk8mcvat7ap1rtoi0cqovn2q60o
SunBurst Status:New(Passive)
GUID:4a9aa3c54c6c0641
Network Domain Name:legit.windows.
----------------------------------------
DGA Subdomain:dbovr0v2li817nurn2huov
SunBurst Status:New(Passive)
GUID:4a9aa3c54c6c0641
Network Domain Name:domain
----------------------------------------
DGA Subdomain:7utf22v8tfve6le8k70afj1
SunBurst Status:Append(Active)
GUID:4a9aa3c54c6c0641
CNAME FLAG:False
Approx DNS C2 Beacon Time:2021-01-08 22:30-23:00 UTC
Security Process Status:Windows Defender Running
----------------------------------------
DGA Subdomain:1t3fhsv5ai0e7ie5nlvaobv
SunBurst Status:Append(Active)
GUID:4a9aa3c54c6c0641
CNAME FLAG:False
Approx DNS C2 Beacon Time:2021-01-08 22:30-23:00 UTC
Security Process Status:Windows Defender Running
----------------------------------------
DGA Subdomain:20raf7npv6uc5e6p3jof49k
SunBurst Status:Append(Active)
GUID:4a9aa3c54c6c0641
CNAME FLAG:True
Approx DNS C2 Beacon Time:2021-01-08 22:30-23:00 UTC
Security Process Status:Windows Defender Running
----------------------------------------
```

Figure 6: DGA DNS requests decoded from the CTE session. Note that the first two requests only return the unique id and domain since SUNBURST was in its "NEW" operational state. Once transitioned into the "APPEND" state, the process information is contained within the DNS requests. In this case, Windows Defender was running on the SolarWinds host.

Technical Analysis

SUNBURST utilizes a DGA to vary DNS requests to its C2 coordinator domain, avsvmcloud[.]com, which is a MCA-controlled DNS server that likely controls the SUNBURST backdoor. When communicating with the C2 coordinator, SUNBURST continuously sends DGA DNS requests and uses a two-part C2 construct involving both DNS and HTTPS. Victim SolarWinds hosts send DNS queries to a DGA subdomain belonging to one of four C2 coordinator servers, listed below, for operational status updates and/or to resolve and determine its final C2 domain for follow on activity over HTTPS.

- appsync-api.eu-west-1[.]avsvmcloud[.]com
- appsync-api.us-west-2[.]avsvmcloud[.]com
- appsync-api.us-east1[.]avsvmcloud[.]com
- appsync-api.us-east-2[.]avsvmcloud[.]com

If the C2 coordinator responds with a DNS A record IP address, SUNBURST checks the resolved address against a hard-coded list of IP address blocks. If the address falls within an identified IP address block, the backdoor transitions into its associated state. After certain predefined checks, the backdoor starts in the "NEW" state where it generates a subdomain using "GUID +part of network domain" and beacons via DNS expecting to receive a state-changing response. While the DNS beacon is in "NEW" or "APPEND" states, the thread that performs DNS beaconing exits immediately if it received any address other than the ones in the NetBios address family. The thread also exits after three beacon attempts if no DNS response is received. If the DNS beaconing thread exits, SUNBURST will not send another DNS request until either the routine SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInternal invokes the SUNBURST code when the Inventory Manager plug-in is loaded or the SolarWinds Orion Module Engine service is restarted. If SUNBURST is the "APPEND" status, it will communicate via HTTPS when the CNAME ready flag is set to true or idles for 30 minutes to 30 days, which is configurable, before it sends another DNS beacon. The third state is "TRUNCATE", in which the malware is terminated and the C2 operator turns on the kill switch by setting the ReportWatcherRetry key to 3.

If the C2 operator transitions the victim SolarWinds host to the "APPEND" state and responds with a CNAME from the DGA DNS request, SUNBURST uses the returned CNAME domain from the response to initiate HTTPS C2 communications. If analysts observe CNAME resolutions from DNS requests to avsvmcloud[.]com, it is highly likely that the MCA initiated follow-on C2 within the environment. See appendix 1 for full list of known HTTPS C2 Domain names.

DNS A Record Response and State Transitions

If the DNS A record response falls within the following subnet ranges, SUNBURST enters the "APPEND" state. Additionally, if the CNAME ready flag is set to true, a DNS CNAME response can be expected following the next DNS request. Upon receipt of the CNAME DNS response, SUNBURST will initiate C2 communication via HTTPS protocol to the domain specified in the CNAME response. In the HTTP C2 stage, SUNBURST can receive detailed commands such as "RunTask" which allows the execution of an arbitrary command. For the subnets with the CNAME ready flag set to true, the third and fourth notation from the A record IP address are parsed to obtain configuration data such as the proxy method, HTTP headers, the URI scheme, and a delay value. See appendices 2 through 4 for additional details. DGA DNS request beaconing will continue to the C2 coordinator and will consist of the GUID + timestamp and a list of processes (AV and security software status) encoded in the DGA subdomain string. This status is identified as "NetBios" in the decompiled C# as presented in figure 7 below.

- CNAME ready flag set to true on following DGA DNS request for the following subnets:
  18.130.0.0/16
  99.79.0.0/16
  184.72.0.0/15
- State is set to "APPEND" and idles for the following subnets:
  87.238.80.0/21
  8.18.144.0/23
  71.152.53.0/24

If the C2 coordinator DNS A record response falls within subnet ranges listed below, SUNBURST will set the ReportWatcherRetry key to 4 or "NEW" if ReportWatcherRetry was previously set to 5 or "APPEND". DNS A record responses that fall within these subnet ranges will also cause the SUNBURST thread to exit, however it will be called again by the parent process and the DGA beaconing will continue in the status "NEW". DGA DNS beaconing to the C2 coordinator in the "NEW" state consists of the "GUID + domain" encoded in the DGA subdomain string which can receive updates to its state via subsequent DNS IP A record responses. This state is identified as "Ipx" in the decompiled C#.

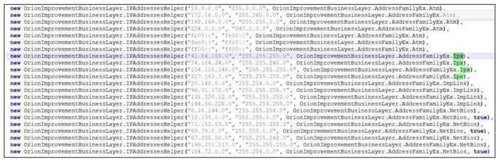
41.84.159.0/24
99.79.0.0/16
184.72.0.0/15
199.201.117.0/24

If the C2 coordinator DNS A record response falls within the following subnet ranges, SUNBURST will terminate and update the configuration key "ReportWatcherRetry" to the value of 3 or "TRUNCATE". This prevents further execution and ends all network activity. This state is identified as "Atm" and "ImpLink" in the decompiled C#.

10.0.0.0/8
192.168.0.0/16
20.140.0.0/15
96.31.172.0/24
131.228.12.0/22
144.86.226.0/24

224.0.0.0/3
fc00:: - fe00::
fec0:: - ffc0::
ff00:: - ff00::

Constructing the DGA Subdomain



```
new OrionImprovementBusinessLayer.IPAddressesHelper("10.0.0.0", "255.0.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("172.16.0.0", "255.240.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("192.168.0.0", "255.255.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("224.0.0.0", "240.0.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("fc00::", "fe00::", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("fec0::", "ffc0::", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("ff00::", "ff00::", OrionImprovementBusinessLayer.AddressFamilyEx.Atm),
new OrionImprovementBusinessLayer.IPAddressesHelper("41.84.159.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.Ipx),
new OrionImprovementBusinessLayer.IPAddressesHelper("74.114.24.0", "255.255.248.0", OrionImprovementBusinessLayer.AddressFamilyEx.Ipx),
new OrionImprovementBusinessLayer.IPAddressesHelper("154.118.140.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.Ipx),
new OrionImprovementBusinessLayer.IPAddressesHelper("217.163.7.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.Ipx),
new OrionImprovementBusinessLayer.IPAddressesHelper("20.140.0.0", "255.254.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.ImpLink),
new OrionImprovementBusinessLayer.IPAddressesHelper("96.31.172.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.ImpLink),
new OrionImprovementBusinessLayer.IPAddressesHelper("131.228.12.0", "255.255.252.0", OrionImprovementBusinessLayer.AddressFamilyEx.ImpLink),
new OrionImprovementBusinessLayer.IPAddressesHelper("144.86.226.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.ImpLink),
new OrionImprovementBusinessLayer.IPAddressesHelper("8.18.144.0", "255.255.254.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios),
new OrionImprovementBusinessLayer.IPAddressesHelper("18.130.0.0", "255.255.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios, true),
new OrionImprovementBusinessLayer.IPAddressesHelper("71.152.53.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios),
new OrionImprovementBusinessLayer.IPAddressesHelper("99.79.0.0", "255.255.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios, true),
new OrionImprovementBusinessLayer.IPAddressesHelper("87.238.80.0", "255.255.248.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios),
new OrionImprovementBusinessLayer.IPAddressesHelper("199.201.117.0", "255.255.255.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios),
new OrionImprovementBusinessLayer.IPAddressesHelper("184.72.0.0", "255.254.0.0", OrionImprovementBusinessLayer.AddressFamilyEx.NetBios, true)
```

Figure 7: Decompiled C# identifying IP blocks.

Depending on the state of SUNBURST, it uses different methods to create the DGA for the subsequent DNS requests to the C2 coordinator. The DGA is generated from four functions within OrionImprovementBusinessLayer.CryptoHelper and encoded with five additional functions as listed below. The Four DGA generation functions are:

- GetNextStringEx()
- GetNextString()
- GetPreviousString()
- GetCurrentString()

The additional nested encoding functions are:

- CreateSecureString()
- CreateString()
- DecryptShort()
- Base64Decode()
- Base64Encode()

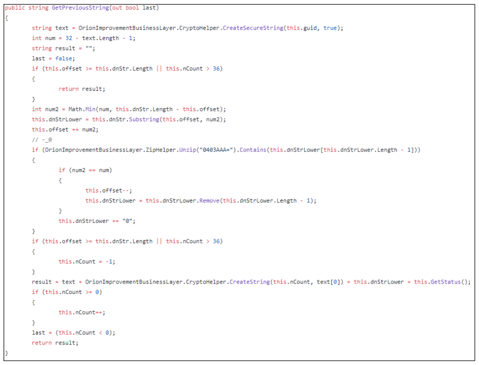
Globally Unique Identifiers

SUNBURST generates the GUID contained in both the "NEW" and "APPEND" states by concatenating the first active network interface MAC address that is not a loopback device, the domain name, and the registry value located in the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid. SUNBURST then MD5 hashes the concatenated string and packs the hash into an 8-byte array using the XOR operation for overlapping bytes. The CreateSecureString() function then "encrypts" this hash using XOR with a random key which is prepended to the GUID. The XOR key and the XOR'ed GUID is then finally base32 encoded into what makes up the first 16-bytes of every DGA DNS request (9-bytes when decoded, the first byte is the XOR key and the remaining 8-bytes make up the GUID).

