Monthly Cyber Threat Intelligence report
September 2023

2023-09-30 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

1. Executive summary

This month, aDvens' CERT highlights five noteworthy vulnerabilities in addition to those already published.

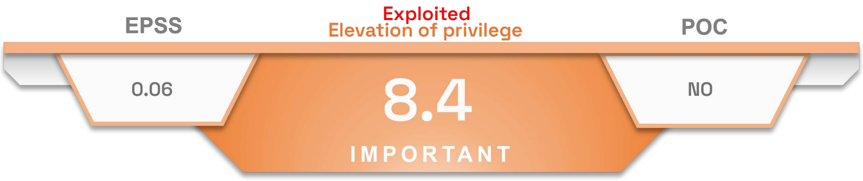
Through two articles, our CTI analysts present analysis of the recent ransomware group AKIRA and the use of a phishing campaign by the cybercriminal group Storm-0324, via the Teams application.This collaborative tool is widely deployed within enterprises.

2. Vulnerabilities

This month, aDvens' CERT highlights five vulnerabilities affecting commonly used technologies (IT/OT) within companies. They are sorted by severity (proofs of concept available, 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. ANDROID - CVE-2023-35674 (Exploited)



Announced in the security bulletin on September 5, 2023, CVE-2023-35674 is a significant vulnerability that impacts the *Android* mobile operating system.

A flaw in the system's configuration allows the execution of a task in the background.

Exploiting this vulnerability enables a local attacker, using crafted requests, to escalate their privileges on the system.

This vulnerability is exploited.

2.1.1. Risk

- Elevation of privilege

2.1.2. Type of vulnerability

- **CWE-371**: State Issues

2.1.3. Severity

Attack vector	Local	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

Android Open Source Project (AOSP)

- Version 11
- Version 12
- Version 12L
- Version 13

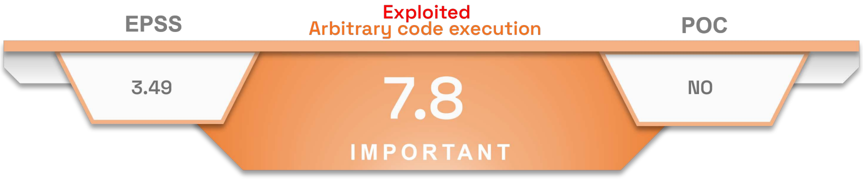
2.1.5. Recommendation

- Apply the update from September 5, 2023.
- Additional information is available on the Android's website.

2.1.6. Proof of concept

No Proof of Concept is available in open sources.

2.2. ACROBAT CVE-2023-26369 (Exploited)



On September 12, 2023, Adobe released security bulletin APSB23-34, highlighting CVE-2023-26369, a critical vulnerability impacting the *Acrobat* software solution. The issue stems from improper data handling while parsing a PDF document. Researchers discovered the potential to inject code beyond allocated space.

A remote attacker can exploit this vulnerability by embedding a payload within a PDF document and persuading the user to open it. Upon opening, the data processing triggers a buffer overflow, enabling the payload to execute on the system.

This vulnerability is exploited.

User interaction is required.

The arbitrary code is executed with the privileges of the user who opened the malicious document.

2.2.1. Risks

- Arbitray code execution
- Denial of service

2.2.2. Type of vulnerability

- **CWE-787** : Out-of-bounds write

2.2.3. Severity

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

2.2.4. Affected products

- Acrobat DC, versions 23.003.20284 and earlier
- Acrobat Reader DC, versions 23.003.20284 and earlier
- Acrobat 2020, versions 20.005.30516 (Mac) and earlier
- Acrobat 2020, versions 20.005.30514 (Windows) and earlier
- Acrobat Reader 2020, versions 20.005.30516 (Mac) and earlier
- Acrobat Reader 2020, versions 20.005.30514 (Windows) and earlier

2.2.5. Recommendation

Apply update

- *Acrobat DC* : update to version 23.006.20320
- *Acrobat Reader DC* : update to version 23.006.20320

- *Acrobat 2020* : update to version 20.005.30524
- *Acrobat Reader 2020* : update to version 20.005.30524

Manual update

- While the *Acrobat* software solution is automatically updated, it is possible to apply patches manually by accessing the **"Help"** menu and selecting **"Check for Updates"**.

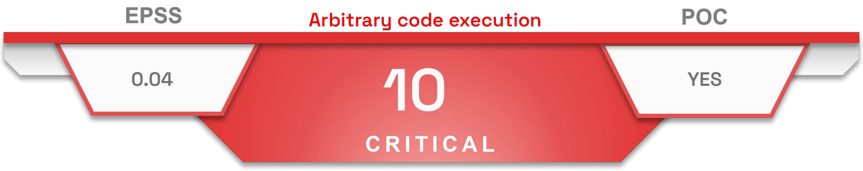
Additional resources

- Additional information can be found on the Adobe's website.
- For Acrobat DC users, Adobe recommends reviewing the Frequently Asked Questions page for in-depth insights.
- Similarly, for Acrobat Reader DC users, Adobe suggests exploring the Frequently Asked Questions (FAQ) page.

2.2.6. Proof of concept

No Proof of Concept is available in open sources.

2.3. MITSUBISHI MELSEC ELECTRIC CVE-2023-1424



EPSS 0.04

Arbitrary code execution

10

CRITICAL

POC YES

Discovered by security researcher Matt Wiseman from the Talos Intelligence Group at Cisco, CVE-2023-1424 is a critical vulnerability impacting several products in the MELSEC IQ-F/IQ-R series.

The researcher identified a buffer overflow flaw.

By exploiting this vulnerability, a remote attacker can send crafted packets to cause a denial of service or execute arbitrary code on the system.

Arbitrary code execution is considered complex. It requires the attacker to have knowledge of the internal structure of the targeted products.

A compromise will require systems to be reset.

2.3.1. Risks

- Arbitray code execution
- Denial of service

2.3.2. Type of vulnerability

- **CWE-119** : Improper Restriction of Operations within the Bounds of a Memory Buffer
- **CWE-120** : Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

2.3.3. Severity

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

2.3.4. Affected products

Products : FX5U-xMy/z x=32, 64, 80, y=T, R, z=ES, DS, ESS, DSS

- Serial number : 17X°°°° or later.
- Versions : from 1.220 to 1.281.

Products : FX5UC-xMy/z x=32, 64, 96, y=T, z=D, DSS

- Serial number : 17X°°°° or later.
- Versions : from 1.220 to 1.281.

Products : FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-T

- Versions : from 1.220 to 1.281.

MELSEC iQ-R series

Products : R00/01/02CPU

- Versions : 35 and prior.

Products : R04/08/16/32/120(EN)CPU

- Versions : from 12 to 68.

Products : R08/16/32/120SFCPU

- Versions : 26 and later.

Products : R08/16/32/120PCPU

- Versions : from 3 to 37.

2.3.5. Recommendation

Fixes

For the MELSEC iQ-F series

Products : FX5U-xMy/z x=32, 64, 80, y=T, R, z=ES, DS, ESS, DSS

- Serial number : 17X°°°° or later.
- Update to version 1.290 or later.

Products : FX5UC-xMy/z x=32, 64 ,96 , y=T, z=D, DSS

- Serial number : 17X°°°° or later.
- Update to version 1.290 or later.

Products : FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS

- Update to version 1.290 or later.

For the MELSEC iQ-R series

Products : R00/01/02CPU

- Update to version 36 or later.

Products : R04/08/16/32/120(EN)CPU

- Update to version 69 or later.

