Weekly Intelligence Summary

Oct 16, 2020 (TLP: WHITE)

In the spotlight this week:

- Discovered by the Tripwire VERT security team, CVE-2020-5135 impacts SonicOS, the operating system running on SonicWall Network Security Appliance (NSA) devices. ***SonicWall NSA***s are used as firewalls and SSL VPN portals to filter, control, and allow employees to access internal and private networks.
- In June 2018, Kaspersky published the first report on a new cluster of activities that they named ***IAmTheKing***, based on malware strings discovered in a malware sample from an unknown family. Over time, they identified three different malware families used by this threat actor, one of which was ***SlothfulMedia***. They discovered rare incidents involving IAmTheKing in central Asian and Eastern European countries. The DHS CISA also reports activity in Ukraine and Malaysia.
- Microsoft announced a critical vulnerability in the ***Windows IPv6 stack***, which allows an attacker to send maliciously crafted packets to potentially execute arbitrary code on a remote system. The proof-of-concept shared with MAPP (Microsoft Active Protection Program) members is both extremely simple and perfectly reliable. It results in an immediate BSOD (Blue Screen of Death), but more so, indicates the likelihood of exploitation for those who can manage to bypass ***Windows 10 and Windows Server 2019*** mitigations. The effects of an exploit that would grant remote code execution would be widespread and highly impactful, as this type of bug could be made ***wormable***. For ease of reference, we nicknamed the vulnerability “***Bad Neighbor***” because it is located within an ICMPv6 Neighbor Discovery “Protocol”, using the Router Advertisement type.
- Mandaint blogged: In some ways, ***FIN11 is reminiscent of APT1***; they are notable not for their sophistication, but for their sheer volume of activity. There are significant gaps in FIN11’s phishing operations, but when active, the group conducts up to five high-volume campaigns a week. Since at least 2016. From 2017 through 2018, the threat group primarily targeted organizations in the financial, retail, and hospitality sectors. However, in 2019 FIN11’s ***targeting expanded*** to include a diverse set of sectors and geographic regions. At this point, it would be difficult to name a client that FIN11 hasn’t targeted.

(cisp-id:9369) Oct 16, 2020
800,000 SonicWall VPNs vulnerable to new remote code execution bug.
Discovered by the Tripwire VERT security team, CVE-2020-5135 impacts SonicOS, the operating system running on SonicWall Network Security Appliance (NSA) devices. SonicWall NSAs are used as firewalls and SSL VPN portals to filter, control, and allow employees to access internal and private networks. Tripwire researchers say SonicOS contains a bug in a component that handles custom protocols. "At this time, SonicWall is not aware of a vulnerability that has been exploited or that any customer has been impacted," a spokesperson told ZDNet in an email.
https://www.zdnet.com/article/800000-sonicwall-vpns-vulnerable-to-new-remote-code-execution-bug/#ftag=RSSbaffb68

(cisp-id:9350) Oct 15, 2020
IAmTheKing and the SlothfulMedia malware family.
In June 2018, Kaspersky published the first report on a new cluster of activities that they named IAmTheKing, based on malware strings discovered in a malware sample from an unknown family. Amusingly, other strings present inside of it invited “kapasiky antivirus” to “leave [them] alone”. Over time, we identified three different malware families used by this threat actor, one of which was SlothfulMedia. #KingOfHearts, #QueenOfHearts & JackOfHearts. The group is characterized by a

mastery of traditional pentesting methodologies and a solid command of Powershell. Data available to us indicates that it has achieved operational success on numerous occasions. In 2020, They discovered rare incidents involving IAmTheKing in central Asian and Eastern European countries. The DHS CISA also reports activity in Ukraine and Malaysia.
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/

