Weekly Intelligence Summary

Jun 26, 2020 (TLP: WHITE)

In the spotlight this week:

- VMware addressed 10 vulnerabilities affecting its ESXi, Workstation and Fusion products. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine.
- A series of zero-day vulnerabilities in a widely used low-level TCP/IP software library developed by Treck Inc., called Ripple20. At least 18 vendors are confirmed affected by Ripple20 vulnerabilities. The Treck networking stack was used by a wide range of industries, the impact will be significant as it ripples out across the ***#SupplyChains***.
- The latest variant of ***Lucifer v.2***, was discovered on May 29 while investigating the exploit of CVE-2019-9081, a deserialization bug in Laravel Framework that can be abused to conduct remote code execution (RCE) attacks. Patches are available for all the weaponized security flaws, but on hosts that have not been updated, attacks using these issues are often trivial to exploit and code execution for the purpose of cryptocurrency mining is one of the ultimate goals.
- Adobe Flash is about to reach its end-of-life date at the end of this year; However, the decline of exploit kits can be linked to the decline of Adobe Flash but exploit kits have not disappeared completely.

(cisp-id:8183) Jun 25, 2020

Lucifer: Devilish malware that abuses critical vulnerabilities on Windows machines.

On May 29, 2020, Unit 42 researchers discovered a new variant of a hybrid cryptojacking malware from numerous incidents of CVE-2019-9081 exploitation in the wild. A closer look revealed the malware, which we've dubbed ***"Lucifer"***, is capable of conducting DDoS attacks and well-equipped with all kinds of exploits against vulnerable Windows hosts. The first wave of the campaign stopped on June 10, 2020. The attacker then resumed their campaign on June 11, 2020, spreading an upgraded version of the malware and wreaking havoc. The sample was compiled on Thursday, June 11, 2020 10:39:47 PM UTC and caught by Palo Alto Networks Next-Generation Firewall. At the time of writing, the campaign's still ongoing. Lucifer is quite powerful in its capabilities. Not only is it capable of dropping XMRig for cryptojacking Monero, it's also capable of command and control (C2) operation and self-propagation through the exploitation of multiple vulnerabilities and credential brute-forcing. Additionally, it drops and runs ***#EternalBlue***, ***#EternalRomance***, and ***#DoublePulsar*** backdoor against vulnerable targets for intranet infections.

https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

(cisp-id:8177) Jun 24, 2020

Magnitude exploit kit – evolution: no Flash, no Exploit-Kits.

Exploit kits are not as widespread as they used to be. In the past, they relied on the use of already patched vulnerabilities. Newer and more secure web browsers with automatic updates simply do not allow known vulnerabilities to be exploited. It was very different back in the heyday of Adobe Flash because it's just a plugin for a web browser, meaning that even if the user has an up-to-date browser, there's a non-zero chance that Adobe Flash may still be vulnerable to 1-day exploits. Now that ***Adobe Flash is about to reach its end-of-life date*** at the end of this year, it is disabled by default in all web browser and has pretty much been replaced with open standards such as HTML5, WebGL, WebAssembly. The decline of exploit kits can be linked to the decline of Adobe Flash but exploit kits have not disappeared completely.

https://securelist.com/magnitude-exploit-kit-evolution/97436/

(cisp-id:8175) Jun 24, 2020

CryptoCore: A Threat Actor Targeting Cryptocurrency Exchanges.

In recent years, cryptocurrency exchanges have become targets for constant attacks, mainly from criminal groups and lone hackers. Threat actors of all kinds try to infiltrate corporate networks for reconnaissance, ransomware deployment, and plainly to steal money from those exchanges, specifically from their "hot" (i.e. active, connected) wallets. This kind of targets is somewhat unique, different from traditional financial institutions for two reasons: (a) Banks in general, and the SWIFT system in particular, are perceived as highly secured targets in comparison to cryptocurrency exchanges. The lower security of those exchanges' networks rises their potential as a lucrative target for cybercriminals. (b) While at first it seems easier to track the stolen money through blockchain, identifying and attributing wallets to entities and individuals is generally more difficult. From the top 3 attacks against Coinbase, Upbit, and Binance (which was hacked at least twice and had its KYC1 leaked), to smaller-scale but still sophisticated attacks, such as those carried out by the DPRK attributed group ***"Lazarus"*** (aka HIDDEN COBRA), or the exploitation of vulnerabilities in the Ethereum platform in the (ultimately unsuccessful) attack on Uniswap and Lenf.me2, attacks against crypto exchanges had had a discernible place in the 2019-early 2020 landscape.

https://www.clearskysec.com/wp-content/uploads/2020/06/CryptoCore_Group.pdf

(cisp-id:8191) Jun 26, 2020

VMware addressed 10 vulnerabilities affecting its ESXi, Workstation and Fusion products, including critical and high-severity code issues on the hypervisor.

VMware ESXi, Workstation and Fusion contain a Use-after-free vulnerability in the SVGA device. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3." reads the advisory published by the company. "A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine.

https://securityaffairs.co/wordpress/105183/security/vmware-flaws-workstation-fusion.html

(cisp-id:8147) Jun 19, 2020

Copy-Paste Compromises: TTP used to target multiple Australian networks.

