September 17 – September 24, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The United States State Department has fallen victim to a data breach. The breach was limited to an unclassified e-mail system, and has led to the exposure of personal data of employees.
- A yet unknown hacking group has compromised Click2Gov, a web-based bill-pay software solution developed by Superion, in a payment-data siphoning campaign that may have been going on since October 2017. It is still unknown how the attacker compromised the Click2Gov server, but researchers asses an Oracle Web Logic exploit may have been used.
- Security researchers have revealed that access to approximately 3,000 breached websites has been offered for sale on a Russian-speaking underground marketplace.
- The hacking group "Magecart" has compromised the services of sueno.co[.]uk, a UK based eCommerce retailer focused on Luxury beds and appliances. In another recent attack, the same group has compromised Newegg, an electronics retailer; the group created a fake Newegg website, and redirected the payment process from the original site to their fake site by injecting it with malicious code.
- The Port of Barcelona has suffered a cyberattack that affected some of its servers and systems, forcing the organization to launch the contingency plan designed specifically for these incidents. The incident did not seem to affect the port's operations in regard to sea traffic.
- Security researchers have warned that the Pegasus spyware, infecting both Android and iPhone mobile devices, is currently being used by 36 operators to conduct surveillance operations in 45 countries. The spyware, created and sold by the Israeli company NSO Group, has been used in the past by government and law enforcement agencies, and was also known to target human rights organizations.
- Japanese cryptocurrency exchange Zaif hs announced that it lost $60 million worth of company and user funds during a security incident that took place on September 14.

VULNERABILITIES AND PATCHES

- Adobe has released patches for the Windows and macOS versions of Acrobat and Reader, one of which fixes a critical flaw that can allow arbitrary code execution.
- Security researchers have exposed a critical vulnerability in software from NUUO, a global vendor of video surveillance equipment, which puts at risk the security of video feeds from over 100 camera brands and more than 2,500 camera models.
- Cisco has patched a vulnerability in its video surveillance manager software that could give an unauthenticated, remote attacker the ability to execute arbitrary commands on targeted systems.
- Security researchers have published a zero-day vulnerability affecting all versions of Windows, after the company had failed to patch it with the 120-days timeframe. The Vulnerability is in the Microsoft JET Database Engine, and could allow an attacker to execute code on the vulnerable system, but requires the victim to open a specially crafted file or visit a malicious web page.

  Check Point IPS blade provides protection against this threat (Microsoft Jet Database Engine Remote Code Execution)

- Security researchers have discovered a high severity privilege escalation vulnerability in some of Honeywell Android-based handheld computers that could be exploited by an attacker to gain elevated privileges. The models affected are CT60, CN80, CT40, CK75, CN75, CT50, D75e, CN51, and EDA series.

THREAT INTELLIGENCE REPORTS

- A new form of malware dubbed “Xbash” detects whether it has infected a Linux or Windows server and operates differently on each. On a Linux it would encrypt files in a mock ransomware attack - but without having a way to decrypt them even if the ransom is paid; on Windows it would run a crypto miner. The malware also operates as a worm, trying to move laterally in a network by scanning for vulnerable ports and using a brute force attack in an attempt to discover weak passwords.
- Europol has released its “Internet Organised Crime Threat Assessment 2018” report, where it stated that Cryptojacking attacks are on the rise, ransomware retains primacy, and "In addition to attacks by financially motivated criminals” there may be an increase in global cyber-attacks due to “the actions of nation states”. The report added that it became "increasingly difficult" to determine whether an attack was a "sophisticated" organized cybercrime group, a state sponsored attacker, or a cybercrime amateur.
- Security researchers have warned that cybercriminals had automated the process of credential stuffing attacks, now using botnets to conduct what consists of trying to log into multiple online services using username and password combination compiled from data breaches. The increase in these attacks, especially against the financial sector, could lead to an effect similar to that of a DDoS attack.