QUALYSEC
BEYOND CYBERSECURITY

2023
MARCH 5TH WEEK

CYBER SECURITY NEWS

CONTACT US

🌐 www.qualysec.com
☎ 865 866 3664
✉ contact@qualysec.com

AlienFox – A Hacking Toolkit That Steals Credential From Multiple Cloud Services

A recently discovered comprehensive toolset dubbed AlienFox toolkit is circulating on Telegram.

It’s a modular set of tools that enables malicious actors to scan for poorly configured servers, potentially leading to the theft of cloud-based email service credentials and authentication secrets.

SentinelOne security researcher Alex Delamotte stated:-

“A new trend in cyberattacks involves exploiting less complex cloud services that are unsuitable for cryptocurrency mining. The spread of AlienFox is an example of this trend, as it allows attackers to expand their operations and launch further campaigns. This development has gone largely unreported in the cybersecurity community.”

Cybercriminals can access a private Telegram channel via which the toolkit is sold to them, which has become the usual method for network hackers and malware authors to engage in transactions.

AlienFox steals credentials & secrets

There are a number of custom tools in AlienFox that were developed by different authors and utilize a variety of modified open-source utilities.

Source : https://cybersecuritynews.com/alienfox-a-hacking-toolkit/

BingBang – A New Bing Vulnerability that Can be Exploited Without Executing a code

Azure Active Directory (AAD) has a new attack vector that affected Microsoft's Bing.com, according to Wiz Research. A widespread AAD misconfiguration is the attack vector, making misconfigured apps vulnerable to intrusion.

Microsoft's AAD, a cloud-based identity and access management (IAM) service, is the standard authentication method for Azure App Services and Azure Functions applications.

"The researchers found several Microsoft applications vulnerable to this attack, one of which was a Content Management System (CMS) that powers Bing.com," says Wiz researchers

"This allowed them to take over Bing.com functionality, modify search results, and potentially enable the Office 365 credential theft of millions of Bing users. These credentials in turn granted access to users' private emails and documents".

Any user from any Azure tenant may log in to a multi-tenant app. The developer must verify the user's original tenant in a multi-tenant app and give access appropriately. Anyone with an Azure account from anywhere worldwide could access the app if they fail to validate this information properly.

Source : https://cybersecuritynews.com/bingbang-flaw/

New Malware Dubbed Mélofée Attacking Linux Servers

ExaTrack found a new undetected implant family called Mélofée that targets Linux systems. Three samples of the previously known malicious software, dating from the beginning of 2022, were found by analysts.

Chinese state-sponsored APT groups, including the notorious Winnti group, are related to the malware.

Capabilities of Mélofée

Researchers analyzed this malware family's capabilities, including a kernel-mode rootkit, and then went deep through an infrastructure pivot maze to find similar adversary toolkits.

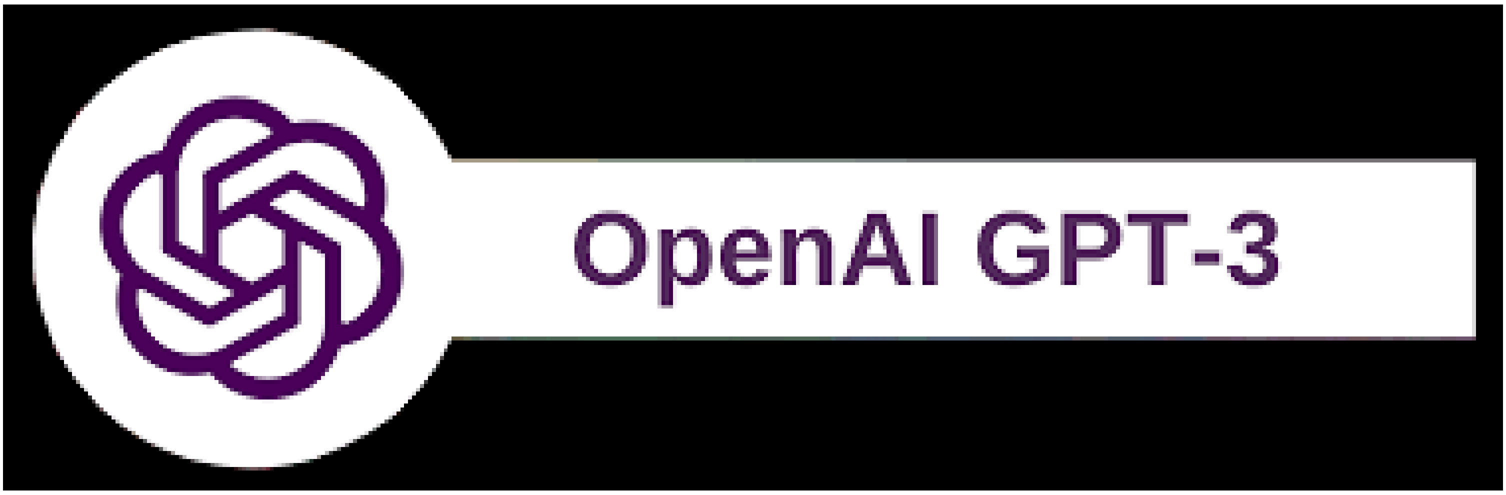
One of the artefacts is to drop a kernel-mode rootkit based on the Reptile, open source project.

