SEPTEMBER 2021

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

For CTA's third quarter newsletter, we chose the theme Cyber Threat Intelligence and Resilience. Not surprisingly, resilience has become a much-discussed concept as organizations face significant uncertainty in both the physical and virtual domains. Further, since these domains are now highly interdependent, resilience in one is critical to resilience in the other. Given the physical and virtual threats we face, the need for organizational resilience is not likely to decrease any time soon.

Creating a resilient organization is not easy. It takes considerable planning, thought, and persistence to ensure that an organization can respond to whatever threat or circumstance emerges. And no matter how carefully an organization plans, what occurs always differs from what was anticipated. However, if a company has planned well based on reliable intelligence, then it can rapidly modify its plan to meet the new circumstances.

Supporting this rapid adaptation is what connects cyber threat intelligence (CTI) to resilience. CTI enables an organization to identify the most likely threats and allocate resources to mitigate them. It allows the organization to prioritize its activities based on the best evidence available, and, since no one has unlimited time or money, prioritization is a necessity. It allows organizations to change their focus rapidly when circumstances demand it. Without good CTI, companies make decisions based on instinct, experience, or media stories which often miss the mark from the real threats they face. CTI is now a critical input to the decision-making process. Unfortunately, for many organizations, finding reliable, useful CTI sources often proves challenging.

CTA tackles this problem head on. We are dedicated to improving the cyber threat intelligence available to the digital ecosystem. Whether through our automated sharing mode, where members provide and consume technical cyber intelligence at speed and at scale, or through our analytic sharing mode, where members provide and consume intelligence in human accessible formats, CTA increases the threat intelligence available to our members. In turn, these members use this intelligence to improve their products and services. CTA also sponsors events like the Threat Intelligence Practitioners Summit track at Virus Bulletin or the Association of Anti-Virus Asia Researchers (AVAR) conference that foster exchanges of different types of CTI. Finally, CTA highlights its members' CTI through webinars, blog posts, social media posts, and joint analytic papers. Whatever its form or structure, CTA's mission is to enable the broadest possible use of cyber threat intelligence to enhance the security of the digital ecosystem.

The articles that follow showcase just a few of the ways that CTA connects threat intelligence and resilience. They show how being a CTA member provides access to high-quality, reliable CTI in both the short and long term. And they demonstrate how CTA is a resilient organization, able to adapt to changing circumstances.

As always, I want to thank our current members for their on-going support and contributions. For those thinking about membership, check us out at www.cyberthreatalliance.org or schedule some time to talk with us. Every member added to CTA adds to our resilience. And that brings us full circle to where we started – deepening the connections between cyber threat intelligence and resilience.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

WELCOMING A NEW CTA BOARD MEMBER

We are pleased to announce that Samantha Madrid, Vice President, Security Business & Strategy, Juniper Networks, has been elected as an Affiliate Director to the CTA's Board of Directors for a two-year term. As a long-time cybersecurity practitioner, she will bring a wealth of experience to the board, as well as providing a different perspective on the issues facing CTA. Samantha will serve on CTA's board alongside representatives from Check Point Security Systems, Cisco, Fortinet, NTT, Palo Alto Networks, Rapid7, and Sophos.

We are looking forward to Samantha helping guide the direction of the CTA alongside our other board members.

SAMANTHA MADRID
VICE PRESIDENT, SECURITY BUSINESS & STRATEGY
JUNIPER NETWORKS

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>5 MILLION
MONTHLY AVERAGE

KILL CHAIN DIVERSITY
(3 MOS AVERAGE)

RECONNAISSANCE	1%
WEAPONIZATION	>0%
DELIVERY	12%
EXPLOITATION	17%
INSTALLATION	52%
COMMAND + CONTROL	16%
ACTIONS ON OBJECTIVES	2%

NOTE: Every IoC submitted to CTA must be accompanied by a kill chain phase.

TOTAL EARLY SHARES

3-5
PER WEEK

490+
IN THREE YEARS

Upcoming Events

VIRTUAL VIRUS BULLETIN 2021

OCTOBER 7-8TH, 2021

CTA is once again sponsoring the Virus Bulletin Threat Intelligence Practitioners' Summit (TIPS). This year, learn how investment in threat intelligence builds cyber resilience, allowing you to be more effective when addressing today's dynamic threat landscape.

Threat Intelligence is a necessary part of any security solution and can dramatically increase the effectiveness and resilience of any cybersecurity product, service, or team. Using threat intelligence to build cyber resilience should be an essential part of any business plan. We are a better team when we work together; our collective efforts magnifies our success and ensures that we are and remain cyber resilient.

