QUALYSEC
BEYOND CYBERSECURITY

2023
MARCH 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

New Android Banking Malware Attacking Over 400 Financial Apps

Several threat actors have already been exploiting a newly discovered Android banking trojan, dubbed Nexus, to penetrate 450 financial applications and steal data.

While this malware was identified by cybersecurity analysts at Italian cybersecurity firm, Cleafy, they affirmed that it is still in its early development stages.

However, ATO attacks against banking portals and cryptocurrency service providers can be conducted using this malware as it is equipped with all the main features.

Cleafy discovered the presence of the new Android banking Trojan known as “Nexus” in June 2022. Although Cleafy first thought Nexus was a highly dynamic variation of the previously tracked Trojan known as “Sova,” additional analysis revealed that Nexus has unique traits and capabilities.

At the time of detection, the malware was discovered to have merged numerous portions of Sova code. Not only that even it also displayed a broad variety of capabilities that allowed it to attack over 200 mobile banking, cryptocurrency, and other financial apps

Source : https://cybersecuritynews.com/new-android-banking-malware-2/

Windows 11, Tesla, macOS & Ubuntu Desktop Hacked – Pwn2Own Day One

On the first day, Pwn2Own Vancouver 2023 hacking challenge participants compromised Windows 11, Tesla, macOS, and Ubuntu Desktop.

AbdulAziz Hariri of Haboob SA, who completed his attack against Adobe Reader utilizing a 6-bug logic chain leveraging many failed fixes that escaped the sandbox and overcame a banned API list, gave the first demonstration of the day. 5 Master of Pwn points and $50,000 are awarded to him.
Microsoft SharePoint was the target of a 2-bug chain that STAR Labs was able to run. They receive 10 Master of Pwn points and $100,000.

Oracle VirtualBox was exploited by Bien Pham (@bienpnn) of Qrious Security (@qriousec) via an OOB Read and a stacked-based buffer overflow. 4 Master of Pwn points and $40,000 are awarded to him.

Tesla – Gateway was the target of a TOCTOU attack by Synacktiv (@Synacktiv). They receive a Tesla Model 3 and $100,000, and 10 Master of Pwn points.

Although the exploit was already known, STAR Labs (@starlabs sg) was successful in its attack against Ubuntu Desktop. They still receive $15,000 in addition to 1.5 Master of Pwn points.

Source : https://cybersecuritynews.com/pwn2own-day-one/

Microsoft Teams, Virtualbox, Tesla Zero-Days Exploited – Pwn2Own Day Two

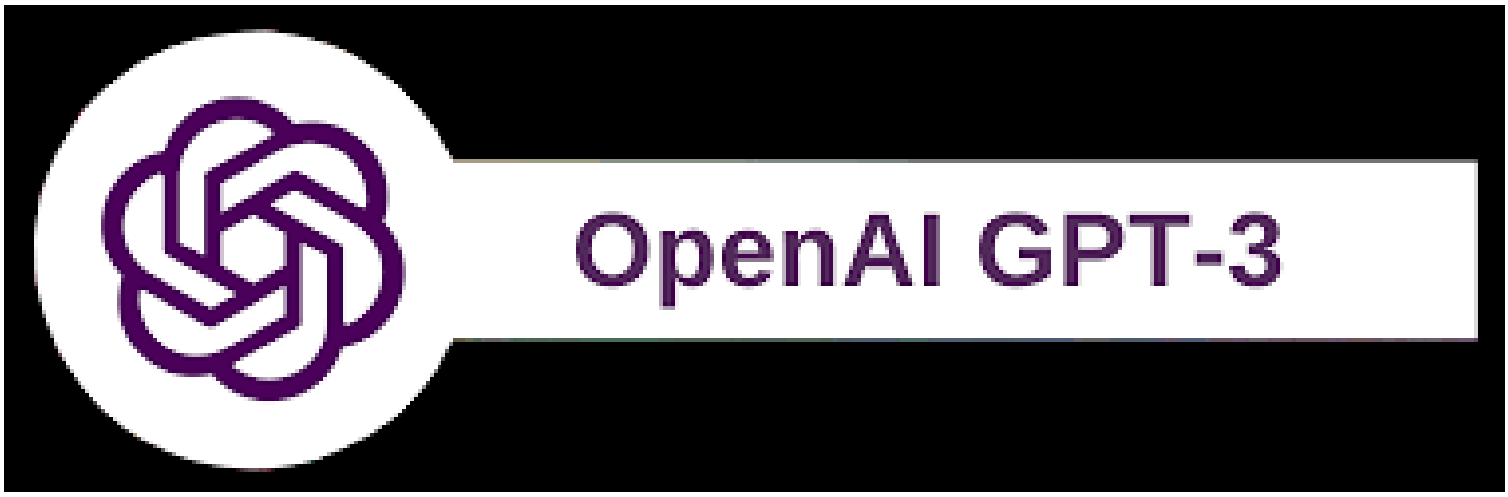
At Pwn2Own Vancouver 2023 Day 2, for 10 unique zero-day exploits, the participants received $475,000 of cash prizes.

