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

Introduction

Ransomware remains one of the most profitable cyberthreats, with new variants and business models evolving faster than many organizations can respond. Fueled by the expansion of Ransomware-as-a-Service (RaaS), the proliferation of stolen data on Dedicated Leak Sites (DLS), and the rise of affiliate-driven operations, these attacks have become both more pervasive and more sophisticated.

The Lynx RaaS group stands out for its highly organized platform, structured affiliate program, and robust encryption methods. In this blog, we provide an exclusive look at Lynx’s affiliate panel, internal communications, and technical arsenal, revealing how this criminal ecosystem orchestrates ransomware attacks and manages victims.

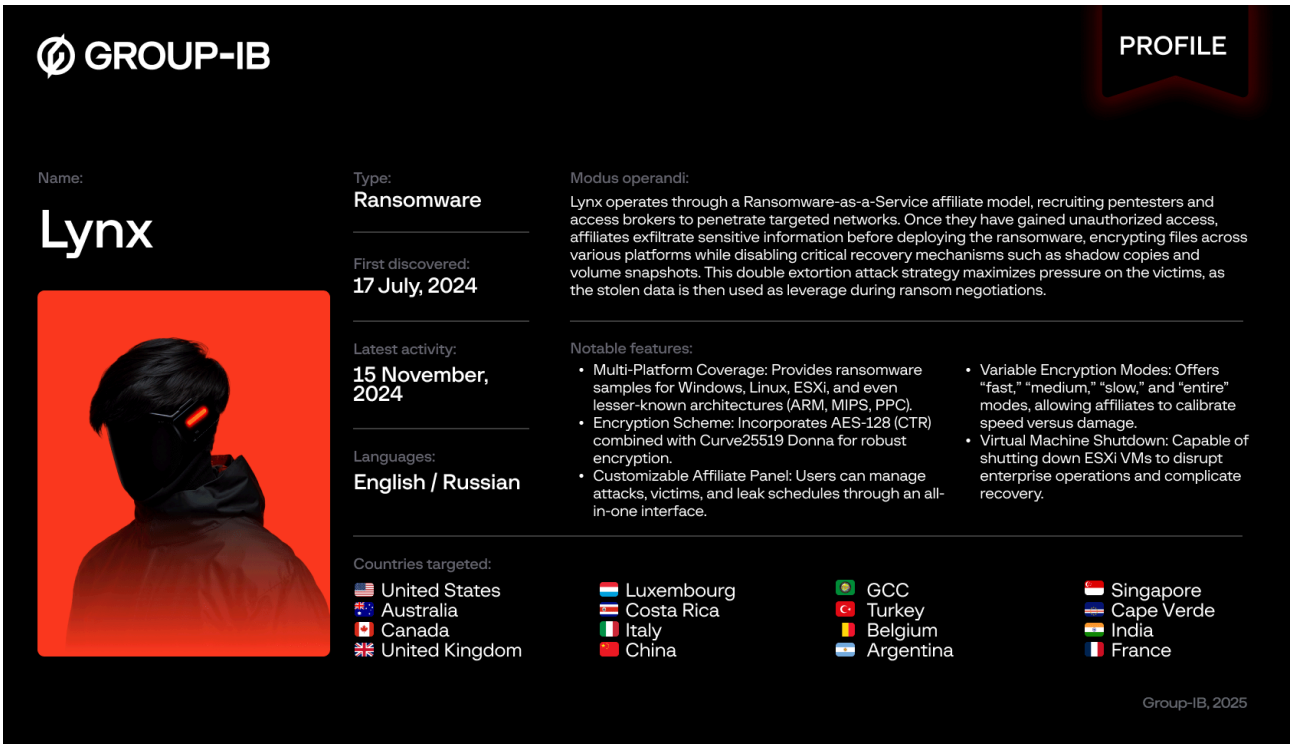
Key Discoveries in this Blog

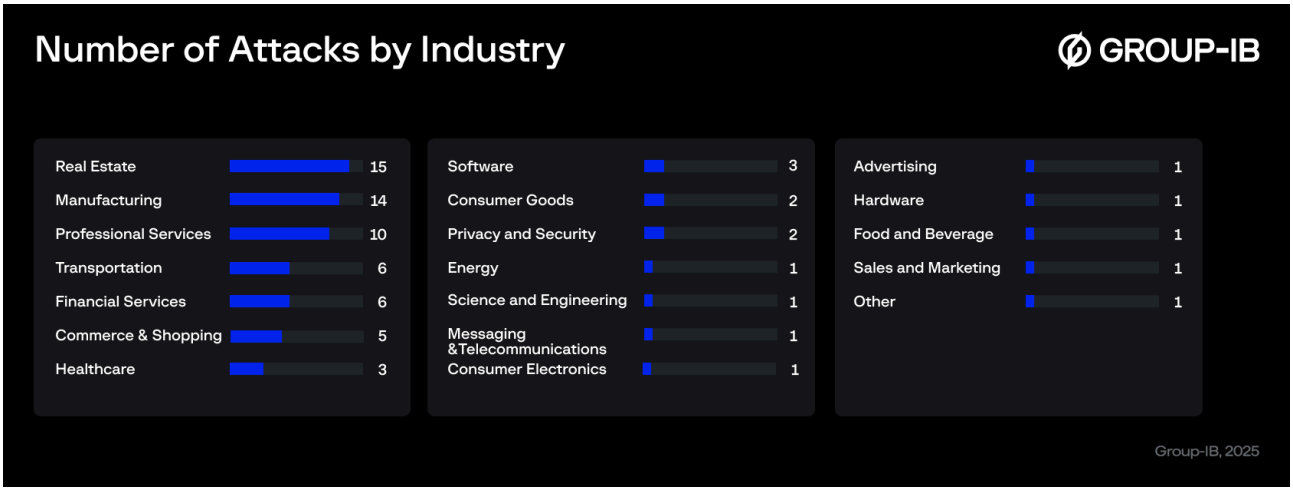
- **Structured RaaS Panel and Workflow:** Lynx’s affiliate panel is divided into multiple sections (e.g. “News,” “Companies,” “Chats,” “Stuffers,” and “Leaks”), each serving a clear purpose. Affiliates can configure victim profiles, generate custom ransomware samples, and even manage data-leak schedules within a single, user-friendly interface.
- **Cross-Platform Ransomware Arsenal:** Lynx provides affiliates with a comprehensive “All-in-One Archive,” containing binaries for Windows, Linux, and ESXi environments, covering a range of architectures (ARM, MIPS, PPC, etc.). This multi-architecture approach ensures broad compatibility and maximizes the impact of attacks in heterogeneous networks.
- **Affiliate Features and Double Extortion:** Affiliates are incentivized with an 80% share of ransom proceeds, reflecting a competitive, recruitment-driven strategy. Lynx’s panel includes a dedicated leak site (DLS) where stolen data is publicly exposed if ransoms go unpaid, adding critical pressure on victims to comply.
- **Customizable Encryption Techniques:** Lynx recently added multiple encryption modes: “fast,” “medium,” “slow,” and “entire”, giving affiliates the freedom to adjust the trade-off between speed and depth of file encryption. The use of Curve25519 Donna and AES-128 encryption emphasizes Lynx’s focus on robust, proven cryptography.
- **Professional Recruitment and Vetting:** The group’s recruitment posts on underground forums emphasize a stringent verification process for pentesters and skilled intrusion teams, highlighting Lynx’s emphasis on

operational security and quality control. They also offer “call centers” for harassing victims and advanced storage solutions for affiliates who consistently deliver profitable results.

Who may find this blog interesting:

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams (CERT)
- Law enforcement investigators
- Cyber police forces





The dedicated leak site (DLS) of the Lynx ransomware serves as a platform where attackers publish announcements regarding attacks and disclose leaked data from their victims.

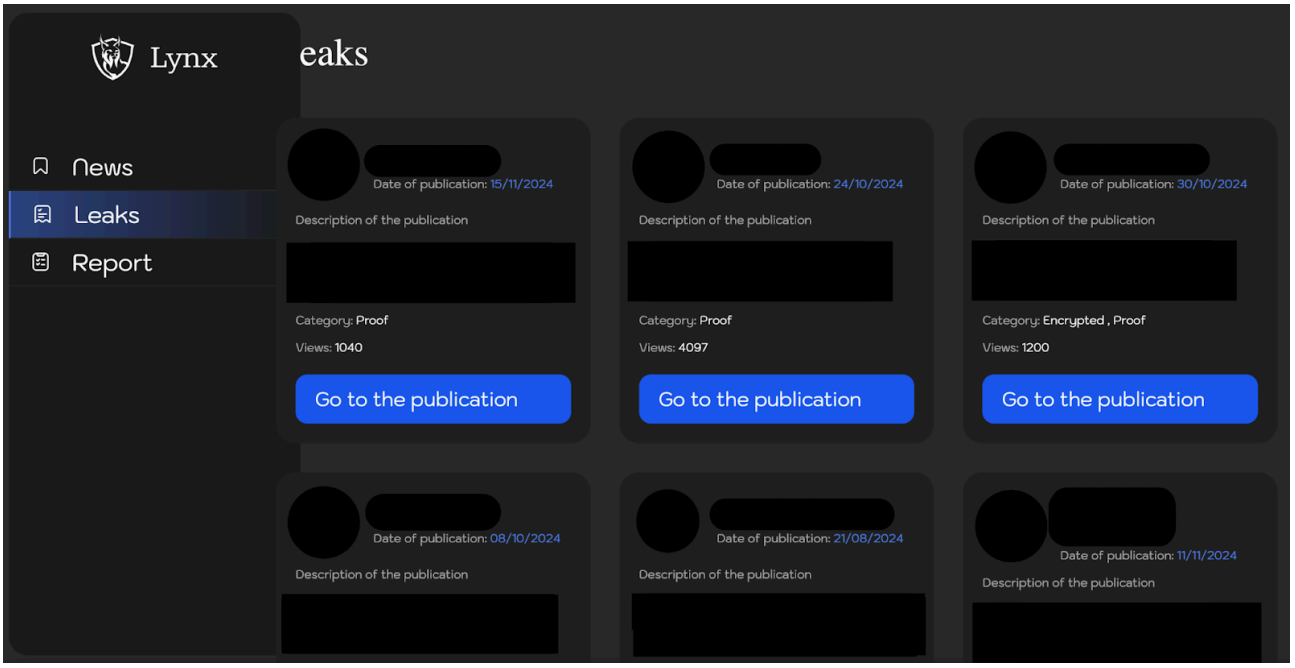


Figure 1. Screenshot of a dedicated leak site (DLS) of Lynx ransomware.

On 8-August 2024, a user named “silencer” started an affiliate program of the Lynx ransomware as a topic on the popular underground dark web forum “RAMP”.

