Digital Asset Redemption

DRKMDR

The "Full Monti"

Individual Threat Actor Attribution in RaaS Operations

January 6, 2025

Author: Matthew Leidlein

Executive Summary

Monti, a ransomware variant first identified in early 2022, was recently observed in an engagement by DAR's threat intelligence team. While "Monti" does not appear on OFAC's list of sanctioned groups and individuals, DAR was able to identify the likely involvement of a sanctioned individual, Mikhail Matveev (aka "Wazawaka"), in the attack.

Sanctions compliance, when applied to ransomware payments, is a fraught process: threat actors hide behind a cloak of anonymity, often for the express purpose of sanctions evasion[1]. When ransomware groups are sanctioned, those groups either dissolve, rebrand, or disappear; when individual threat actors are sanctioned, they often continue to operate within the ransomware economy.

Assessing the involvement of sanctioned threat actors, though uncertain and complicated, may be an important step in assessing the regulatory and reputational risks involved in making ransomware payments.

This report details how DAR's investigation identified Matveev's involvement, by (1) reviewing readily-available open-source intelligence (OSINT) connecting Monti and Matveev; (2) connecting the incident to prior human intelligence (HUMINT) about Matveev, and (3) confirming the connection with Law Enforcement (LE).

[1] See, for instance, "To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions" Mandiant Intelligence, June 2, 2022; https://cloud.google.com/blog/topics/threat-intelligence/unc2165-shifts-to-evade-sanctions.

Key Findings

Mikhail Matveev, a Russian national, was sanctioned by OFAC in May, 2023 for “his role in launching cyberattacks against U.S. law enforcement, businesses, and critical infrastructure.”[2]

According to numerous open-source intelligence observations – including a direct interview with Matveev himself[3] – Matveev has continued to attack companies as a member of several different ransomware groups.

DAR must be constantly vigilant to the possibility a ransomware payment it assists with may reach a sanctioned entity or jurisdiction. Threat intelligence is DAR’s main defense against this possibility; informed attribution precedes any transaction DAR participates in.

In a recent case, DAR was able to identify, with high confidence, a risk that a prospective payment to the “Monti” ransomware group would reach a sanctioned individual, Mikhail Matveev. Upon identifying the highly-likely attribution between Monti and Matveev, DAR flagged the risk for its client and did not make the prospective payment.

Background: Wazawaka Threat Actor Profile

Mikhail Pavlovich Matveev – often known by his alias, "Wazawaka" – is a key figure in the ransomware world, notorious for his brazen personality, versatile technical skills, and association with multiple high-profile ransomware operations. Matveev's unapologetic embrace of his cybercriminal activities have made him both a target of law enforcement and a subject of fascination in the cybersecurity community. He has openly bragged about his exploits, taunted law enforcement agencies, and was an early advocate for “double extortion”, the public release of data stolen from victims who refuse to pay ransoms.

Historical Activities

Matveev has been associated with a wide range of ransomware groups throughout his cybercriminal career. Some of the most notable groups he has been linked to include[4]:

- **LockBit:** Matveev initially worked as an affiliate for the LockBit ransomware gang in 2020, claiming to have earned substantial profits. He maintained connections with prominent LockBit figures like “Bassterlord”, an access broker who supplied initial entry points into victims' systems.

[2] “Treasury Sanctions Russian Ransomware Actor Complicit in Attacks on Police and U.S. Critical Infrastructure.” U.S. Department of the Treasury, May 16, 2023, https://home.treasury.gov/news/press-releases/jy0628.
[3] Dina Temple-Raston. “A Q&A with Wazawaka: The FBI’s Cyber Most Wanted Says New Designation Won’t Affect His Work.” The Record from Recorded Future News, May 20, 2023, https://therecord.media/wazawaka-cyber-most-wanted-interview-click-here.
[4] This section relies heavily on PRODAFT’s outstanding research into Matveev, “Smoke and Mirrors: Understanding the Workings of Wazawaka.” PRODAFT, December 5, 2023. https://25491742.fs1.hubspotusercontent-eu1.net/hubfs/25491742/WAZAWAKA_TLPCLEAR_Report.pdf.

