THREAT INTELLIGENCE REPORT

January 20 – January 26, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- Evilginx2

Detection Summary

- New Threat Protection: 276
- Newly Detected Threats: 4

The following threats were added to Crystal Eye this week:

1. Evilginx2

Evilginx is a go-based man-in-the-middle attack framework that's commonly used in phishing campaigns by security professionals and threat actors. It can facilitate bypassing some MFA implementations using a reverse proxy which passes the authentication request through to the legitimate service. Evilginx uses the concept of phishlets which are customised phishing pages designed to mimic the real login page, with recent implementations utilising fake captcha style landing pages.

Threats Protected: 16
Class Type: Credential-theft
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001 T1566.002	Phishing: Spearphishing Attachment Phishing: Spearphishing Link
Execution	T1204.001 T1204.002 T1204.004	User Execution: Malicious Link User Execution: Malicious File User Execution: Malicious Copy and Paste
Credential Access	T1557 T1539	Adversary-in-the-Middle Steal Web Session Cookie

Current Threat Summary

Known Exploited Vulnerabilities (Week 4 - January 2026)

Vulnerability	CVSS	Description
CVE-2018-14634	7.8	Linux Kernel contains an integer overflow vulnerability that can allow an attacker with local access to escalate their privileges.
CVE-2025-52691	10	SmarterTools SmarterMail contains a vulnerability that can allow an unauthenticated remote attacker to upload arbitrary files to the system via the '/api/upload' endpoint. Exploitation of this vulnerability can enable an attacker to upload a WebShell providing access to the underlying system.
CVE-2026-23760	9.3	SmarterTools SmarterMail contains an authentication bypass vulnerability that can allow an unauthenticated remote attacker to reset the password of an administrator. This vulnerability affects version prior to build 9511. Post exploitation of this vulnerability can enable an attacker to execute operating system commands via built-in functionality, resulting in SYSTEM or root level access on the underlying system.
CVE-2026-24061	9.8	GNU InetUtils contains an argument injection vulnerability in telnetd that can allow a remote attacker to bypass the authentication by passing through an environment variable (USER="-f root") upon connecting. This vulnerability affects versions 1.9.3 through to 2.7, and exploitation can result in an attacker gaining root level privileges on the system.
CVE-2026-21509	7.8	Microsoft Office contains a vulnerability that can result in bypassing OLE mitigations when opening a arbitrarily crafted office file. This security feature protects users from executing embedded COM/OLE controls within the document.
CVE-2024-37079	9.8	Broadcom VMware vCenter Server contains a heap overflow vulnerability within the implementation of the DCERPC protocol that can allow an attacker with network access to execute code on the system.
CVE-2025-68645	8.8	Synacor Zimbra Collaboration Suite (ZCS) contains a file inclusion vulnerability within the RestFilter component that can allow an unauthenticated remote attacker to include files via a specially crafted request to the '/h/rest' endpoint.
CVE-2025-34026	9.2	Versa Concerto SD-WAN orchestration platform contains an authentication bypass vulnerability within the Traefik reverse proxy configuration that can allow an unauthenticated remote attacker to access administrative endpoints. This vulnerability affects version 12.1.2 through to 12.2.0, exploitation of this vulnerability can allow an attacker to access the internal actuator endpoint which provides access to heap dumps and trace logs.
CVE-2025-31125	5.3	Vite Vitejs contains an improper access control vulnerability within the dev server that can allow an unauthenticated remote attacker to read arbitrary file contents. Exploitation of this vulnerability may provide information that can be used in further attacks.
CVE-2025-54313	7.5	Prettier eslint-config-prettier contains embedded malicious code as a result of a successful phishing campaign against a maintainer of the library, which resulted in malicious packages pushed to the npm registry. The malicious code affects versions 8.10.1, 9.1.1, 10.1.6 and 10.1.7, and installation of this package results in the execution of a Windows based malware.
CVE-2026-20045	8.2	Multiple Cisco communication products contain a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code via a specially crafted HTTP request. Exploitation of this vulnerability can result in an attacker gaining access to the underlying system, with post-exploitation enabling elevation of privileges to root.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-january-2026/634

Current Threat Summary

Updated Malware Signatures (Week 4 - January 2026)

Threat	Description
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a "legitimate tool."
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.

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 Hits Last Week

The following chart illustrates the distribution of ransomware attacks by threat group during the analysis period. Nova accounts for 0.95% of total attacks, with 'The Gentlemen' (12.32%), Qilin (11.85%), and Clop (9.95%) leading the threat landscape.

