Sept 6 - 12, 2021

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Mēris, a new distributed denial-of-service (DDos) botnet has broken a record with a 21.8 million requests-per-second attack on Russian internet company Yandex; 250,000 devices are assumed to be compromised.
- MyRepublic, a Singaporean communications services company, has disclosed a data breach exposing government ID cards and information of nearly 80,000 mobile users. The attack was aimed at a third party data storage platform used to store personal data of the company's customers.
- Members of the Groove ransomware gang have posted online 500,000 Fortinet VPN login names and passwords retrieved from exploitable devices. The VPN credentials could allow threat actors to access a network to exfiltrate data, install malware and perform ransomware attacks.

  Check Point IPS provides protection against this threat (Fortinet FortiOS SSL VPN Directory Traversal (CVE-2018-13379))
- United Nations' headquarters computers were hacked earlier this year after a Russian speaking cybercriminal bought user credentials on the dark web for $1000. The purpose of the breach is still unknown at this time.
- Ragnar Locker ransomware group is threatening to leak stolen data from individuals that would attempt to contact the FBI or other authorities. The Ragnar Locker gang had previously targeted large companies with ransomware attacks, demanding millions of dollars in ransom payments.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Ragnar)
- CISA is warning that hackers are exploiting a critical vulnerability tracked as CVE-2021-40539 in Zoho's ManageEngine ADSelfService Plus password management solution that allows them to take control of the system.
- A recently discovered malware called Sidewalk, used in attacks against organizations in Taiwan, Vietnam, the United States, and Mexico, is linked to the Chinese espionage group Grayfly.

VULNERABILITIES AND PATCHES

- A new zero-day vulnerability, tracked as CVE-2021-40444, is affects multiple versions of Windows. This vulnerability is currently distributed via malicious Office 365 documents and entails users to open the file to trigger it.

  Check Point IPS provides protection against this threat (Microsoft Internet Explorer MSHTML Remote Code Execution (CVE-2021-40444))

- Microsoft has patched multiple flaws that could allow an Azure user to infiltrate other customers' cloud instances within Microsoft's container-as-a-service offering. A threat actor could have exploited these issues to execute code on other users' containers, steal customer data, and for cryptomining.
- Netgear has made available firmware updates for more than a dozen of its smart switches used on corporate networks to patch vulnerabilities.
- GitHub has exposed seven severe vulnerabilities in npm packages, tar & @npmcli/arborist, used by npm CLI, which could eventually result in arbitrary code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research top 10 malware for August shows that Formbook infostealer is the most prevalent malware while Qbot banking Trojan has dropped from the list all together.

  Check Point Harmony Endpoint and Anti-Bot provide protection against these threats

- REvil ransomware gang, aka Sodinokibi, responsible for the Kaseya supply chain attack, is back on the scene after shutting down their infrastructure and disappearing for two months.

  Check Point Harmony Endpoint and Anti-Bot provide protection against this threat (Ransomware.Win32.Sodinokibi)

- A dual US - Canadian national has been sentenced to more than 11 years in federal prison for conspiring to launder tens of millions of dollars in wire and bank fraud schemes, including a massive online banking theft by North Korean Cybercriminals, according to the U.S. Department of Justice.
- Security researchers have revealed main criteria used to select ransomware victims. These include targets specifically in the USA, Canada, Australia & Great Britain with revenue of at least $100 million.
- South Korean law enforcement has apprehended a Russian member of the TrickBot gang after US authorities requested an extradition.

For comments, please contact: TI-bulletin@checkpoint.com