JUNE 2021

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

Collaboration. Cooperation. Connections. Partnership. Sharing.

These concepts pervade any discussion about cybersecurity and for good reason. The Internet was born out of a desire to collaborate more easily, and the benefits of connecting across distances have driven its growth. Sharing fuels social media platforms, and partnerships of all kinds have created enormous economic benefits in the digital ecosystem. These ideas are literally built into the structure of cyberspace.

Unfortunately, these characteristics also enable criminals, nation-states, hacktivists, and others to undertake malicious activities at an impressive scope, scale, pace, and distance. Malicious actors use the nature of cyberspace to their advantage, holding at risk the benefits societies have derived from the digital ecosystem. The digital world, while enormously beneficial, has also become quite dangerous.

Despite being inherent to cyberspace, putting these concepts into practice has proved challenging for network defenders. CTA was created to overcome some of the barriers and put these ideas to work in a concrete fashion. We provide a collaboration hub, the infrastructure for sharing, a means to connect, and an ethos of cooperation. Weaving these abilities together enables CTA to speak with a stronger, collective voice in the cybersecurity industry.

In this issue, we explore some of the different ways CTA provides such a collective voice. One article looks at how CTA works with the World Economic Forum's Partnership Against Cybercrime to develop concrete actions businesses can take to reduce their cyber risk. Another discusses our work with the Ransomware Task Force, a volunteer group of more that 50 cyber experts that came together in early 2021 to recommend actions to counter the threat of ransomware. We also examine CTA's Olympics Cybersecurity Working Group and the Elections Cybersecurity Working Group; these two initiatives focus on sharing information about the threats to specific events, thereby improving the industry's collective understanding of those threats and our ability to support those charged with defending the events.

As we head into the second half of 2021, CTA will continue to find opportunities to use its collective voice to improve the cybersecurity of the digital ecosystem. Collaboration, cooperation, connections, partnerships, and sharing are built into CTA's structure, just as they are into the broader Internet. I look forward to seeing where employing these concepts takes us next.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CTA COLLABORATING ON THOUGHT LEADERSHIP

In 2021, CTA has been on the forefront of thought leadership, using our collective voice to address critical topics and global efforts in collaboration with our partners and members. This issue of *CTA in Focus* will address several different ways in which CTA has helped provide a collective voice. See below links to several different papers CTA has helped sponsor in support of our mission to improve the overall cybersecurity of the digital ecosystem.

Ransomware Task Force Framework Report

Guidelines For Establishing & Strengthening Government Vulnerability Disclosure Policies

Cyber Security After the Pandemic

The State of Cyber-Risk Disclosures of Public Companies

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>4 MILLION
MONTHLY AVERAGE

KILL CHAIN DIVERSITY
(2021 AVERAGE)

RECONAISSANCE	1%
WEAPONIZATION	>0%
DELIVERY	17%
EXPLOITATION	14%
INSTALLATION	43%
COMMAND + CONTROL	19%
ACTIONS ON OBJECTIVES	6%

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

TOTAL EARLY SHARES

3-5
PER WEEK

430+
IN THREE YEARS

CTA: A COLLECTIVE VOICE DRIVING CRITICAL INDUSTRY CHANGE

CTA's mission is to improve the overall cybersecurity of the digital ecosystem. With today's dynamic and complex threat landscape, that can only be done when the industry works together. Our strength comes when we collaborate. When we present a collective voice and concerted action, we are able to effect critical change that can have lasting impact across the industry. In this issue, we profile where CTA and our members are collectively making positive global impact in our fight against cybercrime.

CTA Front-and-Center in Cross-Industry Collaboration

REPORT ON THE WORLD ECONOMIC FORUM PARTNERSHIP AGAINST CYBERCRIME

For over four years, CTA has served as a trusted voice for the cybersecurity industry and delivered a cutting-edge threat intelligence sharing operation. Our team's experience in delivering on both of these elements of our mission, as well as our status as a vendor-neutral organization, allows CTA to effectively drive cross-industry initiatives in furtherance of stronger cybersecurity for all. One program in which we have been increasingly involved is the World Economic Forum's Partnership Against Cybercrime (PAC).