DGA Status: NEW

In the SUNBURST "NEW" state, GetCurrentString() and GetPreviousString() are called to create the second part of the DGA subdomain DNS request consisting of the domain through the variables dnStr and dnStrLower, then encoded with CreateSecureString(). See figure 8 on the following page.

DGA Status: APPEND



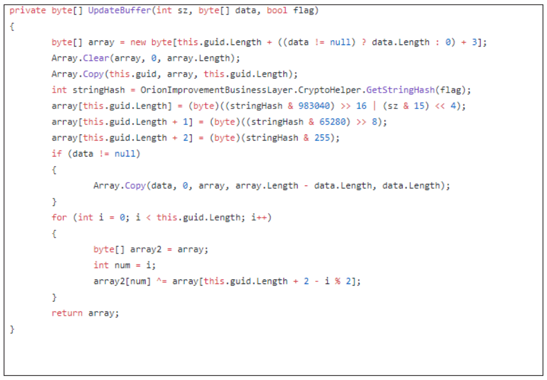
```
public string GetPreviousString(out bool last)
{
        string text = OrionImprovementBusinessLayer.CryptoHelper.CreateSecureString(this.guid, true);
        int num = 32 - text.Length - 1;
        string result = "";
        last = false;
        if (this.offset >= this.dnStr.Length || this.nCount > 36)
        {
                return result;
        }
        int num2 = Math.Min(num, this.dnStr.Length - this.offset);
        this.dnStrLower = this.dnStr.Substring(this.offset, num2);
        this.offset += num2;
        // -_0
        if (OrionImprovementBusinessLayer.ZipHelper.Unzip("0403AAA=").Contains(this.dnStrLower[this.dnStrLower.Length - 1]))
        {
                if (num2 == num)
                {
                        this.offset--;
                        this.dnStrLower = this.dnStrLower.Remove(this.dnStrLower.Length - 1);
                }
                this.dnStrLower += "0";
        }
        if (this.offset >= this.dnStr.Length || this.nCount > 36)
        {
                this.nCount = -1;
        }
        result = text + OrionImprovementBusinessLayer.CryptoHelper.CreateString(this.nCount, text[0]) + this.dnStrLower + this.GetStatus();
        if (this.nCount >= 0)
        {
                this.nCount++;
        }
        last = (this.nCount < 0);
        return result;
}
```

Figure 8: Decompiled GetCurrentString() and GetPreviousString() code.

In the SUNBURST "APPEND" state, SUNBURST class GetNextStringEX() and GetNextString() create the second part of the DGA DNS request. In this state, SUNBURST gathers the status of AV and/or security software and puts it into a 2-byte bitmap using UpdateBuffer().

SUNBURST then sends this bitmap in the second part of the DGA DNS request to the C2 coordinator. A DGA DNS request in the APPEND status consists of a 1-byte XOR key, 8-byte GUID data, + 3-byte timestamp, and + 2-byte security software processes and status.

Additional technical analysis of the decompiled code revealed that there is a flag set in the least significant bit in the 3-byte timestamp created in the GetStringHash() function and packed into 3-bytes in the UpdateBuffer() function while SUNBURST is in the "APPEND" state. This flag notifies the C2 coordinator that SUNBURST is ready to receive a CNAME to start HTTPS C2. SUNBURST will not use the CNAME record and move to the HTTP stage but will run into an "error" state if it receives a CNAME when the "CNAME Is Ready" flag is not set to True. Hence, this flag can tell us if SUNBURST did in fact request a CNAME to be sent from the C2 coordinator by simply analyzing DNS request logs. Again, the CNAME flag is located in the least significant bit in the 3-byte timestamp of an APPEND status DGA DNS request and is highlighted in figure 9 below.



```
private byte[] UpdateBuffer(int sz, byte[] data, bool flag)
{
        byte[] array = new byte[this.guid.Length + ((data != null) ? data.Length : 0) + 3];
        Array.Clear(array, 0, array.Length);
        Array.Copy(this.guid, array, this.guid.Length);
        int stringHash = OrionImprovementBusinessLayer.CryptoHelper.GetStringHash(flag);
        array[this.guid.Length] = (byte)((stringHash & 983040) >> 16 | (sz & 15) << 4);
        array[this.guid.Length + 1] = (byte)((stringHash & 65280) >> 8);
        array[this.guid.Length + 2] = (byte)(stringHash & 255);
        if (data != null)
        {
                Array.Copy(data, 0, array, array.Length - data.Length, data.Length);
        }
        for (int i = 0; i < this.guid.Length; i++)
        {
                byte[] array2 = array;
                int num = i;
                array2[num] ^= array[this.guid.Length + 2 - i % 2];
        }
        return array;
}
```

Figure 9: Decompiled GetNextStringEX(), GetNextString(), GetStringHash(), UpdateBuffer() Code

Decoding DGA DNS Requests

Scripts are available to decode both types of DGA DNS requests. If requested, these scripts enable further analysis of the encoding and decoding functions. Please contact usarmy.gordon.cyber-pro-bde.list.ops@mail.mil for the scripts.

Conclusion

The MCA uses the DNS DGA encoding scheme to change the operational state of the SUNBURST backdoor. As a result, analysts can confirm or deny adversary interaction with a SolarWinds host with a high degree of confidence solely based on DNS request or response logs. The confidence level of this analysis depends on complete log coverage for a particular host, and the confidence level will drop based on missing data. As presented in figure 10, with both DNS request and response data an analyst can confidently assess the state in which SUNBURST was operating. Even if restricted solely to DNS requests or responses, an analyst can still determine if SUNBURST was passively beaconing (in the "NEW" state) or set to active (in the "APPEND" state), including if SUNBURST was requested to initiate HTTPS C2.

CUI Sunburst: Domain Generating Algorithm/Domain Name Service Analysis

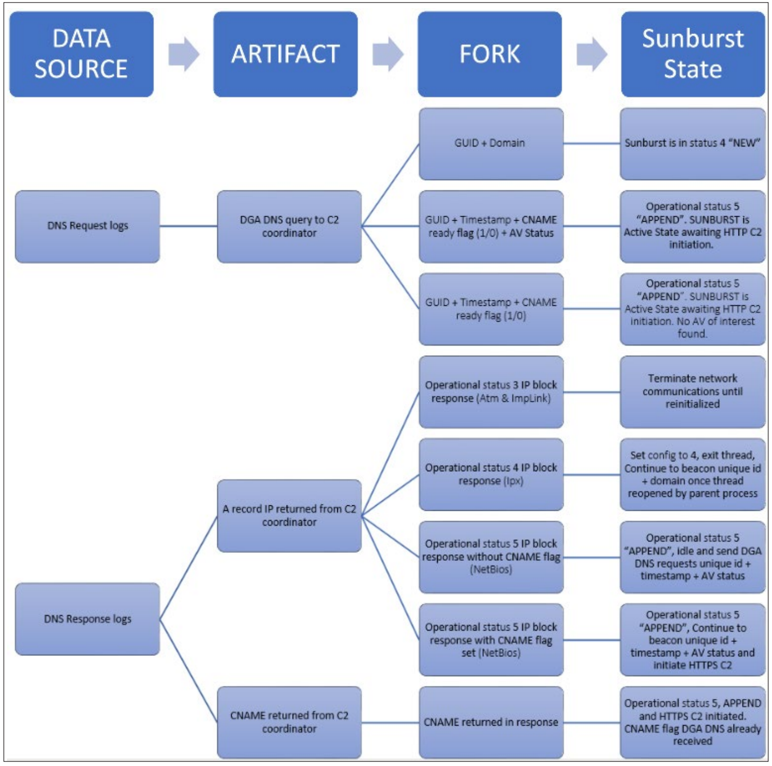
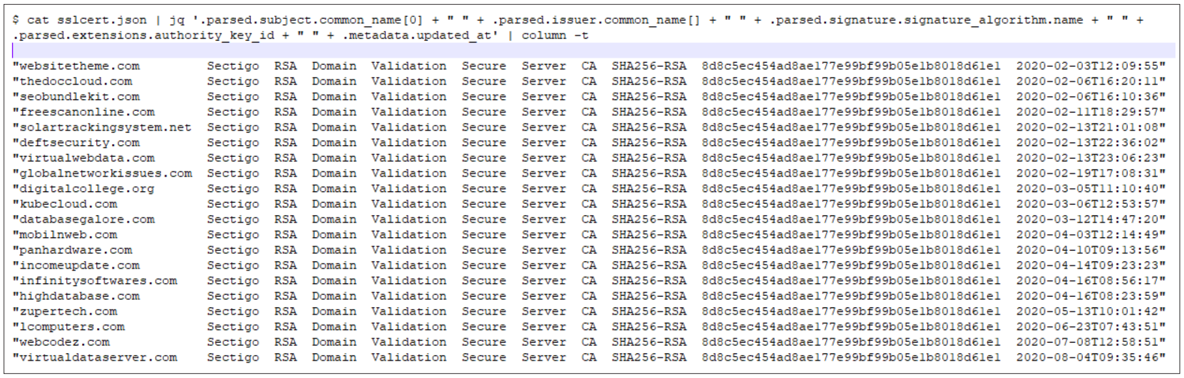

DATA SOURCE
ARTIFACT
FORK
Sunburst State
DNS Request logs
DGA DNS query to C2 coordinator
GUID + Domain
Sunburst is in status 4 "NEW"
GUID + Timestamp + CNAME ready flag (1/0) + AV Status
Operational status 5 "APPEND". SUNBURST is Active State awaiting HTTP C2 initiation.
GUID + Timestamp + CNAME ready flag (1/0)
Operational status 5 "APPEND". SUNBURST is Active State awaiting HTTP C2 initiation. No AV of interest found.
DNS Response logs
A record IP returned from C2 coordinator
Operational status 3 IP block response (Atm & ImpLink)
Terminate network communications until reinitialized
Operational status 4 IP block response (Ipx)
Set config to 4, exit thread, Continue to beacon unique id + domain once thread reopened by parent process
Operational status 5 IP block response without CNAME flag (NetBios)
Operational status 5 "APPEND", idle and send DGA DNS requests unique id + timestamp + AV status
Operational status 5 IP block response with CNAME flag set (NetBios)
Operational status 5 "APPEND", Continue to beacon unique id + timestamp + AV status and initiate HTTPS C2
CNAME returned from C2 coordinator
CNAME returned in response
Operational status 5, APPEND and HTTPS C2 initiated. CNAME flag DGA DNS already received

Figure 10: Flow from artifact to determining the SUNBURST operational state.