- **Babuk:** Matveev, using the alias "Boriselcin," emerged as the public face and spokesperson for the Babuk ransomware affiliate program in late 2020. He was directly involved in the notorious attack on the Washington D.C. Metropolitan Police Department in 2021[5].
- **Payload.bin:** After Babuk shut down, its website redirected to Payload.bin, a site also linked to Matveev. This platform eventually transformed into RAMP, a ransomware forum that Matveev allegedly founded.
- **Hive:** Matveev publicly admitted to working with the Hive ransomware group as an affiliate. The Justice Department indictment against Matveev also accuses him of involvement in Hive ransomware attacks.
- **Monti:** Following Babuk's closure, Matveev became a key figure in the Monti ransomware operation, working closely with Dudka, who is believed to be Monti's developer.
- **Trigona:** Matveev and his team utilized the Trigona ransomware in attacks against various organizations. PRODAFT's highlighted Matveev's admiration for Trigona's features and services, including the built-in call center used to pressure victims into paying ransoms.
- **NoEscape:** Matveev is known to have used the NoEscape ransomware variant since June 2023.
- **Conti:** Matveev and his team also participated as affiliates of the Conti ransomware group. Matveev claimed to have orchestrated a Conti attack against Costa Rica.

Matveev's ability to operate within such a diverse network of ransomware groups highlights his deep knowledge of the cybercriminal underworld, his adaptability, and his sophisticated understanding of the ransomware-as-a-service model.

Attribution Methodology

Attribution in cybercrime is complex. Identifying Mikhail Matveev in a ransomware attack requires a multifaceted approach, examining a combination of technical indicators, behavioral patterns, and known associations. Collaboration and the use of shared tools make it challenging to definitively link attacks to specific individuals.

While Matveev has worked with a wide range of ransomware groups, he and his team have demonstrated preferences for specific tools, tactics, and procedures (TTPs). Here are key indicators that DAR's threat intelligence team uses to assess the possibility of Matveev's involvement:

Observations:

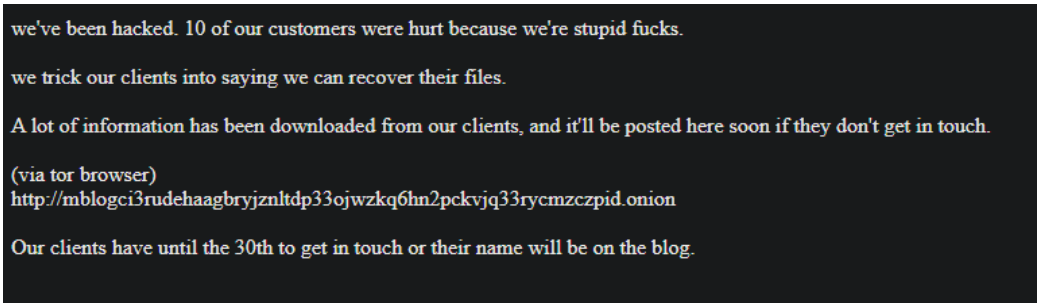
- **Exploitation of Specific Vulnerabilities:** Matveev and his team have a history of targeting known vulnerabilities in systems like Fortinet, Citrix, Mobile Iron, and Papercut. They often leverage publicly available exploits, sometimes with minor code modifications.
- **VPN Brute-Forcing:** Matveev has employed tools and scripts to brute-force credentials for VPNs, particularly targeting Fortinet VPNs. This tactic often serves as an initial access point into victim networks.

[5] "Ransomware Charges Unsealed Against Russian National." United States Department of Justice, May 16, 2023. https://www.justice.gov/usao-dc/pr/ransomware-charges-unsealed-against-russian-national.