The actor has been identified leveraging a number of initial access vectors, with the most prevalent being the exploitation of public facing infrastructure - primarily through the use of remote code execution vulnerability in unpatched versions of Telerik UI. Other vulnerabilities in public facing infrastructure leveraged by the actor include exploitation of a deserialization vulnerability in Microsoft Internet Information Services (IIS), a 2019 SharePoint vulnerability and the 2019 Citrix vulnerability. The actor has shown the capability to quickly leverage public exploit proof of concepts (POCs) to target networks of interest and regularly conducts reconnaissance of target networks looking for vulnerable services, potentially maintaining a list of public facing services to quickly target following future vulnerability releases.

https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf

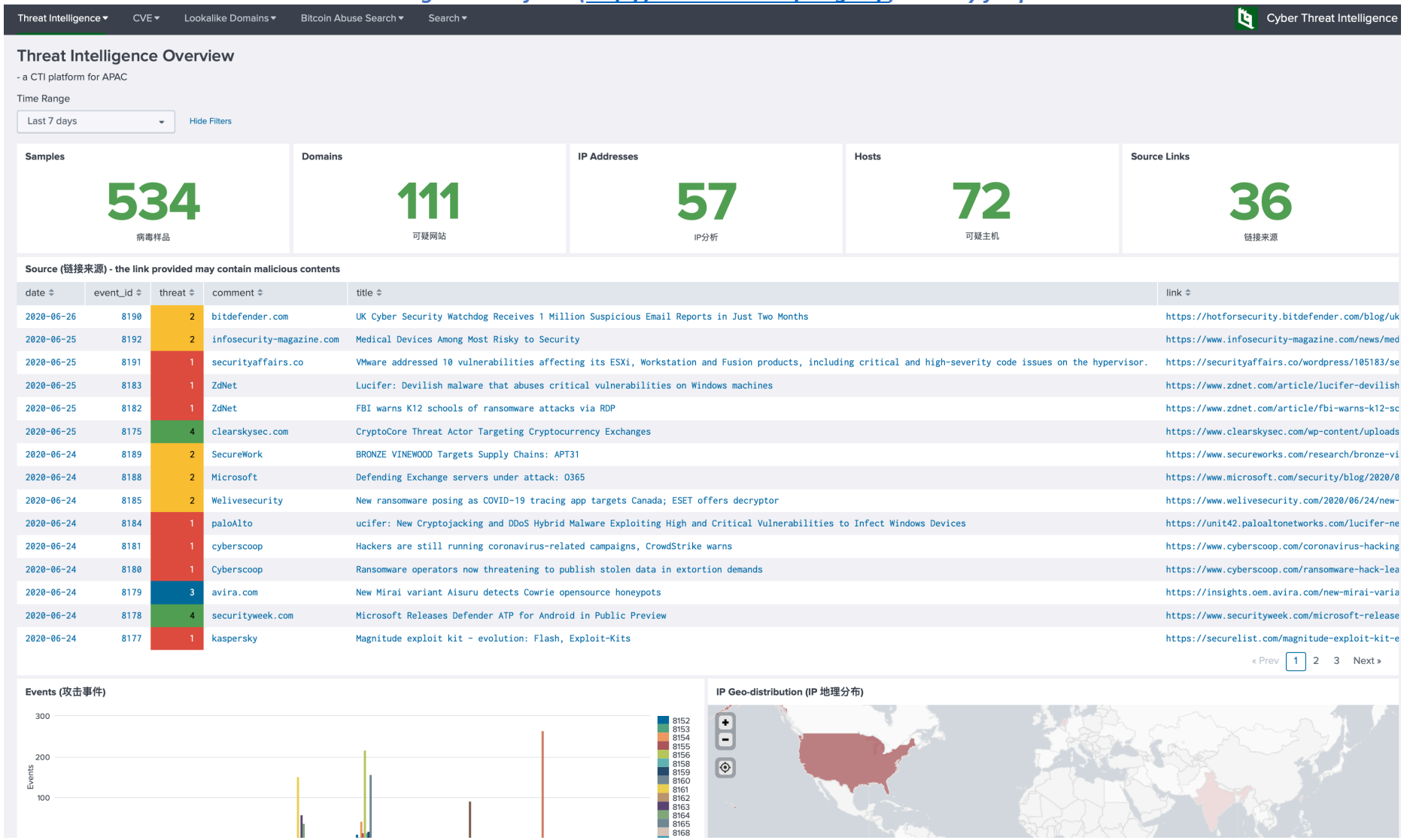
(cisp-id:8157) Jun 19, 2020

Ripple20: 19 Zero-Day Vulnerabilities Amplified by the Supply Chain

The JSOF research lab has discovered a series of zero-day vulnerabilities in a widely used low-level TCP/IP software library developed by Treck, Inc. The 19 vulnerabilities, given the name Ripple20, affect hundreds of millions of devices (or more) and include multiple remote code execution vulnerabilities. An attacker could hide malicious code within embedded devices for years. The interesting thing about Ripple20 is the incredible extent of its impact, magnified by the supply chain factor. The wide-spread dissemination of the software library (and its internal vulnerabilities) was a natural consequence of ***the supply chain "ripple-effect"***. A single vulnerable component, though it may be relatively small in and of itself, can ripple outward to impact a wide range of industries, applications, companies, and people.

https://www.jsof-tech.com/ripple20/

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



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