blackpoint

THREAT PROFILE:

Lynx Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2024

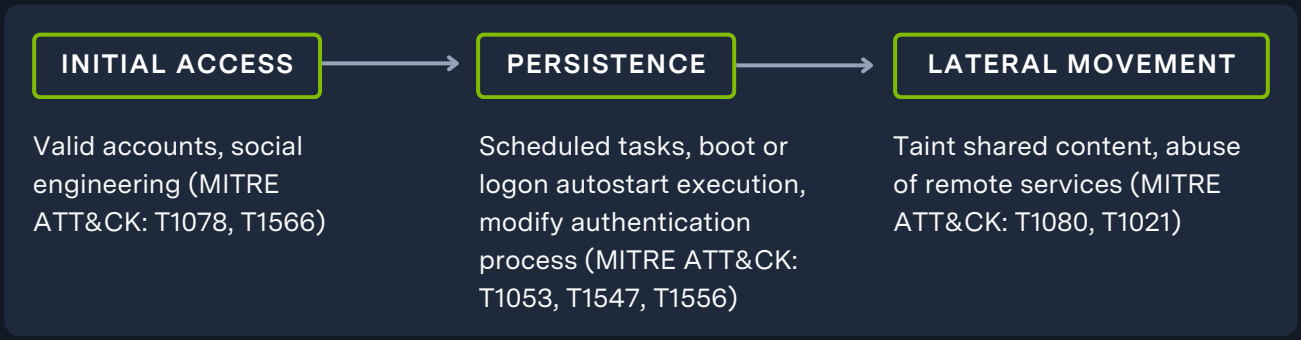
Operation style:
Ransomware-as-a-Service (RaaS) - the group offers an 80/20 split of ransom payments, as well as a call center service for an extra percentage of the ransom payment.

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
- LockBit Ransomware
- Silencer
- Storm-2113
- Water Lalawag



Description

Lynx Ransomware was first identified in July 2024 when the group began posting purported victims on their data leak site, Lynx News. Similar to other ransomware operations, the group claimed via their data leak site that they are financially motivated and have a strict policy on targeting. The group claims that they avoid “socially important” organizations, such as government agencies, hospitals, and non-profit organizations.

The operation operates as a ransomware-as-a-service (RaaS) and a user, silencer, has been observed posting on the cybercriminal forum, RAMP, advertising the operation.

Rather than targeting a single architecture, the Lynx Ransomware variant offers affiliates a complete bundle. The bundle offers executables for Linux x64, Linux ARM, MIPS, ESXi, and more. This allows affiliates to pick whichever variant they need for specific parts of the victim’s network.

Security researchers with Group-IB reported to have gained access to the Lynx affiliate group and gained access to the group’s affiliate panel. The affiliate panel reported featured multiple sections, including “News”, “Chats”, “Companies”, “Stuffers”, and “Leaks”.

- News - serves as a central hub for updates and announcements.
- Chats - provides information about the chats created for negotiations.
- Companies - provides an interface for affiliates to manage victims.
- Stuffers - offers affiliates a streamlined interface to manage any sub-affiliates and team members.
- Leaks - allows affiliates to create and manage publications about companies they have targeted but who haven’t paid.

Lynx Ransomware is similar to the INC Ransom operation; however, it is unverified whether the Lynx group purchased the INC source code or if Lynx is the INC successor.

Lynx Ransomware has been reported to be similar to the INC Ransom Ransomware. Security researchers with SK Shieldus reported that Lynx uses the same strings and encryption algorithms as the INC Ransom group and is similar in functional aspects, such as program execution flow. Additionally, BlackBerry researchers reported that Lynx and INC Ransom have used the same email address, gansbronz[at]gmail[.]com, in the registry information of the public data leak sites.

In May 2024, INC Ransom operators listed their source code for sale on a dark web forum for $300,000. There is an Even Chance that Lynx operators purchased the source code and created their own variant. Both Lynx and INC Ransom use DeviceIoControl functions to control devices and delete backup copies.

Various security researchers have reported that the Windows variants have a 40% code similarity and a 70.8% similarity in specific functions, while the Linux variants have a 91% code similarity and a 87% overall overlap.

Description

Lynx ransomware has been assessed to gain initial access to victim environments via phishing emails with malicious attachments and valid credentials to administrator accounts, which are common tactics observed in ransomware attacks.

