aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report

November 2024

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, the CERT aDvens presents three noteworthy vulnerabilities, in addition to those already published, as well as an analysis of the Ymir ransomware.

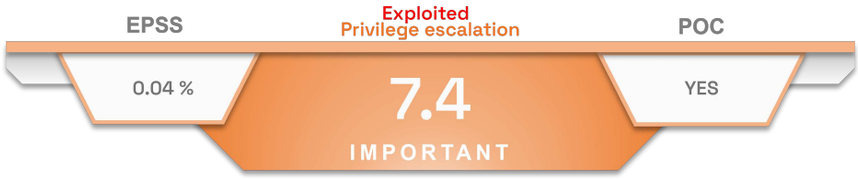
2. VULNERABILITIES

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

2.1. CVE-2024-8068

A proof of concept was published on the 12 November 2024 by security researchers at Watchtowr for CVE-2024-8068 and CVE-2024-8069. The Session Recording Storage Manager in Citrix is a Windows service, which receives recordings *via* Microsoft Message Queuing (MSMQ). The vulnerabilities are present in both the misconfigured and exposed MSMQ instance and the BinaryFormatter class that can be reached from any HTTP host, according to researcher Sina Kheirkhah. Microsoft had already discontinued the use of BinaryFormatter on 8 August 2024.

Shortly after the proof of concept was published, exploit attempts were identified by researchers at the Shadowserver Foundation.



A privilege management flaw in the *Session Recording* component of Citrix Virtual Apps and Desktops allows an attacker to escalate privileges by sending specifically crafted requests.

2.1.1. Type of vulnerability

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

2.1.2. Risk

- Privilege escalation

2.1.3. Severity (CVSS3.1 base score)

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

2.1.4. Impacted products

- **Citrix Virtual Apps and Desktops** :
  - 1912 LTSR versions prior to CU9 hotfix 19.12.9100.6
  - 2203 LTSR versions prior to CU5 hotfix 22.03.5100.11
  - 2402 LTSR versions prior to CU1 hotfix 24.02.1200.16
  - 2407 versions prior to hotfix 24.5.200.8

2.1.5. Recommendation

- Update Virtual Apps and Desktops :
  - 1912 LTSR to version CU9 hotfix 19.12.9100.6 or later,
  - 2203 LTSR to version CU5 hotfix 22.03.5100.11 or later,
  - 2402 LTSR to version CU1 hotfix 24.02.1200.16 or later,
  - 2407 to version hotfix 24.5.200.8 or later.

Additional information is available in the Citrix's advisory.

2.1.6. Proof of concept

A proof of concept is available in open sources.

2.2. CVE-2024-8069

Insecure deserialisation in the *Session Recording* component of Citrix Virtual Apps and Desktops allows an authenticated attacker, by sending specifically crafted requests, to execute arbitrary code with NetworkService Account privileges.

2.2.1. Type of vulnerability

- **CWE-502**: Deserialization of Untrusted Data

2.2.2. Risk

- Remote code execution

2.2.3. Severity (CVSS3.1 base score)

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

2.2.4. Impacted products

- **Citrix Virtual Apps and Desktops** :
  - 1912 LTSR versions prior to CU9 hotfix 19.12.9100.6
  - 2203 LTSR versions prior to CU5 hotfix 22.03.5100.11
  - 2402 LTSR versions prior to CU1 hotfix 24.02.1200.16
  - 2407 versions prior to hotfix 24.5.200.8

2.2.5. Recommendation

- Update Virtual Apps and Desktops :
  - 1912 LTSR to version CU9 hotfix 19.12.9100.6 or later,
  - 2203 LTSR to version CU5 hotfix 22.03.5100.11 or later,
  - 2402 LTSR to version CU1 hotfix 24.02.1200.16 or later,
  - 2407 to version hotfix 24.5.200.8 or later.

Additional information is available in the Citrix's advisory.

2.2.6. Proof of concept

A proof of concept is available in open sources.

2.3. CVE-2024-10914

CVE-2024-10914 affects several D-Link NAS servers that have been discontinued. Shortly after the vendor announced that no patch would be deployed, several threat actors began exploiting this vulnerability. Exploitation is not easy but is simplified by an open-source proof of concept.