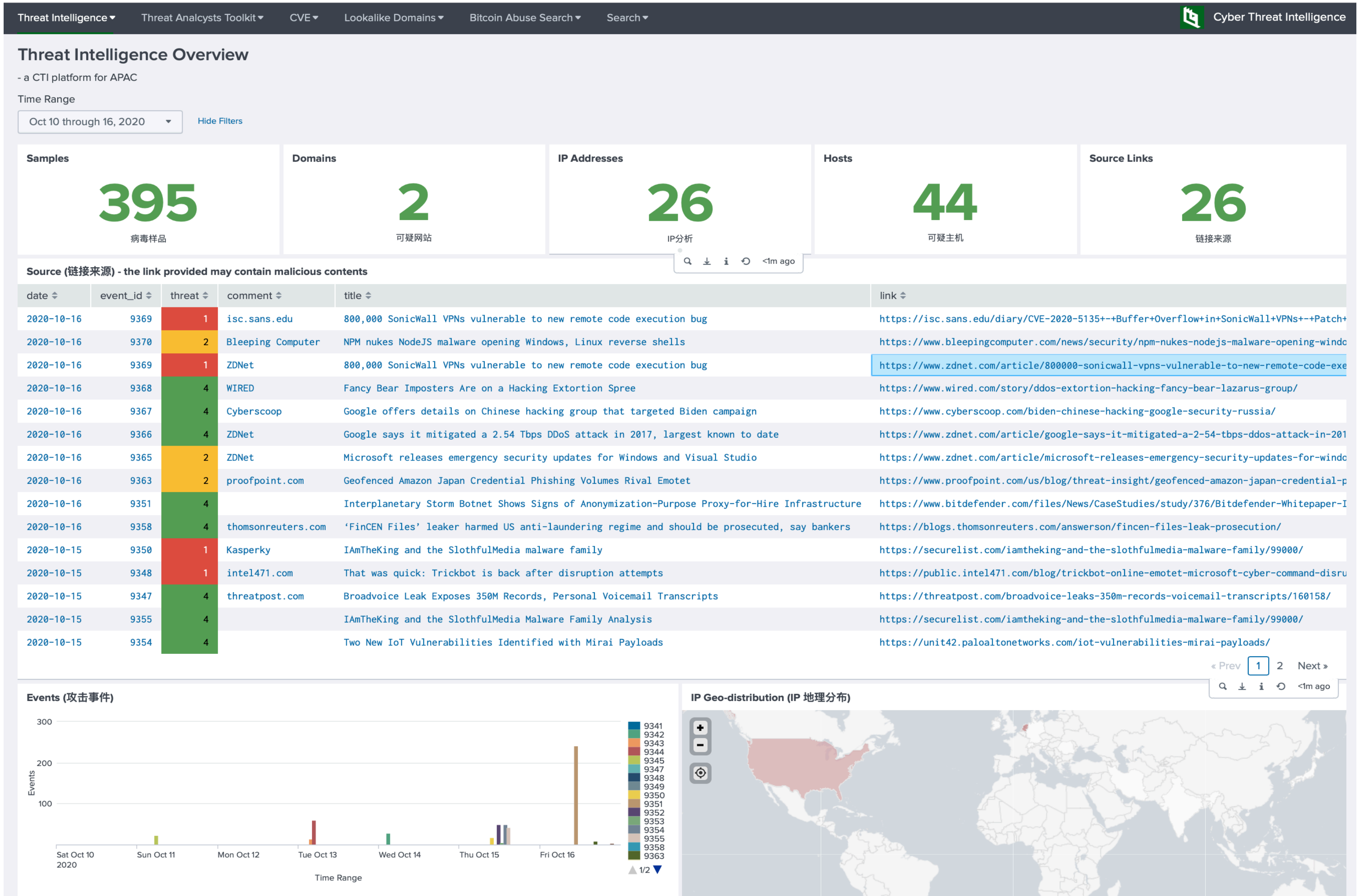
(cisp-id:9348) Oct 15, 2020
That was quick: Trickbot is back after disruption attempts.
On October 14, 2020, the Emotet spam botnet — which is often the precursor to TrickBot being loaded onto a system — began receiving spam templates intended for mass distribution. These spam templates contained a Microsoft Word document attachment with malicious macros that fetch and load a copy of Emotet onto the victim machine. The Emotet bots reached out to their controllers and received commands to download and execute Trickbot on victim machines.
https://public.intel471.com/blog/trickbot-online-emotet-microsoft-cyber-command-disruption-attempts/

(cisp-id:9349) Oct 14, 2020
Microsoft fixes Windows certificate spoofing bug abusing CAT files
Microsoft's October 2020 Patch Tuesday fixed 87 security bugs - Windows Spoofing Vulnerability that abuses CAT files. The vulnerability enables attackers to create "polyglot malware," which merges different file types, to spoof digital signatures. Signature spoofing flaws enable attackers to pass inauthentic, and possibly malicious, executables off as if these were signed by a legitimate corporation. An example would be CVE-2020-1464, a spoofing vulnerability that was actively exploited for two years before being patched by Microsoft during the August 2020 updates.
https://www.bleepingcomputer.com/news/security/microsoft-fixes-windows-certificate-spoofing-bug-abusing-cat-files/amp/

