Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Both Windows and macOS versions of 3CXDesktopApp, a VoIP application of 3CX Communications Company, were compromised and used to distribute Trojanized versions in a large-scale supply chain attack. In this widespread campaign, dubbed SmoothOperator, threat actors have misused 3CX's application with a malicious file that is loaded using 3CXDesktopApp and beacons to the attacker's infrastructure. More than 600,000 companies worldwide which use 3CX may be affected by this attack. The attack is linked to the North Korean Lazarus group, and is tracked as CVE-2023-29059.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Trojan-Downloader.Win.SmoothOperator; Trojan.Wins.SmoothOperator)*

- Australia's largest gambling and entertainment firm, Crown Resorts, has disclosed that it is being extorted by CL0P ransomware group. This extortion attempt is also a result of CL0P's group exploitation of Fortra GoAnywhere vulnerability.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Wins.Clop; Ransomware.Win.Clop; Ransomware_Linux_Clop)*

- The LockBit ransomware group leaked the files taken from South Korean National Tax Service (NTS) on the group's shame blog, after the agency had not paid the ransom that was demanded.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Win.LockBi; Ransomware.Wins.Lockbit)*

- American debt management firm NCB has confirmed that information of 500,000 customers has been disclosed in a security breach. According to the company, the compromised data included both personal and financial information like account balances, salaries, credit card numbers and more.

- TMX Finance, a US based consumer lending company, and its subsidiaries (TitleMax, TitleBucks, and InstaLoan) have reported a data breach that exposed the personal data of over 4.8 million customers. The breach occurred in December 2022 but was discovered only in February 2023.

- The Netherlands' national railway company, NS, has notified about 780,000 customers that their data may have been accessed in a potential data breach.

VULNERABILITIES AND PATCHES

- Customers of QNAP have been advised to take necessary measures to protect their Linux-powered network-attached storage (NAS) devices against a high-severity Sudo privilege escalation vulnerability (CVE-2023-22809).
- Researchers analyzed a high-risk Cross-Site Scripting vulnerability (CVE-2023-23383) in Azure Service Fabric Explorer (SFX) dubbed 'Super FabriXss' that could lead to unauthenticated remote code execution.
- Researchers have discovered a critical remote code execution vulnerability (CVE-2023-25076) in the SNIProxy open-source tool. The vulnerability exists if a user is utilizing wildcard backend hosts when configuring SNIProxy.
- Threat actors are actively exploiting a now fixed vulnerability in Elementor Pro, a widely-used WordPress plugin with over 11 million website users. The plugin enables easy website building for WooCommerce.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released an extensive publication and analysis of the Rhadamanthys infostealer that was launched on the dark web in September 2022. CPR showcases a step-by-step disassembly breakdown of how the malware compiles its own database of stolen Google Chrome information in order to send back to the C2 server.

  Check Point Threat Emulation provides protection against this threat *(InfoStealer.Wins.Rhadamanthys)*

- Researchers have been tracking the hacktivist group Anonymous Sudan, which had been engaged in launching multiple DDoS attacks on organizations in Europe, Australia, Israel and more, often in response to what is perceived as anti-Muslim activity. The group is currently considered and identified as a sub-group of the Russia affiliated hacktivists group Killnet, and supports its agendas.
- Researchers have alerted on a new attack vector in Azure Active Directory (AAD), which is based on a common AAD misconfiguration, exposing misconfigured apps to unauthorized access. Among the vulnerable Microsoft applications also the Bing.com application. The attack can allow unauthorized access and modification of search results.
- Several leading investigative news outlets published an analysis of documents belonging to a Russian IT contractor named NTC Vulkan. The documents include information about projects that were done by the contractor for the Russian GRU Unit 74455, also known as Sandworm Team.