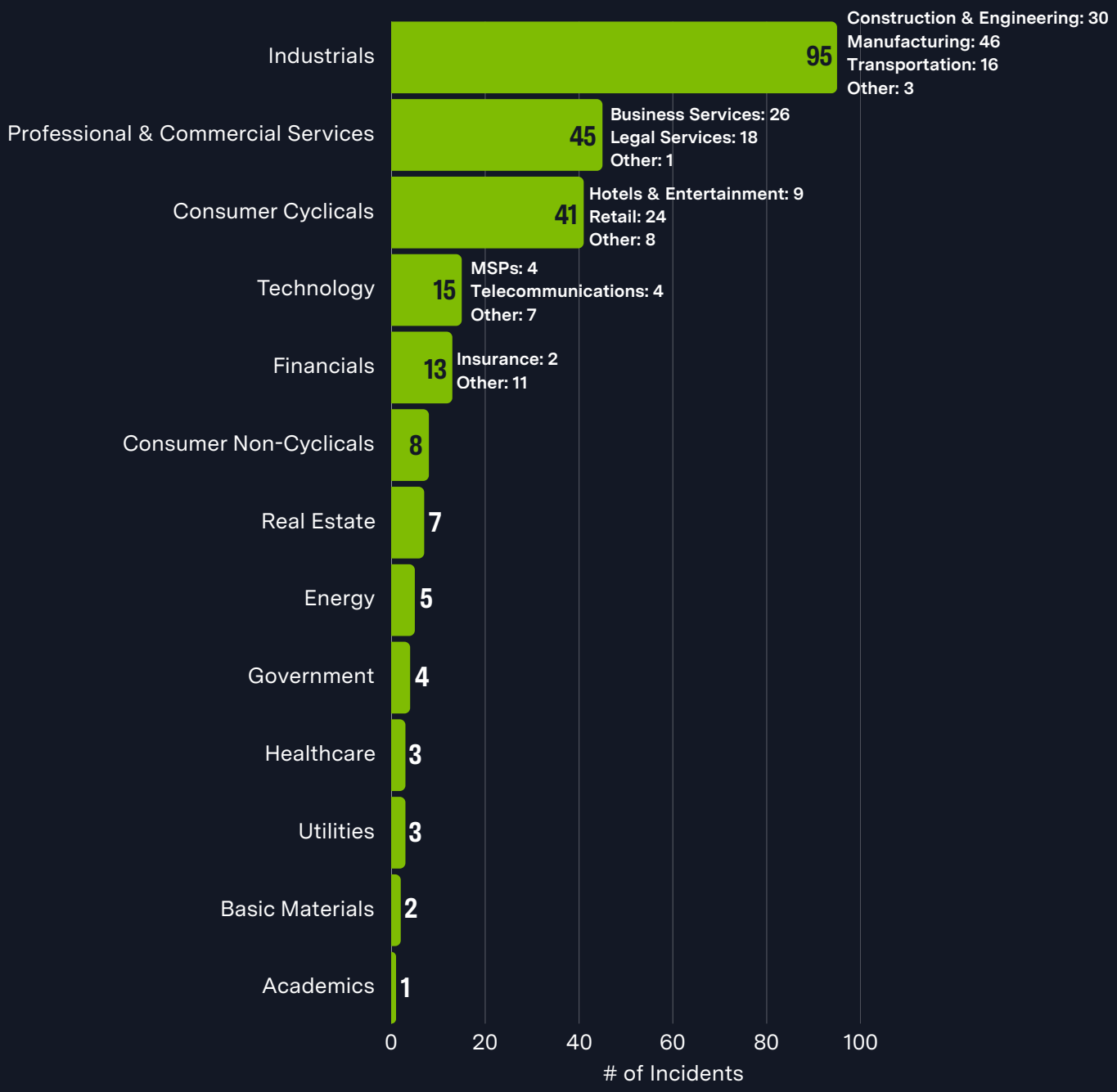
Lynx utilizes scheduled tasks and registry keys for persistence on compromised environments. Similar to other ransomware operations, Lynx deletes backup shadow copies and terminates anti-virus tools.

The Lynx Ransomware has been reported to utilize RDP and SMB file share enumeration for lateral movement. Additionally, the group has been reported to use shared content to spread laterally to other devices within a network.

Lynx Ransomware utilizes Curve25519 Donna for key exchange and AES-128 for file encryption. Both of these encryption techniques are known for their strength and reliability. The ransomware then changes the desktop wallpaper and prints the ransom note on any identified connected printer.