(cisp-id:9336) Oct 14, 2020
FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft.
n some ways, FIN11 is reminiscent of APT1; they are notable not for their sophistication, but for their sheer volume of activity. There are significant gaps in FIN11’s phishing operations, but when active, the group conducts up to five high-volume campaigns a week. While many financially motivated threat groups are short lived, FIN11 has been conducting these widespread phishing campaigns since at least 2016. From 2017 through 2018, the threat group primarily targeted organizations in the financial, retail, and hospitality sectors. However, in 2019 FIN11’s targeting expanded to include a diverse set of sectors and geographic regions.
https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html

(cisp-id:9341) Oct 13, 2020
CVE-2020-16898: “Bad Neighbor”
Microsoft announced a critical vulnerability in the Windows IPv6 stack, which allows an attacker to send maliciously crafted packets to potentially execute arbitrary code on a remote system. The proof-of-concept shared with MAPP (Microsoft Active Protection Program) members is both extremely simple and perfectly reliable. It results in an immediate BSOD (Blue Screen of Death), but more so, indicates the likelihood of exploitation for those who can manage to bypass Windows 10 and Windows Server 2019 mitigations. The effects of an exploit that would grant remote code execution would be widespread and highly impactful, as this type of bug could be made wormable. For ease of reference, we nicknamed the vulnerability “Bad Neighbor” because it is located within an ICMPv6 Neighbor Discovery “Protocol”, using the Router Advertisement type.
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-16898-bad-neighbor/

Our Threat Intelligence Platform (http://dashboard.cisp.org.hk/) is ready for public access.



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Oct 10 through 16, 2020

Samples	Domains	IP Addresses	Hosts	Source Links
395 病毒样品	2 可疑网站	26 IP分析	44 可疑主机	26 链接来源

Source (链接来源) - the link provided may contain malicious contents

date	event_id	threat	comment	title	link
2020-10-16	9369	1	isc.sans.edu	800,000 SonicWall VPNs vulnerable to new remote code execution bug	https://isc.sans.edu/diary/CVE-2020-5135+-+Buffer+Overflow+in+SonicWall+VPNs+-+Patch+
2020-10-16	9370	2	Bleeping Computer	NPM nukes NodeJS malware opening Windows, Linux reverse shells	https://www.bleepingcomputer.com/news/security/npm-nukes-nodejs-malware-opening-windo
2020-10-16	9369	1	ZDNet	800,000 SonicWall VPNs vulnerable to new remote code execution bug	https://www.zdnet.com/article/800000-sonicwall-vpns-vulnerable-to-new-remote-code-exe
2020-10-16	9368	4	WIRED	Fancy Bear Imposters Are on a Hacking Extortion Spree	https://www.wired.com/story/ddos-extortion-hacking-fancy-bear-lazarus-group/
2020-10-16	9367	4	Cyberscoop	Google offers details on Chinese hacking group that targeted Biden campaign	https://www.cyberscoop.com/biden-chinese-hacking-google-security-russia/
2020-10-16	9366	4	ZDNet	Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date	https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-201
2020-10-16	9365	2	ZDNet	Microsoft releases emergency security updates for Windows and Visual Studio	https://www.zdnet.com/article/microsoft-releases-emergency-security-updates-for-windo
2020-10-16	9363	2	proofpoint.com	Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet	https://www.proofpoint.com/us/blog/threat-insight/geofenced-amazon-japan-credential-p
2020-10-16	9351	4		Interplanetary Storm Botnet Shows Signs of Anonymization-Purpose Proxy-for-Hire Infrastructure	https://www.bitdefender.com/files/News/CaseStudies/study/376/Bitdefender-Whitepaper-I
2020-10-16	9358	4	thomsonreuters.com	'FinCEN Files' leaker harmed US anti-laundering regime and should be prosecuted, say bankers	https://blogs.thomsonreuters.com/answerson/fincen-files-leak-prosecution/
2020-10-15	9350	1	Kasperky	IAmTheKing and the SlothfulMedia malware family	https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/
2020-10-15	9348	1	intel471.com	That was quick: Trickbot is back after disruption attempts	https://public.intel471.com/blog/trickbot-online-emotet-microsoft-cyber-command-disru
2020-10-15	9347	4	threatpost.com	Broadvoice Leak Exposes 350M Records, Personal Voicemail Transcripts	https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/
2020-10-15	9355	4		IAmTheKing and the SlothfulMedia Malware Family Analysis	https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/
2020-10-15	9354	4		Two New IoT Vulnerabilities Identified with Mirai Payloads	https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

Get access? please send an email to: admin@dragonadvancetech.com