● **Remote Access Software:** Matveev and his team often use legitimate remote access tools, primarily MeshCentral and AnyDesk, to establish command and control over compromised systems.
● **Cobalt Strike:** Matveev has criticized some ransomware operators for relying solely on Cobalt Strike, a widely-used penetration testing tool often employed by ransomware attackers for post-exploitation activities.
● **PowerShell:** Matveev and his team routinely use PowerShell commands for various tasks, including downloading and executing malicious payloads and establishing persistence within a victim's environment.
● **Open Source Tools and Custom Scripts:** Matveev and his team often rely on freely available tools and write their own simple scripts to carry out attacks. They prioritize efficiency and target "low-hanging fruit" – organizations with easily exploitable vulnerabilities.
● **Data Exfiltration Tools:** Matveev and his team typically use WinSCP and MEGA Client to exfiltrate sensitive data from victim networks.

Behavioral Patterns and Associations:

● **Victim Shaming:** Matveev is known for his aggressive "victim shaming" tactics, publicly releasing sensitive data stolen from organizations that refuse to pay ransoms. This brazen approach to extortion has been a hallmark of his operations, and extends to his negotiation tactics. A good example of Matveev's taunting[6]:



● **Public Persona and Communications:** Matveev has a distinctive public persona, often boasting about his exploits and engaging with journalists and researchers. DAR's intelligence team examines direct interactions, communications with victims, and activity on cybercrime forums to reveal language patterns and behavioral traits consistent with his known style.
● **Victim Engagement:** Matveev is hostile and anti-sympathetic towards victims. Engagement with Matveev (in the capacity of negotiating a ransom) is often met with ridicule and antagonism. Matveev imposes a strict communication cadence and escalates without provocation. This behavior is unlike many ransomware operators who conduct negotiations on behalf of their team.

Considerations:

[6] https://x.com/DarkWebInformer/status/1832594278687625219.

● Matveev is adaptable and has shifted between different ransomware groups and tactics over time.
● Matveev's status within the Russian-speaking ransomware community affords him the ability to join new operations with little or no discretion - making it difficult to track his current involvement.
● His OPSEC practices are inconsistent. While he utilizes VPNs and Tor for anonymity, he has also been known to reveal personal details carelessly.

Treasury Sanctions Context

In May 2023, the United States government initiated a series of actions against Mikhail Matveev for his alleged role in numerous ransomware attacks. These actions, coordinated across multiple agencies, aimed to disrupt Matveev's operations, hold him accountable for his crimes, and deter future cybercriminal activity:

● **The U.S. Department of Justice unsealed two indictments against Matveev**[7]: One indictment, filed in the District of Columbia, charged him with participating in a global ransomware campaign, including the attack on the Washington D.C. Metropolitan Police Department. The second indictment, filed in the District of New Jersey, involved similar charges related to ransomware attacks in that state.
● **The U.S. Department of State announced a reward of up to $10 million** for information leading to Matveev's arrest and/or conviction under the Transnational Organized Crime Rewards Program[8].
● **The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Matveev as a Specially Designated National (SDN)**[9]. This designation, made pursuant to Executive Order 13694, blocked all of Matveev's property and interests in property within U.S. jurisdiction. The designation also prohibits U.S. persons from engaging in any transactions with Matveev.

The combination of criminal charges, a substantial reward offer, and financial sanctions aims to severely limit Matveev's ability to operate and serve as a deterrent to others involved in ransomware activities. In the context of a ransomware incident, the actions provide a clear prohibition against paying a ransom to Matveev.

[7] "Ransomware Charges Unsealed Against Russian National." *ibid.*
[8] "The Department of State Announces Reward Offer Against Russian Ransomware Actor." United States Department of State, May 16, 2023. https://www.state.gov/the-department-of-state-announces-reward-offer-against-russian-ransomware-actor/.
[9] "Treasury Sanctions Russian Ransomware Actor Complicit in Attacks on Police and U.S. Critical Infrastructure." *ibid.*

Background: RaaS Operational Model

The RaaS (Ransomware-as-a-Service) model – generally speaking – operates through a structured developer-affiliate relationship that defines roles, responsibilities, and profit-sharing arrangements. This split structure can be one of the most salient pieces of information during the process of threat actor attribution.