The TIPS track features keynotes, panels and talks with representatives from CTA members and partners, below. Full details of the TIPS agenda can be found **here**. The conference is virtual and free!

Register to attend **here**.

VB2021 localhost

12TH ANNUAL BILLINGTON CYBERSECURITY SUMMIT

OCTOBER 6-8TH, 2021

CTA is proud to again sponsor the Billington CyberSecurity Summit, which is now entering its 12th year.

Join CTA President & CEO, Michael Daniel on Thursday, Oct 7th in a panel presentation: *Next Steps in CDM Information Sharing.*

Panelists will discuss what changes are needed to ensure the overall Federal network is discovering and mitigating cyber threats faster and with greater efficiency and speed. They will explore DHS/CISA's Continuous Diagnostics and Mitigation Plans, where it is, what continues to need to be done and areas such as better data sharing that will require continued interaction and management across the entire government, including DoD and National Security Systems.

Register to attend **here**.

CTA Champions Feature

THE POWER OF THREE

Cyber attacks used to be outliers. State actors performing remote espionage and criminals going after petty cash in an opportunistic manner. Protecting infrastructure was very much an insider game contained in a small community with highly specialized experts, in the know about adversary techniques and infrastructure, sharing information in trusted circles.

The threat landscape has changed dramatically, though. State actors became extremely brazen, disregarding being called out and threatening the continuity of essential services and even core values of democracy and freedom of speech. Cyber criminals have upped their game as well, blackmailing our economy and gaining access to levels of sophistication that were hitherto reserved for state actors.

But even more importantly, industry surveys indicate that cyber attacks are not outliers anymore and are certainly not only a problem of essential infrastructure. In the mean time we became more dependent on connected IT systems for all aspects of our life.

Disruption can be catastrophic and resilience needs to be an integral part of our plans. More and broader awareness raising is needed on this particular aspect.

Fortunately, the defenders have also upped their game, expanding the community and professionalizing analysis and response by using frameworks like MITRE ATT&CK and open-source languages like SIGMA and ZEEK.

They are also adapting to the agility of the adversaries by industry-wide information exchange and deployment of Cyber Threat Intelligence in backbone, perimeter, and endpoint infrastructure.

The three keywords for success here are Precision, Timeliness, and Scale. Precise insight in the threat needs to be converted into mitigation at the same speed and scale as the adversarial action it tries to address.

The essential building blocks for achieving impact in these three areas have gradually been gathered in initiatives like CTA. CTI information on newly identified attacks is deployed in infrastructure worldwide in a question of half an hour nowadays.

It will require persistent effort to keep up with the continuous advances made by the adversaries, to shorten further the timeliness, and to expand the deployment to reach all corners of our connected world and protect as broadly as possible.

We are probably just in the initial stages of this path and continuous innovation in infrastructure, cooperation, and funding will be needed to benefit from the power of three.

FREDDY DEZEURE
CEO OF FREDDY DEZEURE BV
BRUSSELS

Freddy is a recognized thought leader in security, risk and privacy, and a Board Member and Advisory Board Member in several high tech companies.

As a CTA Champion, Freddy advocates for CTA's mission and goals.

CYBER THREAT ALLIANCE
CTA CHAMPION

MARK THOMAS
SENIOR THREAT INTELLIGENCE DIRECTOR
NTT

CTA Member Feature

ENABLING RESILIENCE IN THE FACE OF EMERGING CYBER THREATS

The only constant in the threat landscape is that it is continually changing. Organizations' need to be cognizant of threats which may seek to undermine business stability and continuity. Digital transformation has only accelerated amidst the pandemic. The increasing role of technology, connectivity, and supply chain has created a complex digital ecosystem that we now consider the foundation for our digital way of life.

The threat of ransomware on critical infrastructure and other essential services has emphasized the need for improved cyber resilience. Recent high-profile incidents impacting fuel and food supplies have elevated concerns at both the state and board level. The importance of securing our infrastructure has exacerbated the need to evolve from a reactive to a proactive security posture – one that assumes a breach. This continues to be a shift in mindset for many organizations.

Threat intelligence plays a pivotal role in anticipating and acting upon existing and emerging threats. Much like a lighthouse illuminates waterways made treacherous by hazards, they also serve as a beacon for navigational aid – guiding vessels safely into and out of harbors. Leveraging threat intelligence enables organizations to know the adversary and their tradecraft, informing decisions around cybersecurity investment and priorities. In doing so, organizations become better prepared in protecting, responding to, and recovering from cyber incidents or other credible threat scenarios.

