JUNE 2020

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

Friends of CTA,

In our last newsletter, I described 2020 as a roller coaster. That description seems even more apt now, six months into the year, as a global pandemic, economic uncertainty, and political unrest make the cybersecurity environment even more challenging. We are entering a phase Toffler Associates refers to as "the Great Wait" – the period between the acute response and when long-term solutions such as a vaccine become widely available. We don't know how long this period will last, but we can expect continued turbulence and malicious cyber activity throughout. In such an environment, CTA's threat intelligence sharing mission becomes even more important.

Despite the shift to entirely virtual interactions, CTA stayed busy during Q2 2020. We have formed contributing ally partnerships with the Information Technology ISAC and others to be announced soon, and participated in several ongoing virtual working groups sponsored by the Aspen Institute, the Carnegie Endowment for International Peace, the New York Cyber Task Force, and the World Economic Forum. CTA staff participated in the informal sharing groups that sprang up to fight malicious cyber activity associated with COVID-19. We held CTA's first webinar on how threat sharing improves a company's competitive edge. In the automated intelligence sharing area, our updated platform is working well, and we are diving into the shared data to understand it better. Our early sharing program has maintained a steady cadence of three to four releases per week. CTA's election security working group is looking at how the cybersecurity industry can best support the state and local governments that manage US electoral infrastructure in the run-up to the November election.

During the second half of 2020, our three strategic goals will continue to guide our activities: enabling members to better protect their customers, disrupting malicious cyber activity more systemically, and raising the level of cybersecurity across the digital ecosystem. We will work hard to bring new members into the Alliance, despite the current economic uncertainty related to the pandemic. We will steadily add functionality to the new sharing platform and expand our shared data's depth, breadth, and diversity. Although 2020 conferences will be different than in previous years, we will still sponsor the Threat Intelligence Practitioners' Summit at the annual Virus Bulletin conference as well as the Association of Anti-Virus Asia Researchers' Conference in Vietnam. We will also continue to publish guest blogs from our members and output from our working groups.

Companies need good cybersecurity providers now more than ever. In turn, those providers need access to the best threat intelligence available. CTA members are well-positioned to draw on expertise from across the cybersecurity community to make their products and services even more effective. Thanks to all our current members for the strong support you provide. To the potential members out there, come check out the early sharing content on our website and sign up for a demonstration of our platform. I'm certain you'll find something you can use.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

QUARTERLY SHARING STATISTICS

March - May 2020

TOTAL OBSERVABLES SUBMITTED

12 MILLION

INDICATOR DIVERSITY

FILES **54%**

NETWORK OBSERVABLES **46%**

"EARLY SHARES" THROUGH CTA

50

WEEKLY AVG: 3-4

Our early sharing initiative allows CTA members to share defensive information, such as blog posts, research findings, and data samples, with one another through CTA in advance of public release. We have had over 230 early shares from CTA members since we began this program in 2018. This rate of sharing and the corresponding growth in its depth and scope are a reflection of the growing mutual trust among our members that we have worked hard to cultivate and maintain. You can read more about the program here.

GUEST BLOGS SHOWCASE THE VALUE OF CTA

Many thanks to our members that have contributed to our series of guest blogs on their experiences with CTA. Here are some of the things that these members have been saying:

"The cybersecurity industry is built on trust, collaboration, and sharing. We see CTA as providing a unique platform to nurture those symbiotic relationships." – **Samir Mody, VP Threat Research, K7 Computing**

"Data organization is the foundation upon which any threat intelligence program is built, and CTA gave us the roadmap to get there." – **Wade Woolwine, Principal Security Researcher, Rapid7**

"When someone shares with CTA, the understanding is that everyone can and will use it to make their products better for their customers." – **Ryan Olson, VP Threat Intelligence (Unit 42), Palo Alto Networks**

CTA Member Spotlight

MCAFEE

WITH RAJ SAMANI, FELLOW & CHIEF SCIENTIST

WHY DID MCAFEE HELP TO FOUND CTA?

We know the collaborative nature of our adversary! Indeed, this has been known for many years, and while there is general acceptance that those defenders need to adopt a similar approach, the emergence of the CTA allows this to be done in a structured and organized manner. Our belief remains that we are stronger together, and as we have seen already this approach is proving to be hugely successful in protecting society.