Products : R08/16/32/120PCPU

- Update version 38 or later.

Suggested References:

Mitsubishi provider

- Additonal information is available on the provider's website.

CISA recommends consulting the following documents

- control systems security recommended practices
- Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies
- ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies

2.3.6. Mitigation

- Use vulnerable products within a local network;
- Employ a firewall or a Virtual Private Network (VPN) to restrict access to the local network;
- Implement IP address filtering;
- Restrict physical access to vulnerable products.

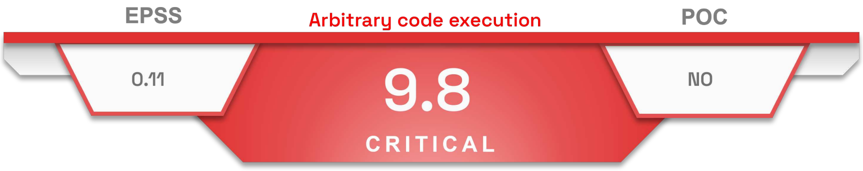
For IP address filtering, additional information is available in the following two documents:

- " *12.1 IP Filter Function* " : User manual MELSEC iQ-F FX5 (Ethernet Communication)
- " *1.13 Security* " - " *IP filter* " : User manual MELSEC iQ-R Ethernet (Application)

2.3.7. Proof of concept

Proof of Concept is available in open sources.

2.4. ACRONIS CVE-2023-41746



Reported on August 31, 2023, in security bulletin SEC-5810, CVE-2023-41746 is a critical vulnerability that affects *Acronis Cloud Manager* for Windows.

The validation of user input data is not performed correctly.

An authenticated attacker can execute arbitrary code on the system with .

By employing crafted requests, an authenticated attacker can execute arbitrary code on the system.

2.4.1. Risk

- Arbitrary code execution

2.4.2. Type of vulnerability

- **CWE-20** : Improper Input Validation

2.4.3. 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

2.4.4. Affected product

- *Acronis Cloud Manager* (Windows), build prior to 6.2.23089.203

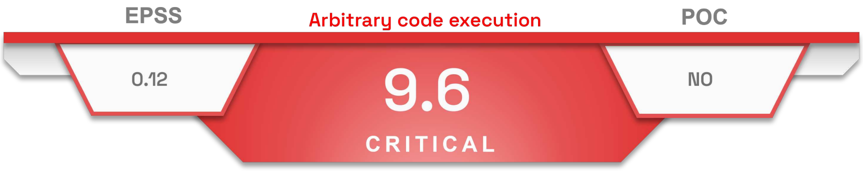
2.4.5. Recommendations

- Update *Acronis Cloud Manager* (Windows) to version 6.2.23089.203 or later.
- Additional information is available on the provider's website.

2.4.6. Proof of concept

No proof of concept is available in open sources.

2.5. GITLAB EE CVE-2023-5009



Discovered by security researcher joaxcar from *HackerOne*, CVE-2023-5009 is a critical vulnerability affecting Gitlab's Enterprise Edition (EE).

The researcher identified inappropriate privilege management within the application. An attacker can exploit scheduled security scan policies to execute a pipeline by impersonating a user.

The risks associated with this cyberattack are manifold. The attacker can compromise data confidentiality, potentially retrieving login credentials or a project's source code. Additionally, the attacker can execute arbitrary code on the vulnerable *Gitlab* instance.

2.5.1. Risks

- Bypass security policy
- Arbitrary code execution
- Impact on confidentiality

2.5.2. Type of vulnerability

- **CWE-269** : Improper Privilege Management

2.5.3. Severity

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

2.5.4. Affected products

Gitlab Enterprise Edition (EE)

- Versions 13.12 and earlier up to 16.2.7
- Versions 16.3 and earlier up to 16.3.4

2.5.5. Recommendations

- Update for GitLab EE to version 16.2.7, 16.3.4, and later.
- Additional information is available on the Gitlab's website.

2.5.6. Proof of concept

No proof of concept is available in open sources.

3. AKIRA

On September 12, 2023, the US Health Sector Cybersecurity Coordination Center (HC3) published an alert report on the newly-formed AKIRA attacker group. Spotted in March of this year, the group already claimed 16 compromised victims. Currently, AKIRA has claimed around sixty victims, including 45 in the United States alone, with significant ransom demands ranging from 200,000 to 4 million US dollars. The most targeted sectors are industry, finance, health and real estate.

3.1. The AKIRA ransomware

This group must not be confused with another ransomware also named Akira, active since 2017, which is not linked to this new group of eponymous attackers.

The newcomer has two variants:

- The Windows variant is a 64-bit binary developed in C++ and delivers a symmetric key encrypted with RSA-4096 encryption,
- The Linux variant targets VMware ESXi servers and uses the Crypto++ library.

The group conducts its initial access with compromised valid credentials, possibly purchased on the Dark Web. However, other vectors of compromise (phishing emails, malicious websites or Trojan horses) cannot be excluded.

Once deployed, the malware deletes Shadow Copies with the following command *via* PowerShell:

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

Once encryption is started, it will spare the files contained in the winnt, temp, thumb, Recycle Bin, System Volume Information, Boot, ProgramData, Windows and Trend Micro folders. Likewise, files with the following extensions are excluded from encryption: .exe, .lnk, .dll, .msi and .sys and akira_readme.txt. Everything else is encrypted with the .akira extension.

The malware uses the Windows Restart Manager API to close any active process or service that would keep a file open. The ransomware performs a memory dump of the LSASS, carried out with Mimikatz, then continues to lateralize itself.

Akira is the first group to use RustDesk, an open-source remote access tool, to navigate its victims' networks. As RustDesk is a legitimate tool, this stealth access does not raise any alarms on compromised networks. Furthermore, attackers enable RDP access on servers, and inhibit security devices by disabling Windows Defender and the Windows firewall.

