TIR-20250529 A Closer Look at Lynx and SafePay Ransomware

5/29/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

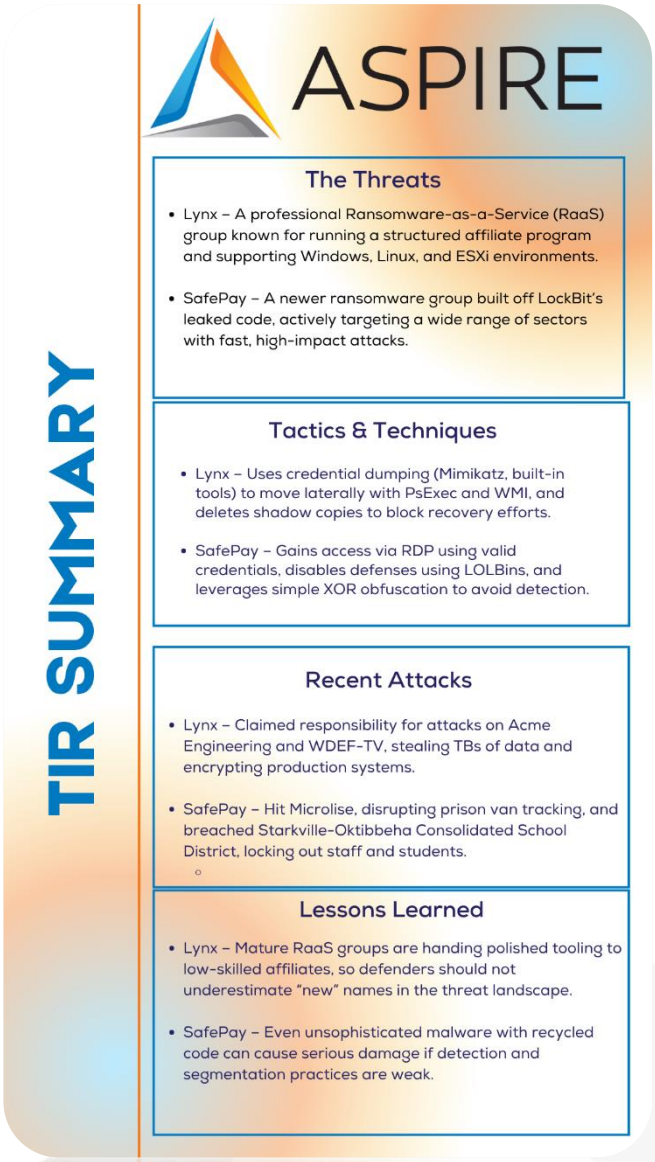
Executive Summary

Lynx and SafePay are two active ransomware groups disrupting critical sectors through distinct but equally damaging methods. Lynx operates with precision, favoring high-value targets in law, finance, and energy. A rebrand of the former INC ransomware group, it relies on a mature affiliate model and low-noise, high-impact extortion.

In contrast, SafePay strikes quickly and loudly, leveraging recycled malware, commercial remote tools, and public data leaks to pressure mid-sized businesses and managed service providers.

Recent months have seen both groups escalate. Lynx is leaning into tailored social engineering and stealthy payload delivery. SafePay is intensifying its pace, often leaking victim data within hours of compromise. Both exploit credential weaknesses and exposed systems, favoring organizations with underdeveloped response capabilities.

The report takes a look at how Lynx and SafePay ransomware groups operate, how they get in, what tools they use, who they've hit recently, and what security teams should be watching for next. It also includes recommendations and MITRE ATT&CK mappings to help security teams stay ahead of how each group actually operates.



LYNX RANSOMWARE

Lynx first emerged in July 2024 as a successor to the INC ransomware family. Researchers at Palo Alto Networks and Fortinet confirmed that the two share significant code overlap. The groups share nearly 50% of matched functions, rising to over 70% when including shared routines. Unlike INC, Lynx offers way more control over how files are encrypted, and it's a lot more flexible in how it operates. The group runs like a well-oiled machine, with a professional affiliate program that hands out ransomware for Windows, Linux, and ESXi systems. Affiliates are given access to an “All-in-One Archive” and a customizable panel with victim tracking, payload generation, and leak site integration.

Public statements from the group claim it avoids targeting hospitals, nonprofits, and government entities, though data leaks suggest these claims are more about optics than strict policy. As of January 2025, Lynx had listed 96 victims on its leak site (over 60% of which were based in the U.S.) with a strong focus on manufacturing, construction, and energy.