Taking a thoughtful approach to collaboration

Late last year, the PAC released a comprehensive roadmap for tackling the diverse global threats posed by cybercriminals. This report, to which CTA contributed extensively, articulated six principles that frame and motivate PAC's ongoing initiatives:

1. Embracing a shared responsibility for collective action against cybercrime
2. Cooperating on the basis of long-term strategic alignment
3. Undertaking trust-building behaviors
4. Systematizing and institutionalizing cooperation
5. Ensuring that cooperation generates value for participants
6. Respecting concerns and challenges

With these principles front-of-mind, the CTA team has helped to drive significant progress over recent months on separate PAC lines of effort focused on building community dialogue around ransomware, mapping the cybercrime ecosystem, and developing 'threat focus cells' composed of willing collaborators to take on specific cybercrime threats.

We have been fortunate in these efforts to be working alongside CTA members —Fortinet, Palo Alto Networks, Check Point, and Cisco —and our longstanding partner, the Cybercrime Support Network, as well as many other outstanding private sector, civil society, and governmental organizations.

Convening the community to tackle ransomware

In its efforts to build shared understanding and strengthen the community of organizations and practitioners under the PAC umbrella who are actively engaged in tackling cybercrime, CTA has played a substantive role in the ongoing dialogue with PAC participants around the issue of ransomware. Given CTA's contemporaneous participation in the IST Ransomware Task Force, CTA's leadership team has been uniquely well-positioned to take the temperature of a wide range of stakeholders and share our understanding of viable approaches to ransomware with the PAC community. (You can read more about how industry can take action based on the task force's recommendations in a recent CTA blog post, Implementing the Ransomware Task Force's Recommendations in the Cybersecurity Industry

Mapping the cybercrime ecosystem

This line of effort is focused on identifying the major elements and relationships in the cybercriminal ecosystem, initially using publicly available research and reporting, and subsequently through contributions from industry and government to a trusted group of stakeholders. The focus of this mapping effort is not on individual cybercriminals but rather on criminal groups and sub-groups, as well as the organizational, financial, and functional relationships between them.

Through this project, which we are leading jointly with Fortinet, we intend to enable senior decision makers to make more strategic resource and targeting decisions; support law enforcement and private sector disruption efforts against major criminal networks; increase the impact of cybercrime investigations; and enable public and private cybercrime investigators to identify common targets of concern and thereby accelerate collaborative efforts. This project is obviously of significant scope, and we have engaged extensively across industry and with leaders in government to ensure that it is viable based on voluntary contributions of resources from PAC participants.

> ***"Since cyber threats are global and have significant economic ramifications, the WEF is well-positioned to recommend changes that will increase the security of the digital ecosystem."***
>
> **Michael Daniel**
> **President & CEO, Cyber Threat Alliance**

Standing up threat focus cells

A related, although separate, line of effort from the cybercrime mapping project relates to the creation of 'threat focus cells.' These trusted groups of stakeholders should come together around common targets of interest and work collaboratively to understand and, ultimately, disrupt those threats. While the envisioned pilot that would have taken business email compromise as its specific focus has proven challenging to realize in practice, the PAC and CTA remain committed to the idea that threat-focused sharing and collaborative disruption efforts are the most viable means of coordinating across stakeholders to tackle cybercriminal threats.

Looking forward

The WEF provides a unique venue in which to engage beyond our membership, but also to bring the perspectives and ideas of our members to this wider audience. As CTA continues its engagement with the PAC, we invite our members to stay tuned for future updates and opportunities to contribute.

CTA Working Groups Making an Impact

CTA 2020 SUMMER OLYMPICS THREAT ASSESSMENT REPORT

CTA established the Olympics Cybersecurity Working Group to share focused information on cyber threats to the 2020 Summer Olympics in Tokyo, Japan and to work with partners to be ready to respond to cyber incidents affect the Games. The Working Group developed a Threat Assessment to provide an overview of prior threat activity targeting past Olympics and organizations related to the Olympics, the potential threat actors that may target the games, the organizations and stakeholders that may be targeted, the potential threat activity that may occur, an overview of Japan's security posture, and lessons learned and recommendations to address these issues. After the Olympics were delayed for a year due to the COVID-19 pandemic, we recently decided to update our assessment to better capture this new world.

This report showcases a core CTA strength — the ability to produce strong analytic outputs that incorporate a wide array of viewpoints from our members, forming a collective view and enabling improved protections and response to incidents. Some of the highlights from this updated report include:

- Given ransomware operators' highly opportunistic nature, they might see the Olympics and Olympics-related organizations as a high-value target with low downtime tolerance
- Nation state actors will conduct offensive campaigns targeting the Olympics and Olympic-related organizations. These actions could take the form of data theft and leaks, disinformation, or disruption of systems involved in the Games
- Malicious apps masquerading as COVID-19 contact tracing apps or apps that manage personal or healthcare information could be pre-positioned on app stores to trick athletes and spectators into downloading them to steal user information and complicate efforts to ensure public health
- Recent campaigns, such as the SolarWinds incident, has increased the chances of a supply chain attack targeting a vendor involved in the Games
- Threat actors could view Japan as having a weakened cybersecurity posture due to a variety of ongoing domestic issues and may view this as an opportunity to conduct offensive cyber offensive operations against a seemingly distracted Olympic host

For our part, CTA members will continue to closely monitor threats and risks to the Games, work as responsible partners with Olympic organizers, and be prepared to respond to any and all cybersecurity incidents that may occur.