Appendix 1 - Known C2 Domains From Open Source Reporting

Appendix 2 - DNS C2 Idle Time



```
$ cat sslcert.json | jq '.parsed.subject.common_name[0] + " " + .parsed.issuer.common_name[] + " " + .parsed.signature.signature_algorithm.name + " " +
.parsed.extensions.authority_key_id + " " + .metadata.updated_at' | column -t

"websitetheme.com          Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-03T12:09:55"
"thedoccloud.com           Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-06T16:20:11"
"seobundlekit.com          Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-06T16:10:36"
"freescanonline.com        Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-11T18:29:57"
"solartrackingsystem.net   Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-13T21:01:08"
"deftsecurity.com          Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-13T22:36:02"
"virtualwebdata.com        Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-13T23:06:23"
"globalnetworkissues.com   Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-02-19T17:08:31"
"digitalcollege.org        Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-03-05T11:10:40"
"kubecloud.com             Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-03-06T12:53:57"
"databasegalore.com        Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-03-12T14:47:20"
"mobilnweb.com             Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-04-03T12:14:49"
"panhardware.com           Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-04-10T09:13:56"
"incomeupdate.com          Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-04-14T09:23:23"
"infinitysoftwares.com     Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-04-16T08:56:17"
"highdatabase.com          Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-04-16T08:23:59"
"zupertech.com             Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-05-13T10:01:42"
"lcomputers.com            Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-06-23T07:43:51"
"webcodez.com              Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-07-08T12:58:51"
"virtualdataserver.com     Sectigo  RSA  Domain  Validation  Secure  Server  CA  SHA256-RSA  8d8c5ec454ad8ae177e99bf99b05e1b8018d61e1  2020-08-04T09:35:46"
```

*Note: All reported C2 domain SSL certificates were signed by the same Certificate Authority "C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA". Additional analysis of the domains, IPs and in what phase they were potentially used, can be found in the Talos intelligence article in the references section. **REFERENCE NOT IN THE REFERENCES SECTION***

4th Octet of an IP Address	DNS C2 Idle time
4 ,5 ,6 ,7 ,12 ,13 ,14 ,15 ,36 ,37 ,38 ,39 ,44 ,45 ,46 ,47 ,132 ,133 ,134 ,135 ,140 ,141 ,142 ,143 ,164 ,165 ,166 ,167 ,172 ,173 ,174 ,175	4-5 hours
16 ,17 ,18 ,19 ,24 ,25 ,26 ,27 ,48 ,49 ,50 ,51 ,56 ,57 ,58 ,59 ,144 ,145 ,146 ,147 ,152 ,153 ,154 ,155 ,176 ,177 ,178 ,179 ,184 ,185 ,186 ,187	8-10 hours
20 ,21 ,22 ,23 ,28 ,29 ,30 ,31 ,52 ,53 ,54 ,55 ,60 ,61 ,62 ,63 ,148 ,149 ,150 ,151 ,156 ,157 ,158 ,159 ,180 ,181 ,182 ,183 ,188 ,189 ,190 ,191	24-26 hours
64 ,65 ,66 ,67 ,72 ,73 ,74 ,75 ,96 ,97 ,98 ,99 ,104 ,105 ,106 ,107 ,192 ,193 ,194 ,195 ,200 ,201 ,202 ,203 ,224 ,225 ,226 ,227 ,232 ,233 ,234 ,235	72-96 hours (3-4 days)
68 ,69 ,70 ,71 ,76 ,77 ,78 ,79 ,100 ,101 ,102 ,103 ,108 ,109 ,110 ,111 ,196 ,197 ,198 ,199 ,204 ,205 ,206 ,207 ,228 ,229 ,230 ,231 ,236 ,237 ,238 ,239	167-169 hours (7 days)
80 ,81 ,82 ,83 ,88 ,89 ,90 ,91 ,112 ,113 ,114 ,115 ,120 ,121 ,122 ,123 ,208 ,209 ,210 ,211 ,216 ,217 ,218 ,219 ,240 ,241 ,242 ,243 ,248 ,249 ,250 ,251	335-337 hours (14 days)
84 ,85 ,86 ,87 ,92 ,93 ,94 ,95 ,116 ,117 ,118 ,119 ,124 ,125 ,126 ,127 ,212 ,213 ,214 ,215 ,220 ,221 ,222 ,223 ,244 ,245 ,246 ,247 ,252 ,253 ,254 ,255	719-721 hours (30 days)
0 ,1 ,2 ,3 ,8 ,9 ,10 ,11 ,32 ,33 ,34 ,35 ,40 ,41 ,42 ,43 ,128 ,129 ,130 ,131 ,136 ,137 ,138 ,139 ,160 ,161 ,162 ,163 ,168 ,169 ,170 ,171	30 minutes- 2 hours

Note: The SUNBURST DNS C2 has a default idle time between 30 minutes and 2 hours. When SUNBURST receives a DNS A Record response with an IP address falling within the NetBios group with CNAME flag, the 4th octet of the IP address will be used to set the idle time of the DNS C2 after the followed HTTP C2 session is created.

21

Appendix 3 - HTTP C2 Header and Content Format

4^{th} Octet of an IP Address	User Agent	C2 Beacon Content Format	C2 Response Content Format
8 ,9 ,10 ,11 ,12 ,13 ,14 ,15 ,24 ,25 ,26 ,27 ,28 ,29 ,30 ,31 ,40 ,41 ,42 ,43 ,44 ,45 ,46 ,47 ,56 ,57 ,58 ,59 ,60 ,61 ,62 ,63 ,72 ,73 ,74 ,75 ,76 ,77 ,78 ,79 ,88 ,89 ,90 ,91 ,92 ,93 ,94 ,95 ,104 ,105 ,106 ,107 ,108 ,109 ,110 ,111 ,120 ,121 ,122 ,123 ,124 ,125 ,126 ,127	SolarWindsOrionImprovementClient/[version number of OrionImprovement\\SolarWinds.OrionImprovement.exe] or SolarWindsOrionImprovementClient/3.0.0.382	OIP	Hexadecimal strings within XML data, which can be extracted using the regular expression "\{ [0-9a-f-]{ 36} \}"|"[0-9a-f]{ 32}"|"[0-9a-f]{ 16} "
128 ,129 ,130 ,131 ,132 ,133 ,134 ,135 ,144 ,145 ,146 ,147 ,148 ,149 ,150 ,151 ,160 ,161 ,162 ,163 ,164 ,165 ,166 ,167 ,176 ,177 ,178 ,179 ,180 ,181 ,182 ,183 ,192 ,193 ,194 ,195 ,196 ,197 ,198 ,199 ,208 ,209 ,210 ,211 ,212 ,213 ,214 ,215 ,224 ,225 ,226 ,227 ,228 ,229 ,230 ,231 ,240 ,241 ,242 ,243 ,244 ,245 ,246 ,247	No User Agent	INFLATE compressed raw bytes	Compressed raw bytes appended after 48 arbitrary bytes
136 ,137 ,138 ,139 ,140 ,141 ,142 ,143 ,152 ,153 ,154 ,155 ,156 ,157 ,158 ,159 ,168 ,169 ,170 ,171 ,172 ,173 ,174 ,175 ,184 ,185 ,186 ,187 ,188 ,189 ,190 ,191 ,200 ,201 ,202 ,203 ,204 ,205 ,206 ,207 ,216 ,217 ,218 ,219 ,220 ,221 ,222 ,223 ,232 ,233 ,234 ,235 ,236 ,237 ,238 ,239 ,248 ,249 ,250 ,251 ,252 ,253 ,254 ,255	Microsoft-CryptoAPI/[OS Version]	INFLATE compressed raw bytes	compressed raw bytes appended after 12 arbitrary bytes
0 ,1 ,2 ,3 ,4 ,5 ,6 ,7 ,16 ,17 ,18 ,19 ,20 ,21 ,22 ,23 ,32 ,33 ,34 ,35 ,36 ,37 ,38 ,39 ,48 ,49 ,50 ,51 ,52 ,53 ,54 ,55 ,64 ,65 ,66 ,67 ,68 ,69 ,70 ,71 ,80 ,81 ,82 ,83 ,84 ,85 ,86 ,87 ,96 ,97 ,98 ,99 ,100 ,101 ,102 ,103 ,112 ,113 ,114 ,115 ,116 ,117 ,118 ,119	No User Agent	OIP	hexadecimal strings within xml data, which can be extracted using regular expression: "\{ [0-9a-f-]{ 36} \}"|"[0-9a-f]{ 32}"|"[0-9a-f]{ 16} "

Note: The 4th octet of the DNS A Record IP Address falls within the NetBios group with hat the CNAME flag is used to set HTTP header and content format of HTTP C2 traffic.

Appendix 4 - HTTP Proxy Type

3rd Octet of an IP Address	Proxy Type
2 ,3 ,6 ,7 ,18 ,19 ,22 ,23 ,34 ,35 ,38 ,39 ,50 ,51 ,54 ,55 ,66 ,67 ,70 ,71 ,82 ,83 ,86 ,87 ,98 ,99 ,102 ,103 ,114 ,115 ,118 ,119 ,130 ,131 ,134 ,135 ,146 ,147 ,150 ,151 ,162 ,163 ,166 ,167 ,178 ,179 ,182 ,183 ,194 ,195 ,198 ,199 ,210 ,211 ,214 ,215 ,226 ,227 ,230 ,231 ,242 ,243 ,246 ,247	system
8 ,9 ,12 ,13 ,24 ,25 ,28 ,29 ,40 ,41 ,44 ,45 ,56 ,57 ,60 ,61 ,72 ,73 ,76 ,77 ,88 ,89 ,92 ,93 ,104 ,105 ,108 ,109 ,120 ,121 ,124 ,125 ,136 ,137 ,140 ,141 ,152 ,153 ,156 ,157 ,168 ,169 ,172 ,173 ,184 ,185 ,188 ,189 ,200 ,201 ,204 ,205 ,216 ,217 ,220 ,221 ,232 ,233 ,236 ,237 ,248 ,249 ,252 ,253	Direct
10 ,11 ,14 ,15 ,26 ,27 ,30 ,31 ,42 ,43 ,46 ,47 ,58 ,59 ,62 ,63 ,74 ,75 ,78 ,79 ,90 ,91 ,94 ,95 ,106 ,107 ,110 ,111 ,122 ,123 ,126 ,127 ,138 ,139 ,142 ,143 ,154 ,155 ,158 ,159 ,170 ,171 ,174 ,175 ,186 ,187 ,190 ,191 ,202 ,203 ,206 ,207 ,218 ,219 ,222 ,223 ,234 ,235 ,238 ,239 ,250 ,251 ,254 ,255	Default
0 ,1 ,4 ,5 ,16 ,17 ,20 ,21 ,32 ,33 ,36 ,37 ,48 ,49 ,52 ,53 ,64 ,65 ,68 ,69 ,80 ,81 ,84 ,85 ,96 ,97 ,100 ,101 ,112 ,113 ,116 ,117 ,128 ,129 ,132 ,133 ,144 ,145 ,148 ,149 ,160 ,161 ,164 ,165 ,176 ,177 ,180 ,181 ,192 ,193 ,196 ,197 ,208 ,209 ,212 ,213 ,224 ,225 ,228 ,229 ,240 ,241 ,244 ,245	Manual

Note: The 3rd octet of the DNS A Record IP Address falls within the NetBios group with CNAME flag is used to set the proxy type of HTTP C2.

