blackpoint

THREAT PROFILE:

Sarcoma Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2024

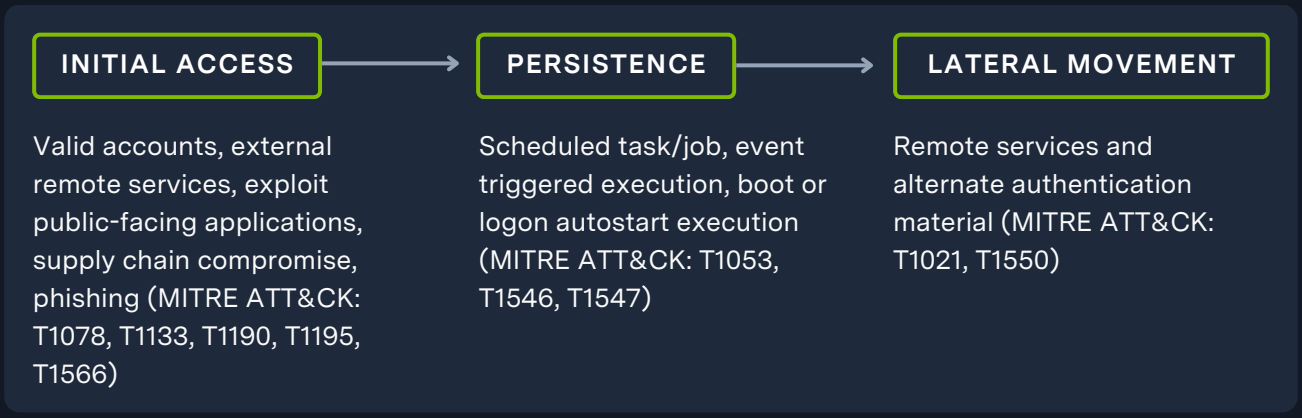
Operation style:
Ransomware-as-a-Service (RaaS)

Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Egregor Ransomware
- Maze Ransomware



Description

Sarcoma is a ransomware operation that was first identified in October 2024. The group operates in the double extortion method, where the group exfiltrates data and threatens to leak that data if the ransom is not paid as well as encrypting the network.

Sarcoma operates as a ransomware-as-a-service (RaaS) and purportedly offers a 70/30 split on payments for affiliates.

Sarcoma operates both a Windows and Linux variant. The Windows variant is written in C++. Sarcoma is reported to utilize a hybrid encryption model, combining ChaCha20 stream cipher with RSA-4096 asymmetric encryption. Other reports indicate the group has used AES-256 with RSA-2048. Both methods utilize CryptoPP library functions with multithreaded architecture for faster encryption.

Sarcoma specifically avoids targeting systems configured with the Uzbek keyboard layout, indicating that the core operators may be located in this region. This is a common tactic observed in ransomware operations to avoid legal repercussions in their local areas.

Sarcoma ransomware disables critical business systems by stopping services and processes related to Microsoft SQL Server and PostgreSQL using PowerShell and WMIC. Additionally, the variant deletes local backups using VssAdmin and wbadmin. The Linux variant uses VMware's vim-cmd utility to enumerate and delete VM snapshots.

Sarcoma moves laterally through compromised networks by using a combination of passive network scanning, ICMP pings, and more. It uses CopyFileA and SMB shares to copy the ransomware payload across the network.

Sarcoma is reported to offer affiliates a 70/30 split of ransom demand payments.

Once the ransomware encrypts the network, it drops ransom notes in each folder and subfolder that were encrypted. The ransom note is extracted from an embedded PDF.

Sarcoma has been reported to focus on larger organizations, specifically those with annual revenues between $1 million and $50 million. The group likely focuses on this revenue because these organizations are more likely to be considered profitable enough to pay a ransom demand but small enough to lack robust security measures.

