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

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, external remote services, exploit public-facing application, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

Scheduled tasks, create account, create or modify system process, boot or logon autostart execution, modify authentication process (MITRE ATT&CK: T1053, T1136, T1543, T1547, T1556)

Taint shared content, abuse of remote services, exploitation of remote services (MITRE ATT&CK: T1080, T1021, T1210)

Diamond Model

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. The group has been reported to operate in a tight, closed model RaaS operation where affiliates are strictly vetted.

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.

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.

- 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 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.

Description

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.

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.

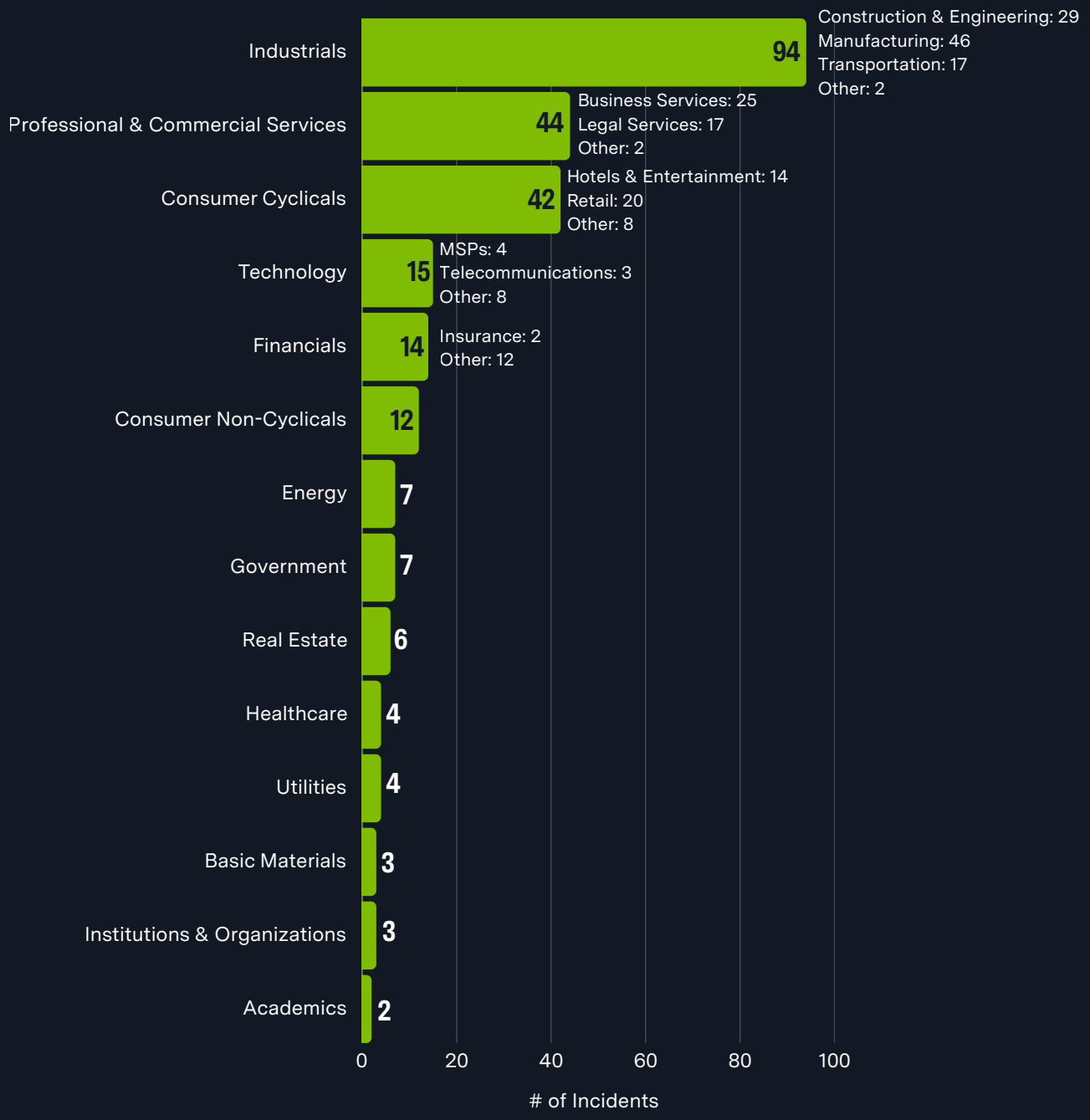
Lynx claims to avoid hospitals, governments, and non-profit organizations in attacks.

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.

Lynx Ransomware is likely to continue targeting victims in critical infrastructures worldwide over the next 6-12 months.

