DECEMBER 2020

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

Friends of CTA,

Whew. 2020 is almost over. Like many people, I will not be sad to see this year end. The loss of life, the negative psychological impact, the economic disruption, and the social upheaval associated with the pandemic have made 2020 a time few of us would want to repeat. Yet, at the same time, the pandemic has magnified the importance of cybersecurity. The explosion in remote work and the dependence on virtual capabilities has transformed cybersecurity from an important consideration to a critical one for many organizations. As a result, the cybersecurity industry ended up with even more work and more responsibility over the course of this year.

The pandemic's effects on CTA have been mixed. On the one hand, we missed the opportunities to connect with existing and potential members at conferences and other events. On the other, the enforced "home" time enabled us to start a **webinar series** and establish a more regular cadence for the **CTA blogs**. We were also able to actively support more external working groups, such as the World Economic Forum's Partnership Against Cybercrime, because all the meetings were virtual.

Beyond these effects, though, CTA continued to hit key milestones. We welcomed two new members, OneFirewall and Anomali, and we deployed our new sharing platform, Magellan. We passed the **100,000,000th shared observable** mark as well as the 300th early share. CTA's Olympic Cybersecurity Working Group produced a **report** on cyber threats to the Tokyo Olympics, and our Election Security Working Group was on stand-by to support state and local election officials during the 2020 U.S. elections.

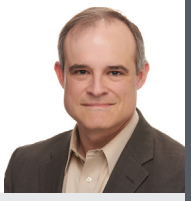
By many measures, 2020 has been a successful year for CTA.

Looking forward to 2021, CTA will continue to grow and mature as an organization. Even if the pandemic begins to recede next year, the workforce changes and digital dependence it accelerated will not be reversed. Nor have the bad guys taken a break; if anything, they have become more brazen. Ransomware attacks have emerged as a major problem for the digital ecosystem. In this kind of environment, the need for cybersecurity providers to share threat intelligence will continue to grow. CTA fills a unique role in this regard for cybersecurity companies by making such sharing regular, scalable, and sustainable, whether in automated or human form. We will also remain engaged with groups like the WEF's PACC, the New York Cyber Task Force, and the Aspen Cybersecurity Group, and we will promote sound cybersecurity policies and practices wherever we can.

We remain committed to CTA's core mission: enabling our members to better protect their customers, using shared information to disrupt malicious activity, and raising the level of cybersecurity across the ecosystem. I look forward to working with you in achieving these goals.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance



CTA WELCOMES ANOMALI & ONEFIREWALL

In mid-November, CTA welcomed two new members into the fold: **Anomali** and **OneFirewall**. These additions are welcome news at the end of this chaotic year, and increase the size of CTA's membership to 28 companies from across the cybersecurity industry and across the world.

ANOMALI®

"When the industry comes together, collective defenses are strengthened and risks are reduced. We're pleased to join CTA and are looking forward to working together."
— John Callon, VP of Solutions & Partner Marketing, Anomali

OneFirewall

"CTA's mission is critical and it led the way. OneFirewall is pleased to be part of the change while better protecting its clients."
— Gabriele Ruzzu, CEO, OneFirewall

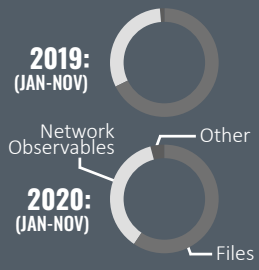
YEAR-END SHARING SNAPSHOT

TOTAL OBSERVABLES SUBMITTED

47 MILLION
SINCE MARCH 2020
(MAGELLAN PLATFORM UPDATE)

110+ MILLION
SINCE FEBRUARY 2017
(CTA PLATFORM 1.0)

OBSERVABLES DIVERSITY



TOTAL EARLY SHARES

150+
2020 YTD

330+
SINCE THE START OF OUR EARLY SHARING PROGRAM IN MAY '18

STRONGER TOGETHER

The events of 2020 have shown that now, more than ever, we need to be actively creating and leveraging opportunities for collaboration in strengthening cybersecurity across the digital ecosystem. The value of CTA rests on the fact that we are stronger together. We know that by bringing this community of defensive actors together, our members are able to more effectively prepare for and respond to major threats. In this feature, we showcase how three of our members perceive the value of CTA's collaborative approach.

As a founding member, Fortinet has seen the CTA grow and evolve since 2014. From the initial idea to create a cyber threat intelligence organization of peers, CTA has always been big on vision, but I think 2020 is really the year that the execution of that vision took hold. This execution has really demonstrated the value of "Stronger Together" as more members benefit from the very things CTA was designed to provide. A main reason for this would be the power of diversity.

