blackpoint

THREAT PROFILE:

Sinobi Ransomware

TABLE OF CONTENTS

Executive Summary	2
Diamond Model	3
Description	4
Previous Targets: Industries & Regions	6
Data Leak Site	8
Vulnerabilities	9
Associations	10
Known Tools	11
Observed Behaviors: Windows	12
Kill Chain	14
MITRE ATT&CK® Mappings	15
References	18

Executive Summary

First Identified:
June 2025

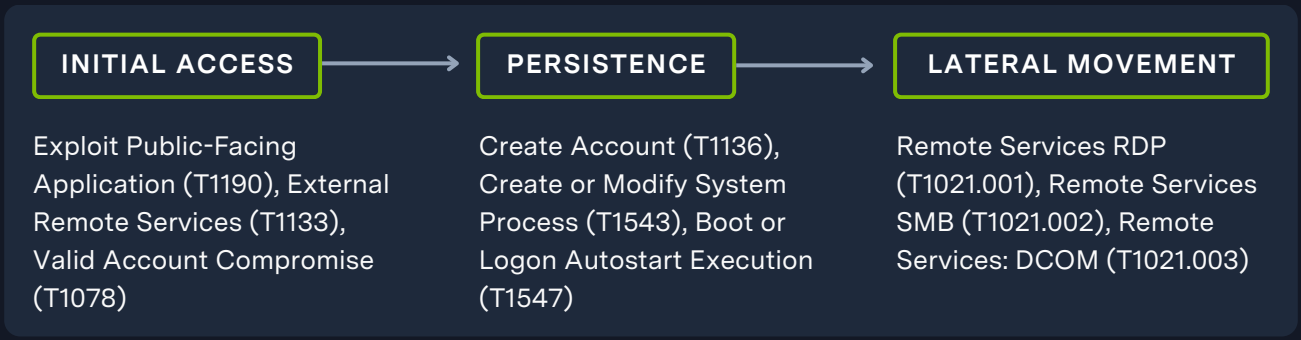
Operation style:
Semi Private Ransomware-as-a-Service (RaaS) - the group maintains affiliates that are strictly vetted and have a positive reputation with the core operators.

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:
- INC Ransom Ransomware
- Lynx Ransomware



Diamond Model

Description

The Sinobi ransomware group first emerged in late June 2025, with significantly increased activity in July 2025, which has continued steady throughout the rest of 2025. The group employs dual extortion in their attacks, thereby doubling the pressure to pay on victim organizations.

Due to similarities in the code, TTPs, and data leak sites (DLS), it is widely believed that Sinobi is an offshoot or rebrand of the Lynx and INC ransomware groups. There is an even chance that Sinobi operators purchased INC Ransom code that was listed for sale in May 2024 for $300,000 USD. All three groups remain active into 2026; it is not known if the operations are being operated in tandem or are separate operations built on shared source code.

The group operates under a semi-private Ransomware-As-A-Service (RaaS) model and employs dual extortion to ensure payout. The group appears to only work with known, vetted affiliates, who conduct the attacks themselves in exchange for shared profits. Since they don't work with individuals they don't already know, information about them and their operations is limited. This has the added benefit of increasing their operational security, suggesting well-connected and experienced operators.

Several reports suggest significant overlaps between Sinobi ransomware and Lynx/INC ransomware variants. In addition, the TOR-based data leak sites for these groups are all very similar in appearance, emphasizing similarities between the groups. Clear web mirrors exist as well.

According to public reporting, the group gains access into victim environments through compromise or exploitation of edge software/devices.

The group employs dual extortion in their attacks, thereby doubling the pressure to pay on victim organizations.

In specific cases, ESentire reported the group gaining access through a public facing SSL VPN via valid account compromise (the account was an MSP account that mapped to a Domain Admin account in the environment).

While in this instance, the group used valid credentials to gain access to the environment via compromised credentials, the group has also been known to exploit vulnerable SonicWall VPNs. Surefire has reported specific vulnerabilities related to SonicWall compromises - CVE-2024-53704. This vulnerability allows attackers to bypass authentication mechanisms and hijack active VPN sessions.