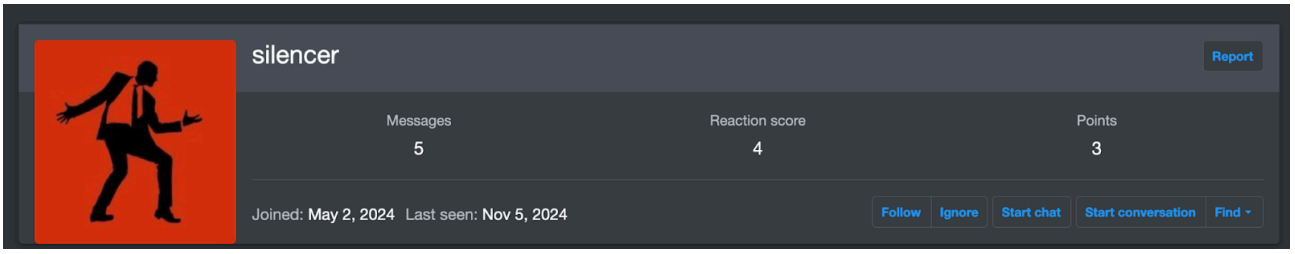


Figure 2. Screenshot of the user profile “silencer” on the RAMP forum.

Information from Affiliate Program Recruitment:

The Lynx ransomware group has published a recruitment post targeting experienced penetration testing teams. The post provides a detailed description of the group’s capabilities, tools, and expectations for potential collaborators, indicating a structured and professionalized criminal operation.

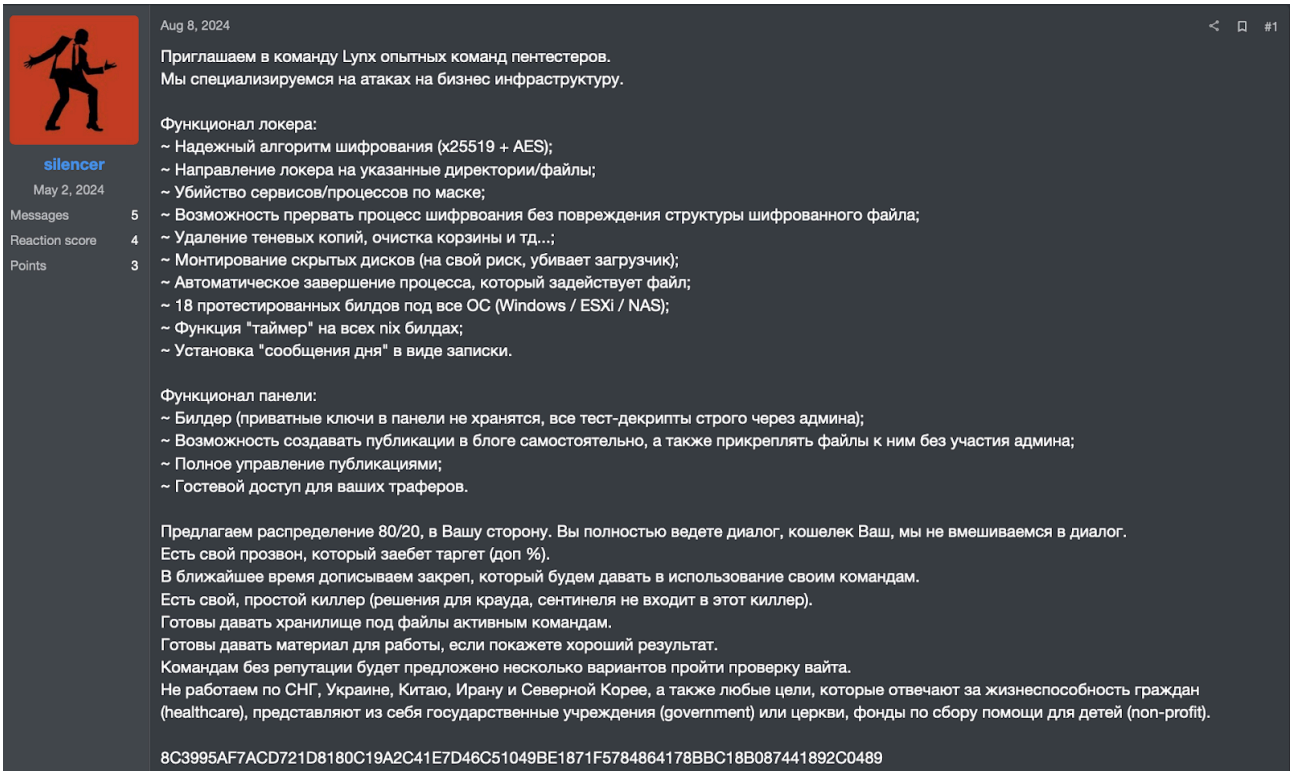


Figure 3. Screenshots of a post by Lynx promoting its ransomware-as-a-service on the RAMP forum.

The following is a translation of the topic posted by Lynx, from Russian to English:

We invite experienced pentesting teams to join the Lynx team.
We specialize in attacks on business infrastructure.

Locker Functionality:
~ Reliable encryption algorithm (x25519 + AES);
~ Directing the locker to specified directories/files;
~ Killing services/processes by mask;
~ Ability to interrupt the encryption process without damaging the structure of the encrypted file;
~ Deleting shadow copies, clearing the recycle bin, etc.;
~ Mounting hidden disks (at your own risk, may corrupt the bootloader);
~ Automatic termination of processes that use targeted files;
~ 18 tested builds for all operating systems (Windows / ESXi / NAS);
~ “Timer” feature available on all nix builds;
~ Setting a “message of the day” as a ransom note.

Panel Functionality:
~ Builder (private keys are not stored in the panel; all test decrypts are strictly handled through the admin);
~ Ability to independently create blog posts and attach files without admin involvement;
~ Full management of publications;
~ Guest access for your traffickers.

We offer an 80/20 split in your favor. You handle all negotiations, the wallet is yours, and we do not interfere in the process.
We have our own call service (“прозвон”) that will harass the target (extra %).
In the near future, we are completing a persistent tool that will be provided to our teams.
We also have a simple killer (doesn’t include solutions for CrowdStrike or Sentinel).
We are ready to provide storage for files to active teams.
We can provide materials for work if you show good results.

Teams without a reputation will be offered several options to pass “white” verification.
We do not work in the CIS, Ukraine, China, Iran, or North Korea, nor do we target entities responsible for the livelihood of civilians (healthcare), government institutions, churches, or children’s charities (non-profits).

Group-IB specialists successfully infiltrated the Lynx RaaS group by leveraging qTox to establish contact with the intruder. This allowed to gain access to the group’s affiliate panel, providing critical insights into its operations.

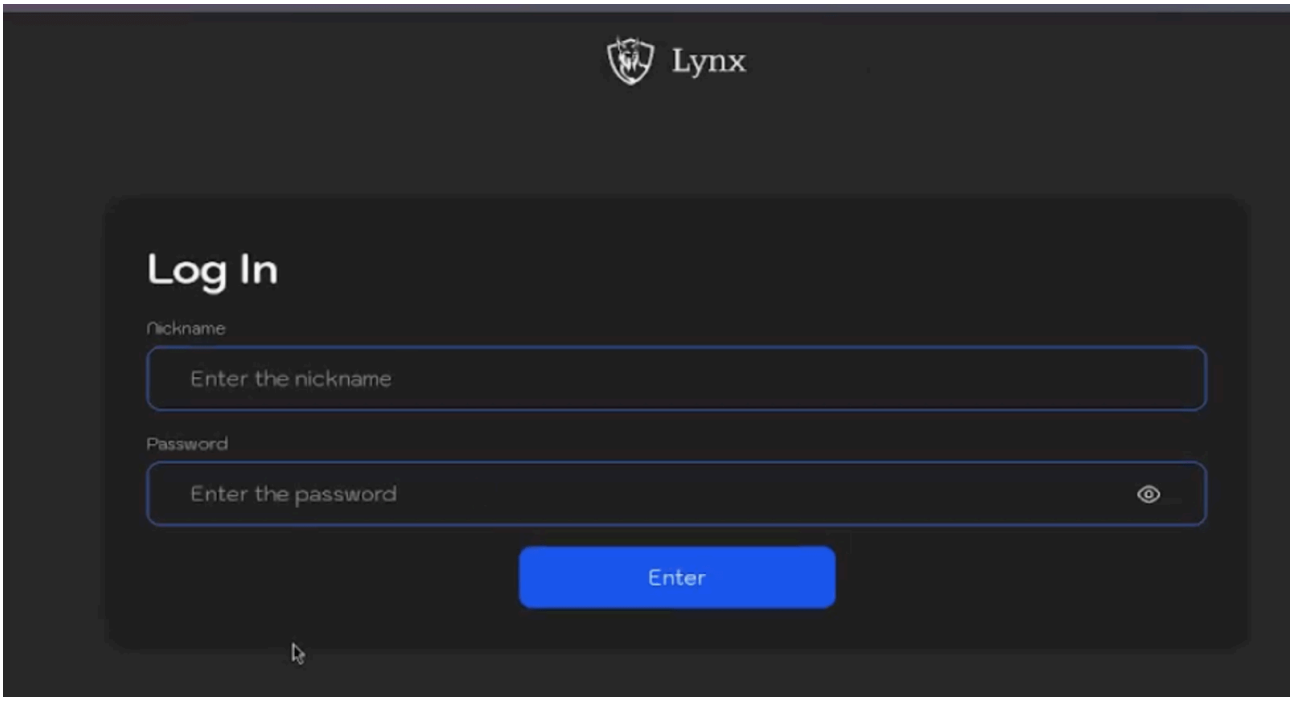


Figure 4. Screenshot of the authentication page of Lynx ransomware group.

The Affiliates’ panel of the Lynx ransomware group featured various sections, including “News,”, “Chats”, “Companies”, “Stuffers” and “Leaks”, each serving distinct purposes within the group’s operations.

News

The “News” section within the Lynx ransomware group’s affiliate panel serves as a central hub for updates and announcements. It provides affiliates with critical information, such as details on new features added to the locker or panel, as well as essential resources like updated mirrors for the group’s blog and admin panel.

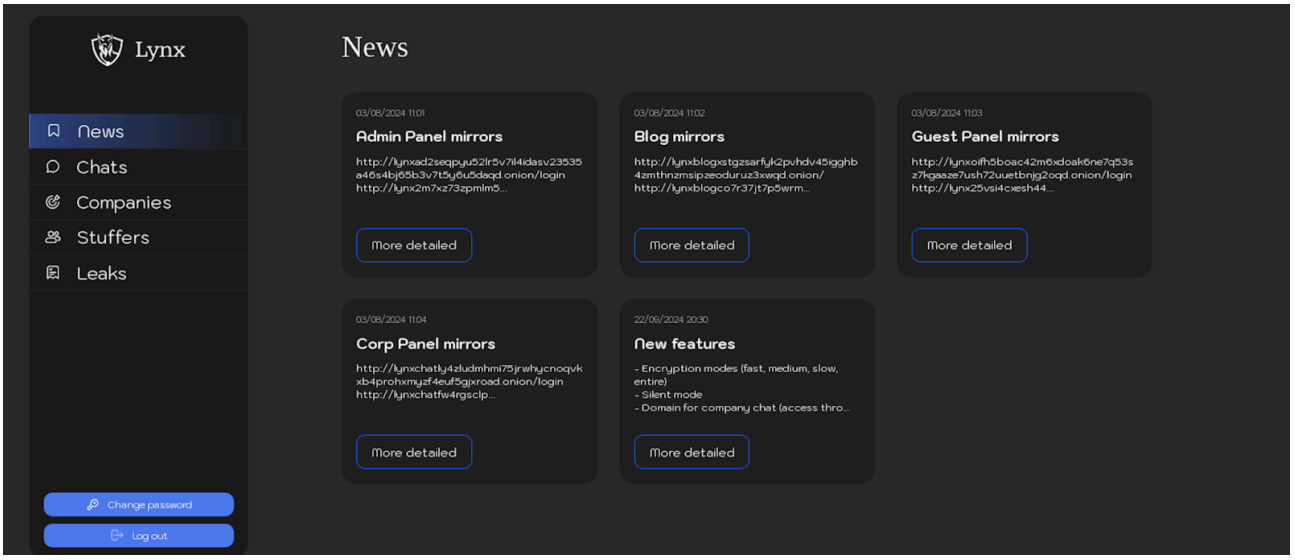


Figure 5. Screenshot of the section “News” of Lynx ransomware panel.

