Edition 191

23rd September 2022

Uber blog on their ongoing security breach

The security breach that hit Uber last week was the work of Lapsus$, Uber said in a blog post. The South American hacking group has attacked a number of technology giants in the past year, including Microsoft, Samsung, and Okta. Uber said it is in close coordination with the FBI and US Justice Department on the matter. While the attackers accessed several internal systems, Uber said it does not appear they infiltrated any public-facing systems, user accounts, or databases that store sensitive user information like credit card numbers. Additionally, Uber said it doesn't appear that the attackers accessed any customer or user data stored by its cloud providers. The hackers did download some internal messages, as well as information from an internal finance team. They also accessed Uber's dashboard at HackerOne, where security researchers report bugs and vulnerabilities. However, any bug reports the attacker was able to access have been remediated, Uber said.

The hacking group told the New York Times that they gained access to Uber's systems through a social-engineering scheme. They sent a text message to an Uber employee claiming to be a corporate IT staffer, which persuaded the staff member to reveal a password. However, Uber clarified Monday that the hacker gained access using credentials from a third-party contractor. Furthermore, the company said it's "likely" that the Lapsus$ hacker obtained the contractor's Uber corporate password by purchasing it on the dark web, after the contractor's

personal device had been infected with malware. After that, Uber said, the hacker repeatedly tried to log in to the contractor's Uber account but was stymied by a two-factor login approval request. However, the contractor eventually accepted one of those requests. From there, the hacker obtained elevated permissions to a number of internal tools, including G-Suite and Slack.

Edited: Original source – ZNet

VMware, Microsoft warn of widespread Chromeloader malware attacks

VMware and Microsoft are warning of an ongoing, widespread Chromeloader malware campaign that has evolved into a more dangerous threat, seen dropping malicious browser extensions, node-WebKit malware, and even ransomware in some cases. Palo Alto Network's Unit 42 noticed that Chromeloader was evolving into an info-stealer, attempting to snatch data stored on the browsers while retaining its adware functions. Microsoft warned about an "ongoing wide-ranging click fraud campaign" attributed to a threat actor tracked as DEV-0796 using Chromeloader to infect victims with various malware.

Analysts at VMware published a technical report describing different variants of Chromeloader that were used in August and this month, some of which are dropping much more potent payloads. The ChromeLoader malware is delivered in ISO files that are distributed through malicious ads, browser redirects, and YouTube video comments. While Chromeloader started as adware, it is a perfect example of how threat actors are experimenting with more potent payloads, exploring more profitable alternatives to advertising fraud.

Edited: Original source – Microsoft

EU moves to protect journalists from spyware

European Union lawmakers are aiming to protect journalists from member states targeting them with spyware following a number of high-profile incidents across the bloc. Alongside measures promoting ownership transparency and editorial independence, the European Media Freedom Act (EMFA) proposed on Friday will introduce “strong safeguards against the use of spyware against media, journalists and their families.” Article 4 of the regulation — an EU instrument which has direct effect without member states’ needing to reflect it with their own legislation — introduces a general prohibition on member states trying to: “detain, sanction, intercept, subject to surveillance or search and seizure, or inspect media service providers or, if applicable, their family members, their employees or their family members, or their corporate and private premises, on the ground that they refuse to disclose information on their sources, unless this is justified by an overriding requirement in the public interest.”

It also explicitly bans any attempt to: “deploy spyware in any device or machine used by media service providers or, if applicable, their family members, or their employees or their family members, unless the deployment is justified, on a case-by-case basis, on grounds of national security”.

Edited: Original source – Digital Strategy

Russian threat group continues to target Ukrainian organisations

A known Russian threat group is targeting Ukrainian organizations with a new info-stealing malware in an espionage campaign. The infostealer uses lures related to the recent Russian attack on Ukraine. Researchers from Cisco Talos linked the campaign to the Russian state-backed threat group Gamaredon, which is known for targeting entities in the Ukrainian government, critical infrastructure, security, defense, and law industries. Researchers claim that Gamaredon's new infostealer is capable of stealing files from attached storage devices (local and remote). The infostealer could be a component of Gamaredon's Giddome backdoor family, however, researchers could not confirm the same.

It comes with clear instructions to steal files with the following extensions: .DOC, .XLS, .RTF, .DOCX, .ODT, .TXT, .JPEG, .PDF, .JPG, .PS1, .ZIP, .7Z AND, .RAR, and .MDB. Moreover, while performing recursive enumeration of files in directories, the stealer avoids system folders and focuses on files of interest. The infostealer is spread using a PowerShell script similar to one mentioned in a recent alert posted by Ukraine CERT regarding Gamaredon's intrusions during H1 2022. The malware is delivered via phishing emails laden with Office documents with malicious VBS macros. It makes POST requests with metadata and its content with each stolen file. It can download more files from the C2 server that delivers instructions on delivered data treatment. The infostealer was added to the Virus Total database over a month ago and detected by 50 antivirus engines.
Edited: Original source – CISCO Talos

Password Management solution LastPass reveals details of about its security breach

Password management solution LastPass shared more details about the security breach that the company suffered in August 2022. The company revealed that the threat actor had access to its network for four days in August 2022. LastPass CEO Karim Toubba explained that there is no evidence that the attackers had access to customer data.

"We have completed the investigation and forensics process in partnership with Mandiant. Our investigation revealed that the threat actor's activity was limited to a four-day period in August 2022. During this timeframe, the LastPass security team detected the threat actor's activity and then contained the incident." reads the Notice of Recent Security Incident published by the company. "There is no evidence of any threat actor activity beyond the established timeline. We can also confirm that there is no evidence that this incident involved any access to customer data or encrypted password vaults."

