July 6 – 12, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has reported eleven malicious applications on Google Store, infected with the Joker infostealer and ad clicker. Joker, first detected in 2017, has used various obfuscation techniques and "in-between" versions to elude detection by Google, who removed the apps following the report.

  Check Point SandBlast Mobile protect against this threat

- Check Point Research reports of increased activity of the Phorpiex botnet, delivering the Avaddon ransomware, a new Ransomware-as-a-Service (RaaS) variant that emerged in early June, via malspam emails.

  Check Point Anti-Bot blade provides protection against this threat (Worm.Win32.Phorpiex)

- A campaign targeting Spanish users has distributed the Cerberus banking Trojan disguised as an Android currency converter on Google Store. The app avoided detection by Google and reached 10,000 downloads by operating in stages, waiting weeks before an update included a dropper module and still more time before downloading its final payload, Cerberus.

  Check Point SandBlast Mobile protect against this threat

- For a second time this year, affordable mobile phones sold under the US Federal Communications Commission's Lifeline program, have been found pre-installed with malware. The ANL UL40 devices come preinstalled with the Android Wotby downloader, later used to install variants of HiddenAds.

  Check Point SandBlast Mobile provides protection against this threat

- The North Korean affiliated APT group Lazarus has diversified its operations to include Magecart style credit card skimming. Researchers reported Lazarus infrastructure has been used since at least May 2019 to skim US and European online shoppers' paycard details on compromised sites, including international fashion chain Claire's, a modeling agency from Milan, a vintage music store from Tehran and more.

VULNERABILITIES AND PATCHES

- Palo Alto Networks has disclosed and patched a critical 10.0 CVSS vulnerability (CVE-2020-2021) in its firewall and enterprise VPN appliances which enables an unauthenticated network-based attacker to access protected resources. US Cyber Command urged all affected users to patch affected devices immediately.
- Citrix has issued security patches for eleven flaws in several of its products. Four of the vulnerabilities can be exploited by a remote unauthenticated user. Threat actors are actively scanning in search of exposed unpatched Citrix platforms.
- A zero-day vulnerability has been discovered in Zoom for windows, which could allow RCE on systems running Windows 7 and earlier. The vulnerability, which requires user interaction to be exploited, has been patched by Zoom.
- Adobe has ended support for the Magento 1 e-commerce platform. Over 100,000 online stores who still run outdated versions expose their clients to Magecart and other types of attacks and are out of compliance with the PCI DSS security standard for handling credit cards.

THREAT INTELLIGENCE REPORTS

- A Russian hacker, arrested in 2016 and extradited to the US, has now been found guilty of breaching LinkedIn, Dropbox and Formspring in 2012. Having stolen around 200 million user records in total and selling them in underground forums, the hacker financed several luxury cars and watches. His sentence will be given in September.
- Researchers have exposed a Russian group they named Cosmic Lynx, which they linked to more than 200 BEC operations since July 2019, targeting large international corporations. The group used bank accounts in Hong Kong and initiated fake acquisition processes posing as high ranking officials in target corporations.
- Researchers have published an analysis of the Evilnum financially motivated APT group, active and tracked since 2018. The group targets Fintech companies, mostly in Europe and the UK, seeking to steal valuable financial information. Evilnum's preliminary attack vector is spear phishing and it shares some of its MaaS tools with the FIN6 and Cobalt APT groups.
- Conti, a new ransomware targeting corporate networks, is thought to be related to Ryuk. First seen in the wild in December 2019, Conti shares code and uses an old version of Ryuk's ransom note and the same TrickBot infrastructure. Researchers believe Conti is a fork or rebranding of Ryuk and considering Ryuk's decrease in attacks, Confi might be its successor.

  Check Point SandBlast provides protection against this threat