QUALYSEC

BEYOND CYBERSECURITY

2023

MAY 3RD WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com

☎ 865 866 3664

contact@qualysec.com

New “Guerilla” Malware Infected Over 9 Million Android-based Devices

The Lemon Group, a prominent cybercrime organization, has planted the ‘Guerilla’ malware on nearly 9 million Android devices, enabling them to execute various malicious activities.

While among all the illicit activities here, we have mentioned the key ones:-

- Intercepting SMS passwords
- Establishing reverse proxies
- Hijacking WhatsApp sessions

A recent Trend Micro report revealed that certain elements of the attackers’ infrastructure exhibit similarities with the Triada trojan operation in 2016, suggesting a potential connection between the two incidents.

Triada was discovered pre-installed in 42 Android smartphone models manufactured by budget-friendly Chinese brands with a global market presence, posing a significant security risk to users.

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

Notorious State-Sponsored Hacker Group Stealthy Infrastructure Uncovered

Group-IB’s cybersecurity researchers made a significant discovery, revealing undisclosed attack infrastructure employed by the highly active state-sponsored group SideWinder. Their targets mainly encompassed entities situated in:-

- Pakistan
- China

In a collaborative report, cybersecurity firms Group-IB and Bridewell disclosed the existence of a comprehensive network consisting of 55 domains and IP addresses exploited by the malicious actor.

While the phishing domains that the researchers identify mimic many organizations from various sectors, including the following:-

- News
- Government
- Telecommunications
- Financial

SideWinder State-Sponsored Hacker Group

Operating since 2012, SideWinder is a long-standing threat actor known for its persistent activity. Their attack strategies heavily rely on spear-phishing techniques to gain unauthorized access to targeted systems.

Source : https://cybersecuritynews.com/sidewinder-state-sponsored-hacker-group/

New Water Orthrus’s Hacker Group Deploys Malware & Steals Credit Card Data

Trend Micro researchers have been monitoring a threat actor known as Water Orthrus since 2021, as they employed pay-per-install networks to distribute the CopperStealer malware.

The malware has undergone several modifications and upgrades by the threat actor to serve different illicit objectives like:-

- Injecting network advertisements
- Obtaining personal information
- Stealing cryptocurrency

While apart from this, cybersecurity experts suggest a potential association between them and the previously reported “Scranos” threat campaign from 2019.

Credential Phishing Campaign

Analysts discovered two new campaigns in March 2023, introducing malware called “CopperStealth” and “CopperPhish,” which share similarities with CopperStealer and are believed to be the work of the same author, suggesting they are the new activities of Water Orthrus.

Source : https://cybersecuritynews.com/hacker-group-deploys-malware/

Hackers Selling Powerful Infostealers on Underground Forums

The role of info stealers (aka stealers) in the cybercrime world has been growing, according to researchers at the SecureWorks Counter Threat Unit (CTU).

While threat actors make use of them to steal the following data from the networks and computer systems that are compromised or breached:-

- Login credentials
- Financial details
- Personal data
- System information

Infostealers are commonly deployed onto computers and devices through various means, including:-

- Phishing attacks
- Compromised websites
- Download of malicious software

By using these above-mentioned TTPs, the threat actors install the info stealer onto the target's system and gain unauthorized access to sensitive information.

Source : https://cybersecuritynews.com/hackers-selling-powerful-infostealers/

Microsoft Cloud Services Scanning Inside of password-protected Zip Files for Malware

Threat actors have been evading in-built scanners in the cloud and local systems but archiving them as password-protected ZIP files. This makes it hard for scanners to crack the password and scan for malicious files.

However, recent reports suggest that Microsoft can scan password-protected archive files in Sharepoint and check for malware.

Security researcher Andrew Brandt posted on infosec.exchange platform that Sharepoint has scanned a couple of his archive files and marked them as "Malware Detected".

He uploaded the files in SharePoint for malware research with the password "infected." Nevertheless, they were scanned and removed by Microsoft.

In his post, he stated, "This morning, I discovered that a couple of password-protected Zips are flagged as "Malware detected" which limits what I can do with those files – they are basically dead space now."

On further discussion, it was denoted that Microsoft scans the contents of Password-protected ZIP files using various methods in all of its cloud services.

Source : https://cybersecuritynews.com/scanning-inside-zip/

Camaro Dragon Hacker Group Attack TP-Link Routers to Deploy Remote Shells

Recently, the cybersecurity experts at Checkpoint identified that the Chinese state-sponsored group “Camaro Dragon” employs a custom “Horse Shell” malware embedded in TP-Link routers’ firmware to target European foreign affairs organizations, leveraging residential networks for their attacks.

The attack targets regular residential and home networks, indicating that infecting a home router does not imply the homeowner was a specific target, but rather a pipe for the attackers’ objectives.

The malware grants threat actors complete device control, enabling them to execute commands, transfer files, and utilize it as a SOCKS proxy for communication relay.

Infection chain

Check Point Research discovered the Horse Shell TP-Link firmware implant in January 2023, revealing its connection to the Chinese “Mustang Panda” hacking group.