First, the increasing diversity of CTA membership provides additional perspectives that can be valuable in addressing different cybersecurity topics and issues. For example, the addition of a member focused on operational technology (OT) brings an important perspective into vulnerabilities, threats and actors. The same with new telecommunication, incident response, and CERT members. These new members also improve the global coverage of CTA as their data centers are spread throughout the world. The diversity of different members focused on different aspects of cybersecurity and threat intelligence covering different parts of the world provides a more complete picture of the threat landscape than any one company could ever achieve on its own.

The second type of diversity benefiting us all is found within our intelligence sharing. Initially, it was usually only founding members sharing information and what they shared most were file samples. Now, with the launch of the Magellan platform to automate information sharing earlier this year we've seen many different members taking advantage of it so we're seeing different viewpoints come in to play. And we're seeing an increase in the different types of IOCs being shared, such as registry keys. With each new IOC type shared, the more context we get. This year, more members came to the table with early shares which has been wonderful and very useful. With our new members, new perspectives, and new IOCs being shared, the collective intelligence available to CTA is a true example of being stronger together.

FORTINET®

DEREK MANKY
CHIEF, SECURITY INSIGHTS & GLOBAL THREAT ALLIANCES

As 2020 thankfully comes to a close and I look back at the impact the global pandemic has had on enterprises around the world, we're truly impressed with everyone's ability to adapt. Unfortunately, adversaries did the same and tried to take advantage for their own gain, making threat intelligence sharing more important than ever.

Our membership in CTA provided a pre-built network of trusted individuals we could share research with to ensure our knowledge of the threats had the widest impact when it was most necessary. The data we received back from CTA members helped us provide even better protection for our own customers. A worldwide crisis didn't inspire us to establish the CTA, but in these moments I'm certain that we are much stronger with the alliance than without.

paloalto® NETWORKS

LEE KLARICH
CHIEF PRODUCT OFFICER

*No one can deny 2020 has been a b*ch of a year. But, through the haze of undefined work hours, relentless COVID-19 news coverage, escalated attacker trends, and much more, there have been some shining moments when it comes to advancing our collective mission to share threat intelligence for positive impact.*

In March 2020, as lockdowns to contain the spread of COVID-19 were implemented rapidly across the world, Sophos chief scientist, Joshua Saxe put out a call on Twitter. Appalled that criminal groups were starting to incorporate references to COVID-19 into a range of cybercrime campaigns, information security analysts – more than 4,000 of them – banded together in a collective show of defiance and formed the COVID-19 Cyber Threat Coalition (CCTC) in a Slack channel created that same day. Since then, the CCTC's work has helped to protect millions of people from becoming victims of cybercrime – a magnitude only possible with the outpouring of collective, unified effort and resources from the volunteers. CCTC works closely with CTA to improve data sharing and product protections among CTA members, and has become an enduring, repeatable foundation our community can use when we need to join together in times of crisis.

Ultimately, success stories about sharing threat intelligence tell us about more than just the names of the organizations joining forces. We learn about character, and we learn about intention. After all, the true shape of complicated things emerges from the union of our experiences. For example, while the CCTC's collaborative initiative protected millions of people from becoming victims of cybercrime, that alone wasn't why the group was successful. It thrived because the core motivation of the members and founders has been to, first, protect anyone who might be in harm's way. There was no profit motive, just a desire to defend those in need, while it seemed like the wolves were at the door. This proves the model is correct, and bridges critical gaps in coverage none of us alone could generate, but we can do more with it. As an industry, we may in the future want to consider sharing machine learning models, or training datasets, just as we share block lists or Yara rules today. We could also strengthen and contribute to emerging standards like STIX and the ATT&CK framework. And, we could participate in industry-specific ISACs and ISAOs. There are many possibilities, and thanks to the CTA, we are that much further ahead to – together – make more positive impact in 2021.

SOPHOS

SARA EBERLE
HEAD OF GLOBAL PUBLIC RELATIONS

JOE LEVY
CHIEF TECHNICAL OFFICER

Neil Jenkins, CAO, on CTA's sharing success in an abnormal year

A SILVER LINING ON 2020

It's safe to say that CTA's sharing and collaboration activities weathered all of the weird 2020-ness of 2020 quite well. Our experience as a mostly virtual community allowed us to continue operations even as the COVID-19 pandemic limited any opportunities to meet in person for happy hours or meetings. We were able to stay strong, share information, and collaborate through some fairly rough times.