Below is a table detailing the observed updates and publication dates from the “News” section of the Lynx ransomware group’s affiliate panel:

Date	**Title of the news:**
03.08.2024	Admin panel mirrors
03.08.2024	Blog mirrors
03.08.2024	Guest panel mirrors
03.08.2024	Corp panel mirrors
22.09.2024	New features

Below are screenshots from the “News” section, showcasing posts related to the mirrors of the Lynx ransomware group’s infrastructure.

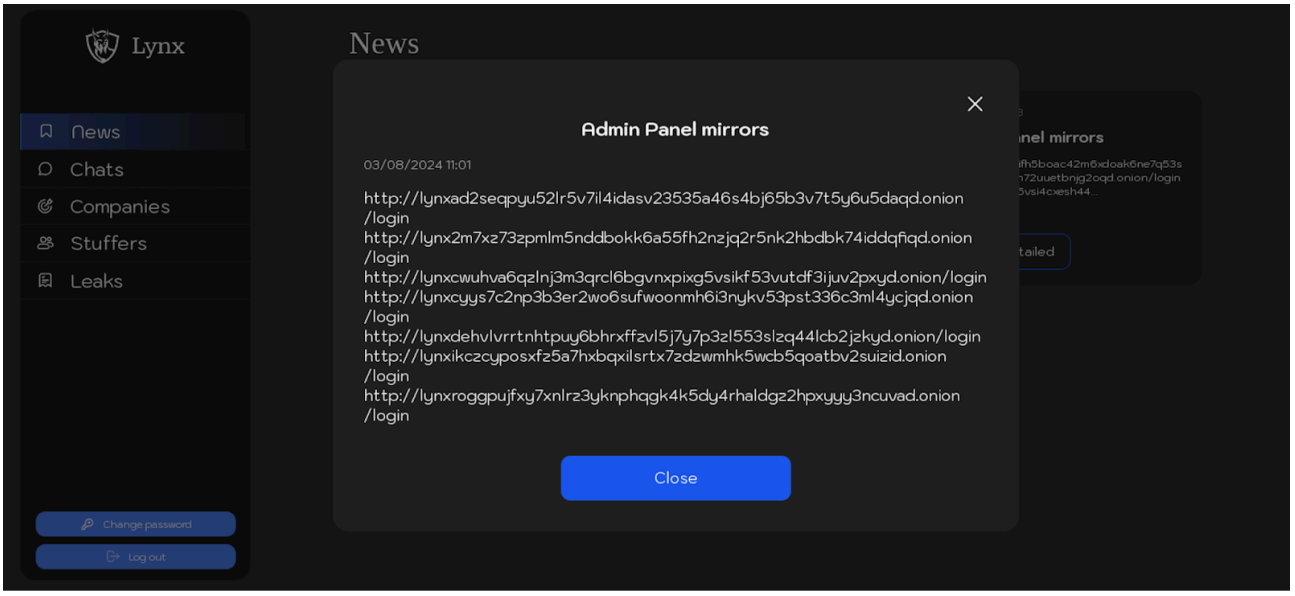


Figure 6. Screenshots of posts in the “News” section of Lynx ransomware panel, dated 3 August 2024.

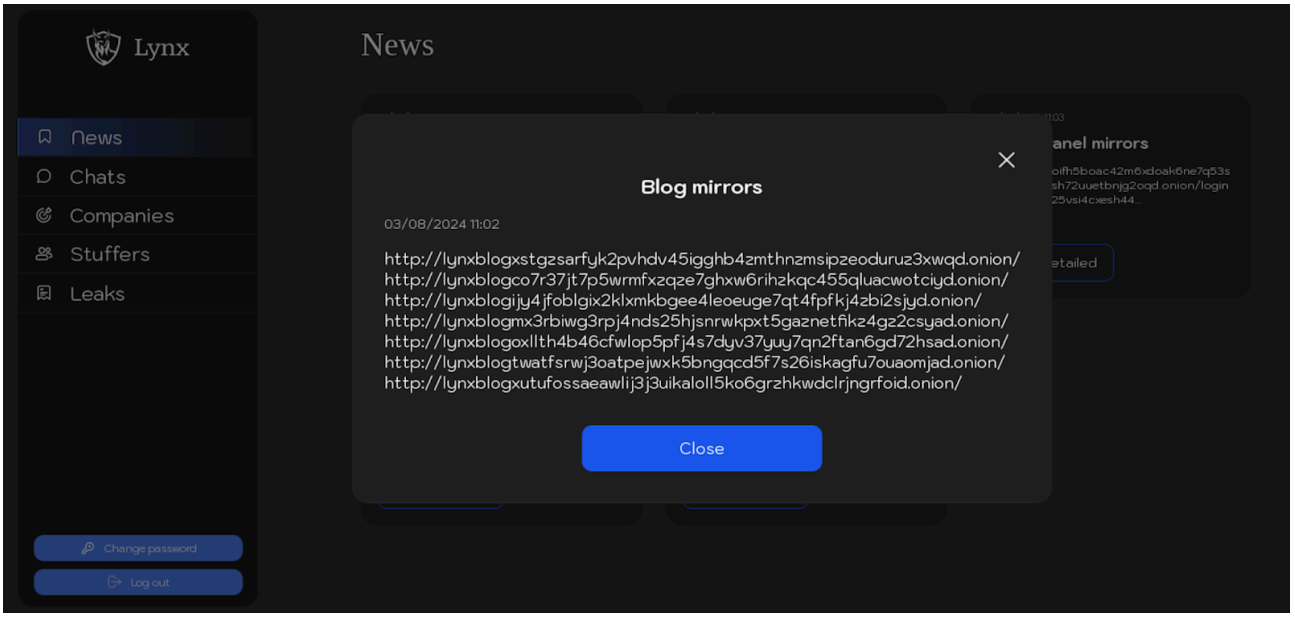


Figure 6. Screenshots of posts in the “News” section of Lynx ransomware panel, dated 3 August 2024.

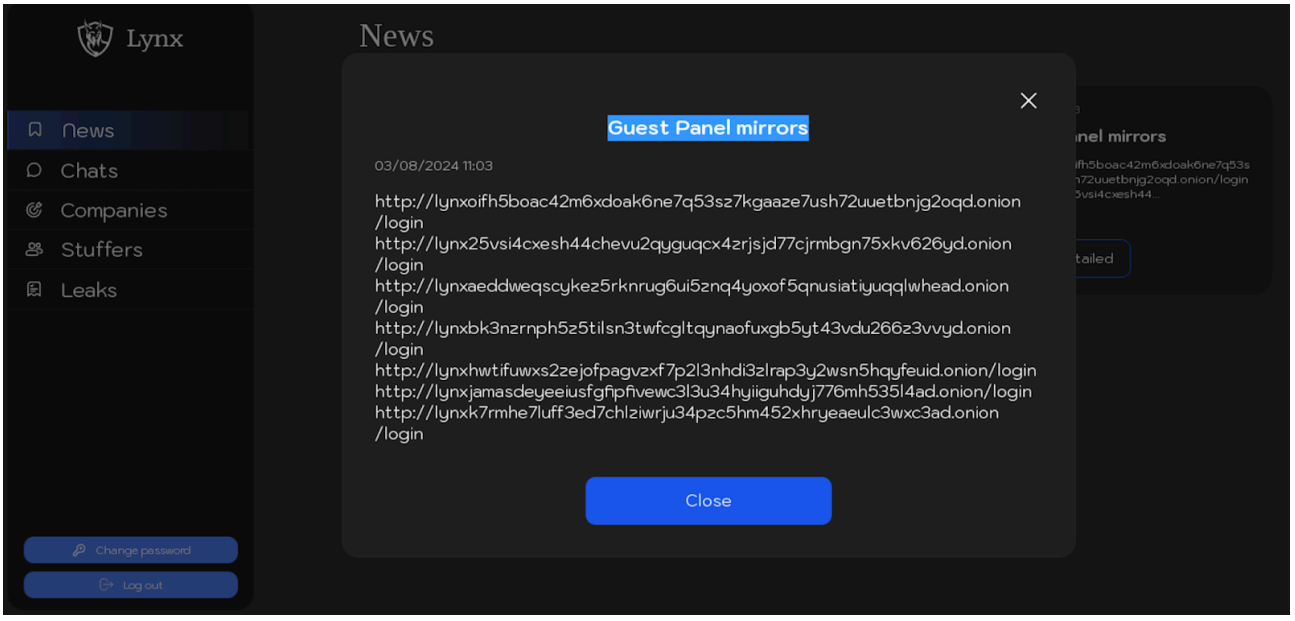


Figure 6. Screenshots of posts in the “News” section of Lynx ransomware panel, dated 3 August 2024.

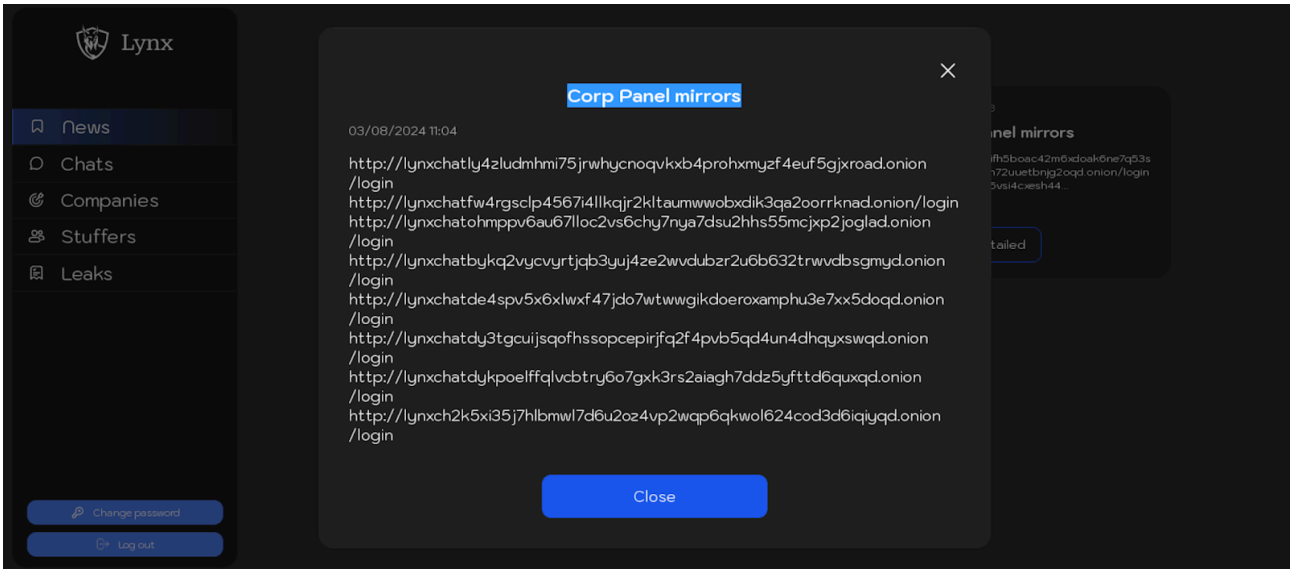


Figure 6. Screenshots of posts in the “News” section of Lynx ransomware panel, dated 3 August 2024.

