# Threat Highlight Report

August 2023

WITH secure

# Contents

# Foreword

WithSecure’s monthly threat highlights report contains our own proprietary data, as well as other carefully curated sources from the wider cybersecurity industry. It is designed to serve as a single-source product, providing an overview of this month’s cybersecurity news, the changing threat landscape, and relevant advice.

This month we look at new vulnerabilities in Ivanti products, some of which are being actively exploited by a highly sophisticated threat actor. We also examine an affiliate campaign which installs a malicious “Digital Pulse” proxy, the exploitation of WinRAR, and as always, we assess the changing hacktivist landscape.

We continue to track the ransomware landscape, including statistics from known attacks, and this month highlight the newcomers “Cloak”, “Metaencryptor” and “Ransomed”.

- Ziggy Davies, Intelligence Analyst

# 1 Monthly highlights

## 1.1 Ivanti EPMM / MobileIron updates

Last month's we reported on the exploitation of a vulnerability (CVE-2023-35078) in Ivanti Endpoint Manager Mobile (EPMM, formerly known as MobileIron), which led to the breaches within the Norwegian government. Since then, further vulnerabilities have been identified.

These include:

CVE-2023-35081, which has a CVSS score of 7.2 allows arbitrary unauthenticated file writes. This can be combined with CVE-2023-25078 to upload and execute files and deploy web shells.

CVE-2023-35082, which is essentially the same vulnerability as CVE-2023-25078, but it applies to a different API endpoint. Initially, Ivanti believed that the vulnerability only existed on MobileIron versions 11.2 and below. Ivanti have since stated that this vulnerability in fact applies to all versions of EPMM, whether they have been patched for CVE-2023-25078 or not.

CVE-2023-32560, which relates to two buffer overflow vulnerabilities in Ivanti's Avalanche product.

CVE-2023-38035, which is another API authentication bypass vulnerability, this time in Ivanti Sentry (formerly known as MobileIron Sentry). This vulnerability is believed to be actively exploited, and according to Ivanti can be abused to "*change configurations, run system commands, or write files onto the system*".

### WithSecure™ Insight

These new vulnerabilities come after a spate of zero-day attacks utilizing MobileIron services to target governmental departments of Norway last month. The assailants remain unknown but are almost certainly advanced and capable threat actor(s), which we reported in July's Threat Highlight Report.

The most recent vulnerability, CVE-2023-38035 is reported to be under active exploitation by both Ivanti and CISA, and there is a realistic possibility it is being abused by the same sophisticated threat actor who carried out last month's attacks, either at that time, or subsequently.

Proof of exploit (PoE) code for this most recent vulnerability has been published online, lowering the barrier for subsequent exploitation by less-skilled threat actors, and making patching even more important.

### What can you do?

Ivanti has released patches for all the vulnerabilities referenced in this article, and you should follow their guidance as appropriate.

Regarding the newest actively exploited vulnerability in Ivanti Sentry (CVE-2023-38035), exposure is limited to Ivanti Sentry versions 9.18 and prior, and Ivanti have released a patch which should be installed urgently, due to the ongoing risk of exploitation. The vulnerability does not impact other Ivanti products, such as Ivanti EPMM or Ivanti Neurons for MDM. Ivanti has noted that while the CVSS score is high, exploitability significantly drops for customers not "*exposing 8443 to the internet*".

## 1.2 Digital Pulse Proxies

Researchers at Alien Labs has tracked a campaign they are calling **ProxyNation**, whereby a threat actor is promoting the installation of a proxy service on infected machines, in order to form part of a proxy network. Access to this proxy network is then sold to users wishing to hide their traffic. Figures provided by Alien Labs show that around 400,000 machines are thought to be infected by the proxy service and acting as exit nodes.

The initial malware sample is signed and only has one detection on Virus Total, suggesting it is unlikely to be detected by traditional AV and security solutions.

The initial delivery mechanism for **Digital Pulse** is unknown, but it appears the malware operators are running an affiliate scheme and rewarding people for distributing the malware. This suggests that the malware can be packaged and delivered in several different ways.

The primary malware sample is written in Go and is packaged using the legitimate software **Inno**, and is installed with the following flags:

`/SP`– Which disables pop-ups
`/VERYSILENT`– Which disables the progress bar pop-up/
`SUPPRESSMSGBOXES`– Which suppresses message boxes and automatically resolves common interaction messages.