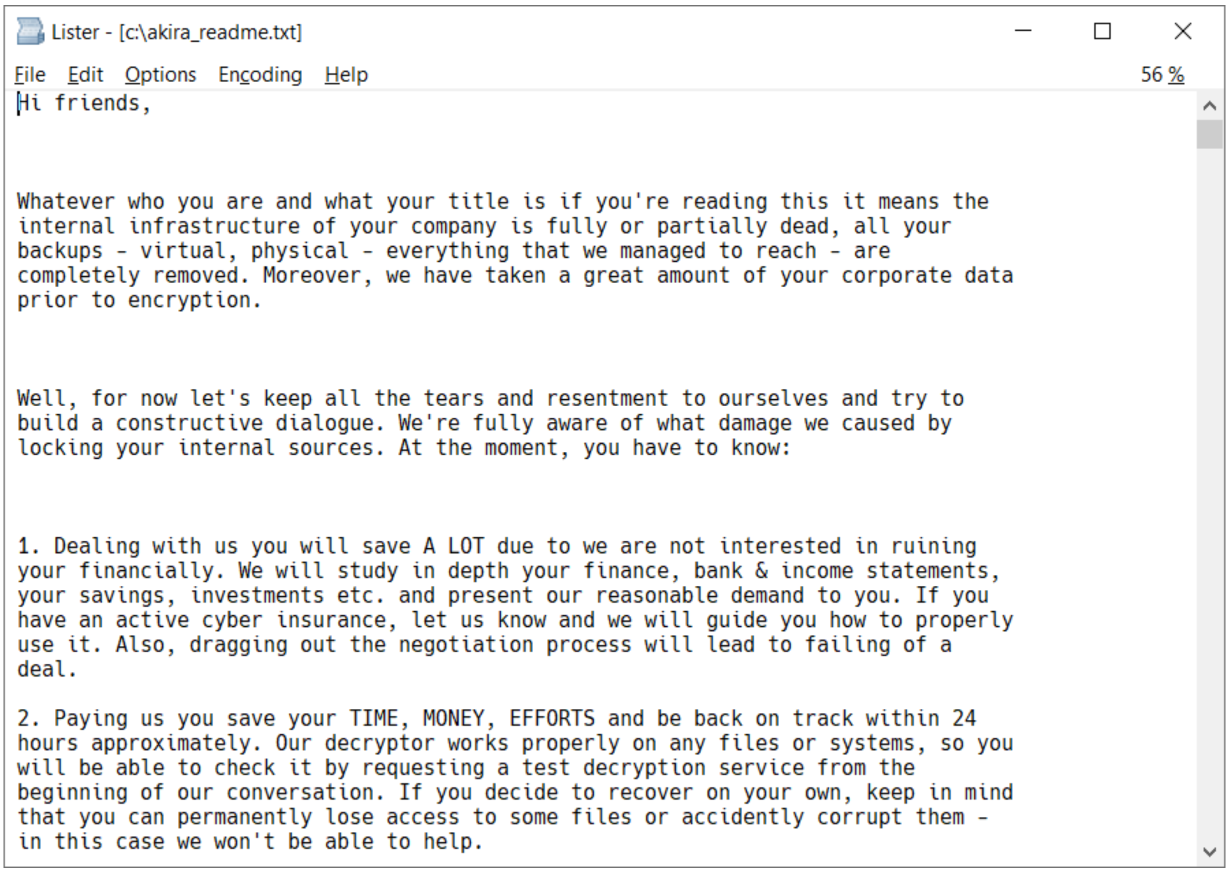
3.2. The AKIRA gang

Security researchers are now pointing to strong similarities between Akira and the Conti group (formerly Ryuk).

The cryptocurrency portfolio models are the same as those previously used by the leading operators of Conti. Additionally, source code samples in malware from both groups show strong analogies, such as the encryption algorithm ChaCha2008, or directories excluded from encryption, such as winnt and Trend Micro.

As a reminder, the Conti group had pledged allegiance to Russia following the offensive in Ukraine in early 2022. In retaliation, the group suffered a significant data leak in February 2022, exfiltrated by one of its own members. The group subsequently fragmented between supports for Russia and Ukraine. All these concordances suggest that the Akira group has its origins in the breakup of Conti, of which it is an emanation.

As such, the ransom note is written in English but contains grammatical errors:

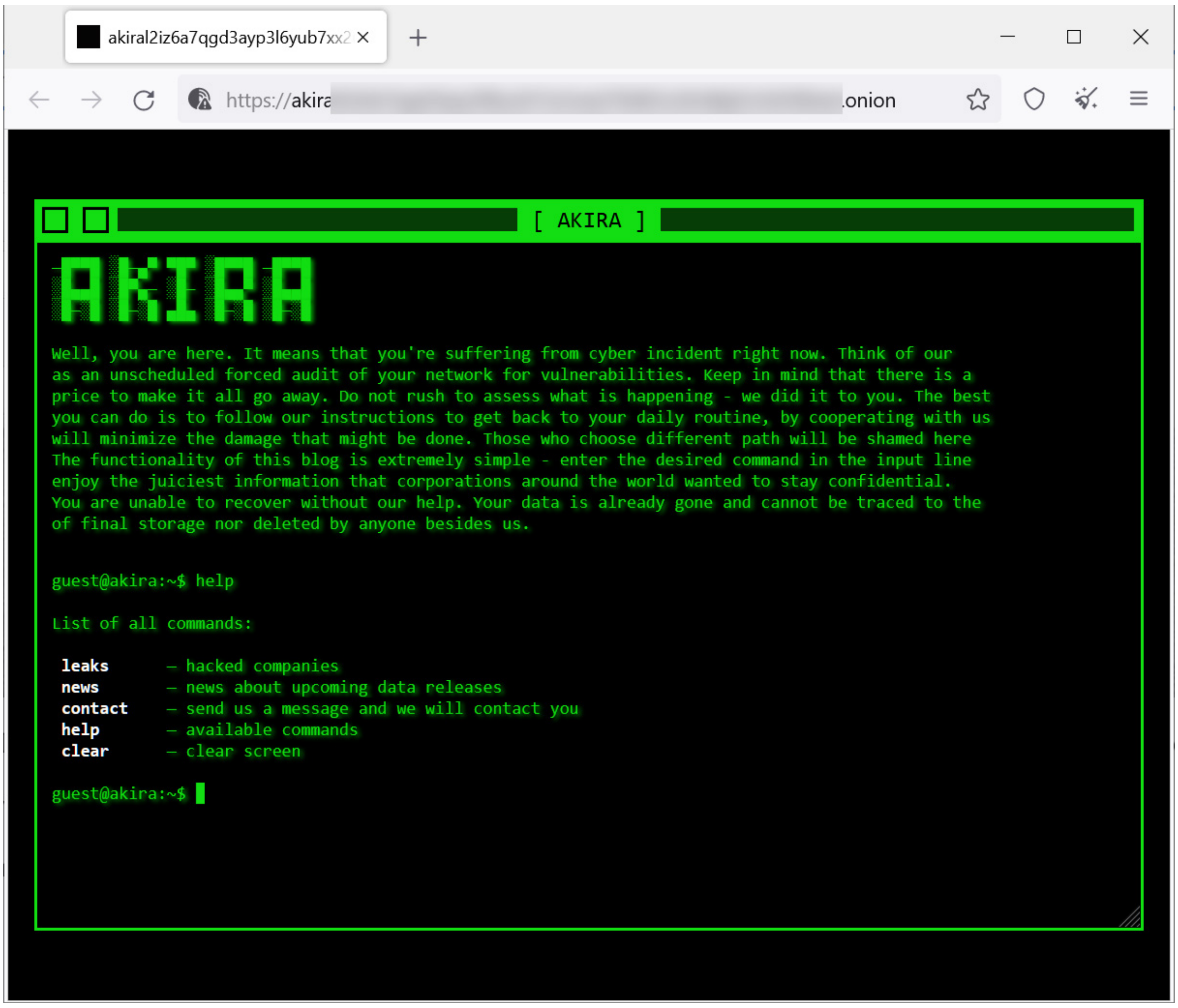

Lister - [c:\akira_readme.txt]
File Edit Options Encoding Help
56 %

```
Hi friends,


Whatever who you are and what your title is if you're reading this it means the
internal infrastructure of your company is fully or partially dead, all your
backups - virtual, physical - everything that we managed to reach - are
completely removed. Moreover, we have taken a great amount of your corporate data
prior to encryption.


Well, for now let's keep all the tears and resentment to ourselves and try to
build a constructive dialogue. We're fully aware of what damage we caused by
locking your internal sources. At the moment, you have to know:


1. Dealing with us you will save A LOT due to we are not interested in ruining
your financially. We will study in depth your finance, bank & income statements,
your savings, investments etc. and present our reasonable demand to you. If you
have an active cyber insurance, let us know and we will guide you how to properly
use it. Also, dragging out the negotiation process will lead to failing of a
deal.

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24
hours approximately. Our decryptor works properly on any files or systems, so you
will be able to check it by requesting a test decryption service from the
beginning of our conversation. If you decide to recover on your own, keep in mind
that you can permanently lose access to some files or accidently corrupt them -
in this case we won't be able to help.
```

Figure 1. AKIRA ransom note (source : Bleeping Computer).

