SEPTEMBER 2020

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

Friends of CTA,

Among the various themes for 2020, strangely waiting seems to be a prominent one. Waiting for a vaccine, waiting to see how on-line education for our kids works, waiting for the economy to improve, waiting for normal routines to begin again – waiting seems to permeate many people's lives around the world right now.

Unfortunately, our cyber adversaries are most definitely not waiting. Malicious cyber activity shows no signs of abating and using cyber means to promote scams and misinformation is only increasing. As a result, CTA and its members are staying busy. During the summer, members submitted more than 14 million observables to CTA's Magellan platform. Early sharing activity maintained its steady cadence of around 4 per week, and member representatives continued to meet bi-weekly to discuss the latest threat trends and research. We reached partnership agreements with the Center for Internet Security, the Information Technology Information Sharing and Analysis Center, and the CSIRT Asobancaria. We did not have a lazy summer.

Heading into the fall, we are looking forward to the usual conference season, even if it will be a little different this year. We are supporting the Billington Cybersecurity Conference in early September and sponsoring the Threat Intelligence Practitioners Summit virtual talks that will be part of the annual Virus Bulletin conference at the end of September. We have lined up a great set of speakers for this event. Be sure to check out CTA's virtual booth at VB2020. And although I will miss the chance to go to Vietnam, CTA will still sponsor the Association of Anti-Virus Asia Researchers' conference.

Finally, I am pleased to welcome Josh Kenway to the CTA staff. We brought Josh on board in the summer of 2019 as a graduate intern and then kept him on part time as he finished his Master's degree at Stanford. Josh started with us full time in August as a Cybersecurity Associate. We are very glad to have him working with us, including on communications products like this newsletter.

Thanks to all our current members for your continued support. To our potential members, I know uncertainty continues to loom large. But I would urge you to consider CTA as a way of hedging your bets. CTA members can draw upon a wide community to answer questions, resolve issues, and respond to cyber threats rapidly. Becoming part of that community would give you a little extra insurance against a bad day in cyberspace. Drop us a line and we'll be happy to talk about the value CTA can provide.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

JOIN CTA FOR VIRTUAL VIRUS BULLETIN 2020

As COVID-19 has continued to disrupt global society, CTA and Virus Bulletin have persevered to deliver what we are confident will be a successful online-only conference to be held September 30th to October 2nd. "VB2020 localhost" is the annual and world-renowned Virus Bulletin international conference gone virtual.

Join us for a CTA-sponsored track at VB2020, the Threat Intelligence Practitioners' Summit (TIPS), to learn how threat intelligence is being deployed as a force multiplier to dramatically increase the effectiveness of cybersecurity products, services, and teams.

This event track will feature keynotes and panels with representatives from CTA members and partners including Fortinet, Palo Alto Networks, Sophos, Dragos, Scitum, and the Dutch NCSC. See details of the full TIPS program here.

It's no conference without a great community, so we hope you'll visit our virtual booth and join us on our VB2020 Discord channel.

Registration is available now.

QUARTERLY SHARING STATISTICS

June - August 2020

TOTAL OBSERVABLES SUBMITTED

14 MILLION

OBSERVABLE DIVERSITY

FILES **59%**

NETWORK OBSERVABLES **41%**

EARLY SHARES THROUGH CTA

47

WEEKLY AVG: 3-4

TOTAL OBSERVABLES SUBMITTED
Since Feb '17

>100 MILLION

(9/9/2020)

CTA Member Spotlight

Symantec™
A Division of Broadcom

WITH JOE CHEN, BROADCOM INC.
ENGINEERING, SECURITY TECHNOLOGIES & ALL ENDPOINT SOLUTIONS

WHY DID SYMANTEC HELP TO FOUND CTA?

We wanted to help create an avenue to collaborate across the industry and share threat intelligence more effectively. Members have worked together on committees and working groups to build trusting relationships. This has gotten us to the point where we are today, where sharing and collaboration is constant and automatic.

WHAT DOES SYMANTEC VALUE MOST ABOUT CTA MEMBERSHIP?

We value the intelligence we receive from other members across a variety of geographical locations and diverse industries and the mutual validation of shared intelligence. These allow us to rapidly deploy protections and improve protections for our shared customers.

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

Early sharing enables members to quickly verify or add detections and protect all of our customers against the bad actors. Additionally, we are all comfortable working together in a steady state, so we can jump right in to respond to a cyber incident as a group when needed.