The malware drops two files:

```
DigitalPulseService[.]exe
DigitalPulseUpdater[.]exe
```

And achieves persistence through the following registry addition:

```
HKCU\Software\Microsoft\Windows\
CurrentVersion\Run\DigitalPulse
```

And creation of the following scheduled task:

```
%AppData%\DigitalPulse\DigitalPulseUpdate.exe
```

The proxy then communicates with its C2, typically over port `7001`, a port which our scans suggest is not commonly legitimately used.

### WithSecure™ Insight

This campaign involves a vast proxy network set up by criminals/threat actors, with access then being sold under the pretext that it is a legitimate service. This is further evidence of the professionalization of the cybercriminal landscape, as proxies and the desire to hide traffic is a necessity for many threat actors.

As this campaign is being run as an affiliate service, initial compromise can come from any infection vector, such as phishing, malvertising, tainted downloads, etc. Prevention therefore relies on good cyber practices across all potential vectors.

### What can you do?

This campaign is targeting Windows machines, but a similar campaign has been detected for MacOS. Furthermore, the malware is written in Go, so could be trivially repackaged for MacOS or Linux systems.

To detect potential compromise please check the following:

Anomalous network connections on the following port:

```
7001
```

The presence of the following directories:

```
%AppData%\DigitalPulse
```

```
HKCU\Software\Microsoft\Windows\
CurrentVersion\Run\DigitalPulse
```

## 1.3 WinRAR exploited

There are two known vulnerabilities in file archive software WinRAR, with one being under active exploitation.

The first, CVE-2023-40477, exists thanks to a flaw in the way WinRAR processes recovery volumes, and if exploited can result in the execution of malicious code, but does require victim interaction in the form of opening the specially crafted .rar file.

This vulnerability was disclosed by user "goodbyeselene" via the Zero-Day Initiative platform and exists due to the way older versions of WinRAR process recovery volumes. An attacker who inserts a specially crafted memory chunk in an archive, can trick WinRAR into writing data outside of its allocated memory, leading to a buffer overflow and the execution of code.

The vulnerability has earned a CVSS score of 7.8, as it does require user interaction in the form of a victim opening the malicious .rar file. But driving user interaction through pretexting is commonplace and trivial for most threat actors, making exploitation very likely.

The second, CVE-2023-38831 has reportedly been under active exploitation since at least April 2023, and involves a specially crafted .zip file which contains an innocuous looking file, that actually results in the execution of malicious code stored in another directory. The exploitation of this vulnerability is associated to the distribution of **DarkMe**, **GuLoader** or **Remcos RAT** malware.

This vulnerability was uncovered Group-IB, which describes the main phase as...

"*...occurring when WinRAR attempts to open the (benign) file that the user wants to access. The ShellExecute function receives the wrong parameter to open the file. The (benign) file name will not match the search criteria, resulting in it being skipped. Instead of finding the intended file, the (malicious) batch file is discovered and executed*".

### WithSecure™ Insight

Archive file types such as .zip and .rar are commonplace and WinRAR is a popular tool used to access and create them, having a reported 500 million userbase worldwide, and our telemetry aligns with that: it is highly prevalent.

While CVE-2023-38831 is already under active exploitation, CVE-2023-40477 is not - but is highly likely to be weaponized by threat actors within a short time. This is because it offers a new way to achieve initial access through the delivery of malicious files across many intrusion vectors, such as phishing, malvertising, SEO poisoning, social engineering, etc.

The threat actor(s) exploiting this vulnerability are targeting users of forums discussing brokerage/finances and cryptocurrency, suggesting they are a financially motivated actor intending to take over victims' accounts/wallets.

### What can you do?

All versions of WinRAR up to 6.23 are vulnerable.

We suggest updating to the newest version wherever possible. This process is manual, as WinRAR does not contain an auto-update or update-reminder function, aggravating the patch process and increasing the risk of hosts going unpatched and remaining vulnerable.

## 1.4 Hacktivism Updates

Pro-Russian hacktivist groups remain a prevalent threat and DDoS attacks continue to be used against targets across Europe, with a focus on nations providing assistance to Ukraine, and more recently targeting the Nordic nations of Norway, Sweden and Finland, with the transportation sector being heavily targeted.

The past month has seen an increase in hacktivist activity targeting Japan. This is due to the recent release of contaminated water relating to Fukushima back into the ocean, an act which has angered many and led to attacks by **Anonymous Italia** and Indonesian group **VulzSec**, in a campaign called #OpJapan. This campaign is one of the first incidences of cyberattacks linked to environmental activism/protest and may be indicative of future tactics for similar groups in Europe and the US.

