MARCH 2020

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

Friends of CTA,

Welcome to 2020. Even though we're only a quarter into the year, it has already been a rollercoaster that shows no sign of stopping. The need for good cybersecurity hasn't decreased—if anything, it's increased. The bad guys are capitalizing on the COVID-19 pandemic to conduct nefarious activities and the surge in remote work opens new attack surfaces. Working together and sharing threat intelligence only becomes more important in these kinds of situations.

To that end, CTA stayed busy during the first quarter of 2020. On the membership front, we welcomed SonicWall into the Alliance and announced a partnership with the Financial Services Information Sharing and Analysis Center to collaborate on threat intelligence. At the RSA 2020 conference, we sponsored the Non-Profits on the Loose event and a set of Lightning Talks; I participated in a panel on managing the US's relationship to the global internet and gave a talk on how threat sharing improves your competitive edge as a cybersecurity company. In the intelligence sharing area, most of our members have upgraded to our new automated sharing platform and we remain on target turn off the old platform on March 31st. We are already seeing the benefits of the new platform: observables, points, and data diversity are all steadily increasing as members take advantage of the new platform's features. Our early sharing program has maintained a steady cadence of three to five releases per week. CTA's working groups have started to bear fruit as well: the Olympic Security Working Group released a joint assessment of cyber threats to the 2020 Tokyo Olympics.

For the rest of 2020, we will continue to focus on our three strategic goals: enabling members to better protect their customers, systematically disrupting malicious cyber activity, and raising the level of cybersecurity across the digital ecosystem. To achieve these goals, we are always interested in new members and partners and look forward to bringing additional members into the Alliance. We plan to steadily add functionality to the new sharing platform and to expand our shared data's depth, breadth, and diversity. As in 2019, we will sponsor the Threat Intelligence Practitioners Summit at the annual Virus Bulletin conference as well as the Association of Anti-Virus Asian Researchers' Conference in Vietnam. We will also publish guest blogs from our members and output from our working groups.

Companies need good cybersecurity providers now more than ever. 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 new platform. We think you'll like what you see.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

QUARTERLY SHARING STATISTICS

TOTAL OBSERVABLES SUBMITTED

~7 MILLION

OBSERVABLES SUBMITTED WITH CONTEXT

~90%

The transition to our new platform is nearly complete. While the sharing requirements and concepts underlying our platform remain largely the same, the new platform leverages an updated scoring algorithm that enables members to share more varied observables and context:

- **Observables Diversity: ↑** (~60% files, ~40% network)
- **Context per Observable: ↑**
- **Diversity of Cyber Kill Chain Submissions: ↑** (including % of 'Command and Control' phase observables)

THANK YOU, HEATHER!

In January, CTA bid farewell to our Chief Operating Officer, Heather King, as she left to work on challenges facing the cybersecurity and technology communities from a new position. Heather was with CTA for over 2½ years and played a key role in transforming CTA from a newly formed startup into full-fledged non-profit with staying power. Heather oversaw a rapid expansion in CTA membership, got our website going, helped identify and hire most of CTA's staff, and served as the face of CTA to our members. She hammered our internal policies into shape, ensured our money was spent wisely, and served as a sounding board for ideas from across the organization. We want to publicly thank Heather for her work and sage counsel. She made a difference, not just for CTA, but for the entire cybersecurity community. We will miss her at CTA but wish her the best in her new role where we know she will continue to make a difference.

CTA Member Spotlight

SOPHOS
WITH JOE LEVY, CTO

Since joining the Cyber Threat Alliance (CTA) in 2017, Sophos has been an active participant, helping steer CTA's actions and support its philosophy that security vendors should share threat intelligence, and that by joining forces we can better protect everyone.

Cybercriminals might be concerned with evading the protections of particular cybersecurity products, but they ultimately don't care which company protects their targets. Similarly, those in the IT security trenches select cybersecurity vendors to protect their operations and users, and shouldn't care where the source of those protections come from, only that they are adequate and timely. While being the first to discover some new threat or provide some new protection is seen as a badge of honor in the industry, it is simply impossible for any single vendor to always be first.

By collaborating through CTA, security providers gain a bigger, broader platform to confront significant issues that impact everyone, such as large, well-financed cybercrime gangs, the security of major world events like the Olympics or national elections, and now, cyber scams leveraging the global concern over the spread of novel coronavirus disease (COVID-19). This collaboration can be viewed as the basis for technological herd-immunity.

"CTA continues to prove that alliances can work. It's been very encouraging to see a growing number of cybersecurity vendors and operators cooperate to share information in efficient ways to altruistic ends," said Joe Levy, Sophos CTO and CTA board member.

"In the coming year, I hope to see us continue to grow our ranks of contributing members, enhance the systems and platforms we use for intelligence sharing, and make practical security improvements to automated threat identification and elimination through the use of evolving workflows and analysis frameworks."

Sophos is a proud member of CTA and will continue to advance the sharing of ideas and threat intelligence, as well as cooperative collaboration. By bringing together the smartest, brightest minds in cybersecurity, we can make the digital world a whole lot safer for everyone.

RSA Conference 2020

CTA IN THE BAY

The RSA conference is an important event for CTA. With over 600 exhibitors and 36,000 attendees, it presented a wealth of opportunities to promote CTA and to introduce ourselves to potential members. We are already in fruitful conversations with new connections made this year, and took advantage of the opportunity to reengage with cybersecurity vendors and organizations that we don't often get to see face-to-face.

Once again we co-hosted a Non-Profits on the Loose soirée—this event's 10-year anniversary—where industry, policy, and government leaders in security and privacy could mingle. Our Lightning Talks event allowed us to showcase to interested companies the benefit of CTA-driven collaboration.

Many thanks to our member speakers—Matt Olney, Derek Manky, Vicky Ray, Joe Levy, and Vikram Thakur—and to Palo Alto Networks for donating the space for us to use at RSA.

Recommendations for Organizers, Athletes, and Attendees

SECURING THE 2020 OLYMPICS

Back in February, CTA released our first event-specific threat assessment report, focused on cyber risks to the upcoming Tokyo 2020 Olympic Games.

Foremost among the hazards identified in the report is the possibility of disruptive attacks or disinformation campaigns conducted by nation-state actors or their affiliates. It is also going to be important for athletes, residents, tourists, and spectators to be attentive to their cyber hygiene throughout the period of the Games to minimize personal exposure to a heightened level of general cybercrime risk. The report also assesses the preparedness of organizers, partners, and others to mitigate the identified risks; and provides recommendations for further improvements to the cybersecurity of the Games. You can read the report in full here.

SonicWall Joins CTA Bringing Total Members to 26

CTA MEMBERSHIP CONTINUES TO GROW

CTA is the cybersecurity industry's premier threat sharing organization. We are very excited to welcome SonicWall as our newest member, as they will bring another perspective to our shared intelligence and bolster our efforts to raise the level of cybersecurity across the digital ecosystem. Collectively, our members share actionable threat intelligence at speed and scale to collaboratively disrupt malicious cyber activity and improve our collective global defenses.

AlienVault (AT&T Cybersecurity) • Check Point • Cisco • Dragos • Fortinet • IntSights • Juniper Networks

K7 Computing • Lastline • McAfee • NEC Corporation • NETSCOUT Arbor • NTT • Palo Alto Networks

Panda Security • Radware • Rapid7 • ReversingLabs • Scitum • SecureBrain (A Hitachi Group Company)

SK Infosec • SonicWall • Sophos • Symantec (A Division of Broadcom) • Telefónica's ElevenPaths • Verizon