"According to the vermagic metadata, it is compiled for a kernel version 5.10.112-108.499.amzn2.x86_64. The rootkit has a limited set of features, mainly installing a hook designed for hiding itself", researchers.

Also, the implant and rootkit were installed using shell commands that downloaded the installer and a custom binary package from an adversary-controlled server.

Source :https://cybersecuritynews.com/malware-attacking-linux-servers/

CYBER SECURITY NEWS



Hackers Exploiting ChatGPT’s Popularity to Spread Malware via Hacked FB Accounts

Researchers recently investigated and uncovered alarming information regarding 13 Facebook pages and accounts.

The threat actors have compromised these pages and profiles, and the most shocking thing about these pages and accounts, they have more than 500k active followers.

The threat actors exploited these compromised pages/accounts with the help of ChatGPT to spread malware using Facebook ads, putting the safety and security of the followers at risk.

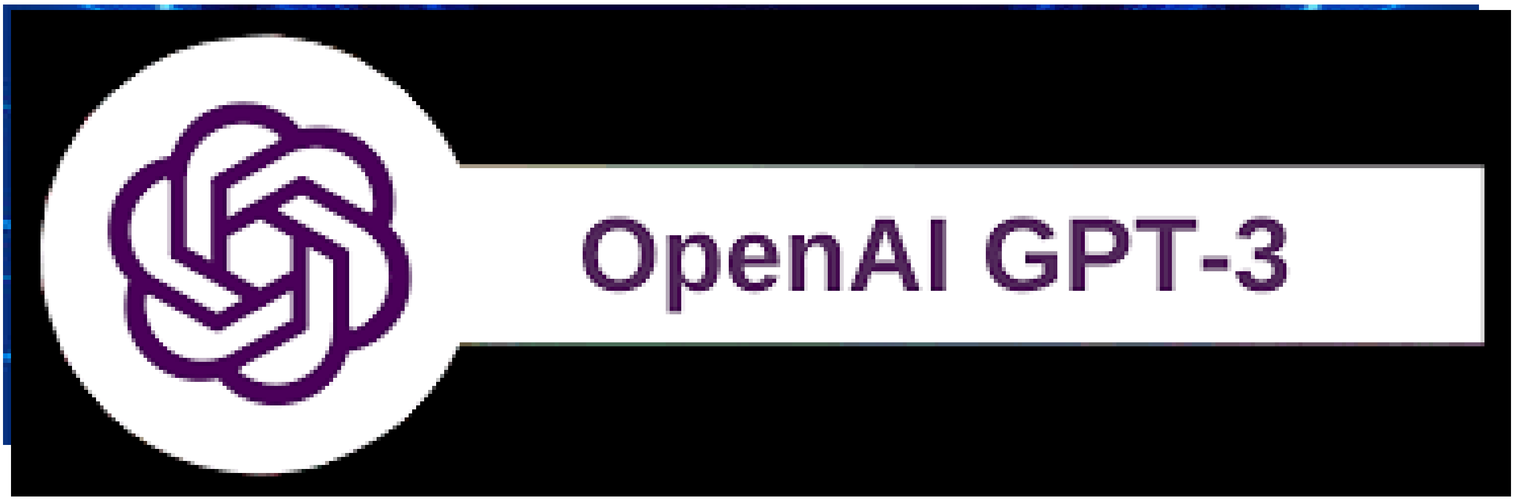
Threat actors use various channels to distribute malware from these compromised accounts and pages. And here below we have mentioned those channels or mediums:-

- Trello boards
- Google Drive
- Several individual websites

A password and the download link are included to lend credibility to the scam. It should also be noted that compromised accounts are also capable of stealing sensitive confidential information as well.