The ransom note invites visitors to go to Akira's .onion website to negotiate with the group *via* a unique password. Additionally, this ransom note also offers the victim a so-called full security audit of their system, to inform them of exploited vulnerabilities.

Akira also stands out with the design of its website, designed like an 80s site, in which visitors can navigate by executing commands:

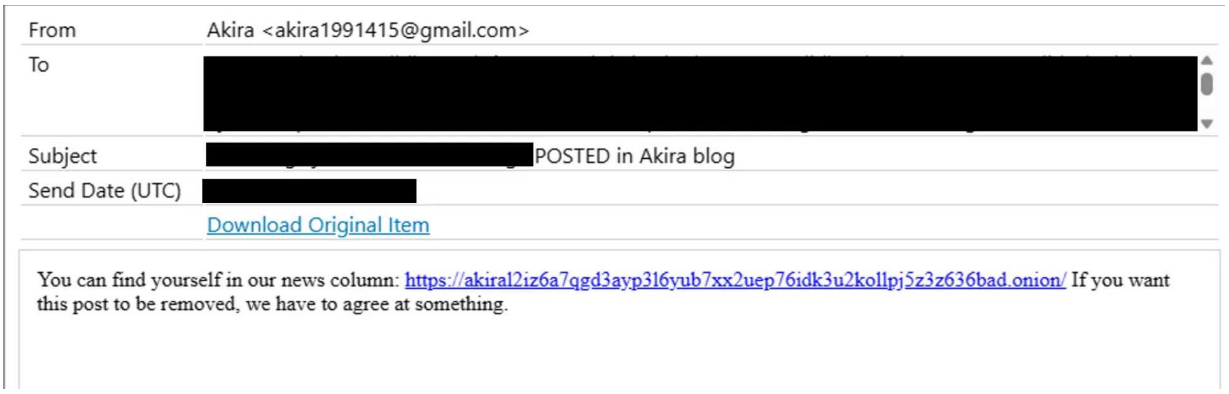


```
Well, you are here. It means that you're suffering from cyber incident right now. Think of our
as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
price to make it all go away. Do not rush to assess what is happening - we did it to you. The best
you can do is to follow our instructions to get back to your daily routine, by cooperating with us
will minimize the damage that might be done. Those who choose different path will be shamed here
The functionality of this blog is extremely simple - enter the desired command in the input line
enjoy the juiciest information that corporations around the world wanted to stay confidential.
You are unable to recover without our help. Your data is already gone and cannot be traced to the
of final storage nor deleted by anyone besides us.


guest@akira:~$ help

List of all commands:

 leaks       - hacked companies
 news        - news about upcoming data releases
 contact     - send us a message and we will contact you
 help        - available commands
 clear       - clear screen

guest@akira:~$
```

Figure 2. AKIRA's Website (source : Bleeping Computer).

The group is now following the trend of its counterparts and practicing triple extortion:

- Encryption of the target's information system,
- Exfiltration and publication of part of the data,
- Contacting the victim's customers and partners to inform them of the attack.



From	Akira <akira1991415@gmail.com>
To	[redacted]
Subject	[redacted] POSTED in Akira blog
Send Date (UTC)	[redacted]
	Download Original Item

You can find yourself in our news column: https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/ If you want this post to be removed, we have to agree at something.

Figure 3. Contact from akira1991415@gmail[.]com address (source: TrueSec).

We can note that despite its doctrine of triple extortion, Akira is still innovating by offering double pricing. Indeed, the victim can choose:

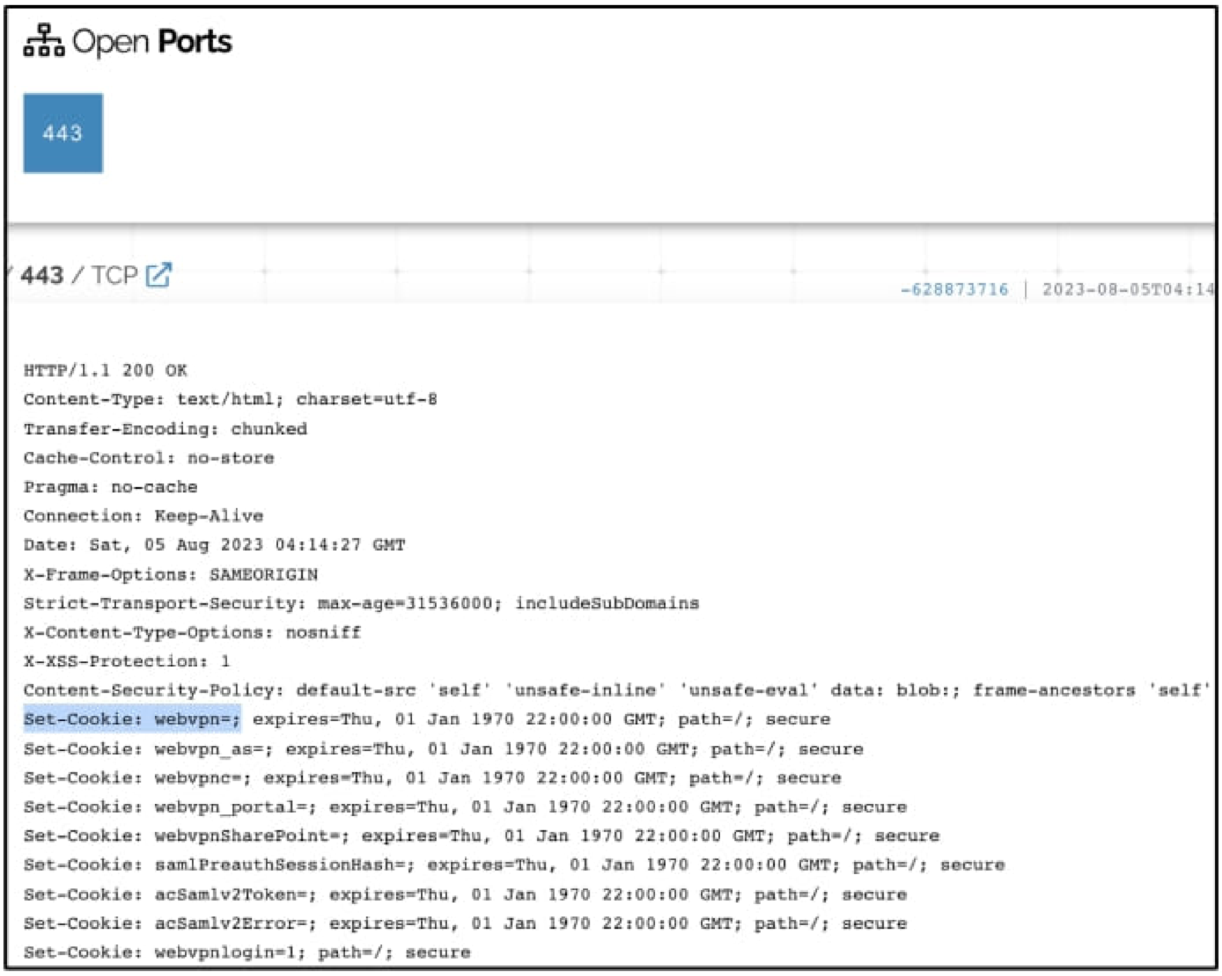
- Either pay the ransom to lift the encryption,
- Or to pay a lower price to remove access to their data exfiltrated and made public.