Tactics and Techniques

Lynx affiliates operate with discipline and intent. Their attacks aren’t fast or noisy, but methodical and carefully staged. The attacks are also tailored to the victim’s environment. Once inside a network, they take their time, often remaining undetected while they map out infrastructure and evaluate which systems are most valuable, calculating how much pressure they can apply.

Initial access typically comes through phishing emails, RDP brute-force attempts, or exploitation of unpatched external-facing services, particularly VPN appliances and remote collaboration platforms. Affiliates don't rely on popular zero-days; they capitalize on weak configurations and old credentials. Once inside, they typically dump credentials using tools like Mimikatz or native Windows commands, then pivot across the network via PsExec or WMI to escalate access and broaden their reach.

The group has a strong understanding of how IT environments are structured. For example, once they've gained privileges, they’ll manually assess business-critical systems and shared drives, often searching for financial data, intellectual property, or legal records before encryption even begins. This is a classic double-extortion setup.

The file encryption stage is especially granular. Lynx's malware supports custom command-line flags, allowing affiliates to decide whether to encrypt only local files or terminate specific processes. The malware is capable of killing security agents or backup software on the fly. Volume Shadow Copy Service (VSS) backups are routinely deleted to prevent easy restoration. Files are appended with the ".lynx" extension, signaling the final stage of the compromise.

On Linux and ESXi systems, Lynx deploys custom payloads designed to disrupt virtual machines and enterprise storage. These are purpose-built tools distributed through the affiliate panel. In fact, affiliates receive an "All-in-One Archive" containing multiple payloads for different operating systems, plus a victim dashboard, a ransom demand calculator, and templates for negotiation. It's ransomware-as-a-service with enterprise-grade logistics.

What sets Lynx apart from other groups like INC or LockBit isn't just the encryption strength, it's the level of operational flexibility they give their affiliates. The malware is modular and can be adjusted to suit the environment it's deployed in. Affiliates are trained and incentivized to make their attacks as damaging and disruptive as possible — not just through encryption, but through carefully timed execution. Attacks often hit during peak hours or operationally sensitive periods to maximize pressure.

There's also a calculated use of exfiltration. Affiliates typically use secure transfer protocols and encrypt the stolen files during transit to avoid detection. In at least one documented case, over 2TB of proprietary engineering designs were exfiltrated before encryption even began. The data is then staged for release on Lynx's leak site, where samples (including HR documents and employee agreements) are posted to prove authenticity.

From a threat detection standpoint, defenders should be looking for unusual PowerShell activity, suspicious parent-child process relationships involving LOLBins like "cmd.exe," and failed or disabled endpoint protection events. Behavioral monitoring is key, as the malware and its handlers are designed to avoid triggering signature-based detections.

Recent Attacks

Lynx has been responsible for high-profile incidents including:

- **Acme Engineering (February 2025)** – Attackers stole 2 TB of proprietary design data and encrypted the company's infrastructure. The attack reportedly disrupted global manufacturing operations.
- **Electrica Energy (December 2024)** – Romania's national energy firm faced downtime after a targeted attack hit both IT and OT systems.
- **Hunter Taubman Fischer & Li (January 2025)** – A U.S. law firm suffered data exposure of sensitive client documents.
- **WDEF-TV (January 2025)** – Lynx leaked internal documents from a CBS-affiliated TV station, despite claiming not to target media or public institutions.

What to Expect Next

Lynx is expected to continue refining its RaaS infrastructure and expanding affiliate recruitment. Future attacks will likely become more selective, with ransom demands tailored to company size and revenue. By shifting to polymorphic payloads and disguising some of their lures as OneNote files, the group is clearly getting better at staying under the radar. Based on recent activity, industries like manufacturing, legal services, and infrastructure should expect to stay on their radar for the foreseeable future.

SafePay

SafePay emerged in October 2024, and took responsibility for attacks against two Huntress customers. Despite its newness, the group quickly established itself through the use of LockBit-derived code and effective double extortion campaigns. Its ransomware adds the .safepay extension to files and drops readme_safepay.txt ransom notes.

The group now claims over 120 victims, including Microlise, Brighton Australia, and multiple school districts such as Starkville-Oktibbeha Consolidated School District (SOCSD). SafePay maintains leak sites on both the Tor network and The Open Network (TON), listing victims and publishing exfiltrated data in ZIP archives or folder trees. SafePay isn't as polished as Lynx, but the operators know what they're doing. SafePay

has shown a surprising level of technical competency, such as burying key strings to avoid detection, and fine-tuning how and where files get encrypted to hit fast and hard.

Tactics and Techniques

SafePay may be a newer name on the ransomware scene, but their playbook is not basic. Despite building their malware on the leaked LockBit source code, they've made enough modifications to set themselves apart, particularly in how they conduct multi-stage attacks and avoid early detection.

