QUALYSEC
BEYOND CYBERSECURITY

2024

MAR 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

Hijacked PyPI Package Installs NovaSentinel Stealer on Windows

A recent investigation has uncovered a flaw in internet-connected doorbell cameras, specifically affecting Ivanti's Pulse Secure appliances.

The NVISO Incident Response team discovered the discovery, which identified two covert TLS-based backdoors, SparkCockpit and SparkTar, allowing attackers to hijack these devices and gain unauthorized access to internal networks.

The investigation was triggered by a critical-sector organization that observed a compromise of their Ivanti appliance, leading to the discovery of these sophisticated backdoors.

Sophisticated Attack Techniques

Both SparkCockpit and SparkTar employ selective interception of TLS communication towards legitimate Ivanti server applications, which helps them avoid detection.

SparkTar is particularly advanced and capable of surviving factory resets and appliance upgrades.

It also allows for file uploads, command execution, and setting up SOCKS proxies to relay attacker traffic directly into the organization's network.

Source : https://cybersecuritynews.com/sparkcockpit-sparktar-malware/

Hacker Group Publicly Announced That They Are Recruiting Pentesters

Hacker groups recruit pentesters because they possess valuable skills in identifying and exploiting vulnerabilities. This aligns with the offensive capabilities that are needed for cyber attacks.

Besides this, Pentesters' expertise in finding security flaws helps enhance the group's ability to compromise systems and networks for malicious purposes.

Daily Dark Web recently discovered and reported that a hacker group, 62IX, officially announced they are actively recruiting pentesters and DDoSers.

Hackers Recruiting Pentesters

It is assumed that the 62IX hacker group is a pro-Russian hacker group. This group has been suspected of attacking several key targets through cyber networks, such as telecommunications firms in Australia and Hong Kong.

The belief is that they have deployed quite a few strategies consisting of malware and social engineering tricks to be able to infiltrate sensitive systems.

Moreover, it has also been claimed that 62IX hacker groups indulged in spying activities on America.

Source : https://cybersecuritynews.com/hacker-recruitment-pentesters/

Elon Musk Sues OpenAI For Breach of Contract

Elon Musk has initiated a lawsuit against OpenAI, the artificial intelligence research lab he co-founded, alleging a breach of the foundational agreement that aimed to ensure the development of artificial general intelligence (AGI) for the benefit of humanity rather than corporate profit.

The lawsuit, filed in the Superior Court of California in San Francisco, names OpenAI, Inc., along with its various affiliated entities and co-founders Samuel Altman and Gregory Brockman, as defendants.

Musk's complaint outlines a series of grievances centered around the deviation of OpenAI from its original mission.

According to the lawsuit, Musk, Altman, and Brockman established OpenAI in 2015 with a clear vision: to develop AGI as a non-profit entity, focusing on open-source projects that would serve humanity's interests rather than those of private, for-profit corporations.

This vision was encapsulated in what Musk refers to as the "Founding Agreement," a commitment that was allegedly reaffirmed on multiple occasions through OpenAI, Inc.'s Certificate of Incorporation and various communications between the parties involved. The lawsuit details Musk's significant contributions to OpenAI, including tens of millions of dollars in funding, strategic advice on research directions, and efforts in recruiting top talent to the organization. These contributions were made with the understanding that OpenAI would remain committed to its founding principles of openness and public benefit.

Source : https://cybersecuritynews.com/elon-musk-lawsuit-openai-breach/

Microsoft Announces Auto-rollout Conditional Access Policies in Entra ID(Azure)

Microsoft has unveiled the automatic rollout of multifactor authentication (MFA)-related Conditional Access policies in Entra ID, marking a pivotal step in the company's Secure Future Initiative.

This initiative aims to enhance customer security measures in anticipation of escalating cyber threats.

The announcement, made during Microsoft Ignite in November 2023, has since seen the implementation of report-only policies for over 500,000 tenants, demonstrating Microsoft's commitment to advancing security protocols for its users.

Elevating Security with Multifactor Authentication

These newly introduced policies focus on multifactor authentication (MFA), a critical security measure designed to protect against unauthorized access.

MFA requires users to provide two or more verification factors to access resources, significantly reducing the risk of compromise.

Microsoft's approach targets various user groups, including administrators of Microsoft admin portals and users enabled for per-user MFA across Entra ID P1 and P2 tenants.

Source : https://cybersecuritynews.com/auto-rollout-of-conditional-access-policies//

Phemedrone Stealer Exploits Windows SmartScreen Flaw to Steal Sensitive Data

The cybersecurity community has recently identified a new threat known as Phemedrone Stealer, a sophisticated malware that exploits a vulnerability in Microsoft Windows Defender SmartScreen, CVE-2023-36025.

This malware has been designed to steal sensitive data, including credentials from multiple platforms and cryptocurrency wallet information.

Sophisticated Data Theft Tactics

Phemedrone Stealer is a . NET-compiled Trojan Stealer that employs advanced tactics to evade detection and harvest data from infected systems.