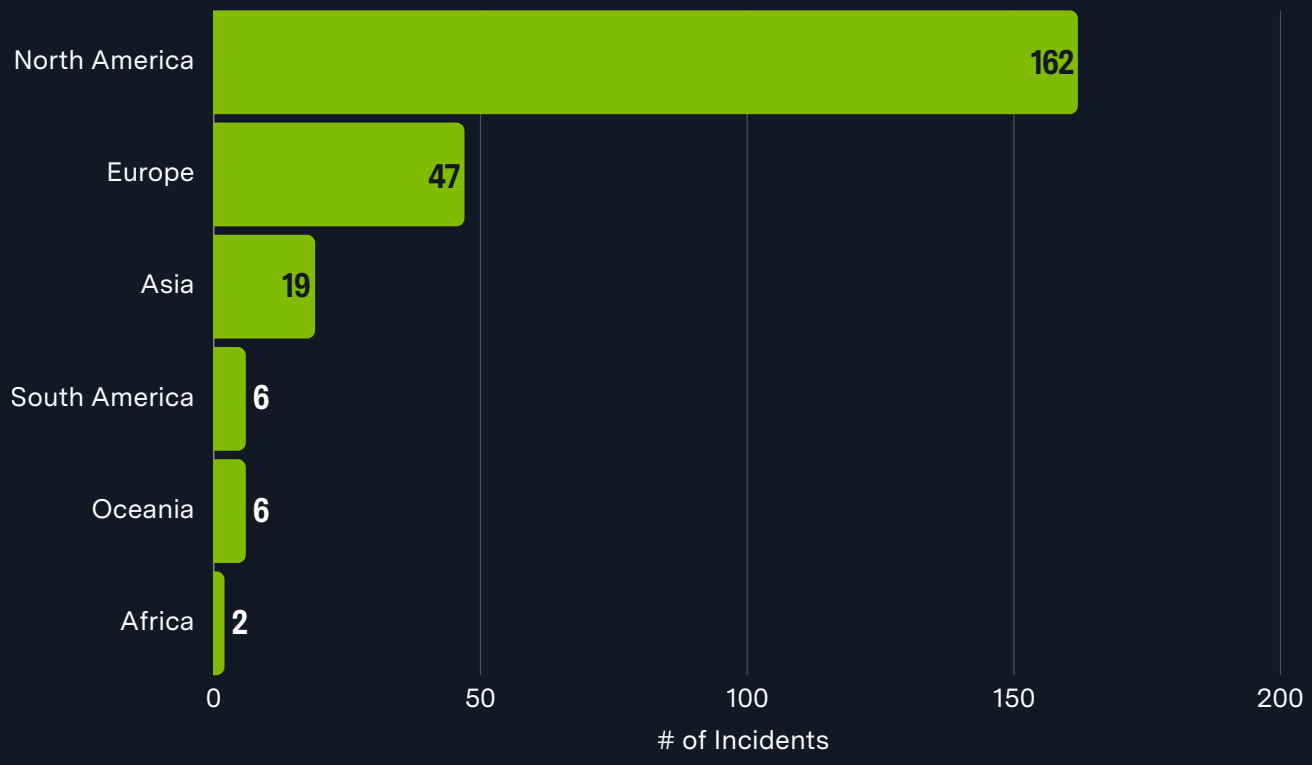
Previous Targets

Previous Industry Targets from 01 Jul 2024 to 30 Jun 2025

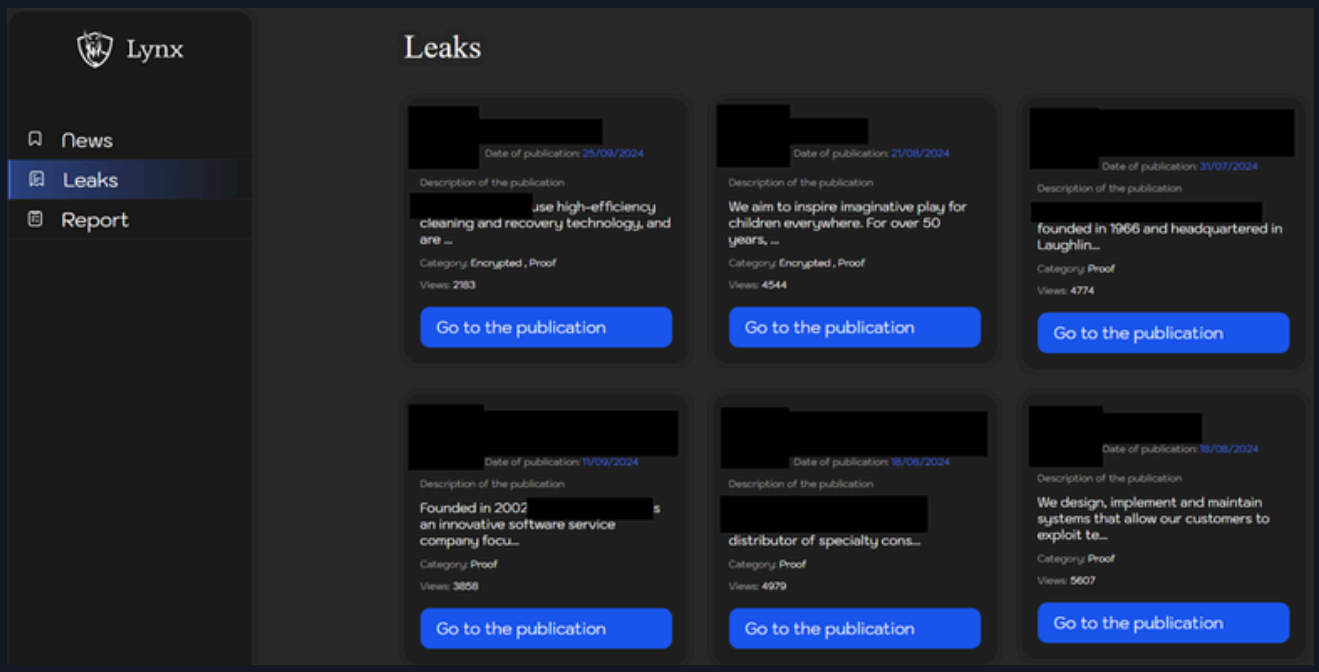


Previous Targets

Previous Victim HQ Regions from 01 Jul 2024 to 30 Jun 2025



Data Leak Site



hxxp://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion/
hxxp://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd[.]onion/
hxxp://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd[.]onion/
hxxp://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad[.]onion/
hxxp://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad[.]onion/
hxxp://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad[.]onion/
hxxp://lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid[.]onion/
hxxp://lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion/disclosures
hxxp://lynxblog[.]net/leaks

Associations

INC Ransom Ransomware

In May 2024, INC Ransom operators posted on a cybercriminal forum that they were selling their encryptor for $300,000. Lynx has been reported to be functionally nearly identical to INC Ransom, indicating that the Lynx operators likely purchased their source code from INC Ransom operators.

LockBit Ransomware

Security researchers have reported that Lynx Ransomware shares similarities with the LockBit Ransomware variant. Multiple security researchers have reported that Lynx operators likely purchased the INC Ransom source code and made modifications, which were likely influenced by the LockBit operation.

Silencer