The threat actors gained access to the Development environment using a developer's compromised endpoint. The company pointed out that the attackers did not have access to the master passwords of its customers' vaults because they haven't access to them, which means that only the owner of a vault can decrypt vault data. The company performed a check of its source code to verify its

integrity after the attack, it added that developers cannot push source code directly from the development environment into production. It has also hired a leading cyber security firm to further enhance the source code safety practices adopted by the company.

Edited: Original source – LastPass

US Cyber Agency CISA orders agencies to patch vulnerability used in Stuxnet attacks

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added half a dozen vulnerabilities to its catalog of Known Exploited Vulnerabilities and is ordering federal agencies to follow vendor's instructions to fix them. Of the six security flaws, only one was disclosed this year. It impacts Trend Micro's Apex One platform for automated threat detection and response. CISA is giving federal agencies until October 6th to patch security vulnerabilities that have been reported between 2010 and 2022.
Exploiting most of them gives an attacker admin-level permissions (local privilege escalation - LPE) on the system while for two the result is remote code execution (RCE). Most of the vulnerabilities that CISA added to its KEV catalog were disclosed in 2013 and were used to root Android devices back in the day, through the Tizi malware.

- CVE-2013-6282 (LPE) -Linux kernel improper input validation that allows read/write to memory, used for rooting Android devices [VROOT]
- CVE-2013-2597 (LPE) - stack-based buffer overflow in Code Aurora audio driver
- CVE-2013-2596 (LPE) - Linux kernel integer overflow
- CVE-2013-2094 (LPE) - Linux kernel privilege escalation

The oldest bug that CISA ordered federal agencies to patch is from 2010 and was used to spread the Stuxnet worm that damaged the centrifuges at the Natanz uranium enrichment plant to slow the country's advancements towards developing nuclear weapons.

CVE-2010-2568 (RCE) - Microsoft Windows parsing shortcuts incorrectly, allowing code execution when displaying an icon of a malicious shortcut file
While the directive is for organizations in the U.S., companies and corporations around the world can use CISA's catalog to improve the security of their networks.

Edited: Original source – CISA

Payment Card Industry Data Security Standard Changes

The upcoming changes to the Payment Card Industry Data Security Standard (PCI DSS) will affect every organization that stores, transmits, or processes cardholder data and/or sensitive authentication data. Effective starting in March 2024, the new standard, known as PCI DSS 4.0, spans dozens of changes in areas including risk assessment, how keys and certificates are managed, and what can be accessed remotely. The update will also impact identity and access

management (IAM) and the technologies used for email filtering, anti-malware, multi-factor authentication (MFA), security information and event management (SIEM), as well as application development.

The requirements affect vast swaths of IT infrastructure--from network devices, virtual machines, authentication servers and cloud infrastructure to payment terminals, payment back-office systems, shopping carts, physical security systems, internal network security controls, and beyond. In addition, DSS v4.0 now defines requirements for specific technologies related to (for example) email filtering, anti-malware, multi-factor authentication, SIEM, and more Software Development Lifecycle (SDLC). For entities with bespoke applications, requirements will include documenting components used in the specific applications, reviewing them, and verifying security controls are properly implemented. Finally, the new standard impact's identity and authentication, including enhanced requirements for reviewing access and managing service and application accounts, in addition to changes to password requirements.

Edited: Original source – PCI Security Standards

Honeypots provide unique view on malicious Docker activity

Cybersecurity firms look to use honeypots to get a view of malicious activity in the cyberspace, such as actively exploited vulnerabilities, the latest tactics and techniques employed by adversaries, and any misconfigurations on platforms. In addition to capturing the TTPs, these honeypots can prove to be a boon by letting investigators make a stealth entry into the infrastructure operated by threat actors. Trend Micro's honeypots found two Docker Hub accounts belonging to TeamTNT, named alpineos and sandeep078, leaking credentials via exposed Docker REST APIs. These Docker Hub profiles were actively used to deploy malicious images containing rootkits, docker escape kits, XMRig Monero miners, credential stealers, Kinsing malware, and Kubernetes exploit kits.

Of the two Docker Hub accounts, alpineos hosted container images with over 150,000 pulls and was used in multiple exploitation attempts. A majority of IP addresses used in the attacks were located in Germany. The researchers explained that threat actors were logged in to their accounts in the DockerHub registry and probably forgot to log out. The attackers had logged into their Docker Hub account using the credentials of alpineos. As organizations are transitioning to the cloud, securing misconfigured container infrastructure and cloud services against cyber threats has become more imperative than ever. Attackers have been found abusing these infrastructures to conduct software supply chain and cryptojacking attacks.
Organizations are urged to take required security measures to secure Docker containers. These include creating policies for access and credential uses, as well as educating developers about the threat models in these environments.

Edited: Original source – Trend Micro

ISO archive hoax via PuTTY session

Mandiant has observed the new campaign and linked it with an emerging threat actor tracked as UNC4034. The threat group has been fabricating job lures for the distribution of AIRDRY malware. In the past, AIRDRY has been used by North Korea-linked hackers in attacks directed at the U.S., South Korea, and Latvia. The attack begins via initial contact over email, followed by a file being shared on Whatsapp. The file is an ISO archive that pretends to be an Amazon Assessment as part of a potential job opportunity. This archive has a text file with an IP address and login credentials, along with an altered version of PuTTY to load a dropper (DAVESHELL) that deploys a newer variant of AIRDRY.

It is suspected that the threat group convinced the victim to execute a PuTTY session using credentials given in the TXT file to connect to the remote host, activating the infection. It seems the use of ISO files may be motivated by Microsoft's decision to block Excel 4.0 and VBA macros. The use of similar ISO files for initial access is expected to witness a rise in the future, affirm experts.

Edited: Original source - Mandiant