Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

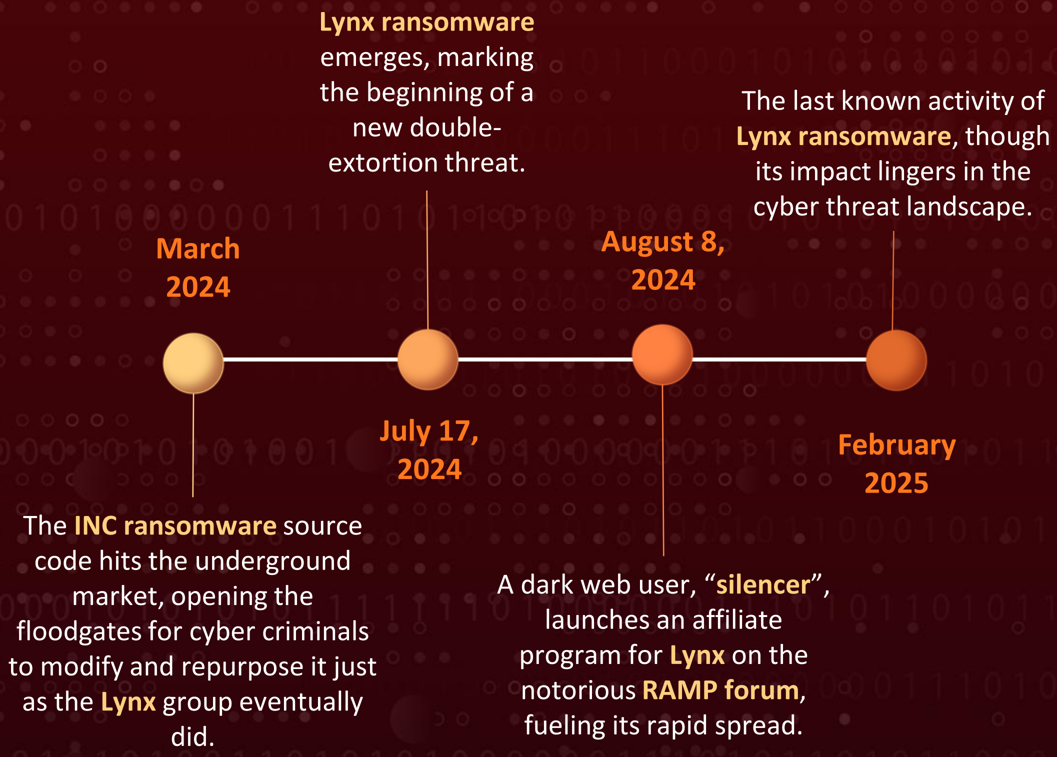
Lynx Ransomware in Action: Pay Up or Face the Consequences

Date of Publication	Admiralty Code	TA Number
February 7, 2025	A1	TA2025033

Summary

Active Since: July 2024
Malware: Lynx Ransomware
Affected Platforms: Windows, Linux
Targeted Industries: Advertising, Aerospace, Agriculture, Automotive, Aviation, Banking, Business Services & Consulting, Construction, Consumer Goods, E-Commerce, Electronics, Energy, Engineering, Environmental Services, Financial Services, Food and Beverage, Government, Hardware, Healthcare, Hospitality, Legal, Manufacturing, Marketing, Media, Mining, Oil & Gas, Privacy and Security, Professional Services, Real Estate, Retail, Technology, Telecommunications, Transportation
Targeted Countries: Argentina, Australia, Bahrain, Belgium, Canada, Cape Verde, China, Costa Rica, Dominica, France, Guatemala, India, Ireland, Italy, Kuwait, Luxembourg, Oman, Qatar, Saudi Arabia, Singapore, Sweden, Thailand, Turkey, United Arab Emirates, United Kingdom, United States
Attack: Lynx is a rapidly evolving Ransomware-as-a-Service (RaaS) operation that employs a double-extortion strategy, crippling victims by encrypting their data while using stolen information as leverage. Designed for multi-platform attacks, it targets Windows, Linux, and ESXi systems, with advanced encryption and disruptive capabilities, including virtual machine shutdowns. Operated through a customizable affiliate model, Lynx provides cyber criminals with a centralized dashboard to manage infections and ransom negotiations.

Attack Timeline



March 2024

The **INC ransomware** source code hits the underground market, opening the floodgates for cyber criminals to modify and repurpose it just as the **Lynx** group eventually did.