It uses a mutex checker to prevent multiple instances. It applies methods to avoid analysis by terminating processes if it detects a virtual machine environment or specific languages associated with the Commonwealth of Independent States (CIS).Targeting Cryptocurrency Wallets

One of the most alarming capabilities of Phemedrone Stealer is its focus on cryptocurrency wallets. It targets wallets such as Armory, Atomic, Bytecoin, Coinomi, Jaxx, Electrum, Exodus, and Guarda, attempting to extract sensitive data from specific directories that store transaction records, account information, and cryptographic keys.

Source : https://cybersecuritynews.com/stealer-exploits-windows/

Juice jacking : Hijacking mobile phones using public charging ports

Reserve Bank of India (RBI) has warned against the dangers of “juice jacking,” a cyberattack targeting mobile users who charge their devices at public USB ports.

This advisory underscores the growing threat cybercriminals pose in public spaces such as airports, hotels, and shopping centers, where unsuspecting users might plug in their devices for a quick charge, only to fall victim to data theft or malware infection.

Understanding Juice Jacking

Juice jacking is a sophisticated form of cyberattack where hackers tamper with public USB charging stations to install malware or conduct hardware modifications that enable them to access data on connected devices.

The term, coined by cybersecurity expert Brian Krebs in 2011, highlights the vulnerability of mobile devices when charged using public USB ports.

According to the Hindu business line, The Reserve Bank of India (RBI) has released a cautionary advisory for mobile phone users, alerting them to the potential security risks associated with public charging ports.

Source : https://cybersecuritynews.com/juice-jacking-hijacking-mobile/

New Bifrost Malware Attacking Linux Servers Evades Security Systems

A new Linux variant of Bifrost, dubbed Bifrose, was observed exhibiting a creative way to avoid detection, such as using a deceptive domain that imitates the official VMware domain.

Bifrost is a remote access Trojan (RAT) that was first discovered in 2004. It is usually distributed by attackers using phishing websites or email attachments.

After being installed on the victim's computer, Bifrost allows the attacker access to confidential information such as the victim's IP address and hostname.

Bifrost's most recent version attempts to bypass security measures and infiltrate target systems.

The cybersecurity industry is concerned about the recent spike in Linux variants of Bifrost, which may indicate an increase in attacks against Linux-based systems.Novel User-Deception Method Used By Bifrost

"The latest version of Bifrost reaches out to a command and control (C2) domain with a deceptive name, download.vmfare[.]com, which appears similar to a legitimate VMware domain.

This is a practice known as typosquatting", Palo Alto Networks shared with Cyber Security News. Researchers have identified the most recent Bifrost sample on a server.

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

GTPDOOR Linux Malware Exploiting GPRS Protocol For Stealthy C2 Communication

Threat actors exploit Linux malware due to the widespread use of Linux servers in critical infrastructure and web hosting.

Linux's prevalence makes it an attractive target for cybercriminals seeking to compromise systems, steal data, or launch distributed denial-of-service (DDoS) attacks.

Cybersecurity researcher specialist in mobile security and IoT security research, HaxRob(@haxrob) recently discovered GTPDOOR, a Linux malware that was found exploiting GPRS protocol for stealthy C2 communication.

GTPDOOR Linux Malware Exploiting GPRS Protocol

GTPDOOR targets telco networks near GRX, and it communicates C2 traffic via GTP-C signaling by blending it with normal traffic.

The below diagram depicts a potential use case where actors exploit established persistence to access compromised hosts through GTP-C Echo Request messages:-GTPDOOR supports remote code execution and can be beaconed by sending TCP packets to its host.

The beacon response hides specific information in a TCP header flag by enhancing its stealth.

Source : https://cybersecuritynews.com/gtpdoor-linux-malware-gprs-c2communication/

Lazarus Hackers Exploited Windows kernel 0-day In The Wild

The Lazarus threat group has been exploiting a Microsoft vulnerability associated with Windows Kernel Privilege Escalation to establish a kernel-level read/write primitive.

This vulnerability was previously unknown which exists in the appid.sys AppLocker driver.

This vulnerability has been assigned with CVE-2024-21338 and has been addressed by Microsoft on their February patch.

Once established, threat actors could perform direct kernel object manipulation in their new version of the FudModule rootkit. There has been a major advancement in the rootkit, which handles table entry manipulation techniques.

Lazarus Hackers Exploited Windows 0-day

According to the Avast report, the threat actors were previously using BYOVD (Bring Your Own Vulnerable Driver) techniques for establishing the admin-to-kernel primitive, which is a noisy method.

But it seems like this new zero-day exploitation has paved a new way for establishing kernel-level read/write primitives. Investigating further, it was discovered that this issue is technically due to a thin line on Windows Security that Microsoft has left for a long time.

Source : https://cybersecuritynews.com/lazarus-windows-kernel-exploit/

Millions Of GitHub Repos Found Infected With Malicious Code

A recent report by security firm Apiiro has revealed that a “repo confusion” attack has compromised more than 100,000 repositories on GitHub.