Developer Side

Ransomware software developers create software to host the command-and-control functions of a ransomware attack, maintain the ransomware payload that encrypt and exfiltrate victims' data, and facilitate the decryption process if a payment is made. Developers' motivation centers on creating reliable software, as failures in these processes discourage payments. Quality ransomware software that encrypts quickly and handles multiple file types without corruption is a valuable asset for affiliates conducting attacks, and how developers encourage their users – ransomware affiliates – to use their ransomware software over another group's.

Affiliate Side

Conversely, the users – "ransomware affiliates" – are the threat actors conducting attacks using the RaaS software from the developers. Typically there is a profit sharing model, where the affiliates take around 80% of a successful ransom, and the developer receives 20% for the use of that RaaS software. However, this profit sharing number is negotiable. Developers might offer "big" ransomware names – such as Matveev – a higher proportion of the ransom (90%/10%, for instance) if he uses their RaaS software over a competitors, knowing his past success rate will be more of a guarantee, and hoping they might gain more users through social capital.

Background: Monti Operational Model

DAR's intelligence and OSINT research describes several tactics, techniques, and procedures (TTPs) commonly employed by the Monti ransomware group[10]:

- **Exploitation of Known Vulnerabilities:** Monti operators have targeted well-known vulnerabilities, such as the Log4Shell vulnerability (CVE-2021-44228), to gain initial access to victims' networks. This tactic leverages existing security flaws in widely used software, often before patches are widely implemented.
- **Remote Monitoring and Maintenance (RMM) Agent Abuse:** Monti actors have been observed using legitimate RMM agents, specifically the Action1 RMM agent, to establish a foothold and move laterally within a compromised network. This tactic exploits the inherent trust and access privileges associated with RMM software for malicious purposes.
- **Credential Dumping, Lateral Movement, and Backup Targeting:** Monti attackers utilize tools like Mimikatz and custom credential dumpers (like "Veeamp" targeting Veeam backup software)

[10] This section also relies heavily on PRODAFT's outstanding research into Matveev, "Smoke and Mirrors: Understanding the Workings of Wazawaka." *ibid*.

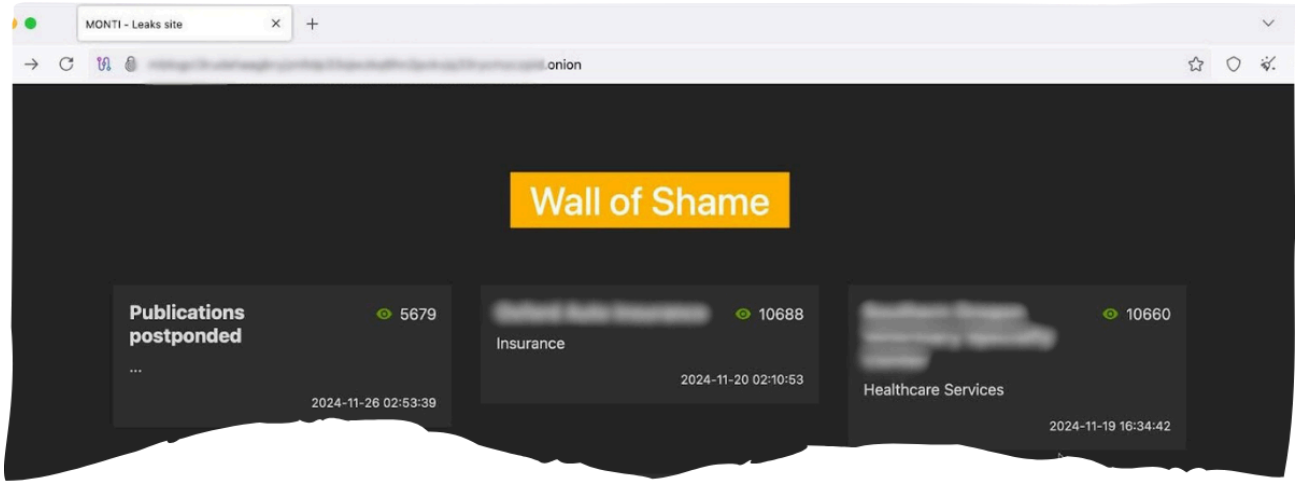
to steal credentials from compromised systems. They then leverage these stolen credentials, along with tools like PSEXEC, to move laterally within the network and gain access to critical systems and data and prevent the victim from restoring by using backup data.