A command injection in the *account_mgr.cgi* script of multiple D-Link network storage servers allows an unauthenticated attacker to execute arbitrary code by sending specifically crafted requests.

Security researchers at the Shadowserver Foundation observed exploitation attempts starting on the 12 November 2024. 1,100 internet-connected devices were identified, mostly located in the United Kingdom, Hungary and France.

2.3.1. Type of vulnerability

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

2.3.2. Risk

- Remote code execution

2.3.3. Severity (CVSS3.1 base score)

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

2.3.4. Impacted products

- **D-Link NAS boxes**:
  - DNS-320 version 1.00
  - DNS-320LW version 1.01.0914.2012
  - DNS-325 versions 1.01 and 1.02
  - DNS-340L version 1.08

2.3.5. Recommendation

As these products are no longer supported, no fixes are available. It is recommended to replace them with an alternative product.

2.3.6. Proof of concept

A proof of concept is available in open sources.

3. THE YMIR RANSOMWARE

Ymir is a ransomware recently identified by Kaspersky's security teams. It is characterised by its advanced stealth capabilities, in-memory execution, and integration with malicious tools like RustyStealer, specialised in stealing credentials.

3.1. Initial discovery and first attacks

The ransomware was initially discovered during a targeted campaign in Colombia. This attack, targeting local organisations, illustrates the growing sophistication of modern ransomware and the use of complex attack chains. This first case may also represent a testing phase before scaling to broader operations.

3.2. Technical analysis of Ymir

3.2.1. Evasion and stealth techniques

Ymir operates exclusively in memory to evade traditional detection tools. It uses native functions like `malloc`, `memchr`, `memcpy` and `memmove` to manipulate its payloads, minimising system traces. This approach makes post-incident forensic analysis extremely difficult as no persistent artifacts (files or logs) are available.

3.2.2. Malicious in-memory execution

Using memory injection techniques, Ymir loads and executes its malicious implants directly into memory, bypassing file-based antivirus solutions. This method exploits legitimate processes to mask malicious activities, complicating detection. Analysts must rely on advanced memory capture tools and behavioral analysis solutions to identify this threat.

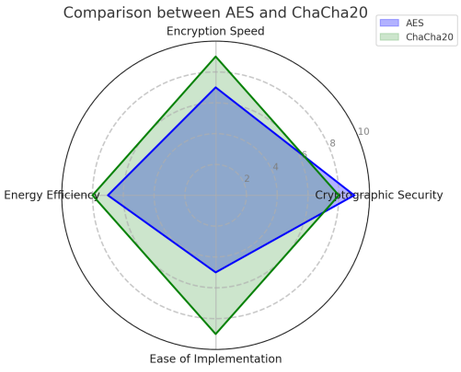
3.2.3. Infection lifecycle

Ymir follows a three-step infection lifecycle:

- **Memory injection**: Uses functions like `malloc` and `memmove` to load payloads directly into memory.
- **Stealth execution**: Integrates into existing processes to mask malicious activities.
- **No persistent artifacts**: No data is written to disk, rendering traditional forensic analysis ineffective.

3.3. Encryption and impact on victim systems

3.3.1. Use of ChaCha20 for encryption



This representation highlights the distinct capabilities of the two algorithms: AES remains the standard, particularly effective in hardware-accelerated systems, while Ymir's `ChaCha20` stands out for its efficiency, speed and simplicity, especially in resource-limited environments.

3.3.2. File renaming strategy

After encryption, files are renamed with a random extension, such as `.6C5oy2dVr6`, to complicate their identification and enhance obfuscation.

3.3.3. Target prioritisation

Ymir prioritises sensitive files (documents, databases) while avoiding those essential to system functionality. This strategy ensures operational continuity, increasing the likelihood of ransom payment.

3.4. Attack vectors and propagation

3.4.1. Exploitation of credentials and remote access

RustyStealer is used to collect credentials (passwords, session cookies), enabling attackers to exploit compromised RDP services to access systems. Once access is obtained, attackers move laterally within the network, compromising additional systems and preparing the ground for Ymir deployment.

3.4.2. Domain controller takeover for wide propagation

Domain controllers are targeted to gain extensive privileges, enabling rapid and large-scale ransomware propagation. Attackers also use discrete channels, such as `PowerShell`, to mask malicious communications and evade detection by the user.