References:

- Asuna-amawaka (Identity Unknown). A Look into SUNBURST's DGA. 20 December 2020. Available from *https://medium.com/insomniacs/a-look-into-sunbursts-dga-ba4029193947*
- Asuna-amawaka (Identity Unknown). Github Entry: SUNBURST-Analysis. Available from *https://github.com/asuna-amawaka/SUNBURST-Analysis*
- Blazier, Nick. The Cloudflare BLOG. A quirk in the SURBURST DGA algorithm. 17 December 2020. Available from *https://blog.cloudflare.com/a-quirk-in-the-sunburst-dga-algorithm/*
- FireEye Threat Research. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Mutiple Global Victims with SUNBURST backdoor. 13 December 2020. Available from *https://www.fireeye.com/blog/threat- research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain- compromises-with-sunburst-backdoor.html*
- FireEye Threat Research. SUNBURST Additional Technical Details. 24 December 2020. Available from *https://www.fireeye.com/blog/threat- research/2020/12/sunburst-additional-technical-details.html*
- FireEye. Github Entry: sunburst_countermeasures. Available from *https://github.com/fireeye/sunburst_countermeasures/blob/main/indicator_relea se/Indicator_Release_NBIs.csv*
- Hjelmvik, Erik. Security Boulevard. Reassembling Victim Domain Fragments from SUNBURST DNS. Available from *https://securityboulevard.com/2020/12/reassembling -victim-domain-fragments-from-sunburst-dns/*
- RedDrip7 (QiAnXin Technology, China). GitHub Entry: SunBurst_DGA_Decode. Available from *https://github.com/RedDrip7/SunBurst_DGA_Decode*
- Secure List. SUNBURST: Connecting the Dots in the DNS Requests. 18 December 2020. Available from *https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/*
- Sophos News. How SunBurst malware does defense evasion. 21 December 2020. Available from *https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware- does-defense-evasion/*
- Truesec (Sweden). Github Entry: sunburst-decoder. Available from *https://github.com/Truesec/sunburst-decoder*

An Analysis of the Strategic and Tactical Risks of Cyberwarfare & Cyberattack Against Unmanned Ground Vehicles (UGVs)

By 1st Lt. John Davis, U.S. Cyber Command Army Reserve Element, U.S. Army Reserve

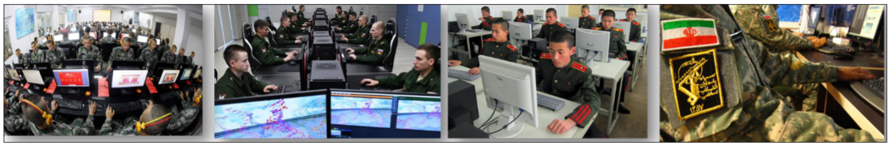


Figure 2: Adversary cyber operators and users

IN OCTOBER 2019, THE ASSOCIATION OF THE UNITED STATES ARMY (AUSA) hosted its annual conference in Washington, D.C. As part of that conference, AUSA hosted its annual defense exposition, particularly exhibiting some of the latest defense industry innovation related to the U.S. Army Futures Command's Cross Functional Teams (CFTs). One of those Cross Functional Teams is the Next Generation Combat Vehicle (NGCV), which includes in its portfolio of requirements the responsibility of replacing the venerable Bradley Infantry Fighting Vehicle (IFV).

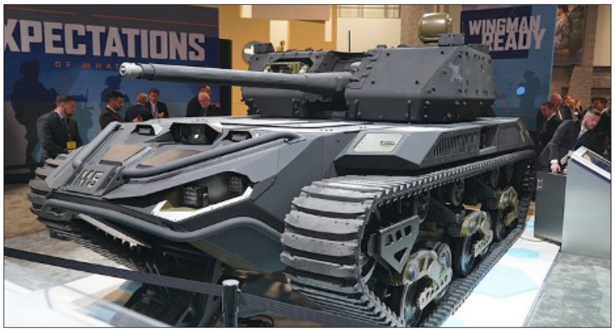


Figure 1: The Ripsaw M5 UGV at AUSA 2019

Related to this CFT's developments at this conference was defense contractor Textron's announcement of the Ripsaw M5 Robotic Combat Vehicle (RCV). The Ripsaw M5 hosts a wide suite of capabilities that make it a potent contender for the NCGV CFT's acquisition efforts, its marketing materials discussing features such as configurable armor; a variety of sensor suites, and modularity for specific mission configuration amongst various unmanned weapons systems. This vehicle may become the future of U.S. Army mechanized infantry formations. In FY2020, $160 million of research, development, testing, & evaluation (RDT&E) was dedicated to this vehicle. Recent advancements have shown deepening technical depth into this vehicle, with all-electric versions scheduled for testing this year and a partnership between Textron & Shield AI aiming to implement "multi-domain autonomy" for this vehicle.

However, Textron also states in its marketing materials that it also has "proven robotic control and interfaces" and "hardened wireless connection[s]." I will preface this analysis by stating that I am not related to the Army Futures Command nor have had experience with the NCGV CFT or M5 first-hand. However, this analysis argues that statements like this by defense industry risk a certain level of presumptiveness towards the enemy cyber threat that threaten U.S. forces from the strategic to tactical levels in combat.

While arguments abound regarding whether the U.S. has faced a true peer-versus-peer conflict since World War II, the threats to the U.S. across ADP 3-0's PMESII-PT operational variables (political, military, economic, social, information, infrastructure, physical environment, and time) have grown exponentially with the rise of the cyber domain. Each of these variables now have a cyber implication, from the political implications of activities within the cyber domain to time arguably becoming much more compressed in the cyber domain. Our adversaries have taken notice of how to exploit these vulnerabilities and are actively seeking to use them against us in future conflict. Through analysis of historical case studies, five potential vulnerabilities for UGVs in near-peer and peer-versus-peer conflict exist. These vulnerabilities include:

- Disruption of Weapons Systems, Sensors, or the entire UGV:

  Enemy forces disrupt or completely disable the utilization of specific weapons systems or suites on an UGV, or potentially disable/destroy the entire UGV.
- Hijacking Direct Control of Systems to Attack Friendly Forces

  Enemy forces directly compromise control suites and repurpose an UGV to attack friendly forces.
- Potential Utilization of Compromised Sensors by Enemy ISR

  Enemy forces compromise sensor communication feeds of an UGV, as well as potentially control suites, but do not alter the UGV's operations. This also potentially enables future transition to direct disruption or destruction operations.
- Feeding of False Data into Sensors

  Enemy forces are able to maliciously alter the data being read by ISR sensors in UGVs and subsequently distort the intelligence picture of friendly forces.

- Malicious Alteration of Advanced AI Systems to Attack Friendly Forces
  Although this potential vulnerability likely requires significant evolution to become a true threat, the implementation of advanced AI raises the possibility of the AI system being turned against friendly forces without security controls.

No matter how much defense industry believes it has "proven" controls and "hardened" connections, our adversaries have repeatedly demonstrated an ability to defeat security measures and conduct significant breaches. At time of writing, the SolarWinds cyberattack is the most recent example of adversarial success against U.S. systems, compromising networks across the U.S. government and internationally. Therefore, defense industry must consider a high possibility that digitized and unmanned combat systems may be compromised in combat and account for this.

South African "Oerlikon" Air Defense System
Iranian propaganda video of captured RQ-170 Sentinel
McDonnell Douglas F-15 Eagle

Figure 3:Analysis of adversary doctrine and associated leadership

Three historical incidents also demonstrate the relevance of the vulnerabilities identified in this analysis. The first the 2007 South African "Oerlikon" Air Defense System incident. During an exercise, and Oerlikon anti-aircraft system opened fire without command. While conflicting reports exists whether a mechanical or software issue caused the disaster, 9 South African Defense Force soldiers were killed and 14 were seriously injured.

The second is the 2011 capture of an U.S. RQ-170 Sentinel drone by Iranian forces. While various news sources debate how the drone was captured by Iranian forces, one theory is that the Iranian military managed to hack the drone into landing in hostile territory, whether by providing a false signal or directly hijacking the communications of the drone itself.

The third is the 2019 U.S. Air Force-sponsored ethical hacking of F-15 Eagles. The ethical hackers recruited by the Air Force managed to "shut down the Trusted Aircraft Information Download Station, which collects reams of data from video cameras and sensors while the jet is in flight," U.S. Air Force Assistant Secretary of the Air Force for Acquisition, Technology and Logistics told Stars and Stripes. The results of the hacking were displayed at the DEFCON 2019 conference.

Chinese "Systems Warfare"
Systems Confrontation and System Destruction Warfare
General Wei Fenghe
Chinese Minister of National Defense
Russian "Hybrid Warfare"
TASK FORCE
2019
General Valery Gerasimov
Chief of the General Staff of the Armed Forces of Russia

Figure 4:Historical incidents referenced in analysis

More importantly and worrying to defense industry is the fact that U.S. adversaries are advocating the use of tactics exploiting these very vulnerabilities in conflict. The two primary, near-peer threats the United States faces are the Chinese and Russian Armed Forces. Chinese "Systems Warfare" doctrine has a heavy focus on the targeting of, disruption, and destruction of enemy information-based (to include cyber) systems. A 2018, USPACOM-sponsored RAND Corporation report, "Systems Confrontation and System Destruction Warfare," discusses at length how the PLA doctrinally intends to incorporate such attacks through "Information Confrontation." Additionally, Larry Wortzel of the U.S. Army War College's Strategic Studies Institute also discusses at length the PLA's intent to harness techniques targeting cyber vulnerabilities in his 2014 analysis titled "The Chinese People's Liberation Army and Information Warfare."