The following text is extracted from published posts detailing the list mirrors of the Lynx ransomware group’s malicious infrastructure:

Admin panel mirrors:

```
http://lynxad2seqpyu52lr5v7il4idasv23535a46s4bj65b3v7t5y6u5daqd.onion/login
http://lynx2m7xz73zpmlm5nddbokk6a55fh2nzjq2r5nk2hbdbk74iddqfiqd.onion/login
http://lynxcwuhva6qzlnj3m3qrcl6bgvnxpixg5vsikf53vutdf3ijuv2pxyd.onion/login
http://lynxcyys7c2np3b3er2wo6sufwoonmh6i3nykv53pst336c3ml4ycjqd.onion/login
http://lynxdehvlvrrtnhtpuy6bhrxffzvl5j7y7p3zl553slzq44lcb2jzkyd.onion/login
```

```
http://lynxikczcyposxfz5a7hxbqxilsrtx7zdzwmhk5wcb5qoatbv2suizid.onion/login
http://lynxroggpujfxy7xnlrz3yknphqgk4k5dy4rhaldgz2hpxyyy3ncuvad.onion/login
```

Blog mirrors:

```
http://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion/
http://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd.onion/
http://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion/
http://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad.onion/
http://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion/
http://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion/
http://lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid.onion/
```

Guest panel mirrors:

```
http://lynxoifh5boac42m6xdoak6ne7q53sz7kgaaze7ush72uuetbnjg2oqd.onion/login
http://lynx25vsi4cxesh44chevu2qyguqcx4zrjsjd77cjrmbgn75xkv626yd.onion/login
http://lynxaeddweqscykez5rknrug6ui5znq4yoxof5qnusiatiyuqqlwhead.onion/login
http://lynxbk3nzrnph5z5tilsn3twfcgltqynaofuxgb5yt43vdu266z3vvyd.onion/login
http://lynxhwtifuwxs2zejofpagvzxf7p2l3nhdi3zlrap3y2wsn5hqyfeuid.onion/login
http://lynxjamasdeyeeiusfgfipfivewc3l3u34hyiiguhdyj776mh535l4ad.onion/login
http://lynxk7rmhe7luff3ed7chlziwrju34pzc5hm452xhryeaeulc3wxc3ad.onion/login
```

Corp mirrors:

```
http://lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion/login
http://lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion/login
http://lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login
http://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login
http://lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd.onion/login
http://lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd.onion/login
http://lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd.onion/login
http://lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd.onion/login
```

Below is a screenshot from the “News” section, highlighting a post about new features introduced to the Lynx ransomware’s locker and affiliate panel. Updates include enhancements to encryption modes and the addition of a non-onion domain for the company chat, allowing access through standard web browsers.

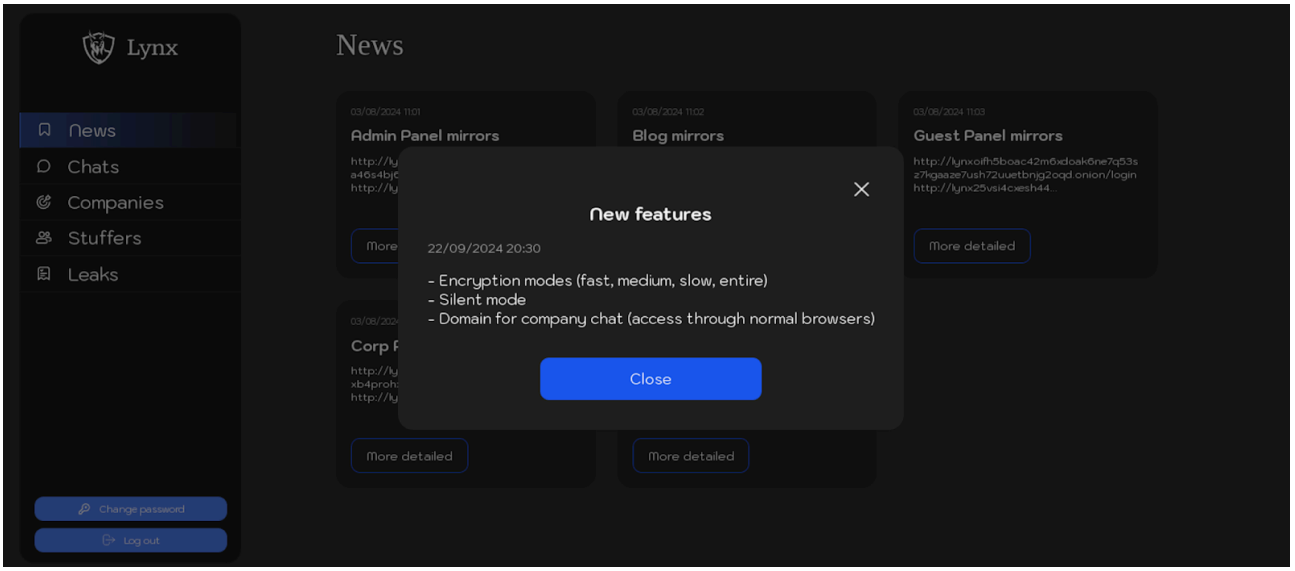


Figure 7. Screenshot of a post in the “News” section of Lynx ransomware panel, dated 22 September 2024.

Text from the post:

– Encryption modes (fast, medium, slow, entire)
– Silent mode
– Domain for company chat (access through normal browsers)

Companies

The “Companies” section provides an interface for affiliates to manage victims. This includes creating victim profiles, configuring victim-specific information, and generating unique ransomware samples tailored to each victim.

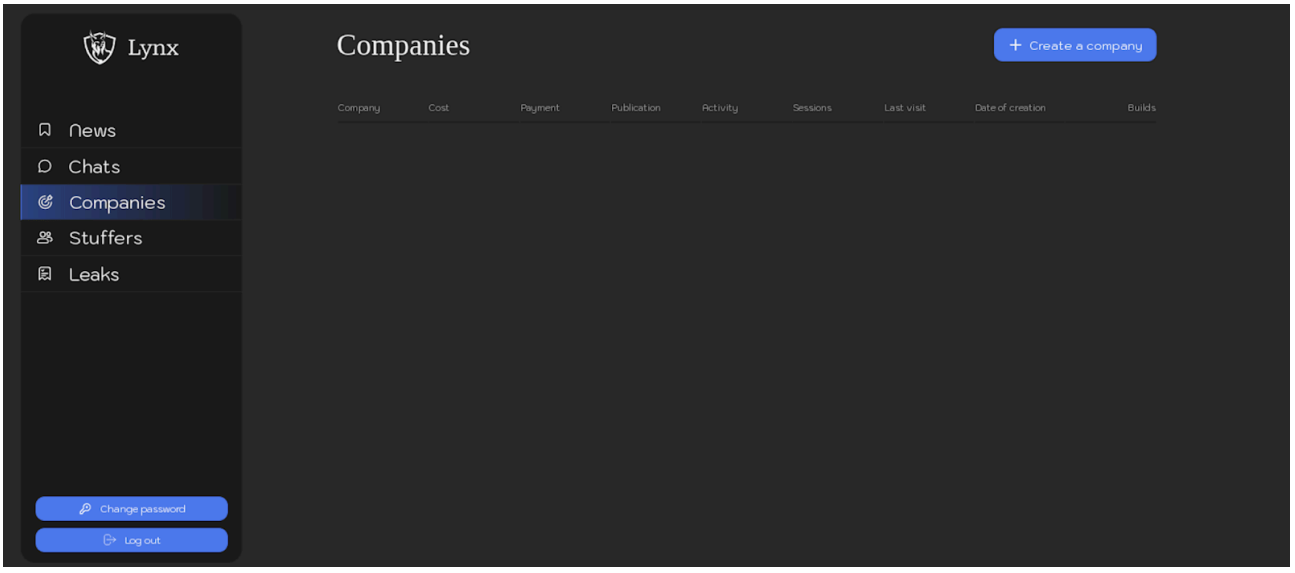


Figure 8. Screenshot of the “Companies” section of Lynx ransomware panel.

Intruder can configure following information about each victim:
– Company Name
– Link to zoominfo
– Country
– Number of Employees
– Income for the year in $
– The cost of the case $

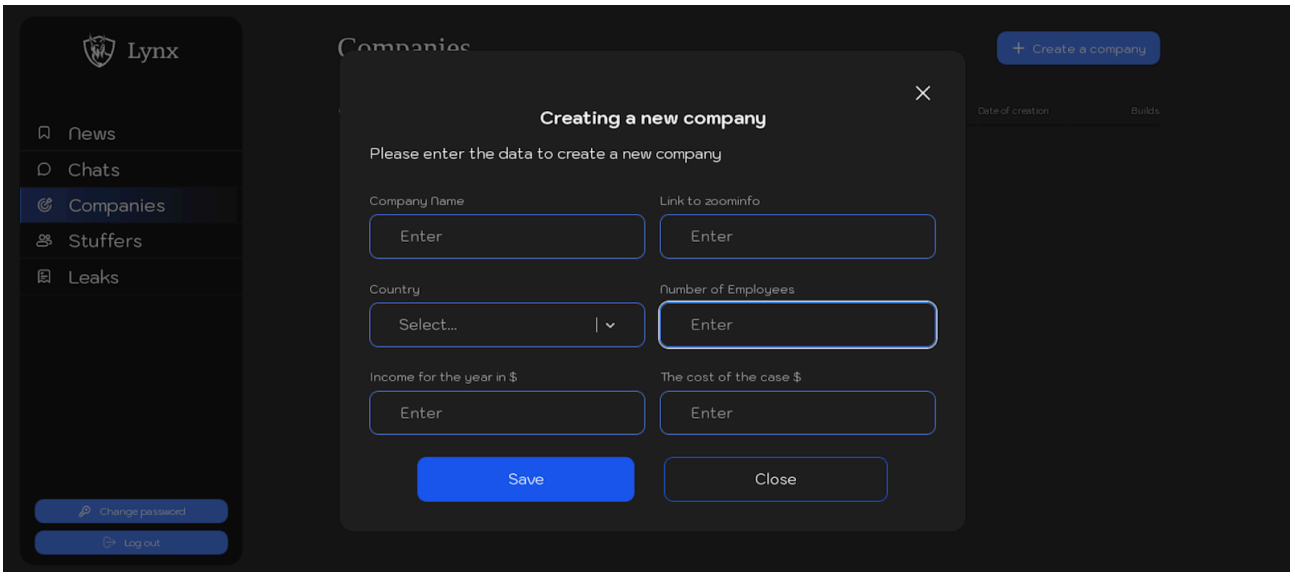


Figure 9. Screenshot of the interface for creating a new company in the “Companies” section of the Lynx ransomware panel.