Russian linked group **Anonymous Sudan** has struck organizations in France this month, claiming they are in response to French statements regarding the recent coup in Niger, with the group also describing France's military presence in Niger as "French imperialism". Of course, the destabilization of African nations is beneficial to Russia, further linking the interests of Anonymous Sudan and Russia, which continues to have a presence in the region with PMC Wagner deploying troops within Central African Republic (CAR) and possibly even Niger itself.

India has seen an increase in DDoS hacktivist activity follow its independence day (15th August) celebrations, with about 1,000 websites targeted. This coincides with the release of a report by Group-IB on hacktivist group **Mysterious Bangladesh**, a group which has heavily targeted Indian entities since June 2022.

There has been increased reporting regarding data leak hacktivist group **KittenSec**, following its leak of data relating to citizens of Panama, Chile and Italy via the group's Telegram channel. Following the leak, the group's apparent leader **Cipherkit** announced their departure from the group and no posts have been made since. **KittenSec** has previously stated its attacks are designed to target corruption, but have not elaborated on this, and prior attacks suggest opportunism rather than targeted attacks.

# 2 Ransomware: Trends and notable reports

The following data is limited to a multi-point of extortion ransomware leak sites that are parseable and captured between 28th July 2023 and 28th August 2023.

This month has seen a significant drop in leak site posts, mainly attributable to a massive drop (-98%) in Clop activity, following their mass exploitation of MOVEit. This is despite large leaks from newcomers such as Cloak, Metaencryptor and Ransomed. Meanwhile LockBit have experienced a boost (+102%) but are apparently falling apart at the seams.

| Group | Victims | Percentage | Change |
|---|---|---|---|
| LockBit | 93 | 25 % | 102 % |
| Alphv | 33 | 9 % | 39 % |
| Akira | 31 | 8 % | 107 % |
| 8Base | 29 | 8 % | -17 % |
| Cloak | 24 | 6 % | New |
| BlackBasta | 21 | 6 % | 62 % |
| NoEscape | 21 | 6 % | 91 % |
| Play | 20 | 5 % | 17 % |
| Medusa | 12 | 3 % | 20 % |
| Metaencryptor | 12 | 3 % | New |
| Rhysida | 11 | 3 % | -27 % |
| BianLian | 10 | 3 % | -33 % |
| Nokoyawa | 8 | 2 % | 300 % |
| Ransomed | 8 | 2 % | New |
| Other | 40 | 11 % | N/A |
| **Total** | **373** | | **-20 %** |

## 2.1 Akira abuses Rust Desk

Conti spin-off group **Akira**, which has been active since at least March 2023 and struck at least 115 organizations in that time is reported to be using some new tactics, techniques and procedures.

Akira is known to target CISCO VPN services and has been doing so for at least three months. It has been using legitimate remote monitoring and management (RMM) tool RustDesk in attacks. Many ransomware groups used RMM tools to achieve persistence and remote access to their victims, but this is the first known instance of RustDesk being used over other options such as AnyDesk or ScreenConnect. This decision is likely due to increase detection surrounding malicious use of common RMM tools and RustDesk's cross-platform compatibility, allowing its usage across a wide range of victim environments.

WithSecure's telemetry indicates some legitimate usage of RustDesk, especially on Windows, and as with the abuse of all RMM tools this makes malicious usage difficult to detect. However, WithSecure$^{tm}$ endpoint detection solutions have good visibility across Windows, MacOS and Linux, including the installation and usage of RustDesk. It is important that any usage of RMM tools outside of approved options is investigated, especially if it is accompanied by further suspicious activity or detections.

## 2.2 Cyclops rebrands into Knight

Ransomware group **Cyclops**, which we first discussed back in June 2023, has recently rebranded and changed name to **Knight**. As part of the rebrand the group has reportedly released new versions of their tooling, and created a new data leak site, though it does not have any victims listed as of yet.

As well as their normal double-extortion campaign, Knight has begun a new “lite” version of its locker, which has been deployed in a spear-phishing campaign. The lite version lacks any exfiltration capability and appears to be standardized for all victims, with all ransom notes being identical and demanding a comparatively low ransom of $5,000.

