TIR-20250211 Game Over - 8Base Arrests and What Happens When Ransomware Groups Go Dark

2/11/2025

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

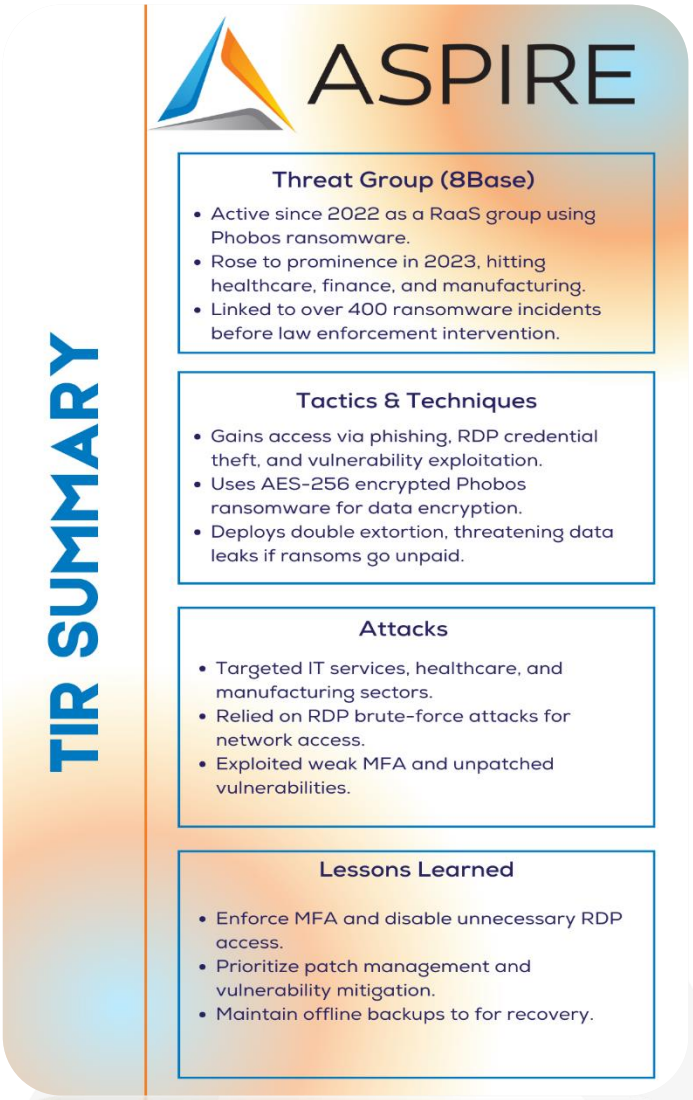
TABLE OF CONTENTS

EXECUTIVE SUMMARY

8Base is a Russian Ransomware-as-a-Service (RaaS) operation that gained prominence in 2023, targeting small and medium-sized businesses through double-extortion tactics. The group leveraged Phobos ransomware, a widely used ransomware strain, to encrypt victims' data and extort payment. Despite being a relatively new threat actor, 8Base demonstrated sophisticated operational security and aggressive negotiation tactics, leading to numerous successful extortion campaigns.

However, that success came to a screeching halt on February 11, 2025, when an international law enforcement operation led by Europol, the FBI, and other agencies resulted in the arrest of four key members of 8Base. Additionally, 27 servers hosting their leak site and infrastructure were seized – a blow to the group's operations.

Although the arrests and seizures are a step in the right direction, history shows that that ransomware groups rarely disappear entirely. Instead, they rebrand, merge with other criminal operations, or migrate to new RaaS platforms. The dismantling of 8Base does not mean the end of its ransomware.



8BASE RANSOMWARE

8Base first appeared in early 2022, operating in the shadows until mid-2023, when its attacks became more frequent and aggressive. Unlike other ransomware groups that develop proprietary malware, 8Base relied on the well-established Phobos ransomware, deploying it through a network of affiliates who executed the attacks. The group focused on industries with low cybersecurity maturity, such as healthcare, financial services, and manufacturing.

8Base uses the double extortion model, meaning victims were not only locked out of their data but also faced the threat of having sensitive information leaked online if they refused to pay. The attack chain often started with phishing attempts, compromised Remote Desktop Protocol (RDP) credentials, or exploiting known vulnerabilities in unpatched systems. Once inside, attackers moved quickly to escalate privileges and spread ransomware across networks.

TACTICS & TECHNIQUES

8Base used a mix of well-known and covert tactics to break into networks and stay undetected. The group heavily relied on **phishing campaigns to trick users** into downloading malicious attachments or clicking on links that deployed malware loaders. Additionally, they exploited **RDP configurations**, using brute-force attacks to gain unauthorized access to systems.