3.5. Incident Response Strategies

3.5.1. Detecting suspicious behaviors

- Deploy EDR/MDR solutions to monitor abnormal behaviors in real time, such as memory injections and network tool usage.
- Configure SIEM rules to detect specific IOCs, such as suspicious RDP connections or unusual processes.

3.5.2. Recovery and data restoration plans

- Maintain regular backups in isolated or immutable environments.
- Test recovery plans through incident simulations.
- Prioritise the restoration of critical systems to minimise downtime.

3.5.3. Awareness and team training

- Train employees on advanced phishing techniques and signs of malicious activity.
- Organise regular attack simulation campaigns to evaluate organisational preparedness.

3.6. Operating Methodology

3.6.1. Threat assessment

Ymir represents a modern ransomware example, leveraging advanced techniques like in-memory execution and third-party tools like RustyStealer. The connection between initial access brokers and ransomware groups is clearly demonstrated here. This targeted methodology renders traditional solutions obsolete, emphasising the need for proactive defenses against these sophisticated threats.

3.6.2. Forecasts for future evolution

Future variants of Ymir could integrate more subtle propagation vectors or adopt evasion mechanisms inspired by advanced phishing techniques, such as misleading formats (e.g., SVG files). These developments highlight the importance of enhancing behavioral detection and monitoring emerging vectors to anticipate these ever-evolving threats.

