TIR-20250225 Monti Ransomware – Resurgence and Recent Attacks

2/25/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

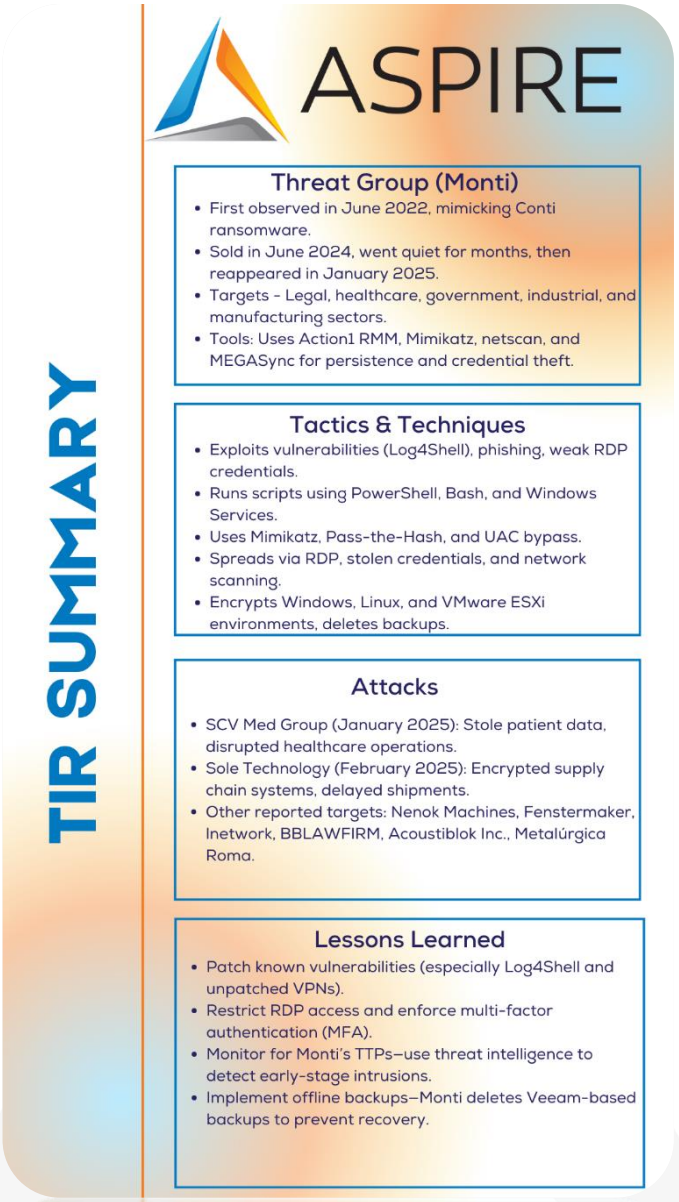
Monti ransomware, first identified in June 2022, has gained notoriety for its similarity to the now-defunct Conti ransomware. Using Conti's leaked source code, M

Monti initially mimicked Conti's tactics, techniques, and procedures (TTPs) and targeted various sectors, including legal, government, and healthcare organizations.

After an active period in 2022 and 2023, the group seemingly disappeared during the summer of 2024. However, reports indicate that in June 2024, Monti was sold to new operators, who took the ransomware underground for nearly six months before re-emerging in early 2025.

Since its resurgence, Monti has launched a series of high-profile attacks on various organizations worldwide.

These attacks demonstrate an evolved approach, with Monti continuing to refine its ransomware payloads and expand its target sectors.



Aspire Technology Partners
(732) 847-9600
www.aspiretransforms.com

MONTI RANSOMWARE

As previously stated, Monti ransomware first emerged in June 2022, drawing immediate attention due to its similarities to Conti ransomware, a notorious ransomware-as-a-service (RaaS) operation that officially disbanded in May 2022. Unlike many emerging ransomware groups that attempt to establish their own unique methodologies, Monti directly copied Conti's tactics, techniques, and procedures (TTPs), going as far as to reuse Conti's leaked source code to build its own encryptor.