CTA Working Groups Driving Collaboration

ELECTIONS CYBERSECURITY WORKING GROUP

In the lead up to the 2020 U.S. Elections, CTA members came together to form an Elections Cybersecurity Working Group to share information and prepare for malicious cyber actors targeting election infrastructure. Luckily, this working group did not need to spring into action in the face of a cyber incident targeting voter registration databases or election management systems, but our internal engagement and relationship building in advance put us in the best position possible to do so if needed.

The working group was established in March 2019, 20 months before Election Day. We met monthly and encouraged members to share information and provide briefings on their work with election officials and research on election threats. These briefings helped to provide a common baseline understanding of the U.S. election system amongst the working group members.

We also built relationships with organizations focused on elections and election security, such as DHS's Cybersecurity and Infrastructure Security Agency (CISA), the Election Infrastructure ISAC, the National Association of Secretaries of State, the National Association of State Election Directors, the Information Technology ISAC, and the Belfer Center's Defending Digital Democracy. If they needed to call on us to help during an incident, we would be ready to help as responsible partners.

We also developed an incident collaboration framework to help guide our responses in the event of an incident. The framework provided methods to identify incidents, how to bring CTA members together quickly, and a blueprint for what questions to ask during an incident and where to reach out for the answers. We even designed potential threat scenarios to guide our planning and preparation, based on potential incidents. Identifying these risks and scenarios helped improved our readiness and put us in a position to succeed.

Although the 2020 U.S. Presidential elections are over, threats to election infrastructure have not disappeared. Accordingly, we continue to maintain distribution lists and collaboration channels to share information as needed. We also continue to work with the election community to make them aware of the capabilities CTA members bring to become an integral part of their planning and preparations. By working together collectively, we hope to improve the overall defenses of our democracy.

Neil Jenkins, CTA's Chief Analytic Officer, oversees CTA's Working Groups through a function of CTA's Algorithm and Intelligence Committee, which is comprised of member representatives from across CTA.

CTA: A MISSION WORTH CHAMPIONING

CTA Champions are individuals who believe in the mission of the Cyber Threat Alliance and wish to lend their time and voice to help advocate for a collective approach to stronger cybersecurity. Champions leverage their industry influence to promote CTA, help expand our industry connections, provide leadership on behalf of CTA at industry events, and provide support and collaboration when appropriate.

CTA welcomes our newest champion, Chandra McMahon, CISO at CVS Health and former senior vice president and chief information security Officer for CTA-member Verizon.

Chandra McMahon
CISO
CVS Health

RAPID7

JEN ELLIS
VICE PRESIDENT OF COMMUNITY AND PUBLIC AFFAIRS

CTA Member Feature

A COLLABORATIVE EFFORT TO TACKLE RANSOMWARE

The Ransomware Task Force is a fantastic example of the security community - including many members of the CTA - coming together to provide a collective voice calling for critical change to tackle one of the most pernicious threats impacting our communities.

In the past month alone, we've seen ransomware attacks shutdown healthcare across Ireland and fuel delivery across parts of the US, and demands of payments in the tens of millions of dollars. In other words, ransomware attacks are not only increasing in frequency, but also in scale and impact.

Recognizing this, the Institute for Security and Technology partnered with the Cyber Threat Alliance and various others to create the Ransomware Task Force; a collaborative effort to drive meaningful change that will reduce opportunities for ransomware attackers and disrupt the ransomware market. Unlike many previous ransomware efforts, this effort focused on actions that would create impact at scale, addressing policymakers in the new U.S. administration and governments around the world, the Task Force specifically avoided rather technical, tactical approaches.

The Task Force aimed to provide a comprehensive set of recommendations that address the issue holistically and change in four key areas: deterring ransomware attacks; disrupting the ransomware business model; helping organizations prepare for attacks; and creating a more effective response to attacks. The final report offers 48 recommendations, which we believe work best in conjunction with each other.