July 17, 2024

Lynx ransomware emerges, marking the beginning of a new double-extortion threat.

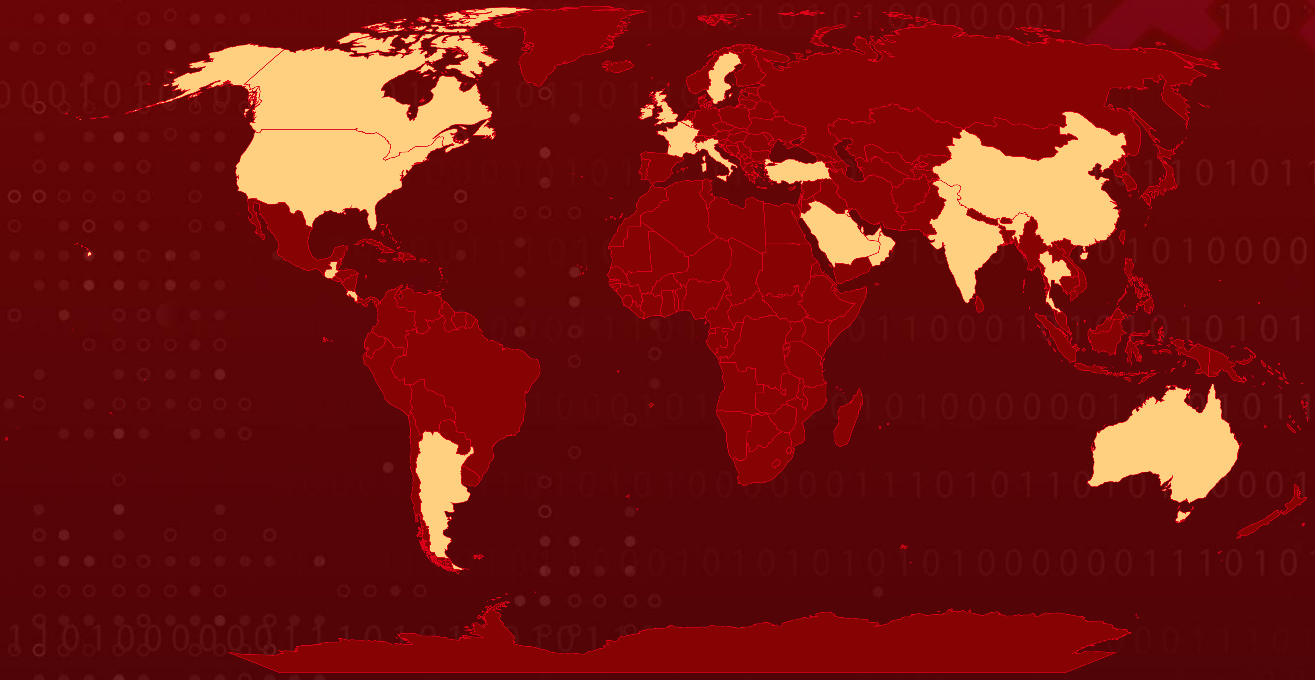
August 8, 2024

A dark web user, "**silencer**", launches an affiliate program for **Lynx** on the notorious **RAMP forum**, fueling its rapid spread.

February 2025

The last known activity of **Lynx ransomware**, though its impact lingers in the cyber threat landscape.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Lynx operates as a Ransomware-as-a-Service (RaaS) operation, leveraging an affiliate-driven model to orchestrate cyberattacks. By recruiting penetration testers and initial access brokers, Lynx affiliates infiltrate targeted networks, establishing unauthorized access before executing their attack. Once inside, they exfiltrate sensitive data, maximizing their leverage before deploying the ransomware payload.

#2 The malware encrypts files while disabling key recovery mechanisms such as shadow copies and volume snapshots, effectively crippling the victim's ability to restore their systems. This double-extortion tactic intensifies pressure on organizations, as stolen data is used as a bargaining chip during ransom negotiations. In recent weeks, Lynx has been notably active, listing multiple compromised companies on its leak site.

#3 Lynx is designed for cross-platform deployment, with ransomware samples available for Windows, Linux, and ESXi, as well as lesser-known architectures like ARM, MIPS, and PPC. This broad compatibility allows affiliates to target a diverse range of systems, including enterprise environments and specialized hardware.