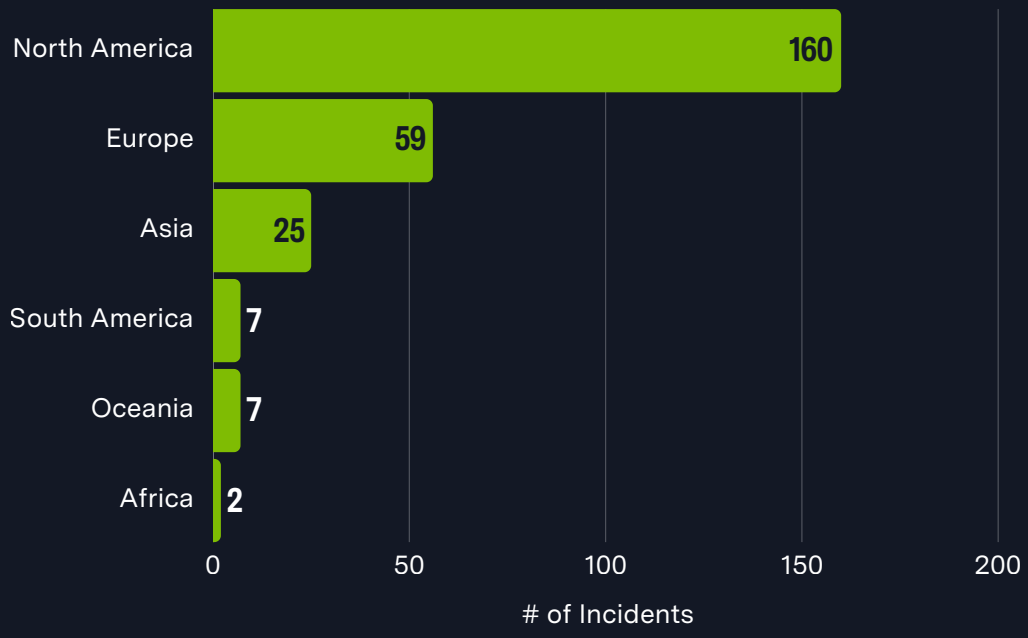
Previous Targets

Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

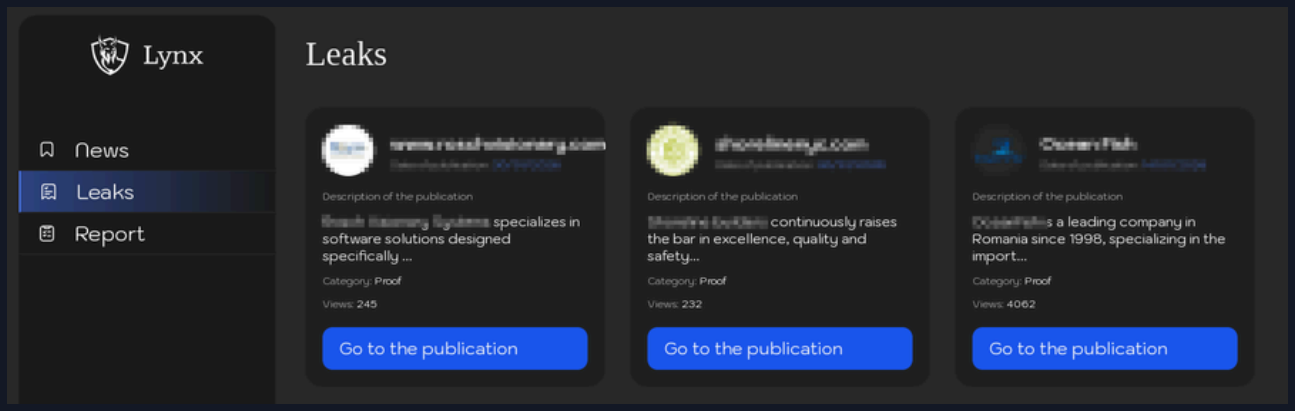


Previous Targets

Previous Victim HQ Regions from 01 Jan 2025 to 31 Dec 2025



Data Leak Site



hxxp://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion/
hxxp://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd[.]onion/
hxxp://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd[.]onion/
hxxp://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad[.]onion/
hxxp://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad[.]onion/
hxxp://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad[.]onion/
hxxp://lynxblogxutufossaeawlij3j3uikalolI5ko6grzhkwdclrjngrfoid[.]onion/
hxxp://lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion/disclosures
hxxp://lynxblog[.]net/leaks

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2019-6693	Hardcoded Cryptographic Key Vulnerability	Fortinet FortiOS	7.5
CVE-2024-0769	Path Traversal Vulnerability	D-Link DIR-859 Router	9.8
CVE-2024-54085	Authentication Bypass Vulnerability	AMI MegaRAC SPx	10