But enabling resilience is more than just about dealing with technological issues – it's an organizational capability which considers culture, shared responsibilities, stakeholder buy-in and business support to ensure continuity. Even if you have all the right measures in place, things can and will go wrong.

Unlocking the business value of intelligence aids in managing down risk. But the key is making it timely and actionable. How you may ask?

- Identifying relevant threats that matter most improves situational awareness – determining adversarial motivations, capabilities, attack vectors, known tactics, techniques, procedures;
- Gaining visibility into attack surface exposure – known exploitable vulnerabilities, leaked credentials;
- Enhancing protections and coverage – threat detection, proactively orchestrating security controls; indicator sharing across borders;
- Reducing speed to detect and respond – automating response playbooks for containment/remediation;
- Improved crisis planning and management – simulating attack scenarios based on real-world threats

Cyber resilience and preparedness go hand in hand with threat intelligence. A resilient business will therefore optimally manage downtime by ensuring the "lights continue to stay on" without adversely affecting operations – minimizing breach scope and impact. This enduring journey starts with understanding the risk landscape: just as a lighthouse shines light to navigate dangerous hazards; threat intelligence provides insights and actions required to swiftly navigate its own kind of threats. Those organizations who effectively integrate intelligence will ultimately be best served by it.

CTA Member Research Spotlight

RANSOMWARE AND INDUSTRIAL CONTROL SYSTEMS

DRAGOS

By Anna Skelton, Senior Intelligence Analyst, and Kyle O'Meara, Principal Adversary Hunter, Dragos

For an organization to remain resilient against potential ransomware attacks, recommendations will remain the same regardless of the ransomware group. The first step should always be conducting architecture reviews to identify all assets, connections, and communications between Information Technology (IT) and Operational Technology (OT) networks.

In December of 2020, Dragos published a whitepaper highlighting the magnitude of this problem, showing that ransomware attacks on industrial control system entities increased more than 500% from 2018 to 2020. Most of these attacks targeted the enterprise IT operations of industrial companies, however, due to poor network segmentation practices and unsecured work from home techniques, they were able to have a significant impact on or pose a major threat to OT systems.

Our most recent research shows that this trend has continued into 2021 with an increase in high visibility ransomware attacks including Molson Coors, Honeywell, Colonial Pipeline, and JBS Foods. Out of 79 ransomware attacks against industrial control system targets tracked by Dragos in June, July, and August, 56% targeted the manufacturing sector. Out of the total 79 attacks, 60% were conducted by two Ransomware-as-a-Service double extortion groups, Lockbit 2.0 and Conti.

In the Ransomware-as-a-Service (RaaS) model, adversaries establish a ransomware platform that is then leveraged by affiliates to target industrial companies, typically with access purchased from a third party. Despite advances in security technology, phishing and a lack of multi-factor authentication remain key vectors for attackers to gain access to IT and OT networks or, as is often the case, to IT first and then OT networks later, causing disruption to industrial control systems entities. Affiliates will then deploy double extortion ransomware, exfiltrating data before locking down systems and threatening to leak the stolen data if the ransom is not paid. This can bring an abrupt halt to operations and cause damage, injury, and loss of life. Any profit gained from ransom payments is typically split between the platform developers and the affiliates.

While a ransomware attack on an industrial IT network may be an inconvenience, a successful attack on an OT network could lead to severe disruption, potentially resulting in loss of life. Dragos has developed a tried and tested approach to helping our customers defend against, or respond to, disruptive ransomware incidents in their operations environments.

*For more information on the threat of ransomware to ICS environments – impacting production and operations as we have seen in the first half of 2021 – join CTA at **VB2021** for Anna and Kyle's talk on protecting ICS environments from ransomware.*

ANNA SKELTON
SENIOR INTELLIGENCE ANALYST
DRAGOS

KYLE O'MEARA
PRINCIPAL ADVERSARY HUNTER
DRAGOS

SAMANTHA MADRID
VICE PRESIDENT, SECURITY BUSINESS & STRATEGY
JUNIPER NETWORKS

CTA Board Member Spotlight

JUNIPER NETWORKS' REFLECTION ON CTA MEMBERSHIP

Juniper Networks was eager to join the Cyber Threat Alliance, as we share the belief that the fight against attackers cannot be won by each vendor acting alone – we all must work together if we're going to turn the tides. In today's turbulent environment, it's especially important that threat-intelligence information sharing becomes commonplace. If you don't know what you're looking for, it becomes difficult to protect the network from an attack.

Individually, each CTA member has visibility into a piece of the threat landscape. The Cyber Threat Alliance facilitates a collaborative environment and provides the opportunity for members to come together to chip away at the advantage attackers may have. When the pieces are combined, it is possible to better protect organizations, which benefits everyone.

