Check Point SOFTWARE TECHNOLOGIES LTD.

September 28 - October 4, 2020

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- French container shipping giant CMA CGM has suffered a ransomware attack by the Ragnar Locker gang. The company alerted its customers that its IT applications are currently unavailable, later confirming that it has been dealing with a cyber-attack.
- Emotet botnet has been leveraging the United States 2020 Presidential elections in a new spam campaign distributing letters allegedly from the Democratic National Convention's Team Blue initiative.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan.Win32.Emotet)*
- Universal Health Services (UHS), a healthcare provider with over 400 facilities in the US, UK and Puerto Rico, had been hit by the Ryuk ransomware. The attack crippled its entire IT infrastructure and phone system in the US, resulting in a transition to all-paper systems.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Ryuk)*
- University Hospital New Jersey has paid a $670,000 ransom to the SunCrypt ransomware operators to prevent a data leak of 240 gigabytes collected from the hospital network, including patient information.
- Facebook has shut down a Chinese campaign that hijacked account credentials and used the associated payment method to purchase ads promoting diet pills, sexual health products and more. Overall, some $4 million had been stolen from the victims.
- Organizations across Japan, Taiwan, China and the US have been targeted by a new espionage campaign carried out by the Palmerworm group, possibly linked to the Chinese government. The campaign leverages a new suite of custom malware.
- Swiss watchmaker Swatch Group, which owns watch brands such as Omega and Longines, has detected a cyber-attack and shut down some of its IT systems, affecting some of its operations.

VULNERABILITIES AND PATCHES

- Three critical and high severity vulnerabilities in the HP Device Manager have been disclosed in a security advisory released by the company. Researchers found that when these flaws are exploited together, attackers could gain system privileges and take over the machine remotely.
- Researchers have exposed a security flaw in Grindr, the popular LGBTQ social networking app with approximately 4.5 million daily users. The bug, that could allow an attacker to easily hijack any user account using only the user's email address, has already been patched.
- Microsoft has released a fix for a bug in the Windows 10 cumulative update, published as part of the September 2020 Patch Tuesday. The update disables the Windows Subsystem for Linux 2 (WSL 2), a tool designed to get a full UNIX system inside of Windows, generating new capabilities for developers.
- Researchers have uncovered that some 60% of the internet-facing email Exchange servers are still vulnerable to a critical remote code execution vulnerability assigned CVE-2020-0688, that had been exposed and patched eight months ago.

  Check Point IPS blade provides protection against this threat *(Microsoft Exchange Server Remote Code Execution (CVE-2020-0688))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has conducted an investigation into 'Volodya', one of the most active exploit developers for Windows. The investigation uncovered over 10 Windows Kernel Local Privilege Escalation vulnerabilities exploited by the actor, many of which were zero-day exploits at the time of development.
- The US Cyber command has issued a warning against a malware dropper called 'SlothfulMedia', which has been distributed by a sophisticated threat actor in attacks against targets in India, Kazakhstan, Kyrgyzstan, Malaysia, Russia and Ukraine.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(RAT.Win32.SlothfulMedia)*
- New ransomware family dubbed 'Egregor' has been revealed by researchers, after infecting approximately a dozen organizations over the past few months, among them the global logistics company GEFCO. The ransomware operates in a double-extortion attack model, collecting sensitive data prior to the encryption.
- Study focusing on the security of biometric security solutions has found several exploitable flaws in four models of facial recognition devices that could allow a threat actor to install an Android package (APK) on the device, obtain remote control to a mobile device and even gain access to its connected machines.
- Researchers demonstrated the dangers of old smart home devices by hacking a simple coffee maker and exploring the possibilities it opens. They were able to trigger the machine remotely, turn on the burner, spin the bean grinder and display a ransom note.