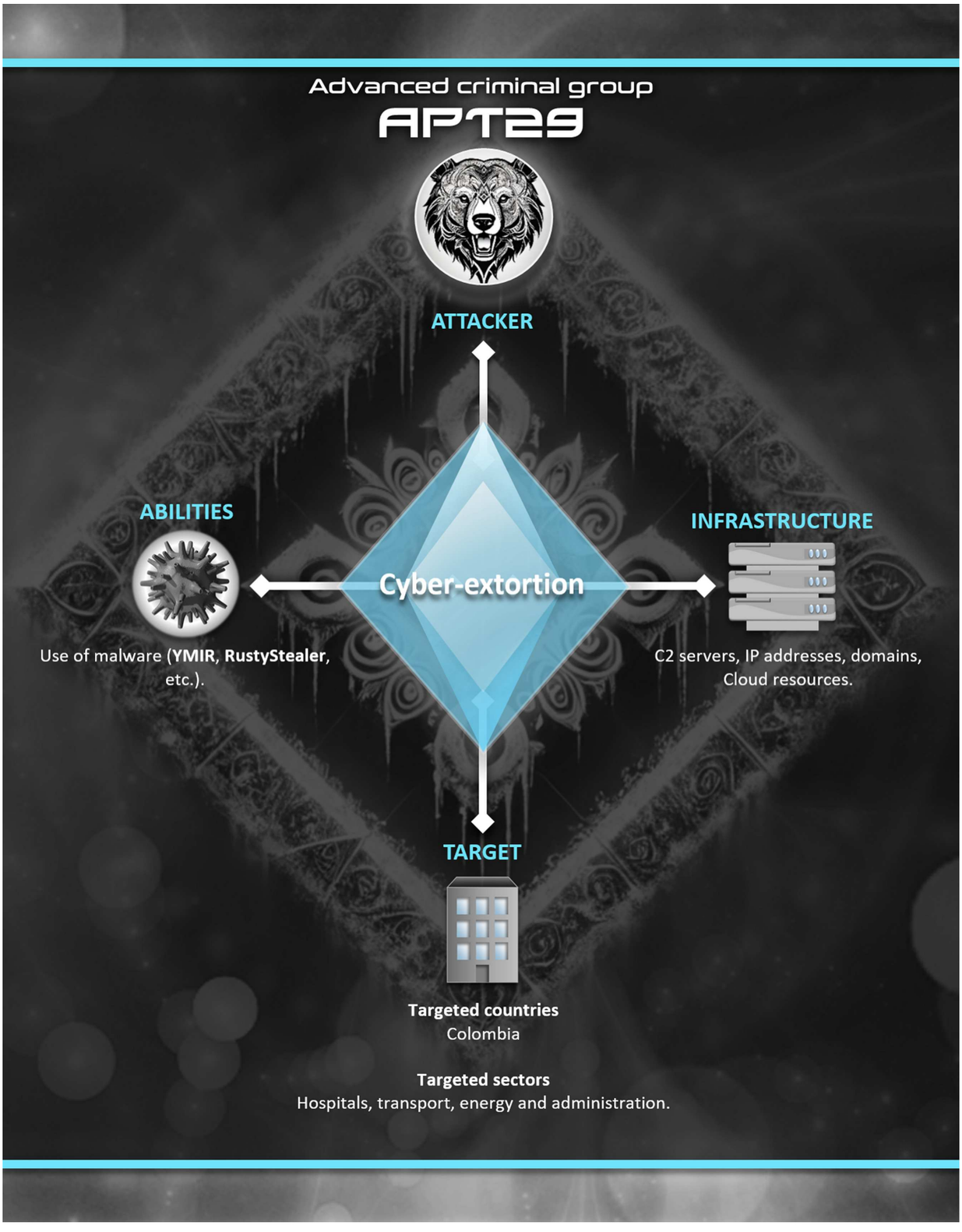


Figure 1. Diamond Model of Ymir.

3.6.3. Mitre ATT&CK Matrix

3.6.4. IOC

TLP	TYPE	VALUE	COMMENTS
TLP:CLEAR	SHA1	3648359ebae8ce7cacae1e631103659f5a8c630e	Sample Ymir
TLP:CLEAR	SHA1	fe6de75d6042de714c28c0a3c0816b37e0fa4bb3	Sample Ymir
TLP:CLEAR	SHA1	f954d1b1d13a5e4f62f108c9965707a2a2a2a3c89	Sample Ymir
TLP:CLEAR	MD5	5ee1befc69d120976a60a97d3254e9eb	RustyStealer
TLP:CLEAR	MD5	5384d704fadf229d08eab696464cbba6	ps1
TLP:CLEAR	MD5	39df773139f505657d11749804953b5	ps1
TLP:CLEAR	SHA256	8287d54c83db03b8adcdf1409f5d1c9b1693ac8d000b5ae75b3a296cb3061c	ps1
TLP:CLEAR	SHA256	51ffc0b7358b7611492ef458fdf9b97f121e49e70a6b53b53èd923b707a03	RustyStealer
TLP:CLEAR	SHA256	b087e1309f3eab6302d7503079af1ad6af06d70a932f7a6a6a421b942048e28a	Trojan.MSIL.Dnoper.sb
TLP:CLEAR	MD5	12acbb05741a218a1c83eaa1cfc2401f	Sample Ymir
TLP:CLEAR	SHA256	cb88edd192d49db12f4f44f764c3bdc287703666167a4ca8d533d51f86ba428d8	Sample Ymir
TLP:CLEAR	IP	74.50.84.181:443	C2
TLP:CLEAR	IP	94.158.244.69:443	C2
TLP:CLEAR	IP	5.255.117.134:80	C2
TLP:CLEAR	IP	85.239.61.60	C2
TLP:CLEAR	SHA256	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f	Sample Ymir
TLP:CLEAR	MD5	dd7799d822f052cfa8ad1e16b33bb2cb	Sample Ymir

3.6.5. YARA

YARA 1: Filescan

This YARA rule allows the detection of the malicious DLL DomainManager.dll.

Source: Kaspersky

```
import "pe"

rule Ymir
{
  meta:
  author = "Kaspersky - GERT"
  description = "Yara rule for detecting the Ymir ransomware."
  target_entity = "file"

  strings:
    $s1 = "powershell -w h -c Start-Sleep -Seconds 5; Remove-Item -Force -Path"
wide ascii nocase
    $s2 = "setup-qtox-x86_64-release.exe" wide ascii nocase
    $s3 = "6C5oy2dVr6" wide ascii nocase
    $s4 = "INCIDENT_REPORT.pdf" wide ascii nocase
    $s5 = "D:20240831154833-06" wide ascii nocase
    $s6 = "ChaCha" wide ascii nocase
    $s7 = "x64dbg" wide ascii nocase
  condition:
    (3 of ($s*)) and pe.imports("msvcrt.dll", "memmove")
}
```