#4 The ransomware employs AES-128 (CTR) encryption combined with Curve25519 Donna, a cryptographic approach that ensures robust data protection against decryption attempts. Affiliates can fine-tune their attacks using variable encryption modes, offering options such as "fast," "medium," "slow," and "entire" to balance encryption speed against inflicted damage.

#5 To further disrupt enterprise operations, Lynx includes functionality to shut down virtual machines on ESXi servers, making recovery efforts significantly more challenging. An integral component of the Lynx ecosystem is its customizable affiliate panel, a centralized interface that enables attackers to manage infections, track victims, and schedule data leaks efficiently.

#6 This level of operational control makes Lynx an attractive choice for cybercriminals seeking an organized, scalable ransomware model. Both Windows and Linux versions of Lynx exist. The ransomware follows standard post-encryption procedures, including appending the ".LYNX" extension to encrypted files and modifying the compromised system's desktop wallpaper with a ransom note.

#7 The Windows variant, written in C++, shares significant portions of its source code with INC ransomware. This threat emerged in August 2023 and was similarly designed for both Windows and Linux environments. Despite its similarities to other ransomware families, Lynx’s active presence and technical adaptability make it a formidable threat in the evolving ransomware landscape. With its continued development and aggressive affiliate model, organizations should remain vigilant against this increasingly prevalent cyber threat.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Harden Virtual and Cloud Environments: Limit administrative access and implement secure authentication for virtualized infrastructure. Watch for unauthorized shutdowns of virtual machines, which Lynx ransomware uses to disrupt operations.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1489 Service Stop	T1562 Impair Defenses	T1057 Process Discovery	T1071 Application Layer Protocol
T1059.004 Unix Shell	T1134 Access Token Manipulation	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery
T1543 Create or Modify System Process	T1055 Process Injection	T1070 Indicator Removal	T1070.004 File Deletion
T1213 Data from Information Repositories	T1083 File and Directory Discovery	T1041 Exfiltration Over C2 Channel	T1059 Command and Scripting Interpreter
T1140 Deobfuscate/Decode Files or Information	T1560 Archive Collected Data	T1005 Data from Local System	T1497 Virtualization/Sandbox Evasion

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	lynxblog[.]net
Email	martina[.]lestariid1898[@]proton[.]me
SHA256	80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441, 80fd105d0685b85c1be5d5d3af63608d2ec91b186d4c591416934fe454770ca1, 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e, 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0, 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a, 432f549e9a2a76237133e9fe9b11fbb3d1a7e09904db5ccace29918e948529c6, 4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412, 9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896, 31de5a766dca4eaae7b69f807ec06ae14d2ac48100e06a30e17cc9acccfd5193, 589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a23, d5ca3e0e25d768769e4afda209aca1f563768dae79571a38e3070428f8adf031, 85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf5683, b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee, ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49, 571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b, eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc, 82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513, c02b014d88da4319e9c9f9d1da23a743a61ea88be1a389fd6477044a53813c72
TOR Address	lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion, lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd[.]onion,

TYPE	VALUE
TOR Address	lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd[.]onion, lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad[.]onion, lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad[.]onion, lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad[.]onion, lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion, lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid[.]onion, lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd[.]onion, lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd[.]onion, lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd[.]onion, lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd[.]onion, lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd[.]onion, lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad[.]onion, lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad[.]onion, lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad[.]onion, lynxad2seqpyu52lr5v7il4idasv23535a46s4bj65b3v7t5y6u5daqd[.]onion, lynx2m7xz73zpmlm5nddbokk6a55fh2nzjq2r5nk2hbdbk74iddqfiqd[.]onion, lynxcwuhva6qzlnj3m3qrcl6bgvnxpixg5vsikf53vutdf3ijuv2pxyd[.]onion, lynxcyys7c2np3b3er2wo6sufwoonmh6i3nykv53pst336c3ml4ycjqd[.]onion, lynxdehvlvrrtnhtpuy6bhrxffzvl5j7y7p3zl553slzq44lcb2jzkyd[.]onion, lynxikczcyposxfz5a7hxbqxilsrtx7zdzwmhk5wcb5qoatbv2suizid[.]onion, lynxroggpujfxy7xnlrz3yknphqgk4k5dy4rhaldgz2hpxyyy3ncuvad[.]onion, lynxoifh5boac42m6xdoak6ne7q53sz7kgaaze7ush72uuetbnjg2oqd[.]onion, lynx25vsi4cxesh44chevu2qyguqcx4zrjsjd77cjrmbgn75xkv626yd[.]onion, lynxaeddweqscykez5rknrug6ui5znq4yoxof5qnusiatiyuqqlwhead[.]onion, lynxbk3nzrnph5z5tilsn3twfcgltqynaofuxgb5yt43vdu266z3vvyd[.]onion,

