December 30, 2019 – January 5, 2020

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Dutch university of Maastricht has been hit by a ransomware attack and its systems are still unavailable, more than a week after the initial detection of the attack. Experts link Clop, the ransomware used in the event, to the Russian cyber threat group TA505.

  Check Point SandBlast provides protection against this threat *(Ransomware.Win32.Clop)*

- Special Olympics NY, a nonprofit organization, has been attacked and its email server exploited for a spear-phishing campaign directed at its pool of donors. Aiming to steal credit card details, the phishing email alerted recipients of a coming charge and redirected them to a malicious link for details update.

- Town of Erie, Colorado, has wired attackers over $1M in a recent BEC (Business Email Compromise) scam. An unverified online request to change bank details led to payment of a municipal contract of a new bridge made to a fraudulent account. According to the FBI, BEC losses in 2018 exceeded $1.2 Billion.

- Mariah Carey's Twitter account, with more than 21M followers, has been hacked and used to share racist and assaulting posts. The Chuckling Squad, responsible for the August hack of Twitter CEO Jack Dorsey's account, assumed responsibility. Adam Sandler's account was also hacked, probably by the same group.

- The US restaurant chain Landry's, which operates more than 600 venues across the country, has been hit by a PoS malware, active in its systems between March and October 2019. Having implemented an end-to-end payment encryption system back in 2016, Landry's announcement stated that, except for rare cases, it prevented the malware from accessing payment card data.

- A Magecart style web skimming attack has been directed at a school management software service platform called Blue Bear, provided by Active Networks. The attack has been reported to affect users paying school fees during October and November 2019.

VULNERABILITIES AND PATCHES

- Three remote code execution vulnerabilities have been exposed in a number of Ruckus wireless router models, which could be exploited to take full control of the devices over the internet. Ruckus routers do not include an automatic update option thus leaving thousands of units exposed, despite published patches.

- Recently published PoC demonstrates that D-Link routers are susceptible for exploitation using two vulnerabilities - CVE-2019-17621 and CVE-2019-20213. D-Link released firmware updates for some of the impacted models.

  Check Point IPS blade provides protection against this threat (Command Injection Over HTTP); dedicated protections for the CVEs will be released in the next online package

- Cisco has patched three critical bugs in its DCNM (Data Center Network Management) platform that could be used for remote attacks. No PoCs for these vulnerabilities have yet been published. Patches for 9 additional less severe bugs were also included.

THREAT INTELLIGENCE REPORTS

- Following the killing of Iranian Maj. Gen. Qasem Soleimani, US CISA (Cybersecurity and Infrastructure Agency) has issued an official warning regarding a rise in Iranian cyber-attacks directed at US industries and government agencies. In one such incident, hackers identified as "Iran Cyber Security Group Hackers" temporarily defaced the homepage of the U.S. Federal Depository Library Program.

- Clop ransomware, used by the Russian APT group TA505, has been continuously developed in recent months and now includes an integrated process killer used to disable Windows Defender and other security services prior to final file encryption, in order to prevent detection.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.Clop)

- Microsoft has filed legal action and taken down fifty domains relating to the North Korean APT37 group (aka Thallium). APT37 has used its infrastructure to target and spy on victims mostly from the US, Japan and South Korea.

- A new investigation into the 2018 Chinese cyberespionage dubbed Cloudhopper, operated by APT10, has found the operation more extensive than initially believed, affecting at least a dozen cloud service providers and granting attackers access to a large number of subsequent clients. Managed service providers formed a main target of the attackers and one hundred thousand US navy personnel records were exposed.