Check Point
SOFTWARE TECHNOLOGIES LTD.

Aug 2-8, 2021

YOUR CHECK POINT
# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Four critical infrastructures organizations in South East Asia have been the target the of a cyberespionage campaign by alleged Chinese threat actors for several months, aiming at exploiting information from the victims' SCADA systems. The targeted sectors included power, water, defense, and communications companies.

- The Australian Cyber Security Centre warns of a possible upsurge in LockBit 2.0 ransomware attacks against Australian targets after gang members expressed their intention to recruit corporate insiders to assist them in breaching and encrypting networks in exchange for multimillion dollar disbursement.

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

- Taiwanese computer company Gigabyte has been the target of the ransomware gang RansomExx, which threatened in a double extortion scheme to release 112 GB of data, including ultra-confidential communications with Intel, AMD and American Megatrends if the victim doesn't pay the ransom.

  *Check Point Harmony Endpoint provides protection against this threat*

- Active exploitation of the CVE-2021-20090 vulnerability has been discovered, targeting millions of home routers and other Internet-of-things (IOT) devices. Threat actors' IP address was located in Wuhan, China, and it appears they were trying to install a Mirai variant on the compromised devices.

  *Check Point IPS provides protection against this threat* *(Command Injection Over HTTP Payload)*

- Researchers have found several denial-of-service (DoS) vulnerabilities in the Cobalt Strike hacking tool that allow blockage of beacon command & control communication channels and prevent new installations.

  *Check Point Anti-Bot provides protection against this threat* *(Backdoor.Win32.CobaltStrike)*

- Researchers have analyzed the malware-as-a-service solution dubbed Prometheus, which distributes many well-known malware. The platform is sold on underground platforms for $250 a month, and was served to attack at least 3000 targets in the US, Germany and Belgium.

## VULNERABILITIES AND PATCHES

- Check Point Research has found vulnerabilities in Amazon Kindle, the world's most used e-reader device. By opening a malicious e-book, hackers would have been able to take full control of the victim's device and acquire sensitive information. Patches were subsequently installed on all Kindle devices by Amazon.
- Dynamic DNS data from millions of endpoints globally, including governments and Fortune 500 companies, could have been exposed through a newly found vulnerability.
- Researchers have exposed nine vulnerabilities, labeled PwnedPiper, in Swisslog's Translogic Pneumatic Tube System (PTS). PTS is used in thousands of hospitals globally, including 80% of the major hospitals in the US. The vulnerabilities have not yet been exploited, and 8 of them have been fixed.
- A new unofficial patch for PrintNightmare zero-day vulnerabilities has been issued, implementing a policy-based workaround.

  *Check Point IPS provides protection against this threat (Windows Print Spooler Remote Code Execution (CVE-2021-34527))*
- Fourteen high severity vulnerabilities dubbed INFRA:HALT have been found, affecting millions of NicheStack industrial control TCP/IP stacks and will be extremely difficult to patch. Among the bugs are remote code execution, denial of service (DoS), and information leak to TCP spoofing and DNS cache poisoning.
- Cisco has delivered patches for its Small Business VPN router to fix CVE-2021-1609 and CVE-2021-1610. These issues could have resulted in the execution of arbitrary code and denial-of-service (DoS) by an unauthenticated remote threat actor.
- A bug in Telegram for Mac could allow saving self-destructing messages and media, without the need for the recipient to open the message.
- An unofficial patch has been issued for Windows PetitPotam vulnerability.

  *Check Point IPS provide protection against this threat (Microsoft Active Directory Certificate Services NTLM Relay)*

## THREAT INTELLIGENCE REPORTS

- The recently emerged ransomware BlackMatter brings together some of the strengths of both REvil and DarkSide. The gang targets both Windows systems and VMware ESXi servers in large companies with annual revenues of over $100 million, but will spare critical industries like healthcare, defense, NGOs etc.

  *Check Point Harmony Endpoint provides protection against this threat*
- An individual associated with the AngryConti ransomware gang has leaked the group's sensitive information and data, including IP addresses for Cobalt Strike C2 servers, training materials, and more.