paloalto NETWORKS

Cyber Threat Alliance Cracks The Code On CryptoWall Crimeware Associated With $325 Million In Payments

October 29, 2015

First-of-its-kind Collaborative Effort Showcases the Power of Threat Information Sharing to Make the Internet Safer

SANTA CLARA, Calif., SUNNYVALE, Calif., and MOUNTAIN VIEW, Calif., Oct. 29, 2015 /PRNewswire/ -- Fortinet (NASDAQ: FTNT), Intel Security (NASDAQ: INTC), Palo Alto Networks (NYSE: PANW) and Symantec Corp. (NASDAQ: SYMC), co-founders of the Cyber Threat Alliance (CTA), today announced the publication of research examining the evolution and global impact of the aggressive CryptoWall ransomware.

CYA"Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat," is the first published report using combined threat research and intelligence from the founding and contributing members of the CTA. This whitepaper provides organizations worldwide valuable insight into the attack lifecycle of this lucrative ransomware family, which is associated with over US$325 million in revenue for the malicious actors behind it, as well as recommendations for prevention and mitigation. The CTA further discovered:

- The $325 million in revenue that went to the attackers included ransoms paid by victims to decrypt and access their files.
- 406,887 attempted CryptoWall infections.
- 4,046 malware samples.
- 839 command and control URLs for servers used by cybercriminals to send commands and receive data.
- The hundreds of millions in damages spans hundreds of thousands of victims across the globe. North America was a particular target for most campaigns.

All of the key findings and intelligence in the report are based on the collective visibility the members of the CTA have into the CryptoWall v3 threat; potential impact may extend beyond this view.

QUOTES

- "The explosion of connected devices and our reliance on digital platforms has created an environment that is both empowering and creating new ways for adversaries to penetrate networks. Managing this risk is a shared responsibility. We need to step forward, and not wait for the adversary to make the move first. This research demonstrates the power of the CTA partnership; when we grow our collective intelligence across all sectors, we can better combat advanced threats, deploy security controls to counteract the latest moves and deliver greater security for our customers and all organizations."

- Derek Manky, global security strategist, Fortinet

- "When we joined the Cyber Threat Alliance, we dedicated ourselves to working closely with our partners in industry and law enforcement to detect and disrupt cybercrime campaigns. This research demonstrates an ability to leverage our collective threat expertise and intelligence to provide enhanced protection for customers, and help us more effectively collaborate with law enforcement in order to disrupt criminal ecosystems and ultimately help bring more cybercriminals to justice."

- Vincent Weafer, vice president, McAfee Labs, Intel Security

- "This type of collaborative research by security vendors reflects the power of effective threat information sharing and the positive effect it can have on helping maintain trust in our digital world. As a founding CTA member, we are committed to the idea that this new way of working together - of combining intelligence on a common adversary and sharing cyberthreat information as a public good - is to the benefit of all organizations in the battle against cybercrime."

- Rick Howard, chief security officer, Palo Alto Networks

- "Our first major target is ransomware threats like CryptoWall, which are growing at an alarming rate and holding critical business and consumer data hostage. By harnessing the power of the industry and sharing data from our vast threat intelligence networks to fight campaigns of this scale, we can make a larger impact on the threat landscape than if we pursue them individually."

- Joe Chen, vice president of engineering, Symantec

RECOMMENDATIONS
The report also highlights key recommendations by the CTA to aid users and organizations in not falling victim to CryptoWall v3 and other forms of advanced malware:

- Ensure that your operating systems, applications and firmware are updated with the latest versions of the software.
- Understand typical phishing techniques and how to thwart them, such as by not opening email from unknown email addresses or attachments of certain file types.
- Keep web browsers updated, and turn on settings to disable browser plugins, such as Java, Flash and Silverlight, preventing them from running automatically.
- Review access and security policies within corporate networks to limit access to critical infrastructure from systems and users who don't need it.

To discuss this research and how threat information sharing can help in the battle against cyberattacks, the founding CTA member CEOs will participate in a Churchill Club panel tonight titled: "Hacks and Deja vu: As the 'Another Day, Another Hack' Mantra Becomes Reality, is an End to Cyber Threats in Sight?"

To learn more about the Churchill Club event, visit: http://bit.ly/1PPextY.

To download a copy of the report or learn more about the CTA, visit: http://cyberthreatalliance.org/.

To attend a webinar on December 1, 2015 discussing the findings of this report, led by members of the Cyber Threat Alliance, register here: https://www.brighttalk.com/webcast/13565/179291.

RANSOMWARE: A GLOBAL AND PERVASIVE THREAT
Ransomware is malware that encrypts a victims' data so that a cybercriminal can hold it for ransom. When the victims pay, usually through an electronic currency like bitcoin, they receive a key from the cybercriminal to unlock their data. If the victims don't pay and haven't backed up their data, it can be lost permanently.

About the Cyber Threat Alliance (CTA)
Co-founded by Fortinet (NASDAQ: FTNT), Intel Security (formerly McAfee), Palo Alto Networks (NYSE: PANW) and Symantec (NASDAQ: SYMC), the Cyber Threat Alliance (CTA) is the industry's first group of cybersecurity solution providers who have come together in the interest of their collective customers to share threat information. The end goal for the information sharing is to raise the situational awareness about advanced cyberthreats and enable members and organizations worldwide to use the latest threat intelligence information to improve defenses against advanced cyber adversaries. For more information about the CTA, please visit: http://cyberthreatalliance.org/.

Logo - http://photos.prnewswire.com/prnh/20151028/281703LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/cyber-threat-alliance-cracks-the-code-on-cryptowall-crimeware-associated-with-325-million-in-payments-300168593.html

SOURCE Palo Alto Networks

Sandra Wheatley, VP of Corporate Communications, Fortinet, 408-391-9408, swheatley@fortinet.com or Chris Palm, Director of Corporate Communications, Intel Security, 408-346-3089, chris_palm@mcafee.com or Jennifer Jasper-Smith, Head of Corporate Communications, Palo Alto Networks, 408-638-3280, jjsmith@paloaltonetworks.com or PaloAltoNetworksPR@vocecomm.com or Kristen Batch, VP of Corporate Communications, Symantec, 650-527-5152, Kristen_Batch@symantec.com