3.3. Group campaign targeting Cisco VPN access

During a campaign on May 2023, the group exploited the CVE-2023-20269 vulnerability to specifically target Cisco VPNs from organizations that do not have multi-factor authentication (MFA) in place.

The group used valid, compromised Cisco accounts to infiltrate networks without deploying backdoors or persistence mechanisms. At this stage, it is still unknown whether these Cisco identifiers were brut-forced or purchased.

Cisco confirmed on August 24, 2023 that its VPN gateways had indeed been used as vectors of compromise. This approach, observed in 8 different attacks, indicates an attack strategy led by Akira group.



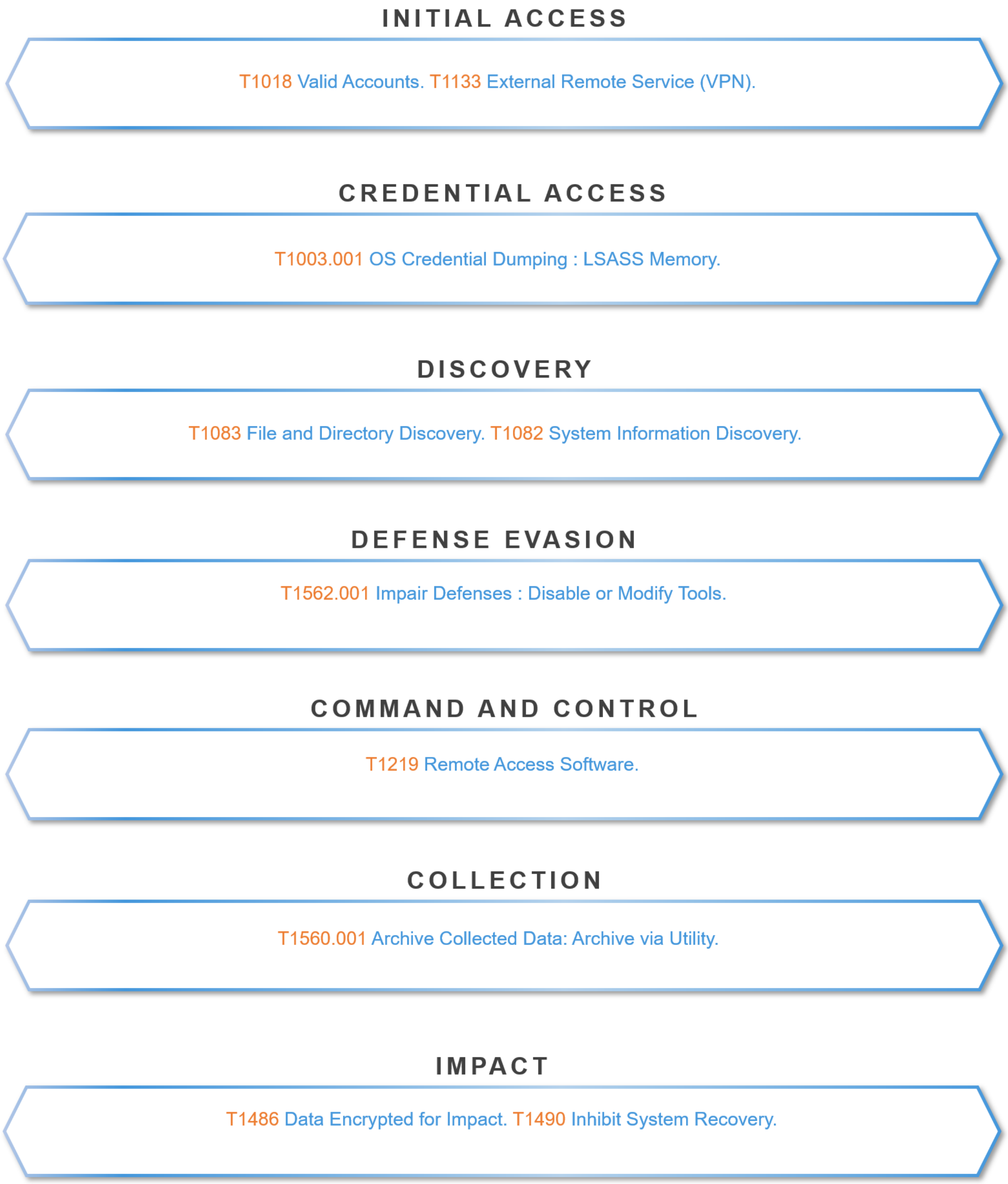
443 / TCP

-628873716 | 2023-08-05T04:14

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Cache-Control: no-store
Pragma: no-cache
Connection: Keep-Alive
Date: Sat, 05 Aug 2023 04:14:27 GMT
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data: blob:; frame-ancestors 'self'
Set-Cookie: webvpn=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpn_as=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpnc=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpn_portal=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpnSharePoint=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: samlPreauthSessionHash=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: acSamlv2Token=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: acSamlv2Error=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpnlogin=1; path=/; secure
```

Figure 4. Cisco VPN features observed in attacks (source: SentinelOne).

3.4. MITER ATT&CK Matrix



INITIAL ACCESS

T1018 Valid Accounts. T1133 External Remote Service (VPN).

CREDENTIAL ACCESS

T1003.001 OS Credential Dumping : LSASS Memory.

DISCOVERY

T1083 File and Directory Discovery. T1082 System Information Discovery.

DEFENSE EVASION

T1562.001 Impair Defenses : Disable or Modify Tools.

COMMAND AND CONTROL

T1219 Remote Access Software.

COLLECTION

T1560.001 Archive Collected Data: Archive via Utility.

IMPACT

T1486 Data Encrypted for Impact. T1490 Inhibit System Recovery.

Figure 5. AKIRA's MITRE ATT&CK.

3.5. IOCs

TLP	TYPE	VALUE
TLP:CLEAR	SHA256	5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
TLP:CLEAR	SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
TLP:CLEAR	SHA256	678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
TLP:CLEAR	SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
TLP:CLEAR	SHA256	8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
TLP:CLEAR	SHA256	1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
TLP:CLEAR	SHA256	9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163
TLP:CLEAR	SHA256	d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959
TLP:CLEAR	SHA256	6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
TLP:CLEAR	SHA256	1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
TLP:CLEAR	Courriel	akira1991415[at]gmail[.]com

3.6. YARA detection rules

```
[TLP:WHITE] win_akira_auto (20230715 | Detects win.akira.)

rule win_akira_auto {

    meta:
        author = "Felix Bilstein - yara-signator at cocacoding dot com"
        date = "2023-07-11"
        version = "1"
        description = "Detects win.akira."
        info = "autogenerated rule brought to you by yara-signator"
        tool = "yara-signator v0.6.0"
        signator_config = "callsandjumps;datarefs;binvalue"
        malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.akira"
        malpedia_rule_date = "20230705"
        malpedia_hash = "42d0574f4405bd7d2b154d321d345acb18834a41"
        malpedia_version = "20230715"
        malpedia_license = "CC BY-SA 4.0"
        malpedia_sharing = "TLP:WHITE"