The Bitcoin wallet included in the ransom note does not appear to have had any deposits, suggesting a lack of success for Knight ‘lite’. There also appears to be a large flaw in the lite campaign; if all victims get the same ransom note, with no unique ID and same ransom amount, how are Knight going to verify which victim has paid and provide them with the decryption key?

## 2.3 Rhysida's connection to Vice Society

Recent ransomware newcomers **Rhysida** has been linked to veterans **Vice Society**, thanks to a dramatic overlap in tactics, techniques and procedures (TTPs), as well as victimology. Rhysida recently made headlines due to its highly disruptive attack on Prospect Medical Holdings, impacting 17 hospitals and 166 health clinics across the US. Vice Society was equally lacking in the ethics and morals department, having carried out several attacks on the health and education sectors.

While overlaps in TTPs are common between ransomware groups, and these links are speculative rather than definitive, it is certainly suspicious that Vice Society hasn't posted on its leak site since June 2023, just when Rhysida started listing victims. If Vice Society changed names due to gaining too much law enforcement and CERT attention, then Rhysida is going the wrong way about keeping things cool with its attacks on the healthcare and education sector.

## 2.4 LockBit imploding?

John DiMaggio of Analyst1 has continued to conduct excellent research into ransomware titan **LockBit** with a third volume to their Ransomware Diaries project. John has infiltrated the group and gained insight into their workings and apparent issues. The key findings include:

- LockBit may be compromised and disappeared from Tox messenger for a period of time.
- LockBit has issues publishing victims' data, likely due to limits with its infrastructure.
- LockBit's affiliates are apparently leaving for competitors
- LockBit has failed to release an updated version of its locker, which is out of character.
- LockBit are apparently trying to acquire lockers from competitors.

All of which are indicative of serious problems within the criminal enterprise, but despite this LockBit continues to strike victims and create vast numbers of posts on its leak site. But perhaps this is the beginning of the end.

## 2.5 Ransomware newcomers

**Metaencryptor**

This group is operating a multi-point of extortion ransomware operation, with an active leak site on the dark web. On the 17th of August the group created 12 posts relating to different victims, but it is highly likely that these were compromised over a much longer period. Of note is that five of the organizations are German, a disproportionate amount, suggesting a targeted victimology or motivation, rather than pure opportunism.

**INC Ransom**

A recent attack by newcomer **INC Ransom** has been dissected by Huntress, and itsreport includes indicators of compromise (IOCs) and TTPs, though much of this overlaps heavily with many other ransomware groups thanks to the professionalization of cybercrime. INC Ransom has posted two victims to its leak site: an Austrian hotel and Dutch electrical company.

**Cloak**

Very little is known about this group, but so far it has listed 24 victims on its leak site. These organizations are global and from various sectors, suggesting an opportunistic threat actor.

# 3 Other notable highlights in brief

## 3.1 LLM 'malvertising' lures

We have touched on the topic of Large Language Model (LLM) and AI lures in malvertising a lot recently, but it is so prolific it is worth repeating. The presence of malicious adverts across social media and on websites is rife, with lures regarding OpenAI, ChatGPT, Google Bard and a fictional Meta AI being used to reel in curious victims.

This behavior is standard for threat actors, who often tailor their phishing and malvertising lures on the zeitgeist, which is most certainly LLMs and AI. The lures being used, often make outlandish claims regarding massive productivity increases using LLMs in an effort to drive user interaction. If a victim interacts with the advert, it can ultimately end in the installation of malware (typically infostealers).

## 3.2 Lapsus$ revisited

The Cyber Safety Review Board have released a report on LAPSUS$, the threat group responsible for high profile attacks on Brazil's ministry of health, Okta, Nvidia, Samsung, Mercado Libre, Ubisoft, T-Mobile, Microsoft, Globant, Uber and Rockstar Games.

This report follows the successful conviction of two UK members of the LAPSUS$ group, who focused on social engineering as a method for initial access, along with the bypass of MFA through SIM-swapping and pioneered techniques such as MFA-fatigue. Most importantly, the report details the TTPs used by LAPSUS$, and includes advice for organizations so that they can avoid similar attacks in the future. Most of these suggestions revolve around identity and access management (IAM), the enforcement of MFA and suitable training surrounding social engineering.