As CTA members migrated to our new platform, Magellan (see right), the total number of shared observables continued to increase throughout the year, approaching 7 million per month. Members are sharing more data, more diverse data, and including more context, such as first- and last-seen and ATT&CK techniques. We also now engage with members more routinely to provide feedback on the data they share to improve standardization and get our members the information they want most, such as file samples. We appreciate our members responding to our feedback to help everyone get the best data possible.

But we can't do it all through automation alone. In 2020, the human-to-human sharing through our Algorithm & Intelligence (A&I) Committee continued to blossom. Through October, members shared over 150 reports through the early share program, reaching a record 20 early shares in October alone. CTA built a relationship with the U.S. Government to get early access to malware samples that will be shared broadly to expose nation-state activity. CTA members reap the benefits of these efforts to prepare their protections in advance of release. Together, our members disrupt adversary activity and protect their customers quickly and efficiently.

The A&I community was also quick to share and collaborate around the immediate concerns of the day in a wild year. We rapidly came together to discuss threats related to COVID-19 lures and malicious domains. We leveraged our A&I discussions to discuss the constant threats of ransomware, DDoS, and other malicious activity tracked by our members. We pulled together resources to develop a joint threat assessment for the Olympics and plan for cyber-related disruptions to the 2020 U.S. elections. Our community approach allows us to quickly pull together a team of experts to work on tough topics.

As we've noted many times before, CTA benefits from the trust between our members. Trust allows them to share high quality information and collaborate both via automated means and through our human connections. 2020 was a pretty awful year for a lot of reasons... but at least we can say that CTA's sharing was a highlight!

Jason Minick, CTO, on our new sharing platform: Magellan

SETTING A NEW STANDARD

This year saw the culmination of extensive work to rebuild our automated sharing platform from the ground up.

The enormous amount of effort that went into this overhaul — both internally and in collaboration with our members — has paid off.

Now that all CTA members have been transitioned to the new platform, Magellan, the results are clear for all to see. We have developed a truly cutting-edge threat intelligence sharing environment.

While our original platform ("CTAP") was similarly ambitious at the time it was created, we always knew that the pace of change in the industry and CTA's membership growth would ultimately necessitate this kind of comprehensive update.

There are numerous ways in which our new Magellan sharing environment outperforms the original CTA platform.

Magellan is more adaptable than its predecessor, and an emphasis on user-friendly and intuitive design cuts across its core features. For example, Magellan's drag-and-drop "Bundle Builder" allows members to rapidly prototype data submissions to better tune their backend workflow. Similarly, a centralized UI, enhanced search functionality, and powerful visualization capabilities help users to more readily pinpoint the insights that they're looking for.

Integrating new members onto the old platform was a somewhat convoluted process, a problem that Magellan has largely solved. It allows us to offer a demo environment for prospective members to get hands-on with the interface and enables them to extract sample data while protecting the overall integrity and security of members' submissions to the production environment.

Integration is as easy as consuming RESTful endpoints, giving our members the flexibility to seamlessly integrate CTA's shared data into their existing frameworks. Our use of the gold standard STIX 2.0 threat intelligence data format ensures that when members make submissions and extract data from our platform, that it is not only standardized and machine-readable, but has the highest available level of linguistic granularity, which in turn means that our data can be both richer and more actionable.

Moving forward, we'll continue to upgrade our platform with the goal of improving sharing functionality and ensuring that our infrastructure is robust to both the changing industry landscape and to future membership growth.

In the meanwhile, we feel good knowing that we're at the forefront of threat intelligence sharing and grateful to our members for joining us on this journey.

CTA Member Spotlight

NTT

WITH MARK THOMAS

SENIOR THREAT INTELLIGENCE DIRECTOR

WHY DID NTT JOIN CTA?

We want to make a difference. Combatting cyberthreats requires global cooperation. NTT is committed to making contributions to society through our business operations and corporate activities. We believe in using technology for good and contributing to international efforts to promote risk management as a key element of cybersecurity in today's world.

Through our membership with CTA, we're able to build trust and improve security hygiene by actively participating in threat research and sharing our intelligence to benefit industry and the broader digital ecosystem.

WHAT DOES NTT VALUE MOST ABOUT CTA MEMBERSHIP?

The value CTA provides is the collective approach in stemming the tide of cybercrime. There is strength in diversity. Members within CTA cover an extensive list of specialized cybersecurity companies, each with a unique view of the threat landscape. By piecing different parts of the puzzle together we can make new discoveries. No organization can individually manage complex threats in isolation.

HOW DOES BEING PART OF CTA HELP NTT TO STRENGTHEN SECURITY FOR YOUR CUSTOMERS?