Once a victim is created, a dedicated chat is automatically generated for that victim. This chat is accessible through the “Chats” section, streamlining communication and management for each case.

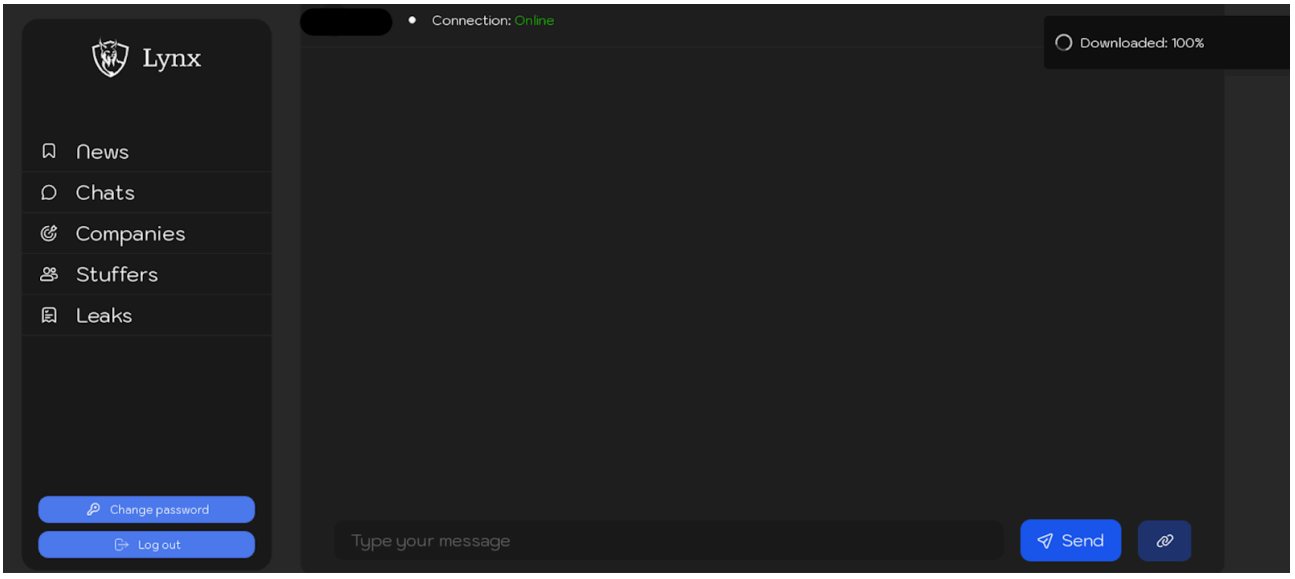


Figure 10. Screenshot of the chat with the victim in the “Companies” section of the Lynx ransomware panel.

The screenshots below display an already created victim, including brief details about the victim and available actions that can be performed for each company. These actions include downloading samples of Lynx ransomware for the victim, changing the password for chat access, banning negotiations with the company, adjusting the ransom amount, or deleting the chat for security purposes.

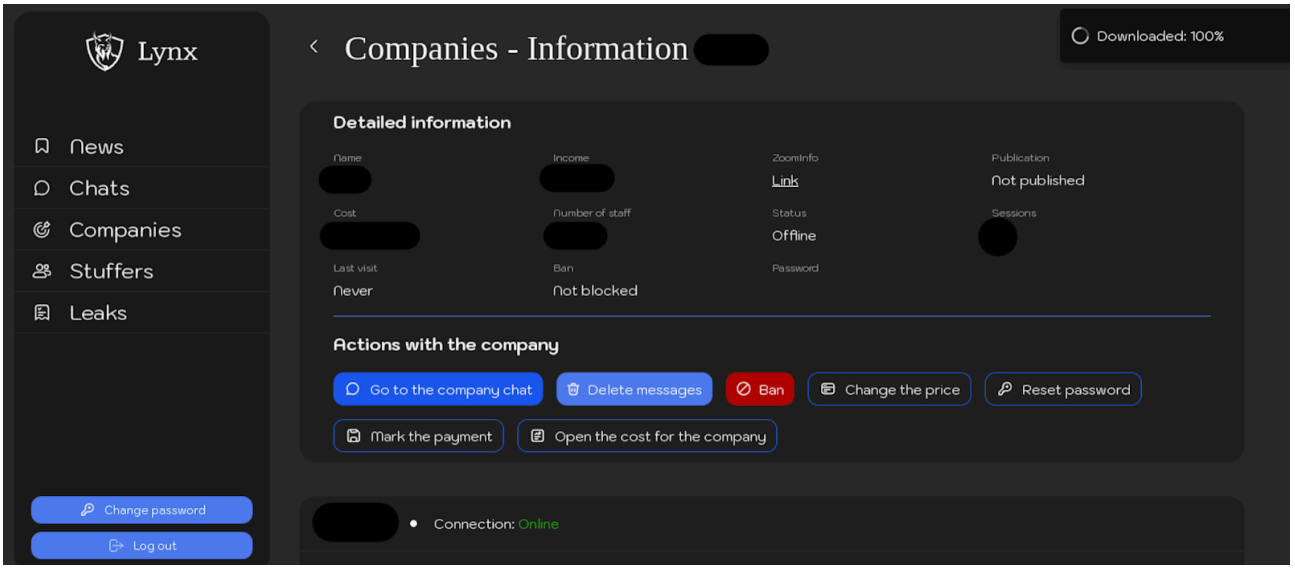


Figure 11. Screenshots of the interface displaying an already created company in the "Companies" section of the Lynx ransomware panel.

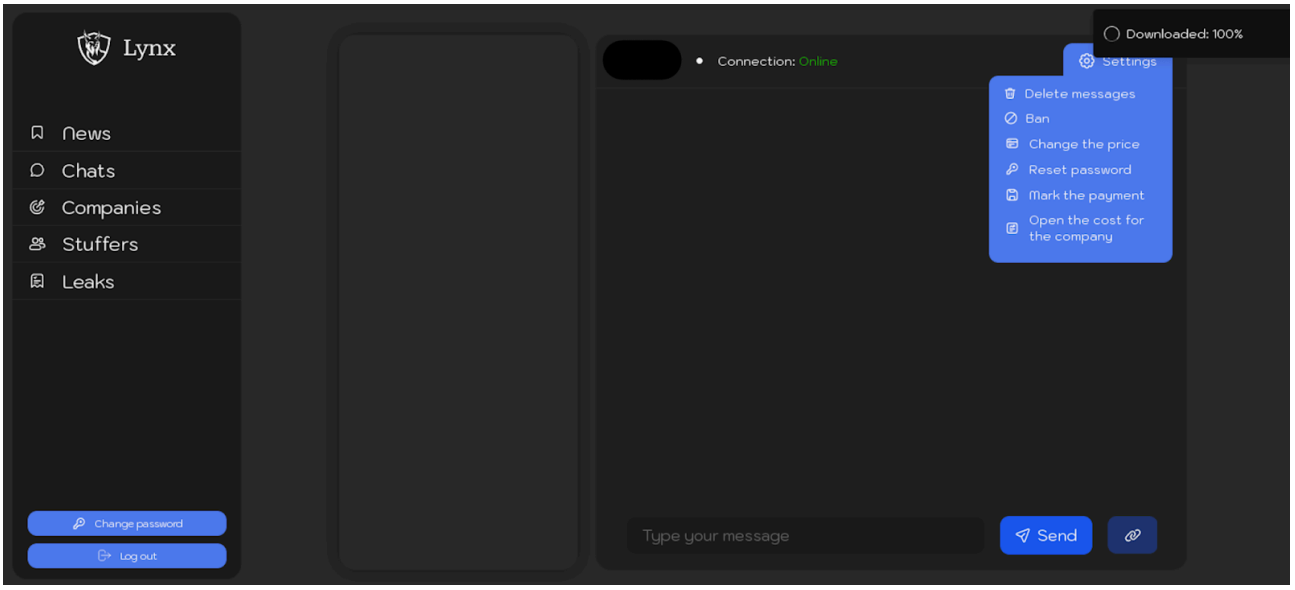


Figure 11. Screenshots of the interface displaying an already created company in the "Companies" section of the Lynx ransomware panel.

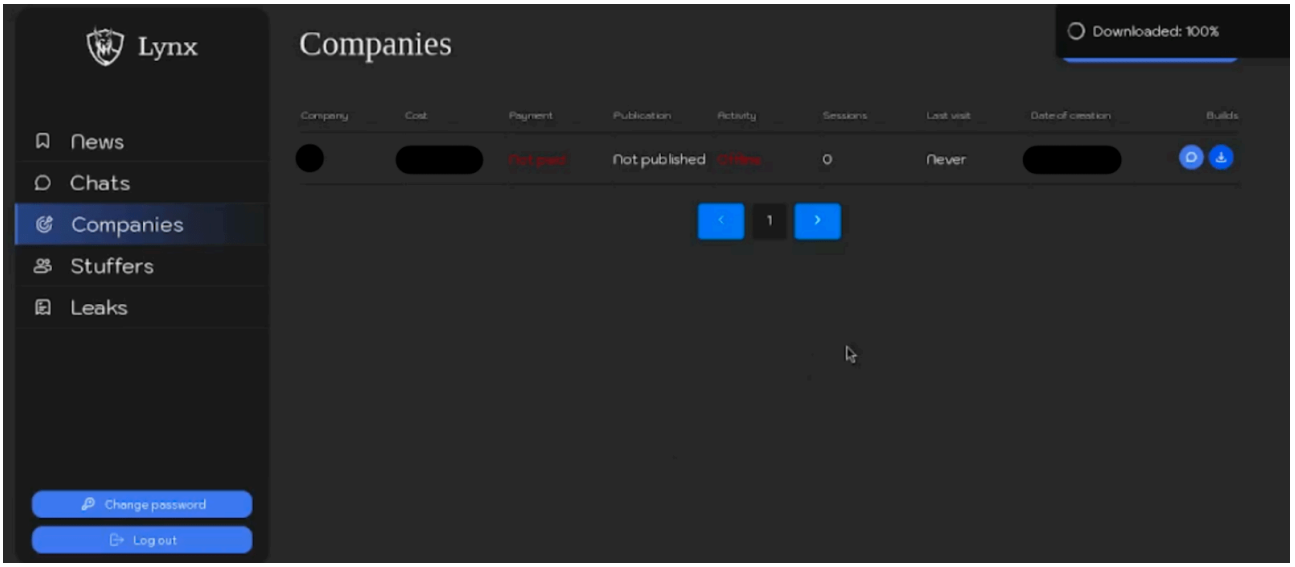


Figure 11. Screenshots of the interface displaying an already created company in the "Companies" section of the Lynx ransomware panel.

Affiliate download archive containing multiple binary builds for various architectures (x86, ARM, MIPS, PPC, ESXi, etc.). This allows affiliates to deploy the ransomware broadly across diverse systems in a victim's corporate network.

All-in-One Archive for Affiliates

Instead of targeting a single architecture, the Lynx ransomware group offers affiliates a complete bundle. Inside this archive, there are executables tailored for Linux x64, Linux ARM, MIPS, ESXi, and more. Affiliates can pick whichever version they need for any specific segment of the victim's network.

Comprehensive Architectural Coverage

Modern corporate networks are rarely homogeneous, they might include virtualized infrastructure (ESXi) and x86_64 servers running Linux or Windows. Having multiple versions at the ready boosts the ransomware's effectiveness, because it can be run on almost any system.