Like many other groups, Sinobi primarily uses RDP and share mounts as their lateral movement mechanisms. This is performed under the user contexts of either compromised users or users created by the group. They utilize valid compromised accounts and newly created accounts to move throughout a victim environment and ultimately to rapidly deploy ransomware.

The group has also been observed enumerating USB devices, potentially suggesting some ability to propagate through infected USB devices.

Description

The group has been observed deploying RMMs (AnyDesk) to ensure persistent access to a host. Additionally, the group has been observed altering user permissions to have higher access as well as creating new domain administrators. This doubles as privilege escalation.

Sinobi has been observed attempting to uninstall security software and deleting shadows on targets, an attempt to impede recovery operations.

The group employs the dual extortion method to increase the pressure on victims to pay. This means that they steal data as well as encrypt environments. The group has been observed using RClone and WinSCP to exfiltrate data to cloud storage.

Once data is exfiltrated, Sinobi ransomware is deployed, resulting in encryption of the environment. Binary analysis suggests heavy overlap between Sinobi ransomware samples and INC/Lynx ransomware samples.

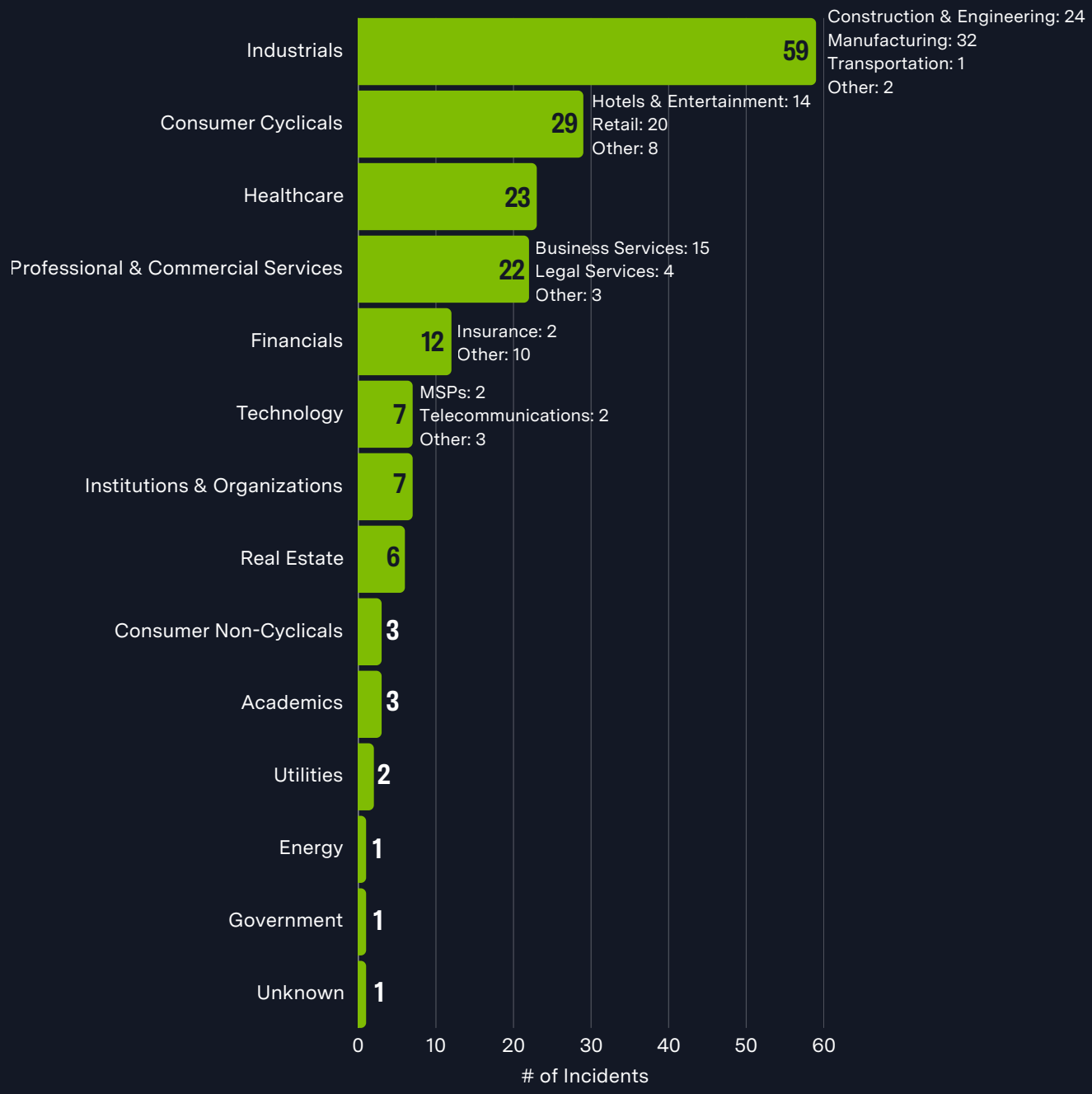
Sinobi has been observed attempting to uninstall security software and deleting shadows on targets, an attempt to impede recovery operations.

