aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report
December 2023

2023-12-31 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

1. Executive summary

This month, CERT aDvens brings you three noteworthy vulnerabilities in addition to those already published.

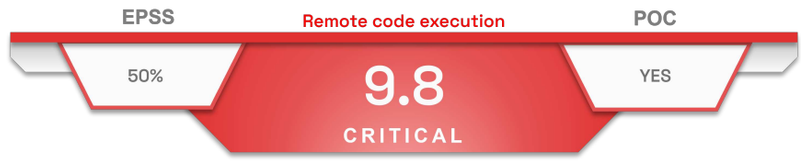
Through two articles, CERT analysts provide an in-depth analysis of various extortion methods employed in ransomware attacks, followed by an overview of the use of **OAuth** applications in conducting cybercriminal activities.

2. Vulnerabilities

This month, aDvens' CERT highlights three vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (availability of proofs of concept, exploitation…). Applying their patches or workarounds is highly recommended.

aDvens' CERT recommends testing proposed workaround measures in a test environment before deploying them in production. This step is crucial to prevent any unintended side effects.

2.1. Apache OFBiz - CVE-2023-49070



On 4 December 2023, Apache published a security advisory concerning a critical vulnerability (CVE-2023-49070) in OFBiz.

Apache OFBiz is an Open-Source resource management software used by companies with more than 10,000 employees.

This vulnerability is due to the presence of a deprecated XML-RPC component. It allows an unauthenticated attacker to inject arbitrary code into vulnerable applications.

2.1.1. Risk

- Remote code execution

2.1.2. Type of vulnerability

- **CWE-94**: Improper Control of Generation of Code ('Code Injection')

2.1.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Affected products

- Apache OFBiz versions 18.12.09 and prior

2.1.5. Recommendation

- Update Apache OFBiz to version 18.12.10 or later.
- Additional information is available in Apache's advisory.

2.1.6. Proof of concept

A Proof of Concept is available in open sources.

2.2. Unitronics - CVE-2023-6448

On 28 November 2023, CISA published an alert concerning vulnerability (CVE-2023-6448) in Unitronics PLCs (Programmable Logic Controllers). This PLC is frequently used in the water treatment, energy, agribusiness and healthcare sectors.

The use of a default administrator password allows an attacker, who has access to these APIs, to take control of the vulnerable system.

This vulnerability is currently exploited by the Iranian group CyberAv3ngers.
The CISA added this CVE to its Known Exploited Vulnerabilities (KEV) repository on 12 December 2023.

2.2.1. Risk

- System compromise

2.2.2. Type of vulnerability

- **CWE-798**: Use of Hard-coded Credentials
- **CWE-1188**: Initialization of a Resource with an Insecure Default

2.2.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Affected products

- Unitronics VisiLogic versions prior to 9.9.00

2.2.5. Recommendation

- Update Unitronics VisiLogic to version 9.9.00 or later.
- Ensure that the PLCs are not exposed online.
- Additional information is available in Unitronics' and the CISA's advisory.

2.2.6. Proof of concept

To date, no Proof of Concept is available in open sources.

2.2.7. Indicators of compromise

TLP	TYPE	VALUE
TLP:CLEAR	MD5	BA284A4B508A7ABD8070A427386E93E0
TLP:CLEAR	SHA1	66AE21571FAEE1E258549078144325DC9DD60303
TLP:CLEAR	SHA256	440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3
TLP:CLEAR	IP	178.162.227[.]180
TLP:CLEAR	IP	185.162.235[.]206

2.3. QNAP - CVE-2023-47565

On 11 December 2023, QNAP issued an alert regarding a vulnerability affecting VioStor NVR (Network Video Recorder), a network-based IP camera surveillance solution.

A lack of control over user-supplied data allows an authenticated remote attacker to modify NTP settings and execute code.

This vulnerability is currently exploited by the Mirai InfectedSlurs variant.
The CISA added this CVE to its Known Exploited Vulnerabilities (KEV) repository on 21 December 2023.

2.3.1. Risk

- Remote code execution

2.3.2. Type of vulnerability

- **CWE-78** : Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.3.3. Severity

Attack vector	Adjacent	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Affected products

- QVR firmware versions 4.X and prior

2.3.5. Recommendation

- Update QVR's firmware to version 5.x or later.
- Additional information is available in QNAP's and the CISA's advisory.

2.3.6. Proof of concept

To date, no Proof of Concept is available in open sources.

2.3.7. Indicators of compromise

TLP	TYPE	VALUE
TLP:CLEAR	SHA256 I Payload	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8 I arm
TLP:CLEAR	SHA256 I Payload	3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8 I arm5
TLP:CLEAR	SHA256 I Payload	75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380 I arm6
TLP:CLEAR	SHA256 I Payload	f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc I arm7
TLP:CLEAR	SHA256 I Payload	8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099 I kdvrarm7
TLP:CLEAR	SHA256 I Payload	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1 I mips
TLP:CLEAR	SHA256 I Payload	a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26 I mpsl
TLP:CLEAR	SHA256 I Payload	cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87 I nigga.sh
TLP:CLEAR	SHA256 I Payload	8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6 I ok.sh
TLP:CLEAR	SHA256 I Payload	35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a I ppc
TLP:CLEAR	SHA256 I Payload	7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2 I sh4
TLP:CLEAR	SHA256 I Payload	29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff I spc
TLP:CLEAR	SHA256 I Payload	cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9 I x86
TLP:CLEAR	SHA256 I Payload	a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d I mpsl
TLP:CLEAR	SHA256 I Payload	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1 I mips
TLP:CLEAR	C2 domain	opewu[.]homes
TLP:CLEAR	C2 domain	wu[.]qwewu[.]site
TLP:CLEAR	C2 domain	dfvzfvd[.]help
TLP:CLEAR	C2 domain	husd8uasd9[.]online
TLP:CLEAR	C2 domain	homehitter[.]tk
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]oss
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]geek
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]pirate
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]dyn
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]libre
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]gopher
TLP:CLEAR	C2 domain	shetoldmeshewas12[.]parody
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]oss
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]geek
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]pirate
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]dyn
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]libre

