QUALYSEC
BEYOND CYBERSECURITY

2023

APRIL 3RD WEEK

CYBER SECURITY NEWS

CONTACT US

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

Threat Actors Using Mimikatz Hacking Tool to Deploy Trigona Ransomware

The Unit42 research team at Palo Alto Networks has recently discovered Trigona ransomware that attacks Windows with uncommon techniques and uses the Mimikatz exploitation tool for Credential Loading, Dumping, Manipulation, and injection before attempting to encrypt the files.

Trigona ransomware was first discovered in October 2022, and it was very active in December 2022. During its last discovery, it has affected almost 15 organizations in Manufacturing, Finance, Construction, marketing, and high technology industries.

As of January and February of this year, four ransom notes of Trigona were found, with two each month.

Unlike other ransomware notes, Trigona notes were not plain-text files. Instead, it is an HTML application with JS embedded. It also contains CIDs (Computer IDs) and VIDs (Victim IDs).

Trigona Ransomware Overview

A security researcher tweeted that the creators obtain initial access to a victim's environment, conducting an active reconnaissance, malware transfer through remote monitoring and management (RMM), and user account creation and deployment.

Source : https://cybersecuritynews.com/mimikatz-hacking-tool-to-deploy-trigona-ransomware/

First-Ever Ransomware Found to be Attacking macOS

LockBit ransomware gang targets Macs with its newly-developed encryptors for the first time, making them potentially the first significant ransomware group to aim at macOS.

Ransomware attacks are widespread. However, creating malware versions for targeting Macs by attackers is uncommon.

Apple computers, although widely used, have a lower presence compared to other platforms like:-

- Windows
- Linux

MalwareHunterTeam first detected samples of ransomware encryptors in VirusTotal's malware analysis repository between November and December 2022.

In a recent tweet, MalwareHunterTeam discussed a new LockBit ransomware variant targeting macOS.LockBit developed an encryptor version for newer Apple processor-based and older Macs that used Apple's PowerPC chips.

LockBit developed an encryptor version for newer Apple processor-based and older Macs that used Apple's PowerPC chips.

Source : https://cybersecuritynews.com/first-ever-ransomware/

Hackers Use Abandoned WordPress Plugins to Backdoor Websites

Threat actors have discovered a new technique to insert malicious code into websites. They are currently utilizing Eval PHP, an abandoned WordPress plugin.

Mostly, website backdoors are programmed in PHP, the foundational language of the modern web. Most other popular CMS platforms, including Joomla, Magento, and WordPress (which make up over 40% of the web), are based on PHP.

PHP is a highly universal language so attackers can abuse it. Backdoors are one of the most widely used (and misused) by attackers. Over the past few weeks, PHP code injections have been discovered. These attacks send a previously known payload that allows the attackers to execute code on the infected website remotely.

The 'wp_posts' table in the databases of the targeted websites is where the malicious code is introduced. As a result, it avoids standard website security procedures like file integrity monitoring, server-side scanning, etc., making it more difficult to detect. The threat actors install Eval PHP using a compromised or newly generated administrator account to accomplish this. This enables them to use [evalphp] shortcodes to introduce PHP code into the site's pages and posts.

Source : https://cybersecuritynews.com/abandoned-wordpress-plugins/

ICICI Bank Data Leak – Millions of Records with Sensitive Data Exposed

Millions of records containing sensitive information, including financial data and client personal documents, were disclosed by ICICI Bank.

During the most recent inquiry, researchers learned that the bank's systems were misconfigured, which allowed the bank to release important information.

With over 5,000 branches across India and a presence in at least another 15 countries globally, ICICI Bank is a multinational Indian bank with a market value of more than $76 billion.

Notably, the Indian government designated the ICICI Bank's resources as "critical information infrastructure" in 2022, meaning any damage could affect national security.

Although the infrastructure of the national bank was in a critical state, the protection of sensitive data was not guaranteed.

Bank and Client Critical Information Disclosed

The Cybernews research team uncovered misconfigured and publicly accessible cloud storage at Digital Ocean bucket – with over 3.6 million ICICI Bank files on February 1. The bank's and its clients' private information was revealed in files.

Source : https://cybersecuritynews.com/icici-bank-data-leak/

Pakistani APT-36 Hackers Using a Linux Malware To Attack Indian Government

Transparent Tribe (aka APT36), an APT group based in Pakistan, has recently been found employing a stealthy tactic to distribute a new Linux Malware called Poseidon.

The cybersecurity researchers at Uptycs have discovered Poseidon, a new Linux malware.

The group masqueraded their attack using a two-factor authentication (2FA) tool commonly used by various Indian government agencies.