YARA 2: aDvens

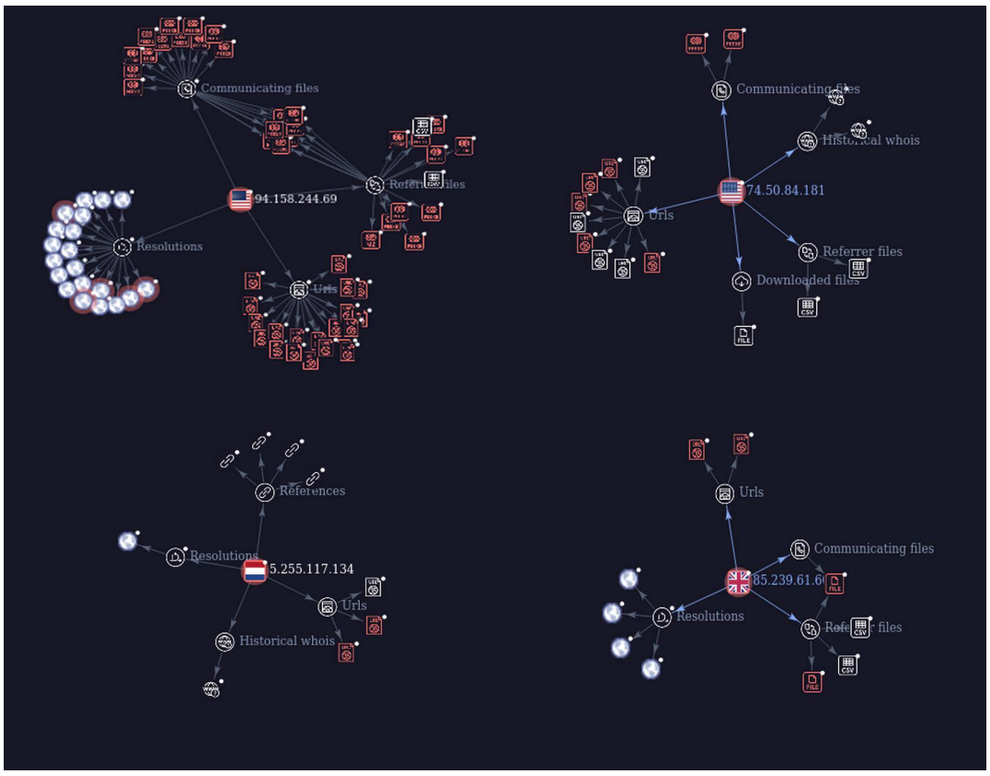
This YARA rule detects Ymir.

Source: aDvens

```
import "pe"

rule Ymir_Ransomware_Detection
{
    meta:
        author = "Advens"
        description = "YARA rule for detecting the Ymir ransomware."
        date = "2024-11-28"
        reference = "https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/"

    strings:
        $s1 = "powershell -w h -c Start-Sleep -Seconds 5; Remove-Item -Force -Path" wide ascii nocase
        $s2 = "setup-qtox-x86_64-release.exe" wide ascii nocase
        $s3 = "6C5oy2dVr6" wide ascii nocase
        $s4 = "INCIDENT_REPORT.pdf" wide ascii nocase
        $s5 = "D:20240831154833-06" wide ascii nocase
        $s6 = "ChaCha" wide ascii nocase
        $s7 = "x64dbg" wide ascii nocase

    condition:
        uint16(0) == 0x5A4D and
        pe.imports("msvcrt.dll", "memmove") and
        (3 of ($s*))
}
```

3.7. Investigation

3.7.1. Analysis of Command and Control (C2) Servers



Initial research focused on C2 servers associated with YMIR, examining their relationships with files, URLs, and DNS resolutions. Several key findings emerged:

- Frequent reuse: Many identified C2s appeared in public databases such as VirusTotal, AbuseIPDB, or ThreatMiner, indicating repeated exploitation of known infrastructures.
- Active and inactive elements: Some C2s were still in use for ongoing campaigns, while others appeared abandoned or inactive, suggesting short cycles or strategic migration to other infrastructures.
- Strategic nodes: Certain IPs, such as 94[.]158[.]244[.]69, stood out for their high activity, acting as central pivots for malicious infrastructure.