TLP	TYPE	VALUE
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]gopher
TLP:CLEAR	C2 domain	shetoldmeshewas13[.]parody
TLP:CLEAR	C2 domain	hujunxa[.]cc
TLP:CLEAR	C2 domain	skid[.]uno
TLP:CLEAR	C2 domain	dogeating[.]monster
TLP:CLEAR	C2 domain	chinkona[.]buzz
TLP:CLEAR	C2 domain	dogeatingchink[.]uno
TLP:CLEAR	C2 domain	infectedchink[.]cat
TLP:CLEAR	C2 domain	infectedchink[.]online
TLP:CLEAR	C2 domain	sdfsd[.]xyz
TLP:CLEAR	C2 domain	gottalovethe[.]indy
TLP:CLEAR	C2 domain	pqahzam[.]ink
TLP:CLEAR	C2 domain	cooldockmantoo[.]men
TLP:CLEAR	C2 domain	chinks-eat-dogs[.]africa
TLP:CLEAR	C2 domain	cnc[.]kintaro[.]cc
TLP:CLEAR	C2 domain	fuckmy[.]site
TLP:CLEAR	C2 domain	fuckmy[.]store
TLP:CLEAR	C2 domain	hbakun[.]geek
TLP:CLEAR	C2 domain	ksarpo[.]parody
TLP:CLEAR	C2 domain	rwziag[.]pirate
TLP:CLEAR	C2 domain	metbez[.]gopher
TLP:CLEAR	C2 domain	rmdtqq[.]libre
TLP:CLEAR	C2 domain	pektbo[.]libre
TLP:CLEAR	C2 domain	mqcgbs[.]gopher
TLP:CLEAR	C2 domain	cbdgzy[.]pirate
TLP:CLEAR	C2 domain	czbrwa[.]geek
TLP:CLEAR	C2 domain	edrnhe[.]oss
TLP:CLEAR	C2 domain	hfoddy[.]dyn
TLP:CLEAR	C2 domain	fawzpp[.]indy
TLP:CLEAR	C2 domain	hxqytk[.]geek
TLP:CLEAR	C2 domain	iaxtpa[.]parody
TLP:CLEAR	C2 domain	mfszki[.]gopher
TLP:CLEAR	C2 domain	qhedye[.]oss
TLP:CLEAR	C2 domain	wnisyi[.]libre
TLP:CLEAR	C2 domain	asdjjasdhioasdia[.]online
TLP:CLEAR	C2 domain	jiggaboojones[.]tech

2.3.8. Detection rules

Snort rules

rule to detect CVE-2023-47565 exploitation attempts

```
alert tcp any any -> any any (msg:"QNAP VioStor - CVE-2023-47565 (InfectedSlurs exploitation attempt)";
flow:to_server,established; content:"POST"; http_method; content:"/cgi-bin/server/server.cgi";
content:"func="; content:"counter="; content:"APPLY="; http_uri; content:"time_mode="; content:"time_YEAR=";
content:"time_MONTH="; content:"time_DAY="; content:"time_HOUR="; content:"time_MINUTE=";
content:"time_SECOND"; content:"enable_rtc="; content:"TIMEZONE="; content:"year="; content:"month=";
content:"day="; content:"CONFIGURE_NTP="; content:"SPECIFIC_SERVER="; http_client_body; sid:1000002;)
```

rule to detect network traffic to InfectedSlurs' C2 Servers

```
alert ip any any -> 45.95.147.226 any (msg:"InfectedSlurs C2 communications"; sid:1000001;)
alert ip any any -> 45.142.182.96 any (msg:"InfectedSlurs C2 communications"; sid:1000002;)
alert ip any any -> 5.181.80.53 any (msg:"InfectedSlurs C2 communications"; sid:1000003;)
alert ip any any -> 5.181.80.54 any (msg:"InfectedSlurs C2 communications"; sid:1000004;)
alert ip any any -> 5.181.80.55 any (msg:"InfectedSlurs C2 communications"; sid:1000005;)
alert ip any any -> 5.181.80.59 any (msg:"InfectedSlurs C2 communications"; sid:1000006;)
alert ip any any -> 5.181.80.81 any (msg:"InfectedSlurs C2 communications"; sid:1000007;)
alert ip any any -> 5.181.80.72 any (msg:"InfectedSlurs C2 communications"; sid:1000008;)
alert ip any any -> 5.181.80.77 any (msg:"InfectedSlurs C2 communications"; sid:1000009;)
alert ip any any -> 5.181.80.102 any (msg:"InfectedSlurs C2 communications"; sid:1000010;)
alert ip any any -> 5.181.80.126 any (msg:"InfectedSlurs C2 communications"; sid:1000011;)
alert ip any any -> 5.181.80.127 any (msg:"InfectedSlurs C2 communications"; sid:1000012;)
alert ip any any -> 91.92.254.4 any (msg:"InfectedSlurs C2 communications"; sid:1000013;)
alert ip any any -> 185.225.74.161 any (msg:"InfectedSlurs C2 communications"; sid:1000014;)
alert ip any any -> 185.150.26.226 any (msg:"InfectedSlurs C2 communications"; sid:1000015;)
alert ip any any -> 194.180.48.202 any (msg:"InfectedSlurs C2 communications"; sid:1000016;)
alert ip any any -> 85.217.144.207 any (msg:"InfectedSlurs C2 communications"; sid:1000017;)
alert ip any any -> 45.139.105.145 any (msg:"InfectedSlurs C2 communications"; sid:1000018;)
alert ip any any -> 162.220.166.114 any (msg:"InfectedSlurs C2 communications"; sid:1000019;)
alert ip any any -> 89.190.156.145 any (msg:"InfectedSlurs C2 communications"; sid:1000020;)
alert ip any any -> 162.246.20.236 any (msg:"InfectedSlurs C2 communications"; sid:1000021;)
alert ip any any -> 194.153.216.164 any (msg:"InfectedSlurs C2 communications"; sid:1000022;)
alert ip any any -> 95.214.27.10 any (msg:"InfectedSlurs C2 communications"; sid:1000023;)
alert ip any any -> 62.113.113.168 any (msg:"InfectedSlurs C2 communications"; sid:1000024;)
alert ip any any -> 194.38.21.42 any (msg:"InfectedSlurs C2 communications"; sid:1000025;)
```