The malware Poseidon is part of the Transparent Tribe's malware family that is used as a second-stage payload. Here below, we have mentioned a few other names of APT36:-

- Operation C-Major
- PROJECTM
- Mythic Leopard

General Targets of APT36

Here below, we have mentioned all the general targets of Transparent Tribe:-

- Indian government organizations
- Indian military personnel
- Indian defense contractors
- Indian educational entities

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

APT28 Hackers Deploy Malware on Cisco Routers Via Unpatched Vulnerabilities

Recently, the following agencies have published a joint advisory to warn of APT28, a Russian state-sponsored group that is found actively deploying the 'Jaguar Tooth,' a custom malware on Cisco IOS routers:-

- The UK National Cyber Security Centre (NCSC)
- The US National Security Agency (NSA)
- US Cybersecurity and Infrastructure Security Agency (CISA)
- US Federal Bureau of Investigation (FBI)

By exploiting the Unpatched vulnerabilities in Cisco routers, threat actors gain access to the target device without any authentication. Here below, we have mentioned the other names of APT28:-

- Fancy Bear
- Strontium
- Pawn Storm
- Sednit Gang
- Sofacy

While cybersecurity analysts and experts have linked this state-sponsored hacking group to Russia's General Staff Main Intelligence Directorate (GRU).

Source : https://cybersecuritynews.com/apt28-hackers-deploy-malware-on-cisco-routers/

Second Google Chrome Zero-Day Bug Actively Exploited in Wild – Update Now!

Recently, Google released an emergency security update to fix another Chrome zero-day vulnerability actively exploited in the wild. This zero-day flaw has been tracked as CVE-2023-2136 and is the second zero-day vulnerability found this year.

In this case, the most exciting development is that Google knows a working exploit for CVE-2023-2136 is already available in the wild.
While Google releases this update through Stable Channel Update for all the major platforms, and here we have mentioned them accordingly:-

- Windows: 112.0.5615.137/138
- Mac: 112.0.5615.137
- Linux: 112.0.5615.165

Second Google Chrome Zero-Day Bug of this year
This newly detected vulnerability is the second Google Chrome zero-day flaw found this year and has been actively exploited in the wild.

Source : https://cybersecuritynews.com/second-google-chrome-zero-day-bug/

What is DNS Filtering? How Does It Works? A Detailed Overview

DNS security is critical in today's world to protect against the growing threat of DNS attacks.

The risk of financial loss, data theft, and reputational damage increases for organizations that do not take DNS security seriously.
The Domain Name System (DNS) is a critical component of the internet that translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.0.1) that computers can understand.
In the modern world, DNS is required because domain names are more straightforward for people to remember than IP addresses.
Without DNS, most people would find the internet experience difficult and unpleasant.
Deploy Secure Web Gateway (SWG) Protect your employees and critical resources from web-based attacks
DNS filtering and security techniques are required to address these issues while balancing censorship concerns.
87% of organizations experienced a DNS attack in the last year, up 8% from the year before, according to IDC's 2021 Global DNS Threat Report.

Source : https://cybersecuritynews.com/dns-filtering/

Hackers Using YouTube as a Malware Distribution Platform Via Hacked YT Channel

Morphisec Threat Labs researchers have recently exposed a sneaky loader called “in2al5d p3in4er” (Invalid Printer) that delivers Aurora information stealer malware through YouTube videos.

Using an advanced anti-VM technique, the in2al5d p3in4er loader, built with Embarcadero RAD Studio, specifically targets endpoint workstations.

Late in 2022, Aurora appeared on the threat landscape for the first time, and it’s an information stealer written in Go programming language.

Abusing YouTube as a Distribution Platform

Aurora is a commodity malware distributed through fake cracked software download sites and YouTube videos to other threat actors looking to use it.

YouTube has become an attractive distribution platform for threat actors looking to spread malware to access sensitive information.

Due to its mass popularity, YouTube has become one of the first choices for threat actors.

DNS filtering is useful for restricting access to websites and online resources based on predefined rules and policies.

Source : https://cybersecuritynews.com/youtube-as-a-malware-distribution-platform/

Hackers Using Old Nokia 3310 Phone to Steal Cars

The car thieves are employing the out-of-date Nokia 3310 phone to access cars through hacking. This new approach is among the significant and distinctive incidents recorded globally regarding car theft.

An analyst at Motherboard's Vice recently found a video in which a guy in a Toyota keeps pressing a button beside the steering wheel.

The engine won't start, and the man is without the key. Indeed, he pulls out a surprising tool to fix the issue, and it's none other than a legendary Nokia 3310 phone.

nnocent-Looking Car Theft Devices

The man connects his Nokia 3310 phone to the car using a black cable. He navigates through options on the tiny LCD screen that reads, "CONNECT. GET DATA."

This video reveals a new form of car theft that is actively happening in the United States.