According to Halcyon, the group primarily targets organizations making $10-$50 million a year, helping guarantee a decent payout for their effort. In 2025, their top vertical was Manufacturing, with Construction & Engineering, Healthcare, and Professional & Commercial Services close behind.

Sinobi claimed 176 attacks from their first known attack on June 7th, 2025 to the end of 2025. Victims have resided in 19 different countries with the vast bulk of organizations residing in the United States.

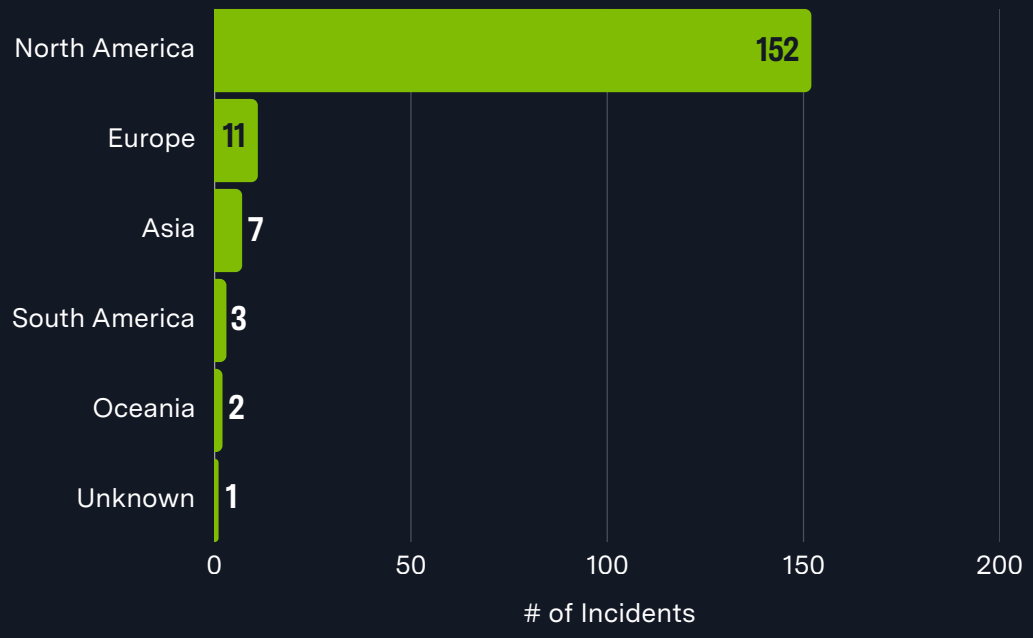
Previous Targets

Previous Industry Targets from 01 June 2025 to 31 Dec 2025



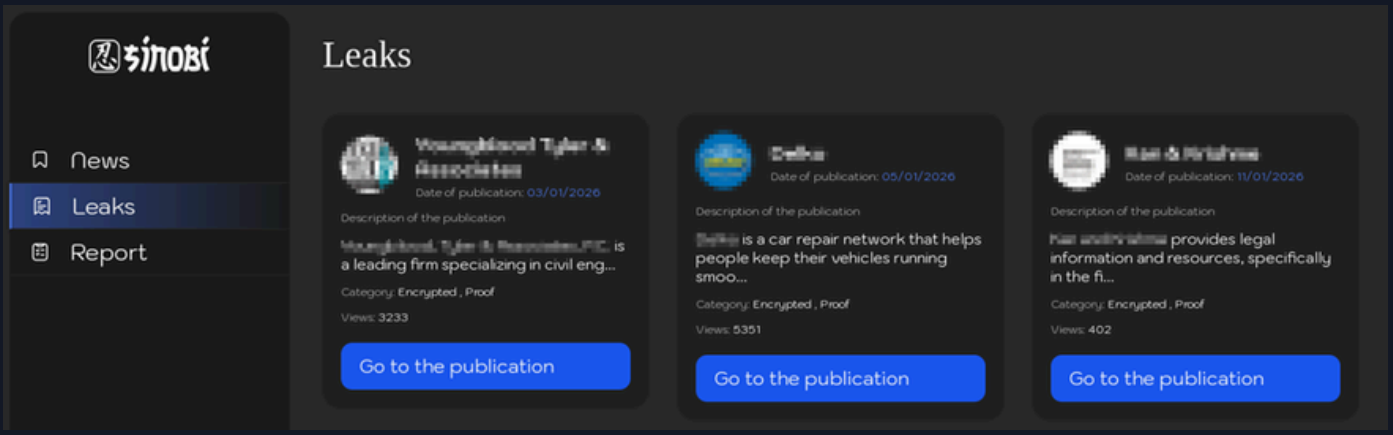
Previous Targets

Previous Victim HQ Regions from 01 Apr 2023 to 31 Mar 2024



The United States is the most frequently impacted country based on victims listed on Sinobi Ransomware's data leak site.

Data Leak Site



hxxp[:]//sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd[.]onion/leaks
hxxp[:]//sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd[.]onion/leaks
hxxp[:]//sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid[.]onion/leaks
hxxp[:]//sinobi7l3wet3uqn4cagjiessuomv75aw3bvgah4jpj43od7xndb7kad[.]onion/leaks
hxxp[:]//sinobi7sukclb3ygtorysbtrodgdbnrmgbhov45rwzipubbzhiu5jvqd[.]onion/leaks
hxxp[:]//sinobi23i75c3znmqqxxyuzqvhxnjsar7actgvc4nqeuhgcn5yvz3zqd[.]onion/leaks
hxxp[:]//sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd[.]onion/leaks

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2024-53704	Improper Authentication Vulnerability	SonicWall SonicOS SSL VPN	9.8

Associations

INC Ransom Ransomware

Due to similarities in the code base of the variants as well as similarities in the data leak sites, there is suspected overlap between Sinobi and the INC ransom variants. There is an even chance that Sinobi operators purchased INC Ransom's source code that was listed on dark web forums for sale in May 2024 for $300,000 USD.

Lynx Ransomware

Sinobi Ransomware maintains similarities to the Lynx operation in both their behaviors and their data leak site appearance. This is likely due to both groups' overlap with the INC Ransom operation. There is an even chance that both operations purchased INC Ransom's source code listed for sale in 2024.