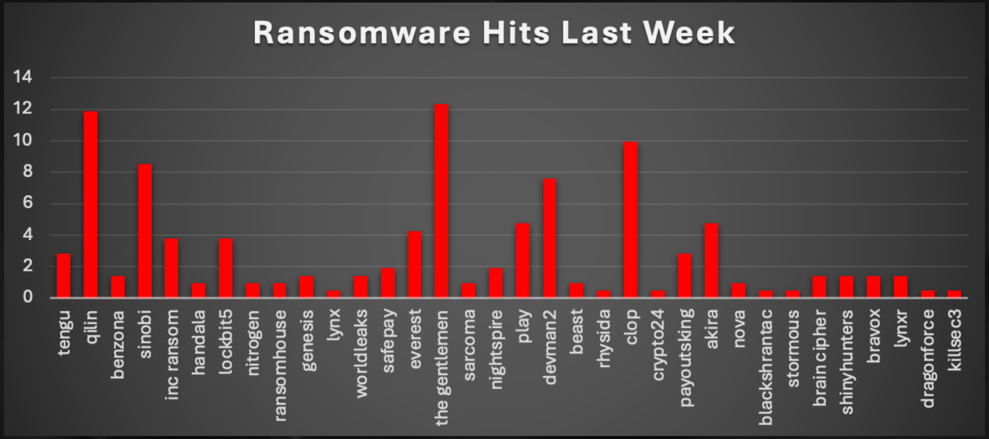


Figure 1: Ransomware Group Hits Last Week

Nova Ransomware

Analysis Period: 17 January 2026 - 23 January 2026

Description

Nova (formerly RALord) is a Ransomware-as-a-Service (RaaS) operation first observed in late March 2025 under the name RALord, rebranding to Nova in April 2025. The group operates a double-extortion model - encrypting victim files while exfiltrating sensitive data to maximise ransom pressure. Nova maintains a Tor-based Data Leak Site (DLS) where victim profiles are published alongside countdown timers and proof-of-theft documentation. The group has claimed victims across multiple continents, targeting sectors including healthcare, education, hospitality, IT services, media and entertainment, construction, and agriculture.

Nova operates an aggressive affiliate recruitment model offering an 85/15 revenue split in favour of affiliates - one of the more generous offerings in the current RaaS landscape. Standalone locker access is available for €200–€300 (lifetime fee), lowering the barrier to entry for less sophisticated actors. The group actively recruits on darknet forums (RAMP, DarkForums) under the username "ForLord," seeking candidates with Rust/Python programming skills, CVE exploitation expertise, and network penetration experience.

Technical Profile

Ransomware Payload: Nova operates two primary payload variants:

- Affiliate variant: Appends .nova extension to encrypted files
- Premium Rust-based variant: Appends .RALord or .ralord extension
- The ransomware is written in Rust—a choice that complicates static analysis and helps evade traditional signature-based detection. Upon execution, the malware opens a console window via conhost.exe and begins scanning for files to encrypt. Ransom notes are dropped with randomised filenames directing victims to qTox for negotiation.
- Platform Support: Cross-platform capability spanning Windows, Linux, and VMware ESXi environments.

Detailed Tactics, Techniques, and Procedures (TTPs)

1. Initial Access (Compromised Credentials & Vulnerability Exploitation)

Nova predominantly gains access through compromised VPN/RDP credentials obtained via credential stuffing attacks, reused passwords, or purchased from Initial Access Brokers (IABs). The group specifically targets organisations with exposed remote access services lacking multi-factor authentication.

Primary access methods include exploitation of vulnerabilities in public-facing applications (VPN appliances, firewalls, remote access gateways), spearphishing campaigns disguised as legitimate business communications (contracts, invoices), AI-powered phishing using LLMs to craft emails indistinguishable from legitimate corporate communications with localised language and tone for specific regional targets.
In a notable shift documented by FBI advisories, ransomware groups including Nova have begun recruiting corporate insiders or unwitting gig workers to physically enter offices and insert USB drives under the guise of IT help desk tasks. Nova affiliates frequently purchase valid domain administrator credentials from IABs, allowing them to bypass perimeter security entirely and begin post-compromise activities immediately.

2. Execution & Operator Control

Upon achieving access, the Nova payload is typically executed via command-line interpreters including PowerShell and Windows Command Prompt (cmd.exe). The Rust-based encryptor executes via conhost.exe console window creation. Operators utilise encoded PowerShell commands to avoid detection, LOLBins (Living Off The Land Binaries) for staging and execution, and user-launched executables from downloads/temp paths. The group employs a 'fast and aggressive kill chain' philosophy, often aiming to complete the transition from initial access to full system encryption within a minimal dwell time window.

3. Persistence Mechanisms

Nova establishes persistence through multiple techniques to ensure malware survives system reboots and maintains long-term presence.

Registry Modification: The ransomware creates and modifies keys within HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run to launch automatically at startup.

Scheduled Tasks: Nova creates Windows scheduled tasks that run with SYSTEM-level privileges, often set to recurring triggers like hourly intervals or user logon events.

Boot Environment Modification: A standout behaviour of the Nova cluster is the forced modification of Windows Boot Configuration Data (BCD) by executing 'bcdedit /set {default} safeboot network', forcing infected systems into Safe Mode with Networking before initiating encryption – a strategic manoeuvre designed to circumvent security software that does not load in Safe Mode.

Remote Access Tools: Deployment of legitimate tools including PuTTY, AnyDesk, LogMeIn for maintaining persistent access via stolen RDP credentials.

4. Privilege Escalation

Nova operators escalate to administrative privileges before encryption. The group leadership confirmed: 'We up perms to root (admin) and run to all disks...no backups because I am encrypting with admin perm, so all backups encrypted.'

Primary escalation methods include credential-based elevation using harvested domain administrator credentials, exploitation of local privilege escalation vulnerabilities within compromised environments, and abuse of elevation control mechanisms.

They bypass User Account Control by modifying registry settings to disable Remote UAC restrictions, allowing elevated commands to be run remotely across the domain without prompting for user intervention.

5. Defence Evasion (Advanced Techniques)

Nova operators are highly adept at neutralising defensive infrastructure using sophisticated evasion strategies.

Security Service Termination: The group systematically identifies and stops processes related to antivirus (AV), endpoint detection and response (EDR), and backup solutions.

Volume Shadow Copy Deletion: To prevent system restoration, Nova executes 'vssadmin.exe Delete Shadows /all /quiet' and 'wmic shadowcopy delete /nointeractive', destroying local recovery options.

