April 29 – May 5, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

# YOUR CHECK POINT THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- A newly reported breach exposes personal information of 80 million American households. Records include full names, addresses, marital status, income brackets and more. The breached database, whose owner has not been revealed, was left unprotected on a Microsoft cloud server.

  *Check Point CloudGuard provides protection against this threat*

- A botnet attack against the popular Electrum bitcoin wallet has now reached over 150,000 infected users and continues targeting authentic Electrum servers with DDoS attack to funnel users to their malicious servers. Stolen users' funds reach $4.6 million.

- American software company Citrix has fallen victim to a cyber-attack exposing company data for roughly five months. The attackers have likely gained access to the network using brute-force password cracking.

- Ransomware attack at Cleveland Hopkins Airport has disabled the flight and baggage information systems. City Hall said attackers have not been contacted and no ransom was paid.

- Over 200 online university campus stores in North America have been hit by a credit card skimming attack dubbed "Mirrorthief". Attackers have compromised the PrismWeb commerce platform and injected a skimming script into the shared JavaScript libraries used by online stores.

- Aluminum producer Norsk Hydro, which suffered a massive cyber-attack by the LockerGoga ransomware in mid-March, estimates its cost at $50 million. The company did not pay ransom and expects its cyber insurance to cover losses.

  *Check Point Sandblast provides protection against this threat (Ransomware.Win32.LockerGoga)*

- A recently disclosed vulnerability in Oracle Weblogic is being actively exploited to install the Sodinokibi ransomware.

  *Check Point IPS blade provides protection against this threat (Oracle WebLogic Server Remote Code Execution (CVE-2019-2725))*

## VULNERABILITIES AND PATCHES

- Check Point Researchers have found critical vulnerabilities in all of ISPsystems products including ISPmanager, Billmanager, DCImanager and VMmanager. This vulnerability allows an attacker to hijack a session of a logged-in user and take control over its websites, virtual machines, billing data, etc.

  *Check Point IPS blade provides protection against this threat (ISPsystem COREmanager Authentication Bypass)*

- Dells SupportAssist software, which arrives preinstalled on laptop and desktop computers, has been reported to suffer from two high-severity flaws which could enable remote code-execution (RCE) and cross-site request forgery (CSRF) attacks.

  *Check Point IPS blade will provide protection against this threat in its next online package (Dell SupportAssist Client Software Remote Code Execution (CVE-2019-3719))*

- Cisco has released security patches to address tens of vulnerabilities in its products. One of the fixed flaws, tracked as CVE-2019-1804, resides in the SSH key management for the Nexus 9000 switches, and could allow attackers to connect to the system with root privileges.

## THREAT INTELLIGENCE REPORTS

- Investigation of the data leaked concerning the activity of the Iranian-linked OilRig (APT 34) APT group reveals the group was targeting 97 different organizations across 27 countries. Organizations included government, media, energy, transportation, logistics and technology service providers and along the way, Oil Rig stole 13,000 credentials used for logging into targets' online services.

- A leading dark web marketplace - Wall Street Market, used for trading drugs, stolen credit card numbers, malicious software and other illegal goods - has been shut down in a joint operation of the Europol, FBI and the Dutch police, who arrested three of its managers.

- United Kingdom’s National Cyber Security Centre (NCSC) report reveals that over 23 million breached accounts have used ‘123456’ as password. Other 7.7 million used ‘123456789’. Other common weak passwords included ‘querty’ and ‘1111111’. A full list of 100,000 failing passwords can be found here.

- Security researches have revealed “Retefe” Banking Trojan has resurfaced with new capabilities, including using the “stunnel” encrypted tunneling mechanism instead of “Tor”, and abusing a legitimate shareware app as an installation technique.

  *Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Banking.Win32.Retefe)*