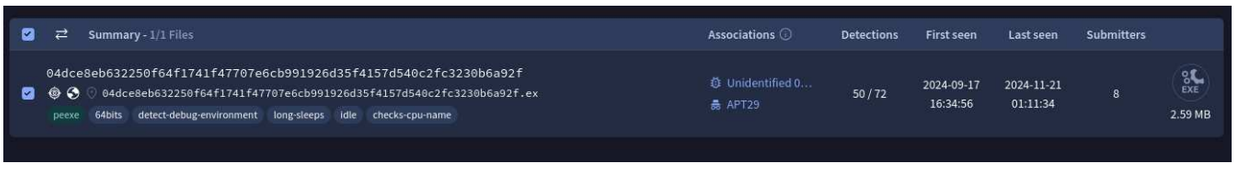
This analysis collected critical IoCs (IPs, domains, associated files) that were instrumental in strengthening detection and prevention efforts.

3.7.2. Creating a YARA Rule for Retrohunt on VirusTotal

A YARA rule was developed based on specific characteristics of Ymir. This rule leverages:

- Specific strings observed in malicious samples (e.g., PowerShell commands, encryption algorithms like ChaCha20).
- Typical behaviors of executable files, such as importing functions associated with msvcrt.dll.
- Technical criteria, such as file size (< 2 MB) and the presence of a PE header.

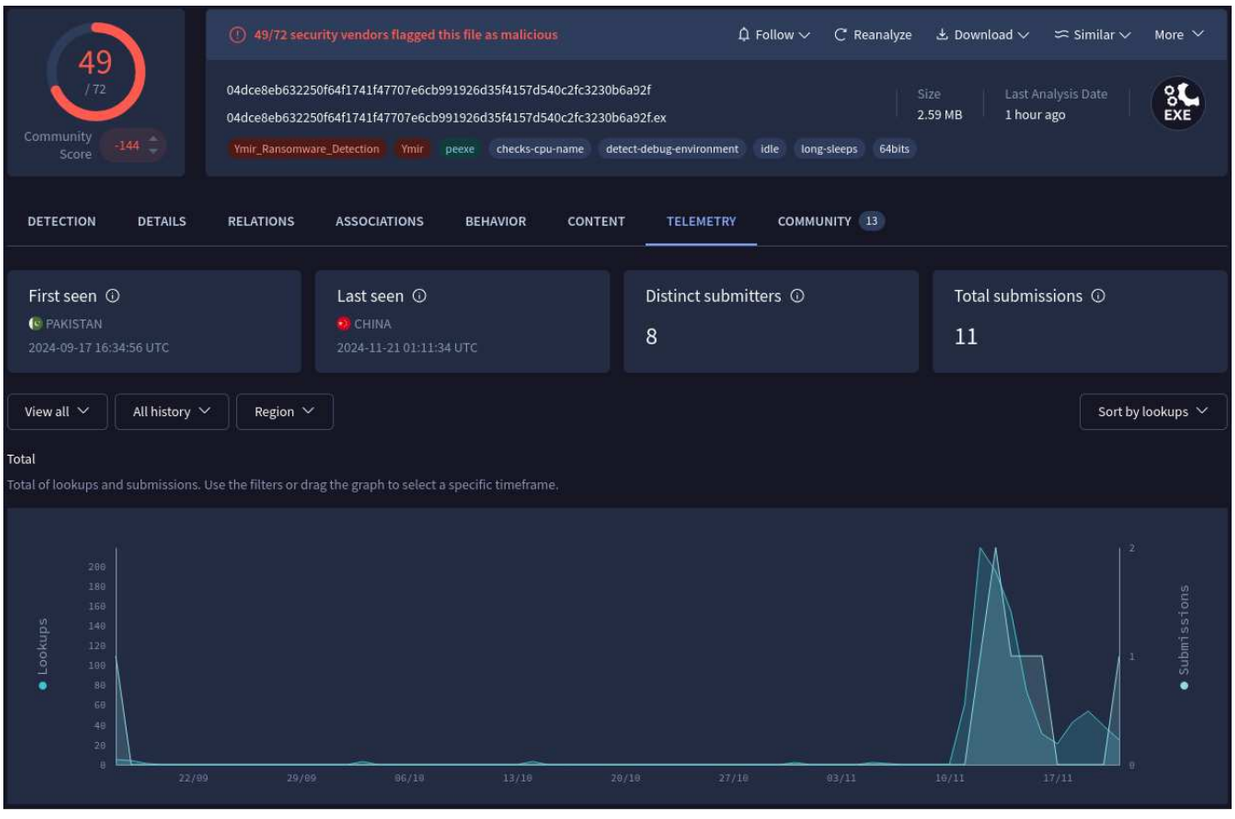
This rule was subsequently used to perform a retrohunt on VirusTotal.