Rust-Based Obfuscation: The group states 'most ransomware groups use C/C++ or Python...Windows Defender alone will capture it. Our lockers building with Rust, anti-detection.' They claim weekly locker updates to evade new Microsoft security measures. The Rust implementation generates 10,000+ functions making reverse engineering extremely difficult.

Remote UAC Bypass: Attackers modify registry to disable Remote User Account Control restrictions.

Indicator Removal: Log clearing, artifact deletion, and cleanup scripts to remove forensic evidence.

Virtualisation/Sandbox Evasion: Delays and checks for analysis tooling/VM traits to avoid sandbox detection.

6. Credential Access (Aggressive Harvesting)

Nova operators aggressively pursue credential access using multiple tools and techniques.

LSASS Memory Extraction: The malware utilises tools like Mimikatz or Procdump to extract cleartext passwords and session tokens from the Local Security Authority Subsystem Service (LSASS) memory.

Browser Password Theft: Stealing credentials stored in browser password managers.

Pass-the-Hash Techniques: Using harvested NTLM hashes for authentication without needing plaintext passwords.

Token Reuse: Capturing and replaying authentication tokens for lateral movement.

Credentials from Password Stores: Extracting saved passwords from Windows Credential Manager, browser caches, and application configuration files.

7. Reconnaissance & Discovery

Nova performs extensive network and system discovery to identify high-value targets.

File and Directory Discovery: Broad traversal before encryption with access spikes across network shares.

System Information Discovery: Host inventory commands, OS/domain enumeration to understand the environment.

Registry Queries: Queries related to security tooling and configurations to identify defensive measures.

Network Share Discovery: Identifying file servers, backup locations, and sensitive data repositories.

Virtualisation Storage: Specifically targeting .vhd, .vhdx, and .vmdk files within VMware and Hyper-V environments to inflict maximum operational disruption.

Cloud and Database Structures: Targeting source code repositories and database structures to increase extortion leverage.

8. Lateral Movement (Enterprise Spread)

Once administrative credentials are secured, attackers pivot across the network using legitimate administrative protocols.

Remote Desktop Protocol (RDP): Primary method for interactive lateral movement across Windows systems.

SMB/Windows Admin Shares: Using ADMIN$ and C$ shares for file transfer and remote execution.

Remote Services: Leveraging WMI/WMIC for distributed commands across the enterprise.

Pass-the-Hash Authentication: Using NTLM hash-based authentication for lateral movement without plaintext passwords.

Lateral Tool Transfer: Moving tools and payloads between systems for mass deployment. SSH connections to ESXi hosts for targeting virtualisation infrastructure.

9. Data Collection & Exfiltration (Double-Extortion Preparation)

Before the encryption phase is triggered, terabytes of data are exfiltrated to support double-extortion operations.

Data from Local System: Sensitive directory harvesting including PII, PHI, financial records, and business agreements.

Data Staging: Large archive staging areas with sudden disk usage spikes before exfiltration.

Archive Collection: Compressing stolen data for efficient transfer.

Exfiltration Over C2 Channel: Data theft via HTTP/HTTPS to private attacker-controlled servers.

Exfiltration Over Alternative Protocols: Using cloud services and custom transfer paths to evade detection. This data theft is central to the 'Double Extortion' model – even if a victim successfully restores from backups, the threat of leaking sensitive data provides secondary leverage to demand payment.

10. Inhibit System Recovery (Backup Destruction)

As a final destructive step before encryption, Nova systematically destroys recovery options.

Volume Shadow Copy Deletion: Executing 'vssadmin.exe Delete Shadows /all /quiet' to remove Windows shadow copies.

WMI Shadow Copy Deletion: Using 'wmic shadowcopy delete /nointeractive' as an alternative deletion method.

Backup Catalogue Removal: Targeting backup software configurations and catalogues.

Backup Process Termination: Stopping backup services (Veeam, Commvault, Acronis) to release file locks. This maximises pressure on victims to pay ransom as traditional recovery methods are rendered ineffective.

11. Encryption & Impact (Ransomware Deployment)

Nova employs a hybrid cryptographic scheme that balances speed with security.

Symmetric Encryption: Files are encrypted using AES-256 in Cipher Block Chaining (CBC) mode, with a unique key generated for each file to prevent batch decryption. Some variants use RC4 for faster encryption of large files.

Asymmetric Wrapping: The AES key is then encrypted with the attacker's RSA-2048 public key and appended to the end of the encrypted file, ensuring only the attacker's private key can decrypt.

File Extensions: Encrypted files receive extensions including .nova (affiliate variant), .RALord/.ralord (premium Rust variant), .LORD, .RNOVA, and variant-specific extensions like .happy11 and .KARMA.

Ransom Notes: Notes following the pattern 'README-[12 random alphanumeric characters].txt' are dropped in each encrypted directory.

12.Command-and-Control / Negotiation / Data Leak

Nova maintains TOR-based infrastructure for operations and victim communications.

Data Leak Sites (DLS): Multiple active onion addresses host victim profiles with in-depth attack reports, often mockingly highlighting failed security products.

Visual Proof-of-Claims: Profiles feature screenshots of encrypted directories, internal network share listings, and samples of exfiltrated documents.

Countdown Timers: Real-time clocks indicating time remaining before full dataset release or sale to third parties.

Negotiation Portal: Secure chat environment (branded as 'Nova Access Portal') for victim communication with specialised 'journalists' and 'lawyers' who assist in drafting publication texts.