    /* DISCLAIMER
     * The strings used in this rule have been automatically selected from the
     * disassembly of memory dumps and unpacked files, using YARA-Signator.
     * The code and documentation is published here:
     * https://github.com/fxb-cocacoding/yara-signator
     * As Malpedia is used as data source, please note that for a given
     * number of families, only single samples are documented.
     * This likely impacts the degree of generalization these rules will offer.
     * Take the described generation method also into consideration when you
     * apply the rules in your use cases and assign them confidence levels.
     */


    strings:
        $sequence_0 = { 4d3bca 7223 49893b 41c7430802000000 41c6431001 e9???????? b8ffffffff }
            // n = 7, score = 100
            //   4d3bca               | mov                 dword ptr [esp + 0x20], ebp
            //   7223                 | inc                 ecx
            //   49893b               | sub                 dh, bh
            //   41c7430802000000     | imul                ebp, edi
            //   41c6431001           | inc                 eax
            //   e9????????           |
            //   b8ffffffff           | movsx               eax, dh

        $sequence_1 = { e8???????? 4c8bc0 488bd3 488d4c2440 e8???????? 488d154de80600 488d4c2440 }
            // n = 7, score = 100
            //   e8????????           |
            //   4c8bc0               | dec                 eax
            //   488bd3               | sub                 esp, ecx
            //   488d4c2440           | dec                 eax
            //   e8????????           |
            //   488d154de80600       | lea                 ebx, [esp + 0x50]
            //   488d4c2440           | dec                 eax

        $sequence_2 = { 488d8597010000 4c8bc7 0f1f840000000000 49ffc0 6642833c4000 75f5 488d9597010000 }
            // n = 7, score = 100
            //   488d8597010000       | dec                 eax
            //   4c8bc7               | mov                 eax, dword ptr [ebp - 8]
            //   0f1f840000000000     | dec                 eax
            //   49ffc0               | mov                 ebx, dword ptr [eax + 0x88]
            //   6642833c4000         | dec                 eax
            //   75f5                 | mov                 eax, dword ptr [ebp - 0x20]
            //   488d9597010000       | dec                 eax

        $sequence_3 = { 742c 4c8bc6 488d15fbf80400 488bcf e8???????? 488d55c0 48837dd810 }
            // n = 7, score = 100
            //   742c                 | dec                 eax
            //   4c8bc6               | mov                 edi, eax
            //   488d15fbf80400       | jmp                 0x3c2
            //   488bcf               | dec                 ecx
            //   e8????????           |
            //   488d55c0             | mov                 edi, ebp
            //   48837dd810           | dec                 eax

        $sequence_4 = { 488bd9 488bc2 488d0d45550400 0f57c0 488d5308 48890b 488d4808 }
            // n = 7, score = 100
            //   488bd9               | mov                 edi, dword ptr [edi + 8]
            //   488bc2               | dec                 eax
            //   488d0d45550400       | test                edi, edi
            //   0f57c0               | jne                 0x4f
            //   488d5308             | dec                 eax
            //   48890b               | mov                 edi, dword ptr [ebp - 0x79]
            //   488d4808             | dec                 eax

        $sequence_5 = { 488d542420 e8???????? 8bf8 85c0 750d f744243010000000 0f95c3 }
            // n = 7, score = 100
            //   488d542420           | test                edi, edi
            //   e8????????           |
            //   8bf8                 | jne                 0x649
            //   85c0                 | mov                 edx, dword ptr [esp + 0x3b8]
            //   750d                 | cmp                 edx, 0x3b9aca00
            //   f744243010000000     | dec                 eax
            //   0f95c3               | lea                 eax, [esp + 0x50]

        $sequence_6 = { 488b842430010000 668910 4c892b e8???????? eb7a 0f1f00 488d4b28 }
            // n = 7, score = 100
            //   488b842430010000     | add                 edx, ecx
            //   668910               | dec                 eax
            //   4c892b               | sar                 edx, 6
            //   e8????????           |
            //   eb7a                 | dec                 eax
            //   0f1f00               | mov                 eax, edx
            //   488d4b28             | dec                 eax

        $sequence_7 = { 0f57c0 0f118580110000 0f57c9 660f7f8d90110000 488d85d9010000 4c8bc7 660f1f440000 }
            // n = 7, score = 100
            //   0f57c0               | mov                 eax, edi
            //   0f118580110000       | nop                 dword ptr [eax + eax]
            //   0f57c9               | dec                 ecx
            //   660f7f8d90110000     | inc                 eax
            //   488d85d9010000       | movups              xmmword ptr [ebp + 0xfc0], xmm0
            //   4c8bc7               | xorps               xmm1, xmm1
            //   660f1f440000         | movdqa              xmmword ptr [ebp + 0xfd0], xmm1

        $sequence_8 = { 4688840da5000000 49ffc1 4983f90a 72a1 0f57c0 0f1185c00c0000 0f57c9 }
            // n = 7, score = 100
            //   4688840da5000000     | cmp                 ecx, dword ptr [eax]
            //   49ffc1               | jne                 0xd18
            //   4983f90a             | dec                 eax
            //   72a1                 | add                 eax, 2
            //   0f57c0               | dec                 ecx
            //   0f1185c00c0000       | sub                 edx, esp
            //   0f57c9               | jne                 0xcc9

        $sequence_9 = { 6666660f1f840000000000 420fb68c0d84000000 83e955 446bc11f b809040281 41f7e8 }
            // n = 6, score = 100
            //   6666660f1f840000000000     | dec    ecx
            //   420fb68c0d84000000    | inc    eax
            //   83e955               | inc                 dx
            //   446bc11f             | cmp                 dword ptr [eax + eax*2], 0
            //   b809040281           | movdqa              xmmword ptr [ebp + 0x1070], xmm1
            //   41f7e8               | dec                 eax