Cybersecurity researchers noted that Monti's operators had likely studied Conti's internal documentation, which was leaked earlier in 2022, including training guides, operational playbooks, and source code snippets. This allowed Monti to bypass the early development stage that most ransomware groups go through, allowing them to launch attacks at full capacity from the beginning. There was also speculation that Monti may have absorbed former Conti members, which could also explain the striking similarities in their tactics and techniques.

Additionally, Conti is a known Russian-based ransomware group, and while Monti's origins have not been officially confirmed, its name, tactics, and techniques closely mirror Conti's. This strong resemblance suggests that Monti could also be a Russian-affiliated operation.

Alleged Connection to Russian National, Mikhail Matveev

Mikhail Pavlovich Matveev, better known by his online aliases "Wazawaka" and "Boriselcin," is well known in the ransomware world. He's been linked to some of the most notorious ransomware operations, including LockBit, Babuk, Hive, and Conti. Now, new findings suggest he may also have ties to Monti ransomware.

According to Digital Asset Redemption (DAR), their investigation connected Matveev to Monti through open-source intelligence (OSINT), human intelligence (HUMINT), and law enforcement sources. While Monti itself isn't officially sanctioned, DAR warned that ransom payments to the group could end up in Matveev's hands - an issue since he's already sanctioned by the U.S. Department of the Treasury's OFAC regulations.

Matveev has a reputation for mocking law enforcement and openly flaunting his involvement in cybercrime. He was also an early adopter of double extortion tactics. Given his deep history in ransomware operations, there's a strong possibility that Monti is another extension of his cybercriminal empire.

Early Attacks and Activity (2022 - 2023)

Monti's first confirmed incident occurred in July 2022, when a BlackBerry incident response team was called in to investigate a ransomware attack. The attack had encrypted nearly 20 user hosts and over 20 VMware ESXi servers, mirroring Conti's signature approach of targeting virtualized environments. Further investigations revealed that Monti's operators had exploited the Log4Shell vulnerability (CVE-2021-44228) in a victim's VMware Horizon server, allowing them to gain initial access before deploying the ransomware payload.

Throughout 2022 and 2023, Monti continued to launch high-profile attacks against organizations in legal, government, healthcare, and financial services sectors. Their primary strategy was to steal data before encrypting systems, following the double extortion model, where victims were not only locked out of their files but also threatened with public data leaks if they refused to pay the ransom.

By late 2023, Monti had built a reputation as a persistent ransomware operation, but towards the end of the year, their activity dropped significantly. Researchers speculated whether the group had disbanded or was simply restructuring. However, in June 2024, Monti's operators announced that the ransomware had been sold to new owners, marking a new phase in its lifecycle.

New Ownership and Monti's Transformation (2024 - 2025)

After Monti was sold in June 2024, the group went quiet for six months, sparking speculation about whether the new operators had shut down or were restructuring. Then, in January 2025, Monti re-emerged with a string of attacks on Nenok Machines, Fenstermaker, SCV Med Group, Inetwork, BBLAWFIRM, Acoustiblok Inc., Metalúrgica Roma, and Sole Technology. It turns out Monti never truly disappeared - its activity was just inconsistent, and it's possible the group had been targeting smaller organizations that didn't make headlines before launching attacks on larger, more high-profile victims.

The new attacks could mean a strategic relaunch, with improved infrastructure and enhanced encryption techniques. The new Monti operation now demonstrates more

advanced tactics, such as modified encryption algorithms, evasion techniques to bypass security tools, and refined persistence mechanisms using remote monitoring software. These changes suggest that Monti's new operators are more sophisticated cybercriminals, potentially linked to established ransomware-as-a-service (RaaS) operations.