Despite significant overlaps, Check Point Research identifies the activity cluster separately as “Camaro Dragon,” even though it shares traits with the “Mustang Panda” hacking group.

Source : https://cybersecuritynews.com/camaro-dragon-hacker-group/

Hackers are Actively Using the new.zip Domain for Malicious Attacks

Top-Level Domains (TLDs) have been extremely popular ever since the emergence of the internet. ICANN is the organization that is responsible for these TLD registrations.

Domains ending with any characters like .xyz, .top, etc., are being registered by this ICANN.

In addition to TLDs, there is a “gTLD” program in which companies can register their own trademark as a TLD. For instance, “google.com” can be named as “.google.”

However, gTLD is not cheap and there is a very low success ratio. There have been dozens of gTLDs approved recently and are currently in use.

Google has applied for several gTLDs previously, in which “.zip” was also one of them. It was approved in 2014, as per reports.

.Zip Domain Security Risks

Security experts have warned that the new ‘.zip’ top-level domain (TLD) could facilitate the spread of malware and undermine legitimate sources.

Some of the .zip domains registered recently

Source : https://cybersecuritynews.com/zip-domain-for-malicious-attacks/

PharMerica Hacked – Over 5 million Patients record stolen

Reports indicate that PharMerica Healthcare has faced a data breach resulting in 5.8 million records being exposed.

PharMerica is one of the Fortune 1000 companies that provide Pharmacy management services to customers worldwide. It has a revenue of $2.1B annually, with around 5000 employees working worldwide.

According to the data breach report, PharMerica Corporation, located in Kentucky, US, was attacked by threat actors and has stolen patients' sensitive information.

The Attorney General's Office's report suggests that the breach happened on 12th March and was discovered on 21st March.

On March 28th, 2023, the Money Message ransomware group claimed responsibility for this data breach and threatened to leak the data to the public if the company refused to meet its demands.

According to the Money Message ransomware group, nearly 4.7TB of data was stolen that includes Social Security Numbers (SSNs), health information, and medical records of victims, which were published on the Clearnet hacking forum when the threat actors' deadline for the ransom expired.

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

Multiple Counter-Strike Zero-Day Flaw Let Hackers Control Client Machine

Neodyme researchers discovered three distinct RCE vulnerabilities in Counter-Strike: Global Offensive, where each vulnerability is exploited through a malicious Python server upon game client connection.

Despite fixing several critical vulnerabilities with a patch dated 04/28/2021, Counter-Strike: Global Offensive remains popular with 21 million monthly players, largely due to the range of game modes available on community servers.

Multiple Counter-Strike Zero-Day Flaw

The extensive availability of game modes, community servers, and modding support in Counter-Strike: Global Offensive results in a significant attack surface, with various parsers handling potentially malicious data directly from the game's server.

The source engine's TCP-like network stack, which is based on UDP, presents inherent complexities and vulnerabilities that have been exploited in previous attacks.

While cheater communities like UnknownCheats are frustrating for gamers, they provide valuable resources for security researchers, such as detailed reverse engineering posts and cheat tools that aid in understanding the network protocols.

Source : https://cybersecuritynews.com/counter-strike-zero-day-flaw/

BPFDoor – New Stealthy Backdoor Malware Targets Linux Systems

A completely new and previously unreported form of BPFdoor was recently discovered and examined by Deep Instinct's threat lab.

The malware's use of a Berkley Packet Filter, an unusual method of obtaining instructions and avoiding detection that gets beyond firewall limits on incoming traffic, gives it its name.

The malware is linked to Red Menshen (Red Dev 18). This Chinese threat actor has been seen targeting political, educational, and logistical institutions and telecommunications companies in Asia and the Middle East since 2021.

BPFDoor Targeting Linux Systems

To establish a persistent, long-term footing in already-breached networks and environments, BPFdoor is a Linux-specific, low-profile, passive backdoor that primarily ensures that an attacker can re-enter an infected machine for an extended time after compromise.

BPFdoor was initially known for its practical and elegant design and a strong emphasis on stealth, which is critical in ensuring undetected long-term persistence.

Source : https://cybersecuritynews.com/bpfdoor-targeting-linux-systems/

CYBER SECURITY NEWS

Bl00dy Ransomware Gang Exploiting Printer Vulnerability to Attack Schools

A joint Cybersecurity Advisory (CSA) from the FBI and CISA have been published on actively exploiting the vulnerability in some versions of PaperCut NG and PaperCut MF, identified as CVE-2023-27350.

This makes it possible for an unauthenticated actor to execute malicious code remotely. In March 2023, PaperCut made a fix available.

The Bl00dy Ransomware Gang attempted to use weak PaperCut servers to attack the Education sector.

“In early May 2023, according to FBI information, the Bl00dy Ransomware Gang gained access to victim networks across the Education Facilities Subsector where PaperCut servers vulnerable to CVE-2023-27350 were exposed to the internet,” reads the security advisory.

“Ultimately, some of these operations led to data exfiltration and encryption of victim systems.”

Source : https://cybersecuritynews.com/bl00dy-ransomware-gang/

“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