June 22 - 28, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have discovered an ongoing, evolving campaign from a known hacking group called "DarkCrewFriends." This campaign targets PHP servers, focusing on creating a botnet infrastructure that can be leveraged for several purposes such as monetization and shutting down critical services.

  Check Point IPS provides protection against this threat (Command Injection Over HTTP, PHP Web Shell Generic Backdoor)

- An ongoing Magecart attack has been targeting 8 US city websites, all built on the Click2Gov platform that allows governments to provide services such as e-payment and complaint management. The attack allows credit card skimmers to steal payment and personal information of all citizens using the websites.

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

- Docker servers have been hit with what seems to be the first organized and persistent series of attacks that infect misconfigured clusters with DDoS malware. According to researchers, the two botnets are running versions of XORDDoS and the Kaiji malware, both first spotted to target a complex cloud setup.

  Check Point Anti-Bot blade provides protection against this threat (Backdoor.Linux.Xorddos)

- A European bank has been hit by the largest ever DDoS attack that peaked at a record 809 million packets per second. Most IP addresses behind the attack were utilized as a part of a DDoS attack for the first time ever, meaning that it might be an entirely new botnet.

- LG Electronics has been hit by Maze ransomware. The attackers claim to have stolen over 40GB of information including source code and proprietary information for projects that involve large US companies.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Ransomware.Win32.Maze)

- "GoldenSpy" backdoor has been found in a Chinese bank's official tax software. The bank reportedly forced at least 2 western companies, a UK-based technology vendor and a major financial institution, to install the tax software, produced by the Golden Tax Department of Aisino Corporation, for paying local taxes.

  Check Point SandBlast and anti-Bot provide protection against this threat (Goldenspy)

VULNERABILITIES AND PATCHES

- Researches have disclosed that 300 Windows 10 executables are vulnerable to DLL hijacking. The vulnerability can be exploited with a VBScript containing the ability to use a legitimate Windows executable for side loading of an arbitrary DLL of the attacker's choice that may allow attacker to gain administrative privileges and bypass UAC (User Account Control) entirely.
- Apache has released a security advisory for Apache Tomcat, patching a vulnerability that could cause a denial-of-service condition (CVE-2019-10072).

  Check Point IPS provides protection against this threat (Apache Tomcat Denial of Service (CVE-2019-10072))
- Cisco has released a security advisory on a Telnet vulnerability (CVE-2020-10188) affecting Cisco IOS XE devices. A remote attacker could exploit this vulnerability to take control of an affected system.
- NVIDIA has released a software security update for NVIDIA GPU Display Driver. This update addresses issues that may lead to denial of service, escalation of privileges, or information disclosure.
- A vulnerability has been found in Bitdefender Anti-virus (CVE-2020-8102), which allows an external, specially crafted, web page to run remote commands inside the Safepay Utility process.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed the latest Coronavirus-themed cyber-attacks. As businesses transition their workforces back to the office, hackers are distributing phishing emails and malicious files disguised as Coronavirus training materials. The latest data also shows that the risk of an organization being impacted by a malicious coronavirus-related website depends on whether the country it is located in has gone back to business or is still under lockdown.
- Researches have stated that the "CryptoCore" group, believed to operate out of Eastern Europe, has stolen around 200 million dollars from cryptocurrency exchanges via supply-chain attack over two years.
- Lucifer, a new variant of powerful crypto-jacking and DDoS malware, has been exploiting severe vulnerabilities in order to infect Windows machines in a currently active campaign.

  Check Point SandBlast provides protection against this threat (Cryptominer.Win32.Lucifer)
- A new ransomware variant called "WastedLocker" is demanding payment of millions of dollars in a wave of attacks against US organizations including eight Fortune 500 companies. The ransomware is developed by Evil Corp group, also known as the Dridex gang, members of which have recently been charged by the US Department of Justice.

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