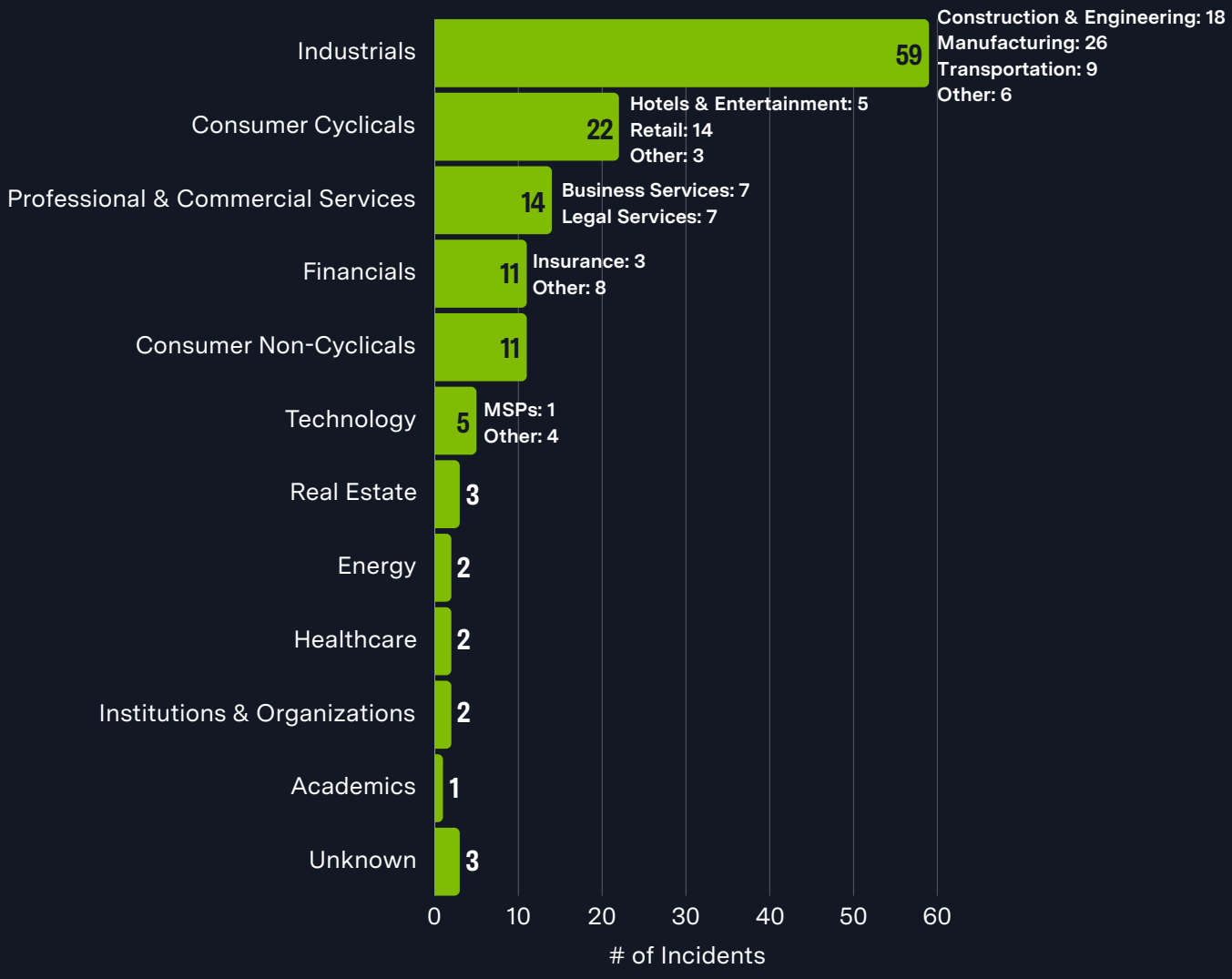
While Sarcoma was first discovered in 2024, the tactics of the group indicate that the operators are technically sophisticated and have likely operated within other operations or under a different brand prior to the creation of the Sarcoma variant.

