Check Point
SOFTWARE TECHNOLOGIES LTD.

April 26 - May 2, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Elekta, a Swedish provider of oncology and radiology systems, has suffered a ransomware attack that led to the takedown of its cloud storage systems. The attack caused disruptions and delays in the cancer treatments given at Yale New Haven Health, an Elekta client, among other US customers.

- Attacks targeting Israeli companies leveraging the Pay2Key ransomware, affiliated with Iranian actors, have been observed in the past few days. Among the victims is fashion firm H&M Israel. Attacks against Israeli targets are also expected to take place on May 7th, this week, on Jerusalem Day as set by the Islamic Republic of Iran. Hackers are expected to attempt website defacements, as well as minor hacking activities.

  Check Point SandBlast Agent provides protection against this threat (Ransomware.Win32.Pay2Key)

- Despite designated arrests by Spanish police, the FluBot Android botnet has resumed its activities, and has been spreading through Europe via an SMS package delivery scheme, in which tens of thousands of SMS messages are sent per hour with the FluBot download link.

- The Metropolitan Police Department of Washington DC has been hit by the Babuk ransomware and had their files leaked online. The ransomware gang claims to have stolen some 250 gigabytes of data including police reports, arrest records, internal memos and documents shared with the FBI.

  Check Point SandBlast Agent provides protection against this threat

- Hackers suspected to be linked to the Chinese government have deployed a new malware dubbed 'PortDoor' in the systems of the design division of Marine Engineering, the engineering company in charge of the design of the Russian Navy's submarines. The attack relied on spear-phishing.

- Experian, a top-three credit bureau, has left the credit card scores of almost all American citizens exposed to the public though an unprotected API tool, Experian Connect API. The company has since fixed the flaw.

- CISA has been investigating a possible incident in which five government agencies may have been breached via exploits to Pulse Connect Secure VPN vulnerabilities, exposed earlier this month.

VULNERABILITIES AND PATCHES

- Financially motivated threat group has been exploiting a SonicWall VPN zero-day vulnerability to deploy malware used to deliver the 'Fivehands' ransomware, most notably against European and North American targets. The flaw, assigned CVE-2021-20016, is a critical SQL injection vulnerability.
- A collection of memory allocation vulnerabilities dubbed 'BadAlloc' has been revealed, affecting a wide array of IoT and OT devices in industrial, medical, and enterprise networks. Exploitation of these flaws could enable actors to bypass security controls and execute arbitrary code.
- Apple has fixed a vulnerability in its macOS application notarization process, Gatekeeper. The flaw enables malicious applications to run without being blocked or flagged by MacOS security measures, simply by being double-clicked by the user.
- New remote unauthorized access vulnerability has been discovered in Aruba AirWave Management Platform, a designated platform for on-premises campus environments. The flaw, assigned CVE-2021-25151, has already been patched.

THREAT INTELLIGENCE REPORTS

- The FBI and CISA have issued a review of cyber-attack activities run by the Foreign Intelligence Service of Russia, known as SVR, against the US and allied countries. The SVR has been focusing on Cloud environment targets since 2018, and heavily relies on false identities and cryptocurrency transactions.
- Researchers have covered current activities carried out by Ghostwriter, an espionage group responsible for influence campaigns promoting narratives concerning NATO's presence in Eastern Europe. Recently, the group has expanded its activities, leveraging compromised social media accounts of right party Polish officials to distribute content designed to create domestic political disruption.
- New backdoor has been added to the tool arsenal of Naikon APT, a group linked to the Chinese government that targets government and military targets in Southeast Asia. The backdoor, dubbed 'Nebulae' by researchers, is used as part of the first stage of the attack.

  Check Point SandBlast Agent provides protection against this threat
- New cryptocurrency stealer tool dubbed 'WeSteal' has been offered for sale in dark-web forums. The python-based malware searches for strings related to wallet addresses found on victims' clipboards.

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