The Russian Armed Forces utilize the concept of what is commonly called "Hybrid Warfare." In 2017, then-director of RAND Corporation's International Security and Defense Policy Center Chris Chivvis testified before the U.S. House Armed Services Committee with his brief "Understanding Russian 'Hybrid Warfare' and What Can be Done About It." In his brief, he highlights how one of Hybrid Warfare's three main characteristics is the usage of 'economy of force,' with Russia recognizing cyber operations giving it an ability to force-multiply above its conventional military capabilities. While much of Hybrid Warfare is focused at operations outside of military force, the Russian Armed Forces have also demonstrated a clear capability and intent to harness cyber capabilities for tactical exploitation on the battlefield. In 2016, the Center for Naval Analysis, under contract with the Office of the Chief of Naval Operations, analyzed this with their report "Russia's Approach to Cyber Warfare." In this report, CNA discussed how the Russians view cyber as a subcomponent of Information Warfare and how pro-Russian hackers have neutralized power grides in support of military operations.

Indeed, Ukraine has proven to be a significant incubator for the Russians on tactical implementation of cyber operations in kinetic warfare. Thankfully, the Army seems to be drawing lessons learned from Ukraine. Aaron Brantly and COL Liam Collins, writing on behalf of West Point's Modern War Institute, discuss at length on the AUSA's website these advancements at length. Additionally, MAJ Ronald Sprang evaluates Russian CEMA in Ukraine in his analysis at the U.S. Army Command and General Staff College's School of Advanced Military Studies in a monograph titled "The Development of Operational Art and CEMA in Multi-Domain Battle during the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016." In particular, he highlights "Operation Armageddon," which both he and cybersecurity firm LookingGlass Cyber identify as an ongoing (through at least 2015) operation to employ cyber capabilities for kinetic battlefield effect. With these contexts in mind, defense industry modernization efforts cannot assume going forward that their systems are sufficiently protected from evolving cyber threats. Failure to acknowledge this risk of presumptiveness risks disaster for U.S. forces on a battlefield. Utilizing the Army's Decisive Action Training Environment (DATE) Scenario, I have comprised a wargame demonstrating each vulnerability's potential impact on the battlefield and follow-on implications from the tactical to strategic level.

In this scenario, U.S. forces intervene following the invasion of U.S. ally South Torbia by North Torbia. Following the repulse of North Torbian forces, U.S. forces invade North Torbia proper to remove the North Torbian government from power. As U.S. forces drive North Torbian forces back, North Torbian-ally Olvana intervenes to support North Torbian forces from being overrun in the capital of Baguio.

A component of the 1st Armored Division, 6th Squadron, 1st Cavalry Regiment, has had their recon platoons' 18 Bradley IFVs replaced with 18 new M5 Ripsaw UGVs to conduct forward scouting ahead of the 1st ABCT, who is leading the charge into the city.

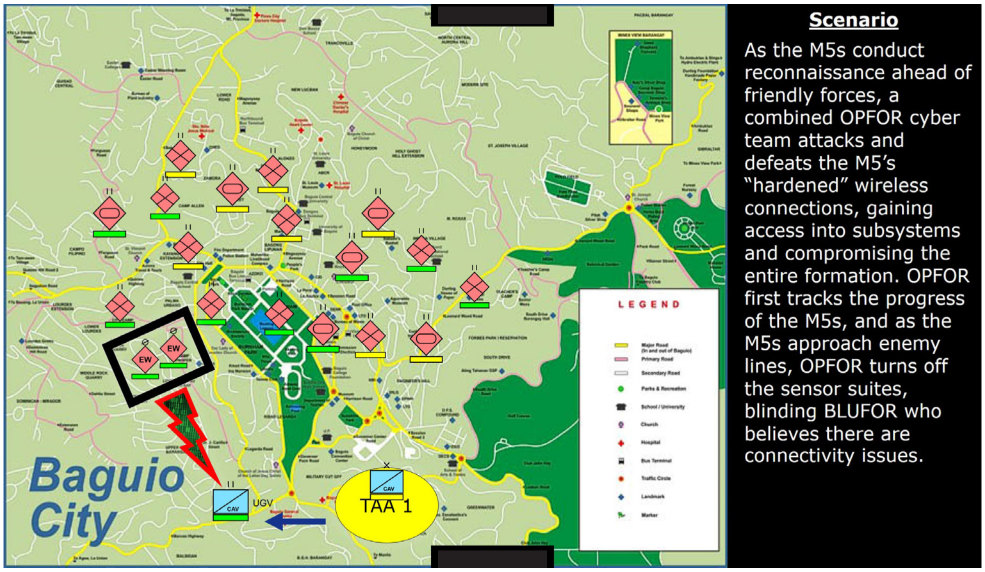
As the M5s scout ahead, the enemy already has the M5's systems compromised by North Torbian cyber forces who are acting in conjunction with Olvanan cyber. They track the progress of the scout drones, and as they approach enemy lines the drone sensors are turned off, blinding friendly forces who may believe there are connectivity issues.

In the meantime, the North Torbian-Olvanan cyber forces direct the M5s to return to friendly forces via automated command. SIGINT assets placed into the M5s read that there are no significant signatures being detected due to enemy interference, and as the M5s return to the Tactical Assembly Area, friendly forces are fired upon by the UGVs who are now under enemy control.

The end result is an ambush on the TAA which renders the rest of the CAV REG, already degraded due to combat losses on the push towards Baguio, combat ineffective. They were caught entirely by surprise. Combined North Torbian-Olvanan forces are then able to launch a counterattack on the TAA and disrupt the entire 1st Armored Division's attack into Baguio and retake the initiative.

While the strategic implications of such an outcome could be staggering to consider, the outcome does not have to result like this. If defense industry and Army acquisition efforts truly take into consideration the risks our adversaries pose against emerging technologies, the risks can potentially be mitigated. Perhaps safeguards can be put into place allowing a human operator to take over at the first sign of trouble. Maybe an auto-shutdown sequence can be implemented if any sign of tampering occurs. Regardless of the solution, the Army and the greater defense industry owes it to Soldiers and the American public to fully consider the risks of UGVs as they evolve on the battlefield to more primary roles. 🟥

Scenario Depiction:



Scenario

As the M5s conduct reconnaissance ahead of friendly forces, a combined OPFOR cyber team attacks and defeats the M5's "hardened" wireless connections, gaining access into subsystems and compromising the entire formation. OPFOR first tracks the progress of the M5s, and as the M5s approach enemy lines, OPFOR turns off the sensor suites, blinding BLUFOR who believes there are connectivity issues.

Color by numbers: inside a Dharma ransomware-as-a-service attack

By Sean Gallagher, Senior Threat Researcher at Sophos

OVER THE PAST YEAR, ransomware operators and their affiliates have moved increasingly toward the use of commodity malware and off-the-shelf tools to attack their victims, from initial compromise to deployment of their file-encrypting malware. And these attacks are often "fileless", leaving no tell-tale files on their targets' computers other than whatever was used to establish a foothold in the first place.

Even when there are bits of forensic evidence left behind, they are often components that don't point back to a specific actor. Often attackers use a mix of native Windows tools, common freeware and open-source utilities, and off-the-shelf software originally developed for penetration testers and other security professionals. In late 2020 and early 2021, for example, multiple ransomware operators increasingly used Cobalt Strike attack tools – following a leak of some of that penetration testing toolkit's code online.

Entry-level cybercriminals have also embraced the off-the-shelf toolkit approach, as evidenced by data collected in recent Dharma ransomware attacks. Multiple recent attacks documented by SophosLabs and Sophos MTR have revealed a toolset used by Dharma "affliliates" that explains why attacks from so many different Dharma actors seem so identical, down to the tools and commands they use.

Instant Dharma

Dharma is a very long-lived family of ransomware, first spotted in 2016. Despite its longevity, Dharma continues to be a threat to many organizations, and especially to small and medium-sized businesses. While other, newer ransomware families have grabbed recent headlines with high-profile victims and multi-million-dollar demands, Dharma has continued to be among the most profitable.

Part of the reason for that success is the version of the ransomware-as-a-service (RaaS) business model chosen by Dharma's operators. Actors with access to the Dharma source code continue to innovate around delivering the ransomware as a packaged business for less-sophisticated criminal operators.

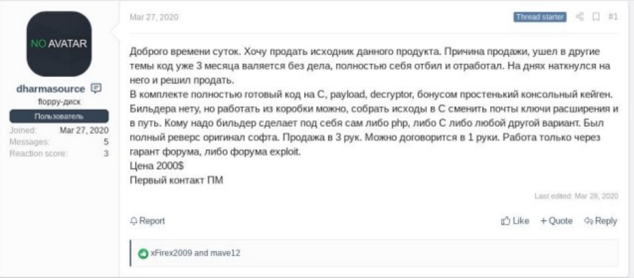
In other words, Dharma has become a sort of fast-food style franchise for cybercrime.

The Dharma RaaS we've investigated is targeted at entry-level cyber-criminals, and provides a paint-by-the-numbers approach to penetrating victims' networks and launching ransomware attacks. The actors using this particular RaaS are equipped with a package of pre-built scripts and "grey hat" tools that requires relatively little skill to operate—a combination of internal Windows tools, legitimate third-party "freeware" software, well-known security tools and publicly-available exploits. All of these components are integrated into a single toolkit through bespoke PowerShell, batch, and AutoIT scripts (https://www.autoitscript.com/site/).

This pre-packaged toolkit, combined with back-end technical support, significantly extends the reach of the Dharma RaaS operators, allowing them to profit while their afililates do the hands-on-keyboard work of breaching networks, dropping ransomware, and managing "customer service" with the victims.

Ransomware economics

It/s not clear that the original developers of Dharma (formerly known as CrySis) are the ones behind the current RaaS business model. There are many Dharma variants, due to the sale and modification of its source code to multiple malware developers. In March of 2020, a collection of source code for one variant of Dharma was offered for sale (https://nakedsecurity.sophos.com/2020/03/31/dharma-ransomware-source-code-on-sale-for-2000/) on Russian-language crime forums for $2000 through an intermediary.



dharmasource
floppy-диск
Пользователь
Joined: Mar 27, 2020
Messages: 5
Reaction score: 3

Mar 27, 2020

Доброго времени суток. Хочу продать исходник данного продукта. Причина продажи, ушел в другие темы код уже 3 месяца валяется без дела, полностью себя отбил и отработал. На днях наткнулся на него и решил продать.