Providing customers with a safe and secure experience is an essential part of good customer service. As members of the Cyber Threat Alliance, we share and receive unique Indicators of Compromise (IoCs). This intelligence gets fed into Juniper's SecIntel and Advanced Threat Protection (ATP) services so that customers are better able to automatically detect and defend against the newest kinds of attacks across a much broader set of attack vectors. Juniper also finds tremendous value from the CTA's Early Share program. Blogs are received by member companies ahead of public disclosures, which allows time to enact defensive measures for customers before threat actors are alerted and before copycats attempt similar attacks.

Working with the Cyber Threat Alliance has allowed the teams at Juniper Networks to embark on new and exciting projects, such as creating new algorithms based on shared intelligence that will improve organic threat detection capabilities, and working on value-added partnerships and technical integrations with other member organizations.

It's not just the data and mission of the CTA that is valued, but the relationships that have been built and will continue with members from other organizations because each individual offers a different and unique perspective. Diversity and inclusion is valued within working groups and teams because they are tasked with solving some of the world's toughest challenges! Challenges that can only be addressed by bringing different ideas and perspectives to the forefront. At Juniper Networks, diverse world views breed innovative ideas. Juniper is excited to infuse the CTA with those values, and I am particularly excited to be the CTA's first female board member. Representation matters, and hopefully other talented women and underrepresented individuals in cybersecurity will see more diversity in leadership positions and gain the confidence and opportunity to become leaders themselves.

In today's world we are constantly faced with new cybersecurity challenges and are always looking for innovative ways to mitigate concerns. Although progress can seem doubtful at times with new attack techniques emerging, IoT device numbers increasing, and network architectures becoming more complex, breaches most often boil down to humans as the common weakness. One of the most significant cybersecurity challenge is removing human fallibility from the attack vector equation. If vendors can work together to mitigate the threat of attackers exploiting human vulnerability, I have faith that we can overcome the challenges associated with this.

As a proud member of the CTA, Juniper hopes to continue to promote the importance of data sharing. Organizations like the Cyber Threat Alliance will be at the forefront of leading this movement and encouraging others to collaborate to ensure the safety of the global digital ecosystem.

NEIL JENKINS
CHIEF ANALYTIC OFFICER
CYBER THREAT ALLIANCE

CTA Working Groups

LOOKING BACK AT CTA'S OLYMPICS CYBERSECURITY WORKING GROUP

CTA continues to identify areas where we can share information and collaborate on defensive issues. The Olympics have become a common target for a variety of cyber incidents, such as criminal activity, espionage, and disruption. In the summer of 2019, with the 2020 Tokyo Olympics approaching, we established the Olympics Cybersecurity Working Group (OCWG). This community focused on the potential threats and was ready to respond to any significant incidents that occurred.

CTA's event-focused working groups, such as the OCWG, follow a three-part plan: Share, Partner, and Prepare. For the Olympics, we did what CTA is best at. We provided a forum for a trusted group of experts to share information on what they were seeing. The OCWG then took this a step further and built CTA's first threat assessment. The assessment included a review of cyber incidents seen in previous Olympics, the likely threat actors, the operations and tactics they could use, the potential targets, and the security environment. The threat assessment represented a collective view of CTA's focus areas for the games. After the Games were delayed due to the COVID-19 pandemic, we updated the threat assessment in April 2021 based on the new threat landscape.

Our working groups provide a focused partnership within CTA. But we also leverage these groups to engage with external partners. CTA built a relationship with the Tokyo Olympic Committee and government agencies in Japan to make them aware of our activity and give them an opportunity to reach a significant section of the cybersecurity community at once. We provided the Threat Assessment to the Tokyo Organizing Committee for their use in preparing for the 2020 Summer Olympics. We also posted it online so that others could leverage the expertise of CTA's members. These partnerships expanded the reach of our work, helping to increase the security of the entire ecosystem.

Finally, our working groups give us an opportunity to prepare for any significant cyber incidents that our members may encounter. For the Olympics, the threat assessment provided the blueprint for our planning. It provided scenarios for us to consider and plan for how CTA members could collaborate during that incident. We used these scenarios to update CTA's incident collaboration framework specifically for the Olympics. We were ready to bring members together in a moment's notice to share information on what was happening and how we could best respond. Best of all, we already had the main points of contact for the Olympics together and they knew each other. If a significant incident had occurred, we were ready to convene the right people and avoid a scramble in the middle of an incident.

CTA is in the process of collecting lessons learned from the OCWG to improve future event-focused working groups. Through such efforts we can leverage CTA's core principles to improve our global ecosystem.