Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 12 - 18, 2024

Report Summary:

- **New Threat Detection Added** – 2 (UAC-0125 Rogue RDP Cookbox Malware and Citrix Session Recording RCE (CVE-2024-8069))
- **New Threat Protections - 249**

The following threats were added to Crystal Eye XDR this week:

1. UAC-0125 Rogue RDP Cookbox Malware

Cookbox is designed to compromise and extract sensitive information from affected systems. It starts with a phishing email which includes attachments containing configuration files for setting up Remote Desktop Protocol (RDP) sessions (".rdp" files). Launching these files initiated an outgoing RDP connection to the attacker's server. However, the configuration of the RDP files allowed access to local resources such as disks, network shares, printers, COM ports, audio devices, and the clipboard during the connection. This setup not only exposed local resources but also potentially enabled the execution of third-party programs or scripts on the victim's computer.

Threats Protected: 118
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1204.002	Malicious File
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1055	Process Injection
Credential Access	T1056.001	Keylogging
Discovery	T1082	System Information Discovery
Collection	T1113	Screen Capture
Command-and-Control	T1071.001	Web Protocols

2. Citrix Session Recording RCE (CVE-2024-8069)

A critical privilege escalation vulnerability has been identified in Citrix's Virtual Apps and Desktops solution. This flaw allows authenticated users to gain SYSTEM-level privileges on the server hosting the virtual applications and desktops. Exploiting this vulnerability enables attackers to impersonate any user, including administrators, and monitor or manipulate user activities. The centralised nature of this system amplifies the potential impact, making it imperative for organisations to apply necessary patches and security measures promptly.

Threats Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Reject	Drop
Connectivity	Disabled	Disabled
OT	Disabled	Disabled

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1078	Valid Accounts
Privilege Escalation	T1068	Exploitation for Privilege Escalation

Known exploited vulnerabilities (Week 2 November 2024):

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-november-2024/525

Updated Malware Signatures (Week 2 November 2024)

Threat	Description
Qakbot	A malware designed to acquire valuable data such as banking credentials and is also capable of stealing FTP credentials and spreading across a network by utilising SMB.
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Groups and Attack Coverage:

Name of Ransomware Group	Overall Percentage of total attack coverage
RansomHub	11.76%
Bianlian	5.88%
Killsec3	7.35%
El Dorado	1.47%
Meow	13.24%
Lynx	13.24%
Eraleign (APT73)	2.94%
Rhysida	1.47%
Space Bears	1.47%
Black Suit	10.29%
Hunters	7.35%
RA group	2.94%
3AM	1.47%
Kairos	8.82%
Everest	5.88%
Embargo	1.47%
Hellcat	1.47%

