Check Point
SOFTWARE TECHNOLOGIES LTD.

Nov 16 - 22, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- With Black Friday weekend approaching, Check Point Research has found an 80% increase in malicious phishing campaigns targeting online shoppers in the form of “special offers”.

  Check Point Anti-Phishing provides protection against this threat

- Managed.com, a provider of managed web hosting solution, has been hit by ransomware attack. The company has taken down its entire web hosting infrastructure, including WordPress, DotNetNuke, email, DNS, FTP services, RDP access points, and online database. One of the indirect victims of this attack was DERBY – Griffin Hospital, with its website going offline, but no sensitive information was exposed.

  Check Point SandBlast Agent provides protection against this threat

- The Biden-Harris presidential campaign site has been hacked and defaced by a Turkish hacker. The website vote.joebiden.com showed a message in Turkish for 24 hours and is currently taken offline.

- The Christian faith app Pray.com has suffered a data leak from its Amazon Web Services S3 bucket due to misconfiguration in its integration with AWS CloudFront content delivery network (CDN). The leak exposed PII, church donation information, photos, and users’ contact lists of over 10 million people.

  Check Point CloudGuard provides protection against this threat

- The municipal services in Kuurne, Belgium, have been hit by the WannaMine cryptominer. The municipality’s services have been taken offline until the investigation and mitigation is done.

  Check Point SandBlast Agent and Anti-Bot provides protection against this threat *(Trojan.Win32.WannaMine)*

- The Munich GWG housing association has been hit by a ransomware attack. Much of the company’s IT system and data is affected, including backup servers.

  Check Point SandBlast Agent provides protection against this threat

- Manchester United football club has disclosed a security breach that impacted their internal system. There are currently no signs of compromise to personal data associated with fans or customers.

VULNERABILITIES AND PATCHES

- Facebook has patched a bug in its Messenger app for Android. The bug could allow callers to connect audio calls without the caller's knowledge or approval.
- Google has released a chrome security update addressing multiple vulnerabilities. Some of them could allow an attacker to take control of an affected system.
- A security vulnerability in Bumble, a popular dating app, could have exposed the personal information of its entire 100 million users. The flaw was found in the user request server-side verification.
- VMware has addressed two exploitable ESXi vulnerabilities that were disclosed during the Tianfu Cup International PWN contest (CVE-2020-4004, CVE-2020-4005).
- Drupal has released a security update patching a critical remote code execution vulnerability allowing attackers to add a second extension to a malicious file and upload it on a Drupal site, then running unauthorized code on the vulnerable website.
- An unpatched security flaw in GO SMS Pro messaging app for Android, with over 100 million installs, exposes sensitive media shared between users including private voice messages, photos, and videos.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published a report about the threats of voice phishing, listing their different techniques used in attacks as seen in the wild.
- A new variant of the point-of-sale Grelos skimmer malware has been identified. The malware is targeting the payment-card data of online retail shoppers on dozens of compromised websites.
- Researches reveal the Qbot banking Trojan operation group is now deploying the recently exposed ransomware variant, Egregor.

  Check Point SandBlast Agent and Anti-Bot provide protection against this threat *(Trojan.Win32.QBot)*
- The Trickbot cyber gang has released the 100 version of the Trickbot malware with additional features for detection evasion. One of the malware's new features is the ability to inject malicious DLL into the Windows wermgr.exe executable directly from memory using code from the "MemoryModule" project.

  Check Point SandBlast Agent and Anti-Bot protect against this threat *(Botnet.Win.Trickbot; Trojan-Banker.Win32.TrickBot)*
- The Mount Locker ransomware operation is currently targeting files used by TurboTax tax returns software, aiming to encrypt tax-related files prior to the tax season.

  Check Point SandBlast Agent provides protection against this threat