## 3.3 VirusTotal trends

VirusTotal has released a report titled "*Malware Trends Report: Emerging Formats and Delivery Techniques*", and its key findings include:

- *Email attachments continue to be a popular way to spread malware.*
- *Tradition file types (Excel, RTF, CAB, ZIP, RAR) are becoming less popular.*
- *OneNote and JavaScript are the most rapidly growing formats for malicious attachments.*
- *ISO files for malware spreading are a flexible alternative for both widespread and targeted attacks. Distribution as heavily compressed attachments makes them difficult to scan by some security solutions.*
- *ISO files are being disguised as legitimate installation packages for a variety of software, including Windows, Telegram, AnyDesk, and malicious CryptoNotepad, among others.*

# 4 Threat data highlights

## 4.1 Vulnerabilities & Exploits

**What is everyone talking about?**
The following are vulnerabilities which have been heavily discussed on social media this month.

1. CVE-2023-35078, CVE-2023-35081, CVE-2023-35082, CVE-2020-32560, CVE-2023-38035
**Ivanti (EPMM, Avalanche, Sentry)**
Unsurprisingly the vulnerabilities in Ivanti products which have been under active exploitation by a high sophistication threat actor have been heavily discussed this month.

2. CVE-2023-40477, CVE-2023-38831
**WinRAR**
One of these vulnerabilities is already actively exploited, and the other is likely to weaponized due to the prevalence of WinRAR.

3. CVE-2023-36874
**Windows Error Reporting Service Bug**
A proof of concept (PoC) and Cobalt Strike beacon object file (BOF) for this vulnerability is available, allowing attackers to escalate their privilege to SYSTEM level.

### What have we seen?

While old and proven vulnerabilities dominate our telemetry, the following are some more recent CVEs that are within the most popular exploits for August in our data:

1. CVE-2023-23397

**Microsoft Outlook**
This low complexity zero-touch vulnerability is widely exploited, even though it was patched by Microsoft in March. It involves a custom message, which then provides the attacker with a victim's NTLM hash, which can then be used in NTLM relay attacks to escalate privilege.

2. CVE-2023-21716

**Microsoft Word**
An unauthenticated, remote attacker can create a malicious rich-text format (RTF) document which, when opened or previewed by a user running vulnerable version of Microsoft Word will allow RCE with the privileges of the affected user.

3. CVE-2023-21608

**Abobe Acrobat Reader**
This vulnerability is a favorite for phishing, and involves the delivery of a malicious PDF file which when opened can result in RCE with the privileges of the affected user.

## What vulnerabilities are being newly exploited?

The following are additions to CISA's known exploited vulnerability catalog. Four have received a "CRITICAL" CVSS rating.

| CVE ID | Vendor / Product | CVSS Rating | What's the vulnerability? |
|---|---|---|---|
| CVE-2017-18368 | Zyxel P660HN-T1A Routers | Critical | Zyxel P660HN-T1A routers contain a command injection vulnerability in the Remote System Log forwarding function, which is accessible by an unauthenticated user and exploited via the remote_host parameter of the ViewLog.asp page. |
| CVE-2023-24489 | Citrix Content Collaboration | Critical | Citrix Content Collaboration contains an improper access control vulnerability that could allow an unauthenticated attacker to remotely compromise customer-managed ShareFile storage zones controllers. |
| CVE-2023-26359 | Adobe ColdFusion | Critical | Adobe ColdFusion contains a deserialization of untrusted data vulnerability that could result in code execution in the context of the current user. |
| CVE-2023-38035 | Ivanti Sentry | Critical | Ivanti Sentry, formerly known as MobileIron Sentry, contains an authentication bypass vulnerability that may allow an attacker to bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration. |
| CVE-2023-38180 | Microsoft .NET Core & Visual Studio | High | Microsoft .NET Core and Visual Studio contain an unspecified vulnerability that allows for denial-of-service. |
| CVE-2023-27532 | Veeam Backup & Replication | High | Veeam Backup & Replication Cloud Connect component contains a missing authentication for critical function vulnerability that allows an unauthenticated user operating within the backup infrastructure network perimeter to obtain encrypted credentials stored in the configuration database. This may lead to an attacker gaining access to the backup infrastructure hosts. |
| CVE-2023-38831 | RARLAB WinRAR | High | RARLAB WinRAR contains an unspecified vulnerability that allows an attacker to execute code when a user attempts to view a benign file within a ZIP archive. |
| CVE-2023-32315 | Ignite Realtime Openfire | High | Ignite Realtime Openfire contains a path traversal vulnerability that allows an unauthenticated attacker to access restricted pages in the Openfire Admin Console reserved for administrative users. |

# Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

Our latest reports: Threat-Research