Exmatter malware levels up: S-RM observes new variant with simultaneous remote code execution and data targeting

s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up

David Broome, Gavin Hull

4 June 2024

10 min read

S-RM's incident response team has observed a new variant of the data exfiltration tool, Exmatter, being used by a LockBit affiliate on a recent ransomware engagement.

In this special edition of the Cyber Intelligence Briefing, S-RM cyber experts, David Broome and Gavin Hull, explore the technical details underpinning this development, what it means for potential victims, and how organisations can identify and mitigate similar malware in their environments.

What is Exmatter?

Exmatter is a custom-built data exfiltration tool which aims to automate and increase the efficiency of data exfiltration from victims' systems by targeting specific directories and file types for collection and exfiltration. The tool's creation and use has been attributed to a ransomware affiliate tracked by Microsoft as Velvet Tempest (previously tracked as DEV-0504), which has deployed the following ransomware payloads between December 2021 and June 2022: Ryuk, Revil, LockBit 2.0, BlackMatter, Conti and BlackCat aka AlphV. S-RM has observed this affiliate deploying LockBit 3.0 payloads since August 2023..

A new variant?

In a recent engagement, S-RM identified a LockBit affiliate using a new variant of Exmatter malware to exfiltrate sensitive data from the client's network prior to the deployment of ransomware. The Exmatter binary was discovered using the file names 'SMSAgent.exe', '<company_name>.exe' and '<company_domain_name>.exe' (company name redacted), with the SHA1 hash 7c67976bfc3ef3c673d5cabc60b7f6fbe0ab19dc. Analysis of the Exmatter binary revealed that, beneath multiple layers of obfuscation, including the use of Spanish to write its functions, and encoding large sections of the malware in Base64, were features we have not previously observed.

The two most significant developments we detected in Exmatter's code were its ability to read mapped network drives from the registry of the host system, and its facilitation of inter-process communication ('IPC') between multiple binary processes across multiple systems through the use of an open-source module named TinyIPC.

```
internal class Aborda
{
    // Token: 0x060002A6 RID: 678 RVA: 0x00011CB4 File Offset: 0x0000FEB4
    private static List<string> Algalia(RegistryKey registryKey_0 = null)
    {
        try
        {
            if (registryKey_0 == null)
            {
                registryKey_0 = Registry.CurrentUser;
                registryKey_0 = registryKey_0.OpenSubKey("Network", true);
            }
        }
        catch (Exception exception_)
```

Figure 1 – Querying of the Network registry key HKEY_CURRENT_USER\Network*\RemotePath, which stores the UNC paths of mounted shares.

```
List<string> list = new List<string>();
try
{
    foreach (string name in registryKey_0.GetSubKeyNames())
    {
        RegistryKey registryKey = registryKey_0.OpenSubKey(name, true);
        object value = registryKey.GetValue("RemotePath");
        list.Add(value.ToString());
        list.AddRange(Aborda.Algalia(registryKey));
    }
}
catch (Exception exception_2)
{
    Amillarar.Adelante(exception_2);
}
return list;
```

Figure 2 – Storing the RemotePath registry values as a list of UNC paths of mounted shares.

```
if (Acaezcan.Activan && Acaezcan.Alamar > 0)
{
    this.amistan = new TinyMessageBus(Acaezcan.Alamar.ToString());
    this.Almená();
}
```

Figure 3 – Instantiation of the TinyMessageBus class for IPC communication.

The use of IPC allowed it to move laterally between network shares on the victim's network, simultaneously targeting data for exfiltration whilst remotely executing itself on other systems. If executed with administrator rights, it was also able to modify the permissions of files using the command 'takeown', which uses the SeTakeOwnershipPrivilege Microsoft API, giving the threat actor ownership permissions over files they were previously denied access to. This not only sped up the process of exfiltration, but also gave Exmatter more autonomy to target a larger number of systems and data with minimal input from the threat actor.

The binary also contained a Base64 encoded WebDAV client configured to a WebDAV server controlled by the threat actor, which was used for command and control. Exmatter then used the HTTP PUT method over port 80 to transfer data from the victim's network, ultimately resulting in the exfiltration of up to 1TB of data.

Towards automation and autonomy

Our analysis of Exmatter demonstrates that threat actors are becoming increasingly sophisticated in their ability to exfiltrate large amounts of data from victim networks whilst remaining undetected. The new functions highlight a growing trend towards automation and autonomy, with malware authors continuously finetuning their source code to reduce the time needed to achieve their objectives and minimise the need for human input.

Protection

In response to this increasing sophistication, organisations need to be proficient at detecting and preventing the use of data exfiltration tools in their environment. Sensitive data is a primary target for cyber criminals who seek to use it as leverage over their victims. Below, we have outlined five recommendations for identifying and mitigating these threats in your environment.