It will take time to see the recommendations adopted, so the Task Force has identified key focus areas for immediate attention. This starts with recognizing that ransomware is not a niche technology problem, but rather a serious societal issue that deserves focus from senior political and community leaders. We are urging these leaders to make ransomware a national security priority and take a comprehensive whole-of-government approach, not only on a national level, but also in coordination and collaboration internationally.

As part of this international approach, eliminate safe harbors provided by governments that allow cyber criminals to thrive within their borders. There also needs to be greater scrutiny on cryptocurrencies to ensure that the same level of oversight that applies to other financial systems applies here too, and to make it harder for ransomware attackers to realize their profit.

On the matter of payments, the Task Force has not recommended prohibiting them, but we have looked for ways to give victim organizations an opportunity to consider alternatives. For example, we have recommended that further cost-benefit analysis of payment be required before a payment, and that governments set up contingency funds to support providers of essential services in responding to attacks.

We also recommended that these critical organizations and small-to medium businesses get more support in preparing for, and responding to, attacks, in the forms of consistent but tailored actionable guidance, technical support from MSPs and relevant ISACs, and more financial support so they are better able to invest in cybersecurity.

In closing, we would like to thank all the CTA members that participated in the Task Force and helped us understand the dynamics of the challenge we are addressing, and identify the correct recommendations to drive critical change.

CTA Webinar Series

STRIKING IT RICH: HOW TO EXTRACT VALUE FROM SHARED THREAT INTELLIGENCE

Featuring:

Check Point SOFTWARE TECHNOLOGIES LTD · cisco · Symantec. A Division of Broadcom

Everyone in the cybersecurity industry knows that intelligence sharing can be valuable. However, getting value out of sharing efforts often proves quite frustrating. Ad hoc efforts can provide key information on specific issues, but they do not scale and are hard to maintain. Automated sharing scales, but finding what you need in the flood of resulting data is difficult.

The Cyber Threat Alliance works hard to make intelligence sharing valuable to its members, whether at a human or an automated scale. Over the past four years, our members have learned some key lessons about how to extract value out of CTA's shared intelligence.

Recently, Michael Daniel, CTA's President and CEO, sat down with Broadcom Symantec's Joe Chen, Check Point's Dorit Dor, and Cisco Talos' Matt Watchinski, representing three of the founding member companies of CTA to discuss their perspectives on the value of cyber threat intelligence sharing.

SINCE THE REALITY OF SHARING HAS OFTEN DIFFERED FROM THE PROMISE OF SHARING, WHAT HAS MADE CTA EFFECTIVE AT OVERCOMING THOSE HURDLES?

Joe: I've had a pleasant sharing experience. The founding members at CTA put our money where our mouth is to make sure everything runs smoothly.

Dorit: It is important to have the same agreement and agenda regarding how much Information is shared.

Matt: When you have the will and capability to do something you can be way more successful at it.

IF YOU WERE ADVISING A COMPANY LOOKING TO GET INTO SHARING RELATIONSHIPS, WHAT ADVICE WOULD YOU GIVE THEM?

Dorit: I would advise them to have the same goals in mind. Sharing is valuable when all parties involved trust each other.

Joe: Something that's really wonderful that people aren't aware of is low volume high impact sharing. I would definitely recommend they look into it.

HOW DO YOU SEE GOVERNMENTS FITTING INTO THESE SHARING ARRANGEMENTS? WHAT IMPROVEMENTS WOULD YOU LIKE TO SEE?

Matt: If governments can't participate in the short term, the best thing they can do is amplify our voices.

Joe: I hope governments around the world see us as an extension of infrastructure. Government can use us to help them protect important infrastructure.

WHAT DO YOU HOPE ORGANIZATIONS WILL CONSIDER WHEN SHARING THREAT INTELLIGENCE WITH OTHERS?

Matt: They should follow the CTA model. The CTA bylaws helped set the standard and the groundwork for success. This is key for having a sustainable organization.

Dorit: Creating a common language and response to issues would be helpful as possible.

Joe: Join CTA! It's a no brainer. You will have access to so much information and people in the field.

IS THERE ANY POINT YOU'D LIKE TO END WITH?

Dorit: Share intelligence with organizations that can leverage it. Know what you are sharing and why.

Matt: I want more companies to join CTA. Help us keep the world safe!

For the full interview, please visit our website.

JOE CHEN
Vice President of Engineering, Broadcom Symantec

DORIT DOR
Vice President, Products, Check Point Software Technhologies

MATT WATCHINSKI
Vice President, Engineering, Cisco Talos