    condition:
        7 of them and filesize < 1219584
}
```

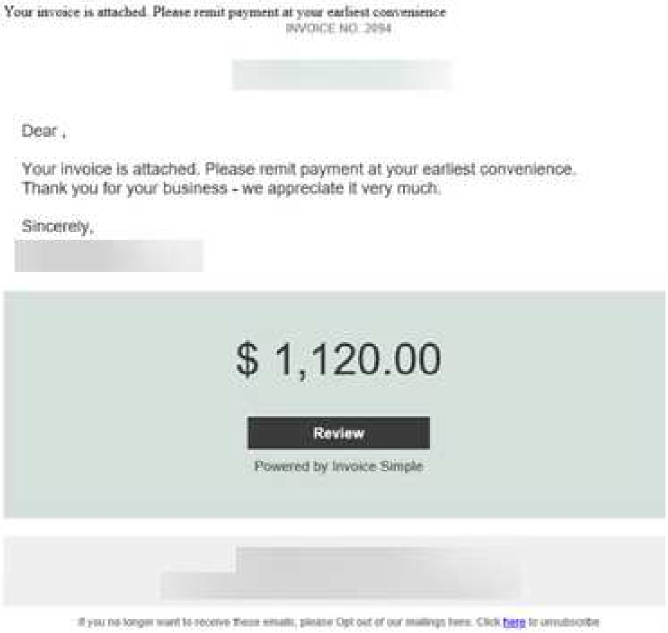
4. Storm-0324: Phishing via Microsoft Teams

On September 12, 2023, Microsoft's Threat Hunting team officially reported on a new cybercriminal group called Storm-0324 (aka TA543 or Sagrid). This group is known to specialize in the resale of access brokers obtained through phishing e-mails. Microsoft's report focuses on a new attack modus operandi used by this group, phishing via Microsoft Teams.

4.1. Background

Investigations into Storm-0324 confirm that, in recent years, this actor has enabled the deployment of several malicious tools such as Clop, Mazeet, REvil ransomware, JSSLoader and Trickbot - the latter being used in the early stages of the Sangria Tempest (FIN7) ransomware attack - or the Gootkit and Dridex Trojans. The Gozi infostealer and the Nymaim malware are also part of the Storm-0324 arsenal.

Most of the initial access needed to deploy these malicious tools is obtained via targeted phishing operations. The Storm-0324 malware relies on traffic distribution systems (TDS) such as BlackTDS and Keitaro to evade detection by filtering and protection solutions. The contents of phishing e-mails are generally of a professional nature, inviting the victim to click on a link to a supposed document management service such as Docusign or Quickbooks.



Your invoice is attached. Please remit payment at your earliest convenience
INVOICE NO: 2094

Dear ,

Your invoice is attached. Please remit payment at your earliest convenience.
Thank you for your business - we appreciate it very much.

Sincerely,

$ 1,120.00

Review

Powered by Invoice Simple

If you no longer want to receive these emails, please Opt out of our mailings here. Click here to unsubscribe

Figure 6. Storm-0324 Phishing Mail - Source: Microsoft

Victims are ultimately redirected to a SharePoint server hosting a malicious compressed file in Microsoft Office documents, Windows Script File (WSF), Epika or VBScript format, containing a JavaScript code that finally triggers the download of the payload to the victim's workstation by exploiting the CVE-2023-21715.

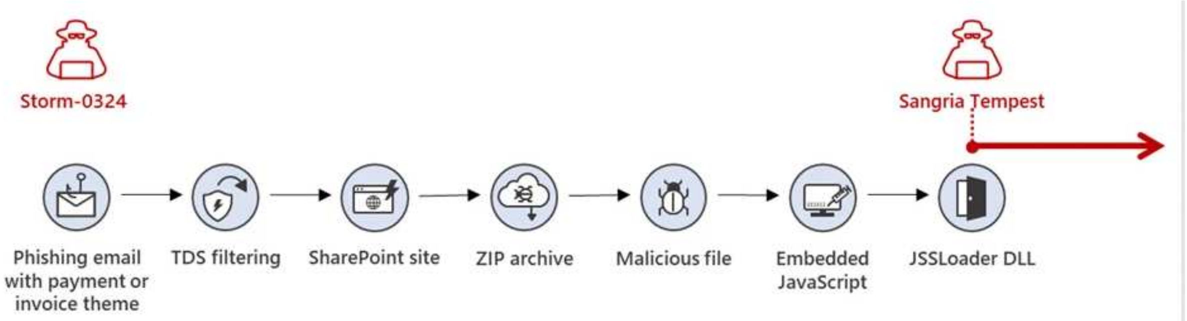
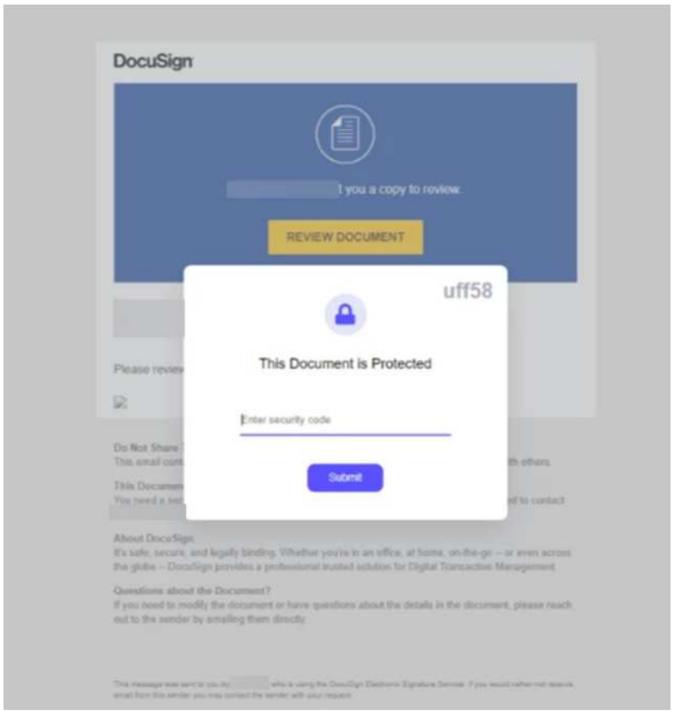


Figure 7. JSSLoader infection chain by Storm-0324 - Source : Microsoft

Storm-0324 is currently applying this MOA to the implementation of the Sangria Tempest ransomware, deploying JSSLoader as a payload. It should be noted that some phishing e-mails can be personalized by adding codes or passwords "securing" the redirection to the malicious document. This trick not only reduces the victim's vigilance, but also blocks analysis of the document hidden behind the link.



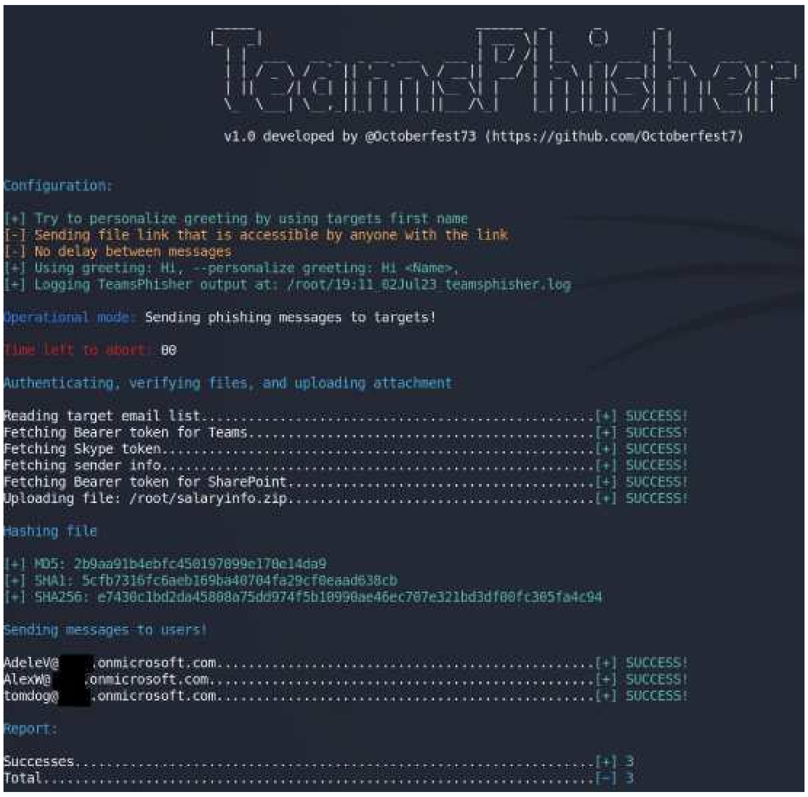
It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management.

If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly.

Figure 8. Authentication request - Phishing - Source : Microsoft

4.2. New MOA

The first observations of this new MOA date back to July 2023. The previously exposed infection chain is modified: redirect links leading to a malicious file hosted on SharePoint are now shared on Microsoft Teams. This change in modus operandi is accompanied by the use of a new Python tool named TeamsPhisher, enabling attachments to be added to messages intended for Teams users whose organizations authorize external communications.



```
                              TeamsPhisher
         v1.0 developed by @Octoberfest73 (https://github.com/Octoberfest7)

Configuration:

[+] Try to personalize greeting by using targets first name
[-] Sending file link that is accessible by anyone with the link
[-] No delay between messages
[+] Using greeting: Hi, --personalize greeting: Hi <Name>,
[+] Logging TeamsPhisher output at: /root/19:11_02Jul23_teamsphisher.log

Operational mode: Sending phishing messages to targets!