YARA rules

```
rule infected_slurs_scripts_1 {
   meta:
      description = "infected-slurs-scripts-1"
      author = "Akamai SIRT"
      date = "2023-11-20"
   strings:
      $s1 = "ftpget.sh ftpget.sh && sh ftpget.sh;curl http://" fullword ascii
      $s2 = "chinese family" fullword ascii
      $s3 =
"\\x23\\x21\\x2F\\x62\\x69\\x6E\\x2F\\x73\\x68\\x0A\\x0A\\x66\\x6F\\x72\\x20\\x70\\x72\\x6F\\x63\\x5F\\x64\\
x69\\x72\\x20\\x69\\x6E\\x20\\x2F\\x70\\x72\\x6F\\x63\" fullword ascii
      $s4 = "/bin/busybox hostname TBOT" fullword ascii
   condition:
      3 of them
}
```

```
rule infected_slurs_scripts_2 {
   meta:
      description = "infected-slurs-scripts-2"
      author = "Akamai SIRT"
      date = "2023-11-20"
   strings:
      $s1 = ";<=>?@ABCDEFGJIMOPQRSTUVWX[\\^_`abcxyz{|}~" fullword ascii
      $s2 = "#$%&'()*+,234567" fullword ascii
      $s3 = "BOOOOOOONS_" fullword ascii
      $s4 = "npxXoudifFeEgGaACScs" fullword ascii
   condition:
      3 of them
}
```

```
rule infected_slurs_bins {
   meta:
      description = "infected-slurs-bins"
      author = "Akamai SIRT"
      date = "2023-11-20"
   strings:
      $s1 = "attack_gre.c" fullword ascii
      $s2 = "attack_ongoing" fullword ascii
      $s3 = "ensure_single_instance" fullword ascii
      $s4 = "/home/landley/aboriginal/aboriginal/build/temp-armv7l/gcc-core/gcc/config/arm/pr-support.c"
fullword ascii
      $s5 = "words_left" fullword ascii
      $s6 = "kutil_strncmp" fullword ascii
      $s7 = "fflush_unlocked" fullword ascii
      $s8 = "methods_len" fullword ascii
   condition:
      6 of them
}
```

3. Ransomware : understanding the extortion ecosystem

This article highlights extortion methods used by attackers to persuade victims to pay a ransom. For reasons of simplification, these methods are grouped into two ecosystems:

- **Elementary extortion ecosystem** : focuses on basic attack layers
- **Multi-layered extortion ecosystem** : focuses on multiple attack layers

3.1. Elementary extortion ecosystem

This system is made up of three methods.

3.1.1. Pure

In case of pure extortion, the victim's data is exfiltrated by the attackers without being encrypted. This method is applied in attacks known as: *encryption-less ransomware* or *encryption-less attacks*.

- This method has been observed among several groups of attackers, including: Babuk, SnapMC, Karakurt, Donut, RansomHouse, BianLian, CI0p, and Lapsus$...

3.1.2. Simple

This simple extortion method involves encrypting the victim's data. Encrypted, the data is unusable and can only be decrypted using a specific decryption key. This method can be applied to an entire system or specifically to a few files. Encryption is carried out via a ransomware : a malware designed to deny a user or organisation access to files on their system. The most famous ransomware of this type is North Korean: WannaCry.

- This method has been observed among several groups of attackers, including: KniveSpider (Ukrainian), UNIT 180 (North Korean), APT 38 (North Korean)...

3.1.3. Double

Attackers exfiltrate the victim's data before encrypting it. Becoming famous in 2019, the double extortion method was first observed by the threat group TA2101 against the private security company *Allied Universal*. The attackers used Maze ransomware to encrypt the data and threatened to leak the extorted data.

- This method has been observed among several groups of attackers, including: LockBit, Hive, Industrial Spy, Egregor, DarkSide, Avaddon, Ragnar Locker, REvil / Sodinokibi, DoppelPaymer / BitPaymer, Conti...

3.1.4. Infographic synthesis

Below is an infographic synthesis which highlights the three methods presented previously.

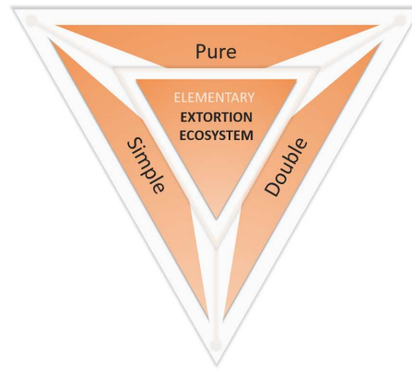


Figure 1. Infographic synhtesis of the elementary extortion ecosystem.

3.2. Multi-layered extortion ecosystem

This ecosystem is made up of six methods.

3.2.1. Operational incapacity

This method consists of carrying out a distributed denial of service attack in order to render the services of the victim's organisation inoperative. In addition to the damage caused by ransomware (the encryption of data), victims also experience loss of income due to the downtime caused by the DDoS attack. This method is often categorised as triple or quadruple extortion.

- This method has been observed among several groups of attackers, including: LockBit, REvil, Avos Locker, Avaddon…

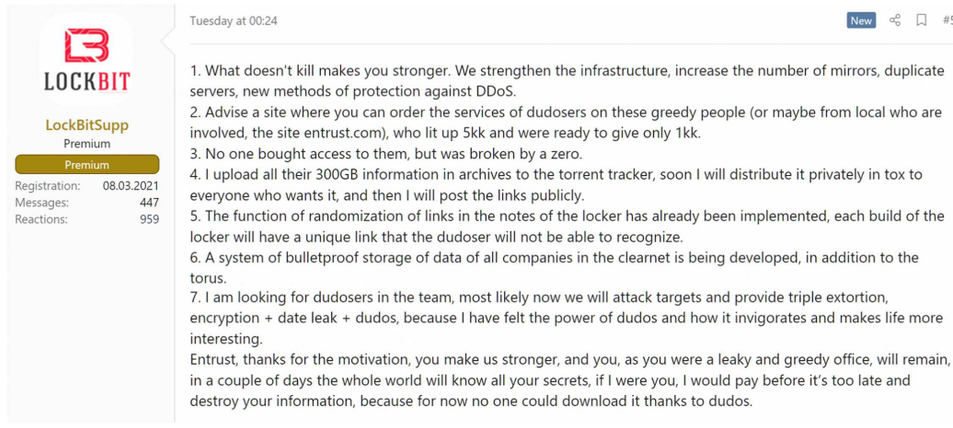


Figure 2. Cybercrime syndicate LockBitSupp announces use of DDoS attack in August 2022 (see n°7).

