QUALYSEC
BEYOND CYBERSECURITY

2023

APRIL 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

38 Minecraft Copycat Games on Google Play Infect over 140 Million Users Monthly

Recently, a group of threat actors have disguised their malware as 38 Minecraft-inspired games on Google Play, infecting unsuspecting devices with the insidious 'HiddenAds' adware.

While players get lost in the blocky world of Minecraft clones, the adware stealthily runs in the background, generating revenue for the malicious operators.

McAfee's Mobile Research Team, part of the App Defense Alliance, uncovered the adware set to safeguard Google Play from potential threats.

Distribution

With a staggering 140 million active players every month, Minecraft's popularity as a sandbox game has prompted various game publishers to try and replicate its success.

Approximately 35 million Android users worldwide fell victim to the adware hidden in Minecraft-like games, with the majority of downloads originating from the following countries:-

- The United States
- Canada
- South Korea
- Brazil

Source : https://cybersecuritynews.com/38-minecraft-copycat-games/

RTM Locker Ransomware Attacks Linux, NAS, and ESXi Servers

The RTM Locker ransomware gang has been discovered to utilize a Linux encryptor that focuses explicitly on virtual machines on VMware ESXi servers, making it the most recent instance of an enterprise-oriented ransomware attack.

Uptycs' Threat Intelligence unit uncovered the RTM Locker threat faction while conducting dark web reconnaissance.

Since 2015, the RTM cybercrime group has been involved in financial fraud, using a custom-made banking trojan to steal money from their targets.

Trellix cybersecurity firm and Uptycs recently revealed that RTM Locker initiated a new Ransomware-as-a-Service (RaaS) venture, actively hiring affiliates, including ex-Conti cybercriminals.

Technical Analysis

RTM Locker and Babuk ransomware share commonalities, such as ECDH Curve25519 for asymmetric encryption and random number generation.

However, Babuk uses sosemanuk, while RTM Locker uses ChaCha20 for asymmetric encryption, which differentiates the two.

Upon initial inspection of the ransomware binary, it became apparent that the program was tailored towards ESXi due to two ESXi commands at the beginning of the code.

The binary is statically compiled and stripped, which allows it to run on various systems and makes reverse engineering a challenging task.

Source : https://cybersecuritynews.com/rtm-locker-ransomware/

Google Dismantles CryptBot Info-stealing Malware Infrastructure That Hacked 670,000 Computers

Google uses Cryptbot info stealer for infecting Chrome users and stealing data, taking down associated malware infrastructure.

The sole goal of this lawsuit is to reduce the victims' data theft by disrupting the complete infrastructure and distribution network of the CryptBot info-stealing malware.

In 2022, it was reported that CryptBot, which is a Windows malware, infected more than 670,000 computers to steal the following sensitive data from Chrome users:-

- Authentication credentials
- Social media account logins
- Cryptocurrency wallets

Legal Strategy & Disruption

It is believed that the operators and distributors of CryptBot info-stealer are Pakistan-based and run globally. On several types of claims, the legal complaint is based, and the claims are like:-

- Computer fraud
- Computer abuse
- Trademark infringement

Source : https://cybersecuritynews.com/google-dismantles-cryptbot-info-stealing-malware-infrastructure-that-hacked-670000-computers/

Thousands of Apache Superset Servers Open to RCE Attacks

Cybersecurity analysts at Horizon3 detected that thousands of Apache Superset servers are exposed to RCE attacks at default configurations.

This could allow the threat actors to perform the following illicit activities:-

- Access data
- Modify data
- Harvest credentials
- Execute commands

Apache Superset is an open-source tool that is used for:-

- Data visualization
- Data exploration

Initially, this tool was developed for Airbnb, but in 2021, it became a top-level project at the Apache Software Foundation.

Technical Analysis

Attackers could take advantage of the default Flask Secret Key utilized by Apache Superset for signing authentication session cookies to create fake session cookies.

Consequently, servers that haven't altered the key may be susceptible to unauthorized access with elevated privileges.

Source : https://cybersecuritynews.com/thousands-of-apache-superset-servers-open-to-rce-attacks/

Ukrainian Arrested for Selling Sensitive Data of Over 300 Million Users to Russia

The Ukranian Cyber police officers tracked down the 36-year-old resident of Netishyn as he was selling the personal data of more than 300 million victims from different countries.

The data includes

- Passports
- Birth certificates
- Driver's license
- Bank account data
- Taxpayer numbers etc.,

Furthermore, the suspect was an administrator of a closed telegram channel that he used to sell these personal data. The price of this data varies from $500 to $2000. As per reports, this data belonged to the citizens of Ukraine and the European Union.