1. **Block inbound SMB connections to endpoints via Group Policy Object (GPO).** As Exmatter utilises IPC to perform lateral movement and remote execution, blocking inbound SMB connections on endpoints can limit its ability to function. On Windows devices, this can be achieved by disabling the following settings on endpoints using Microsoft Defender firewall: File and Printer Sharing (SMB-In), Netlogon Service (NP-In), Remote Event Log Management (NP-In), and Remote Service Management (NP-In).
2. **Disable Windows administrative shares.** Exmatter abuses Windows administrative shares to perform lateral movement, a type of share enabled by default in Windows environments to facilitate the remote management of hosts by administrators and software. Organisations should consider if administrative shares are needed in their environment, and if not, consider disabling them. These can be disabled via GPO or by changing the following registry subkeys to the value 0:
   Disabling administrative shares on servers:
   HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
   DWORD Name = AutoShareServer
   Value = 0
   Disabling administrative shares on endpoints:
   HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
   DWORD Name = AutoShareWks
   Value = 0
3. Use an intrusion detection system (IDS). Exmatter exfiltrates data via the HTTP PUT method, making it difficult for the victim to detect it leaving their network. This is a common issue for many organisations, with large amounts of HTTP traffic allowing threat actors to disguise their data exfiltration and remain undetected. Whilst identifying data exfiltration can be difficult, organisations can utilise intrusion detection systems (IDS) to monitor their network traffic and detect anomalous behaviour, alerting IT staff to any irregularities in the flow of data.
4. **Limit the use of web browser-based password managers.** Exmatter targets .sqlite files that are commonly used by web browsers to store sensitive information such as usernames and passwords. Theft of these files from your environment could lead to a much larger and more protracted compromise of your user accounts and data. Consider limiting the use of web browser-based password managers for your organisation’s users to prevent the theft of credentials.
5. **Conduct tactical threat hunting.** Understanding normal processes and behaviour in an environment is essential to identifying anomalies that are associated with malicious activity. Process, file integrity, and command monitoring can give defenders enhanced visibility into their network to detect deviations from baseline activities. These can then be combined with SIGMA rules to conduct threat hunting exercises to identify activity associated with lateral movement and data exfiltration.

Technical details

Overview

Indicator name	Description
Malware family	Exmatter
Action on objectives	Collect and exfiltrate sensitive data
Delivery mechanism	Deployed via GPO, remote execution over network shares
Attack chain stage	Exfiltration prior to ransomware deployment
Target operating system	Windows
Code language	.NET
Type of file	.exe
File name	SMSAgent.exe , <company_name.exe>, <company_domain_name.exe>
File path	C:\Windows\SMSAgent.exe
File size	396Kb
SHA1	7c67976bfc3ef3c673d5cabc60b7f6fbe0ab19dc
MD5	d8b56615a416e27272e3a8dc6a6467bf
SHA256	f13aae2f4995b0eb5ccf9f487003cd2c645d157f45ba6b79af6d39c18832bfc2
SSDEEP	12288:EDeBtyNAO1cgp9a7UT11H111TPro2KDzG/zUOrOeMrOFSW2PD2dUWF883n9aMpH7:ED0yNAO1cgp+UT11H111TPro2KDzG/zR

Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Signer	No signature found
Compile time	2024-01-18 01:37:26
VirusTotal	Not present

Directories ignored by Exmatter

1. \System Volume Information
2. C:\Users\All Users\Microsoft
3. C:\ProgramData
4. C:\Windows
5. C:\$Recycle.Bin
6. C:\Documents and Settings
7. C:\PerfLogs
8. AppData\Roaming\Microsoft
9. AppData\Local\Microsoft
10. AppData\Local\Packages
11. C:\Program Files
12. C:\Program Files (x86)
13. Application Data

File types targeted by Exmatter

1. .pdf
2. .doc
3. .docx
4. .docm
5. .xls
6. .xlsx
7. .xlsm
8. .ppt
9. .pptx
10. .pptm
11. .xps
12. .accdb
13. .png
14. .jpg
15. .jpeg
16. .bmp

17. .rdp
18. .sql
19. .sqlite
20. .db
21. .json
22. .msg
23. .pst
24. .zip
25. .rtf
26. .ipt
27. .dwg
28. .txt

Exmatter arguments

Argument	Function
ipc	Initiates a TinyIPC connection in slave mode, with the specified IPC node number. This number needs to be greater than 1 as its value. For example, -ipc 373737.
ipcpref	Sets the IPC number to start from. If not selected, a random number is chosen between 100,000 and 999,999.
path	Sets a specific path to target, such as the UNC path
norewrite	Disables ‘Breaker mode’
w	Default argument, runs expected behaviour of the malware

```
foreach (string a in amarillento)
{
    if (!(a == "-ipc"))
    {
        if (!(a == "-ipcpref"))
        {
            if (!(a == "-path"))
            {
                if (!(a == "-norewrite"))
                {
                    if (a == "-w")
                    {
                        flag = false;
                    }
                }
                else
                {
                    Acaezcan.Class0.bool_0 = false;
                }
            }
```

Figure 4 – Argument parser using cascaded conditional IF ELSE clause.

How can S-RM help?

If you are concerned about your organisation's ability to detect and prevent the use of data exfiltration tools like Exmatter in your environment, have recently detected suspicious activity within your network, or have additional questions about this piece, our team is available to help. Please contact us for more information.

Subscribe to our insights

Get industry news and expert insights straight to your inbox.