3.2.2. Externalised coercion

Often considered quadruple extortion, this method consists of inciting the payment of the ransom by directly threatening the collateral victims. Customers, patients or business partners of the targeted organisation are directly contacted by the attackers. Contact can be made via telephone calls, letters, emails and SMS. The attackers threaten to publish the extorted data and trick the collateral victim into paying a micro-ransom. Attackers can also encourage collateral victims to put pressure on the organisation to pay the full ransom. In 2020, *Vastaamo*, a Finnish private psychotherapy service provider, was the victim of a ransomware attack. On 21 October, *Vastaamo* announced that the data of 36,000 patients had been extorted. On 24 October, several patients were contacted by the attackers to make micro-ransom payments.

- This method has been observed among several groups of attackers, including: REvil, SunCrypt…

Figure 3. VX Underground published on YouTube an audio recording of the threat actor SunCrypt. Attackers put pressure on the victim so that the organisation pays the ransom.

3.2.3. Revile on the victim's website

Although being rare, this method consists of modifying the website of the targeted organisation in such a way as to notify visitors that it is the victim of a cyberattack. The modification can be an addition of text or an image. This method can be used by attackers when the targeted organisation tries to remain discreet so as not to reveal the incident caused by the cyberattack. During the year 2022, the threat group Industrial Spy modified the index page of an organisation's website by specifying the quantity of data extorted and added an address to communicate with the attackers.

- This method has been observed among several groups of attackers, including: Industrial Spy, L4NC34 Ransomware…

Figure 4. Modification of a website by the L4NC34 Ransomware threat group.

3.2.4. Reporting a ransomware attack

This method recently appeared during the month of November 2023. Its purpose is to put pressure on the victim organisation by reporting the cyberattack to the authorities. In America, the SEC (*Securities and Exchange Commission*: the American federal body for regulation and supervision of financial markets) imposes a deadline for organisations to notify of a cybersecurity incident. Individuals can report the incident if the organisation does not do so. If the incident is not reported, the victim organisation may be fined. In November 2023, the threat group operating the AlphV / BlackCat ransomware filed a complaint with the SEC against MeridianLink.

- This method has been applied by one threat group: AlphV / BlackCat.

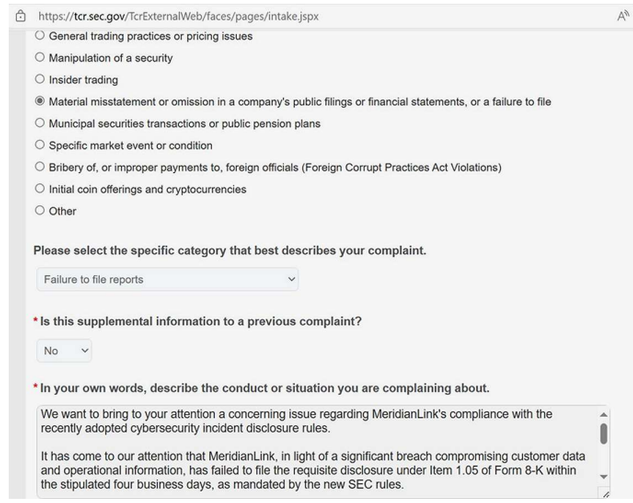


Figure 5. A screen capture of AlphV / BlackCat.

3.2.5. Reputational damage

The attackers announce the cyberattack to the media and/or on social media networks. Industrial Spy regularly published on Twitter (*X*) the list of its victims, also including screenshots and the logos of the targeted brands. Ragnar Locker broadcasted advertisements on the social network *Facebook* to put pressure on *Campari* (Italian organisation specialising in alcohol and spirits).

- This method has been observed among several groups of attackers, including: Industrial Spy, Ragnar Locker, Bl00dy…

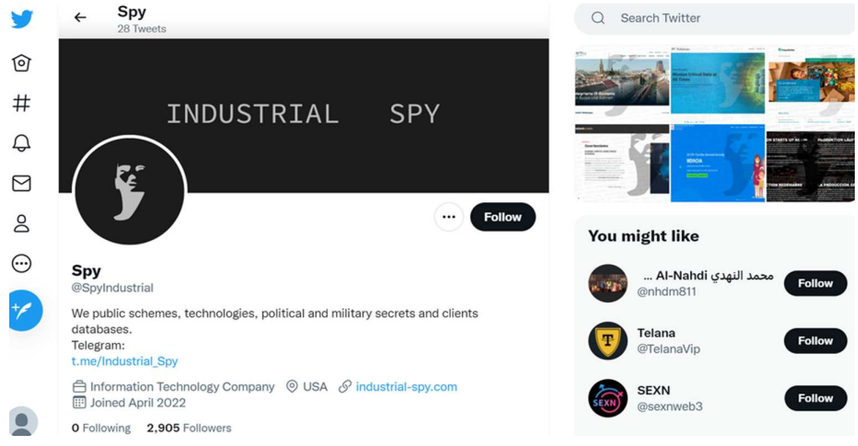


Figure 6. A screen capture of the Twiter (X) account of the threat group Industrial Spy.

3.2.6. Death threat

Although very rare, this method involves threatening the lives of the families of the targeted organisation. In September 2022, the threat group BI00dy publicly announced on Telegram death threats against those who refused to pay the ransom. The victims will be "hunted by assassins".

- This method has been applied by one threat group: BI00dy.