Affiliate Dashboard: Control panel tracking active infections, ransom negotiations, and exfiltration status with custom payload builders for Windows, Linux, and VMware ESXi.

MITRE ATT&CK TTP Matrix

The table below summarises Akira's tactics and techniques mapped to the MITRE ATT&CK framework:

Tactic	Technique (ID)	Nova Implementation
Initial Access	Valid Accounts (T1078)	Stolen credentials from IABs
Initial Access	Phishing (T1566)	AI-powered spear phishing
Execution	Command & Scripting (T1059)	PowerShell/CMD, LOLBins
Persistence	Boot/Logon AutoStart (T1547)	Run keys, registry modification
Persistence	Scheduled Task (T1053)	SYSTEM-level scheduled tasks
Defence Evasion	Impair Defences (T1562)	Terminating AV/EDR processes
Defence Evasion	Obfuscated Files (T1027)	Rust 10,000+ functions obfuscation
Credential Access	OS Credential Dumping (T1003)	Mimikatz, LSASS extraction
Discovery	Network Share Discovery (T1135)	Scanning backups, VHDX/VMDK
Lateral Movement	Remote Services (T1021)	RDP, SMB admin shares
Exfiltration	Exfil Over C2 Channel (T1041)	HTTP/HTTPS to attacker servers
Impact	Data Encrypted (T1486)	AES-256/RSA-2048, .nova/.RALord
Impact	Inhibit Recovery (T1490)	vssadmin/WMI shadow deletion

Indicators of Compromise (IOCs)

Infrastructure / C2:

- TOR Onion Addresses:

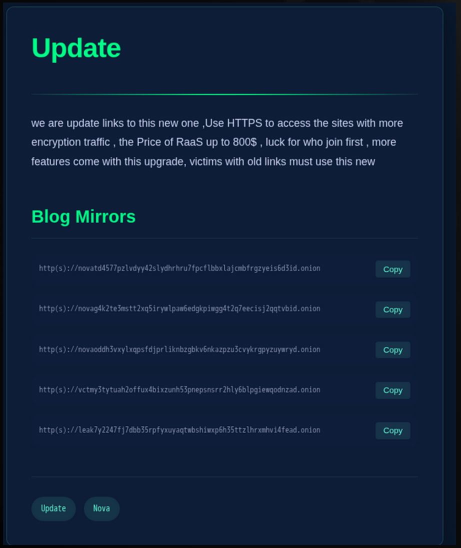
novavdivko2zvtrvtllnq45lxhba2rfzp76qigb4nrliklem5au7czqd.onion (ACTIVE)

novadmrkp4vbk2padk5t6pbxolndceuc7hrcq4mjaoyed6nxsqiuzyyd.onion (ACTIVE)

novav75eqkjoxct7xuhhwnjw5uaaxvznhtbykq6zal5x7tfevxzjyqyd.onion

novavagygnhqyf7a5tgbuvmujve5a2jzgbrq2n4dvetkhvr2zjg27cad.onion

pifk3xu3vad6cuxsjll4qjomyaaaoyvnyqppro75pazadzctrrvpdnyd.onion



Update

we are update links to this new one ,Use HTTPS to access the sites with more encryption traffic , the Price of RaaS up to 800$, luck for who join first , more features come with this upgrade, victims with old links must use this new

Blog Mirrors

http(s)://novatd4577pzlvdyy42slydhrhru7fpcflbbxlajcmbfrgzyeis6d3id.onion Copy

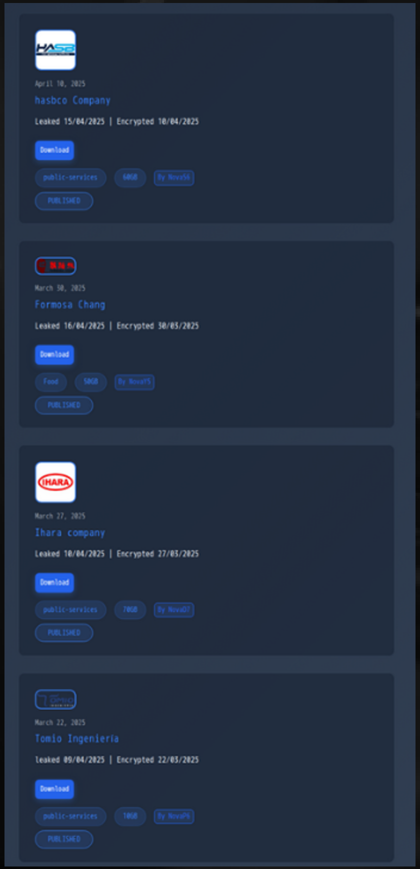
http(s)://novag4k2te3mstt2xq5irywlpaw6edgkpiwgg4t2q7eecisj2qqtvbid.onion Copy