Once inside a network, 8Base affiliates used tools like Mimikatz to extract credentials from memory, allowing for privilege escalation and lateral movement. They used PsExec and Windows Management Instrumentation (WMI) for remote execution, allowing them to spread the ransomware payload across multiple machines efficiently. Attackers would often disable endpoint detection and response (EDR) solutions, modifying registry settings to prevent security software from detecting malicious activity.

To ensure maximum damage, 8Base ransomware operators **deleted volume shadow copies using PowerShell commands** and **disabled system recovery options**, leaving victims with few options for data restoration. The Phobos ransomware strain

utilized **AES-256 and RSA encryption**, ensuring files were rendered completely inaccessible without the private decryption key.

After encryption, victims were presented with ransom notes instructing them to initiate communication through secure email or Tor-based portals. If ransom demands were not met, stolen data was published on 8Base's leak site as further leverage. Some victims who attempted to negotiate were subjected to increased ransom demands, as 8Base affiliates were known for their aggressive bargaining tactics.

8Base showed a clear grasp of forensic countermeasures, using secure deletion techniques to wipe logs and cover their tracks. The group regularly switched up its command-and-control (C2) infrastructure, making it harder for cybersecurity teams to trace their movements or shut them down. These tactics helped 8Base stay under the radar for long stretches, prolonging the damage to their targets.

Phobos and Its Connection to 8Base

Phobos is a ransomware strain that first appeared in 2019, evolving from the older Dharma ransomware family. It has been widely used by cybercriminals, including 8Base affiliates, due to its ease of deployment and strong encryption capabilities.

Phobos Ransomware Features:

- Uses AES-256 encryption, making decryption without the key nearly impossible.
- Targets Windows-based networks, spreading via exposed RDP services.
- Includes automated propagation mechanisms, moving laterally across networks.
- Uses custom ransom notes, instructing victims to contact attackers via email or Tor-based portals.

8Base's use of Phobos highlights how RaaS groups can launch attacks without building their own ransomware, allowing them to move fast and hit hard.

LAW ENFORCEMENT

On February 11, 2025, Europol, in collaboration with the FBI and Swiss authorities, announced the arrest of four individuals tied to the 8Base ransomware group. The operation was part of a broader international cybercrime crackdown that led to the seizure of 27 servers used to facilitate ransomware attacks and manage victim negotiations. Europol reported that these individuals were key figures responsible for orchestrating ransomware campaigns and managing ransom payments through cryptocurrency laundering networks.

Authorities identified over 400 confirmed victims, some of whom had already been warned prior to encryption. The operation also uncovered details about 8Base's financial infrastructure, revealing how ransom payments were funneled through various digital currency exchanges and laundering services to obscure the origins of illicit funds.

Sample of Victim List

- The Traffic Tech (Gulf) - A logistics and transportation company.
- Telepizza - A multinational pizza delivery chain.
- Quikcard Solutions Inc. - A provider of health and benefits programs.
- Jadranka Group - A conglomerate involved in tourism and hospitality.
- Dental One - A dental service provider.
- ANL Packaging - A manufacturer of plastic packaging products.
- BTU SA - An Argentine company specializing in engineering and construction projects.

While these arrests and server takedowns have significantly disrupted 8Base's operations, law enforcement officials caution that the group's affiliates and operators are still active. Many RaaS groups rely on decentralized structures, meaning that other operators could continue using Phobos ransomware under different banners. In addition, some of the group's stolen data and decryption keys may still be in circulation,

creating the potential for further extortion attempts even after the group's infrastructure has been dismantled.

Law enforcement stressed that this takedown is just one piece of a broader effort to disrupt ransomware operations, with ongoing collaboration between cybersecurity experts, financial institutions, and global agencies. Even with this success, security professionals can't afford to be complacent - ransomware groups have a history of rebranding and resurfacing under new names.

Ransomware Rebranding Cycle

If history has taught us anything, it's that cybercriminal organizations do not simply vanish - they adapt. Following the takedown of Conti ransomware in 2021, its members didn't retire; they joined forces with other gangs, spawning groups like BlackCat, AvosLocker, and Hive. A similar fate may await 8Base.

Ransomware operators are creatures of habit. They reuse infrastructure, recycle ransom note language, and sometimes even forget to change old email addresses linked to their previous aliases. BlackMatter, for instance, was identified as a rebranded version of DarkSide due to its nearly identical encryption techniques and operational guidelines. The same scenario could unfold with 8Base. Security professionals must continue tracking these actors to identify emerging threats before they strike again.

