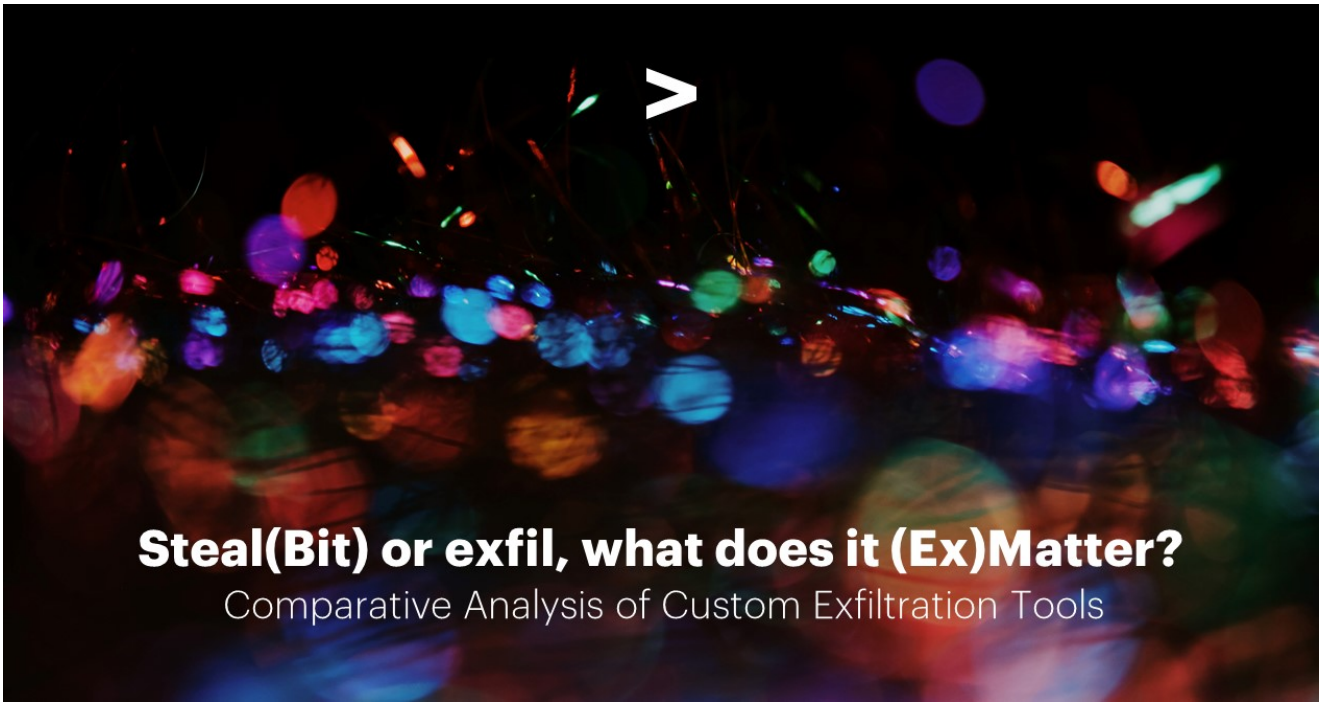
Steal(Bit) or exfil, what does it (Ex)Matter? Comparative Analysis of Custom Exfiltration Tools

accenture.com/us-en/blogs/security/stealbit-exmatter-exfiltration-tool-analysis



Security
Cyber Defense

June 28, 2022

Share

In the proliferation of Ransomware as a Service (RaaS) operations as showcased by our previous blog, "Diving into double extortion campaigns", tools to aid data exfiltration tactics have become a commodity. In addition to using ubiquitous tools such as Rclone, MegaSync, and FileZilla, ransomware and extortion groups have crafted custom exfiltration tools tailored to their operations. The continued use and development of these custom tools is a testament to their success, often simplifying and accelerating data exfiltration.

In this blog, we will examine two (2) exfiltration toolsets identified during CIFR incident response engagements conducted between the fourth quarter of 2021 and the first quarter of 2022: StealBit and ExMatter. We will provide a comparative and temporal analysis of the tools and the ongoing utilization and development efforts observed over time.

