Analyzing Exmatter: A Ransomware Data Exfiltration Tool

Published: 2022-03-22 · Archived: 2026-04-05 13:44:32 UTC

Having conducted more than 3,200 incident response engagements in 2021, Kroll's Threat Intelligence team now tracks more than 200 ransomware threat actor groups. Kroll's global Incident Response teams are very familiar with actions traditionally associated with a network intrusion, from initial access to lateral movement to privilege escalation to data exfiltration—and in the case of financially motivated actors, ransomware deployment. In this blog post, we will examine one of those tools, Exmatter.

In Q4 2021, Kroll analyzed multiple samples of a custom exfiltration tool called Exmatter. It's the third exfiltration toolset utilized by ransomware operators observed in the wild, after the release of Ryuk Infostealer in January 2020 and StealBit, which is associated with the LockBit 2.0 operator. Both the Ryuk Infostealer and Stealbit are capable of programmatic identification of files of interest, followed by automatic exfiltration of data. Ransomware groups in particular are known to harness custom data exfiltration tools to accelerate the information theft. Although Exmatter was originally associated with the now-defunct BlackMatter Ransomware-as-a-Service (RaaS) operation, Kroll has since observed variants of this tool being used by other RaaS groups.

The use of customized tools like Exmatter puts greater pressure on organizations to use effective endpoint detection and response capabilities along with cyber security best practices.

Accelerating the Exfiltration Process

Exmatter is designed to steal a range of user files, databases and compressed files (including email and zip archive files) from multiple directories and then upload them to a preconfigured server via Secure File Transfer Protocol (SFTP). This tool has been observed shortly before ransomware deployment on the victim's network. Interestingly, Kroll has identified attackers targeting specific file extensions indicative of web and application source code, shortcuts for Remote Desktop, and CAD/GIS files in their data theft efforts. This process of reducing data sources to the specific types of business-critical files is designed to speed up the exfiltration process by collecting the data that attackers believe will be of the greatest relevance and/or sensitivity during a ransom negotiation. Kroll assesses that it may increase pressure on an organization to make a ransom settlement when that organization is presented with a curated file tree of sensitive files. The expeditious nature of this custom file collection means the activity is more likely to complete successfully while also evading detection by traditional cyber security mechanisms.

Kroll's analysis identified that, upon enumerating the logical drives on a victim's computer, Exmatter iterates through all its folders but ignores certain directories, including directories inside "C:\ProgramData\" (see Table 1). Kroll assesses that these operating system directories generally contain files of low value when viewed from the perspective of compelling a ransomware payment. Upon identification of PDFs, Microsoft Office, OpenOffice and StarOffice files (including documents, spreadsheets and presentation files, along with other file extensions as described in Table 2), a queue is established to prioritize the most recently modified files ahead of older files. Kroll has also identified another limiting factor: after identifying file extensions of interest, Exmatter only exfiltrates files larger than 1,024 bytes.

Table 1: exclude files in any of the following directories

Excluded Filepaths	
C:\Documents and Settings	C:\ProgramData\WindowsHolographicDevices
C:\PerfLogs	C:\Recovery
C:\Program Files\Windows Defender Advanced Threat Protection	C:\System Volume Information
C:\Program Files\WindowsApps	C:\Users\All Users
C:\ProgramData\Application Data	C:\Users\Default
C:\ProgramData\Desktop	C:\Users\Public\Documents
C:\ProgramData\Documents	C:\Windows
C:\ProgramData\Microsoft	System Volume Information
C:\ProgramData\Packages	
C:\ProgramData\Start Menu	
C:\ProgramData\Templates	