В комплекте полностью готовый код на C, payload, decryptor, бонусом простенький консольный кейген. Бильдера нету, но работать из коробки можно, собрать исходы в C сменить почты ключи расширения и в путь. Кому надо бильдер сделает под себя сам либо php, либо C либо любой другой вариант. Был полный реверс оригинал софта. Продажа в 3 рук. Можно договорится в 1 руки. Работа только через гарант форума, либо форума exploit.
Цена 2000$
Первый контакт ПМ

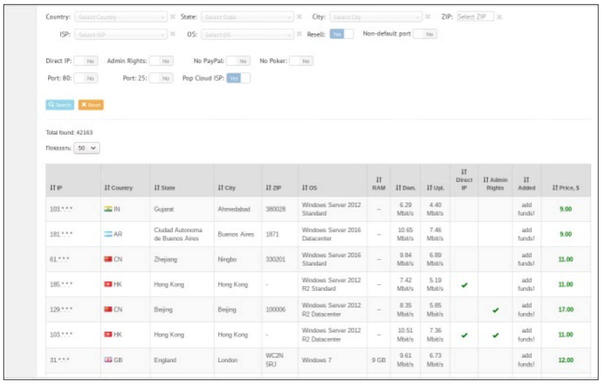
Last edited: Mar 28, 2020

xFirex2009 and mave12

A forum post from March 2020 offering the Dharma ransomware source code for $2000.

That wide availability has made Dharma the center of a three-tier criminal ecosystem based on a "syndication" business model:

- Dharma RaaS providers offer the technical expertise and support, operating the back-end systems that support ransomware attacks.
- "Affiliates" (often entry-level cybercriminals) pay for the use of the RaaS, and carry out the targeted attacks themselves, using a standard toolkit.
- Other actors provide stolen credentials and other tools on criminal forums that enable the Remote Desktop Protocol attacks that are the predominant means of initial compromise for Dharma actors. (RDP attacks are the root cause of about 85 percent of Dharma attacks, based on statistics provided by Coveware at https://www.coveware.com/dharma-ransomware-payment.)



Country: Select Country ✕ State: Select State ✕ City: Select City ✕ ZIP: Select ZIP ✕
ISP: Select ISP ✕ OS: Select OS ✕ Resell: Yes Non-default port No

Direct IP: No Admin Rights: No No PayPal: No No Poker: No
Port: 80: No Port: 25: No Pop Cloud ISP: Yes

Total found: 42163

Показать: 50

IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
103.*.*.*	IN	Gujarat	Ahmedabad	380028	Windows Server 2012 Standard	–	6.29 Mbit/s	4.40 Mbit/s			add funds!	9.00
181.*.*.*	AR	Ciudad Autonoma de Buenos Aires	Buenos Aires	1871	Windows Server 2016 Datacenter	–	10.65 Mbit/s	7.46 Mbit/s			add funds!	9.00
61.*.*.*	CN	Zhejiang	Ningbo	330201	Windows Server 2016 Standard	–	9.84 Mbit/s	6.89 Mbit/s			add funds!	11.00
185.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2012 R2 Standard	–	7.42 Mbit/s	5.19 Mbit/s	✓		add funds!	11.00
129.*.*.*	CN	Beijing	Beijing	100006	Windows Server 2012 R2 Datacenter	–	8.35 Mbit/s	5.85 Mbit/s		✓	add funds!	17.00
103.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2012 R2 Datacenter	–	10.51 Mbit/s	7.36 Mbit/s	✓	✓	add funds!	11.00
31.*.*.*	GB	England	London	WC2N 5RJ	Windows 7	9 GB	9.61 Mbit/s	6.73 Mbit/s			add funds!	12.00

A dark web site selling RDP credentials, including some with administrative privileges. These marketplaces in some cases allow buyers to verify the accounts work before they buy them.

Ransom demands from Dharma actors trend below those of the other major types of targeted ransomware over the past year. In December of 2019, when the average ransomware demand had surged to $191,000, the average Dharma ransom demand was only $8,620. That's in part due to the types of targets hit by Dharma (mostly small and medium businesses), and in part because of the skills, experience and location of the affiliates running the attacks. In any case, Dharma operators make up for the lower ransom demands with volume—Dharma remains one of the most profitable ransomware families, according to Coveware.

Dharma uses a complicated two-stage decryption process that partitions the affiliate actors from the actual key retrieval process. Victims who contact the attackers are given a first-stage tool that extracts information about the files that were encrypted into a text file. That text file gets cut-and-pasted into email and is sent back to the affiliates—who then have to submit that data through a portal for the RaaS to obtain the actual keys. This keeps the affiliates dependent on the RaaS, and it keeps them paying for service.

Just how well the decryption process works depends greatly on the expertise and the moods of the affiliates. Occasionally an actor will hold back some of the keys with additional demands. And there's constant "churn" among the front-end actors, as the "subscriptions" of some to RaaS services expire and others with less experience take their place, resulting in occasional misfires.

The Dharma playbook

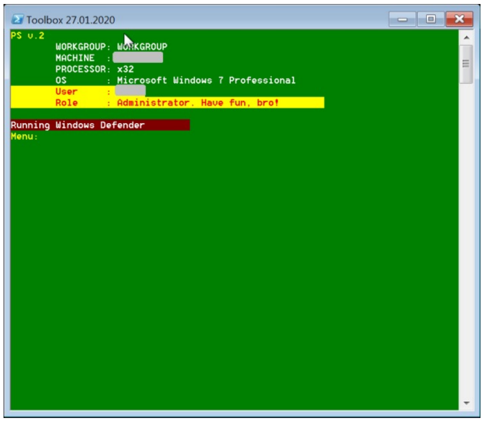
Dharma ransomware attacks are not exactly "fileless", but they do make use of remote files delivered through an RDP client drive mapping. Most Dharma operators don't make significant changes to the source. But Dharma RaaS operators appear to package together a number of tools and best practices for their "affiliates" to use once they've gotten onto a victim's network.

These tools aren't completely automated, as every attack does not follow the same exact steps. However, they do follow something amounting to step-by-step instructions, akin to a telemarketer's script, allowing some room for improvisation. And one of those tools is a menu-driven PowerShell script that installs and launches the components required to spread ransomware across the network.

After getting an RDP connection, the attacker maps a directory containing the RaaS toolkit on their local drive as a network drive accessible from the remote desktop. The contents of this directory include a number of applications previously identified as potentially unwanted applications (such as the Mimikatz password extraction tool), customized hacking tools, and freeware versions of a variety of legitimate system utilities. (A full list of the files is included in the indicators of compromise file on SophosLabs' GitHub page at https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Dharma-RaaS.csv.)

The kit also includes the Dharma ransomware executable, and a collection of PowerShell scripts, most of which we were unable to recover for analysis. However, we did recover a master script from console logs. Called toolbelt.ps1, the menu-driven console script automates the use of the tools, allowing attackers to simply type in the number associated with each pre-scripted element.

When executed, it identifies itself in the console frame as "Toolbox," and if executed with administrative privileges, advises the user/attacker, "Have fun, bro!



```
PS v.2
        WORKGROUP: WORKGROUP
        MACHINE  : [redacted]
        PROCESSOR: x32
        OS       : Microsoft Windows 7 Professional
        User     : [redacted]
        Role     : Administrator. Have fun, bro!

Running Windows Defender
Menu:
```

The startup screen for toolbelt.ps1

The "menu" selections in Toolbox aren't displayed as a menu by the script as it executes, though they are largely documented in the script itself. Tools are downloaded to the remote computer by the script as needed, executed, and in many cases deleted after use.

These tools, for the most part, break down into the following categories:

- Custom scripts for tasks such as purging system memory and shutting down services (such as anti-malware programs) that could interfere with ransomware deployment.
- Password viewers, including custom versions of the Mimikatz open source password stealer, the LaZagne open-source password scraper, and the freeware NirSoft Remote Desktop PassView password viewer tool.
- Process viewing/killing tools—including GMER (http://www.gmer.net/: a software tool written by a Polish researcher Przemysław Gmerek, for detecting and removing rootkits) and Process Hacker (https://github.com/processhacker/processhacker/: an open-source process monitoring and manipulation tool)
- Freeware utilities, including two

to remove software packages that interfere with ransomaware deployment (Revo Uninstaller: https://www.revouninstaller.com/revo-uninstaller-free-download/, and IOBit Uninstaller: https://www.iobit.com/en/advanceduninstaller.php), and a screen locker to deny access to a system under attack.

- Windows built-in tools, including the Remote Desktop Connection (RDP) client, Windows Active Directory management snap-in (dsa.msc), Windows Task Manager, the Group Policy Management Console snapin (gpmc.msc), the PowerShell command shell, and the cmd.exe Windows command shell.
- Network scanners for identifying other computers and network drive shares.
- AutoIT-compiled executables and PowerShell scripts to launch the ransomware.

Playing by the book

While the toolbelt.ps1 script is somewhat self-documenting, it's clear that the end users of the script—the Dharma affiliates—are also operating from some other form of documentation. The "toolbelt" gives them all the access they need to move laterally across the network, exploiting domain administrator level credentials that they either steal or create through elevated privileges, but it's not clear how fully automated some of the steps of that process are. Those steps are likely detailed in a how-to document created by the Dharma RaaS operators.

A typical attack looks like this, based on telemetry we gathered during our investigations:

- After gaining RDP access to the network, the attacker launches the toolbox script itself (toolbelt.ps1 -it 1)
- They then run a PowerShell script from the toolbox script called delete-avservices.ps1(which attempts to shut down antivirus software).
- GMER (gamer.exe) is launched to check running processes from the script.
- ProcessHacker is installed and launched by the toolbox script to check for and stop Windows services.
- A custom AutoIT wrapper of Mimikatz and the NL Brute password attack tool is launched.
- The ipscan2.exe advanced IP scanner tool is used to find other targets on the network.
- The RDP client mstsc.exe is launched to connect to other systems.
- The ransomware launching package, takeaway.exe—an AutoIT script—is executed. It launches the Dharma ransomware (winhost.exe), and then runs a PowerShell script called purgememory.ps1 (which we didn't capture the contents of).

The ease with which Dharma attackers are able to take these tools and effectively spread ransomware on victims' networks demonstrates the risks posed by both grey hat and legitimate but potentially unwanted administrative tools. And it underlines the risks associated with improperly secured RDP servers, the major vector for most targeted ransomware attacks. Given that many of these attacks are made with stolen credentials purchased in forums, the Dharma attacks may be just one of many intrusions onto victims' networks.