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

Any opportunity to identify new threat indicators or gain insight into a threat campaign can be incredibly powerful. Moreover, our ability to contribute toward protecting the customers of our industry partners means that we can be safe in the knowledge that we are maintaining a safer world for all of us.

HOW DOES BEING PART OF CTA HELP MCAFEE STRENGTHEN SECURITY FOR CUSTOMERS?

As mentioned above, a wider collections approach allows us to identify threat indicators that we may be unaware of. Equally, the early accessibility of threat research from industry partners gives us valuable context when determining the adversary and the campaigns they carry out.

WHAT VALUE DOES MCAFEE GAIN FROM PARTICIPATING IN CTA WORKING GROUPS?

The Working Groups give us a narrower focus on threat campaigns that go beyond indicator sharing. Working with industry partners means that we can collectively build a better intel picture of the adversary that is imperative in mapping our activities of more capable actors.

HOW DO YOU SEE CTA FITTING INTO THE FUTURE OF THE CYBERSECURITY LANDSCAPE?

Cybercriminals do not respect international borders. Their ability to traverse through multiple jurisdictions dramatically increases their ability to obfuscate activities. The role of cybersecurity and indeed the CTA is to ensure a collective voice is heard to provide the defenders of our society every tool within their arsenal to protect and work the necessary public bodies to send the message that cybercrime is *not* a risk-free activity.

WHAT MOST EXCITES YOU ABOUT THE WORK YOU HAVE BEEN ABLE TO DO THROUGH CTA?

This may sound somewhat simplistic, but every month the report we receive detailing the sharing statistic is imperative. In amongst the tens of thousands of new threats we are able to identify thanks to industry partners is another parent no longer being scammed by going to a malicious site, or another company no longer getting breached because the malware is now correctively identified. We have to remember the lack of cybersecurity has a human cost.

CTA & Our Partners Respond to the Ongoing Crisis

CYBERSECURITY & COVID-19

With work-from-home and learn-from-home becoming the norm for most, at least temporarily, the importance of collaboration in defending our digital ecosystem has never been greater. CTA has worked hard to support our partners and members in their efforts to protect their customers. Of course, our automated threat intelligence sharing and human-speed sharing through our Committees and Working Groups continues, with an increased focus on the cybersecurity risks associated with the ongoing pandemic. This includes 13 instances of COVID-19-specific early sharing among our membership as well as automated sharing of pandemic-related IoCs (files and domains). However, CTA and our staff have also taken a number of steps supplemental to our usual operations in order to support the efforts of the wider cybersecurity community during this challenging time.

On March 31, 2020, CTA announced that we would be joining 12 other non-profit organizations to support the Global Cyber Alliance "Work From Home. Secure Your Business." campaign. The very next day, CTA published a consolidated list of COVID-19 resources and blog posts from our members and partners offering a wide variety of cybersecurity advice for businesses and individuals on how to protect themselves during the ongoing disruption arising from the COVID-19 pandemic. This list is updated on an ongoing basis as CTA members and partners publish new resources.

The CTA team has also been enthusiastic in its support of the COVID-19 Cyber Threat Coalition (CTC), a global volunteer community focused on preventing cyber criminals from taking advantage of the widespread disruption and anxiety to advance their malicious goals. CTA's Neil Jenkins was invited to join the CTC Steering Committee and also participated in the CTC's May 7 virtual town hall (right- bottom). During this event Neil outlined the unique value that CTA can contribute in tackling cyber threats in the current context.

During a May 15 interview with the CTC (right- top), Michael Daniel, our President & CEO, offered his insights on the cyber-security risks arising as a result of the pandemic. In particular, he affirmed that while CTA is "not seeing an increase in the overall volume of malicious activity than we were, say, six months ago, what we are seeing is a dramatic shift in the themes of these attacks. The bad guys are really trying to take advantage of people's fears about COVID-19; including a veritable tsunami of phishing emails with COVID-19 as the lure." Michael also contributed to a virtual panel discussion on tackling cyber threats in this era, which was organized by Open Austria, the country's official presence in Silicon Valley.

