blackpoint

THREAT PROFILE:

Lynx Ransomware

Table of Contents

Executive Summary

First Identified:
2024

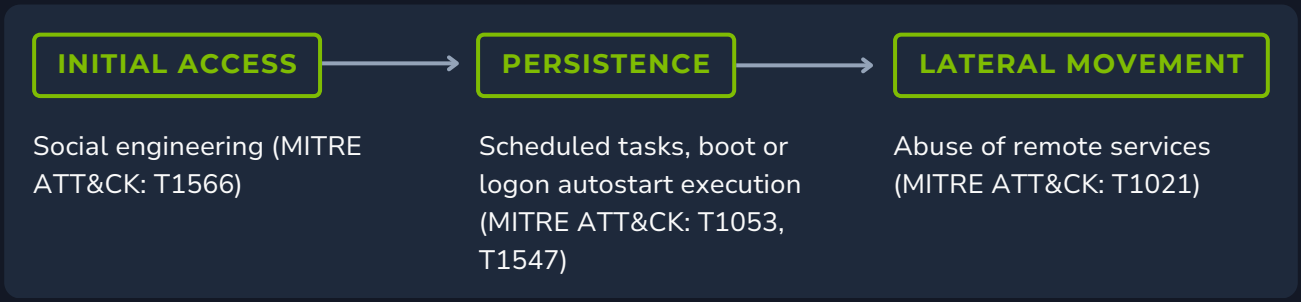
Operation style:
Ransomware-as-a-Service (RaaS)

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 (Construction & Engineering)

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- INC Ransom Ransomware
- 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.

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 uses the DeviceIoControl function to control devices and delete backup copies. In the Lynx ransomware variant, the DeviceIoControl function only works when both the "--file" and "--dir" arguments are not used.

Lynx Ransomware reportedly attempts to change the privileges of files before encrypting them, which requires the operator to obtain administrative privileges. Lynx ransomware does not have a separate privilege escalation function.

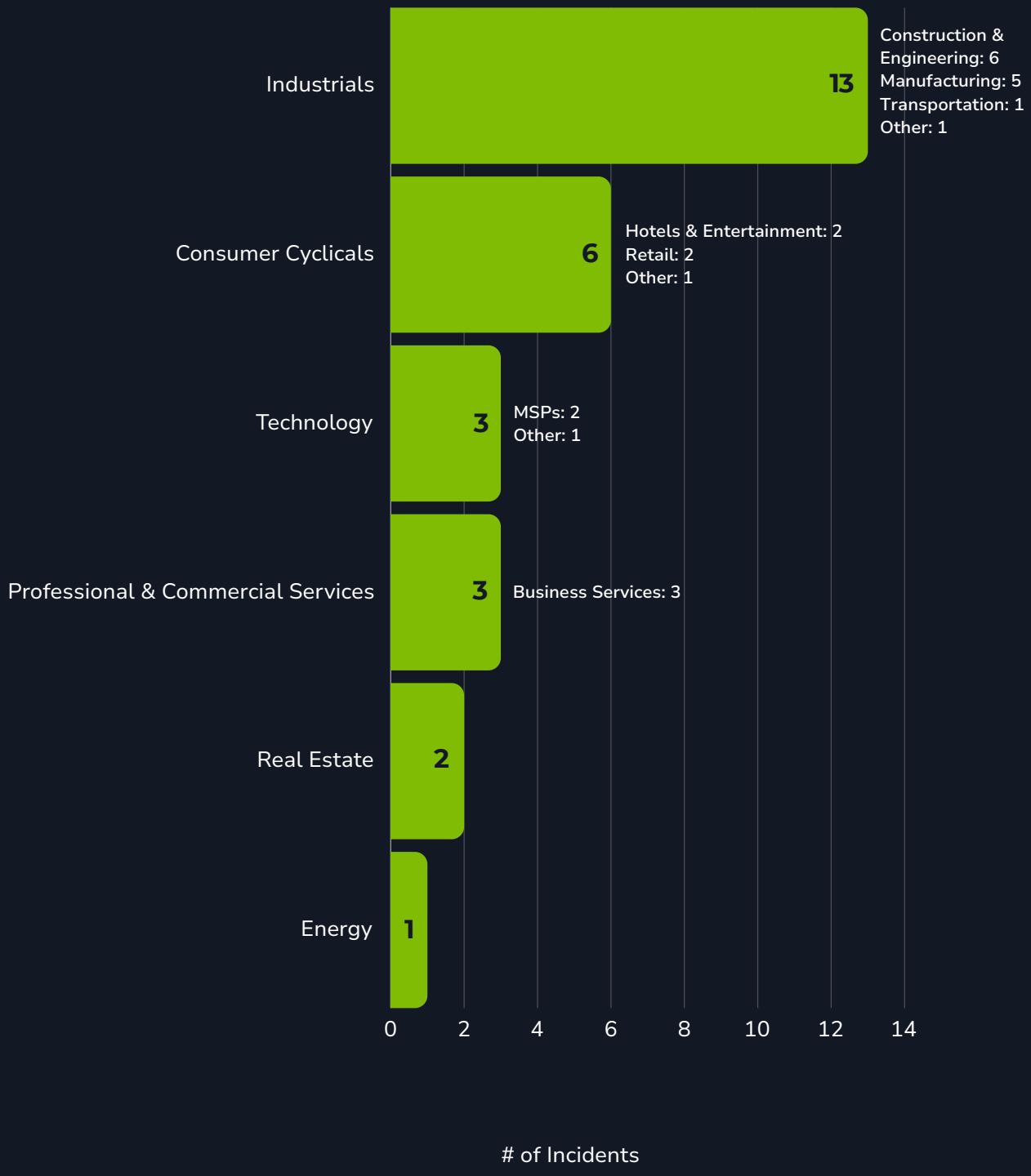
Lynx Ransomware is similar to the INC Ransom operation; however, it is unverified whether the Lynx group purchased the INC source code or if Lynx is the INC successor.