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

I am excited about the future of our new automated sharing platform. A lot of work was put into the platform to get to where it is today, and it has a scoring system that rewards sharing valuable context. It easily allows all members to share intelligence, validate the intelligence we receive from other members, and quickly deploy detections.

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

Our research reflects our rich telemetry and wide portfolio. We share as much as we can to help others in the industry. Staying competitive in this industry is about what you do with intelligence, not about what unique intelligence you have. By sharing early, members are able to review and prepare defenses in real time, improving the ecosystem as a whole.

Looking back and ahead on information sharing through CTA

RICK HOWARD: CHAMPION ON A MISSION

Rick Howard is a military and cybersecurity industry veteran, a former CSO for Palo Alto Networks, and currently serves as CSO, Chief Analyst, and Senior Fellow at CyberWire. We joined Rick in his virtual podcast studio, the venue for CyberWire's CSO Perspectives, for a conversation about CTA and its role within the cybersecurity industry. While at Palo Alto Networks, Rick was involved in the early development of CTA, and we are delighted to have him back on board as a CTA Champion, advocating for our mission within and beyond the community.

In the final two years of his 23-year career in the U.S. military, Rick Howard was running the show at the U.S. Army CERT. In this role, he was responsible for coordinating between offensive and defensive operations to avoid metaphorical entanglements of each side's virtual wires.

"It was horrible back in those days; it was all turf wars," Howard recalls. "Everybody thought that what they were doing was the only thing that mattered. Even the defensive people and the offensive people within the Army itself didn't want to talk to each other."

Howard is similarly unequivocal in asserting that this philosophy of walled gardens and blinkered perspectives was in no way unique to the armed services or to the American context. "That culture has been in the network defender community forever," he emphasizes.

"We used to think that the intelligence that each company collected was somehow proprietary and that what mattered was that my intelligence was better than your intelligence, but that's not true at all. You might have one piece that I don't have, but I know that I have two pieces that you don't, so it would be better if we were to combine our efforts."

There were many moments where, Howard suggests, one might have thought that this approach would finally hit a dead end. However, progress on information sharing has been at best incremental since those early days, and, at times over the past two decades, even entirely stagnant. Despite numerous crises and failures arising from an atomized approach to securing the digital ecosystem, in many parts of the industry that perspective remains in ascendance.

"Since the 1990s, we had been sharing threat intelligence among peers with emails, spreadsheets, and documents, but for a long time nothing really changed. The great innovation of the Cyber Threat Alliance was in realizing that to get in front of the bad guys, we needed to automate that process."

Out of this regularized, automated sharing, CTA has been able to build trusted mechanisms and venues to facilitate gradually more sensitive cooperation, including through our Early Sharing activities. "What's great about that," says Howard in reference to this growing program, "is that it is something we can point to that speaks directly to the value of CTA."

Looking forward, though, Rick Howard wants to see more sharing, with a higher degree of automation, across a larger number and variety of trusted parties. Moreover, he says, "we want the members of CTA to share everything they know about every adversary that they're tracking, down the intrusion kill chain, for all the products that they offer."

"This is obviously a huge vision," admits Howard, "but it is the security umbrella that we need."

Threat intelligence sharing has not, historically, been a natural or risk-free activity for cybersecurity providers and government institutions. However, when sharing intelligence through CTA, "we all agree to follow the same rules and the additional protection extends across the entire community, so misunderstandings can be avoided."

Howard sees himself as a cheerleader. "I always want to go faster. I want us to get there next week; and I'm frustrated at the glacial pace that the industry is moving in terms of buying into the vision."

But in his role as a CTA Champion, and now removed from direct involvement with CTA through Palo Alto Networks, Howard relishes the prospect of combating the naysayers: "I can really challenge people who don't agree with the philosophy of what CTA is trying to do."

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

Cybersecurity is a team sport. We recognize that there is always room for improvement; we can always be better. Sharing intelligence always helps further protect our customers and our customers' customers. These are our families, friends, and neighbors. Helping each other benefits everyone.

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

Cyber criminals are constantly evolving. They take advantage of what is going on in the real world and when significant events happen, they attack. CTA is built on trust and collaboration; with this, we collectively get ahead of the bad guys.

Timely collaboration for stronger cybersecurity defense

IN FOCUS: CTA EARLY SHARING

Through our Early Sharing program, members regularly share critical defensive information with one another through CTA in advance of public release. This sharing can involve the distribution of analysis, blog posts, research findings, and samples related to malicious cyber activity. Critically, it enables our members to respond more effectively to these publications. Members can leverage their data, analysis, and cybersecurity products to expose malicious activity more broadly, prevent additional harm, and mitigate risks quickly ahead of time, rather than scrambling to protect customers after reports are made public.