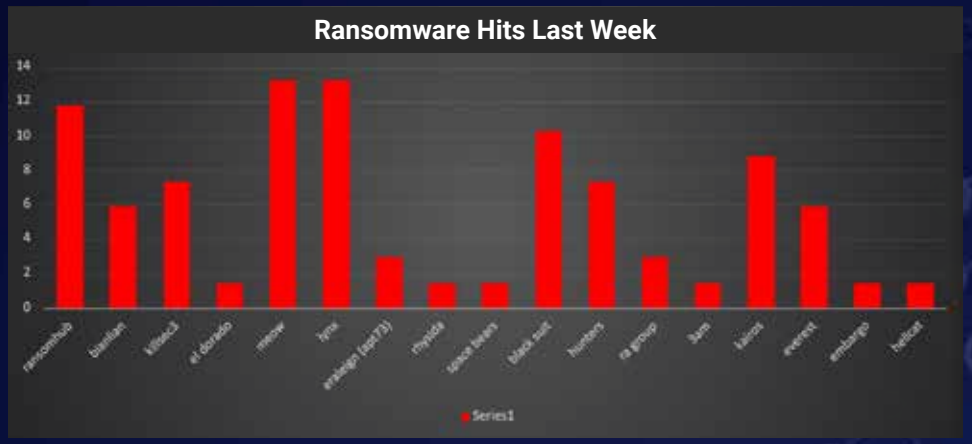
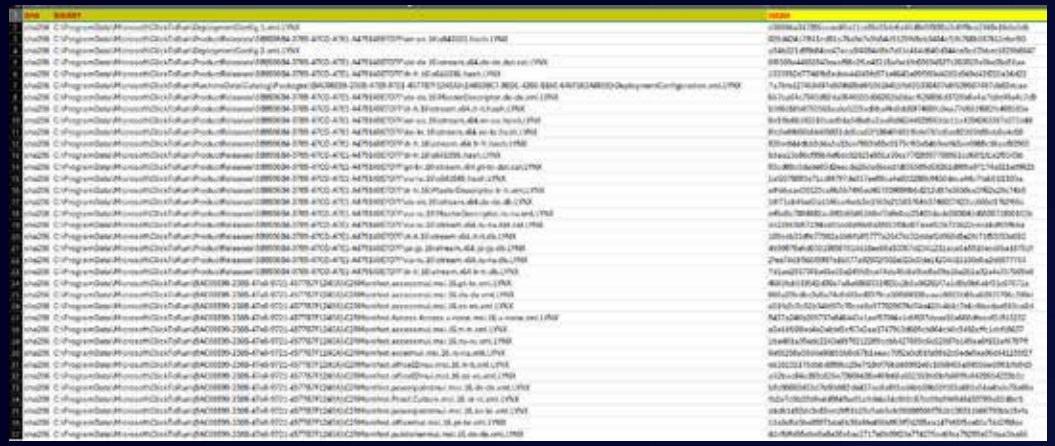


Figure 1: Ransomware Group Hits Last Week

Lynx Ransomware Group Report

Based on the latest Analysis on 14-Nov-2024, In the latest analysis conducted by Red Piranha, the Lynx ransomware samples were found to utilise advanced encryption techniques, including AES-128 in CTR mode and Curve25519 Donna algorithms. During the encryption process, all affected files have the `.lynx` extension appended to them, effectively locking users out of their data.

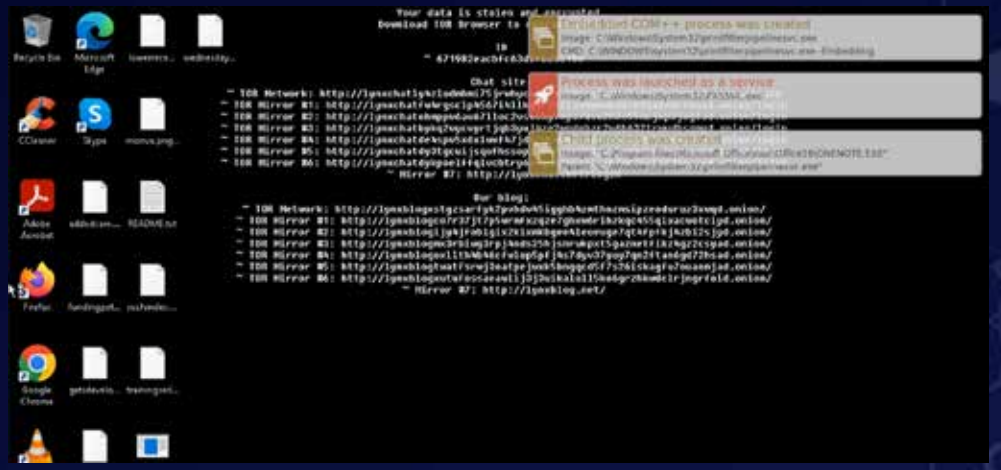


This variant, developed specifically for the Windows platform, is written in C++ to enhance its functionality and effectiveness.

Detailed TTPs

Primary Execution and Privileges:

The Lynx ransomware employs System Services (T1569) and Service Execution (T1569.002) techniques, requiring elevated privileges (Administrator/SYSTEM). The malware leverages Windows Service Control Manager (services.exe) for execution, utilising process ID 6224 (hash: 9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896.exe). Remote execution capabilities are enabled through PsExec and sc.exe utilities.



