Oct 11 – 17, 2021

Check Point SOFTWARE TECHNOLOGIES LTD.

# YOUR CHECK POINT THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Israeli Medical Center Hillel Yaffe has been targeted by ransomware affecting the hospital’s computer systems, which have been working in a limited capacity since the attack occurred.

- Russia-based group TA505 is running a new email phishing campaign dubbed MirrorBlast, targeting financial organizations with malicious macro-embedded Excel documents.

  *Check Point Threat Extraction provides protection against this threat*

- CISA has alerted that US Water and Wastewater Systems (WWS) Sector facilities were targeted multiple times in ransomware attacks in the course of the past two years.

- Security researchers have identified Iran-linked hacker group targeting American and Israeli defense technology companies in extensive password spraying attacks targeting their Office365 accounts.

- Taiwanese computer giant Acer has confirmed that its offices in India were breached by Desorden threat group affiliates, who stole 60GB of data.

- Banco Pichincha, Ecuador's largest private bank, has been victim of a cyberattack that shut down the bank’s applications, portals, networks, and ATM machines.

- US Korean American bank, Pacific City Bank, has been the victim of a ransomware incident in which hackers accessed loan application documents including tax returns or payroll records.

- British Sunderland University has issued a statement regarding widespread operational issues that have taken down most of its IT systems due to a major cyberattack.

- Chinese-speaking APT group “IronHusky” has been leveraging a Windows zero-day vulnerability (CVE-2021-40449) in the Windows Win32k kernel driver to deploy a previously unknown Remote Access Trojan “MysterySnail” to set up a command-and-control point for espionage purposes.

  *Check Point IPS provides protection against this threat* *(Microsoft Win32k Elevation of Privilege (CVE-2021-40449))*

## VULNERABILITIES AND PATCHES

- After seeing reports of stolen crypto wallets triggered by free airdropped NFTs, Check Point Research investigated OpenSea, the world's largest NFT marketplace. The investigation led to the discovery of critical security vulnerabilities on OpenSea's platform that, if exploited, could have led hackers to hijack user accounts and steal entire crypto wallets of users, by sending malicious NFTs.
- Apple has issued iOS 15.0.2 and iPadOS 15.0.2 in an attempt to patch CVE-2021-30883, a zero-day vulnerability that is actively exploited in the wild and could lead to execution of arbitrary code with kernel privileges.
- Technical data on how to exploit the Apache server vulnerability CVE-2021-40438 has been published, indicating that it might soon start to be widely exploited by threat actors.

  *Check Point IPS provides protection against this threat (Apache HTTP Server Server-Side Request Forgery (CVE-2021-40438))*
- Vulnerabilities have been discovered in the Nitro Pro PDF reader (CVE-2021-21796, CVE-2021-21797), triggered when opening a malicious PDF, could allow threat actors to execute code in the application.

## THREAT INTELLIGENCE REPORTS

- Government officials from over 30 countries have declared they would start disrupting the cryptocurrency payment channels exploited by ransomware groups to finance their campaigns.
- Mathematical symbols on fake company logos are now being used in phishing campaigns to avoid detection, redirecting victims to fake voicemail, requesting Office365 credentials to access it.
- Google Threat Analysis Group has announced it had sent about 50,000 alerts of state-sponsored phishing or hacking attempts to users throughout 2021, a 33% increase in comparison to 2020. The increase is mainly due to a large campaign by Russian group Fancy Bear.
- Analysis highlights how threat actors use DocuSign in email phishing campaigns.
- Australia's Minister for Home Affairs has released the "Australian Government's Ransomware Action Plan", a set of new measures the country will implement in an attempt to address the rising menace.
- A Google Play store app for Android, "Blender Photo Editor-Easy Photo Background Editor", containing malicious code that steals users' Facebook credentials to run ad campaigns on the user's behalf with their payment information, has been downloaded by thousands and is still available on the store.

  *Check Point Harmony Mobile provides protection against this threat*