Lorenz Abuses Magnet RAM Capture

arcticwolf.com/resources/blog/lorenz-ransomware-getting-dumped/

by Steven Campbell, Ross Phillips, Seth Battles, and Markus Neis

February 23, 2023

Executive Summary

As organizations implement additional security controls and detections, threat actors adjust to bypass them. Since our initial investigation into a Lorenz ransomware intrusion that exploited a Mitel MiVoice VoIP appliance, we have observed a shift in the group's Tactics, Techniques, and Procedures (TTPs).

The Arctic Wolf Labs team recently investigated additional Lorenz ransomware intrusions, which also exploited a Mitel MiVoice VoIP appliance vulnerability (CVE-2022-29499) for initial access. In at least one case in late-2022, we observed the threat actors leveraging a compromised VPN account to regain access to the victim's environment and execute Magnet RAM Capture—a free tool that is typically used by law enforcement and forensic teams to capture the physical memory of a victim's device—on a Mitel Digital Voicemail system (running Microsoft Windows Server 2016). The threat actors leveraged Magnet RAM Capture to bypass the victim's EDR (Endpoint Detection and Response). Arctic Wolf Labs has informed Magnet Forensics about the known abuse of their tool by the Lorenz group.

We have published a compiled list of Indicators of Compromise (IOCs) and related artifacts we observed in this intrusion to our GitHub here. Also included in our GitHub are Sigma and YARA rules that our team developed to assist defenders in detecting unexpected use of Magnet RAM capture on their hosts.

Note: Arctic Wolf Labs has deployed detections in our platform to identify potential malicious activity associated with the Lorenz ransomware group, including the TTPs mentioned in this blog.

Key Findings

- The Lorenz ransomware group targeted the same victim and adapted their TTPs to successfully bypass security controls when the first attempt was not successful.
- This is the first Lorenz ransomware intrusion publicly documented where the threat actors leveraged Magnet RAM Capture to dump memory.

Substantive Analysis

In at least one intrusion, the Lorenz ransomware group was not able to start the encryption process due to their registry modification attempts and PowerShell commands being blocked by the EDR. The techniques and procedures in this intrusion were almost identical to the Lorenz ransomware case we investigated in September 2022.

We observed the use of the Chisel tunneling tool, dumping of LSASS, and encryption attempts via BitLocker Drive Encryption. Notably, data exfiltration did not occur until the threat actors noticed their PowerShell commands were being prevented by security controls. Approximately two hours after unsuccessful data encryption, we observed the threat actors download and execute FileZilla on multiple systems to exfiltrate as much data as possible. Like other Lorenz intrusions, the threat actors exfiltrated the data to Digital Ocean IP addresses.

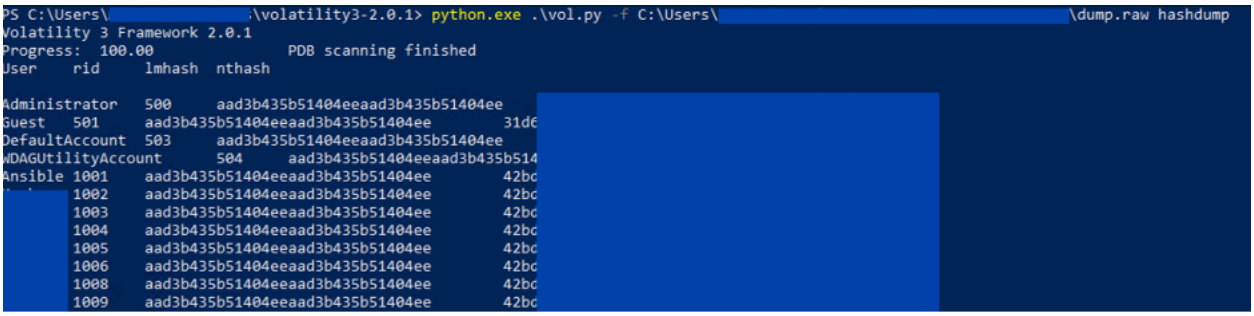
However, data exfiltration and extortion were not enough for Lorenz, and approximately a month later, the threat actors leveraged compromised VPN credentials to regain access. The compromised VPN credentials were tied to a vendor account used to service the Mitel infrastructure, which were obtained via activity from the previous incident when the credentials had been reset but set to "User must change password at next logon," which prompted the threat actors to change the password when logging in via the vendor account.