Conclusion

The arrests of key 8Base operators are a step forward, but ransomware remains a persistent threat. The Phobos ransomware strain used by 8Base remains a threat, and its affiliates could easily rebrand or shift to other ransomware services.

To stay ahead of ransomware attacks, organizations need to strengthen access controls, implement robust endpoint detection, and continuously monitor for risks. The 8Base takedown is a reminder that ransomware gangs will continue operating as long as vulnerabilities exist, and victims pay ransoms.

ASPIRE'S RECOMMENDATIONS

8Base may be disrupted, but that doesn't mean organizations can let their guard down. Ransomware is still a persistent threat, and staying proactive is the always the best option. Aspire Technology Partners recommends the following to help keep your organization safe:

- **Enforce Strong Multi-Factor Authentication (MFA)** – Require MFA for all remote access points, particularly for RDP and VPN connections, to mitigate the risk of credential-based attacks.
- **Deploy Endpoint Detection and Response (EDR) Solutions** – Utilize advanced EDR tools to detect and block ransomware behaviors, such as credential dumping, unauthorized privilege escalation, and anomalous network activity.
- **Enforce Principle of Least Privilege (PoLP)** – Restrict administrator privileges to essential users only, and regularly audit permissions to prevent unauthorized access.
- **Develop a Comprehensive Incident Response Plan** – Ensure that a well-documented ransomware incident response plan is in place, including clear steps for containment, eradication, and recovery. Regularly test the plan through tabletop exercises.
- **Implement Regular Offline Backups** – Maintain up-to-date, immutable backups that are disconnected from the network to ensure quick recovery in the event of an attack.

MITRE MAP

Initial Access	T1078 – Valid Accounts T1133 – External Remote Services
Execution	T1059 – Command and Scripting Interpreter
Privilege Escalation	T1552 – Unsecured Credentials
Impact	T1486 Data Encrypted for Impact

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)

MD5

- 0900b61febed8da43708f6735ed6c11b
- 20d9fa474fa2628a6abe5485d35ee7e0
- 2809e15a3a54484e042fe65fffd17409
- 62885d0f106569fac3985f72f0ca10cb
- 69788b170956a5c58ebd77f7680fde7c
- 9376f223d363e28054676bb6ef2c3e79
- a567048dd823ff2d395ddd95d1fa5302
- b119cdd3d02b60009b9ad39da799ed3b
- db74cd067d4a0562b26ea4f10e943e3b
- e59ffeaf7acb0c326e452fa30bb71a36

SHA1

- aed68cfa282ec2b0f8a681153beaebe3a17d04ee
- b092a6bf7fb6755e095ed9f35147d1c6710cf2c4
- c88fad293256bfead6962124394de4f8b97765aa
- cb37b10b209ab38477d2e17f21cae12a1cb2adf0

SHA256

- 0000599cbc6e5b0633c5a6261c79e4d3d81005c77845c6b0679d854884a8e02f
- 2704e269fb5cf9a02070a0ea07d82dc9d87f2cb95e60cb71d6c6d38b01869f66
- 32a674b59c3f9a45efde48368b4de7e0e76c19e06b2f18afb6638d1a080b2eb3
- 482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52
- 518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
- 58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6
- 7451be9b65b956ee667081e1141531514b1ec348e7081b5a9cd1308a98eec8f0
- 9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c
- a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2
- c0539fd02ca0184925a932a9e926c681dc9c81b5de4624250f2dd885ca5c4763
- f1425cff3d28afe5245459afa6d7985081bc6a62f86dce64c63daeb2136d7d2c
- f3be35f8b8301e39dd3dffc9325553516a085c12dc15494a5e2fce73c77069ed
- fc4b14250db7f66107820ecc56026e6be3e8e0eb2d428719156cf1c53ae139c6

Domain

- adstat477d[.]xyz
- demstat577[.]xyz
- serverxlogs21[.]xyz

SUPPORTING DOCUMENTATION

Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown | Europol

8BASE, THE NEWLY DISCOVERED RANSOMWARE GANG - Hackmanac

8base ransomware site taken down in global police operation | TechRadar

Law enforcement arrests 4 people in connection to 8base ransomware

8Base Ransomware: A Heavy Hitting Player - VMware Security Blog - VMware

8Base ransomware gang escalates double extortion attacks in June

Ransomware review: June 2023 - ThreatDown by Malwarebytes

8Base Ransomware Activity Spikes, Researcher Warn | Cyware Alerts - Hacker News

8Base - SentinelOne

ASIA Phobo Ransomware used by 8base - LevelBlue - Open Threat Exchange

logpoint-etpr-8base.pdf

Ransomware Spotlight: 8Base | Trend Micro (US)

8Base Threat Actor Profile - Quorum Cyber

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.