A user on the cybercriminal forum, RAMP, that has been reported to offer the Lynx affiliate program as a target. The user has been observed targeting experienced penetration testing teams for recruitment and posting details of the group's capabilities, tools, and expectations.

Storm-2113

Lynx Ransomware operator group tracked by Microsoft.

Water Lalawag

Lynx Ransomware operator group tracked by Trend Micro.

Known Tools

Amazon S3 Buckets	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.
AutoDesk Cloud Services	A cloud service that allows users to upload analytics or data to a remote server. This tool is likely used for data exfiltration.
cmd	A program used to execute commands on a Windows computer.
conhost.exe	A Windows utility that is used to provide the ability to drag and drop files/folders directly into Command Prompt.
ConnectWise	Formerly ScreenConnect. A self-hosted remote desktop software application that can be used to remotely access victim environments.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
Microsoft OneNote	A digital note-taking app that provides a place for users to keep their notes, research, plans, and information. Threat actors have been observed using OneNote attachments in phishing emails to deploy malware.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
netscan	A utility that scans within a subnet or IP range to check for devices.
nmap	An open-source utility for network discovery; it runs on all major computer operating systems and includes multiple tools that can be used to transfer data, compare scan results, and generate packets.
NotePad	A simple text editor for Windows; it creates and edits plain text documents.
Ping	A tool used to test whether a particular host is reachable across an IP network.