The majority of these Dharma affiliate attacks can be blunted by ensuring RDP servers are patched and secured behind a VPN with multi-factor authentication. Organizations need to remain vigilant about credential theft through phishing, particularly as they adjust to having more employees working remotely. And attention needs to be paid to access given to service providers and other third parties for business purposes. 🟥

Army National Guard Transitions Cyber Task Force Mission

By Steve Stover, Public Affairs Officer, 780th Military Intelligence Brigade (Cyber)

THE TRANSITION OF AUTHORITY between two Army National Guard battalions was a quiet and seamless affair, taking place without the traditional 'pomp and circumstance' normally associated with significant Army events.

The transition marked the end of a 15-month deployment for the Soldiers of the 124th Cyber Protection Battalion (CPB), who hail from Arkansas, Maryland, Missouri, Nebraska, Virginia and Utah, and the beginning for the Army National Guardsmen of the 123rd CPB, who call Illinois, Minnesota, Virginia, and Wisconsin their home states.

The battalions complete the fourth and begin the fifth iterations of Task Force Echo (TFE). TFE exists under the operational control of the 780th Military Intelligence Brigade (Cyber) and enables cyberspace operations in support of U.S. Cyber Command (USCYBERCOM). The 780th MI Brigade falls under the operational control of U.S. Army Cyber Command (ARCYBER).

Col. Matthew Lennox, commander of the 780th MI Brigade, recently hosted an awards ceremony for the departing 124th CPB staff and remarked on the exceptional experience and expertise of the National Guard Soldiers.

Lennox said "I was impressed by the Soldiers of Tasks Force Echo IV. They brought their real world experience managing networks to the Army and made our organization better. Their knowledge and experience enabled teams within the Cyber National Mission Force and the different service Joint Force Headquarters to accomplish their mission. The Task Force Echo Soldiers were integral members of the brigade team."

Command Sgt. Maj. (CSM) Timothy Hawley, the senior enlisted leader of the 124th CPB and TFE IV, commented on the challenges of COVID presented for their mission and how proud he is of the professionalism and dedication of his Soldiers.

"This deployment didn't go as we all had envisioned it. COVID threw a wrench into all the things we had planned for our Soldiers this past year," said Hawley. "We asked junior Soldiers to perform roles normally assigned to field grade officers and moved others into positions that they were not necessarily comfortable with. In the end the mission was extremely successful."

"We pushed through some extremely important events in history without a hiccup or glitch," added Hawley. "The professionalism and dedication of this Task Force was superb and second to none. It was a true testament of the (124th CPB) Soldiers and what the National Guard can truly bring to the fight. I am extremely proud of each of you and look forward to seeing you all again."

Lt. Col. John Truax, commander of the 124th CPB and TFE IV, echoed Hawley's praise.

"This has been a year full of firsts. Under extremely challenging and dynamic conditions, every Soldier in this task force stepped up to support one another, the mission, and our nation," said Truax. "The CSM and I are incredibly proud of the men and women in this formation. We could not have asked for better talent or a better team. The strong professional relationships forged with the 780th MI Brigade, ARCYBER, and USCYBERCOM by previous Task Force Echo rotations remain critical elements of our success now and in the future."

Since August 15, 2017, more than 600 Army National Guard Soldiers have been assigned to the task force, working alongside the 780th to conduct cyberspace operations in support of USCYBERCOM and the CNMF.

Hawley said the task force is a demonstration of the benefits of the partnership that has been built between the Army's active and reserve components.

"This deployment allows the National Guard to continue to show the Army, USCYBERCOM, and ARCYBER that we are capable and ready to support the cyber mission," said Hawley. "We bring a highly trained and motivated force to the fight, ready to get our hands dirty. The Soldiers get to use their civilian experience to give back to their country." ■

FORT GEORGE G. MEADE, Md. -- Col. Matthew Lennox, commander of the 780th Military Intelligence Brigade (Cyber), presents service awards to Army National Guard Soldiers assigned to Task Force Echo IV as they prepare to return to their home states. The Soldiers were deployed for more than a year conducting operations in support of U.S. Cyber Command and the Cyber National Mission Force. The more than 150 Soldiers assigned to TFE IV consisted of Soldiers primarily assigned to the 124th Cyber Protection Battalion, who hail from Arkansas, Maryland, Missouri, Nebraska, Virginia, and Utah. (Photo by Steven Stover)

Cyberspace Battalion Continues Growth with Activation of New Company

By Staff Sgt. John Portela, Public Affairs Noncommissioned Officer, U.S. Army Cyber Command

FORT GORDON, Ga. – The 915th Cyberspace Warfare Battalion conducted a ceremony here Jan. 29, 2021 to formally activate its Bravo Company.

The activation is the Army Cyber Command (ARCYBER) battalion's latest step in its commitment to building the Army's information advantage capabilities, a process that began with the launch of the 915th under the command and administrative authority of ARCYBER's 780th Military Intelligence Brigade in 2018. Since then, the battalion has grown to more than 100 Soldiers and activated three companies and two Expeditionary Cyber-Electromagnetic Activities (CEMA) Teams, or ECTs.

The ECTs are designed to provide CEMA -- integrated cyberspace, electronic warfare, network, spectrum management, intelligence and information operations support and effects -- to tactical commanders during training events and real-world operations.

Lt. Col Matthew Davis, commander of the 915th, called the activation of B Co. "an exciting and rewarding time" upon which the unit can build its capabilities. "Once you have the blueprint, the blueprint lets you build capacity," Davis said. "So Bravo Company's most important job for the foreseeable future is to develop and train their first team so they can get that one off the ground."

As the company continues to develop its potential, its Soldiers will be taking on a large share of ARCYBER's CEMA Support to Corps and Below requirements, multiplying the battalion's operational prowess and building support to Army and joint maneuver commanders in the information environment.

Capt. James Conway, the newly appointed commanding officer of B Co., said the company is ready to move forward and build, train, and validate its members to conduct operations and missions.

"It's a huge leap forward, and a good stepping stone for expeditionary cyber and expeditionary CEMA … to provide units at different echelons with capabilities that they may not have had before; to bring a different perspective to help them engage and win against the enemy," he said.

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace, electronic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries. ■

FORT GORDON, Ga. -- Lt. Col. Matthew Davis, commander of the 915th Cyberspace Warfare Battalion (right), and Capt. James Conway, the newly appointed commander of the battalion's Bravo Company, unfurl the company's guidon at the ceremony activating the unit, at Fort Gordon, Ga., Jan. 29, 2021. The ceremony was modified for the current operational environment during the COVID-19 pandemic, while continuing to honor military traditions. (Photo by Staff Sgt. John Portela).

Cyber Soldiers Join Prestigious Sergeant Audie Murphy Club

By Steve Stover, Public Affairs Officer, 780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, Md. – Sgt. Maj. Nathaniel Piper, the 780th Military Intelligence Brigade (Cyber) S-3 (operations), and Staff Sgt. Daniel Colón, E Company, 782nd Military Intelligence Battalion (Cyber), were recently inducted into the prestigious Sergeant Audie Murphy Club (SAMC).

According to U.S. Army Forces Command regulation 600-80-1, the Sergeant Audie Murphy Award (SAMA) is an "elite award for Noncommissioned Officers (NCOs) whose leadership achievements and performance merit special recognition. The SAMA is a means of recognizing those NCOs who have contributed significantly to the development of a professional NCO Corps and a combat ready Army. Awardees exemplify leadership, characterized by personal concern for the needs, training, development and welfare of Soldiers, and concern for families of Soldiers."

Sgt. 1st Class Prince Yohannes, a recipient of the SAMA and a cyberspace operations noncommission officer (NCO) assigned to B Company, 781st MI Battalion, was Staff Sgt. Colón's sponsor for the final Phase III (MDW) board, and discussed the SAMA process.

"You must be nominated by your chain of command and earn the award by going on a journey to find out who you are as a leader and build upon that to become an even greater leader for the Soldiers, Army Civilians, and your organization," said. "You must currently meet the black standard in each event for the Army Combat Fitness Test, pass a written test, write an essay, and go to levels 1 to 3 boards."

Colón said that although he has attended nearly 30 boards in his previous six years of Army service – Sergeant and Staff Sergeant Promotion Boards, Soldier/NCO of the Month and Quarter Boards, and Best Warrior Competitions – to prepare the 3 level boards under the SAMA process he spent the past year attending study hall sessions and studying in any downtime he had.

"I read through endless regulations and would engage with the Non-Commissioned Officers in my company to discuss their respective additional duties and Army Programs in depth," said Colón. "I would study during lunch, before and after work, and throughout the weekends trying to refine my knowledge for the SAMA process."

Colón said he believes in everything the Sergeant Audie Murphy Club stands for and plans to use what he has learned and what he will continue to learn as a SAMC member to improve himself and grow as leader in order to better serve his unit and his Soldiers.

"The SAMA process is extremely challenging and extremely time consuming. I wanted to prove to myself that I could accomplish this goal while still maintaining all my other priorities: graduate school, mission, my Soldiers, my additional duties, etcetera," said Colón. "Although it is a prestigious award, I was more focused on the professional and leader development, rather than the award itself."

"I try to use my experience with boards to prepare other Soldiers for the board process, including the promotion board. I hope to mentor and prepare other Noncommissioned Officers to appear before the SAMA Board," added Colón. "Although I told myself the SAMA Boards would be my absolute last, I still want to challenge myself. I currently have my eyes set on the 2021 Best Warrior Competition (mission pending)!"

Sgt. Maj. Piper also received the Sergeant Audie Murphy Award in a recent March ceremony. Yohannes describes Piper as a "servant leader."

"He gives his intention backing them with genuine and sincere actions," said Yohannes. "We are leaders in the business of taking care of people first, and SGM Piper has taken care of all of us and we appreciate it 100 percent and therefore we selected him for be a recipient of the SAMA."

Piper gave this advice to current and future NCOs.

"Don't prepare for your next position," said Piper. "Be ready to take on the responsibility when called upon."

Brigade Soldiers interested in earning the Sergeant Audie Murphy should talk to their unit first sergeant or reach out to Sgt. 1st Class Yohannes or Staff Sgt. Colón. ■

Staff Sgt. Daniel Colón

Sgt. Maj. Nathaniel Piper,

Sgt. 1st Class Prince Yohannes

Got What it takes?