We typically see between 2 and 4 early shares per week from our members, and have had over 280 early shares since the program first began. Members retain control over their analysis, with the sharing member designating an embargo period and protocol (TLP:RED, for example) for each share that they make. This program is managed through CTA's Algorithm & Intelligence Committee, which includes all CTA members, ensuring equitable participation regardless of membership level.

TOTAL EARLY SHARES SINCE MAY 2018

280+

For cybersecurity companies – whose bottom line depends on being ahead of the curve on emerging threats – to open a window into their investigative approaches and share their insights for the collective good would have been unthinkable just years ago. The fact that CTA has been able to facilitate this level of impactful sharing reflects the confidence of CTA members in one another, as well as in our organization, processes, and infrastructure. This program now forms a crucial part of CTA's day-to-day operations, and our members recognize and appreciate its value to their businesses, as well as to the overall security of the digital ecosystem.

CISCO'S LEAP OF FAITH: MAKING EARLY SHARING 'NORMAL'

with Matt Olney, Director, Talos Threat Intelligence and Interdiction, Cisco

WHY WOULD CISCO WANT TO SHARE DEFENSIVE INSIGHTS WITH COMPETITORS THROUGH THE CTA EARLY SHARING PROGRAM?

Early Sharing allows us to achieve force-multiplication for the impact of our research, meaning that the work we do at Cisco can protect more people. It's also great for our business that other CTA members are doing the same thing in-kind. We are able to get heads-up information about what's going on that we may not otherwise have had access to, allowing us to build better protections for our customers.

WHAT WERE THE MAJOR OBSTACLES TO EARLY SHARING AMONG CYBERSECURITY PROVIDERS THAT EXISTED PRIOR TO CTA?

The biggest obstacle was the lack of a clear framework for sharing, which CTA now provides. Being a member of CTA gives us the ability to work directly with the intelligence teams of other companies on a consistent basis, including through personnel moves and changes in structure. Having this persistent framework of connections in place ahead of time gives us an overarching construct that helps us tackle major problems that we have to work together to solve.

WHAT MOTIVATED THE TEAM AT CISCO TO SHARE YOUR VPNFILTER RESEARCH IN 2018 PRIOR TO GENERAL PUBLICATION?

We were eager to get that information out because we were concerned about what the actor might do if we didn't have a cohesive, industry-wide response. CTA was the perfect instrument in that moment for us to use in creating as broad a response as possible.

WHAT DID YOU TAKE FROM THAT INITIAL FORAY INTO EARLY SHARING?

It was one of the most interesting points in my career; and it reinforced that what we were sharing was important. We were briefing some of the smartest people in the industry – research team leads from different security companies – and had to hold our ground, defend our research, and explain why it mattered. This allowed the other teams to act with confidence on that information, because they had been able to challenge and come to understand our assertions.

HOW HAS THE GROWTH OF CTA'S EARLY SHARING PROGRAM SINCE 2018 BENEFITED CISCO?

Our first early share was critical in normalizing that kind of sharing to a point where we now receive multiple early shares per week. This gives us a good sense of where different research groups are heading and what they're looking at. There is no shortage of malicious activity out there for us all to investigate, and there are very few organizations that are dedicated to facilitating this kind of sharing. Having a defined set of companies that we are interacting with and exchanging information ahead of time is really beneficial. The program also allows us to contribute observations, questions, and feedback on the actors that different groups are focused on. In that sense, the human-speed dynamic for early sharing of blogs, research, and so on works really well.

HOW DO YOU EXPLAIN THE VALUE-ADD OF CTA AND OUR EARLY SHARING PROGRAM TO YOUR CUSTOMERS?

Like anything else in sales, it depends on the customers. Some are savvy enough to be interested in this space and ask those kinds of questions, so we make sure that our sales force understands how we work together and what 'wins' for our business result from our membership with CTA. For certain customers to trust in our business, it is important that Cisco be seen as part of the broader security ecosystem, rather than a standalone vendor.

HOW WOULD YOU LIKE TO SEE THE EARLY SHARING PROGRAM EVOLVE AS CTA CONTINUES TO GROW?

CTA already has different kinds of members and every company has its own unique viewpoint onto the threat landscape. With a larger and more diverse CTA membership, we'll be able to get an even broader set of outlooks and develop a more complete understanding of adversarial activity.