Initial access tends to rely on stolen or weak credentials, often leading to Remote Desktop Protocol (RDP) sessions. Unlike more advanced groups that drop backdoors or create new accounts, SafePay tends to keep things quiet by working directly off the access they already have.

Once inside, SafePay disables security tools with precision. They've reused the same LOLBin sequence seen in previous INC Ransomware campaigns to shut down Windows Defender, suggesting a common playbook, or perhaps even shared operators. They also manually navigate through the system to adjust virus and threat protection settings through the Windows GUI, which most users wouldn't normally touch. That alone can be a detection signal for defenders.

For reconnaissance, SafePay uses the PowerShell script ShareFinder.ps1 to map out network shares. If it's blocked, they find a way around it, either disabling protections or retrying later. File archiving is done using WinRAR, and data exfiltration is carried out via FileZilla. Interestingly, they uninstall both tools after each use, likely to reduce forensic evidence. This install-use-delete cycle isn't something you typically see with lower-skill actors.

SafePay uses common techniques for privilege escalation, including token impersonation and enabling SeDebugPrivilege. They also bypass User Account Control (UAC) with COM object abuse, a trick borrowed from other groups like ALPHV and LockBit. After establishing elevated access, they run commands to delete shadow copies, tamper with boot configurations, and begin encryption. They do this all within minutes of reconnecting to the network.

The ransomware itself runs multithreaded encryption processes, and the group has baked in basic anti-analysis tricks like string obfuscation and runtime thread manipulation. While these features aren't groundbreaking, they're effective enough to

slow down quick-and-dirty reverse engineering. The presence of a Cyrillic-based language check acts as a geographic filter, preventing deployment on machines in Eastern Europe, which likely helps the group avoid regional law enforcement.

Recent Attacks

- **Microlise (November 2024)** – Disrupted logistics tracking for DHL and prisoner transport systems in the UK.
- **Brighton Australia (March 2025)** – SafePay exfiltrated 160GB of architectural files, legal documents, and financial records.
- **SOCSD (December 2024)** – Starkville school district was forced offline after ransomware encrypted network infrastructure.
- **Zamzows Inc. (February 2025)** – U.S. lawn and garden retailer suffered data leaks tied to financial records.
- **Snow Brand and Triton Sourcing** – Early victims in SafePay's first published batch of leaks.

What to Expect Next

SafePay's use of LockBit's builder, combined with its custom tooling, suggests continued evolution. Its public visibility will likely attract more affiliates, pushing the group to optimize ransomware execution speed and C2 infrastructure. Expect more attacks on K-12 education, logistics, and mid-size enterprises with weak RDP hygiene and little segmentation.

Conclusion

Lynx and SafePay may operate differently, but the outcome is the same - data exposure and financial loss. Lynx runs like a well-oiled extortion machine. The group is organized, patient, and selective about who it targets. SafePay is less organized but fast, relying on

borrowed code, weak passwords, and speed to make an impact before defenders can react.

What ties them together is their ability to exploit the basics. Both groups exploit open RDP, misconfigured firewalls, weak credential policies, and slow detection. Both groups lean hard on double extortion tactics and public leak sites, applying pressure where it hurts, which is reputation, operations, and customer trust.

At this point, it's not a matter of if these groups (or groups like them) will hit your sector. It's whether you've done enough to slow them down, detect them early, and recover without paying. That means closing obvious gaps and assuming your backups are part of the target.

ASPIRE'S RECOMMENDATIONS

Lynx is methodical and relies on fine-tuned payload control, often targeting regulated industries. Defenses must focus on blocking silent lateral movement, stopping encrypted file shares, and detecting misuse of backup and business software.

- Monitor for abuse of Restart Manager API
  - Lynx uses the Restart Manager to unlock active files for encryption. Flag unusual API calls, especially on file servers.

- Harden backup solutions against tampering
  - Lynx routinely targets Veeam, Exchange, and other backup-related services. Implement separate credentials, MFA, and immutable storage for backup systems.

- Audit file share permissions and network-mounted drives
  - Lynx payloads include flags to encrypt network drives. Overly permissive shares are prime targets—lock them down and monitor access patterns.

- Detect early payload testing with .lynx extension decoys

  - Drop fake files with .lynx extensions in honeypot directories and monitor for access or modification.

- Hunt for PowerShell abuse tied to process termination or OneNote activity
  - Lynx uses PowerShell to kill processes, print ransom notes, and sometimes even interact with OneNote.

- Block known Tor nodes and Lynx's public leak domains
  - DNS and egress filtering should include known Lynx infrastructure such as lynxblog[.]net and associated .onion mirrors.

