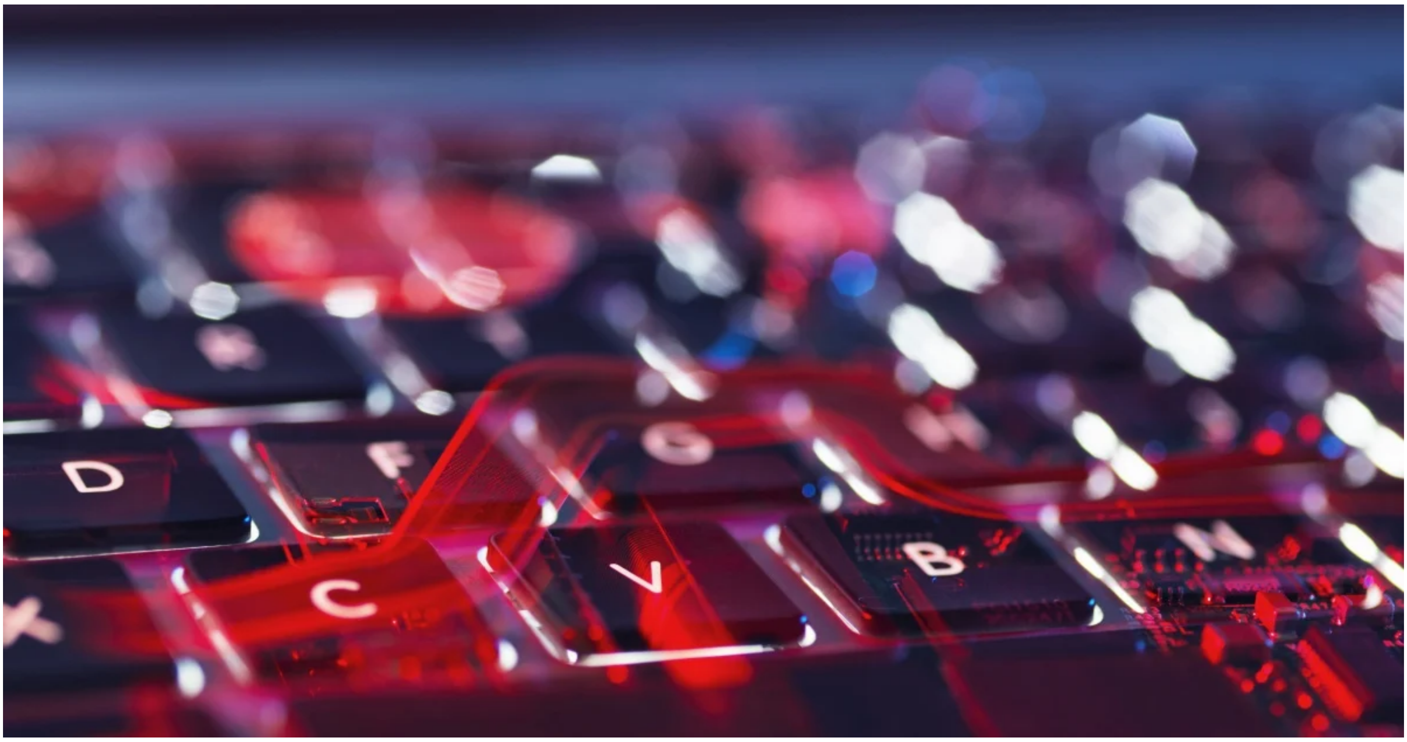
Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics



Attackers deploying the Noberus (aka BlackCat, ALPHV) ransomware have been using new tactics, tools, and procedures (TTPs) in recent months, making the threat more dangerous than ever.

Among some of the more notable developments has been the use of a new version of the Exmatter data exfiltration tool, and the use of Eamfo, information-stealing malware that is designed to steal credentials stored by Veeam backup software.

How does Noberus operate?

Noberus is widely believed to be a successor payload to the Darkside and BlackMatter ransomware families, which were developed by a group Symantec, by Broadcom Software, tracks as Coreid (aka FIN7, Carbon Spider). Darkside was used in the Colonial Pipeline ransomware attack in May 2021. The extreme amount of public and law enforcement attention that attack attracted led Coreid to shut down Darkside and replace it with BlackMatter. Coreid runs a ransomware-as-a-service (RaaS) operation, which means it develops the ransomware but it is deployed by affiliates for a cut of the profits. The ransomware being deployed by different affiliates can sometimes explain the different TTPs and attack chains used in Noberus attacks.