The retrohunt results highlighted an implant detected by a specific rule. This implant was first observed on September 17, 2024, at 16:34:56 and last seen on November 21, 2024, at 01:11:34. It is associated with APT29, a well-known actor in the cyber threat landscape. The executable was identified as malicious or suspicious by 50 out of 72 analysis engines and was submitted by 8 different sources.

Date	Region	Name	Source
2024-09-17 16:34:56 UTC	PAKISTAN	unlock.bin	68924c59 - web
2024-11-12 18:26:49 UTC	UNITED KINGDOM	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f (2)	7faaae43 - web
2024-11-12 18:26:59 UTC	UNITED KINGDOM	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f (2)	7faaae43 - web
2024-11-13 10:46:08 UTC	ITALY	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f	7f666e75 - community
2024-11-13 21:28:07 UTC	INDIA	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f.exe	85beec9e - web
2024-11-14 06:22:28 UTC	JAPAN	file	364d4d88 - api
2024-11-15 01:17:05 UTC	KOREA, REPUBLIC OF	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f.exe	7ea08672 - web
2024-11-16 15:09:31 UTC	GERMANY	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f	7a4d5f37 - api
2024-11-20 12:20:59 UTC	CHINA	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f.ex	b3366c9f - community
2024-11-20 12:22:59 UTC	CHINA	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f.ex	b3366c9f - community

The submitted file appeared under slightly different names, though most submissions identified it as a Windows executable. This suspicious file circulated globally. Its diffusion over more than two months and varied geographic origin suggest it may have been used in a global campaign or spotted in diverse environments. The initial submission under the name unlock.bin suggests an attempt at obfuscation or use in specific processes. Additionally, the submission frequency significantly increased after November 12, 2024, reflecting either heightened activity or improved recognition of its malicious nature.



The graph illustrates the lifecycle of YMIR as currently understood.

Stage 1: Initial Spike (September 17–22, 2024)

Description

A very high volume of lookups was observed immediately after the initial detection of the file in Pakistan, with over 200 requests. No notable submissions were recorded at this stage, suggesting primarily exploratory activity.

Analysis

This spike may be attributed to a preliminary alert in a localized environment, prompting analysts or automated systems to massively examine the file. It is possible that this file was used in a first wave of a malicious campaign, limited to a specific area, or attracted attention following detection by automated tools.

Stage 2: Inactivity Period (September 22 – Early November 2024)

Description

Following the initial spike, lookups dropped drastically and remained nearly nonexistent for over a month. No new submissions were recorded during this period.

Analysis

This inactivity period may reflect a strategic latency phase, where attackers suspended the active use of the file to reduce detection risk. This behavior is typical of Advanced Persistent Threats (APTs), which favor discrete tactics and use their tools sparingly to avoid drawing attention.

Stage 3: Resumption of Activity (November 10–15, 2024)

Description

From November 10, a notable increase in lookups and submissions was recorded. Lookups peaked again around November 12, while submissions increased progressively.

Analysis

This resumption likely coincides with a new wave of detection or the publication of a global alert. Two main scenarios can explain this intense period:

- An active campaign deploying this file in multiple environments, leading to increased detection.
- The publication of IoCs by researchers or cybersecurity organizations, prompting analyses by concerned parties.

Additionally, this increase may indicate that the file was identified in a strategic environment (e.g., governmental, industrial, or financial infrastructures), leading to heightened vigilance and broader exposure.

Consultations and Submissions

A major spike in consultations was observed around November 12, 2024, followed by a gradual decline. Simultaneously, submissions increased significantly after November 10, 2024, following a similar trend. This correlation indicates heightened attention to this file, likely in response to an alert or growing recognition of its malicious nature, prompting thorough analyses.

