APRIL EDITION 2022

THE THINGS YOU SHOULD KNOW

GITHUB: ATTACKER BREACHED DOZENS OF ORGS USING STOLEN OAUTH TOKENS

GitHub revealed today that an attacker is using stolen OAuth user tokens (issued to Heroku and Travis-CI) to download data from private repositories.

Since this campaign was first spotted on April 12, 2022, the threat actor has already accessed and stolen data from dozens of victim organizations using Heroku and Travis-CI-maintained OAuth apps, including npm.

"The applications maintained by these integrators were used by GitHub users, including GitHub itself," revealed Mike Hanley, the Chief Security Officer (CSO) at GitHub. GitHub Security identified the unauthorized access to GitHub's npm production infrastructure on April 12 after the attacker used a compromised AWS API key. The attacker likely obtained the API key after downloading multiple private npm repositories using stolen OAuth tokens.

"Upon discovering the broader theft of third-party OAuth tokens not stored by GitHub or npm on the evening of April 13, we immediately took action to protectGitHub and npm by revoking tokens associated with GitHub and npm's internal use of these compromised applications," Hanley added.
The impact on the npm organization includes unauthorized access to private GitHub.com repositories and "potential access" to npm packages on AWS S3 storage.

SPANISH FA REPORT CYBER-ATTACK TO POLICE AFTER EMAIL ACCOUNTS, PRIVATE TEXTS STOLEN

The Royal Spanish Football Federation (RFEF) has reported to the police that it was the victim of a cyber attack.

Documents and information from email accounts, private texts and audio conversations from top executives of the federation, including president Luis Rubiales, have been stolen in recent months.
"It is likely that this private information obtained illegally and with clear criminal purposes has been offered to different media," the RFEF said on Thursday.

An unnamed journalist warned the RFEF ahead of the publication of such information that his media outlet had been given access to illegally stolen material from an anonymous source that made contact using an encrypted voice.

"The media outlet in question claimed to have received, through third parties, confidential contracts, private WhatsApp conversations, emails and abundant documents regarding the RFEF management," the statement added. "If authentic, it would mean a crime of disclosure of secrets and a violation of the fundamental rights of the people attacked."

The Spanish FA has reported these "criminal and mafia" acts to all corresponding organizations and said it has hired a private company to increase security and prevent future attacks.

ACTIONS TARGET RUSSIAN GOVT. BOTNET, HYDRA DARK MARKET

The US Federal Bureau of Investigation (FBI) says it has disrupted a giant botnet built and operated by a Russian government intelligence unit known for launching destructive cyberattacks against energy infrastructure in the United States and Ukraine. Separately, law enforcement agencies in the US and Germany moved to decapitate "Hydra," a billion-dollar Russian darknet drug bazaar that also helped launder the

profits of multiple Russian ransomware groups.

FBI officials said they disrupted "Cyclops Blink," a collection of compromised networking devices managed by hackers working with the Russian Federation's Main Intelligence Directorate (GRU).

A statement from the US Department of Justice (DOJ) says that GRU's hackers built Cyclops Blink by exploiting previously undocumented security weaknesses in firewalls and routers made by both ASUS and WatchGuard Technologies. The DOJ said it did not seek to disinfect compromised devices; instead, it obtained court orders to remove the Cyclops Blink malware from its "command and control" servers — the hidden machines that allowed the attackers to orchestrate the activities of the botnet.

The FBI and other agencies warned in March that the Cyclops Blink malware was built to replace a threat called "VPNFilter," an earlier malware platform that targeted vulnerabilities in a number of consumer-grade wireless and wired routers. In May 2018, the FBI executed a similar strategy to dismantle VPNFilter, which had spread to more than a half-million consumer devices. On the other hand, German authorities seized the server infrastructure for the Hydra Market, a bustling underground market for illegal narcotics, stolen data and money laundering that's been operating since 2015. The German Federal Criminal Police Office (BKA) said that Hydra roughly had 17 million customers and over 19,000 vendors, with sales amounting to at least 1.23 billion euros in 2020 alone.

In a statement on the Hydra takedown, the US Department of Treasury said blockchain researchers had determined that approximately 86 per cent of the illicit Bitcoin received directly by Russian virtual currency exchanges in 2019 came from Hydra.

The Treasury sanctioned a number of cryptocurrency wallets associated with Hydra and a virtual currency exchange called "Garantex," which the agency says processed more than $100 million in transactions associated with illicit actors and darknet markets.

THE ORIGINAL APT: ADVANCED PERSISTENT TEENAGERS

LAPSUS$, a juvenile data extortion group whose short-lived, low-tech, and remarkably effective tactics have put some of the world's biggest corporations on edge. Since surfacing in late 2021, LAPSUS$ has gained access to the networks or contractors for some of the world's largest technology companies, including Microsoft, NVIDIA, Okta, and Samsung. LAPSUS$ typically threatens to release sensitive data unless paid a ransom, but with most victims, the hackers ended up publishing any information they stole (mainly computer source code).

