April 8 – 14, 2019

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Hackers have hijacked the website of the popular video editing software VSDC and replaced its download links to malware versions. Users from the UK, USA, Canada, and Australia were directed to copies infected with Bolik banking Trojan and KPOT info stealer.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Banker.Win32.Bolik2; Banker.Win32.kpot)

- Check Point researchers have detected a new campaign by the MuddyWater Iranian APT group, currently targeting Belarus, Turkey and Ukraine.

  Check Point SandBlast Anti-Virus and Anti-Bot blades provide protection against this threat

- An APT spyware framework that has been in operation for at least 5 years dubbed TajMahal, has been unveiled. Currently only one of the victims has been detected, a Central Asian diplomat. Some of its unique capabilities are to steal data from a CD burnt by the victim and the printer queue.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Spyware.Win32.TajMahal)

- Japanese optics manufacturer Hoya Corporation has been hit by a cyber-attack infecting its computers with credential stealers and cryptominers thus slowing systems in a manner that led to a partial shutdown of its production lines in Thailand for three days.

- Attackers have used credentials for one of Microsoft's customer support agents to access Microsoft email accounts. The company has sent incident notification emails to affected clients alerting them that their email address, folders, and communicated email addresses might have been breached.

- A new targeted attack against organizations in the satellite and communications industry echoes techniques seen in campaigns from the MuddyWater APT group. The campaign leverages vulnerabilities in WinRAR recently disclosed by Check Point researchers.

  Check Point SandBlast Agent and IPS blades provide protection against this threat (RARLAB WinRAR ACE Format Input Validation Remote Code Execution (CVE-2018-20250))

VULNERABILITIES AND PATCHES

- Multiple security vulnerabilities, which have been exposed in Verizon Fios Quantum Gateway Wi-Fi routers, could allow remote attackers to take complete control over the affected routers, exposing every other device connected to them.

  Check Point IPS blade will provide protection against this threat in its next online package

- Microsoft and Adobe have released their April 2019 software updates. Microsoft patched a total of 74 CVE-listed vulnerabilities, 13 of which are rated critical and two have been reported to be actively exploited in the wild. Adobe has addressed a total of 40 security vulnerabilities in its products, including Flash Player, Adobe Acrobat and Reader, and Shockwave Player.

  Check Point IPS blade provides protection against these threats

- Security researchers have discovered new vulnerabilities in the WPA3-Personal protocol, which allow potential attackers to crack Wi-Fi network passwords and get access to encrypted network traffic exchanged between the connected devices.

- Vulnerabilities in several plugins of WordPress, the open-source internet content management system (CMS), have been actively exploited in the wild. These flaws enable attackers to inject content into plugins which is eventually executed by web browsers of the users visiting hacked sites. More than 90,000 affected websites using these plugins are required to remove or update them immediately.

  Check Point IPS blade will provide protection against this threat in its next online package

THREAT INTELLIGENCE REPORTS

- The U.S. Department of Homeland Security (DHS) and the FBI have issued a joint malware analysis report on a new Trojan backdoor dubbed HOPLIGHT, used by the North-Korean APT group Lazarus.

  Check Point Anti-Virus blade provides protection against this threat *(Trojan.Win32.Hoplight)*

- Exodus spyware, recently found in Google Play Store directed at Android platforms, has been modified to target Apple iOS mobiles. Deployment of the iOS version was detected outside the App Store through Italian and Turkmenistani phishing sites by abusing Apple's Developer Enterprise program.

  Check Point SandBlast Mobile customers are protected from this threat

- Anubis, an Android banking Trojan, has evolved to contain encryption, RAT functionality and device locking capabilities that nearly qualify it as an Android ransomware. Countless Anubis versions have been identified in the official Android app store and this January it was used in a campaign targeting 377 bank applications from 93 countries all over the globe.

  Check Point SandBlast Mobile customers are protected from this threat