Security researchers have theorized that Sarcoma operators may be linked to the former Maze and Egregor Ransomware operators. This assessment is based on architectural choices including multithreaded encryption, strategic directory avoidance, and the group's data leak site mirroring those of Maze and Egregor.

Sarcoma has proven to be a capable and persistent ransomware operation and will likely continue to target organizations over the next 6-12 months for financial gain.

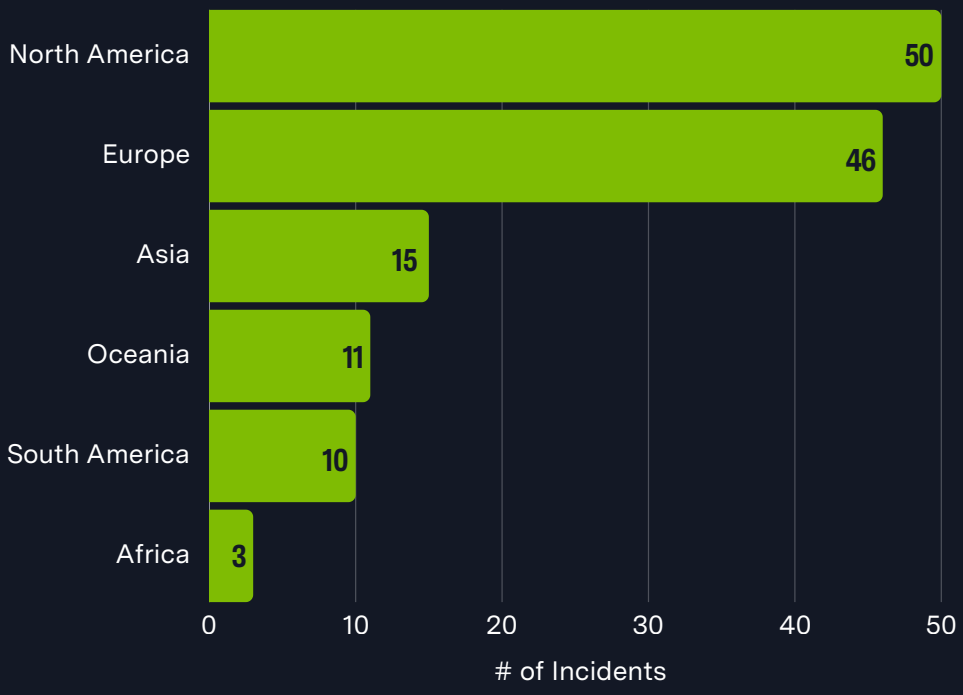
Previous Targets

Previous Industry Targets from 01 Oct 2024 to 30 Sep 2025



Previous Targets

Previous Victim HQ Regions from 01 Oct 2024 to 30 Sep 2025



Data Leak Site

hxxp://sarcomawmawlhov7o5mdhz4eszxxlkyaoiyiy2b5iwxnds2dmb4jakad[.]onion/

Associations

Egregor Ransomware

Security researchers have reported that Sarcoma's operation bears resemblance to the now-defunct Egregor Ransomware operation. This assessment was based on architectural choices including multithreaded encryption, strategic directory avoidance, and a TOR-based leak site that resembles the leak site of Egregor.

Maze Ransomware

Security researchers have reported that Sarcoma's operation is similar to the now-defunct Maze Ransomware's operation; the assessment is based on the same factors as those listed above for Egregor Ransomware.

Known Tools

7-Zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
Amazon S3 Bucket	A service that offers object storage through a web service interface, is often used to host tools and malware.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
curl	An open-source command-line tool for transferring data using various network protocols.
Google Drive	A file storage and synchronization service that threat actors have used to host malware or export stolen files to.
MEGA	A cloud storage and file hosting service.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PsExec	A command-line utility that allows users to execute processes on remote systems; it is part of the Sysinternals suite and is frequently used by system admins for remote management tasks. The tool is also repeatedly abused by threat actors for lateral movement and remote execute.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.