Source : https://cybersecuritynews.com/hackers-exploiting-chatgpts-popularity-to-spread-malware/

CYBER SECURITY NEWS



Europol Warns That Hackers Use ChatGPT to Conduct Cyber Attacks

Europol Innovation Lab recently conducted workshops with experts from Europol to investigate the potential for criminal abuse of language models like ChatGPT and their usefulness for investigators.

In the Europol Innovation Lab, innovative solutions are developed for improving the way that law enforcement investigates, tracks, and disrupts terrorists and criminal organizations by making use of emerging technologies.

It is no secret that ChatGPT has been a big success for investors and users alike. Due to this, the platform is also becoming a target for cybercriminals looking for easy money.

There has been a revolution in NLP due to the advent of large language models, which allow computers to generate human-like text with increasing precision.

The workshops aim to increase awareness of the potential abuse of LLMs, foster dialogue with AI companies to enhance safeguards, and encourage the creation of secure and reliable AI systems.

Source : https://cybersecuritynews.com/hackers-use-chatgpt-to-conduct-cyber-attacks/

CYBER SECURITY NEWS

MacStealer – New macOS-Based Malware Steals Passwords, Cookies & Credit Cards From Browser

Uptycs threat research team recently discovered “MacStealer,” a new information-stealing malware designed to target Apple’s macOS operating system. It aims to steal various sensitive information, including credentials stored in the:-

- iCloud KeyChain
- Web browsers
- Cryptocurrency wallets
- Potentially sensitive files

MacStealer is a malware-as-a-service (MaaS) distributed for $100, including premade builds enabling purchasers to spread the malware via Telegram as a command-and-control (C2) platform, making it a significant threat for exfiltrating data.

Specifically, this bug affects macOS versions Catalina and later runs on CPUs with M1 and M2 cores, which are the latest lineups from Apple.

Source : https://cybersecuritynews.com/macos-based-malware/

Linux Kernel Vulnerabilities in Ubuntu Let Hackers Launch DOS Attack & Execute Arbitrary Code

Several security vulnerabilities were recently addressed by Canonical in both Graphviz and the Linux kernel of Ubuntu.

Recent discoveries include null pointer dereference vulnerabilities in Graphviz and improper handling of indirect branch prediction isolation between L1 and L2 VMs in the KVM VMX implementation of the Linux kernel.

Linux Kernel Flaws

According to the ubuntu report, There is a risk of exposure of sensitive data from the host OS or other guest VMs if indirect branch prediction isolation is improperly handled between L1 and L2 virtual machines.

It has recently been discovered that the Xen network backend driver in the Linux kernel, in certain circumstances, exhibited a race condition when dealing with dropped packets and could not handle them properly.

Using this vulnerability, a hacker could cause a kernel deadlock, execute arbitrary code and cause a system crash by exploiting it.

The Linux kernel’s implementation of the USB Gadget file system contains a race condition that can lead to use-after-free vulnerabilities in some circumstances, and Gerald Lee discovered this vulnerability.

Source : https://cybersecuritynews.com/linux-kernel-vulnerabilities/

Explosive USB Drive Bomb that Gets Detonated when Plugged into Computer

Journalists across Ecuador were targeted using a novel bomb resembling a USB drive. Once inserted into a computer, these devices detonate.

According to a report from CBS News, over five Ecuadorian journalists, they received a USB letter bomb from Quinsaloma.

The letters represented “a new escalation in violence against the press, said Fundamedios NGO, and called for “immediate intervention of the State.”

Envelopes with USB sticks were addressed to Lenin Artieda, an Ecuavisa private TV station journalist.

Juan Zapata, the interior minister, stated that all the devices were dispatched from a single town. Among them, three were sent to media outlets in Guayaquil, and the remaining two were directed toward the capital city, Quito.

On Monday, Interior Minister Juan Zapata reported that several letter bombs were dispatched to at least five journalists employed at radio and television stations in Ecuador. This country has been severely affected by violence. Regrettably, one of the bombs detonated; however, it did not result in significant injuries.

Source : https://cybersecuritynews.com/explosive-usb-drive/

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT

☎ +91 865 866 3664 www.qualysec.com ✉ contact@qualysec.com