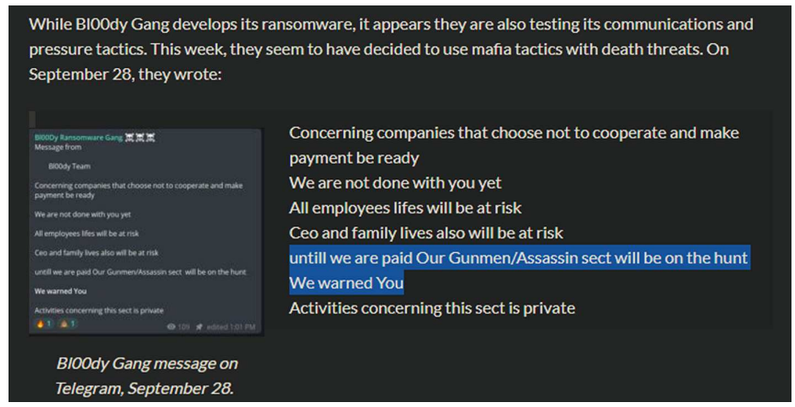


Figure 7. A screen capture of the databreach website.

3.2.7. Infographic synthesis

Below is an infographic synthesis which highlights the six methods previously presented.

Figure 8. Infographic synthesis of the multi-layered extortion ecosystem.

3.3. Lack of consensus

There is no consensus to categorise all additional methods used by threat groups. These are sometimes categorised as triple extortion, quadruple extortion, or more.

3.3.1. Example 1

CloudFlare does not seem to consider the DDoS attack as triple extortion, but as the 7th method of pressure.

7. Adjonction d'une attaque DDoS

Alors que l'entreprise visée croule déjà sous les nombreuses tâches à accomplir (contacter les autorités et les clients, localiser les fichiers de sauvegarde et minimiser les mouvements latéraux), certains acteurs malveillants peuvent également la menacer d'une attaque par déni de service distribué, voire tout bonnement en lancer une. L'engorgement d'un réseau pendant une période mouvementée ajoute du stress et mobilise de nouvelles ressources informatiques.

Figure 9. From the article "Ransomware Attackers Step Up Extortion Tactics" - CloudFlare.

3.3.2. Example 2

Infographic from *Recorded Future* on modeling the extortion ecosystem:

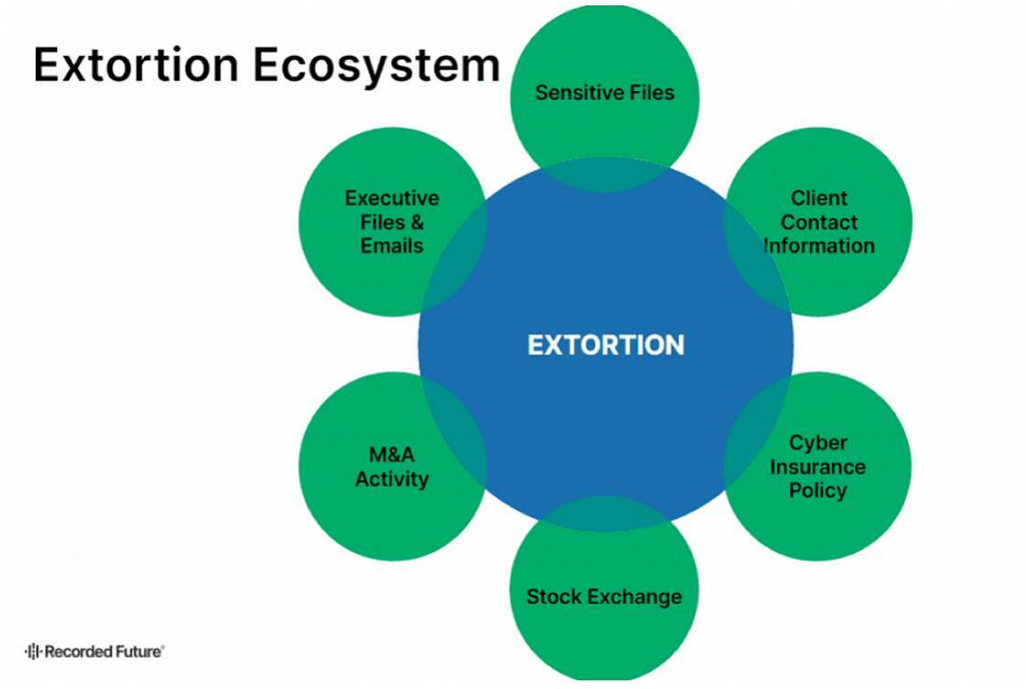


Figure 10. From the article "Ransomware gang wants to short the stock price of their victims" - Recorded Future.

3.3.3. Example 3

PaloAlto highlights the DDoS attack as a triple extortion.

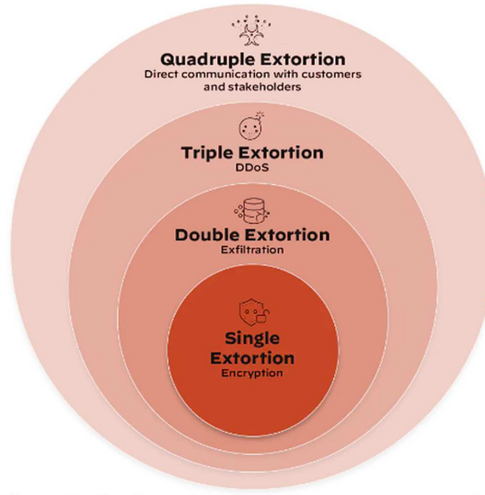


Figure 1. The four phases of ransomware extortion

Figure 11. From the article "What is Multi-Extortion Ransomware?" - PaloAlto.

3.3.4. Simplicity

For simplicity, all additional methods can be categorised as **multi-layered** or **multifaceted**.

3.4. Cyber-psychology

3.4.1. Two wars

A ransomware cyberattack constitutes a technical warfare in itself: the use of malware, encryption technologies, the attacker's infrastructure…

However, alongside the technical warfare, there lies another war : the psychological warfare which involves the use of planned psychological operations to influence the emotions, attitudes, and behavior of victims.