- **Data Exfiltration:** Monti operators prioritize stealing sensitive data from victims' networks for double extortion purposes. They often use file-sharing websites like dropmefiles.com[.]ua and temp[.]sh, along with data transfer tools like PuTTY and WinSCP, to exfiltrate this data.
- **Intermittent Encryption:** Monti ransomware (like Conti, its predecessor) is known for employing intermittent encryption, encrypting only portions of targeted files to speed up the encryption process and potentially evade detection.
- **Multi-Platform Targeting:** Monti ransomware has variants for both Windows and Linux operating systems, demonstrating its ability to target a wider range of systems and environments.
- **Ransomware-as-a-Service (RaaS) Model:** While initially operating as a closed RaaS, Monti eventually opened up its affiliate program, recruiting other cybercriminals to carry out attacks using its ransomware. Recruitment efforts eventually stalled, and the group is believed to be operating autonomously once again - consisting of a small team of individual contributors who split the proceeds of a successful ransom.
- **Focus on High-Value Targets:** Monti operators tend to prioritize targeting organizations in sectors like government, legal, and healthcare, likely due to their perceived willingness to pay ransoms to restore critical services and protect sensitive data.
- **Similarity to Conti TTPs:** Monti intrusion activity has closely aligned with some TTPs employed by Conti ransomware operators. This lends credence to Matveev's claims of involvement in the attack on Costa Rica. Monti initially appeared to use the version of Conti source code that leaked in 2022; subsequent updates to Monti's source code have reduced the similarity between Monti and Conti's leaked code[11].

On June 12, 2024, Monti's TOR site announced that the project had been sold, putting some prior intelligence about the makeup of the RaaS program into question[12]. DAR's intelligence team finds no corroborating evidence of the claimed transaction, and treats the announcement with a high degree of skepticism. Monti's uncertain ownership structure highlights the importance of case-by-case investigations into potential threat actor attribution.

On November 26, 2024 an announcement on the official Monti blog stated, "Publications postponed" - an indication that no further announcements of Monti's victims would be made until further notice.

[11] Morales, Nathaniel, and Joshua Paul Ignacio. "Monti Ransomware Unleashes a New Encryptor for Linux." Trend Micro (US). https://www.trendmicro.com/en_us/research/24/l/monti-ransomware-unleashes-new-encryptor-for-linux.html.
[12] "Monti Ransomware Sold! New Owners Hint at Future Plans." Cybersecurity News , November 27, 2024. https://cybersecuritynews.com/monti-ransomware-sold.



On November 29, 2024, Russian state news announced Matveev's arrest in Kallingrad[13]. On November 30, 2024, an independent security researcher reported that Matveev had posted bail and was released awaiting trial[14].

Investigation: DAR's Recent Monti Case Analysis

Attribution Methodology

DAR's attribution process relies on:

- Analysis of negotiation transcripts and initial contact interactions
- Behavioral patterns consistent with Matveev's known historical activities
- Analysis of threat actor capabilities and infrastructure
- Intelligence confirmation from trusted sources
- Intelligence sharing with federal law enforcement and international law enforcement

Case Involvement

DAR identified Wazawaka's involvement in the Monti ransomware negotiations from the first interaction. His signature intimidation tactics and aggressive negotiation style during victim engagement provided clear attribution markers. Analysis of negotiation transcripts and initial contact interactions confirmed his presence through these unmistakable behavioral patterns.

[13] "В Калининграде буду судить программиста, разыскиваемого ФБР" ["In Kaliningrad, a programmer wanted by the FBI will be tried"]. RIA Novosti, November 29, 2024. https://ria.ru/20241129/sud-1986456557.html.
[14] https://x.com/club31337/status/1862985153183633466

Developer Attribution

Upon case intake, DAR received an image of the ransom note left on the victim's systems. The threat actor identified themselves as part of the Monti group: The note was an exact match with prior Monti observations, beginning, "All your files are currently encrypted by MONTI strain. If you don't know who we are - just "Google it.""[15].