TACTICS & TECHNIQUES

As Monti ransomware makes waves under new ownership, its operators have refined their tactics and techniques, making their attacks more effective. The ransomware group has moved beyond simply leveraging Conti's leaked code and has incorporated more sophisticated approaches to initial access, execution, persistence, and impact. Below is an in-depth breakdown of Monti's latest tactics and techniques.

Exploiting Public-Facing Applications for Initial Access

Monti continues to exploit vulnerabilities in **public-facing applications**, a tactic that has been at the core of its operations since its early days. The group frequently takes advantage of outdated or unpatched systems, particularly VMware Horizon servers, which have been targeted using the Log4Shell (CVE-2021-44228) vulnerability. By exploiting such flaws, Monti can gain a foothold in the network without requiring user interaction, allowing them to bypass traditional email-based security defenses.

In recent attacks, Monti has also targeted misconfigured Remote Desktop Protocol (RDP) services and VPN solutions that lack multi-factor authentication (MFA). Attackers use brute-force methods or credentials obtained from previous data breaches to access accounts and escalate privileges.

Using Remote Monitoring and Management (RMM) Tools for Persistence

Monti is increasingly relying on Remote Monitoring and Management (RMM) tools like Action1 RMM, AnyDesk, and Atera to establish persistence in compromised networks. These tools, originally designed for legitimate IT management, enable Monti operators to maintain long-term remote access while avoiding detection.

Unlike traditional malware-based persistence techniques, RMM tools are often whitelisted in enterprise environments, allowing Monti to remain undetected by endpoint detection and response (EDR) solutions. Once installed, Monti operators can execute commands, move laterally, and deploy additional payloads without triggering security alerts.

Leveraging Living-Off-the-Land Binaries (LOLBins) for Evasion

Monti's latest attacks show an increased reliance on Living-Off-the-Land Binaries (LOLBins) - legitimate system tools that cybercriminals abuse to execute malicious actions. These tools, such as PowerShell, WMIC (Windows Management Instrumentation Command), and PsExec, allow attackers to blend in with normal system activity while executing ransomware payloads.

For example, Monti has been observed using PowerShell scripts to disable security solutions, clear event logs, and establish scheduled tasks for persistence. Additionally, the group leverages Windows Defender's built-in anti-malware scanning interface (AMSI) to execute malicious commands in memory, making traditional file-based detection methods ineffective.

Targeting VMware ESXi and Linux Systems with Improved Encryption

While many ransomware groups primarily target Windows environments, Monti has significantly improved its Linux-based encryptor, with a specific focus on VMware ESXi servers. The latest Linux variant, identified as Ransom.Linux.MONTI.THGOCBC, introduces several changes from previous versions, including:

- **Switching from Salsa20 to AES-256-CTR encryption**, making decryption efforts more difficult.
- **Using the "--type=soft" parameter to shut down virtual machines** before encryption, allowing attackers to minimize corruption and avoid alerting system administrators.
- **Appending the "MONTI" infection marker to encrypted files**, which helps operators track compromised systems.

These improvements indicate that Monti is refining its Linux-based attacks, likely in response to organizations increasingly relying on virtualized environments for critical infrastructure.

Image 1: Ransom Note

All of your files are currently encrypted by BIDON strain. If you don't know who we are - just "Google it."

As you already know, all of your data has been encrypted by our software.
It cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files. However,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.

We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of whole compromised data immediately.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://myosbja7hixkkjqihsjh6yvmqplz62gr3r4isctjjtu2vm5jg6hsv2ad.onion/chat/[snip]/

Also visit our blog (via Tor):
http://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid.onion/

Source: Ransomware.live

Data Exfiltration and Double Extortion Tactics

Monti has fully adopted double extortion, where files are not only encrypted but also exfiltrated before encryption. This allows the group to pressure victims into paying the ransom by threatening to leak sensitive data on dark web forums.