Ultimately this access allowed Lorenz to pivot into the Mitel environment and set up Chisel as a SOCKS proxy as well as obtaining additional credentials and creating accounts for persistence.

Operating within kernel mode gives an adversary access to the most privileged areas of an operating system. To obtain kernel-level privileges threat actors often leverage a technique known as “Bring Your Own Vulnerable Driver” (BYOVD). BYOVD allows a threat actor full kernel memory read and write operations and gives them the ability to evade endpoint security solutions by removing telemetry sources. Multiple threat actors have leveraged BYOVD to bypass and disable endpoint security solutions, including Lazarus, AvosLocker, and BlackByte.

Well-known vulnerable driver exploits are easily detected by most EDRs, forcing advanced threat actors to research kernel driver vulnerabilities and develop exploits, which can be a time-consuming and tedious task.

Lorenz, however, did not use a vulnerability to gain kernel access; instead, they leveraged Magnet RAM Capture, a user-mode application which comes equipped with a signed kernel driver, like many other RAM acquisition tools, to directly access the physical memory. The use of Magnet RAM Capture allowed the threat actor to bypass the EDR on the victim host and enabled them to obtain a memory dump of the host. Although a RAM capture is not completely structured, threat actors can extract sensitive information like credentials via readily available memory forensics tools.



Example of obtaining credentials from RAM Capture

Conclusion

The Lorenz ransomware group consistently shows inventive ways to achieve their objectives. This added technique demonstrates how the Lorenz threat actors are willing to adjust their TTPs to evade security controls. In this case, they relied on a known RAM Capture tool to bypass an EDR solution.

Many security vendors provide free tools to help security professionals perform better research and security investigations. Even with access controls, threat actors will continue to find ways to obtain and abuse legitimate tools to bypass security controls.

Recommendations

Ensure Secure Password Reset After a Compromise

When leveraging the “User must change password at next logon” ensure all accounts that received the prompt have successfully changed their password and logged in; this includes user, service, and vendor accounts.

If not, threat actors could leverage previously compromised credentials to reset the password and obtain access again, negating the password reset. Administrators should also understand all accounts tied to the service so that all resets can be tracked and recorded.

For user or vendor accounts that are tied to individuals outside of your organization, consider not using the “User must change password at next logon” feature. Instead, reset the password directly with a new value and send the password to the account holder out of band. Ensure the user resets the password upon logging in to the account.

Implement Multi-factor Authentication

Implement multi-factor authentication (MFA) wherever possible within your environment, especially VPN accounts. Multi-factor authentication reduces the impact leaked or compromised credentials have on an organization.

Conduct Network and Host Baselines to aid in Monitoring of Malicious Traffic and Binaries

Understanding your environment can help you identify malicious traffic and binaries in a more efficient manner. For example, if your organization does not use Magnet RAM Capture for legitimate business purposes or there is no purpose for it to be present on a target system, the use of the binary could potentially be a good indicator that malicious activity is present in your environment. Understanding your environment’s baseline and approved software will ensure malicious activity is caught earlier in the kill chain.

Audit or Block Unwanted Drivers using Windows Defender Application Control (WDAC)

Organizations can consider auditing or blocking unwanted drivers via Windows Defender Application Control (WDAC). Microsoft has detailed many methods of restricting unwanted drivers in their “Microsoft recommended driver block rules” article.

Detection Opportunities

Multiple detection opportunities exist and below we provide a subset based on the Magnet RAM Capture sample observed during the Lorenz intrusion:

SHA256 72dc1ba6ddc9d572d70a194ebdf6027039734ecee23a02751b0b3b3c4ea430de

The Arctic Wolf Labs team has developed Sigma and YARA rules that can assist defenders in detecting unexpected use of Magnet RAM capture on their hosts.