Table 2: include files matching any of the following extensions

Included Extensions	
.doc, .docx (Microsoft Word)	.json
.xls, .xlsx, .xlsm (Microsoft Excel)	.msg
.ppt, .pptx (Microsoft PowerPoint)	.pdf
.3ds (Autodesk 3D Studio)	.pst (Microsoft Outlook Mailbox [personal storage table])
.accdb (Microsoft Access Database)	.rdp (Microsoft RDP Shortcut)
.aspx (Microsoft Active Server Page)	.sda (OpenOffice Draw)
.catdrawing, .catpart, .catproduct (CATIA CAD)	.sdm (StarOffice Mail & Various CAD/GIS tools)
.config	.sdw (OpenOffice Document)
.cs (C# Source Code)	.sqlite (SQLite Database)
.csv (Comma Separated Values)	.ts
.dwt (AutoCAD or Adobe Dreamweaver)	.zip
.dxf (AutoCAD)	

Anti-Forensic Cleanup & Capability Enhancements

As soon as all the selected data has been exfiltrated from the victim's endpoint, Exmatter leverages anti-forensic techniques, removing any traces of itself from the device by invoking PowerShell to overwrite the first 65,536 bytes of the malicious file and subsequently delete itself. Kroll's incident responders have observed multiple variants of the tool adding updates to the inclusion and exclusion list and implementing the use of a WebDav client as a secondary method of exfiltrating data should the primary use of SFTP fail. This suggests that attackers are continuing to evolve their tools to overcome defender obstacles while stealing valuable data in the shortest possible time.

More recently, Kroll's incident response investigators have observed a new variant of the Exmatter tool being used for exfiltration prior to Conti ransomware deployment. This variant includes a date range filter for the targeted data, indicating it may still be in development even after the alleged shutdown of the BlackMatter actor group in November 2021.

Exmatter Analysis in Action

In an analysis of Exmatter, Kroll's Malware Analysis and Reverse Engineering team confirmed the sample was a .NET Windows executable file that had been compiled with Themida, an anti-reverse engineering software protection utility. Through static and dynamic analysis, Kroll successfully extracted the unpacked executable embedded within the file.

Kroll found that any file matching the conditions in Tables 1 and 2 would be sent via SFTP to a remote server over TCP port 22 using a hardcoded username and password within the file. The team identified additional embedded configuration data, including a failover WebDav option should SFTP fail, as well as a SOCKS5 proxy configuration with the localhost IP address.

Kroll also identified that the malicious file would accept command-line arguments as well. If the string “nownd” or “-nownd” was passed to the file on execution, the file would attempt to hide its own window in order to avoid visual detection by any end user on the system.

Recommendations for Detecting Reconnaissance and Lateral Movement

During the early stages of a network intrusion, threat actors frequently utilize tools with legitimate purposes to surreptitiously engage in malicious activities. Tools such as ADFind and Advanced IP Scanner, for example, are widely used for network and Active Directory administration but can also be abused to aid in reconnaissance. When able to, attackers also use legitimately signed binaries, such as those belonging in the Windows Sysinternals suite, and leverage their capabilities to carry out malicious activities ranging from credential dumping (ProcDump) to widespread malware and ransomware deployment (PsExec).

Due to their legitimate purposes, these tools often do not raise suspicion when used in enterprise networks and thus provide threat actors with the ability to bypass traditional security apparatuses, including antivirus software. Kroll has also observed threat actors tampering with Group Policy Objects (GPO) to weaken the technical security posture of an organization. Once the initial stages of an attack are successfully carried out using such tools and attackers have identified that they’ve not yet been detected, threat actors may then introduce custom and unique tooling to focus on and accomplish their actions on an objective, such as data exfiltration. Kroll recommends the following strategies for detecting reconnaissance and lateral movement:

- Employ Next-Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR) on all devices within your environment to enable early detection and response to these threats. Based upon available organizational staffing, outsourcing the monitoring of your EDR solution may be a prudent approach to risk management given the 24x7 nature of the current cyber risk environment.
- Implement cyber security best practices, including MFA, patching and least privilege. A focus on reliable offline tested immutable backups is also important; you can find more here.
- Map your cyber security posture to a framework. The CIS Top 18 is a great solution for many organizations.

Gartner’s Market Guide for Digital Forensics and Incident Response Services highlights the growing need for malware analysis as part of effective incident response. If organizations are unable to undertake this type of analysis themselves, they can reach out to Kroll’s security and cyber risk experts at any time.