Straightforward Cross-Compilation

Thanks to Linux's versatile cross-compilation toolchains, attackers easily build different variants (e.g., linux-armv7, linux-mips, linux-s390x). These toolchains allow static and dynamic linking (musl vs. glibc) so the binaries can run smoothly in minimal or containerized environments.

Musl Binaries

Some binaries in the archive carry a -musl tag. These are linked against the musl C library, making them more portable to edge environments and containers that might not have the standard glibc libraries installed.

Maximizing Reach in Targeted Attacks

Even in a targeted attack, the affiliate benefits from having every possible version. Once they infiltrate a network, they can discover which architectures are present, like ESXi hosts, ARM-based systems, or IBM mainframes and deploy the matching binary without needing to recompile or fetch anything else.

List of samples in archive:

```
linux-arm64
linux-armv5-musl
linux-armv7
linux-esxi
linux-ppc64le
linux-x64
linux-arm64-musl
linux-armv6
linux-armv7a
linux-mips
linux-riscv64
linux-x86
linux-armv5
linux-armv6-musl
linux-armv7l-musl
linux-mipsel-lts
linux-s390x
windows
```

Chats

The “Chats” section provides information about the chats created for negotiations with victims.

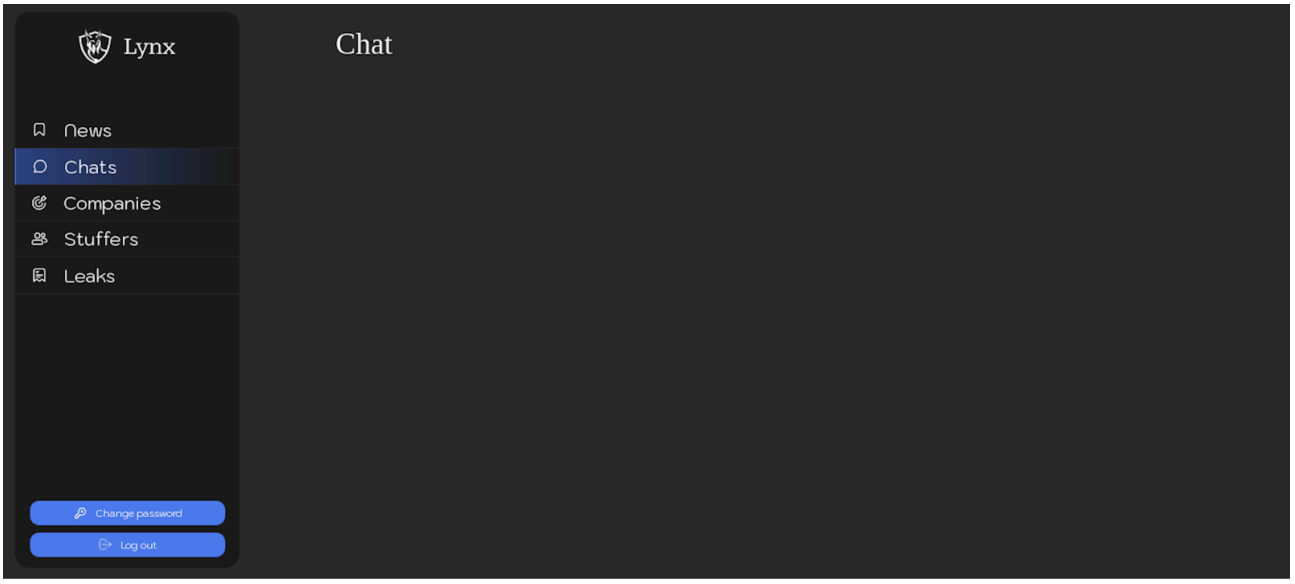


Figure 12. Screenshot of the “Chat” section of the Lynx ransomware panel.

Stuffers

The “Stuffers” section offers affiliates a streamlined interface to manage their sub-affiliates or team members for collaborative efforts. Affiliates can easily add a new “stuffer” by assigning a unique login and password, enabling secure and individualized access for each team member.

Below are screenshots providing an overview of how it appears in the affiliate panel:

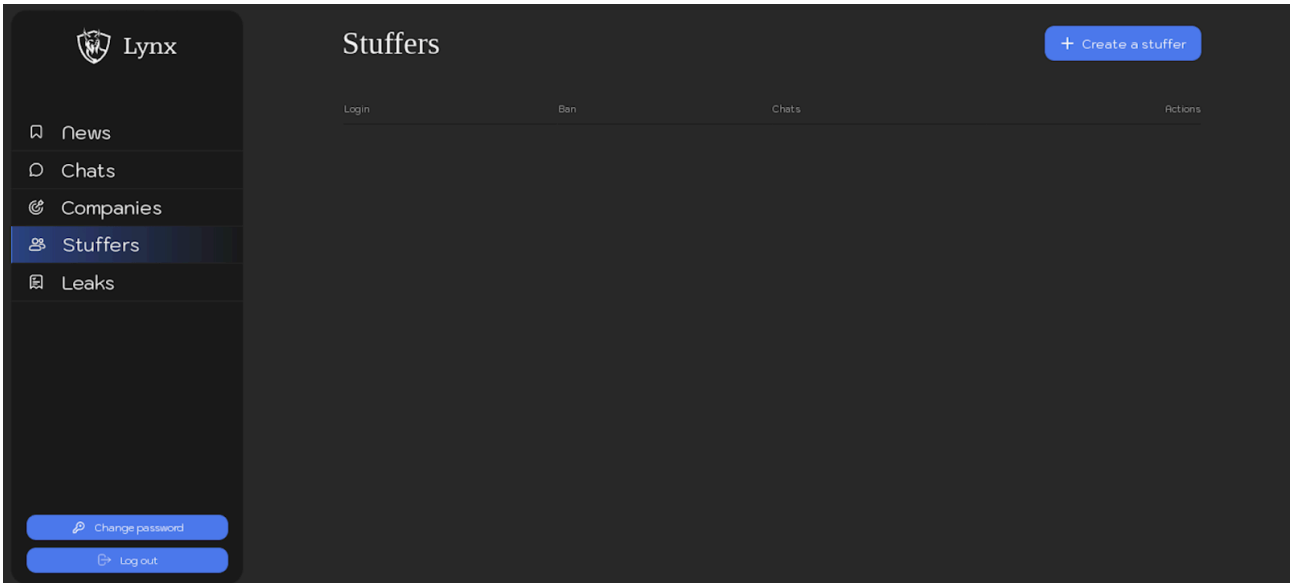


Figure 13. Screenshots of the interface for creating a stuffer or sub-affiliate in the "Stuffer" section of the Lynx ransomware panel.

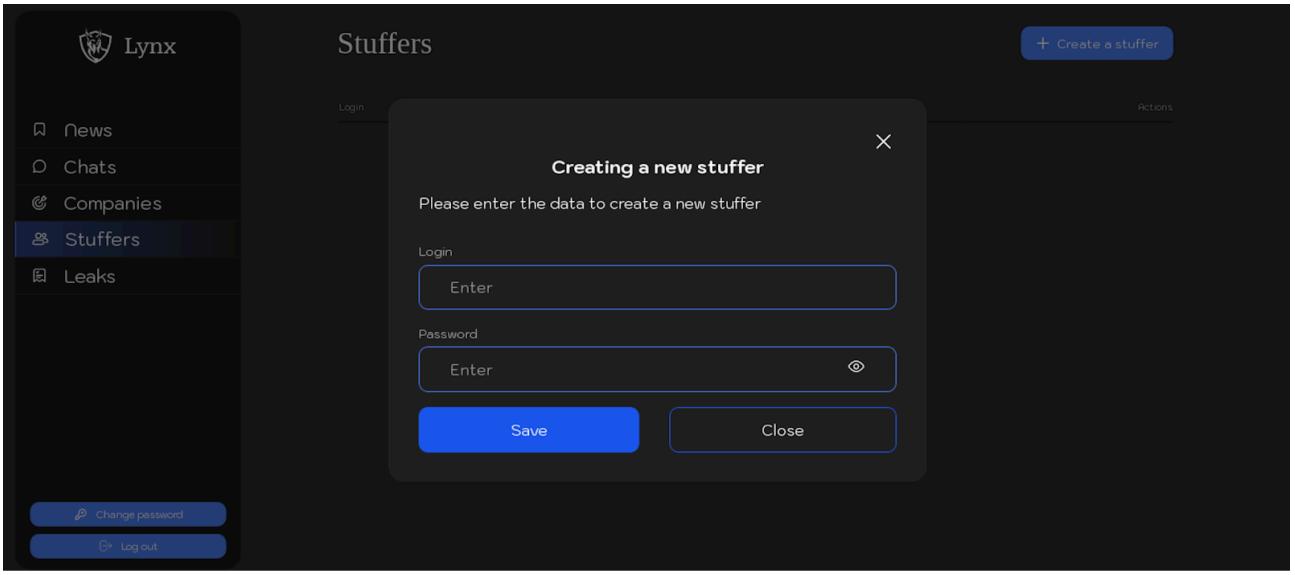


Figure 13. Screenshots of the interface for creating a stuffer or sub-affiliate in the "Stuffer" section of the Lynx ransomware panel.

Leaks

The “Leaks” section allows affiliates to create and manage publications about companies that have been attacked but have not paid the ransom. Affiliates can schedule these publications, customize the attacked company’s logo, select a company from the list in the “Companies” section, specify a publication time, choose a publication category, add a description of the leak, generate a password, and attach relevant files.

Below are screenshots showcasing the affiliate panel interface for creating and scheduling publications:

Figure 14. Screenshots of the interface for scheduling a publication in the "Leaks" section of the Lynx ransomware panel.

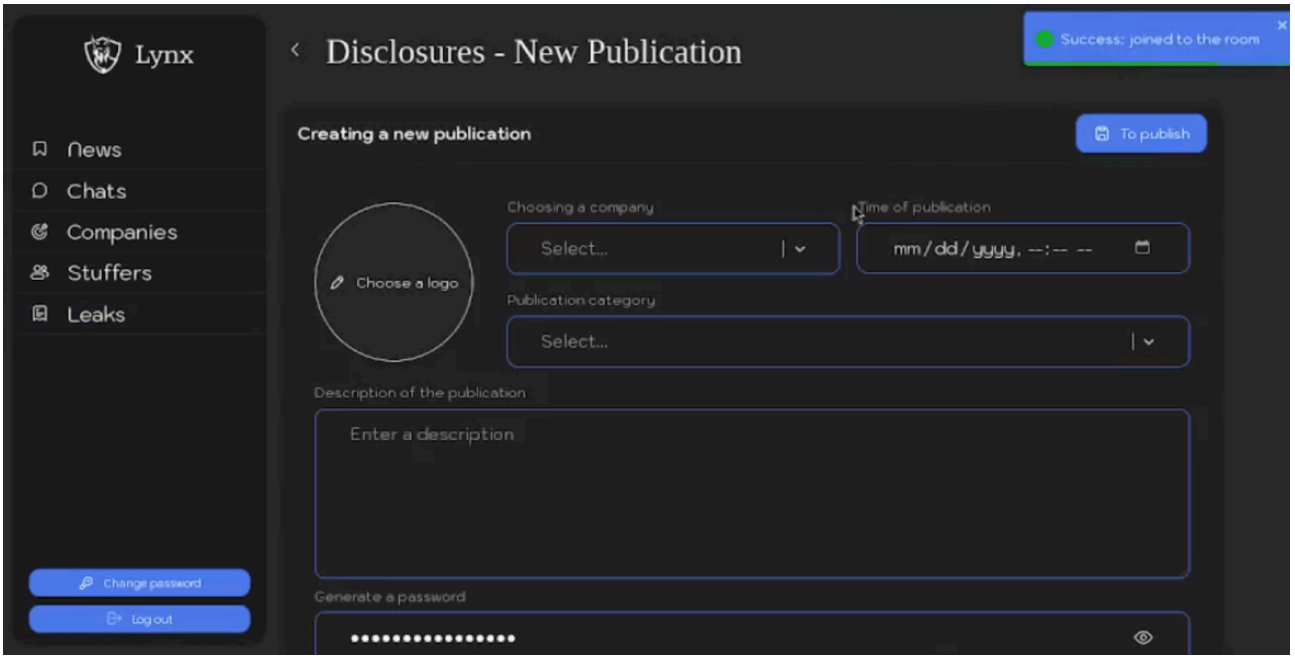


Figure 14. Screenshots of the interface for scheduling a publication in the "Leaks" section of the Lynx ransomware panel.