Below is an infographic that depicts the extortion ecosystem at the heart of both wars:

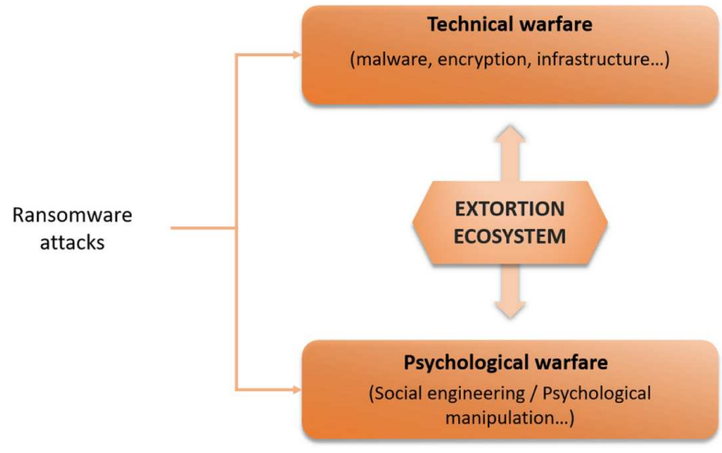


Figure 12. The extortion ecosytem is a the center of both war : the technical warfare and the psychological warfare (for simplification, the third war - economic warfare - is not shown).

3.4.2. The complex backbone of an extortion ecosystem

The backbone of an extortion ecosystem is partially crafted by several tools of psychological manipulation. The tools regularly observed among threat group are the following: lying, intimidation, isolation and subduing.

The malicious purpose of exploiting these tools is about persuading victims to do something that attackers want them to do.

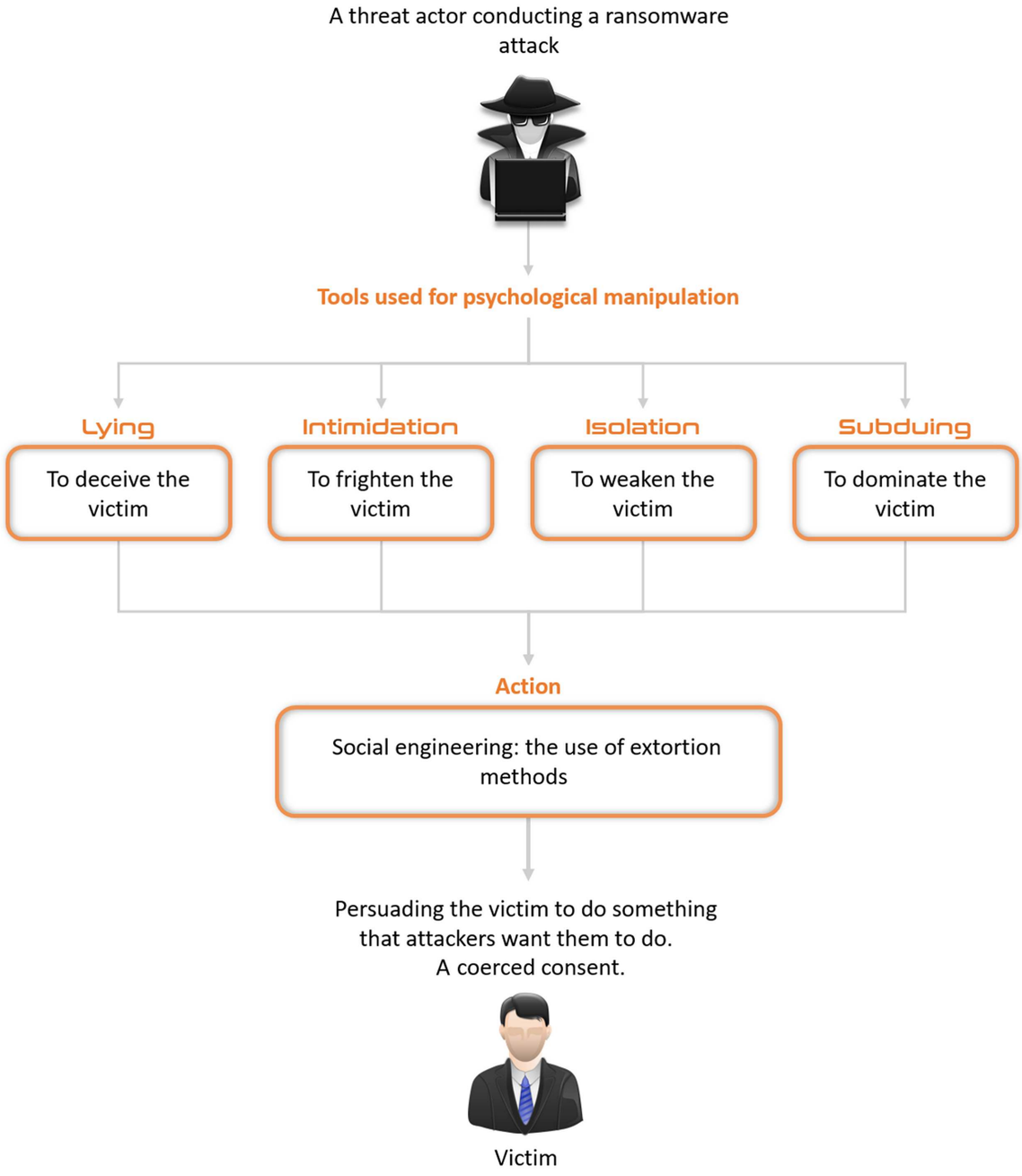


Figure 13. Cyber-psychology infographic (not exhaustive): mental manipulation tools partially constitute the backbone of an extortion ecosystem.

4. OAuth applications : Abusive usage by cybercriminal groups

On 12 december 2023, *Microsoft* warned of the abuse of **OAuth** (Open Authorisation) applications by cybercriminal groups to automate attacks. Several types of attacks have been observed ranging from phishing to the deployment of virtual machines for cryptomining purposes.

4.1. The history of OAuth

OAuth is a protocol that allows one application to interact with another without transmitting passwords. The protocol uses authorisation tokens to prove the identity of consumers and service providers.