http(s)://novaoddh3vxylxqpsfdjprliknbzgbkv6nkazpzu3cvykrgpyzuywryd.onion Copy

http(s)://vctmy3tytuah2offux4bixzunh53pnepsnsrr2hly6blpgiewqodnzad.onion Copy

http(s)://leak7y2247fj7dbb35rpfyxuyaqtwbshiwxp6h35ttzlhrxmhvi4fead.onion Copy

Update Nova



April 10, 2025

hasbco Company

Leaked 15/04/2025 | Encrypted 10/04/2025

Download

public-services 60GB By Nova56

PUBLISHED

March 30, 2025

Formosa Chang

Leaked 16/04/2025 | Encrypted 30/03/2025

Download

Food 50GB By NovaYS

PUBLISHED

March 27, 2025

Ihara company

Leaked 10/04/2025 | Encrypted 27/03/2025

Download

public-services 70GB By NovaD7

PUBLISHED

March 22, 2025

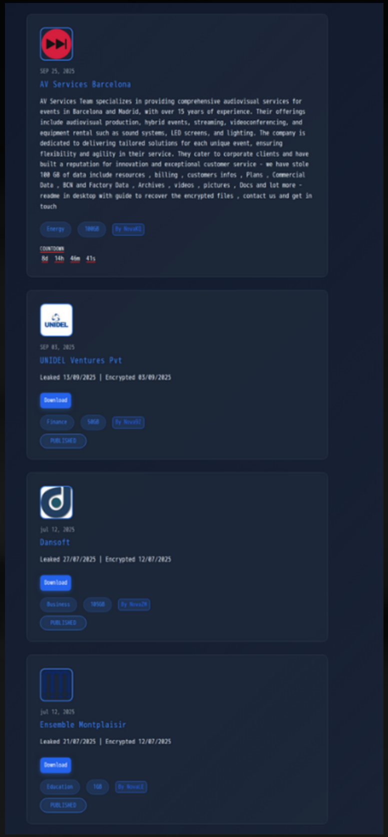
Tomio Ingeniería

leaked 09/04/2025 | Encrypted 22/03/2025

Download

public-services 10GB By NovaP6

PUBLISHED



SEP 25, 2025

AV Services Barcelona

AV Services Team specializes in providing comprehensive audiovisual services for events in Barcelona and Madrid, with over 15 years of experience. Their offerings include audiovisual production, hybrid events, streaming, videoconferencing, and equipment rental such as sound systems, LED screens, and lighting. The company is dedicated to delivering tailored solutions for each unique event, ensuring flexibility and agility in their service. They cater to corporate clients and have built a reputation for innovation and exceptional customer service - we have stole 100 GB of data include resources , billing , customers infos , Plans , Commercial Data , BCN and Factory Data , Archives , videos , pictures , Docs and lot more - readme in desktop with guide to recover the encrypted files , contact us and get in touch

Energy 100GB By NovaKQ

COUNTDOWN

8d 14h 46m 41s

SEP 03, 2025

UNIDEL Ventures Pvt

Leaked 13/09/2025 | Encrypted 03/09/2025

Download

Finance 50GB By Nova9Z

PUBLISHED

jul 12, 2025

Dansoft

Leaked 27/07/2025 | Encrypted 12/07/2025

Download

Business 105GB By NovaZK

PUBLISHED

jul 12, 2025

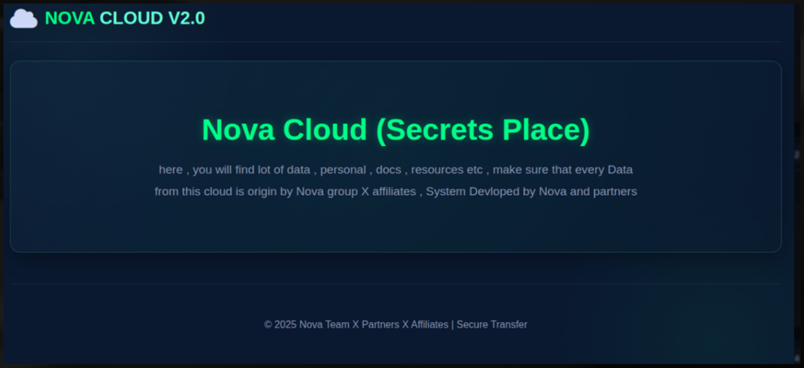
Ensemble Montplaisir

Leaked 21/07/2025 | Encrypted 12/07/2025

Download

Education 1GB By NovaLE

PUBLISHED

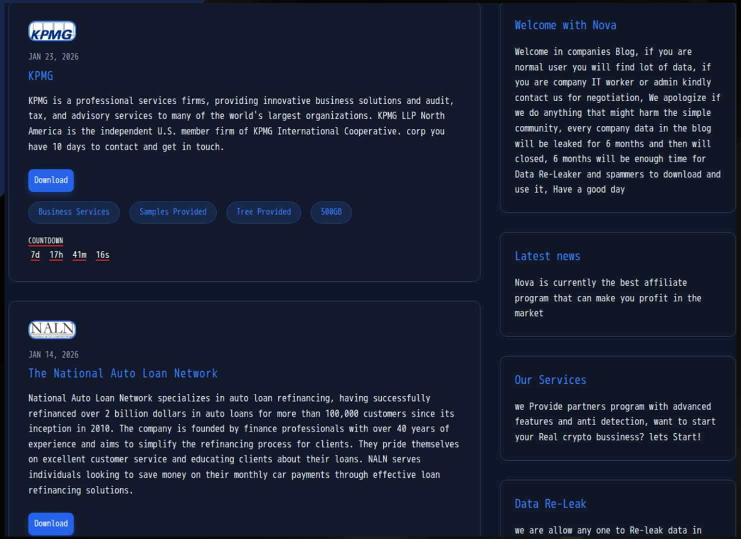


NOVA CLOUD V2.0

Nova Cloud (Secrets Place)

here , you will find lot of data , personal , docs , resources etc , make sure that every Data from this cloud is origin by Nova group X affiliates , System Devloped by Nova and partners

© 2025 Nova Team X Partners X Affiliates | Secure Transfer



JAN 23, 2026

KPMG

KPMG is a professional services firms, providing innovative business solutions and audit, tax, and advisory services to many of the world's largest organizations. KPMG LLP North America is the independent U.S. member firm of KPMG International Cooperative. corp you have 10 days to contact and get in touch.

