Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Guacamaya hacking group claim to have breached the Attorney General of Colombia, and leaked massive amount of data that revealed identities and methods of Australian Federal Police secret agents working to stop major drug importations to Australia. The breached data includes five million emails and tens of thousands of documents.
- Automaker Toyota has warned customers that their personal information may have been compromised after an access key was accidentally published on GitHub for almost five years. The automaker has reported that no credit card data or phone numbers have been exposed.
- The pro-Russian hacktivist group 'KillNet' has launched several DDoS attacks against major airlines' websites in the United States, making them inaccessible.
- Threat actors have launched a cyberattack against Tata Power Company Limited, India's largest power generation company, which allegedly affected some of its IT systems. The company is yet to share details on the scale of the attack.
- Online shopping company Woolworths has reported a data breach impacting over two million Australian users of its MyDeal subsidiary. The company said the breach was due to a compromised user credential that was used to gain unauthorized access to MyDeal's customer relationship management system.
- Hackers have hijacked the official Twitter account of the Indian Embassy in Ireland and performed various cryptocurrency fraudulent activities by impersonating Elon Musk - the hackers edited the embassy's Twitter account profile picture and name to that of Elon Musk to appear legitimate.
- Researchers have identified a new Chinese Advanced Persistent Threat cyberespionage group (APT) dubbed WIP19 that has been targeting Telecom and IT service providers in the Middle East and Asia.
- Security Researchers have revealed a campaign by the POLONIUM cyberespionage group that targeted a dozen Israeli companies using custom backdoors and spying tools. According to their findings, POLONIUM is based in Lebanon and is likely to coordinate its activities with other threat actors tied to Iran's Ministry of Intelligence and Security (MOIS).
- Threat Actors have been targeting Windows 10 and 11 home users with malicious JavaScript files that impersonate Windows Security updates to deliver the Magniber ransomware.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Magniber)

VULNERABILITIES AND PATCHES

- Zimbra has released a patch to an ongoing exploitation of CVE-2022-41352, along with mitigation steps that can be implemented to prevent exploitation.
- Security researchers have reported CVE-2022-36067 - a critical remote code execution vulnerability that would allow hackers to bypass vm2 sandbox environment and run shell commands on the machine hosting the sandbox.
- Security researchers have recently discovered nine vulnerabilities in the Robustel R1510 industrial cellular router that if exploited could lead to remote code execution. The researchers have said that a patch is available and users are encouraged to update the affected products: Robustel R1510, version 3.3.0 and 3.1.16.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports that during September 2022, the infostealer Vidar has entered the top ten most prevalent malwares list following a fake Zoom campaign. Cyberattacks in Eastern European countries have increased dramatically and Education/Research is the most impacted sector worldwide.
- The Microsoft Threat Intelligence Center (MSTIC) has disclosed new ransomware dubbed 'Prestige' that is being used by threat actors to target transportation and logistics organizations in Ukraine and Poland. The ransomware was first observed in the wild on October 11, and is yet to be linked to a specific threat actor.
- Security researchers have discovered a new attack framework dubbed 'Alchimist' and a new RAT malware dubbed 'Insekt' that targets Windows, macOS, and Linux. The researchers say that Alchimist has a web interface in Simplified Chinese with remote administration features such as establishing remote sessions, deploying payload to the remote machines, capturing screenshots, performing remote shellcode execution, and running arbitrary commands.
- A new report suggests that there is a possible connection between Ransom Cartel, which is a Ransomware as a Service (RaaS) that was first seen in mid-December 2021, and the notorious REvil ransomware group operators who went quiet in October 2021 due to major multi-government entities pursuing the group. The researchers identified technical similarities and overlaps between Ransom Cartel and REvil.
- Researchers have discovered a relatively new ransomware dubbed "Royal" that uses various infection vectors, depending on the targeted victim. Although uncertain at this point, the group may employ the double extortion tactic in its attacks.