Note: Arctic Wolf Labs has deployed detections in our platform to identify potential malicious activity associated with the Lorenz ransomware group, including the TTPs mentioned in this blog.

Hunting for Execution

Magnet RAM Capture requires admin privileges and can either be executed via GUI or the command line.

Both types of execution can be identified by leveraging PE header metadata for process execution events, as these details have been defined by Magnet Forensics and have been consistent over various identified versions of the tool.

Example Process Create Event

```
Process Create:
Description: Magnet RAM Capture
Product: Magnet RAM Capture
Company: Magnet Forensics Inc.
OriginalFileName: MRC.exe
```

If execution is done via the command line, defenders can monitor for Magnet RAM Capture parameter invocations.

Parameter	Description
/accepteula*	Accepts the EULA (no user interaction required)
/go*	<optional output path, including output file name> – No user input required; start RAM capture immediately, saving to a .raw file in the current folder unless a path is provided (if the path contains spaces, use quotes around the entire path).
/split	500MB|1GB|2GB|4GB – Split the RAM capture into segments of 500MB, 1GB, 2GB, or 4GB (e.g. /split 2GB) – requires /go parameter.
/silent*	Captures RAM in the background; no interface or progress displayed – requires /go parameter.
/?	This help screen

***Source**: Magnet RAM Capture*

*Required parameters to successfully invoke Magnet RAM capture via command line.

Example Process Create Event

```
Process Create:
CommandLine: "C:\<SNIP>\<magnet_path>\magnet.exe" /silent /go debug.raw /accepteula
```

Driver Load

The Magnet RAM capture main executable contains multiple signed drivers for various CPU architectures within its PE resources. A driver for the correct architecture is dropped into the same directory from where the tool was executed with a .tmp extension.

Example Driver Load Event

```
Driver loaded:
ImageLoaded: C:\<SNIP>\<magnet_path>\magA46.tmp
Hashes:
MD5=35AEF87E63302FB7273870CFF3117279
SHA256=5FFF657939E757922941162376ADB86B7A37DC329A1F9969C70F23E7D54B7B4C
IMPHASH=99ABE3BC6F5A07246949FFC36BC1F543
Signed: true
Signature: Magnet Forensics Inc.
SignatureStatus: Valid
```

We have extracted the drivers and recommend detecting on driver load events that contain any of the values seen below:

SHA256	MD5	SHA1
5FFF657939E757922941162376ADB86B7A37DC329A1F9969C70F23E7D54B7B4C	35AEF87E63302FB7273870CFF3117279	68DB
C0CAFFD00B9576725ACF9DBE15AF8FC64EA000CB527F1FBCAA3CBDCF52C99152	F6D77EF0B07B6FFF1B91357C890DCF88	5D798
3766619B7564F84185CF8CC952EE5513C45C6D858EF971C5FD1B0BDF234B8BAA	FFDC58CD04A6E6295725F1C9B9C0D0CE	CB330
654629028CF878126A25B8449B5F1AC4D828B5ADC03BB393062D46415A78F39B	1DD0E3E168B5B4704583B59E0F5A63A2	B7C36

Service Creation

Magnet Ram Capture creates a kernel driver service with a service name consisting of the FileDescription name of the driver that is used with an ImagePath pointing to a .tmp file which is the signed driver that gets written into the same directory from where the tool was executed.

```
Windows Event ID 7045
ServiceName: MagnetRAMCapture Driver
ImagePath: C:\<SNIP>\<magnet_path>\mag7E01.tmp
ServiceType: kernel mode driver
StartType: demand start
```

Indicators of Compromise (IOCs)