Known Tools

RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
schtasks	A utility used to schedule execution of programs or scripts on a Windows system to run at a specific date and time.
Service Control Manager	A system process under the Windows NT family of operating systems that can start, stop, and interact with Windows service processes.
temp.sh	A temporary file upload service that is frequently abused for data exfiltration.
VMware CLI Tools	A collection of utilities that allow users to manage and configure virtual machines (VMs) and VMware vSphere environments using command-line commands, rather than a graphical user interface (GUI).
wbadmin	A command line utility that is used to back up and restore OS, drive volumes, files, folders, and applications from a command line interface.
WinExec	A built-in scripting function that executes a Windows command as if it was entered at the command prompt.
WinSCP	A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
WSAStartup	A Windows function that allows an application or DLL to specify the version of Windows Sockets required and retrieve details of the specific Windows Sockets implementation.

Observed Behaviors: Windows

Tactic	Commands Observed
Execution	WinExec
Persistence	schtasks
Defense Evasion	"powershell -w h -c Start-Sleep -Seconds 5; Remove-Item -Force -Path \""
Discovery	GetKeyboardLayout GetIpNetTable mw_send_ping
Lateral Movement	mw_net_use_copy LogonUserA
Command and Control	CopyFileA
Impact	vssadmin.exe delete shadows /all Get-Service Set-Service Stop-Service Stop-Process _write CryptoPP::RSAFunction FAIL_STATE_NOTIFICATION.pdf - ransom note

Observed Behaviors: Linux

Tactic	Commands Observed
Defense Evasion	IFS=$'\n' for i in $(vim-cmd vmsvc/getallvms); do ii=$(echo $i \| cut -d " " -f1) in=$(echo $ii \| grep -E '^[0-9]+$') vim-cmd vmsvc/snapshot.removeall $in 2>&1
Discovery	vim-cmd vmsvc/getallvms
Impact	vim-cmd vmsvc/snapshot.removeall LibTomCrypt

MITRE ATT&CK® Mappings

Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Compromise	
T1566: Phishing	
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	
T1129: Shared Modules	
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1546: Event Triggered Execution	.011: Application Shimming
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys/Startup Folder
Privilege Escalation	
T1055: Process Injection	

MITRE ATT&CK® Mappings

Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
Defense Evasion	
T1027: Obfuscated Files or Information	
T1036: Masquerading	
T1055: Process Injection	
T1070: Indicator Removal	
T1112: Modify Registry	
T1562: Impair Defenses	.001: Disable or Modify Tools
T1574: Hijack Execution Flow	.001: DLL
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1110: Brute Force	
Discovery	
T1018: Remote System Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	

MITRE ATT&CK® Mappings

Discovery	
T1087: Account Discovery	
T1614: System Location Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1550: Use Alternate Authentication Material	
Collection	
T1005: Data from Local System	
T1113: Screen Capture	
T1560: Archive Collected Data	
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1090: Proxy	
T1105: Ingress Tool Transfer	
Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	

MITRE ATT&CK® Mappings

Exfiltration	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Encrypted for Impact	
T1490: Inhibit System Recovery	
T1657: Financial Theft	

References

- Halcyon (2025, October 15) “Sarcoma.” https://www.halcyon.ai/threat-group/sarcoma
- Halcyon RISE Team (2025, March 14) “Halcyon Threat Insights 014: March 2025 Ransomware Report.” https://www.halcyon.ai/blog/halcyon-threat-insights-014-march-2025-ransomware-report
- Lobo, Mario (2025, August 19) Lumu: “Advisory Alert: Sarcoma Ransomware Double Extortion Threat.” https://lumu.io/blog/sarcoma-ransomware-double-extortion-threat/#elementor-toc__heading-anchor-5
- Martire, Luigi; Paganini, Pierluigi (2025, May 20) Unipegaso University: “Sarcoma Ransomware Unveiled: Anatomy of a Double Extortion Gang.” https://www.tinextacyber.com/wp-content/uploads/2025/05/Sarcoma-Ransomware.pdf

Adversary Pursuit Group

blackpoint