Monti uses tools like MEGASync, WinSCP, and Rclone to transfer stolen data to cloud storage services before deploying its encryption payload. Some victims have reported that ransom notes include a preview of stolen files. By using data exfiltration before encryption, Monti ensures that even if victims restore their systems from backups, they still face the risk of data exposure.

Network Propagation Through Credential Dumping and Lateral Movement

Monti operators prioritize network propagation, making certain that once initial access is gained, they can move laterally and infect as many systems as possible. The group uses credential dumping techniques to extract usernames and passwords from compromised machines, often leveraging:

- Mimikatz to extract credentials stored in memory.
- Veeam-Get-Creds and Veeamp to steal backup credentials from Veeam Backup & Replication software.
- LSASS memory dumps to obtain Active Directory administrator credentials.

Once credentials are acquired, Monti uses Remote Desktop Protocol (RDP), SMB, and PsExec to move laterally and deploy ransomware across multiple endpoints, including backup servers.

Disrupting Incident Response and Recovery Efforts

Monti employs several techniques to disrupt incident response efforts, making recovery more challenging for targeted organizations. These include:

- **Disabling security tools** – PowerShell scripts and registry modifications are used to disable Windows Defender, antivirus solutions, and forensic logging tools.
- **Clearing event logs** – The attackers erase Windows Event Logs to cover their tracks and prevent forensic analysis.
- **Encrypting backup servers** – By targeting Veeam and other backup solutions, Monti ensures that victims cannot easily restore encrypted files.

Organizations that do not implement offline backups or immutable storage often find themselves unable to recover from Monti ransomware attacks, increasing the likelihood of ransom payments.

Recent Attacks

SCV Med Group (January 2025)

On January 31, 2025, SCV Med Group, a healthcare provider in Santa Clarita, California, was targeted by the Monti ransomware group. The attack resulted in the compromise of sensitive patient records and internal documentation, including data related to primary care services and weight management programs. While the full extent of the breach remains undisclosed, Monti likely used double extortion tactics, stealing data before encryption to pressure victims into paying a ransom.

Given the sensitive nature of medical data, this attack raises concerns over HIPAA compliance, regulatory penalties, and patient privacy risks. If stolen records include personally identifiable information (PII) or medical histories, affected individuals could be vulnerable to identity theft and fraud. SCV Med Group has not confirmed whether it paid the ransom or managed to restore its systems independently.

Sole Technology (February 2025)

On February 11, 2025, Sole Technology, a well-known footwear and apparel company, also fell victim to a Monti ransomware attack. The breach was confirmed after RedPacket Security reported that Sole Technology had been added to Monti's leak site with a "full leak" designation, indicating that internal company data was likely exposed.

The attack disrupted supply chain management systems, encrypted financial records, and impacted logistics operations, potentially delaying shipments and affecting business continuity. Given the nature of the breach, Monti may have also exfiltrated sensitive corporate data, such as supplier contracts, product designs, and financial reports, using double extortion to demand payment.

Sole Technology has not disclosed whether it paid the ransom, but if a "full leak" occurred, it suggests that either negotiations failed or the ransom was not paid. The company may now face financial losses and legal scrutiny, especially if customer or employee data was exposed.

Conclusion

Monti's disruption in 2025, after its sale in June 2024, shows that cybercriminal operations don't just disappear - they evolve. The group has sharpened its tactics and expanded its targets, making it clear that businesses can't afford to be complacent. Strong endpoint security, regular patching, and employee training on phishing threats are essential to reducing the risk.

Monti's resurgence is another reminder that ransomware isn't going away anytime soon. Security teams need to stay ahead by tracking shifts in attack methods and reinforcing defenses to keep up with these constantly adapting threats.