Vice reported that even car thieves are using small gadgets, sometimes disguised as Bluetooth speakers or phones, to access and control a car's system.

Even without technical expertise, thieves can now steal cars in under 15 seconds using this method without requiring the car key.

Source : https://cybersecuritynews.com/hackers-using-old-nokia-3310-phone-to-steal-cars/

QBot Malware Hijack Business Emails To Drop Malware Via Weaponized PDF Files

Beware of the latest phishing campaigns that distribute the QBot malware via PDFs and Windows Script Files (WSF) to infiltrate your Windows devices.

Qbot (aka QakBot, QuackBot, and Pinkslipbot) is a sneaky cyber threat once a banking trojan. Still, it has become malware that opens doors for other malicious actors to enter corporate networks.

Qbot achieves initial access by dropping dangerous payloads like:-

- Cobalt Strike
- Brute Ratel
- Other malware

As a result, the compromised device becomes accessible to other threat actors.

Once Qbot has created an entry point, other cybercriminals can spread throughout the network, stealing confidential information and deploying ransomware as extortion.

Statistical Analysis

Malicious PDF attachments were first received on the evening of April 4, followed by a mass email campaign that started at 12:00 pm the next day and continued until 9:00 pm, with approximately 1,000 letters detected.

Source : https://cybersecuritynews.com/qbot-malware/

Critical Flaw in Hikvision Video Storage Let Attacker Gain Admin Rights

The Chinese-based Video surveillance equipment manufacturer has disclosed a critical flaw in their storage products, allowing threat actors to obtain admin permissions. This flaw can be exploited by sending specially crafted messages to the affected devices.

CVE-2023-28808: Improper Access Control in Storage Products
CVSS Score: 9.1
CVSS Vector : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Some Storage products, like Hikvision's Hybrid SAN/Cluster storage, have an access control vulnerability that can be exploited by sending a specially crafted message to the affected devices.
To exploit this vulnerability, the threat actor must already have access to the network to send a specially crafted message to the affected devices.
How to Upgrade
Updates are available for all vulnerable devices. Hikvision has requested users use "Internet Explorer" to upgrade the version.

Source : https://cybersecuritynews.com/critical-flaw-hikvision/

Israeli Spyware Firm QuaDream Shut Down After Its Hacking Tools Exposed In Attacks

There have been accusations on QuaDream, the Israeli firm using hacking tools for spying on journalists, opposition figures, and advocacy organizations in at least 10 countries, shut down its complete operations.

As per the Calcalist's sources, the company's employees were notified of being laid off as it was about to cease its operations soon. This comes soon after the Cyber unicorn Snyk's layoff of 128 employees when they raised $200 million.

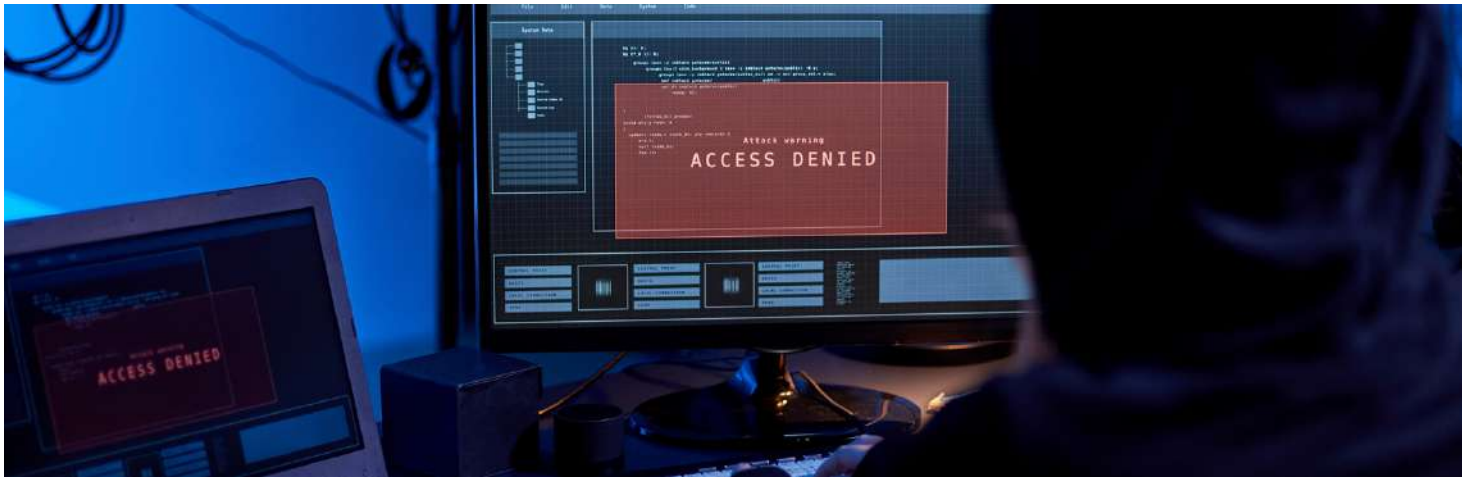
Citizen Lab and Microsoft Expose

It was reported that the firm was using hacking tools for illegal activities in almost 10 countries that, include North America and Europe according to reports from Citizen Lab and Microsoft.