CTA will continue to work closely with our members and partners to ensure the strongest possible cybersecurity protection for their customers during this ongoing crisis. While much remains uncertain, we hope that the values of community and collaboration that CTA embodies can help the industry keep on track and build back even stronger when that time comes.

In the meanwhile, CTA wishes you and yours the very best of health.

CTA Webinars & Fireside Chats Get Off The Ground

CTA OUTREACH GOES DIGITAL

With in-person events seemingly off the table for the foreseeable future, CTA has begun offering webinars and fireside chats accessible to anyone interested in learning more about our mission. To date, we have offered one of each, addressing different aspects of how CTA's model of sharing and collaboration helps move us towards a more secure cyberspace.

Another key route to building greater awareness of CTA and our mission is through the press. From January through May, CTA had 70 media engagements, including a recent op-ed from Neil Jenkins on the importance of information sharing that was picked up by CyberScoop.

Check out the Events page of our website for details on our webinars and fireside chats, as well as other events (including a virtual edition of the VirusBulletin conference) that CTA will be attending or sponsoring over the coming months.

Leveraging CTA's Ecosystem of Trust to Secure Events & Counter Threats

CTA WORKING GROUPS, EXPLAINED

FROM NEIL JENKINS, CHIEF ANALYTIC OFFICER

As CTA continues to grow and mature, we want to leverage the trust we're fostering between members to better protect customers, disrupt adversaries, and elevate the digital ecosystem. CTA led the way in establishing automated information sharing between cybersecurity providers. That foundation provides us with an opportunity to do more.

BUILDING FROM A STRONG FOUNDATION

Since 2017, our members have shown that it is possible to share indicators of compromise and the context necessary to understand them and action them through automation, all while remaining competitive in how they use that information to protect their customers. With that foundation, we sought to bring our members together to share additional information, analysis, and context at human speed.

Our Algorithm & Intelligence Committee provides an opportunity for threat intelligence researchers to meet and talk on a regular basis. We began small, asking members to discuss recently published research on new threats or talk about trends they see from their unique perspectives. Naturally, researchers did what researchers do: they asked questions of each other, challenging some assumptions and providing their various views of the problems. We also began to share information on new and emergent threats, often sharing details in real-time via collaboration channels.

These briefings provided an opportunity for them to grow more comfortable with one another and fostered trust. The VPNFilter incident in May 2018 was the first sign of this trust in action. Cisco's Talos group chose to provide their research to members early to enable the broadest possible protections and holistically disrupt the actor's infrastructure. Members saw the utility of this approach and began sharing more research. Since VPNFilter, CTA members have now shared over 230 reports with each other early.

Growing trust within CTA has nurtured greater collaboration.

MORE COLLABORATION, STRONGER DEFENSE

What if we could leverage this trust to plan for cybersecurity incidents that are likely to affect important events? What if we could come together to actively share information targeting specific threats with the goal of increasing protections across CTA and ultimately disrupting the actors? These are the goals of our new Working Groups. CTA has established three Working Groups and invited our members to participate and work together for the greater good.

So far, we have established Working Groups that focus on the cybersecurity of the 2020 U.S. Elections and democratic elections around the globe and the (now) 2021 Tokyo Summer Olympics. These two event-focused Working Groups provide a forum for members to share information directly related to these events and to provide a core group of people to collaborate in the event of a cyber incident affecting those events. We can also use these groups to reach out to other partners in the ecosystem to share information around these events and prime the pumps for collaboration in an incident. As an example of the work we can do together, we published CTA's first Threat Assessment for the Olympics in February of this year.

We also establish Working Groups around specific malware that poses a unique or novel threat to the security of our members' customers. Our goal is to focus information sharing on these threats so that our members can more effectively disrupt critical nodes in the malware killchain. These Working Groups may also leverage our shared information to work with others in the ecosystem, including governments, to have a more lasting disruptive effect.

IT ALL COMES DOWN TO TRUST

All of CTA's activities are rooted in our shared mission and our trust in one another to share quality information and improve protections across the global digital ecosystem. CTA's Working Groups provide an opportunity for us to plan, prepare, and act together. If you are interested in our working groups and are not yet a CTA member, we hope you'll consider joining us.

WANT TO LEARN MORE ABOUT OUR WORKING GROUPS?

CONTACT CTA TODAY