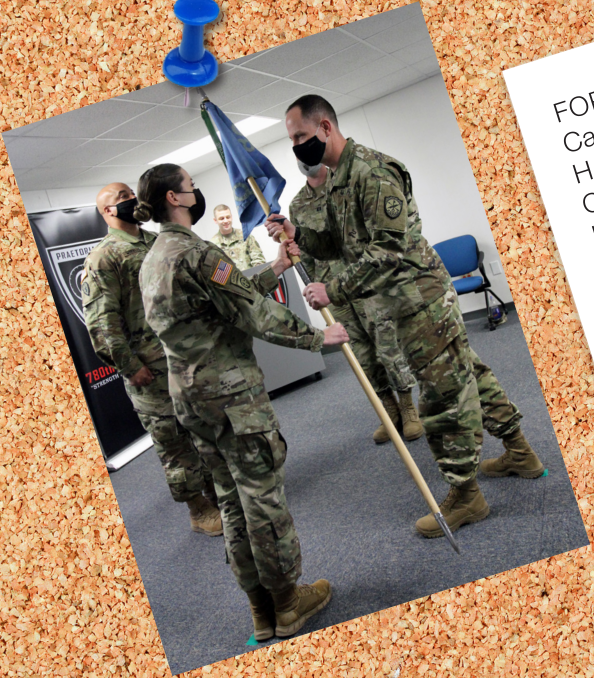
780th MI BDE POC, Sgt. 1st Class Prince Yohannes

prince.s.yohannes.mil@mail.mil

FORT GEORGE G. MEADE, Md. –Col. Matthew Lennox, commander of the 780th Military Intelligence Brigade (Cyber), and Command Sgt. Maj. Ronald Krause, the brigade's senior enlisted leader, set the example by receiving their COVD-19 vaccine at McGill Training Center.

FORT GEORGE G. MEADE, Md. –Col. Ben Sangster, the deputy commanding officer for the 780th Military Intelligence Brigade (Cyber), was the guest speaker at the Chaplain's monthly Resiliency Talk Luncheon on April 6 in the Brigade Annex. Col. Sangster talked about his faith and how it applies to his personal and professional life and the importance of Family; his home and his work Family.

FORT GEORGE G. MEADE, Md. – Col. Matthew Lennox, commander of the 780th Military Intelligence Brigade (Cyber), and Command Sgt. Maj. Ronald Krause, the brigade's senior enlisted leader, had a discussion with all the company, detachment and battalion command teams about their upcoming Extremism Stand-Down events, and reminded them to be: Caring, Committed, and Coachable.



FORT GEORGE G. MEADE, Md. – Capt. Lauren Feifer (left), commander, Headquarters and Headquarters Company (HHC), 780th Military Intelligence (MI) Brigade (Cyber), signifies her assumption of command by accepting the unit guidon from Col. Matthew Lennox, commander, 780th MI Brigade, during a change of command ceremony in the Brigade Annex, March 5.

FORT GEORGE G. MEADE, Md. – Capt. Aaron Bishop, commander of the Headquarters & Headquarters Company (HHC), 780th Military Intelligence Brigade (Cyber), hosted a Change of Responsibility ceremony whereby 1st Sgt. (1SG) Stan Collins relinquished his authority as the company's senior enlisted leader and "Keeper of the Colors" to 1SG Edgar Morales, on January 27 in the Brigade Annex.

FORT BLISS, Tx – Expeditionary Cyber-Electromagnetic Activities (CEMA) Team 3 is shown here at the zeroing and qualification range as part of the Soldier Readiness Processing (SRP) process in preparation for an overseas deployment in support of combatant command CEMA requirements.

FORT GEORGE G. MEADE, Md. – Cyber Corps' Command Sgt. Maj. (CSM) Cecil Reynolds (left), CSM Ronald Krause (right), the 780th Military Intelligence Brigade's senior enlisted Leader, and Non-Commissioned Officers from the Cyber Center of Excellence, instructors and drill sergeants, discussed the 17-series career management field and other topics, to include broadening assignments, March 16, in the brigade annex.

FORT GEORGE G. MEADE, Md. – Chaplain (Capt.) John Han, 781st Military Intelligence Battalion (Cyber), and Staff Sgt. Jamilia Leary, the religious affairs non-commissioned officer for the 780th MI Brigade (Cyber), facilitated safeTALK training for D Company, 781st MI Battalion in the Brigade Annex. LivingWorks safeTALK is a four-hour face-to-face workshop featuring presentations, audiovisuals, and skills practice. Participants learn how to prevent suicide by recognizing signs, engaging someone, and connecting them to an intervention resource for further support. If you require support, the 780 MI Brigade Unit Ministry Team can be reached at: usarmy.meade.780-mi-bde.mbx.unit-ministry-team@mail.mil.

FORT GORDON, Ga. – Pvt. Cierra Shakir inspired an amazing Christmas House Toy Drive collection effort leading the Archers to winning a new “HUMANITARIAN” streamer for most toys donated. For her incredible accomplishment, Shakir was awarded an impact Army Achievement Medal by Lt. Col. Wayne Sanders, commander, 781st Military Intelligence Battalion (Cyber).

FORT GORDON, Ga. -- Capt. Rebecca Marigliano, U.S. Army Cyber Command, and Capt. Stuart Topp, team lead, 781st Military Intelligence Battalion (Cyber), reacted with uncanny instincts stabilizing and likely reducing the threat to loss of life of a heat stroke casualty while out running. They used previous EMT training to expertly manage the situation and efficiently direct EMS to the casualty. For their swift action Lt. Col. Wayne Sanders, commander, 78 1st MI BN, recognized both with impact AAMs.

FORT GORDON, Ga. -- The Archers enjoyed a COVID safe rockclimbing Warrior Adventure Quest morale building activity. This picture shows the incredible spirit of Soldiers adapting and overcoming challenges—nothing can stop the world’s greatest team!

Word of the Day: Idle Prayer

By Chaplain (Capt.) Warren Moore, 915th Cyberspace Warfare Battalion

"The prayer that wants [lacks] a good aim wants [lacks] a good issue." – Thomas Watson, English, Puritan Preacher and Author

"Determine how the task should be done differently next time. The facilitator guides the unit in self-determining how the task(s) might be performed more effectively in the future. The unit identifies problems and provides solutions as well as identifies who is responsible for making the recommended changes. Additionally, the facilitator guides the discussion to determine if there is a more effective way to train the tasks to achieve the commander's intent." p. 4, The Leader's Guide to After-Action Reviews

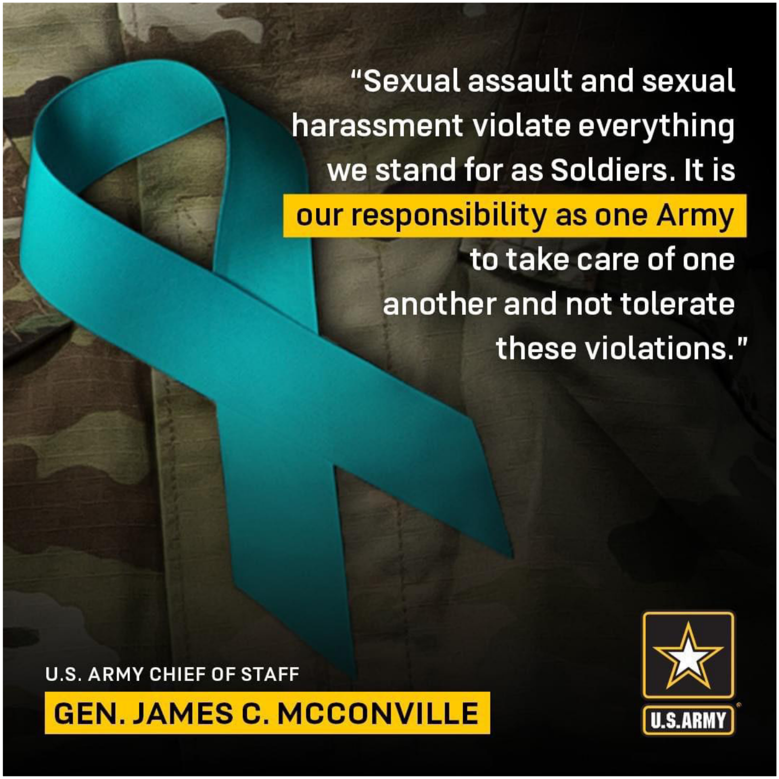
Give me three ups and three downs concerning this training. I think many of us recognize that a proper After Action Review (AAR) is supposed to be better than that. The danger of taking something that is regularly done, like prayer or an AAR, and making it perfunctory is that the intended result, increased trust in the process and growth, does not happen. Self-reflection, brainstorming, synergy, adaptation, and the budding planning process that should occur is stripped down to platitudes and watch-checking until we think we've done good enough. We need to do better, but how?

Our attitude towards the process and the time we set aside for it needs to be positive. We need to expect good results. This type of optimism not only helps us in the process, but, moving forward, we will begin to see how we personally can be involved in implementing those changes, and we can then personally celebrate good results. We take ownership.

Sometimes we need a guide. We need an example of what right looks like. That might mean opening an AR, FM, TC, TM, DA PAM, etc. and walking through what is doctrinal and traditional in light of our experience to help shape our constructive feedback to our commander. This isn't always necessary, but, for some, it can help them get over generalizations by giving them the vocabulary and precision they need to go through the process.

We need to be honest. Some Soldiers don't want to embarrass their leadership. Some Soldiers don't think that anything will ever change. Some Soldiers are afraid of the response they might receive if they gave a real assessment of a training activity. An AAR is done in a public forum. Several leaders will have the opportunity to consider the results. Some may disagree with an assessment, while others will agree. We must operate in good faith that good leaders will hear and implement feedback into their planning cycle. This might not result in the changes that we think are best, but it will facilitate growth that might be better than the Soldier could have anticipated.

When you have the opportunity to provide feedback, whether that is in prayer or during something like an AAR, be honest, use a guide, and keep a positive attitude. Your participation can spur your own growth, encourage others, and help your leadership keep everyone moving forward. ■



"Sexual assault and sexual harassment violate everything we stand for as Soldiers. It is **our responsibility as one Army** to take care of one another and not tolerate these violations."

U.S. ARMY CHIEF OF STAFF

GEN. JAMES C. MCCONVILLE

Reminder...If You Need Help:

- BDE SARC: 301-833-6406
- BDE VA: 301-833-6407
- Fort Meade 24/7: 443-845-0876
- Fort Gordon: 706-791-6297
- JBSA: 202-808-7272
- Hawaii: 808-655-9474

NEXT QUARTER'S BYTE IS focused on what motivates and interests our Soldiers, Civilians and their Family members after duty hours and outside work. If you have any fellow co-workers who inspire others, have interesting hobbies or talents, write a synopsis paragraph and send it to Steven Stover at steven.p.stover.civ@mail.mil NLT May. 14, 2021. Articles are due NLT May 31, 2021.

AVENGER CON