Noberus sparked interest when it was first seen in November 2021 because it was coded in Rust, and this was the first time we had seen a professional ransomware strain used in real-world attacks coded in that programming language. Rust is a notable language as it is cross-platform. Coreid claims that

Noberus is capable of encrypting files on Windows, EXSI, Debian, ReadyNAS, and Synology operating systems.

Noberus emerged shortly after BlackMatter announced it was being retired. Coreid sets out in the rules of its affiliate program that Noberus cannot be used to attack:

- The Commonwealth of Independent States or neighboring countries
- Organizations in or related to the healthcare sector
- Charitable or non-profit organizations
- Affiliates are also advised to avoid attacking the education and government sectors.

When announcing Noberus, Coreid underlined the features that appeared designed to emphasize its superiority to rival ransomware, including that each advert is provided with an entrance through its own unique onion domain; the affiliate program architecturally excludes all possible connections with forums; even if a full-fledged command line shell is obtained, the attacker will not be able to reveal the real IP address of the server, and encrypted negotiation chats that can only be accessed by the intended victim.

The ransomware also offered two encryption algorithms (ChaCha20 and AES), as well as four encryption modes - Full, Fast, DotPattern and SmartPattern. Full is the most secure but also the slowest mode. SmartPattern offers encryption of “N” megabytes in percentage increments. By default, it encrypts with a strip of 10 megabytes every 10 percent of the file starting from the header, which would be an optimal mode for attackers in terms of speed and cryptographic strength. Sentinel Labs recently published a report where it referred to this kind of encryption as “intermittent encryption” and mentioned how it had been adopted by certain ransomware operators, including Noberus, Black Basta, and more.

The percentage of each ransom that is paid to Noberus affiliates varies depending on the ransom amount. Coreid has continuously updated Noberus since its launch in November 2021 to make its operation more efficient. They will also cull affiliates if they are not bringing in enough money, encouraging them to “contact less professional teams”. In December 2021, the ransomware added a new “Plus” role for affiliates that had brought in more than $1.5 million. It gave access to:

- DDoS - used to target domains with DDoS attacks
- Calls - adding a field to indicate the phone numbers of the victim or add a contact number for the affiliate to communicate directly with victims if they wish
- Brute - making it possible to brute force NTDS, Kerberos tickets and other hashes for free

Coreid made a major update to Noberus in June 2022, which included:

- Introducing an ARM build for encryption of non-standard architectures
- Introducing SAFEMODE - Added encryption functionality to the Windows build via rebooting into safe mode (--safeboot) and safe mode with networking (--safeboot-network)

Coreid also made some updates to the locker, by adding new restart logic, and simplifying the Linux encryption process. In a July 2022 update the team added indexing of stolen data - meaning its data leaks websites can be searched by keyword, file type, and more.

The continuous updating and refining of Noberus’ operations shows that Coreid is constantly adapting its ransomware operation to ensure it remains as effective as possible. The FBI issued a warning in April

2022 saying that between November 2021 and March 2022 at least 60 organizations worldwide had been compromised with the Noberus ransomware - the number of victims now is likely to be many multiples of that.

Noberus and Exmatter: New version of data exfiltration tool used in ransomware attacks

In August 2022, a heavily updated version of the Exmatter (Trojan.Exmatter) data exfiltration tool was observed being used alongside Noberus in ransomware attacks.

Exmatter was discovered by Symantec researchers in November 2021 being used alongside the Blackmatter ransomware. It was designed to steal specific file types from a number of selected directories and upload them to an attacker-controlled server prior to deployment of the ransomware itself on the victim's network. Even at the time of its discovery, various variants of the tool were seen, as its developers continued to refine it to optimize its operation and expedite exfiltration of a sufficient volume of high-value data in as short a time as possible.