Aspire's Recommendations

Given Monti ransomware's evolving tactics and ability to compromise organizations across multiple industries, businesses must implement targeted security measures to defend against its techniques. Aspire Technology Partners recommends the following to help keep your organization safe:

- Secure Remote Access and VPNs
  - Disable Remote Desktop Protocol (RDP) if not needed. If RDP is required, restrict access to specific IP addresses and enforce multi-factor authentication (MFA).
  - Monitor and restrict VPN access. Ensure VPN solutions are fully patched to prevent exploits like Log4Shell (CVE-2021-44228), which Monti has previously used.
  - Deploy brute-force protection for remote logins. Use account lockout policies and log monitoring to detect failed login attempts.
- Harden VMware ESXi and Linux Systems
  - Restrict access to VMware ESXi servers. Use firewall rules to allow only trusted IPs and implement strong authentication.

  - Monitor for unauthorized virtual machine shutdowns. Monti uses the --type=soft shutdown command to avoid detection before encrypting ESXi systems.
  - Disable SSH if not required. If SSH is needed, implement key-based authentication and restrict access to trusted users.
- Prevent Lateral Movement and Credential Theft
  - Block execution of Mimikatz and similar tools. Use Application Control Policies (AppLocker or WDAC) to prevent unauthorized credential dumping tools from running.
  - Enforce least privilege access. Limit administrative accounts and regularly audit user permissions to prevent privilege escalation.
  - Monitor for suspicious network scanning. Monti uses tools like netscan to identify accessible systems - set up alerts for unusual scanning behavior.
- Detect and Block Initial Access Techniques
  - Implement email filtering for phishing defense. Monti has used phishing campaigns to gain access - block executable attachments and flag emails from unknown senders.
  - Deploy endpoint detection and response (EDR) solutions. Ensure EDR tools can detect PowerShell abuse, LOLBins, and unauthorized RDP sessions, which Monti exploits.
  - Use network segmentation to isolate critical assets. Prevent an attacker from easily moving through the network by separating sensitive systems.

MITRE MAP

Initial Access	T1190 – Exploit Public Facing Application T1566 – Phishing
Execution	T1059.001 – Command and Scripting Interpreter T1059.004 – Command and Scripting Interpreter: Bash
Persistence	T1219 – Remote Monitoring and Management T1543 – Create or Modify System Process: Windows Service
Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism: Bypass Use Access Control T1558.002 – Steal or Forge Kerberos Tickets
Defense Evasion	T1070.001 – Indicator Removal on Host: Clear Windows Event Logs T1027 – Obfuscated Files or Information T1218.005 – Signed Binay Proxy Execution: Mshta
Credential Access	T1003.001 – OS Credential Dumping: Mimikatz T1552.001 – Unsecured Credentials: Credentials in Fils

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both

automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Veeam Credential Dumper SHA-256 hashes:

- 9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732
- df492b4cc7f644ad3e795155926d1fc8ece7327c0c5c8ea45561f24f5110ce54
- 78517fb07ee5292da627c234b26b555413a459f8d7a9641e4a9fcc1099f06a3d

SUPPORTING DOCUMENTATION

[MONTI] - Ransomware Victim: sole technology - RedPacket Security

monti details

Monti Ransomware Strikes SCV Med Group: Latest Cyber Attack Unveiled - UNDERCODE NEWS

Monti Ransomware Strikes Sole Technology: A New Threat Emerges - UNDERCODE NEWS

Ransom! sole technology – Cybersecurity News Everyday

Monti Ransomware Targets nenokde: A New Attack Unveiled - UNDERCODE NEWS

Monti Ransomware: the new threat to systems - SOS Ransomware

The Curious Case of “Monti” Ransomware: A Real-World Doppelganger

Ransomware.live - Ransom Notes for monti

Monti Ransomware Unleashes a New Encryptor for Linux | Trend Micro (US)

Monti Ransomware Sold! New Owners Hint Future Plans

Monti Ransomware Unleashes a New Encryptor for Linux | Trend Micro (US)

Monti Ransomware New Linux Variant Attacking Industries

The "Full Monti": Individual Threat Actor Attribution in RaaS Operations

Monti ransomware targets legal and gov’t entities with new Linux-based variant | The Record from Recorded Future News

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.