This type of attack involves exploiting a flaw in the way that Git, the version control system used by GitHub, handles repository names and can lead to malicious code being injected into legitimate repositories.

This highlights the need for improved security measures to prevent such attacks and protect the integrity of code stored on GitHub.

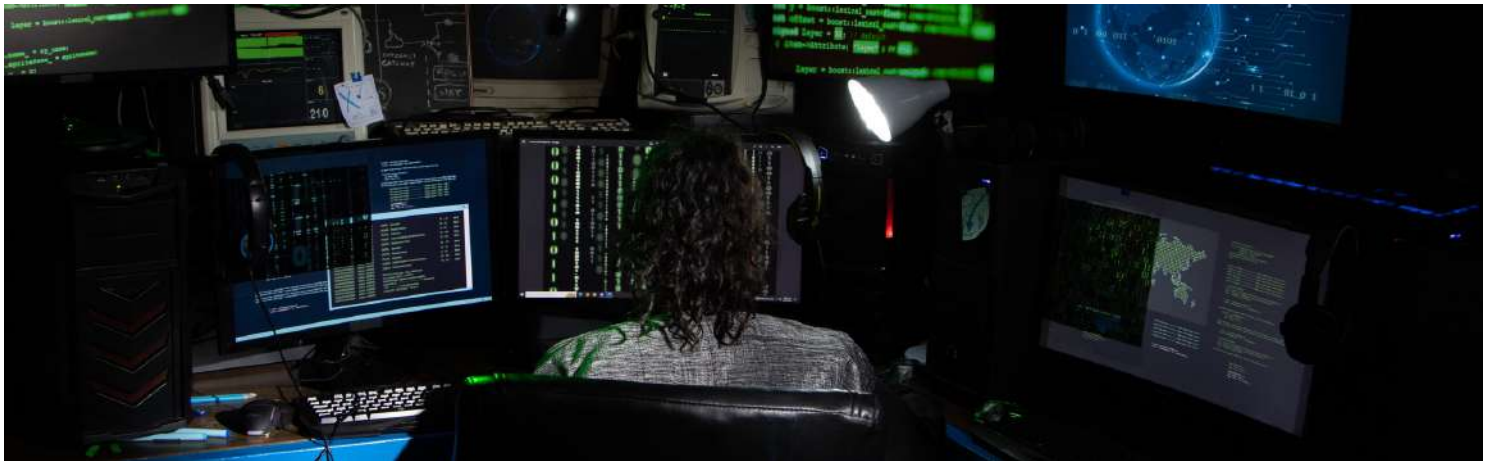
This attack technique exploits the expansive scale and unguarded accessibility of the GitHub platform to launch attacks on unprepared developers.

How Does It Work?

1. Cloning Popular Repos: Attackers target popular repositories like TwitterFollowBot, WhatsappBOT, etc., and create copies of them.

Injecting Malware: These copies are infected with malware designed to steal login credentials, browser data, and other sensitive information.

Source : https://cybersecuritynews.com/github-repos-malware-attack/



Internet-connected Doorbell Cameras Flaw Let Attackers Hijack Devices

The severe security flaws in popular video doorbell cameras could allow attackers to hijack these devices.

The investigation revealed that doorbells sold under various brand names but manufactured by the same company, Eken Group Ltd., are vulnerable to hacking, posing a significant risk to consumer privacy and safety.

You can analyze a malware file, network, module, and registry activity with the ANY.RUN malware sandbox and the Threat Intelligence Lookup that will let you interact with the OS directly from the browser.

A Shocking Discovery

The security flaws were discovered by Consumer Reports' privacy and security test engineers, Steve Blair and David Della Rocca.

They managed to hack into doorbell cameras from thousands of miles away, capturing images of the journalist's backyard and deck. These devices, meant to monitor strangers at the door, ironically allowed the engineers to spy on the homes of the people they were supposed to protect.

Source : https://cybersecuritynews.com/internet-connected-doorbell-cameras-flaw/

HackerGPT 2.0 – A ChatGPT-Powered AI Tool for Ethical Hackers & Cyber Community

HackerGPT is an advanced AI tool created specifically for the cybersecurity industry, handy for individuals engaged in ethical hacking and cyber security research like bug bounty hunters.

This sophisticated assistant is at the forefront of cyber intelligence, providing an extensive collection of hacking methods, tools, and tactics. HackerGPT is not just a place for storing information; it actively assists users in navigating the intricacies of cybersecurity.

Various tools powered by ChatGPT, like OSINVGPT, PentestGPT, WormGPT, and BurpGPT, have already been created for the cyber security community, and HackerGPT is now adding to this legacy.

The Goal of HackerGPT 2.0:

This tool utilizes ChatGPT's advanced features and specialized training data to support a range of cybersecurity activities such as network and mobile hacking. It also helps comprehend various hacking techniques without the need for unethical methods like jailbreaking. HackerGPT provides prompt responses to user inquiries while following ethical standards. It offers support for GPT-3 and GPT-4 models, giving users access to various hacking techniques and methodologies.

Source :https://cybersecuritynews.com/hackergpt-2-0/

“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