Known Tools

Function	Tool	Description
Execution	cmd	Utility used to execute commands on Windows systems.
	WMI	Microsoft's framework for managing data and operations used to execute commands and queries remotely.
Persistence	AnyDesk	Remote access tool abused for persistent access.
Privilege Escalation	net	Windows utility abused to add new administrator accounts to elevate privileges.
Defense Evasion	Revo Uninstaller	Tool that removes programs and residual artifacts.
	Service Control Manager	Windows utility used to start/stop services.
Credential Access	ProcDump	Dumps LSASS memory for credential extraction.
	Windows Credential Manager	Windows utility that stores credentials; frequently abused to steal valid credentials.
Lateral Movement	RDP	Microsoft protocol used to remotely connect to a Windows computer.
Command and Control	nginx	Hosts attacker-controlled infrastructure for anonymized C2 over TOR.
Exfiltration	Rclone	Command line program used to manage, sync, and transfer files.
	WinSCP	Transfers files over SFTP/FTP.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	Executes Windows commands via cmd /c to perform system and domain actions
		Executes rclone.exe to copy data to attacker-controlled remote storage
		Calls CryptStringToBinaryA to decode attacker Curve25519 public key
		Generates AES-128-CTR key and counter via Curve25519-derived function
		Generates cryptographic material using CryptGenRandom
Persistence	Command Execution	Creates a local user account using net user Assistance /add
		Adds user to local Administrators group for persistent privileged access
		Adds user to Domain Admins group for persistent domain-wide access
Privilege Escalation	Command Execution	Elevates privileges by adding user to local Administrators group
		Elevates privileges by adding user to Domain Admins group
	Configuration Change	Enables SeTakeOwnershipPrivilege to override file ownership restrictions
Defense Evasion	Command Execution	Forces immediate system reboot to apply defensive changes
		Terminates processes holding file handles using Restart Manager APIs
	Configuration Change	Disables Carbon Black Defense service (cbdefense)
		Modifies cbdefense service binary path