The threat intelligence collaboration NTT enjoys with our CTA partners serves as a force multiplier by way of visibility into threats supported by subject matter experts. Collaboration through CTA helps enable NTT to gather and process information and intelligence beyond that of our own reach, and use that input to help improve our own intelligence as well as supported technologies and services. Through our partnership we can act faster and more effectively to minimize harm to our clients.

WHAT ARE YOU MOST EXCITED ABOUT IN TERMS OF THE WORK YOU'VE BEEN ABLE TO DO THROUGH CTA?

CTA membership has enabled us to continue maturing our security research as well as helping to build deeper relationships with other CTA members. Our joint research focused on emerging threats targeting major events such as the 2020 Tokyo Olympics has also been well supported. This open and transparent dialogue creates trust which better serves the cybersecurity industry.

NTT IS A REGULAR CONTRIBUTOR TO OUR EARLY SHARING PROGRAM. CAN YOU TALK ABOUT THE VALUE THIS PROGRAM BRINGS AND WHY YOU SUPPORT IT SO STRONGLY?

Intelligence without action is worthless. CTA's Early Sharing program allows us to contribute and receive vital intelligence, which can be leveraged in an actionable way. When we discover new insights or context which could mutually benefit other members, it is important to share. Reciprocity here is key; success comes down to the free flow of information amongst CTA members leading to better solutions and technologies, with earlier, stronger protections for all.

While shared information is generally under embargo until the originating member goes public, this window allows NTT to conduct supporting analysis within our research teams, collaborate with our multiple SOCs, proactively hunt for IoCs, and prepare protections as well as clear communications for our clients before the information is publicly available. This has contributed significant value to NTT and our clients behind the scenes.

WHY IS INFORMATION SHARING SO IMPORTANT IN TODAY'S TUMULTUOUS CYBERSECURITY ENVIRONMENT?

Cybercrime is borderless and therefore our response also needs to be borderless. Information sharing is not new, but more recently we've seen growth in its adoption. The threat landscape is asymmetric. We know threats continue to evolve – rising rates of internet connectivity, and growing dependence upon technology within society contribute to this. This evolution creates risk.

To counter that, a "Detect once, share with many" approach enables participants to reduce mean time to respond and will raise the level of situational awareness across the entire digital ecosystem. This frees up human capital to focus on other more advanced threats.

WHAT DO YOU SEE AS THE MOST SIGNIFICANT EMERGING CYBERSECURITY CHALLENGES AND HOW CAN CTA HELP TO MITIGATE THESE CONCERNS?

COVID-19 has emphasized the need for organizations to be cyber resilient and to dynamically respond to the shifting threat landscape. The rise of remote working amid the pandemic has heightened technology-related risks, making it crucial for all organizations to review their architecture and controls. CTA plays an integral role by facilitating a collaborative environment in which members can openly exchange threat intelligence for use within their products/services.

As CTA onboards new members, all members will have even better visibility into the threat landscape.

CTA engagements in the year of COVID

2020 EVENTS RETROSPECTIVE

Through the disruption of COVID-19, CTA has maintained a steady cadence of virtual event attendance and worked hard to engage the cybersecurity community around issues related to information sharing. This includes sponsoring and coordinating the Threat Intelligence Practitioners' Summit at the **Virus Bulletin Conference** in late September.

More recently, we attended and co-sponsored the **Association of Antivirus Asia Researchers (AVAR) Conference** and emphasized to practitioners the importance of enhanced threat intelligence sharing across this important geographic region.

We also co-sponsored **CyberNextDC**, a staple of the CTA events calendar going back to our inception as an organization. This event was once again a great success. CTA staff and members participated in a range of panels, including discussions of the lessons learned about securing elections over recent cycles.

In addition, 2020 saw the launch of CTA's **webinar series**, which features cybersecurity leaders and threat intelligence researchers in discussion with members of CTA's leadership team. These webinars are still freely available on-demand:

Taking a Byte Out of Cybercrime
with Kristin Judge from the Cybercrime Support Network

Key Findings from Netscout's 1st Half 2020 Threat Intelligence Report
with Richard Hummel from Netscout

Stasis or Progress: Taking a Long View on Cybersecurity Policy
with Neill Sciarrone from Trinity Cyber

The Road Not Taken: Why Routing Security Matters
with Alissa Starzak from Cloudflare

The Power of Collaboration: Creating Adversarial Playbooks to Disrupt Malicious Actors
with Rick Howard from CyberWire

Making the Impossible Possible: How We Built a Successful Threat Intelligence Sharing Program Where Competitors Trust and Collaborate
with Derek Manky from Fortinet

How Threat Sharing Hones Your Competitive Edge
with Michael Daniel from CTA