JAN 14, 2026

The National Auto Loan Network

National Auto Loan Network specializes in auto loan refinancing, having successfully refinanced over 2 billion dollars in auto loans for more than 100,000 customers since its inception in 2010. The company is founded by finance professionals with over 40 years of experience and aims to simplify the refinancing process for clients. They pride themselves on excellent customer service and educating clients about their loans. NALN serves individuals looking to save money on their monthly car payments through effective loan refinancing solutions.

Welcome with Nova

Welcome in companies Blog, if you are normal user you will find lot of data, if you are company IT worker or admin kindly contact us for negotiation, We apologize if we do anything that might harm the simple community, every company data in the blog will be leaked for 6 months and then will closed, 6 months will be enough time for Data Re-Leaker and spammers to download and use it, Have a good day

Latest news

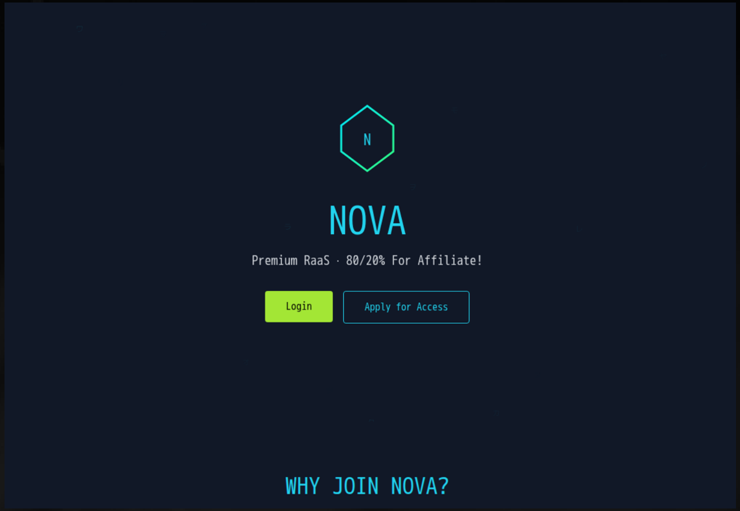
Nova is currently the best affiliate program that can make you profit in the market

Our Services

we Provide partners program with advanced features and anti detection, want to start your Real crypto bussiness? lets Start!

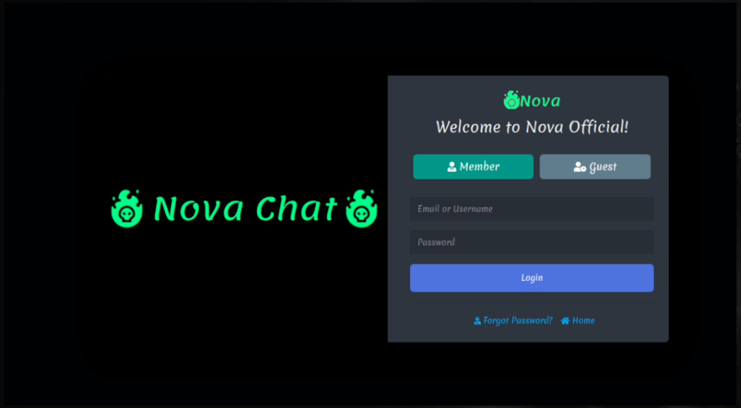
Data Re-Leak

we are allow any one to Re-leak data in

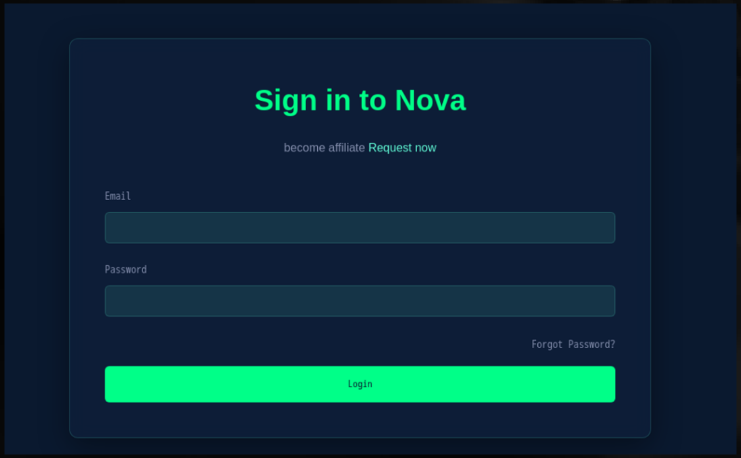


Premium RaaS · 80/20% For Affiliate!

WHY JOIN NOVA?



Welcome to Nova Official!