Technical Information

The ransomware is available in both Windows and Linux versions, though the latter has yet to be reported in the wild. Its features are relatively standard for ransomware, displaying typical behavior seen in other threats of its kind. The file extension used is ".LYNX", which is appended to encrypted files.

Overall summary of the command line options of both Windows and Linux versions:

Options	**Description**	**Windows**	**Linux**
file	Encrypt only specified file(s)	v	v
dir	Encrypt only specified directory(ies)	v	v
mode	slow(25%), medium(15%), fast(5%), entire(100%)	v	v
esxi	Force stop all ESXi VMs		v
delay	Delay encryption for N minute(s)		v
fork	Fork process		v
motd	Setup ransom note in message of the day		v
verbose	Print logging messages	v	v
help	Print help menu	v	v
silent	Enable silent encryption (no extension and notes will be added)	v	
stop-processes	Stop processes via RestartManager	v	
encrypt-network	Encrypt network shares	v	
load-drives	Load hidden drives (will corrupt boot loader)	v	
hide-cmd	Hide console window	v	
no-background	Don't change background image	v	
no-print	Don't print note on printers	v	
kill	Kill processes/services	v	
safe-mode	Enter safe-mode	v	

Windows

When comparing our sample to those reported in October 2024, a key difference is that Lynx ransomware has introduced a **"mode" option** – fast/medium/slow/entire, enabling the attacker to choose the percentage of a file to encrypt, allowing them to decide the trade-off between speed and the amount of data encrypted. In contrast, earlier

versions of Lynx have only 1 default option which is simply encrypting 1MB for every 6MB (this is actually ~16% which is the “medium” mode).

Figure 15. Command-line options of Windows version of Lynx ransomware

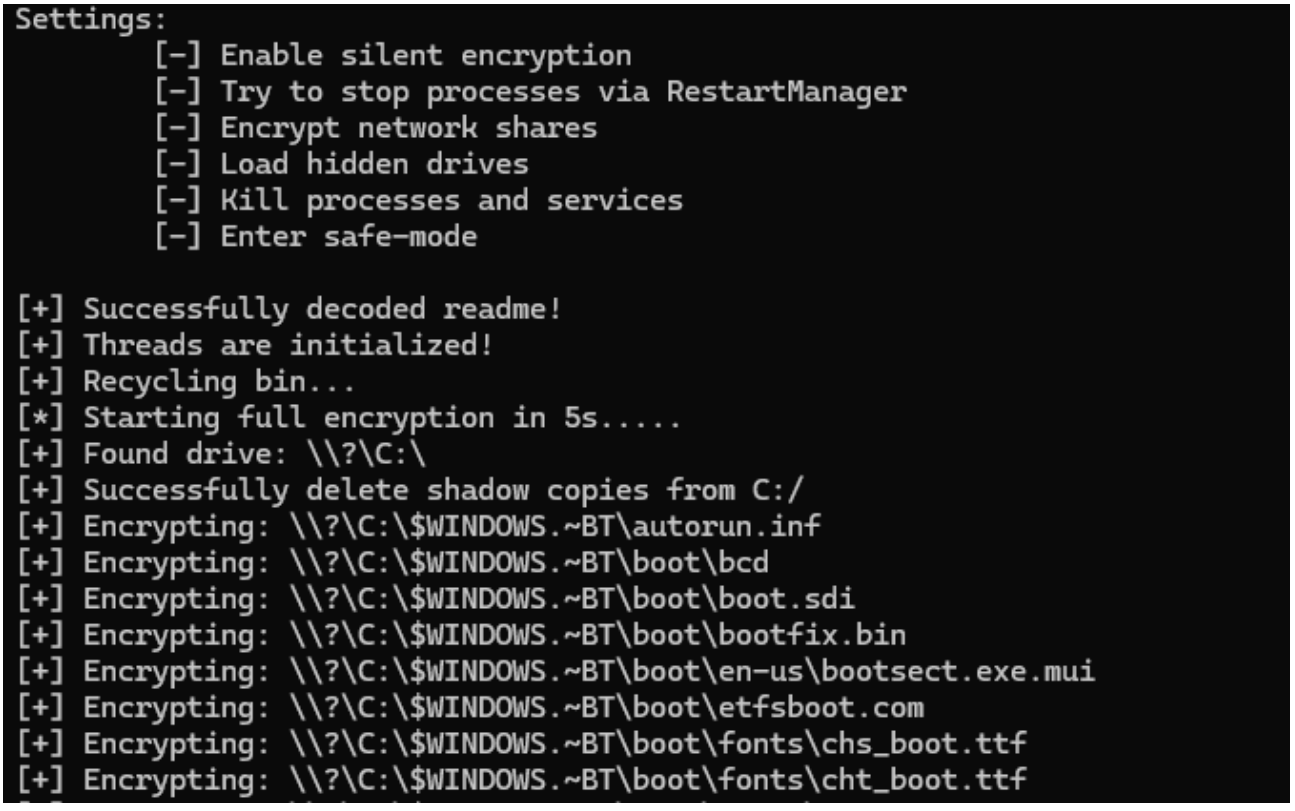


Figure 16. Verbose logs during encryption

Ransom note is base64 encoded and embedded in the binary. It is dropped in every encrypted directory.

```
Your data is stolen and encrypted.
Download TOR Browser to contact with us.

ID
 ~ [redacted]

Chat site:
 ~ TOR Network: http://lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion/login
 ~ TOR Mirror #1: http://lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion/login
 ~ TOR Mirror #2: http://lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login
 ~ TOR Mirror #3: http://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login
 ~ TOR Mirror #4: http://lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd.onion/login
 ~ TOR Mirror #5: http://lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd.onion/login
 ~ TOR Mirror #6: http://lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd.onion/login
 ~ Mirror #7: http://lynxchat.net/login

Our blog:
 ~ TOR Network: http://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion/
 ~ TOR Mirror #1: http://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd.onion/
 ~ TOR Mirror #2: http://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion/
 ~ TOR Mirror #3: http://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad.onion/
 ~ TOR Mirror #4: http://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion/
 ~ TOR Mirror #5: http://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion/
 ~ TOR Mirror #6: http://lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid.onion/
 ~ Mirror #7: http://lynxblog.net/
```

Figure 17. Lynx ransom note

Environment preparation

To ensure a smooth encryption process, it does a few things

- When determined to have insufficient access to the files to be encrypted, it attempts to escalate privileges. It enables “SeTakeOwnershipPrivilege” for the current process access token, and takes ownership of the file object. It is then used to change the Discretionary Access Control List (DACL) of the file object.
- Uses Windows Restart Manager to terminate processes that are currently using the targeted resources.
- When the option “load-drives” is enabled, it enumerates all volumes, and the system will attempt to mount any unmounted volumes and assign it a drive letter.

Whitelisted extensions

```
.exe, .dll, .msi, .lynx
```

Blacklisted services and processes

```
Services: "sql", "veeam", "backup", "exchange"
Processes: "sql", "veeam", "backup","exchange", "java", "notepad"
```

Encryption Scheme

The ransomware utilizes a multi-threaded approach to speed up the encryption process by creating a number of threads equal to four times the number of CPU cores in the system. It uses the Windows I/O Completion Port mechanism to efficiently manage asynchronous I/O operations, allowing threads to handle disk read/write tasks without blocking the encryption process.

The ransomware employs the combination of Curve25519 Donna and AES-128 in CTR mode for file encryption. Lastly, it then renames the file with a .LYNX extension.

Post-encryption

It performs the usual post-encryption steps, changing the desktop wallpaper of the compromised machine to a ransom note. It will also attempt to print the ransom note on connected printers. It enumerates all the local printers, excluding “Microsoft Print to PDF” and “Microsoft XPS Document Writer”, and proceeds to send the ransomware note as a print job to them.

Figure 18. Ransom note set as wallpaper

Delete Shadow Copies

The ransomware attempts to delete shadow copies by resizing the maximum amount of volume shadow copy storage space. This is done via DeviceIoControl() using the IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE (0x53C028) control code. By setting the maximum space to 1 byte, it effectively forces Windows to delete all existing volume snapshots.

```
memset(&diffAreaSize, 0, 0x10);
diffAreaSize.MaximumSpace = 1i64;          // 1 byte of storage
hVolume = CreateFileW(volPath, 0x12019Fu, 3u, 0, 3u, 0x80u, 0);
hObject = hVolume;
if ( hVolume == -1 )
{
  if ( g_opt_verbose )
  {
    LastError = GetLastError();
    FormatMessageW(0x1200u, 0, LastError, 0x409u, Buffer, 0x100u, 0);
    my_sprintf2(L"[-] Couldn't delete shadow copies from %c:/: %s\n", v2, Buffer);
  }
}
else
{
  if ( DeviceIoControl(
         hVolume,
         IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE,
         &diffAreaSize,
         0x18u,
         0,
         0,
         &BytesReturned,
         0) )
  {
```

Figure 19. Code snippet of deleting shadow copies

Linux

The Linux version of the ransomware is much simpler and linux versions of ransomware are usually developed to target ESXI systems. To start encryption, one has to specify either a file or directory for the linux version.

The encryption scheme is the same as Windows. However, compared to the Windows version which uses 4x the cores, the Linux version spawns threads equal to 2x the number of cores to process files.

