Sept 20 - 26, 2021

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Conti ransomware gang has hit Covisian's Spanish and Latin America subsidiary, Europe's major customer service and call center providers, affecting several of their internal systems. According to the company, there were no discussions or negotiations about any ransom.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Win32.Conti)*

- Threat actors are targeting Canadian voice-over-Internet provider VoIP.ms with a ransom DDoS attack. The company, which provides voice-over-IP services to businesses worldwide, is working to stabilize its website after their DNS and operations were severely disrupted.

- FamousSparrow cyberespionage APT group has been exploiting the ProxyLogon Microsoft Exchange flaw and SparrowDoor backdoor on hotels, governments, private businesses and various other sectors worldwide.

  Check Point IPS provides protection against this threat *(Microsoft Exchange Server Remote Code Execution (CVE-2021-26855))*

- Two US farmers' cooperatives have been attacked by ransomware groups: NEW Cooperative, a grain cooperative with sixty locations throughout Iowa was victim of BlackMatter ransomware demanding $5.9 million not to leak stolen data and provide a decryption key. Crystal Valley, a Minnesota farming supply cooperative, has suffered a ransomware attack affecting their computer systems and daily operations.

  Check Point Harmony Endpoint provides protection against this threat

- BlackMatter ransomware gang has launched a cyberattack against Marketron, business software solution provider for more than 6000 broadcast and media organizations.

  Check Point Harmony Endpoint provides protection against this threat

- United Health Centers, a Californian health care provider, has fell victim to a ransomware attack disrupting all of their branches, leading to patient data theft.

VULNERABILITIES AND PATCHES

- Chrome 94.0.4606.61 for Windows, Mac and Linux is being released by Google, in order to patch a critical zero-day vulnerability (CVE-2021-37973) exploited in the wild.
- Netgear has patched a severe remote code execution (RCE) vulnerability tracked as CVE-2021-40847 found in the Circle parental control service, which runs with root permissions on almost a dozen modern Small Offices/Home Offices (SOHO) Netgear routers.
- Experts have revealed a new vulnerability in Apple's macOS Finder, which allows threat actors to run commands on Macs using any available macOS version. The patch Apple issued is only partly addressing the flaw as it can still be exploited by changing the protocol used to execute the embedded commands from file:// to FiLe://.

  Check Point IPS provides protection against this threat (Apple MacOS Finder Remote Code Execution)
- Bugs in Microsoft Exchange's Autodiscover have enabled a leak of nearly 100,000 login names and passwords for Windows domains around the world: Expert revealed how the incorrect implementation of the Autodiscover protocol, rather than a bug in Microsoft Exchange, causes Windows credentials to be leaked to third-party untrusted websites.
- VMware urges to immediately patch severe CVE-2021-22005 vulnerability, as threat actors are targeting Internet-exposed VMware vcenter servers 6.7 and 7.0 deployments leading to remote code execution.

THREAT INTELLIGENCE REPORTS

- Raidforum a data breach marketplace and hacker forum, has mistakenly exposed internal pages from its website, meant for staff members only.
- The European Commission has officially linked Russia to Ghostwriter hacking operation which targets high-profile EU officials, politicians, journalists, and the general public by accessing computer systems and stealing data. The EU is accusing Russia of interference in the German parliamentary elections.
- Researchers have found that the large-scale phishing-as-a-service (PhaaS) BulletProofLink operation is the behind various phishing campaigns that targeted many corporate organizations lately.
- The NSA, FBI and CISA alert on an unusually high number of Conti ransomware attacks on US targets.

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