Sign in to Nova

become affiliate Request now

Communication Identifiers:

- Session: 054f55ec93aca9bac362b9d91eff36a7ce451e7caba47c0b2e004ba429f9529c79
- Tox: 8E9A6195A769FE7115F087C61D75CF32874C339B3AB0947D07480C9A8A12DA5009151BE6A51F
- Telegram: @NovaSupport

Malware Samples:

- SHA-256: 456b9adaabae9f3dce2207aa71410987f0a571cd8c11f2e7b41468501a863606
- MD5: ef846baabc14fe461cff4c4a0fd5056f, be15f62d14d1cbe2aecce8396f4c6289, 4566f5ba6d1a1db0dd7794ea8d791b3f

File Indicators:

- Extensions: .nova, .RALord, .ralord, .LORD, .RNOVA, .happy11, .KARMA
- Ransom Notes: README-[random].txt, HOW_TO_RECOVER_DATA.html
- Registry: HKLM\SOFTWARE\NovaRansom

Command-Line Artefacts:

- vssadmin.exe Delete Shadows /all /quiet
- wmic shadowcopy delete /nointeractive
- bcdedit /set {default} safeboot network (EDR Bypass)

PGP:

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGNBGjOVRwBDADr6SA5p6Lqve69WGbvDlz75WD06GXKecP+ko
qPwj0X/a7/6D677zToqSE0Lm8ROBNEEZWbNdHTKiEz5MUwkWW9b
4MyZeWfZ3LodE1jSHFHE6i8qQGM
QzuauXpZtabJiuLeL5iBhrsNktC4Zv+T4ySQZpcT7v5VBN38tlF2UA3m1
arGTE75W7Ew+TgqYOpRnOW8RInc1JNh+tPszcWwzSmJRUkW5oJX7
9EQPu1FOot3befVQy0WTViYedsJ4TvHJZ8CAivJ/+DsMlhl6UG0wli5w
2KeGNVsWPIQCTYOzCO2B7qSEGSMtb7HVp6k7Dvi2yZWRm99iUyan
Z5cGpqlPyXEtaHZ7eOrQRMTKo71Zt+lrlCjePrqU/ik7Sq6o9zyFaTzCe1K
OWXV06/amNgj0ICOS4hGLiCSFkfOKDR6xrBzs70x3AVD
/IRXczW7vCz34myJ2QQVqt/olqpohcHPAV+rrmfWgnEYXHt5oPhSlijm
NzCrrYGlhNZWvqBRkUBuLQ0AEQEAAbQmbm92YSAoTm92YV9TdG
FyKSA8bm92YTFAb25pb25tYWlsLm9yZz6JAdEEEwEKADsWIQRZd
CljGnML+3TBQwqTUHMmkHWCIAUCaM5VHAIbAwULCQgHAgIiAgY
VCgkICwIEFgIDAQIeBwIXgAAKCRCTUHMmkHWCIC2FDADRZW7gC
HY4HwvFrzj9FZ8UCBKpEMe2L8XXGRGvQFqos0tOExAWoon8G3QX
4BzzMFxLZMpmpyAHoiRakKw8yMxONLnc2CxeKjUduEgOflW+a3InlO
9EiktQXvzpW4wVafRFqPH2JYroOpIV+eghJ5f/l6VjokztS1f/OIczDdram
6KbzsrOUfaHrRLMWlSpgNQcPethXMcnuy5cs1ja85KL7OpaRnvqQTae
G2bZu/NN4F4KO7WJz7mtyUB0cbFB1S5ADac9yK5ZRETLt34Zt2v3W
PjYKQa6cAq1lUDLMhvVUKCzIT6n+hOJKdnYPJH3vJP/L6vFQVzoifoY+
Xsd3h+6JD8G/LrIxV1kCnNcekG0bEDV83/aY0eiDd7KfqKfF9QciosHQ
+0tdDKqQlHmAem5V9h0otqfH1ENUpk6tj4Tlnn/8MovZvQxWLgSbPG
F9VG/smmY/BIH5t6ODn8/QQ8F9bqptARWe33rny+5mjeVhNV3+3pw
/Idk8eKMaX6j5V+5AY0EaM5VHAEMALI7HRwcKn22nZZKBMHkOUKU
5AbABSNQI0CsceLbRu3slat3Bab3rHEu9yKM08e7/j3NzTffA61MhScT
mlgi6fxgojVNKvHVC9m9YyGUOwW49M4Tl1W0edvF6wYuuw7QiCWj
HtPOEk4BDXl/IcV+vwyt+u2y4r8JZtTPW5Z+L83nzYNJmd8/WYMBX
A7XZoRvtJvhzN2bzvYdftLl7B9E6Svk4OKSp+bqcD7MxZN1NowsEqOp
L41tSXtCTDXXV8jTfJR0xFVQweug2af4qLCMNk6T7+m3x5aEAmGFnn
vsaC0iN3XXn21304+vy4T7gZ0mSkHQqZ1CFUc+s1CfxAKWn9xC7et8r
tlkUzySUZVuChdaWhvlQ5lQ05NLHOIsBYrT+VlaiZmznkdwYZ4EDLa3
pB0w3Z0ld/LYH31x3EqC9+LqZ6RQCEAhWC3moDU3zJyil8khbybkQ
A+IGfU2+xXZEeQeQ4yUlvAZD8jWKzvmz4LwSS1m5lOPazP+L0Eow+l
EuQARAQABiQG2BBgBCgAgFiEEWXQilxpzC/t0wUMKk1BzJpB1giAF
AmjOVRwCGwwACgkQk1BzJpB1giAgOQwA0KTiW0yuVsny8iRUyRV7
Q1EuClk4/CetF9wL
pHcTbbz/wxu2SGO88NNUdNsp6NFWVL/qTPIn+vqfdcrtHXQGILfdnO
zi8dacf2yvScRyBFf5sU3nRCTWyhPhlnztjZ4O3Xov0EQy3YwRE44d5y
AdhJA5KoHbZCVociDSZ1QpL9fXHNZKQBFFuTQ6GBKYi1AazYJLiqsO
cRYJVBrqkD5F6cu4YLv6d0BoXEru9/2V0ND4DuWCZ8KFJ0fTS7X1Hi
Paj1rCBMz8lI3dCfNUU5v3nrLjHB08YPTShJmJRj6fVvej8LM21VKOyCK
GOyzT7abhnVoNNmpSqZhG0VkbZCth/wjs6Ifcw8hgotp56RcuwMm3
xFu5ieuvli40betXWCnKhDj0UGbolEwabm7Qq1CHD6d6b8qtlZtd910B
s/BCIKwOY7Oenpn0n+w+iIANdVjy614IrBtYNq1b1i2fOaTxI11XtpQ7KFg
FQ4QW

