October 21 – October 27, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Procter & Gamble's site, 'First Aid Beauty' has been infected by a Magecart credit card skimmer for the past five months. The heavily obfuscated and encrypted skimmer specifically targeted US victims using Windows systems. Earlier this week the FBI has issued a warning advising SMSB to beware of E-skimming attacks.
  The Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Magecart)
- A DDoS attack has hit AWS DNS web service. The attack lasted for eight hours and affected access to many AWS S3 services which rely on external DNS queries including Amazon's Relational Database Service (RDS) and Elastic Load Balancing (ELB). US East Coast was particularly severely hit.
- Johannesburg, South Africa, has experienced a ransomware attack that compromised its municipal services. The hacking group, Shadow Kill, asked for a ransom of $33,000.
- An ongoing spear-phishing campaign aimed at NGOs, including the Red Cross, UNICEF and various other UN organizations has been exposed. The campaign was active since March 2019 and used legitimate SSL certificates to appear as genuine MS Office 365 login pages. The identity of the attackers is yet unknown.
- Elasticsearch database hosted by AWS, belonging to Autoclerk, a contractor who manages travel arrangements for US government and military personnel, has leaked sensitive PII (Personally Identifiable Information) including hotel reservations, check-in times and room numbers.
- Unsecured Elasticsearch database belonging to Adobe Creative Cloud subscription service has exposed data of 7.5 million users. Adobe shut off public access to the database but the exposed information could lead to targeted phishing attacks on its users.
- Pilz, a German global manufacturer of automation tools, has suffered a ransom attack and a week later is still disconnected from its customers and branches in 76 countries. The ransomware used, BitPaymer, known since 2017, has been tied to several high profile incidents; most recently French TV station M6.

  Check Point SandBlast Agent provides protection against this threat

VULNERABILITIES AND PATCHES

- Check Point Research has discovered a vulnerability (CVE-2019-11478) in the Selective ACKnowledgment (SACK) mechanism of the OpenBSD operating system, allowing an attacker to manipulate the communication and cause a DoS (Denial of Service) on the sender's side.

  The Check Point Firewall protects against this threat (sk156192)

- Researchers have discovered a vulnerability (CVE-2019-0941) that could lead to a new type of cache poisoning attack on sites using a Content Distribution Network (CDN). An error page returned to a malformed HTTP request sent to the attacked site is cached by the CDN service and replied to future legitimate requests thus could render the service unavailable.

- Several critical vulnerabilities have been discovered in the Mozilla Firefox web browser and Firefox Extended Support Release (ESR), and a high-severity bug has been reported for Google Chrome, all of which could allow for arbitrary code execution.

- PHP7 remote code execution vulnerability (CVE-2019-11043) which has been recently patched, is now exploited in the wild to take over servers. PoC for the vulnerability has been published on Github earlier this week and threat actors were quick to take advantage of the bug.

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

- Vulnerabilities in the Click-to-Pray-eRosary, a $100 electronic prayer device which syncs with the Pope's Worldwide Prayer Network, allow brute force attackers to access users account details, including user phone number, height, weight and complete prayer history and progress.

THREAT INTELLIGENCE REPORTS

- Tracking the origins of DarkRat, a malware spread by RIG Exploit Kit, Check Point Researchers describe its business model, from the HackForums.net underground market to its presumed original developer.

  Check Point Anti-Virus blade provides protection against this threat (RAT.Win32.DarkRat)

- 42 Google Play Store apps with 8 million users have been found to include adware, developed by a Vietnamese university student. All apps were registered to the student's real details.

  Check Point SandBlast Mobile provides protection against this threat

- Raccoon, a new info stealer operating since April 2019 in a MaaS (Malware as a Service) model, has gained popularity and infected hundreds of thousands of endpoints in just a few months. Threat actors behind it are believed to be Russian speakers and its development is continuing. Functionality includes collection of credit card information, cryptocurrency wallets, passwords, emails, cookies and more.

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