It was also reported that the suspect received payments for data sales in currencies prohibited from usage inside Ukraine.

Ukrainian Law Enforcement Officers searched the suspect's home and found Mobile phones, 3 dozen hard drives, SIM cards, and computer and server equipment seized immediately. However, the origin of these data is still unknown and is being investigated.

Source : https://cybersecuritynews.com/ukrainian-arrested/

SLP Protocol Vulnerability Lets Attackers Launch Powerful 2,200x DDoS Attack

The Service Location Protocol (SLP) has been found to have a new reflective Denial-of-Service (DoS) amplification vulnerability.

Threat actors can exploit this vulnerability to execute extensive DDoS attacks with a staggering amplification of 2,200X.

Researchers at BitSight and Curesec have tracked the vulnerability as “CVE-2023-29552,” which has exposed around 54,000 exploitable instances of the SLP used by over 2,000 organizations.

Threat actors can leverage these instances for conducting DDoS amplification attacks. Organizations worldwide have unknowingly deployed vulnerable devices, and here they are mentioned below:-

- Konica Minolta printers
- VMWare ESXi Hypervisors
- Planex Routers
- IBM Integrated Management Modules

Technical Analysis

SLP mainly facilitates the communication and connection between devices on LAN, an old internet protocol introduced in 1997.

While it does so through a service availability system that operates on port 427 using UDP and TCP, organizations have exposed SLP on tens of thousands of devices never designed to be exposed on the public internet over the years.

Source :https://cybersecuritynews.com/slp-protocol-vulnerability-launch-ddos/

RustBucket – A macOS Malware Attack Mac Users Via PDF Viewer App

Cybersecurity analysts at Jamf Threat Labs have recently uncovered a macOS malware family. The new malware family has been tracked as "RustBucket," which downloads and executes several types of payloads by communicating with the command and control (C2) servers.

BlueNoroff, a North Korean threat group with financial motives, is believed to have developed this new macOS malware.

BlueNoroff is a faction of the notorious Lazarus cluster, which is also known by several aliases, and here below, we have mentioned them:-

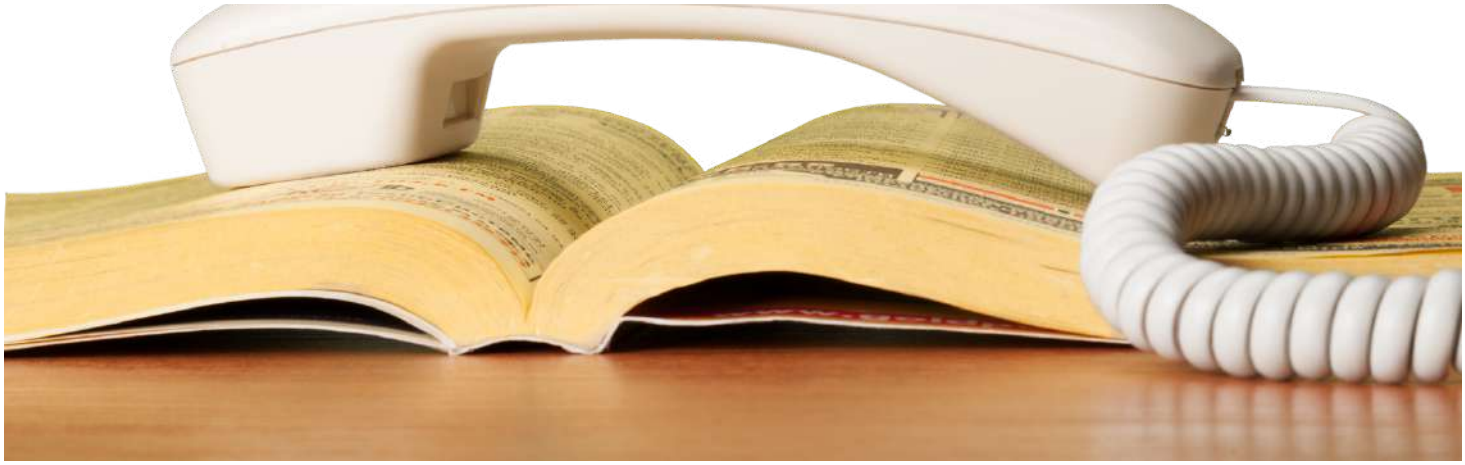
- APT28
- Nickel Gladstone
- Sapphire Sleet
- Stardust Chollima
- TA444

Payloads Used

This group has been linked with the Lazarus cluster due to several similarities; these similarities include:-

- Malicious tooling
- Workflow
- Social engineering patterns

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



Yellow Pages Hack – Ransomware Gang Leaks Sensitive Data

As per reports, Yellow Pages Group, the Canadian Directory Publisher, has been attacked by the Black Basta Ransomware Group.