Microsoft blogged about its attack at the hands of LAPSUS$ and about the group targeting its customers. It found LAPSUS$ used a variety of old-fashioned techniques that seldom show up in any corporate breach post-mortems, such as:

• Targeting employees at their personal email addresses and phone numbers

• Offering to pay $20,000 a week to employees who give up remote access credentials

• Social engineering help desk and customer support employees at targeted companies

• Bribing/tricking employees at mobile phone stores to hijack a target's phone number

• Intruding on their victims' crisis communications calls post-breach

The smash-and-grab attacks by LAPSUS$ obscure some of the group's less public activities, which according to Microsoft, include targeting individual user accounts at cryptocurrency exchange platforms to drain crypto holdings.
In some ways, the attacks from LAPSUS$ recall the July 2020 intrusion on Twitter, wherein the accounts of Apple, Bill Gates, Jeff Bezos, Kanye West, Uber and others were made to tweet messages inviting the world to participate in a cryptocurrency scam that promised to double any amount sent to specific wallets. The flash scam netted the perpetrators more than $100,000 in the following hours.

RAIDFORUMS GETS RAIDED, ALLEGED ADMIN ARRESTED

The US Department of Justice (DOJ) said that it seized the website and user database for RaidForums, an extremely popular English-language cybercrime forum that sold access to more than 10 billion consumer records stolen in some of the world's largest data breaches since 2015. The DOJ also charged the alleged administrator of RaidForums — 21-year-old Diogo Santos Coelho of Portugal — with six criminal counts, including conspiracy, access device fraud and aggravated identity theft.

The "raid" in RaidForums is a nod to the community's humble beginnings in 2015 when it was primarily an online venue for organizing and supporting various forms of electronic harassment. According to the DOJ, that early activity included 'raiding '— posting or sending an overwhelming volume of contact to a victim's online communications medium — and 'swatting,' a practice of making false reports to public safety agencies of situations that would necessitate a significant, and immediate armed law enforcement response."

But over the years, as trading in hacked databases became a big business, RaidForums emerged as the go-to place for English-speaking hackers to peddle their wares. Perhaps the most bustling marketplace within RaidForums was its "Leaks Market," which described itself as a place to buy, sell, and trade hacked databases and leaks.

WHAT IS SWATTING? - A NEW UPCOMING TREND.

Swatting is a dangerous hoax where hackers and other malicious parties dupe heavily-armed authorities and special services into responding to a false report. The swatters that call in these false reports hope that special units and emergency services will swarm in on innocent targets.

The term "swatting" is derived from the acronym SWAT — the special weapons and tactics force of the United States that is called in for a serious emergency like someone holding hostages, bomb threats, active shooters, or other serious criminal activity.

Though having SWAT teams respond to emergencies is a popular form of swatting incidents, swatters have also sent fire departments, police, ambulances, and even high-cost, cash-only pizza deliveries to targets. This means that, although SWAT is a special force in the United States, anyone in the world can become the victim of a swatting attack.

Many cases of swatting have stemmed from the online gaming community. Rival gamers might go after one another through swatting attacks, for example. Even so, anyone who gives away too much information about themselves on social media, in comment sections, in private messages, or through phone calls could easily become a victim.

MALWARE PROTECTION

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software." Common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

How do I protect my network against malware?

Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. However, some advanced malware will eventually make its way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defences. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

How do I detect and respond to malware?

Malware will inevitably penetrate your network. You must have defences that provide significant visibility and breach detection. In order to remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyber threats.

Types of malwares

Virus
Viruses are a subgroup of malware. A virus is a malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

Worms
Worms are malicious software pieces that rapidly replicate and spread to any device within the network. Unlike viruses, worms do not need host programs to disseminate. Instead, a worm infects a device via a downloaded file or a network connection before it multiplies and disperses exponentially. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

Trojan virus
Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

Spyware
Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to the predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

Adware
Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases, adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.

Ransomware
Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they

know. When the attacker receives payment, the data is unlocked.

Fileless malware

Fileless malware is a type of memory-resident malware. As the term suggests, it is malware that operates from a victim's computer's memory, not from files on the hard drive. Because there are no files to scan, it is harder to detect than traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted.

How to Remove Malware from a Computer

Antivirus software works by scanning the files on your system, looking for characteristics of known viruses; the vendor maintains a library of hundreds of thousands of malicious code types, from which it draws these digital earmarks. Therefore, it is critically important to update antivirus software regularly to maintain access to the most current library, as variants and new malware types appear regularly.

If the antivirus tool recognizes an infected file or the virus itself, and if there is a straightforward way to remove the malicious code, it will do so. Or it will sequester the infected file in a quarantine folder. Not all viruses can be easily or cleanly removed; some will require expert assistance. Additionally, no antivirus software is perfect or entirely up to date. Some newer viruses can evade detection. So, if your system is behaving erratically or if you have suffered a data loss or system damage, it's best to engage an expert consultant to diagnose the problem, remove the malware, and restore functionality.

Some Free Malware removal tools are:

- Malwarebytes
- Bitdefender
- Kaspersky

Avast