Time left to abort: 00

Authenticating, verifying files, and uploading attachment

Reading target email list...............................................[+] SUCCESS!
Fetching Bearer token for Teams.........................................[+] SUCCESS!
Fetching Skype token....................................................[+] SUCCESS!
Fetching sender info....................................................[+] SUCCESS!
Fetching Bearer token for SharePoint....................................[+] SUCCESS!
Uploading file: /root/salaryinfo.zip....................................[+] SUCCESS!

Hashing file

[+] MD5: 2b9aa91b4ebfc450197099e170e14da9
[+] SHA1: 5cfb7316fc6aeb169ba40704fa29cf0eaad638cb
[+] SHA256: e7430c1bd2da45808a75dd974f5b10990ae46ec707e321bd3df00fc305fa4c94

Sending messages to users!

AdeleV@[redacted].onmicrosoft.com.......................................[+] SUCCESS!
AlexW@[redacted].onmicrosoft.com........................................[+] SUCCESS!
tomdog@[redacted].onmicrosoft.com.......................................[+] SUCCESS!

Report:

Successes...............................................................[+] 3
Total...................................................................[-] 3
```

Figure 9. TeamsPhisher Console - source : Github

In response to this new tactic, Microsoft has made a number of updates to its Teams solution, including visually highlighting the fact that a user is from outside an organization, allowing users to be blocked in one-to-one conversations, and notifying administrators of the creation of new domains within their networks.

4.3. Conclusion

This new modus operandi adopted by Storm-0324 once again illustrates the adaptability of cybercriminals in the race for initial access.

The detection of any compromise by the Storm-0324 group is all the more important as the initial access obtained in the targeted system is then offered for sale, thus multiplying the possibility of it being exploited by a ransomware group.

4.4. Recommandations

In the face of these phishing attempts via Microsoft Teams, several recommendations can be applied to reduce this threat:

- Set up and, if possible, disable external access in Microsoft Teams.
- Set up multi-factor authentication for access to Microsoft Teams.
- Reinforce employee awareness of phishing and social engineering techniques.
- Block the execution of Javascript or Bscript content from downloads.

Further recommendations are available on the Microsoft blog. To protect against this new threat, the Microsoft team is providing a query to detect potentially shared files using TeamsPhisher.

The request must be modified with the personal SharePoint domain name ("mysharepointname").

```
let allowedSharepointDomain = pack_array(
'mysharepointname' //customize Sharepoint domain name and add more domains as needed for your query
);
//
let executable = pack_array(
'exe',
'dll',
'xll',
'msi',
'application'
);
let script = pack_array(
'ps1',
'py',
'vbs',
'bat'
);
let compressed = pack_array(
'rar',
'7z',
'zip',
'tar',
'gz'
);
//
let startTime = ago(1d);
let endTime = now();
DeviceFileEvents
| where Timestamp between (startTime..endTime)
| where ActionType =~ 'FileCreated'
| where InitiatingProcessFileName has 'teams.exe'
    or InitiatingProcessParentFileName has 'teams.exe'
| where InitiatingProcessFileName !has 'update.exe'
    and InitiatingProcessParentFileName !has 'update.exe'
| where FileOriginUrl has 'sharepoint'
    and FileOriginReferrerUrl has_any ('sharepoint', 'teams.microsoft')
| extend fileExt = tolower(tostring(split(FileName,'.')[-1]))
| where fileExt in (executable)
    or fileExt in (script)
    or fileExt in (compressed)
| extend fileGroup = iff( fileExt in (executable),'executable','')
| extend fileGroup = iff( fileExt in (script),'script',fileGroup)
| extend fileGroup = iff( fileExt in (compressed),'compressed',fileGroup)
//
| extend sharePoint_domain = tostring(split(FileOriginUrl,'/')[2])
| where not (sharePoint_domain has_any (allowedSharepointDomain))
```

```
 | project-reorder Timestamp, DeviceId, DeviceName, sharePoint_domain, FileName, FolderPath, SHA256,
FileOriginUrl, FileOriginReferrerUrl
```

4.5. JSS Loader IoCs

TLP	TYPE	VALUE
TLP:CLEAR	SHA256	dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d
TLP:CLEAR	C2 Domain	bikweb[.]com
TLP:CLEAR	SHA256	a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044
TLP:CLEAR	C2 Domain	monusorge[.]com
TLP:CLEAR	SHA256	7a17ef218eebfdd4d3e70add616adcd5b78105becd6616c88b79b261d1a78fdf
TLP:CLEAR	C2 Domain	injuryless[.]com

5. Sources

GOOGLE ANDROID CVE-2023-35674

- https://exchange.xforce.ibmcloud.com/vulnerabilities/265268
- https://www.cybersecurity-help.cz/vdb/SB2023090551
- https://nvd.nist.gov/vuln/detail/CVE-2023-35674
- https://source.android.com/docs/security/bulletin/2023-09-01?hl=fr
- https://vuldb.com/?id.239439

ACROBAT CVE-2023-26369

- https://exchange.xforce.ibmcloud.com/vulnerabilities/265786
- https://www.cybersecurity-help.cz/vdb/SB2023091235
- https://nvd.nist.gov/vuln/detail/CVE-2023-26369
- https://helpx.adobe.com/security/products/acrobat/apsb23-34.html

MITSUBISHI MELSEC ELECTRIC CVE-2023-1424

- https://exchange.xforce.ibmcloud.com/vulnerabilities/256027
- https://www.cybersecurity-help.cz/vdb/SB2023052433
- https://nvd.nist.gov/vuln/detail/CVE-2023-1424
- https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-003_en.pdf
- https://www.talosintelligence.com/vulnerability_reports/TALOS-2023-1727
- https://www.cisa.gov/news-events/ics-advisories/icsa-23-143-03
- https://www.mitsubishielectric.com/fa/download/index.html
- https://www.cisa.gov/resources-tools/resources/ics-recommended-practices
- https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- https://www.cisa.gov/news-events/news/targeted-cyber-intrusion-detection-and-mitigation-strategies-update-b

ACRONIS CVE-2023-41746

- https://exchange.xforce.ibmcloud.com/vulnerabilities/264925
- https://nvd.nist.gov/vuln/detail/CVE-2023-41746
- https://vuldb.com/fr/?id.238525
- https://security-advisory.acronis.com/advisories/SEC-5810
- https://security-advisory.acronis.com/updates/UPD-2303-79b2-e072

GITLAB CVE-2023-5009

- https://exchange.xforce.ibmcloud.com/vulnerabilities/266347
- https://nvd.nist.gov/vuln/detail/CVE-2023-5009
- https://www.cybersecurity-help.cz/vdb/SB2023092502
- https://thesecmaster.com/how-to-fix-cve-2023-5009-a-critical-vulnerability-in-gitlab-scan-execution-policies/

AKIRA

- https://www.hhs.gov/sites/default/files/akira-ransomware-sector-alert-tlpclear.pdf
- https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/
- https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/
- https://www.bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/
- https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication
- https://www.truesec.com/hub/blog/a-victim-of-akira-ransomware
- https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/
- https://malpedia.caad.fkie.fraunhofer.de/details/win.akira

Storm-0324: Phishing via Microsoft Teams

- https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/
- https://www.bleepingcomputer.com/news/security/microsoft-notorious-fin7-hackers-return-in-clop-ransomware-attacks/
- https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#ELBRUS
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715?ocid=magicti_ta_support