System Reconnaissance Phase:

The malware conducts systematic reconnaissance through Registry queries (T1012) and System Information Discovery (T1082). Specifically observed activities include:

- Machine GUID extraction from the registry
- Computer name identification
- Language support enumeration

These discovery operations shape the malware's subsequent behaviour and targeting decisions.

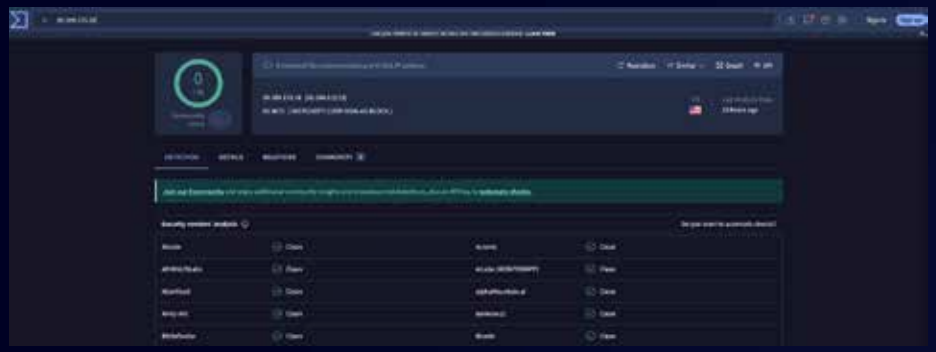
Encryption and Impact Stage:

The final attack phase implements Data Encryption for Impact (T1486), targeting both local and network resources. Key characteristics include:

- 16 instances of ransomware-style file renaming operations
- 10 confirmed LYNX ransomware signatures
- Potential encryption of cloud storage objects
- Capability to encrypt critical system files and disk partitions

Indicators of Compromises (IOCs)

- **9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896.exe**
- 20.189.173.16 (not yet flagged on Virustotal as malicious)



c38894a347095ccac80a11ce3fa03dc6a10d8d3f939a3c8ff9ca2340c16da5db
059d424c7f811cd91a76a9e7e3b54d9129fb9eb3404cf1fb768b587612ebef80
a54b321d99b84ee47aca5f4084d8b7d01c414d640d344ce3cd7bbec1828b6047
0f8309a44692543eaaf98c2f1e45215afac1fd05694527c263525e3be36d51aa
1333852d77f48fb5edda44045fd571e8643a09f383d4282d949d42f222a34d22
7a7bfe127419497d909609d4f50616415fb605330437b8f539507497db03dcae
6b7ca04c7543d92da3646555d56202b2dacf626856d3728b8a4a7b0d48a4c7d9
b586168b8703163aafa0223ed5baf4e0dd6974690c0ea77d661f682fc489585e
0e1f9c6b582510ced9da548e8a2ae8b56244529983da11a4204263367e372d48

The list of IOCs attached in an excel sheet.

Mitigations:

- Monitor service creation and registry modifications
- Implement strict privilege controls on service management
- Maintain secure, offline backups
- Monitor for suspicious PsExec and service control manager operations
- Deploy ransomware-specific endpoint protection