The Tesla Model 3, the Microsoft Teams communication platform, the Oracle VirtualBox virtualization platform, and the Ubuntu Desktop operating system were all on the list of targets that were hacked.

Thomas Imbert made the first demonstration (@masthoon), and Thomas Bouzerar (@MajorTomSec) of Synacktiv (@Synacktiv), showed a three-bug chain against Oracle VirtualBox, with a host EoP. There was already one bug in existence. In addition, they receive 8 Master of Pwn points and $80,000.

Microsoft Teams was also hacked by Team Viettel (@vcslab) using a 2-bug chain, earning them $75,000 and 8 Master of Pwn points.
Tesla – Infotainment David Berard exploited unconfined Root (@ p0ly_) and Vincent Dehors (@vdehors) of Synacktiv (@Synacktiv) via a heap overflow and an OOB write. After collecting $250,000 and 25 Master of Pwn points, they are eligible for a Tier 2 reward.

Source : https://cybersecuritynews.com/pwn2own-vancouver-2023/



ChatGPT Privacy Bug Exposes Chat Histories to Other Users

A severe flaw recently affecting ChatGPT, an artificial intelligence chatbot developed by OpenAI, exposed chat history and consequently caused an outage.

After observing Chinese characters in the title of their conversation history, a ChatGPT user on Reddit first reported the error.
As some users could view the history of other users' conversations, this flaw has raised questions about users' privacy.
The problem is an important warning to be cautious while sharing sensitive information with ChatGPT. The company cannot remove specific prompts from a user's history, and talks may be utilized for training, according to a FAQ on OpenAI's website, which asks users to refrain from sharing sensitive information in their conversations.

ChatGPT Bug Revealed Conversation History of Individuals
The flaw turned out to be the cause of the sidebar's display of Chinese language, despite the fact that the problem was initially reported on Reddit by a user who believed their account had been hacked.

Source : https://cybersecuritynews.com/chatgpt-privacy-bug/

Hackers Attack Administrative Organizations Using PowerMagic and CommonMagic Malware

Significant numbers of cyberattacks are executed in a political or geopolitical context that Kaspersky researchers and the international community are identifying.

In recent weeks, reports have surfaced of attacks carried out by an advanced threat actor using a previously unknown malicious framework, CommonMagic, and a new backdoor, PowerMagic.

At least one malware piece has been used as part of operations since September 2021, which is believed to be the case.

As a result, this type of malware continues to be developed, and it continues to target organizations in the administrative, agricultural, and transportation sectors for the purpose of espionage.

The hackers could make it impossible at this point to connect with other campaigns by combining unsophisticated techniques used by multiple actors with original malicious code that had never been seen before.

While the CommonMagic appears to have been active since 2021, the adversary intensified its efforts last year and continues to be active today.