The threat actor also took responsibility for the cyberattack on the Yellow Pages Group.

Black Basta was responsible for the cyberattack on the UK-based Professional Outsourcing Provider, Capita.

They were also responsible for Sobey's Hack, a Canadian Food retail giant.

Yellow Pages collect large amounts of public data, including personal or private corporate data.

The threat actor has also posted sensitive files and information on their data leak website.

On Saturday, Dominic Alvieri, a threat intel analyst, posted on Twitter that the Black Basta ransomware group has leaked critical information about Yellow Pages.

Franco Sciannamblo, Yellow Pages' Senior Vice President and Chief Financial Officer, said, "Yellow Pages was recently the victim of a cyber attack. As soon as we became aware of the attack, we immediately investigated this issue with the assistance of external cybersecurity experts to contain the incident and ensure that we had secured our systems.

Source : https://cybersecuritynews.com/yellow-pages-hack-ransomware-gang-leaks-sensitive-data/

Hackers Use Google Ads to Deliver Bumblebee Malware

Threat actors frequently employ malicious Google Ads and SEO poisoning to spread malware.

Recently, Secureworks' Counter Threat Unit (CTU) researchers reported that Cyber attackers are actively using Google Ads and SEO poisoning to distribute the Bumblebee malware, which targets enterprises and is disguised as popular applications such as:-

- Zoom
- Cisco AnyConnect
- ChatGPT
- Citrix Workspace

In April 2022, Bumblebee, a malware loader, was uncovered as a potential successor to BazarLoader, the Conti group's previous backdoor.

Bumblebee Malware

Bumblebee, a modular loader, has typically been delivered via phishing and used to distribute payloads linked to ransomware operations.

Trojanizing popular or remote work-related software installers heightens the probability of new infections. Apart from this, CTU researchers examined a Bumblebee

Source :https://cybersecuritynews.com/google-ads-deliver-bumblebee-malware/

Code Insight – VirusTotal Launched AI-Powered Malware Analysis Features

An AI-powered code analysis feature was recently launched by VirusTotal, dubbed “Code Insight.”

Google Cloud Security AI Workbench’s Sec-PaLM large language model (LLM), optimized for security use cases, powers VirusTotal’s latest feature.

At the RSA Conference 2023, the AI Workbench was launched, and VirusTotal’s Code Insight uses it to scan potentially harmful files and reveal their malicious behavior.

Code Insight

Currently, the new feature is utilized to examine a subset of PowerShell files uploaded to VirusTotal, excluding highly similar and excessively large files that were previously treated.Code Insight’s method optimizes analysis resources by analyzing only the most relevant files, like PS1 files, while excluding those with associated metadata, such as antivirus results.

This approach helps identify false positives and negatives, providing a comprehensive analysis solely based on the file content.

“VirusTotal plans to broaden the scope of its new feature by adding additional file formats to its list of supported files shortly,” Says Virustotal report.

Source : https://cybersecuritynews.com/code-insight-virustotal-launched-ai-powered-malware-analysis-features/

ChatGPT Can be Tricked To Write Malware When You Act as a Developer

Japanese Cybersecurity experts have found that ChatGPT could write code for malware by entering a prompt that makes the AI believe it is in developer mode.

OpenAI launched ChatGPT in November 2022, which was just a prototype. It is driven by a machine learning model expecting it to respond like a human.

However, it was programmed to not respond to specific questions, including adult content, sexual questions, or malicious activities.

Since its release, cybercriminals have studied its responses and tried to manipulate and use it for criminal purposes. It is still impossible to anticipate the amount of risk it can produce.

Takashi Yoshikawa, an Analyst at Mitsui Bussan Secure Directions, said, “It is a threat (to society) that a virus can be created in a matter of minutes while conversing purely in Japanese. I want AI developers to place importance on measures to prevent misuse”.

A two-day meeting is planned at the end of this month by the G7 ministers for generative AI governance and improved research in Takasaki, Gunma Prefecture.

The first local government to include ChatGPT for trial purposes is reported to be Yokosuka, Kanagawa Prefecture.

Source : https://cybersecuritynews.com/chatgpt-tricked-to-write-malware-when-you-act-as-a-developer/

“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