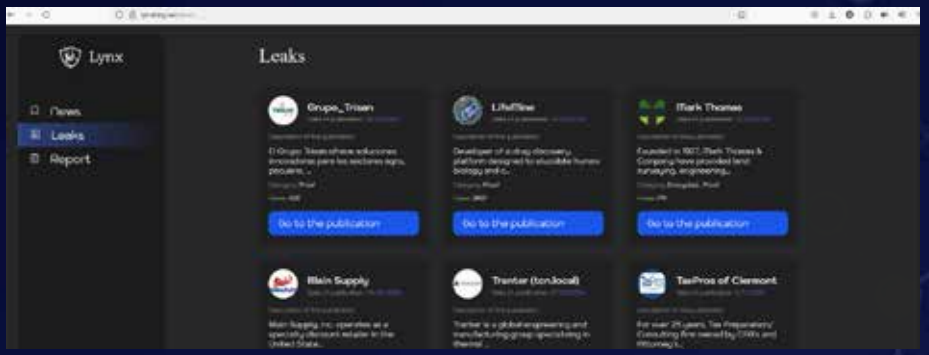


Figure 5: Screenshot of Leak Site used by Lynx

Ransomware Victims Worldwide

A recent analysis of ransomware impacts across various countries highlights the United States as the most affected, accounting for a dominant 60.29% of total incidents. Following are Canada, the United Kingdom, and Australia, each recording 4.41% of attacks. Poland and Brazil show notable impacts with 2.94% each. Several other nations, including Italy, India, Germany, Romania, Belgium, Argentina, Cape Verde, South Korea, Spain, Switzerland, Israel, Sweden, and Mexico, experienced minimal impacts, each contributing 1.47% to the total attack distribution. This distribution underscores the extensive reach and diverse impact of ransomware attacks worldwide, with a significant concentration in North America, particularly the United States.

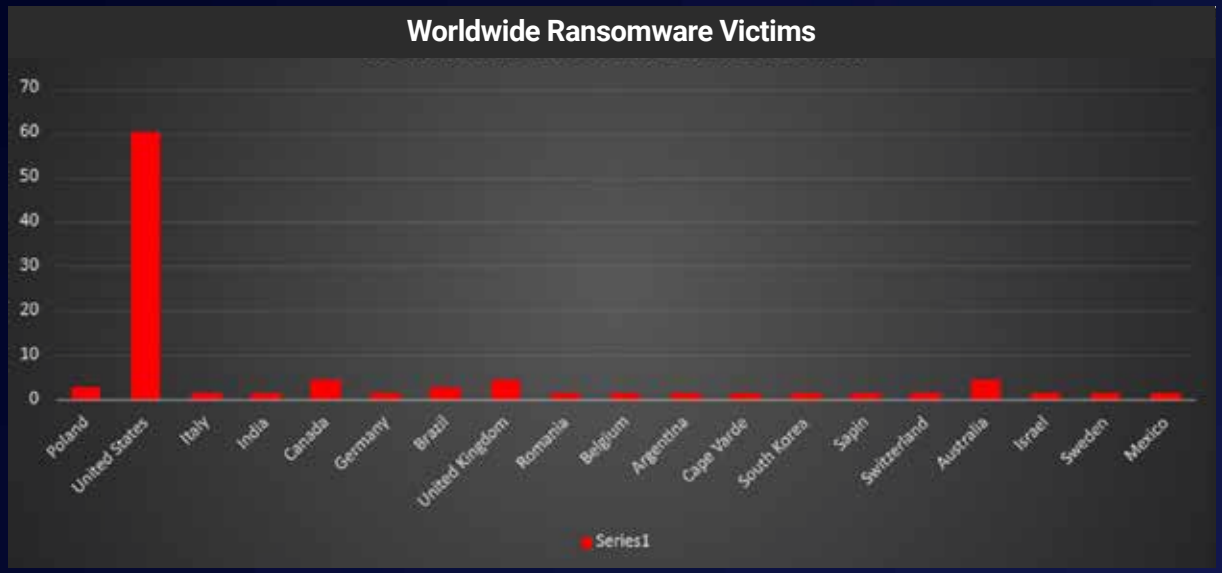


Figure 6: Ransomware Victims Worldwide

Ransomware Victims Industry-wise

A recent look into ransomware attacks across industries reveals Healthcare as the hardest hit, making up 14.71% of all incidents - a clear favourite target for cybercriminals. Manufacturing and Construction aren't far behind, each suffering 8.82% of the attacks, showing how critical infrastructure is being heavily targeted. The Business Services, Retail, and Education sectors also face significant challenges, with each accounting for 4.41% of the impact. Law Firms follow closely at 5.88%, reflecting the growing risk in legal sectors.

Other industries, including Industrial Machinery, Agriculture, Banking, Finance, Real Estate, Hospitality, and Consumer Services, have also been affected, each contributing 2.94% to the overall numbers. Meanwhile, sectors like Trading, Internet Services, Chemicals, Food & Beverage, Airlines, Government, and Telecommunications saw smaller shares, with each at 1.47%. This spread highlights the wide-ranging nature of ransomware, with attackers zeroing in on sectors critical to daily life, such as Healthcare, Manufacturing, and Education.