For several months, the company had been in very bad shape, which ended after the report from Citizen Lab and Microsoft.

The company has only two employees to look after the computers and other equipment. In contrast, the board of directors is trying to dismantle the company by selling its intellectual property, reads the Calcalist report says.

Source : https://cybersecuritynews.com/israeli-spyware-firm-quadream-shut-down/



APT41 Hackers Using 'Google C2' Red Team Tool as a Payload in Mass Cyber Attacks

A group from China attacked a media organization in Taiwan, which is not yet known, and used Google's platform to spread a red team tool called Google Command and Control (GC2) as a final payload.

While it's part of their wider efforts to carry out harmful and malicious actions using Google's resources.

The Threat Analysis Group (TAG) of Google recently identified a campaign that a group of hackers carried out called HOODOO. At the same time, this group is known by various names based on geography and location, which is being monitored by the TAG.

Here below, we have mentioned all the other names of "HOODOO":-

- APT41
- Barium
- Bronze Atlas
- Wicked Panda
- Winnti

Strategic Perspective — Government-Backed Hackers Likely to Look to Criminals for Inspiration Targeting Cloud

Usually, we imagine military and espionage technology becoming available to the public after some time in a process called "spin-off."

Source : https://cybersecuritynews.com/apt41-hackers-using-google-c2-red-team-tool/

Vice Society Ransomware Uses PowerShell Script to Automate Steal Data

Researchers from Palo Alto Networks Unit42 uncovered the ransomware gang “Vice Society” that has stolen data from the victim network with the help of a custom-built Microsoft Powershell script.

Ransomware groups use an excessive number of methods to steal data from victims.

While some groups use external tools like FileZilla, WinSC, rclone etc Other groups use LOLBAS (living off the land binaries and scripts) methods like PowerShell scripts, RDP copy and paste and Wininet.dll (Microsoft’s Win32 API).

The script and method used by the Vice Society gang is explained below.

Attack Flow

Most threat actors use built-in methods like LOLBAS for stealing the data, which removes the need for bringing in an external tool that will be detected by security software or security personnel.

Built-in methods evade these security mechanisms since they operate in the environment.

Threat actors use PowerShell scripts to hide in plain sight in a native Windows environment.

Source : https://cybersecuritynews.com/vice-society-ransomware-2/

Russia-linked APT29 Attacking NATO and European Union Countries

The Polish military, along with its CERT.PL recently discovered that a Russian state-sponsored group of hackers, dubbed APT29 (aka Cozy Bear and Nobelium), is actively targeting the NATO and European Union countries and in Africa, but to a lesser extent.

The cyberespionage group's campaign focused on obtaining sensitive information from foreign ministries and diplomatic entities through data harvesting techniques.

Poland's Military Counterintelligence Service and CERT.PL has advised all potential targets to enhance the security of their IT systems and improve attack detection mechanisms to safeguard against the actor's interests.

Technical Analysis

By creating fake emails pretending to be embassies from European countries, the attackers have targeted diplomatic personnel using spear-phishing tactics to direct victims to malicious websites.

According to the BlackBerry report, They also employed the emails' ISO, IMG, and ZIP files as attachments, intending to deploy malware onto the target's computer systems.

Source : https://cybersecuritynews.com/russia-linked-apt29-attacking-nato-and-european-union/

ChatGPT Account Take Over Vulnerability Let Hackers Gain User's Online Account

A renowned security analyst and bug hunter, Nagli (@naglinagli), recently uncovered a critical security vulnerability in ChatGPT.

With just a single click, a threat actor could easily exploit the vulnerability and gain complete control of any ChatGPT user's account.

As a result, opening the doors to sensitive data let attackers execute unauthorized actions; the whole is termed "Account Take Over."

ChatGPT Account Takeover

Account takeover is a sneaky cyber attack where an attacker or hacker gains access to your account unauthorizedly by either exploiting in the system or stealing your login details.

It is possible for an attacker to conduct a variety of malicious activities after having gained access to a target system or device:-

- Theft of personal information
- Fraudulent transactions
- Spread malware

To access a victim's ChatGPT account, the attacker exploits a web cache deception vulnerability. This ChatGPT Account Take Over bug made a single-click attack possible, enabling a remote attacker to compromise any user's account and completely take over the account.

Source : https://cybersecuritynews.com/chatgpt-account-take-over-vulnerability/

“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