Ransom notes are dropped in every directory and could also be set up as a message of the day (MOTD).

```
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Your data is stolen and encrypted.
Download TOR Browser to contact with us.

ID
 ~ [redacted]

Chat site:
 ~ TOR Network: http://lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion/login
 ~ TOR Mirror #1: http://lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion/login
 ~ TOR Mirror #2: http://lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login
 ~ TOR Mirror #3: http://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login
 ~ TOR Mirror #4: http://lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd.onion/login
 ~ TOR Mirror #5: http://lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd.onion/login
 ~ TOR Mirror #6: http://lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd.onion/login
 ~ Mirror #7: http://lynxchat.net/login
```

Figure 20. Ransom note set as MOTD

```
Usage: ./lynx-ransomware <ARGUMENTS>
Arguments:
        --file <filePath>                                Encrypt only specified file(s)
                --file /test/test.txt
                --file /test/test.txt,/test/test2.txt
        --dir <dirPath>                                  Encrypt only specified directory(ies)
                --dir /test/
                --dir /test/,/test2/
        --mode <mode>                                    Encryption mode
                --mode fast                              Encrypt 5% from entire file
                --mode medium                            Encrypt 15% from entire file (default)
                --mode slow                              Encrypt 25% from entire file
                --mode entire                            Encrypt 100% from entire file
        --help                                           Print this message
        --verbose                                        Enable verbosity
        --esxi                                           Force stop all ESXi VMs
        --delay <N>                                      Delay encryption for N minute(s)
        --fork                                           Fork process
        --motd                                           Update "Message of the day"
```

Figure 21. Command-line options of linux version of Lynx ransomware

Stopping ESXI and removing snapshots

It writes the following command in a file named "**kill**" and proceeds to execute the file. It forcefully terminates all the virtual machines on the ESXi host using their World IDs.

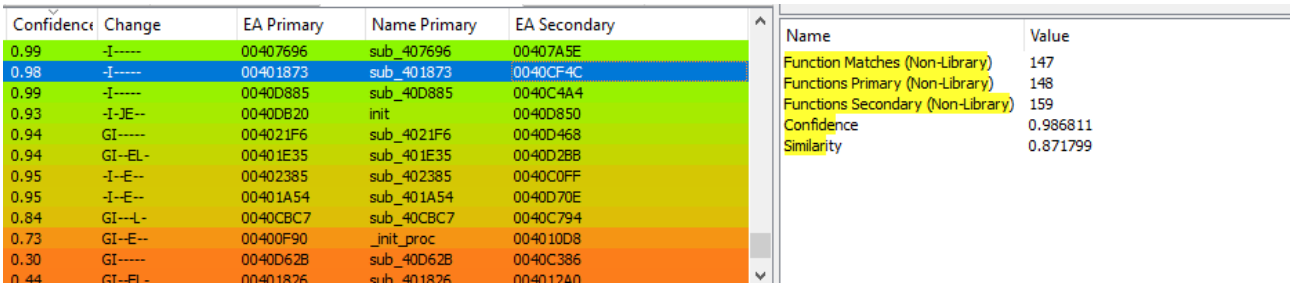
```
for i in $(esxcli vm process list | grep 'World' | grep -Eo '[0-9]{1,8}'); do esxcli vm process kill
```

To remove virtual machine snapshots, it writes the following command in a file named "**delete**" and proceeds to execute the file.

```
for i in $(vim-cmd vmsvc/getallvms | awk '{print $1}' | grep -Eo '[0-9]{1,8}'); do vim-cmd vmsvc/sna
```

Comparison with INC

It has been previously reported that the Windows version of the Lynx ransomware closely resembles INC ransomware, suggesting that they may have purchased the source code of INC ransomware. The features of the analysed Linux version of Lynx exhibited strong similarities as well. We decided to compare it with the Linux ESXI version of INC ransomware (SHA256: c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef) using BinDiff. There were a total of 147 non-library function matches between the 2 samples, making roughly > 91% overlapping functions. The overall similarity stood at 87% with a 98% confidence.



Confidence	Change	EA Primary	Name Primary	EA Secondary
0.99	-I-----	00407696	sub_407696	00407A5E
0.98	-I-----	00401873	sub_401873	0040CF4C
0.99	-I-----	0040D885	sub_40D885	0040C4A4
0.93	-I-JE--	0040DB20	init	0040D850
0.94	GI-----	004021F6	sub_4021F6	0040D468
0.94	GI--EL-	00401E35	sub_401E35	0040D2BB
0.95	-I--E--	00402385	sub_402385	0040C0FF
0.95	-I--E--	00401A54	sub_401A54	0040D70E
0.84	GI---L-	0040CBC7	sub_40CBC7	0040C794
0.73	GI--E--	00400F90	_init_proc	004010D8
0.30	GI-----	0040D62B	sub_40D62B	0040C386
0.44	GI--EL-	00401826	sub_401826	004012A0

Name	Value
Function Matches (Non-Library)	147
Functions Primary (Non-Library)	148
Functions Secondary (Non-Library)	159
Confidence	0.986811
Similarity	0.871799

Figure 22. BinDiff comparison of Lynx sample and INC sample

Conclusion

Lynx has emerged as a formidable RaaS operator by combining a versatile arsenal of ransomware builds, a structured affiliate ecosystem, and systematic extortion tactics. Their panel's features: from victim management to scheduled leak publications, demonstrate an industrial-scale approach to cybercrime.

Notably, in-depth analysis revealed a significant code overlap with INC ransomware (over 90% of the Linux ESXi variant functions match when compared via BinDiff). This strongly indicates that Lynx may have purchased or adapted the INC ransomware source code, enabling them to build upon existing malware capabilities. For organizations, this underscores the importance of continually updating incident response procedures, investing in real-time threat intelligence, and fostering a security-first culture.

As RaaS groups like Lynx push the boundaries of cyber extortion, only a proactive and adaptive defensive strategy will safeguard critical data and maintain business resilience.

Recommendations

Although ransomware operators often target critical sectors, any organization can become a victim. The recent growth of affiliate programs, where established groups equip new partners with advanced tools, amplifies these threats. Below are essential steps to protect mission-critical operations and data:

- **Implement MFA and Credential-Based Access:** Use multi-factor authentication wherever possible, especially for privileged or high-risk accounts. This adds a second layer of validation, making unauthorized

entry more difficult.

- **Deploy Advanced EDR Solutions:** Behavioral detection capabilities help identify ransomware indicators on managed endpoints, enabling quicker response. This proactive approach allows you to investigate and remediate both known and emerging threats.
- **Regularly Schedule Backups:** Backups serve as a safety net if files are encrypted. Store them offline or on separate networks to protect against lateral movement by attackers.
- **AI-Based Detection and Analytics:** Employ platforms that can analyze and quarantine suspicious files before they execute. Solutions like Group-IB's Managed XDR with Threat Intelligence provide:
    - Insights into TTPs used by ransomware groups, enabling faster security pivots.
    - Multi-layered security (endpoint, email, web, network) with automated detection and response.
- **Prioritize Software Updates:** Unpatched vulnerabilities are prime targets for initial compromise. Establish a routine review process for applying critical updates.
- **Security Awareness Programs:** Humans are often the weakest link. Conduct regular phishing drills, and teach employees to report suspicious emails or incidents promptly.
- **Ongoing Technical Audits:** Annual or biannual checks of infrastructure can uncover hidden weaknesses. Monitor digital hygiene and ensure strict access control and configuration management.
- **Never Pay the Ransom:** Paying attackers only encourages further extortion. Contact experienced IR teams as soon as possible to manage containment, eradication, and recovery efforts.

MITRE ATT&CK

T1059 (Windows); T1059.004 (Linux/Unix Shell) Command and Scripting Interpreter (Windows/ Linux)	The ransomware supports command-line options on both Windows and Linux, including custom parameters (e.g., –mode, –esxi), enabling affiliates to automate encryption and process termination.
T1134 Access Token Manipulation	Lynx ransomware attempts to escalate privileges. It enables "SeTakeOwnershipPrivilege" for the current process access token, and takes ownership of the file object. It is then used to change the Discretionary Access Control List (DACL) of the file object.
T1490 Inhibit System Recovery	Lynx attempts to delete or resize Volume Shadow Copies (Windows) and removes ESXi snapshots, hindering standard backup and recovery procedures.
T1005 Data from Local System	Files identified for encryption are enumerated locally or on mounted drives/volumes (including hidden volumes loaded with load-drives).
T1486 Data encrypted for impact	Lynx's core functionality is encrypting files (Windows/Linux). Ransom demands are communicated via ransom notes, changed wallpapers, or printed notes.

Public Available Indicators of Compromise (IOCs)

Filename	SHA256
svhost.exe.bin	80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441
Frantic_Setup.exe	80fd105d0685b85c1be5d5d3af63608d2ec91b186d4c591416934fe454770ca1
build.exe	3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e
	97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0
windows.exe	468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
	432f549e9a2a76237133e9fe9b11fbb3d1a7e09904db5ccace29918e948529c6
win.exe	4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412
	9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896
dd.exe	31de5a766dca4eaae7b69f807ec06ae14d2ac48100e06a30e17cc9acccfd5193
	589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a23
windows.exe	d5ca3e0e25d768769e4afda209aca1f563768dae79571a38e3070428f8adf031
win.exe	85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf5683
	b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee
win.bin	ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49
11.exe	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
win.ex	eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
	82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513
	c02b014d88da4319e9c9f9d1da23a743a61ea88be1a389fd6477044a53813c72

Network Indicators

hxxp://lynxblog[.]net/
hxxp://lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion
hxxp://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd[.]onion
hxxp://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd[.]onion
hxxp://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad[.]onion
hxxp://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad[.]onion

hxxp://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad[.]onion
hxxp://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion
hxxp://lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid[.]onion
hxxp://lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd[.]onion
hxxp://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd[.]onion
hxxp://lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd[.]onion
hxxp://lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd[.]onion
hxxp://lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd[.]onion
hxxp://lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad[.]onion
hxxp://lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad[.]onion
hxxp://lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad[.]onion
hxxp://lynxad2seqpyu52lr5v7il4idasv23535a46s4bj65b3v7t5y6u5daqd[.]onion
hxxp://lynx2m7xz73zpmlm5nddbokk6a55fh2nzjq2r5nk2hbdbk74iddqfiqd[.]onion
hxxp://lynxcwuhva6qzlnj3m3qrcl6bgvnxpixg5vsikf53vutdf3ijuv2pxyd[.]onion
hxxp://lynxcyys7c2np3b3er2wo6sufwoonmh6i3nykv53pst336c3ml4ycjqd[.]onion
hxxp://lynxdehvlvrrtnhtpuy6bhrxffzvl5j7y7p3zl553slzq44lcb2jzkyd[.]onion
hxxp://lynxikczcyposxfz5a7hxbqxilsrtx7zdzwmhk5wcb5qoatbv2suizid[.]onion
hxxp://lynxroggpujfxy7xnlrz3yknphqgk4k5dy4rhaldgz2hpxyyy3ncuvad[.]onion
hxxp://lynxoifh5boac42m6xdoak6ne7q53sz7kgaaze7ush72uuetbnjg2oqd[.]onion
hxxp://lynx25vsi4cxesh44chevu2qyguqcx4zrjsjd77cjrmbgn75xkv626yd[.]onion
hxxp://lynxaeddweqscykez5rknrug6ui5znq4yoxof5qnusiatiyuqqlwhead[.]onion
hxxp://lynxbk3nzrnph5z5tilsn3twfcgltqynaofuxgb5yt43vdu266z3vvyd[.]onion
hxxp://lynxhwtifuwxs2zejofpagvzxf7p2l3nhdi3zlrap3y2wsn5hqyfeuid[.]onion
hxxp://lynxjamasdeyeeiusfgfipfivewc3l3u34hyiiguhdyj776mh535l4ad[.]onion
hxxp://lynxk7rmhe7luff3ed7chlziwrju34pzc5hm452xhryeaeulc3wxc3ad[.]onion

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