Check Point
SOFTWARE TECHNOLOGIES LTD.

Aug 23 - 29, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Karapatan, the Philippine human rights alliance, has suffered a massive and prolonged Distributed Denial of Service (DDoS) attack. The attack targeted the online solidarity campaign #StopTheKillingsPH and was allegedly conducted by the local government.
- EskyFun, a Chinese mobile gaming company, has suffered a data breach exposing the information of over 1 million gamers on an unsecured server.
- FIN8, a financially motivated cybercrime gang, has breached the network of a US financial organization with a new malware known as “Sardonic”.
- Users of OpenSea, a peer-to-peer marketplace for crypto collectibles and non-fungible tokens (NFT), are being targeted in an ongoing tech-support phishing attack that aims to steal cryptocurrency funds and NFTs. Threat actors have been lurking the OpenSea Discord server, waiting for users asking for support and answering them with links to private chats where they conduct their phishing attack.
- The Boston Public Library (BPL) has been hit by a cyberattack, leading to a system-wide outage, and online library services that require login remained unavailable.
- A new campaign has been initiated by the APT threat group Earth Baku, leveraging a new toolset and focusing on targets in the Indo-Pacific region. Their tools include SQL injection and exploit of Microsoft Exchange Server ProxyLogon as entry vectors, new shellcode loaders, and Cobalt Strike as a payload.

  Check Point IPS and Harmony Endpoint provide protection against this threat *(Microsoft Exchange Server Remote Code Execution (CVE-2021-26855))*

- Microsoft warns of a widespread credential phishing campaign that leverages open redirect links in email communications as a vector to trick users into giving in their credentials.

  Check Point Harmony Email & Office provides protection against this threat

VULNERABILITIES AND PATCHES

- A recently reported flaw in Azure Cosmos DB could have allowed any Azure user to remotely take-over other users' databases without any authorization.
- Atlassian has released patches to fix a critical flaw (CVE-2021-26084) affecting the Confluence enterprise collaboration product.
- Kaseya has released a security update addressing multiple zero-day server-side vulnerabilities in "Kaseya Unitrends".
- Security vendor F5 has addressed more than a dozen server vulnerabilities in its BIG-IP networking device that could lead to complete system takeover.
- Researches have discovered a vulnerability that allowed to bypass PIN codes on contactless credit and debit cards from MasterCard and Maestro.
- Experts have discovered a critical remote code execution vulnerability (CVE-2021-32941) that can be exploited to hack the network video recorder manufactured by physical security company Annke.

THREAT INTELLIGENCE REPORTS

- The Federal Bureau of Investigation (FBI) has released a flaw alert on the Hive ransomware attacks that includes technical details and indicators of compromise associated with the operation of the gang.

  Check Point Harmony Endpoint provides protection against this threat

- LockFile, a newly discovered ransomware family, is leveraging a technique called "intermittent encryption" to bypass protection – it does not encrypt the beginning of the file and only encrypts parts of it. LockFile is exploiting recently disclosed flaws such as ProxyShell and PetitPotam to mount Windows servers.

  Check Point IPS and Harmony Endpoint provide protection against this threat (Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); Microsoft Active Directory Certificate Services NTLM Relay)

- Phorpiex botnet has shut down all operations on May 2021 and as of this week, the operation posted its source code for sale in multiple dark web forums.
- Experts have discovered a modified version of WhatsApp for Android, which offers extra features that install the Triada Trojan on infected devices.

  Check Point Harmony Mobile provides protection against this threat