When Lynx ransomware begins encryption, it uses the "medium" mode from the INC Ransom variant. The ransomware encrypts 1MB of every 6MB of the file; files smaller than 1MB are completely encrypted. This differs from INC Ransom, in that INC Ransom offers a "fast" and a "slow" mode of encryption as well.

Lynx ransomware has been assessed to gain initial access to victim environments via phishing emails with malicious attachments, which is a common tactic observed in ransomware attacks.

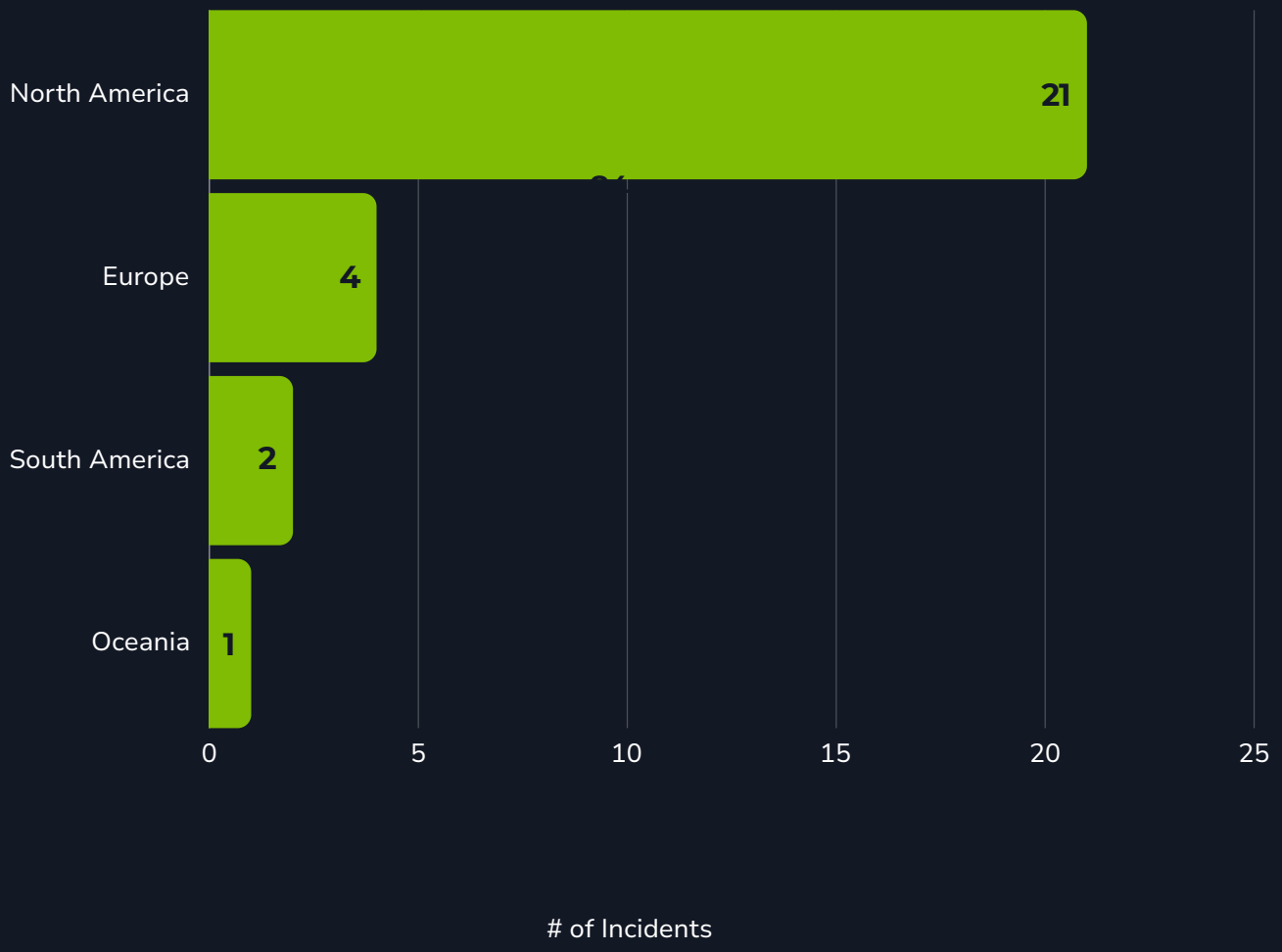
Previous Targets: Lynx

Previous Industry Targets from 01 Jul 2024 to 01 Oct 2024

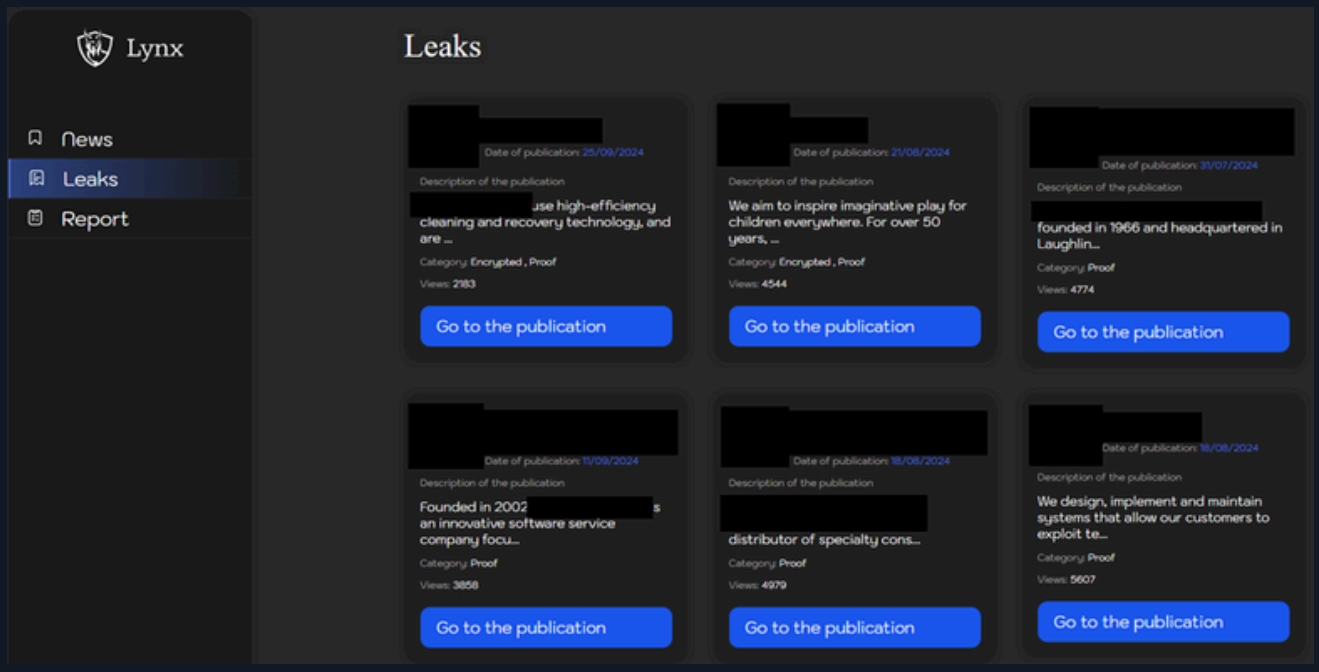


Previous Targets: Lynx

Previous Victim HQ Regions from 01 Jul 2024 to 01 Oct 2024



Data Leak Site: Lynx



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: Lynx

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.