Source : https://cybersecuritynews.com/hackers-attack-administrative-organizations/

Hackers Attack .NET Developers Using Malicious NuGet Repository Packages

There is a concerning trend among cybercriminals targeting individuals working with the .NET framework using a sneaky tactic called typosquatting.

This involves creating fake packages that mimic the names of legitimate software and distributing them through the popular NuGet repository.
Cybersecurity researchers Natan Nehorai and Brian Moussalli from JFrog have detected this ongoing campaign involving malicious software distribution through fraudulent packages.

In just one month, three of these packages have been downloaded more than 150,000 times. The extensive downloads of malicious NuGet packages could indicate many compromised systems among .NET developers.
However, it is also possible that the cybercriminals behind this attack deliberately sought to legitimize their fake packages by artificially inflating download numbers.

Source : https://cybersecuritynews.com/hackers-attack-net-developers/

Ferrari Hacked – Attackers Stolen Payment Data & Demand For Ransom

Recently, the renowned manufacturer of sports cars Company “Ferrari” from Italy reported that a ransomware attack targeted their IT systems and accessed or stole sensitive data.

The company stated that customer contact information might have been compromised and that the attackers demanded a ransom for not disclosing the data.

Ferrari Took Swift Action.

As soon as Ferrari received the ransom demand, the company took swift action by initiating an investigation in partnership with a renowned third-party cybersecurity firm on a global scale.

“Upon receipt of the ransom demand, we immediately started an investigation in collaboration with a leading global third-party cybersecurity firm.” Company said.

Apart from this, the appropriate authorities have already been notified of the ransomware attack and the demanded ransom. It has been mentioned that the company is confident that the authorities will be able to investigate the incident thoroughly and enforce the law severely in this case.

Ferrari has not disclosed the exact date of the ransomware attack incident. However, it is believed to be linked to reports of an attack in October 2022.

Source : https://cybersecuritynews.com/ferrari-hacked/

Meta Manager Was Hacked By Surveillance-For-Hire Software for Around One Year

A U.S. and Greek national, Artemis Seaford, who worked for Meta's trust and safety team while headquartered in Greece, was subjected to a year-long wiretap by the Greek national intelligence service and compromised using a strong cyber espionage tool.

It shows that the illegal use of spyware is expanding beyond authoritarian governments' use against journalists and opposition figures. It has started infiltrating European democracies, even ensnaring a foreign national working for a significant international firm.

A Dual U.S.-Greek National Was Targeted With a Cyberespionage Tool

Although the exact cause of her compromise is unknown, it is clear that her phone had been infected with the "Predator" spyware; she might be the first American to have had such technology used to spy on her in Europe, says the report.

Documents reveal that after scheduling a Covid vaccination appointment, the state immediately sent her a confirmation SMS. Five hours later, however, she received another SMS requesting her to confirm the appointment by clicking on a link. Predator was downloaded onto her phone via this malicious link.

Source : https://cybersecuritynews.com/meta-manager-was-hacked/

Bitcoin ATMs Hacked – Attackers Exploiting a 0-Day Vulnerability in Its Platform

General Bytes, a Prague-based company, announced on 18 March that it had received a hacker warning saying it had remotely uploaded a Java application to its management platform to steal user information and funds in a hot wallet.

It is believed that the attacker could identify several CAS services running on port 7741 by scanning the IP address space of Digital Ocean, including the General Bytes Cloud service and other providers of GB ATM services.

The company's website indicates that the company has sold over 15,000 Bitcoin ATMs around the globe to customers in close to 150 countries.

What Happened?

A customer can deploy a General Bytes ATM using a standalone management server or by using a cloud-based service that General Bytes offers.

Using code execution, the attackers could access the database and API keys of hot wallets and exchanges to gain access to funds.

This allowed the attackers to steal usernames and password hashes and disable two-factor authentication in the accounts, allowing them to transfer the funds from hot wallets.

Source : https://cybersecuritynews.com/bitcoin-atms-hacked/

“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