It was introduced with *Twitter* in 2007 to enable third-party applications to access the Twitter API without needing user credentials. In 2010, it was *Google*'s turn to offer this service to application publishers. Today, many major companies such as *Amazon*, *Netflix*, *PayPal*, *Microsoft*, *LinkedIn* and *Facebook* provide applications that integrate this protocol.

The use of the **OAuth** protocol would seem to be a guarantee of password security. However, criminal groups continue to improve their techniques and adapt to their environment. Back in 2011, *SANS* already warned of the possible malicious uses of this protocol.

4.2. Use of OAuth applications to deploy virtual machines for cryptomining

Attackers targeted Microsoft user accounts using *phishing* or *password spraying* techniques. However, this initial access phase was not the attackers' ultimate goal, as their aim was to create or modify **OAuth** applications to launch larger-scale attacks.

After compromising an initial Microsoft user account, the Storm-1283 group modified an existing **OAuth** application, assigning it with all the rights needed to deploy virtual machines. These virtual machines enabled the threat actors to mine cryptocurrency. The attackers repeated the procedure to deploy other virtual machines using a new **OAuth** application.

These attacks resulted in costs to targeted organisations ranging from **US$10,000 to US$1.5 million**, depending on the scale and duration of the attack.

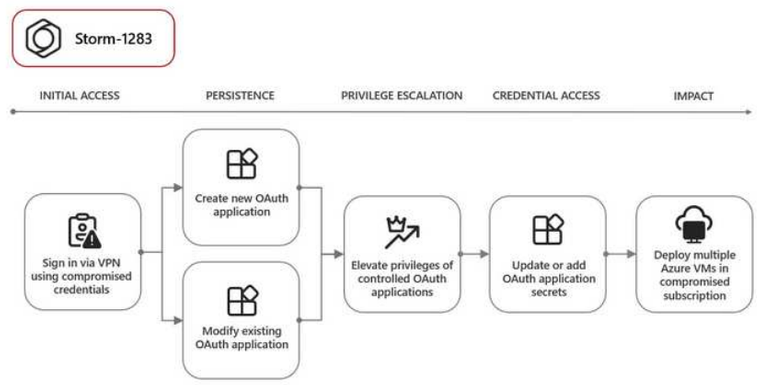


Figure 14. Kill chain of the cryptomining campaigns - Source : Microsoft.

4.3. Use of OAuth applications for phishing and to compromise emails

In their report, *Microsoft*'s security researchers highlight the use compromised **OAuth** applications to launch *phishing* campaigns.

As in the previous campaign, an attacker compromised a Microsoft user account for the initial access. This time, the cybercriminal's objective was not to perform *mining* operations but to carry out phishing attacks with these malicious applications to recover **OAuth** tokens.

The cybercriminal sent a phishing kit from the included email account to several targets in different organisations. This phishing email contained a URL that redirected victims to a *Microsoft* login page. By clicking on this link, users' session cookie tokens are then retrieved by the attacker.

In some cases, the attacker exploited the compromised user account to search mailboxes for financial information. This data is then used in more targeted social engineering campaigns.

4.4. Use of OAuth applications for spamming activities

In its report, *Micosoft* highlights a third campaign linked to the illegitimate use of **OAuth** applications, attributed to the Storm-1286 group.

After compromising an account without multi-factor authentication, cybercriminals added specific rights to **OAuth** applications: *email*, *profile*, *openid*, *Mail.Send*, *User.Read* and *Mail.Read*.

These permissions enabled Storm-1286 to control the compromised email account and send thousands of emails per day. Using a legitimate domain for this type of campaign avoids being blocked by security equipments in charge of detecting phishing and spam e-mails.

In some cases, Storm-1286 waited several months after gaining the initial access and configuring the **OAuth** applications before spamming using these applications.

Microsoft's security researchers are not the only ones to observe the malicious use of **OAuth** in attacks. In fact, as early as January 2023, *Proofpoint* observed campaigns resorting to this abuse.

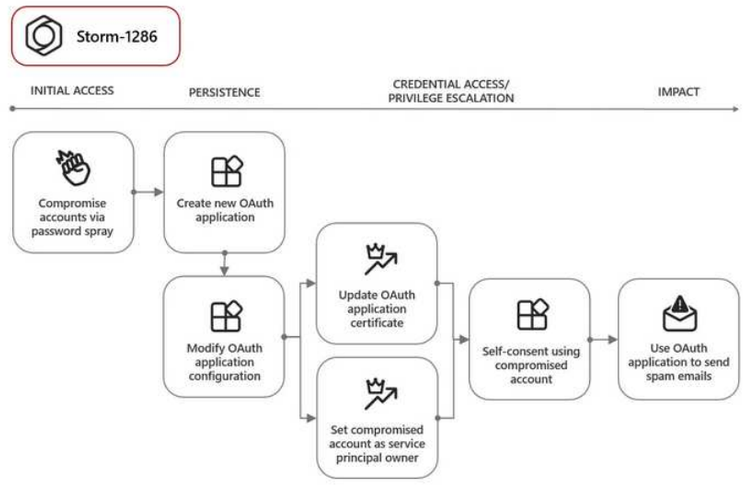


Figure 15. Kill chain of the spamming campaigns - Source : Microsoft.

4.5. Use of malicious OAuth applications

In January 2023, *Proofpoint* researchers discovered a new OiVaVoii campaign involving **OAuth** applications. This campaign targeted corporate CEOs with spear-phishing and personalised lures.

The attackers created **OAuth** applications that met *Microsoft*'s requirements for *verified publisher* status, and thus inspired confidence in the application's users. They then used a compromised Office 365 **OAuth** account to send phishing emails asking users to grant rights to these malicious **OAuth** applications.

The cybercriminals were then able to exfiltrate data, gain access to e-mail accounts and maliciously use legitimate domains.

The *verified publisher* status of an **OAuth** application is not a guarantee of its legitimacy, and vigilance from every user is essential.