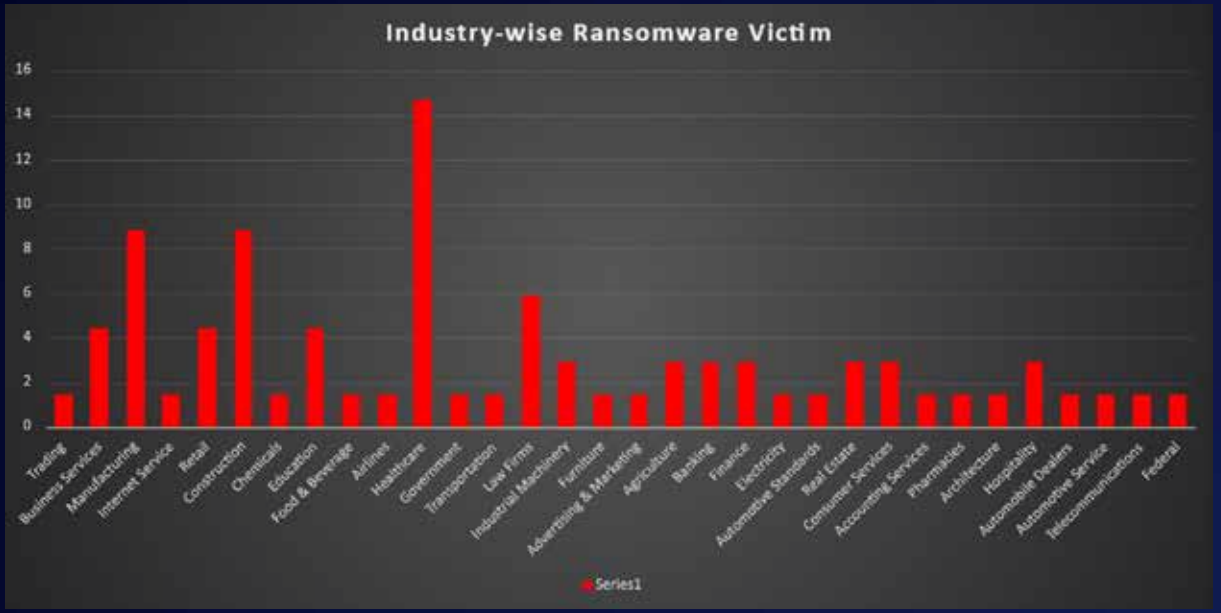


Figure 7: Industry-wise Ransomware Victims

DETAILED MITIGATION STRATEGIES

1. Service Creation and Registry Monitoring:

- Implement real-time monitoring of Windows Service Control Manager activities
- Deploy tools to track suspicious registry modifications, especially in HKLM and HKCU hives
- Create alerts for unauthorised service installations
- Monitor PsExec and sc.exe usage across the network
- Set up logging for Windows Registry Key Modification events

2. Privilege Control Implementation:

- Enforce strict User Account Control (UAC) settings
- Implement the principle of least privilege for service accounts
- Restrict administrative and system-level access
- Configure Service Control Manager access controls
- Monitor and audit privilege escalation attempts
- Limit permissions for registry modification

3. Endpoint Protection Enhancement:

- Deploy anti-ransomware modules with behaviour monitoring
- Implement file entropy monitoring for encryption detection
- Configure blocking rules for known Lynx hash signatures
- Enable process chain analysis
- Set up application whitelisting
- Monitor and block suspicious AutoStart execution attempts

4. Backup and Recovery Strategy:

- Maintain 3-2-1 backup rule (3 copies, 2 different media, 1 offsite)
- Implement immutable backup solutions
- Regular testing of backup restoration procedures
- Segment backup networks from the main infrastructure
- Enable versioning for critical files
- Regular validation of backup integrity

5. Network Security Controls:

- Monitor and restrict PsExec usage across the network
- Implement network segmentation
- Configure SMB share access controls
- Enable detailed logging of network file access
- Monitor for suspicious remote service creation attempts
- Restrict service account network permissions