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Defense Evasion	Configuration Change	Modifies file DACLs to grant Everyone full access
		Takes ownership of protected files to bypass access controls
Exfiltration	Command Execution	Exfiltrates data using Rclone with attacker-supplied configuration
Impact	Command Execution	Deletes Volume Shadow Copies by resizing diff area to zero via DeviceIoControl
		Encrypts files using AES-128-CTR encryption
	Configuration Change	Changes desktop wallpaper via registry modification
	Output / Artifact	Drops ransom note titled README.txt

Kill Chain

Initial Access

- Valid account compromise
- SSL VPN exploitation

Persistence

- Rogue RMM deployment

Defense Evasion

- Imparing/disabling defenses

Lateral Movement

- RDP and SMB

Exfiltration

- Data theft via RClone and WinSCP

Impact

- Ransomware execution in environment.

MITRE ATT&CK® Mappings

Reconnaissance	
T1595: Active Scanning	.002: Vulnerability Scanning
Resource Development	
T1650: Acquire Access	
Initial Access	
T1190: Exploit Public-Facing Application	
T1133: External Remote Services	
T1078: Valid Account Compromise	
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
Persistence	
T1136: Create Account	.001: Local Account .002: Domain Account
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	
Privilege Escalation	
T1098: Account Manipulation	.007: Additional Local or Domain Groups
Defense Evasion	
T1006: Direct Volume Access	

MITRE ATT&CK® Mappings

Defense Evasion	
T1027: Obfuscated Files or Information	.002: Software Packing
T1036: Masquerading	.005: Match Legitimate Resource Name or Location
T1055: Process Injection	.001: Dynamic-Link Library Injection
T1562: Impair Defenses	.001: Disable or Modify Tools
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1552: Unsecured Credentials	.001: Credentials in Files
T1555: Credentials from Password Stores	.004: Windows Credential Manager
Discovery	
T1016: System Network Configuration Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account .002: Domain Account
T1120: Peripheral Device Discovery	
T1482: Domain Trust Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .003: Distributed Component Object Model

MITRE ATT&CK® Mappings

Collection	
T1005: Data from Local System	
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1071: Application Layer Protocol	
T1090: Proxy	
Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1485: Data Destruction	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1491: Defacement	.001: Internal Defacement
T1657: Financial Theft	

References

- Barry, Christine (2025, November 18) Barracuda: “Sinobi: The bougie-exclusive ransomware group that wants to be a ninja.” https://blog.barracuda.com/2025/11/17/sinobi--the-bougie-exclusive-ransomware-group-that-wants-to-be-a
- eSentire Threat Response Unit (2025, August, 27) “Threat Actors Deploy Sinobi Ransomware via Compromised SonicWall SSL VPN Credentials.” https://www.esentire.com/blog/threat-actors-deploy-sinobi-ransomware-via-compromised-sonicwall-ssl-vpn-credentials
- Halcyon (n.d.) “Threat Actor: Sinobi.” https://www.halcyon.ai/threat-group/sinobi
- NIST National Vulnerability Databas (2025, October 31) “CVE-2024-53704.” https://nvd.nist.gov/vuln/detail/CVE-2024-53704
- Ransomware Live (n.d.) “Sinobi.” https://www.ransomware.live/group/sinobi
- Surefire Cyber (2025, September 3) “Threat Actor Profile: Sinobi.” https://www.surefirecyber.com/threat-actor-profile-sinobi

Adversary Pursuit Group

blackpoint