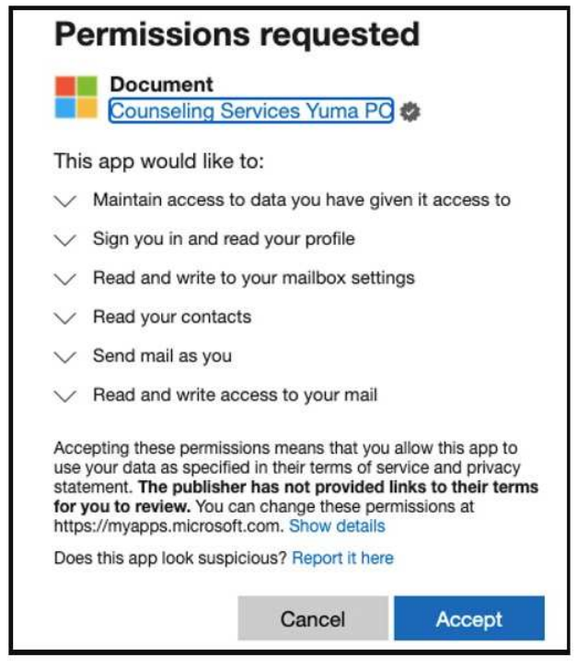


*Figure 16. **OAuth** application using Microsoft's logo and a verified publisher status - Source : ProofPoint.*

4.6. Mitre ATT&CK matrix

INITIAL ACCESS

T1078 Valid Account. T1566 Phishing.

PERSISTENCE

T1098 Account Manipulation.

PRIVILEGE ESCALATION

T1548 Abuse Elevation Control Mechanism. T1134 Access Token Manipulation. T1528 Steal Application Access Token.

CREDENTIAL ACCESS

T1557 Adversary-in-the-Middle. T1110 Brute Force. T1528 Steal Application Access Token.

IMPACT

T1496 Resource Hijacking. T1657 Financial Theft.

4.7. Recommendations

The recommendations for mitigating the risks associated with this *modus operandi* are :

- Implementing multi-factor authentication (MFA)
- Prevent malicious e-mails from reaching users. To do this, mail servers offer security features that can be activated to help detect spam or phishing e-mails.
- Check all applications and permissions to ensure that applications only access necessary data, and that they respect the principles of least privilege access.

4.8. Microsoft 365 Defender detection track

The following rules can be used to ensure the absence of compromise by analysing activity logs:

Detection of suspicious connection attempts

```
IdentityLogonEvents
| where Timestamp > ago(3d)
| where ActionType == "LogonFailed" and LogonType == "OAuth2:Token" and Application == "Microsoft Exchange
Online"
| summarize count(), dcount(IPAddress), dcount(CountryCode) by AccountObjectId, AccountDisplayName,
bin(Timestamp, 1h)
```

Detection of OAuth application creation

```
CloudAppEvents
| where ActionType in ("Add application.", "Add service principal.")
| mvexpand modifiedProperties = RawEventData.ModifiedProperties
| where modifiedProperties.Name == "AppAddress"
| extend AppAddress = tolower(extract('\"Address\": \"(.*)\",',1,tostring(modifiedProperties.NewValue)))
| mvexpand ExtendedProperties = RawEventData.ExtendedProperties
| where ExtendedProperties.Name == "additionalDetails"
| extend OAuthApplicationId = tolower(extract('\"AppId\":\"(.*)\"',1,tostring(ExtendedProperties.Value)))
| project Timestamp, ReportId, AccountObjectId, Application, ApplicationId, OAuthApplicationId, AppAddress
```

5. Sources

Vulnerabilities

- https://nvd.nist.gov/vuln/detail/CVE-2023-49070
- https://lists.apache.org/thread/jmbqk2lp4t4483whzndp5xqlq4f3otg3
- https://nvd.nist.gov/vuln/detail/CVE-2023-6448
- https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf
- https://downloads.unitronicsplc.com/Sites/plc/Visilogic/Version_Changes-Bug_Reports/VisiLogic%209.9.00%20Version%20changes.pdf
- https://nvd.nist.gov/vuln/detail/CVE-2023-47565
- https://www.cisa.gov/news-events/ics-advisories/icsa-23-355-02
- https://www.qnap.com/en/security-advisory/qsa-23-48
- https://www.akamai.com/blog/security-research/qnap-viostor-zero-day-vulnerability-spreading-mirai-patched
- https://www.akamai.com/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days

Ransomware : understanding the extortion ecosystem

- https://www.cloudflare.com/fr-fr/the-net/ransomware-extortion/
- https://fr.wikipedia.org/wiki/Ran%C3%A7ongiciel_en_tant_que_service
- https://www.01net.com/actualites/ransomware-les-pirates-de-blackcat-testent-un-nouveau-moyen-de-pression.html
- https://www.silicon.fr/ransomwares-triple-extorsion-408946.html
- https://en.wikipedia.org/wiki/Vastaamo_data_breach
- https://www.youtube.com/watch?v=htsSaPNgm8s
- https://blog.sucuri.net/2020/04/analyzing-decrypting-l4nc34s-simple-ransomware.html
- https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/
- https://www.01net.com/actualites/ransomware-les-pirates-de-blackcat-testent-un-nouveau-moyen-de-pression.html
- https://www.malwarebytes.com/blog/news/2023/11/ransomware-gang-files-sec-complaint-about-target
- https://www.it-connect.fr/le-gang-de-ransomware-blackcat-denonce-sa-victime-aux-autorites-pour-lui-mettre-la-pression/
- https://www.lemondeinformatique.fr/actualites/lire-le-ransomware-ragnar-locker-s-offre-des-pubs-sur-facebook-81003.html
- https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims
- https://www.databreaches.net/leaked-lockbit-3-0-builder-used-by-bl00dy-ransomware-gang-in-attacks/
- https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

OAuth applications : Abusive usage by cybercriminal groups

- https://www.proofpoint.com/fr/threat-reference/OAuth
- https://www.proofpoint.com/us/blog/cloud-security/dangerous-consequences-threat-actors-abusing-microsofts-verified-publisher
- https://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/
- https://www.sans.org/blog/four-attacks-on-oauth-how-to-secure-your-oauth-implementation/