Indicator	Type	Context
138.68.62[.]46	IP Address	Data exfiltration via FileZilla
192.241.152[.]84	IP Address	Chisel Tunnel
138.68.50[.]118	IP Address	Chisel Tunnel
206.189.198[.]191	IP Address	Data Exfiltration via FileZilla
23.28.148[.]190	IP Address	Used to connect to the victim's SSL VPN
45.61.136[.]141	IP Address	Used to connect to the victim's SSL VPN
97FF99FD824A02106D20D167E2A2B647244712A558639524E7DB1E6A2064A68D	SHA256	Chisel Tunnel**
72DC1BA6DDC9D572D70A194EBDF6027039734ECEE23A02751B0B3B3C4EA430DE	SHA256	Magnet RAM Capture*
5FFF657939E757922941162376ADB86B7A37DC329A1F9969C70F23E7D54B7B4C	SHA256	Signed Driver used by Magnet RAM Capture
C:\Users\MRCv120.exe	Filepath	Magnet RAM Capture*
MagnetRAMCapture.sys	Filename	PE Original Name of Signed Driver used by Magnet RAM Capture
debug.raw	Filename	Observed name for RAM capture output
\tmp\.tmp\mem	Filepath	Chisel Tunnel

** Magnet RAM Capture can be used for legitimate purposes. We recommend leveraging the hash values to hunt for potential malicious activity, but also leverage environment context to make a determination on the legitimacy of the tools in your environment.*

*** Chisel can be used for legitimate purposes. However, in most instances that Arctic Wolf Labs has observed the tool has been used for malicious activity. We recommend leveraging the hash values to hunt for potential malicious activity, but also leverage environment context to make a determination on the legitimacy of the tools in your environment.*

MITRE ATT&CK Matrix

Tactic	ID	Name	Details
Initial Access	T1190	Exploit Public-Facing Application	Lorenz exploited CVE-2022-29499 on an exposed Mitel device, achieving Remote Code Execution (RCE).
Persistence	T1078	Valid Accounts	The threat actors leveraged compromised VPN credentials to regain access. The threat actors created an additional account on the Mitel Digital Voicemail system.
Command & Control	T1095	Non-Application Layer Protocol	Lorenz set up a SOCKS proxy via Chisel on the Mitel device.
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	The threat actors dumped LSASS memory. The threat actors used Magnet RAM capture to acquire a physical memory dump.
T1003.002 T1003.004	OS Credential Dumping: Security Account Manager OS Credential Dumping: LSA Secrets	The threat actors used Magnet RAM Capture to acquire a physical memory dump.	
Execution	T1059.001	Command and Scripting Interpreter: Powershell	Lorenz executed multiple Powershell commands that were prevented by the EDR.
Data Exfiltration	T1048.002	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	The threat actors exfiltrated data via FileZilla.
Defense Evasion	T1553.002	Subvert Trust Controls: Code Signing	Magnet RAM Capture comes with a signed driver that allowed the threat actor to bypass the EDR.

Note: To download a full listing of IOCs, artifacts, and detections for mentioned in this blog, refer to our GitHub here.

For additional recommendations and insights regarding Lorenz ransomware, check out our first blog, Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free, published on September 12, 2022.

References

By Steven Campbell, Ross Phillips, Seth Battles, Markus Neis

Steven Campbell | Senior Threat Intelligence Researcher

Steven Campbell is a Senior Threat Intelligence Researcher at Arctic Wolf Labs and has more than eight years of experience in intelligence analysis and security research. He has a strong background in infrastructure analysis and adversary tradecraft.

Ross Phillips | Senior Threat Intelligence Researcher

Ross is a Sr. Threat Intelligence Researcher at Arctic Wolf Labs with almost a decade of experience in the security landscape. Prior to this, Ross worked as a Technical Lead for the Arctic Wolf SOC and an Internal Tech Resident at Google after graduating from Rochester Institute of Technology in 2012 majoring in Information Security & Forensics.

Seth Battles | Senior Forensics Analyst

Seth Battles is a Senior Forensics Analyst with Arctic Wolf Incident Response. He has years of experience in various facets of security operations, with a focus on incident response. His technical proficiencies include Digital Forensics, Exploit analysis, and Offensive Security.

Markus Neis | Principal Threat Intelligence Researcher

Markus Neis is a Principal Threat Intelligence Researcher in Arctic Wolf Labs focused on leading advanced threat research. He has more than a decade of experience in researching adversary tradecraft and responding to sophisticated attacks.