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

Function	Tool	Description
Initial Access	Microsoft OneNote	Part of the Microsoft suite frequently abused to send malicious attachments.
Execution	cmd	Utility used to execute commands on Windows systems.
	MMC	Microsoft Management Console. Tool used to manage administrative tools.
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
	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
	ScreenConnect	AKA ConnectWise. RMM tool that can be used to gain persistent remote access to victim environments.
	Regedit	Windows Registry Editor. Windows utility used to modify registry keys.
Privilege Escalation	SC Manager	Windows utility that starts/stops services to gain elevated privileges.
	secedit	Windows utility that modifies system security configurations.
Defense Evasion	Windows Restart Manager	Legitimate API abused to disable security tools, terminate process, and manipulate system processes.
Credential Access	Mimikatz	Hacktool used to extract Windows passwords in plain-text from memory.
Discovery	ipconfig	Windows utility that enumerates network configurations.
	nbtstat	Tool used to troubleshoot NetBOIS name resolution issues.
	nmap	Windows utility used for network discovery and scanning.
	Notepad	Windows utility frequently abused to view logs and collected text artifacts.

Known Tools

Function	Tool	Description
Discovery	nslookup	Windows utility used to query DNS servers.
	Ping	Windows utility used to check host reachability.
	Reg	Windows utility used to query Windows Registry.
	route	Windows utility used to view, add, or modify the local IP routing table.
	SoftPerfect	Tool that scans networks for connected devices, shared folders, and open ports.
	systeminfo	Windows utility that gathers detailed system information.
	Task Manager	Windows utility that enumerates processes and performance.
Lateral Movement	Impacket	Tool for working with network protocols; frequently abused for lateral movement.
	net	Windows utility abused for discovery, lateral movement, and more.
	NetExec	Network exploitation tool that automates SMB/WinRM lateral movement.
	RDP	Microsoft protocol used to remotely connect to a Windows computer.
Exfiltration	Amazon S3 Buckets	Cloud storage containers used to store and manage data as objects.
	Restic	Backup program frequently abused to exfiltrate stolen data.
	temp.sh	Temporary file hosting service frequently abused to host stolen data.
Impact	7-zip	Open-source file archiver used to compress, decompress, and encrypt files.
	VssAdmin	Command line tool abused to delete Volume Shadow Copy Service (VSS).
Infrastructure	TOR	Open-source software enabling anonymous malicious activities, such as command and control, operating data leak sites, and more.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	Bypass UAC prompts via explorer.exe /NoUACCheck
		Abuse of Microsoft Edge renderer process (msedge.exe --type=renderer ...)
		File and device interaction via CreateFileW()
		Device interaction via DeviceIoControl()
		Process termination setup via OpenProcess(PROCESS_TERMINATE)
		Service interaction via ControlService()
		Service manager access via OpenSCManagerW()
		Service handle access via OpenServiceW()
		Restart Manager initialization via RstrtMgr API
		SID creation via AllocateAndInitializeSid()
		I/O completion handling via GetQueuedCompletionStatus()
		Spreadsheet execution from network share via EXCEL.EXE \\<domain>\... \Beebe_WinMerge.xlsx
		Hash validation tooling via GetHashCode.exe
		Veeam agent interaction via Veeam.EndPoint.Tray.exe -CheckNumberOfRunningAgents
Persistence	Configuration Change	Autostart persistence via DesktopConnector.Applications.Tray.exe (StartType: Auto)
Privilege Escalation	Command Execution	Process access using elevated rights via OpenProcess()
Defense Evasion	Command Execution	File truncation and manipulation via SetEndOfFile()
		File truncation and manipulation via SetEndOfFile()

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Defense Evasion	Command Execution	ACL manipulation via SetEntriesInAclW()
		Security descriptor modification via SetNamedSecurityInfoW()
		Privilege lookup and adjustment via LookupPrivilegeValueW() / AdjustTokenPrivileges()
		Device control abuse via DeviceIoControl()
Discovery	Command Execution	Host reachability testing via PING.EXE <hostname>
		Process enumeration via CreateToolhelp32Snapshot()
		Process enumeration via Process32FirstW() / Process32NextW()
		Service status enumeration via QueryServiceStatusEx()
		Dependent service enumeration via EnumDependentServicesW()
		Drive type discovery via GetDriveTypeW()
		Network resource enumeration via WNetOpenEnumW() / WNetEnumResourceW()
		Directory enumeration via enum_dir
		Volume enumeration via FindFirstVolumeW() / FindNextVolumeW()
		Printer enumeration via EnumPrintersW()
		DNS and analytics interaction via DADispatcherService.exe
Collection	Output/Artifact	Sensitive infrastructure documentation accessed via Notepad from network share
Command and Control	Command Execution	Printer subsystem abuse via StartDocPrinterW()
		Print job initiation via StartPagePrinter()