The note directed the victim to a non-repudiable TOR website which hosted the negotiation chat, and also to Monti's data leak and shaming site, also a TOR site. Negotiations were conducted via the TOR website, a clear indication that the threat actor was indeed affiliated with Monti. DAR assisted the client with obtaining "proof of life" in the negotiation – evidence that the threat actor had exfiltrated data and could decrypt encrypted files.

Affiliate Attribution

DAR attributed the attack to Matveev because of his distinctive engagement style during ransom negotiations. These behavioral fingerprints are consistently observed and documented in Matveev's involvement across multiple ransomware operations, making it a reliable identifier for attribution purposes. Matveev's signature approach includes:

- Intense, aggressive negotiation tactics
- Distinctive bullying patterns
- Consistent behavioral markers across multiple operations
- Unique victim engagement methods

During negotiations, these behavioral tactics were quick to emerge. The victim was mocked for attempting to negotiate the amount of a prospective cryptocurrency payment. Despite ongoing communication between the victim and threat actor, the victim received an email threat from an anonymous @proton[.]me address, apparently to pressure for a faster resolution. Similar pressure was applied in the TOR chat panel.

The consistency and uniqueness of these patterns provides a high degree of confidence in attributing Monti operations to Matveev when these specific negotiation characteristics are present. When DAR's attribution suggests the involvement of a sanctioned geography, entity, or individual, DAR consults the

[15] Anuj Soni and Ryan Chapman, "The Curious Case of "Monti" Ransomware: A Real-World Doppelganger," BlackBerry Blog, 7 Sept. 2022, https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger.

Federal Bureau of Investigation to be sure its findings match those of US Law Enforcement (as OFAC recommends[16][17]).

Law Enforcement Verification

Upon identifying Matveev's behavioral patterns using Monti ransomware, bolstered by Prodaft's report tying Matveev as an affiliate to the Monti ransomware group, DAR escalated the case to the FBI field office assigned to Matveev. This step ensured proper sanctions compliance evaluation and maintained the necessary distinction between Monti as a RaaS platform and Matveev as a sanctioned affiliate.

Implications

Threat actor attribution extends beyond simple categorization of ransomware groups – such as Hive, Lockbit, Conti, etc. – as sanctioned or not. Sanctioned individuals like Matveev actively operate as affiliates across multiple platforms, including within non-sanctioned groups. A group-level sanctions assessment alone fails to identify the involvement of sanctioned individuals operating within technically "clean" platforms. Affiliate-level attribution addresses these inadequacies by evaluating all likely recipients of a prospective ransom payment.

The RaaS model splits responsibility between developers and affiliates, allowing sanctioned individuals to operate within non-sanctioned ransomware platforms. When sanctioned individuals like Matveev deploy ransomware through non-sanctioned groups, an affiliate-centric attribution process using available behavioral markers, technical indicators, and negotiation patterns can help identify their presence.

Attribution confidence increases when multiple technical and behavioral indicators align. The combination of specific tool preferences, communication patterns, and operational behaviors reduces uncertainty – both tactical (when engaging the threat actor) and regulatory (when contemplating the legal implications of different response options)s. Law enforcement verification provides an additional layer of confidence when evaluating potential sanctions risks.

Appendix: Does Every Monti Incident Involve Matveev?

Not necessarily. Matveev's involvement in Monti remains unclear and it is possible that he is one of several affiliates of a development program in which he maintains no direct involvement.

---

[16] U.S. Department of the Treasury, Office of Foreign Assets Control, "Advisory on Potential Sanctions Risks for Facilitating Ransomware
Payments" October 1, 2020. https://ofac.treasury.gov/recent-actions/20201001.

[17] U.S. Department of the Treasury, Office of Foreign Assets Control, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" September 21, 2021.
https://ofac.treasury.gov/media/912981/download?inline.