In brief:

- Discovered in 2021, StealBit and ExMatter are custom exfiltration tools that were originally known to be utilized by LockBit and BlackMatter ransomware operations, respectively.
- A testament to their functionality and effectiveness, these tools have gained popularity across the ransomware and extortion ecosystem.
- Since their original discovery, Accenture Security has observed modified versions of the tools utilized in multiple ransomware incidents involving BlackCat (aka ALPHV) and LockBit operators, as well as recent adoption by Conti operators, from the fourth quarter of 2021 and the first quarter of 2022.
- Based on comparative analysis of the tools, while data exfiltration is the consistent operational objective, the path to achieve that objective and the supporting functionality of each exfiltration tool varies slightly based on configuration, implementation details, and the operational environment. These variations can create challenges for network defenders.
- Furthermore, based on analysis of more than 15 samples, ExMatter adopts a more targeted approach to file discovery and exfiltration, while StealBit casts a wider net, especially for newer versions with geolocation restrictions removed.
- Of note, a modified version of ExMatter discovered in the first quarter of 2022 includes targeting of Computer Assisted Design (CAD) files, which suggests the operators are interested in exfiltrating data related to engineering documents or product designs that are common in industrial environments across the automotive, aviation, and manufacturing sectors.
- Based on analysis of samples obtained from various collection sources, Accenture Security assesses with high confidence that the tools are being continuously developed and improved upon by their authors, and utilization of the tools will continue into the second quarter of 2022 and beyond.

Q1 2022 Intrusion Analysis Insights

Symantec first publicly described **ExMatter** in November 2021 and connected the tool with at least one affiliate using the BlackMatter ransomware variant at the time. The presence of a modified version of ExMatter (aka Fendr) was revealed through investigations conducted by Accenture Security during several distinct ransomware incidents. Between the fourth quarter of 2021 and the first quarter of 2022, CIFR incident responders identified BlackMatter and BlackCat ransomware operators using various versions of the tool to aid exfiltration operations, as well as Conti ransomware operators during the same time period.

LockBit, formerly known as ABCD ransomware, was first launched in September 2019. However, it was not until LockBit's v2.0 release in June 2021 that the group developed and utilized the **StealBit** exfiltration tool in its operations.

During a recent investigation involving the LockBit v2.0 ransomware, Accenture Security discovered that the operators initially attempted to download StealBit from a remote server, but ultimately pivoted to the open-source utility Rclone as attempts to utilize the tool were prevented. This data point is a testament to the group's versatility as it shows that while the LockBit operators may prefer to use their custom tools, they will ultimately adopt a path of least resistance to achieve their objectives. Furthermore, development efforts for StealBit might have slowed as the more recent compiled versions observed were from the fourth quarter of 2021, which included updates for broader targeting through removal of geolocation restrictions, as well as the removal of creation time-date-stamp.

Industries impacted include the financial services, retail, professional services, and energy sectors, with victims across North America, Europe, and Australia.

Accenture Security assesses with high confidence that the tools are being continuously developed and improved upon by their authors as the more recent samples analyzed include additional features and options for customization. For example, a recent version of ExMatter analyzed during an incident response engagement included specific targeting of CAD files, which suggests the operators may be interested in exfiltrating sensitive intellectual property related to engineering documents or product designs that are common in industrial environments such as the automotive, aviation, and manufacturing sectors.

Technical Analysis – Comparing StealBit and ExMatter

Both custom exfiltration tools are designed to work on a 32-bit Windows system (Intel 386 or later). Each tool also includes obfuscation techniques that can mask certain data, or code. Important information such as network information of the command-and-control (C2) server address is encrypted in StealBit, while variants of ExMatter's code are protected and obfuscated using ConfuserEx (a free, open-source, .NET code protector), and Themida.

The following table is a comparison summary of the StealBit and ExMatter tools:

<<< Start >>>

	StealBit	ExMatter
File Type	Win32 EXE.	Win32 EXE (.NET).
Operating System	Windows Vista and later versions.	Windows XP and later versions.
Targeting Approach	Targets all files except specific blacklisted items. Avoids common system files and programs.	Targets specific sets of files based on defined criteria. Avoids common system files and programs.
Obfuscation	Data encrypted with Rivest Cipher 4 (RC4) and XOR.	Code is Protected by ConfuserEx, with some less-prevalent variants utilizing other options.
Usage Flexibility	Accepts specific command-line parameters.	Accepts specific command-line parameters.
Network	Uses HTTP PUT method for exfiltration. C2 infrastructure identified during analysis is hosted by nine (9) unique hosting services / ASNs.	Uses secure file transfer protocol (SFTP), SOCKS5, or WebDAV for exfiltration. C2 infrastructure identified during analysis is hosted across two (2) unique hosting services / ASNs, with over 85% hosted by one (1) provider / ASN.

<<< End >>>

<<< Start >>>

Full technical Analysis, countermeasures and TTPs

READ MORE

<<< End >>>

If you have an incident or need additional information on ways to prevent, detect, respond to, or recover from, cyberthreats, contact a member of our CIFR team 24/7/365 by phone 888-RISK-411 or email CIFR.hotline@accenture.com.

Accenture Security *is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.*

Cyber Investigations, Forensics and Response (CIFR)

The CIFR team helps Accenture’s global clients prepare for, respond to and recover from cyber intrusions and minimize business impact.

Accenture Cyber Threat Intelligence

Subscription Center

Subscribe to Security Blog Subscribe to Security Blog

Subscribe