Water Lalawag

Lynx Ransomware operator group tracked by Trend Micro.

Known Tools: Lynx

Text in **bold** indicates behaviors that have been observed by Blackpoint's SOC.

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.
ConnectWise	Formerly ScreenConnect. A self-hosted remote desktop software application that can be used to remotely access victim environments.
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.
netscan	A utility that scans within a subnet or IP range to check for devices.
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.
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.
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.

Observed Lynx Behaviors: Windows

Text in green indicates behaviors that have been observed by Blackpoint's SOC.

Execution	explorer.exe Notepad.exe "\\$domain\nas\IT\Beebe\beebedesign website, DNS, email, etc\DNS Records from AWS - COVI.txt" EXCEL.EXE "\\$domain\nas\IT\Beebe\Egnyte Migration\Beebe_WinMerge.xlsx" windows.exe conhost.exe 0xffffffff -ForceV1 CreateFileW
Persistence	explorer.exe /NoUACCheck regedit.exe ScreenConnect.Client.exe 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 AllocateAndInitializeSid AdjustTokenPrivileges SetNamedSecurityInfoW RmRegisterResources
Privilege Escalation	ServerManager.exe mmc.exe C:\Windows\system32\dnsmgmt.msc explorer.exe SecurityHealthSystray.exe powershell.exe conhost.exe 0xffffffff -ForceV1 Veeam.EndPoint.Tray.exe -NoControlPanel -CheckNumberOfRunningAgents CcmExec.exe SCNotification.exe SeTakeOwnershipPrivilege SetEntriesInAclW SetNamedSecurityInfoW LookupPrivilegeValueW AdjustTokenPrivileges

Observed Lynx Behaviors: Windows

Defense Evasion	explorer.exe /NoUACCheck ALEService.exe GetHashCode.exe "NetWrix Account Lockout Examiner Freeware License1000000ALEe" conhost.exe 0xffffffff -ForceV1 GetHashCode.exe "NetWrix Account Lockout Examiner Freeware License1000000ALE" conhost.exe 0xffffffff -ForceV1 TerminateProcess stop_services ControlService enc_del_shadow_copies
Discovery	explorer.exe netscan.exe ALEService.exe GetHashCode.exe "NetWrix Account Lockout Examiner Freeware License1000000ALEe“ CreateToolhelp32Snapshot Process32FirstW OpenProcess OpenSCManagerW OpenServiceW QueryServiceStatusEx RmGetList LookupPrivilegeValueW GetDriveTypeW WNetOpenEnumW WNetEnumResourceW enum_dir FindFirstVolumeW FindNextVolumeW EnumPrintersW EnumDependentServicesW
Lateral Movement	cmd.exe PING.EXE in2924-dpt5820

Observed Lynx Behaviors: Windows

Collection	DesktopConnector.Applications.Tray.exe StartType:Auto 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 13372976569528800520696 conhost.exe 0xffffffff -ForceV1
Exfiltration	Notepad.exe "\\$domain\nas\IT\Beebe\beebedesign website, DNS, email, etc\DNS Records from AWS - COVI.txt" EXCEL.EXE "\\$domain\nas\IT\Beebe\Egnyte Migration\Beebe_WinMerge.xlsx"
Impact	RstrtMgr – Restart Manager API SetEndOfFile RmStartSession GetQueuedCompletionStatus StartDocPrinterW StartPagePrinter DeviceIoControl

Execution Options: Lynx

--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: Lynx

Initial Access	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	
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
Privilege Escalation	
T1134: Access Token Manipulation	
Defense Evasion	
T1027: Obfuscated Files or Information	
T1036: Masquerading	.005: Match Legitimate Name or Location
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion

MITRE ATT&CK® Mappings: Lynx

Defense Evasion	
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
Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account .002: Domain Account
T1135: Network Share Discovery	
T1652: Device Driver Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol
Collection	
T1005: Data from Local System	
T1113: Screen Capture	

MITRE ATT&CK® Mappings: Lynx

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
Exfiltration	
T1041: Exfiltration Over C2 Channel	
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1657: Financial Theft	

References

- 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/
- 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/
- 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
- 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
- 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