Known Tools

PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
SC Manager	A system process under the Windows NT family of operating systems that can start, stop, and interact with Windows service processes.
Windows Registry Editor	Regedit. A graphical tool in the Microsoft Windows OS that enables authorized users to view the Windows registry and make changes.
Windows Restart Manager	A library for reducing required reboots during software updates. The tool is often used by threat actors to support the encryption process and retrieve processes running on the system.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Behaviors: Windows

Tactic	Commands Observed
Execution	explorer.exe /NoUACCheck msedge.exe --type=renderer --string-annotations=is-enterprise-managed=yes --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=959 --time-ticks-at-unix-epoch=-1728452222843688 --launch-time-ticks=62467984654 --field-trial-handle=19680,i,15019798532265350999,15797442694679624294,262144 --variations-seed-version --mojo-platf DeviceIoControl() RstrtMgr â€“ Restart Manager API HANDLE process_handle = OpenProcess(PROCESS_TERMINATE, FALSE, pe.th32ProcessID) printf(L"[+] Process %s with PID: %d was killed successfully\n", pe.szExeFile, pe.th32ProcessID); mmc.exe C:\Windows\system32\dnsmgmt.msc CreateFileW AllocateAndInitializeSid GetQueuedCompletionStatus EXCEL.EXE "\\$domain\nas\IT\Beebe\Egnyte Migration\Beebe_WinMerge.xlsx" GetHashCode.exe "NetWrix Account Lockout Examiner Freeware License1000000ALEe" GetHashCode.exe "NetWrix Account Lockout Examiner Freeware License1000000ALE" GetHashCode.exe "NetWrix Account Lockout Examiner Freeware License1000000ALEeâ€œ EXCEL.EXE \\$domain\nas\IT\Beebe\Egnyte Migration\Beebe_WinMerge.xlsx Veeam.EndPoint.Tray.exe -NoControlPanel -CheckNumberOfRunningAgents ControlService OpenSCManagerW OpenServiceW
Persistence	DesktopConnector.Applications.Tray.exe StartType:Auto
Privilege Escalation	OpenProcess
Defense Evasion	SetEndOfFile SeTakeOwnershipPrivilege SetNamedSecurityInfoW

Observed Behaviors: Windows

Tactic	Commands Observed
Defense Evasion	SetEntriesInAclW LookupPrivilegeValueW AdjustTokenPrivileges DeviceIoControl
Discovery	PING.EXE in2924-dpt5820 CreateToolhelp32Snapshot Process32FirstW QueryServiceStatusEx EnumDependentServicesW Process32NextW DADispatcherService.exe -f "C:\Users\$username\AppData\Roaming\Autodesk\CDX\Version15.8.0\All64\15.8.0.1827\MC3\Json" -a "https://ase.autodesk.com/adp/v1/analytics/upload" -tfct 1337297656952880052069 6 GetDriveTypeW WNetOpenEnumW WNetEnumResourceW enum_dir FindFirstVolumeW FindNextVolumeW EnumPrintersW
Collection	Notepad.exe "\\$domain\nas\IT\Beebe\beebedesign website, DNS, email, etc\DNS Records from AWS - COVI.txt"
Command and Control	StartDocPrinterW StartPagePrinter
Impact	TerminateProcess stop_services TerminateProcess(process_handle, 0); RmRegisterResources enc_del_shadow_copies RmGetList RmStartSession

Observed Behaviors: Linux

Tactic	Commands Observed
Impact	for i in $(esxcli vm process list \| grep 'World' \| grep -Eo '[0-9]{1,8}'); do esxcli vm process kill -t=force -w=$i; done" for i in $(vim-cmd vmsvc/getallvms | awk '{print $1}' | grep -Eo '[0-9]{1,8}'); do vim-cmd vmsvc/snapshot.removeall $i; done

Execution Options

Command	Description
--file	Encrypts only the selected file.
--dir [directory path]	Encrypts only the selected director.
--help	Display descriptions on execution arguments.
--verbose	Display debugging logs.
--stop-processes	Terminate the process if the target file is running immediately before encrypting it.
--encrypt-network	Encrypt the network shared resources.
--load-drives	Mount hidden drives.
--hide-cmd	Hide the command prompt window that appears when the ransomware runs.
--no-background	Disable the wallpaper change function.
--kill	Terminate specific processes and services.
--safe-mode	Boot in safe mode. (There is a code to check if this argument has been entered, but no code to actually boot in safe mode or automatically restart the ransomware after reboot).