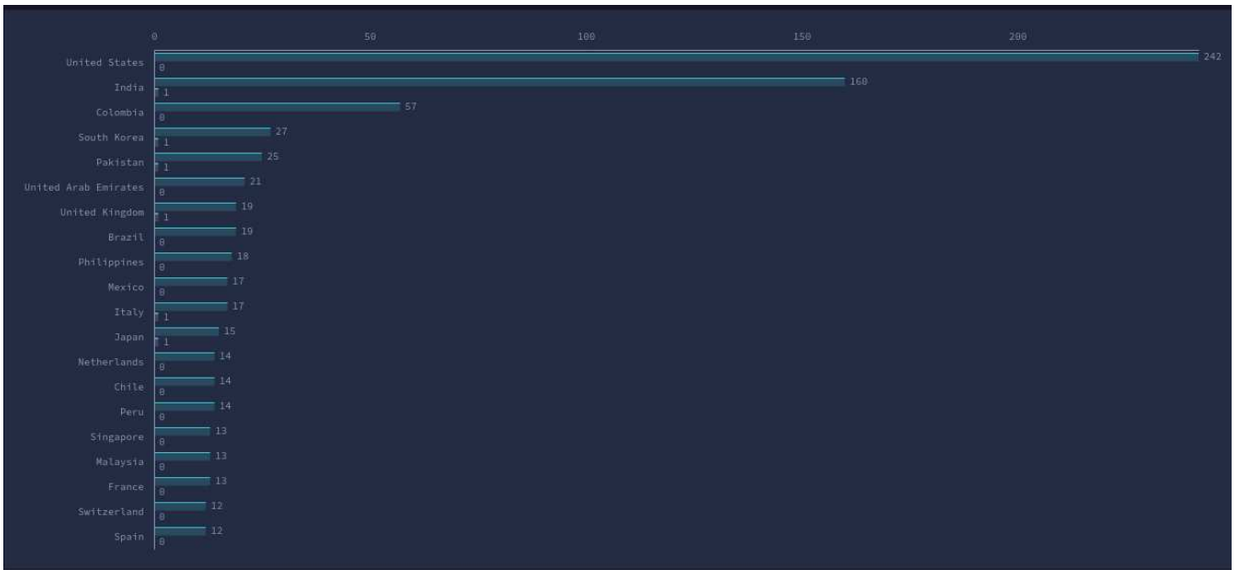


Figure 2. Volume of consultations observed on VT since September

The file was submitted from various regions around the world, including Pakistan, the United Kingdom, Germany, and China, reflecting global distribution or a large-scale targeted campaign. The main activity was concentrated between November 10 and November 20, 2024, suggesting an intensification of efforts to detect this file or an active campaign during that period.

3.8. Conclusion

YMIR represents a highly advanced and sophisticated threat. Its techniques, such as in-memory execution combined with elaborate evasion mechanisms (debugger detection, artificial delays, passive behaviors), demonstrate a significant level of professionalism, characteristic of APT groups. These methods enable YMIR to effectively bypass many traditional detection systems.

Furthermore, the rapid development of technologies, particularly the integration of artificial intelligence into malicious tools, paves the way for even more formidable threats. With AI, new variants of YMIR could emerge, incorporating even more sophisticated mechanisms and dynamically adapting to targeted environments.

4. SOURCES

4.1. CVE-2024-8068 and CVE-2024-8069

- https://nvd.nist.gov/vuln/detail/CVE-2024-8068
- https://nvd.nist.gov/vuln/detail/CVE-2024-8069
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0964/
- https://labs.watchtowr.com/visionaries-at-citrix-have-democratised-remote-network-access-citrix-virtual-apps-and-desktops-cve-unknown/
- https://thehackernews.com/2024/11/new-flaws-in-citrix-virtual-apps-enable.html
- https://www.cybersecuritydive.com/news/citrix-session-recording-cves-hackers/732794/
- https://x.com/Shadowserver/status/1856435596085895328

4.2. CVE-2024-10914

- https://nvd.nist.gov/vuln/detail/CVE-2024-10914
- https://cyble.com/blog/no-fix-for-critical-command-injection-vulnerability-in-legacy-d-link-nas-devices/
- https://securityaffairs.com/170995/iot/cve-2024-10914-d-link-nas-flaw-exploited.html
- https://x.com/Shadowserver/status/1856635619839008810

4.3. Ymir ransomware

- https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/
- https://www.virustotal.com/gui/file/04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f/telemetry