SafePay is fast and relies on weak credentials, misconfigured firewalls, and stealthy exfiltration. The focus here is on tightening access controls, catching credential dumping early, and flagging exfiltration prep.

- Immediately audit RDP and VPN for weak or misconfigured access
  - SafePay is known to exploit Fortigate misconfigs and log in with valid domain creds that bypass MFA. Check RDP logs and enforce IP allowlists.

- Flag batch file execution from unusual directories (e.g., C:\ProgramData)
  - SafePay's deployment often begins with batch scripts like 1.bat. Restrict execution and monitor high-risk folders.

- Block or monitor use of WinRAR and FileZilla on non-admin systems
  - These tools are consistently used for staging and exfiltration. Their presence during business hours should raise red flags.

- Deploy behavior-based detection for ScreenConnect installs
  - SafePay installs ScreenConnect as a service for persistence. Treat new installs of remote management software as high risk.

- Track use of LOLBins like regsvr32 and bcdedit in privilege escalation chains
  - SafePay mimics techniques from INC and LockBit, including COM-based UAC bypass and system recovery tampering.

- Block outbound connections to known C2 infrastructure and TON domains
  - SafePay communicates with infrastructure like 88.119.167[.]239 and maintains a leak site on The Open Network. Block and monitor DNS logs for signs of contact.

MITRE MAP

Lynx

Initial Access	T1566.001 - Phishing
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell
Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Key/ Startup Folder
Defense Evasion	T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control T1027 – Obfuscated Files or Information
Impact	T1486 – Data Encrypted for Impact

SafePay

Initial Access	T1190 – Exploit Public Facing Application T1078 – Valid Accounts
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell T1059.001 - Command and Scripting Interpreter: PowerShell
Persistence	T1543.003 - Create or Modify System Process: Windows Service
Defense Evasion	T1027.002 - Obfuscated Files or Information: Software Packing T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control
Credential Access	T1003 – Credential Dumping

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Lynx

- Ransom note
  - README.txt
- File extension
  - .lynx
- Leak site
  - lynxblog[.]net, multiple Tor mirrors
- Known C2 domains and email
  - martina.lestariid1898@proton[.]me
- SHA256
  - 31de5a766dca4eaae7b69f807ec06ae14d2ac48100e06a30e17cc9acccfd5193
  - 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e
  - 432f549e9a2a76237133e9fe9b11fbb3d1a7e09904db5ccace29918e948529c6
  - 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
  - 4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412
  - 571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
  - 589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a23
  - 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441
  - 85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf5683
  - 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0
  - 9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896
  - b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee
  - d5ca3e0e25d768769e4afda209aca1f563768dae79571a38e3070428f8adf031
  - eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
  - ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49
  - f71fc818362b1465fc1deb361de36badc73ac4dd9e815153c9022f82c4062787

SafePay

- Ransom Note
  - readme_safepay.txt

- File Extension
  - .safepay

- SHA256
  - 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae
  - e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346

- IPV4
  - 206[.]217[.]206[.]10
  - 206[.]217[.]206[.]57
  - 38[.]180[.]62[.]88
  - 68[.]235[.]46[.]80
  - 52[.]26[.]33[.]146

- File Path
  - locker.dll
  - readme_safepay.txt

SUPPORTING DOCUMENTATION

IOC Related to SafePay Ransomware Attack - LevelBlue - Open Threat Exchange

Ransomware Roundup – Lynx | FortiGuard Labs

Acme Engineering Hit by Lynx Ransomware Attack

Weak Passwords Led to (SafePay) Ransomware | NCC Group

Lynx Ransomware: A Rebranding of INC Ransomware

Lynx Ransomware: Attack Vectors, Impact, And Mitigation Strategies

CBS affiliate purportedly compromised by Lynx ransomware gang | SC Media

Lynx Ransomware

Ransomware attack likely responsible for IT crisis at SOCSD - The Dispatch

SafePay ransomware gang claims attack on UK's Microlise • The Register

SafePay ransomware: Obscure group uses LockBit builder, claims 22 victims | SC Media

SafePay Ransomware Report | Quorum Cyber

Malware analysis SafePay Malicious activity | ANY.RUN - Malware Sandbox Online

[SAFEPAY] - Ransomware Victim: conduent[.]com - RedPacket Security

SafePay Ransomware: A New Threat with Sophisticated Techniques

Microlise Confirms Data Breach as Ransomware Group Steps Forward - SecurityWeek

Cat’s out of the bag: Lynx Ransomware-as-a-Service | Group-IB Blog

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.