MITRE ATT&CK® Mappings

Resource Development	
T1587: Develop Capabilities	.001: Malware
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .004: Unix Shell
T1106: Native API	
T1203: Exploitation for Client Execution	
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
T1556: Modify Authentication Process	

MITRE ATT&CK® Mappings

Privilege Escalation	
T1055: Process Injection	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1134: Access Token Manipulation	
Defense Evasion	
T1027: Obfuscated Files or Information	
T1036: Masquerading	.003: Rename Legitimate Utilities .005: Match Legitimate Name or Location
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1140: Deobfuscate/Decode Files or Information	
T1222: File and Directory Permissions Modification	
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
T1562: Impair Defenses	.001: Disable or Modify Tools .009: Safe Mode Boot
T1564: Hide Artifacts	.001: Hidden Files and Directories
Discovery	
T1012: Query Registry	

MITRE ATT&CK® Mappings

Discovery	
T1018: Remote System Discovery	
T1049: System Network Connections Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account .002: Domain Account
T1135: Network Share Discovery	
T1614: System Location Discovery	
T1652: Device Driver Discovery	
Lateral Movement	
T1080: Taint Shared Content	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
Collection	
T1005: Data from Local System	
T1113: Screen Capture	

MITRE ATT&CK® Mappings

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
T1573: Encrypted Channel	.001: Symmetric Cryptography .002: Asymmetric Cryptography
Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1491: Defacement	.001: Internal Defacement
T1657: Financial Theft	

References

- Acronis Threat Research Unit (2025, August 04) “MSPs a top target for Akira and Lynx Ransomware.” https://www.acronis.com/en-us/tru/posts/msps-a-top-target-for-akira-and-lynx-ransomware/
- Albuquerque, Pietro (2025, January 28) Group-IB: “Cat’s out of the bag: Lynx Ransomware-as-a-Service.” https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/
- Broadcom (2025, February 14) “Lynx Ransomware, established in 2024.” https://www.broadcom.com/support/security-center/protection-bulletin/lynx-ransomware-established-in-2024
- Chhaparwal, Pranay Kumar; Yates, Micah; Chang, Benjamin (2024, October 10) Palo Alto: “Lynx Ransomware: A Rebranding of INC Ransomware.” https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/
- Cyble (2025, March 06) “Threat Actor Profile: Lynx Ransomware.” https://cyble.com/threat-actor-profiles/lynx-ransomware/
- DarkTrace (2025, February 27) “New Threat on the Prowl: Investigating Lynx Ransomware.” https://www.darktrace.com/blog/new-threat-on-the-prowl-investigating-lynx-ransomware
- Imano, Shunichi; Gutierrez, Fred (2025, February 14) Fortinet: “Ransomware Roundup – Lynx.” https://www.fortinet.com/blog/threat-research/ransomware-roundup-lynx
- MOXFIVE (2025, March 04) “MOXFIVE Threat Actor Spotlight - Lynx.” https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-lynx
- Nexton Threat Research Team (2024, October 11) “In-Depth Analysis of Lynx Ransomware.” https://www.nextron-systems.com/2024/10/11/in-depth-analysis-of-lynx-ransomware/
- Özeren, Sila (2025, February 06) Picus Security: “Lynx Ransomware: Exposing How INC Ransomware Rebrands Itself.” https://www.picussecurity.com/resource/blog/lynx-ransomware
- Rapid7 Labs (2024, September 12) “Ransomware Groups Demystified: Lynx Ransomware.” https://www.rapid7.com/blog/post/2024/09/12/ransomware-groups-demystified-lynx-ransomware/
- SK Shieldus (2024) “Keeping Up with Ransomware.” https://www.skshieldus.com/download/files/download.do?o_fname=Keep%20up%20with%20Ransomware_Emergence%20of%20Lynx%20ransomware%20and%20analysis%20of%20connectivity%20with%20INC%20Group.pdf&r_fname=20240927174026206.pdf
- SOCRadar (2025, August 29) “Dark Web Profile: Lynx Ransomware.” https://socradar.io/dark-web-profile-lynx-ransomware/
- The BlackBerry Research and Intelligence Team (2024, October 14) “Lynx on the Prowl: Targeting SMBs with Double-Extortion Tactics.” https://blogs.blackberry.com/en/2024/10/lynx-ransomware
- Traynor, Orlaith (2025, March 28) CybelAngel: “Lynx Ransomware: Double Extortion, Ethics & Affiliate Payouts.” https://cybelangel.com/lynx-ransomware-double-extortion/
- WatchGuard (2024) “Lynx (Active).” https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/lynx
- Wes (2024, July 29) Medium: “Threat Report: Lynx Ransomware.” https://medium.com/@phishfinding/threat-report-lynx-ransomware-cb2881e9b7b2

Adversary Pursuit Group

blackpoint