October 5-11, 2020

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Healthcare technology firm eResearchTechnology, providing software for hospitals and clinics, has been hit by the Ryuk ransomware, leading to delays in COVID-19 treatment development.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Ransomware.Win32.Ryuk)

- Check Point Research has reported that attackers are launching phishing campaigns targeting Amazon consumers in preparation for Amazon's annual Prime Day. Over a quarter of the domains containing the word Amazon and registered during the last month are malicious.
- Asian food delivery app Chowbus has been breached, leading to an extensive data theft. Over 400,000 customer records including names, email addresses, phone numbers and home addresses were stolen.
- The US Justice Department has revealed 92 domains used by Iran's Islamic Revolutionary Guard Corps (IRGC) to host fake news outlets in multiple languages as part of a global disinformation campaign.
- The virtual conference platform Playback Now has been leveraged for a credit card skim and financial data theft attack. Attackers impersonated the platform's official website and injected a reference to the rogue website into dozens of Magneto e-commerce websites.
- Docsketch electronic document-signing service has announced a data breach, as hackers gained access to its database containing contact information and form fields related to documents filed out by users.
- The FBI and CISA have released a warning against a campaign leveraging multiple vulnerabilities, old and new, to gain access to federal, state and local computer networks, carried out by foreign government-linked threat actors. Elections support systems were accessed, but elections data has not been compromised.
- Georgia Department of Human Services has been hit by a cyber-attack, exposing personal information of adults and children who have cases with child protection services.
- The Springfield Public School district in Massachusetts has been hit with ransomware, forcing a complete shut-down of its systems and of over 60 schools, accommodating 25,000 students and 4,500 employees.

VULNERABILITIES AND PATCHES

- Researchers have discovered 55 security flaws, 11 of them critical, in multiple Apple services. Among the flaws is a wormable cross-site scripting (XSS) vulnerability that could enable iCloud data theft.
- Cisco has addressed three high severity vulnerabilities in WebEx video conferencing system, Video Surveillance 8000 Series IP Cameras and Identity Services Engine. The IP Cameras flaw could allow an attacker to execute arbitrary code and cause the device to reload, resulting in a DDoS attack.
- Researchers have uncovered 'The Prisoner of Azure-Kaban' - six vulnerabilities, three of them critical, in Azure Sphere, a new IoT security solution for cloud connected devices.
- Comcast XR11 voice remote controller, used for over 18 million devices across the US, has been found to be vulnerable to a man-in-the-middle attack leveraging its RF communication, that could turn the device into an eavesdropping tool.
- QNAP has patched two critical vulnerabilities in Helpdesk, an app built-in to its Network Attached Storage (NAS) servers. The flaw might enable an attacker to take over the vulnerable device.

THREAT INTELLIGENCE REPORTS

- Check Point Research has warned against a surge in ransomware attacks, led by Maze and Ryuk. In Q3, there were 50% more ransomware attacks globally than in Q2, and the number of Ryuk attacks against healthcare organizations doubled.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Ransomware.Win32.Ryuk; Ransomware.Win32.Maze)*

- MosaicRegressor is a campaign relying on a modified Hacking Team tool to attack the machine's UEFI firmware, in charge of loading the operating system, and deliver a persistent malware. Diplomats worldwide are among its targets.

  Check Point SandBlast Agent provides protection against this threat

- Researchers have investigated BAHAMUT, a quality threat group that targets government and human rights entities across India, the Emirates, Saudi Arabia and the Middle East, and uses zero-day exploits and malicious apps available in Google Play Store and App Store for infection.
- The US Cyber Command has gained access to the Trickbot botnet management panel and acted to disconnect all infected machines from the C&C servers and deceive its operators by adding forged records to the botnet database.
- New IoT botnet dubbed HEH had been discovered by researchers. The botnet targets routers, servers and IoT devices and features a disk-wiping function, which allows it to wipe all data from the infected systems.