TYPE	VALUE
TOR Address	lynxhwtifuwxs2zejofpagvzxf7p2l3nhdi3zlrap3y2wsn5hqyfeuid[.]onion, lynxjamasdeyeeiusfgfipfivewc3l3u34hyiiguhdyj776mh535l4ad[.]onion, lynxk7rmhe7luff3ed7chlziwrju34pzc5hm452xhryeaeulc3wxc3ad[.]onion

Recent Breaches

https://zamzows.com/
https://scottengr.com/
https://tri-sen.com/
https://jalaramproduce.com/
https://kpiengineering.com/
https://www.sibelco.com/en/sustainability/glass-recycling-north-america
https://sce.org.sg/
https://alocenter.se/
https://www.enginepowersource.com/
https://www.sunnydayssunshinecenter.com/
https://www.marukai.com/
https://www.sentinelsystems.com/
https://www.clutchindustries.com.au/
https://thewendtagency.com/
https://loweengineers.com/
https://www.delta-screens.com/
https://www.rossi-realestate.com/
https://worldwidefoam.com/
https://www.ddcwsa.com/
https://kassincarrow.com/
https://www.mintz.com/
https://www.kinseth.com/
https://novati.com.au/
https://delapandwaller.com/
https://sergas.com/
https://www.conad.it/
https://www.gossettmotors.com/
https://d7roofing.com/
https://exceltransportation.com/
https://www.jimthompson.com/en

References

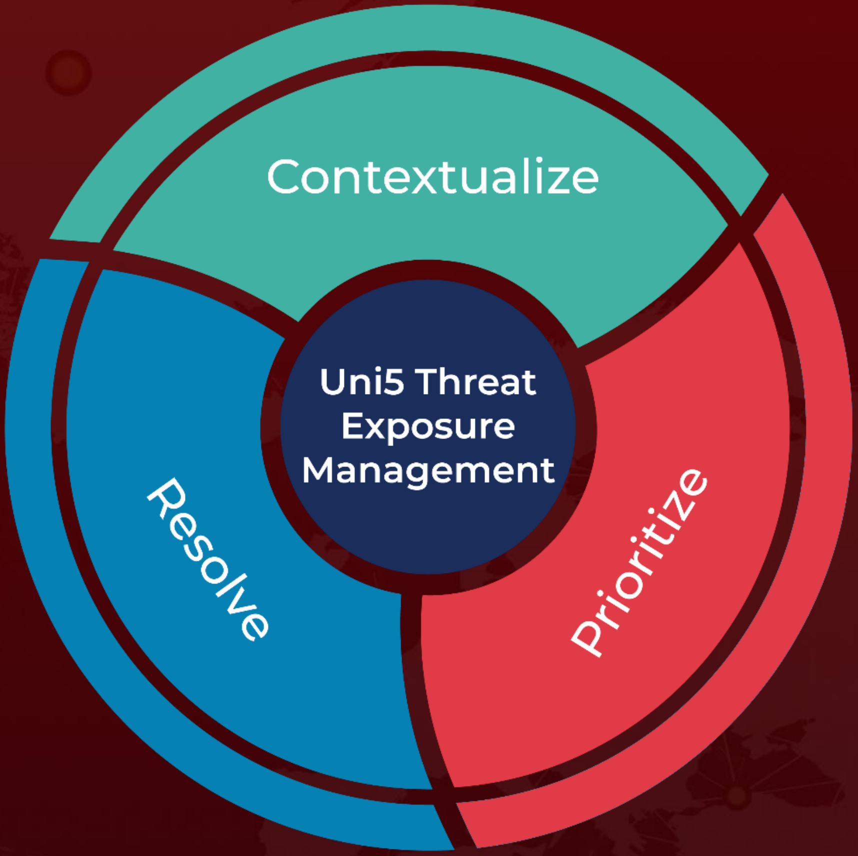
https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/

https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 7, 2025 • 4:00 AM

More at www.hivepro.com