This latest version of Exmatter has reduced the number of file types it attempts to exfiltrate. It will now exfiltrate files with the following extensions only:

- .pdf, .doc, .docx, .xls, .xlsx, .png, .jpg, .jpeg, .txt, .bmp, .rdp, .txt, .sql, .msg, .pst, .zip, .rtf, .ipt, .dwg

Other new features include:

- Addition of third exfiltration capability (FTP) to SFTP and WebDav, which were present in older versions.
- Reports: Ability to build a report listing all processed files.
- Eraser: Can corrupt processed files (not turned on in version analyzed).
- Self-destruct: Configuration option, which, when enabled, will make the tool self-destruct and quit if executed in a non-corporate environment (outside of a Windows domain).
- Socks5: Socks5 support was removed.
- In at least one attack, the tool was deployed via GPO.

In addition to this, the malware was extensively rewritten, and even existing features were implemented differently. This was possibly a bid to avoid detection. Whether Exmatter is the creation of Coreid or a skilled affiliate of the group is not clear, but its use alongside two different iterations of Coreid's ransomware is notable. Its continuous development also underlines the focus of the group on data theft and extortion, and the importance of this element of attacks to ransomware actors now.

Noberus and Eamfo: Attackers using malware to steal credentials from Veeam

At least one affiliate of the Noberus ransomware operation was spotted in late August using information-stealing malware that is designed to steal credentials stored by Veeam backup software. Veeam is capable of storing credentials for a wide range of systems, including domain controllers and cloud services. The credentials are stored to facilitate the backup of these systems. The malware

(Infostealer.Eamfo) is designed to connect to the SQL database where Veeam stores credentials, and it steal credentials with the following SQL query:

- select [user_name],[password],[description] FROM [VeeamBackup].[dbo].[Credentials]

Eamfo will then decrypt and display the credentials.

Eamfo appears to have been in existence since at least August 2021 and there is evidence that it has previously been used by attackers using the Yanluowang and LockBit ransomware families. A recent report from BlackBerry also detailed Eamfo being used alongside a new ransomware strain it dubbed Monti, which appears to be based on the leaked source code of the Conti ransomware. The TTPs used in Monti attacks also closely resemble former Conti attack chains, suggesting those behind Monti may be former affiliates of that group. Conti was developed by a group Symantec tracks as Miner.

Stealing credentials from Veeam is a known attack technique that can facilitate privilege escalation and lateral movement, providing the attackers with access to more data they can potentially exfiltrate and more machines to encrypt.

Noberus attacks involving Eamfo seen by Symantec also utilized GMER, a relatively old rootkit scanner that can be leveraged by ransomware actors to kill processes. GMER usage by ransomware attackers appears to have become more frequent in recent months, and it was also seen in the Monti attack detailed by BlackBerry.

Conclusion

There’s no doubt that Coreid is one of the most dangerous and active ransomware developers operating at the moment. The group has been around since 2012, and became well-known for using its Carbanak malware to steal money from organizations worldwide, with the banking, hospitality and retail sectors among its preferred targets. Three members of the group were arrested in 2018, and in 2020 the group changed its tactics and launched its ransomware-as-a-service operation. Its continuous development of its ransomware and its affiliate programs indicates that this sophisticated and well-resourced attacker has little intention of going anywhere anytime soon.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

File hashes (SHA256)

ad5002c8a4621efbd354d58a71427c157e4b2805cb86f434d724fc77068f1c40 – Trojan.Exmatter

8c5b108eab6a397bed4c099f13eed52aeeec37cc214423bde07544b44a62e74a – Ransom.Noberus

78517fb07ee5292da627c234b26b555413a459f8d7a9641e4a9fcc1099f06a3d –Infostealer.Eamfo

9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732 –Infostealer.Eamfo df492b4cc7f644ad3e795155926d1fc8ece7327c0c5c8ea45561f24f5110ce54 –Infostealer.Eamfo

029dde7c2ec880fb3d3e95e6a8376739b4bc46a0ce24012e064b904e6ecb672c –Ransom.Noberus

72f0981f18b969db2781e874d249d8003c07f99786e217f84cf54a148de259cc –Ransom.Noberus

18c909a2b8c5e16821d6ef908f56881aa0ecceeaccb5fa1e54995935fcfd12f7 – GMER Driver

e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173 – GMER

ed6275195cf9fd758fb7f8bce868c14dc9e9d6b7aa6f472f714bce5ed7fabf7f – Masqueraded PAExec

5799d554307906e92749a0c45f21baff28d83b1cedccbf7cb6f2b98ac1b00930 – Masqueraded PAExec

File Names

sync_enc.exe

without_cert.exe

vup.exe

morph.exe

locker.exe

isgmer.exe

kgeyauow.sys