Check Point
SOFTWARE TECHNOLOGIES LTD.

February 17 - 23, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers are following an evolving, ongoing Malspam campaign that is targeting more than 80 Turkish companies with the Adwind remote access Trojan. "The Turkish Rat" uses different evasive methods to bypass security solutions.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan-Downloader.Wins.Generic.A; Win32.Adwind.A-E)

- US Department of Homeland security DHS has announced a ransomware attack on a US natural gas facility. The attackers used a spear phishing link to obtain initial access to the organization's IT network then deployed commodity ransomware that eventually caused the shutdown of the entire pipeline for 2 days.

- MGM resorts have suffered a data breach exposing over 10.6 million guests' names, addresses, and passport numbers. The data breach stems from a security incident that took place last year. Among people affected were business travelers, reporters attending tech conferences, CEOs, government officials, and celebrities like Justin Bieber and Twitter founder Jack Dorsey.

- Defense Information Systems Agency (DISA), responsible to maintain secure communication for the White House, US diplomats, and military troops, has disclosed a data breach that took place between May and July 2019, exposing personal information and social security numbers of over 200,000 individuals.

- ISS World, global facilities company, has suffered a ransomware attack that affected their IT systems, shutting down the company's web site and disabling mail and web access to 43,000 employs.

- Croatia's petrol station chain INA group has been hit by "CLOP" ransomware. The attack affected normal operations such as issuing mobile phone vouchers, electronic vignette and paying utility bills.

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

VULNERABILITIES AND PATCHES

- Cisco has released security updates to address 17 vulnerabilities including remote access and code execution, elevation of privilege, denial of service, and cross-site request forgeries.
- Adobe has released an out-of-band patch to fix two vulnerabilities (CVE-2020-3764, CVE-2020-3765) that may expose user systems to remote code execution.
- A new Vulnerability has been found in Apache Tomcat AJP (CVE-2020-1938) allowing a file read/inclusion in the AJP connector that enables by default configuration port of 8009. A remote, unauthenticated attacker may exploit this vulnerability to execute arbitrary code or obtain sensitive information on the system.

  Check Point IPS blade will provide protection against this threat in its next online package (Apache Tomcat AJP File Inclusion (CVE-2020-1938))
- Researchers have found a vulnerability on 4G/LTE mobile service that could permit a highly-skilled attacker to impersonate the phone's owner and run up bills, upload illegal files under his identities, and intercept unencrypted internet traffic. This is due to a probability that's built into all devices that use LTE service.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have recently discovered a new clicker malware family dubbed Hacken, along with fresh samples of the Joker malware family, in Google Play.

  Check Point SandBlast Mobile provides protection against this threat
- Researchers have found a new remote access Trojan named "Oblique" deployed in a new campaign targeting organizations across Southeast Asia. The attack is being spread through phishing emails attached with malicious Microsoft Office documents.

  Check Point Anti-Virus blade provides protection against this threat (RAT.Win32.ObliqueRAT.TC)
- Active exploits are targeting the recently patched flaw in the popular WordPress plugin Duplicator, which has more than 1 million active installations. Researchers found that 50,000 of the attacks occurred even before fixing the unauthenticated arbitrary file download vulnerability.

  Check Point IPS blade provides protection against this threat (WordPress Sensitive System Files Information Disclosure)
- Researchers have spotted "Operation Transparent Tribe" after 4 years. Pakistan aimed Campaign that targets Indian diplomatic and military interests. The attackers are using a macro document with a fake certificate of a request of an Indian public fund to deploy the attack.