Mitigation Strategies

Recommended CE 5.5 Configuration Actions

- Block Nova Infrastructure: Add known Nova onion addresses to CE SWG blocklists.
- Enable CEASR Policies: Enforce application allowlisting and block execution from user-writeable directories.
- Configure SIEM Alerts: Create correlation rules for shadow copy deletion, mass encryption patterns, and qTox/Session traffic.
- Isolate Critical Assets: Apply micro-segmentation to separate AD, file servers, ESXi hosts, and backup infrastructure.
- Activate MDR Services: Enable Red Piranha's Incident Response Services for 24×7 SOC escalation and containment support.

Worldwide Ransomware Victims by Country

Geographic distribution of ransomware victims shows the United States as the primary target (42.65%), followed by the United Kingdom (8.06%) and Canada (5.69%). European nations collectively represent a significant portion of victims, with growing activity in Asia-Pacific regions.

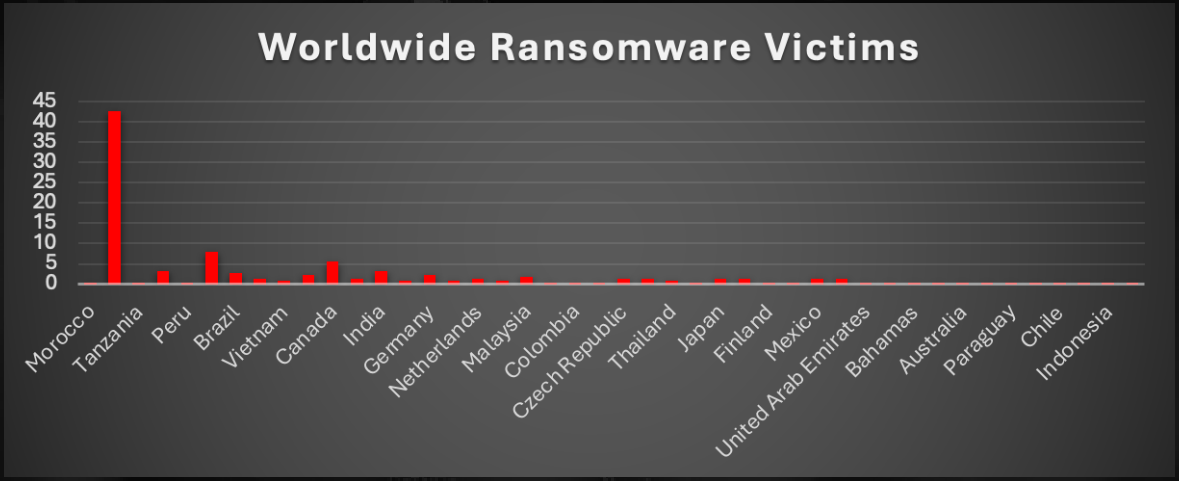


Figure 10: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing leads as the most targeted sector (21.33%), followed by Construction (11.85%) and Business Services (11.37%). Healthcare (4.74%) and Finance (4.27%) remain high-value targets due to sensitive data holdings and operational criticality.

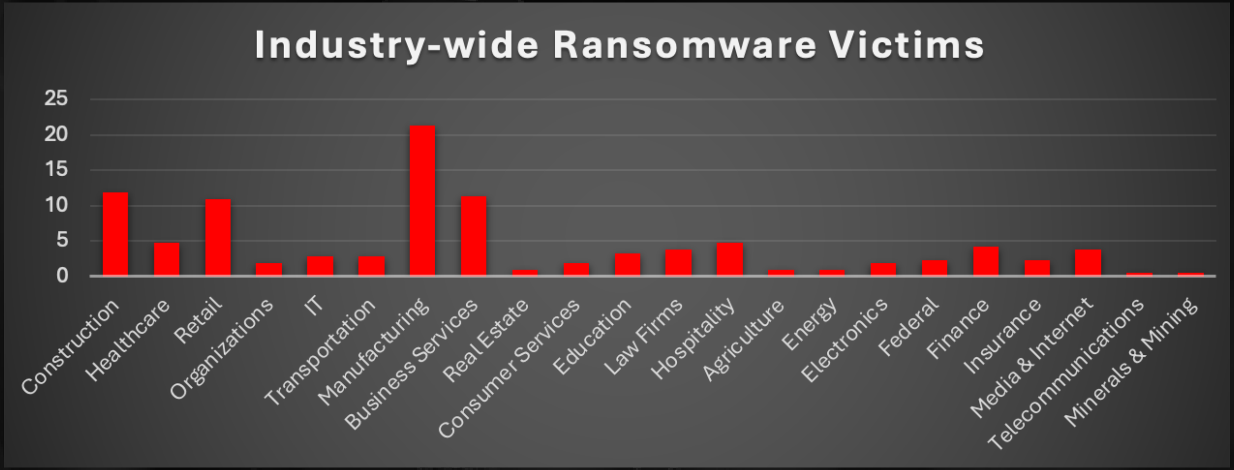


Figure 11: Industry-wide Ransomware Victims