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Impact	Command Execution	Shadow copy deletion via ransomware routine (enc_del_shadow_copies)
		Process termination via TerminateProcess()
		Forced process termination using process handles
		Service shutdown operations (stop_services)
		Shadow copy deletion via ransomware routine (enc_del_shadow_copies)
		Resource registration for shutdown via RmRegisterResources()
		Process impact enumeration via RmGetList()

Observed Behaviors: Linux

Tactic	Evidence Type	Observed Behavior
Impact	Command Execution	Force termination of all running VMs using esxcli vm process kill -t force
		Mass snapshot deletion across VMs via vim-cmd vmsvc/snapshot.removeall

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).

Kill Chain

Initial Access

- Compromised RDP/VPN
- Exploited Vulnerabilities
- Social Engineering Campaigns

Persistence

- Remote Access Software
- Valid Accounts
- Registry Keys and Scheduled Tasks

Defense Evasion

- BYOVD attacks
- XOR string obfuscation
- Terminate security processes
- Modify firewall rules

Lateral Movement

- SMB Share Mounts
- RDP session hijacking
- Cross-system command execution

Exfiltration

- Exploit cloud accounts
- Archived data

Impact

- Encryption using AES-128 in CTR mode with Curve25519 Donna

MITRE ATT&CK® Mappings

Resource Development	
T1587: Develop Capabilities	.001: Malware
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .004: Unix Shell .005: Visual Basic .006: Python .007: JavaScript
T1106: Native API	
T1129: Shared Modules	
T1203: Exploitation for Client Execution	
T1204: User Execution	.001: Malicious Link .002: Malicious File
T1569: System Services	.002: Service Execution

MITRE ATT&CK® Mappings

Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1098: Account Manipulation	.007: Additional Local or Domain Groups
T1136: Create Account	.002: Domain Account
T1137: Office Application Startup	.001: Office Template Macros
T1543: Create or Modify System Process	.003: Windows Process
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
T1556: Modify Authentication Process	
Privilege Escalation	
T1055: Process Injection	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1098: Account Manipulation	.007: Additional Local or Domain Groups
T1134: Access Token Manipulation	
Defense Evasion	
T1027: Obfuscated Files or Information	.003: Steganography .004: Compile After Delivery .010: Command Obfuscation
T1036: Masquerading	.003: Rename Legitimate Utilities .005: Match Legitimate Name or Location

MITRE ATT&CK® Mappings

Defense Evasion	
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1112: Modify Registry	
T1140: Deobfuscate/Decode Files or Information	
T1202: Indirect Command Execution	
T1218: System Binary Proxy Execution	.003: CMSTP .005: Mshta .011: Rundll32
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
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .004: LSA Secrets .005: Cached Domain Credentials
T1056: Input Capture	.001: Keylogging
Discovery	
T1012: Query Registry	

MITRE ATT&CK® Mappings

Discovery	
T1016: System Network Configuration Discovery	
T1018: Remote System Discovery	
T1033: System Owner/User Discovery	
T1046: Network Service 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 .006: Windows Remote Management
T1210: Exploitation of Remote Services	

MITRE ATT&CK® Mappings

Collection	
T1005: Data from Local System	
T1074: Data Staged	.001: Local Data Staging
T1113: Screen Capture	
T1114: Email Collection	
T1115: Clipboard Data	
T1125: Video Capture	
T1185: Browser Session Hijacking	
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1090: Proxy	.002: External Proxy
T1102: Web Service	.001: Dead Drop Resolver .002: Bidirectional Communication
T1104: Multi-Stage Channel	
T1105: Ingress Tool Transfer	
T1219: Remote Access Tools	.002: Remote Desktop Software
T1573: Encrypted Channel	.001: Symmetric Cryptography .002: Asymmetric Cryptography

MITRE ATT&CK® Mappings

Command and Control	
T1132: Data Encoding	.001: Standard Encoding
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/
- DFIR (2025, November 17) “Cat’s Got Your Files: Lynx Ransomware.” https://thedfirreport.com/2025/11/17/cats-got-your-files-lynx-ransomware/
- Halcyon (n.d.) “Lynx.” https://www.halcyon.ai/threat-group/lynx
- Imano, Shunichi; Gutierrez, Fred (2025, February 14) Fortinet: “Ransomware Roundup – Lynx.” https://www.fortinet.com/blog/threat-research/ransomware-roundup-lynx
- Özeren, Sila (2025, February 06) Picus Security: “Lynx Ransomware: Exposing How INC Ransomware Rebrands Itself.” https://www.picussecurity.com/resource/blog/lynx-ransomware
- 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