Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 22 - 28, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Fortinet FGFM Arbitrary Code Execution (CVE-2024-23113) and Grafana DuckDB SQL Injection (CVE-2024-9264))
- **New Threat Protections - 302**

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

1. Fortinet FGFM Arbitrary Code Execution CVE-2024-23113

This critical format string vulnerability affects Fortinet FortiGate devices, primarily via the SSLVPN interface. It allows attackers to exploit unsecured format strings for remote code execution (RCE) by manipulating string inputs. Vulnerable FortiGate versions accept self-signed certificates, increasing exposure, while patched versions require certificates from trusted CAs. This complex vulnerability requires prompt patching.

Threats Protected: 01
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: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Defence Evasion	T1210	Exploitation of Remote Services
Credential Access	T1078	Valid Accounts
Impact	T1499	Endpoint Denial of Service

2. Grafana DuckDB SQL Injection (CVE-2024-9264)

This critical DuckDB SQL injection vulnerability in Grafana allows authenticated users to execute arbitrary DuckDB SQL queries, enabling file reads from the filesystem. It affects versions 11.0.0 through 11.2.1 and relies on the presence of DuckDB, which must be manually installed for exploitability.

Threats Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	RReject	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	T1190	Exploit Public-Facing Application

Known exploited vulnerabilities (Week 3 October 2024):

Vulnerability	CVSS	Description
CVE-2024-9537	9.3 (Critical)	ScienceLogic SL1 Unspecified Vulnerability
CVE-2024-38094	7.2 (High)	Microsoft SharePoint Deserialisation Vulnerability
CVE-2024-47575	9.8 (Critical)	Fortinet FortiManager Missing Authentication Vulnerability
CVE-2024-37383	6.1 (Medium)	RoundCube Webmail Cross-Site Scripting (XSS) Vulnerability
CVE-2024-20481	5.8 (Medium)	Cisco ASA and FTD Denial-of-Service Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-october-2024/514

Updated Malware Signatures (Week 3 October 2024)

Threat	Description
Zeus	Also known as Zbot, this malware is primarily designed to steal banking credentials.
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.
Vidar	A stealer designed to collect sensitive data from infected machines. It usually targets Windows-based machines and is spread through email attachments or downloads from compromised websites.

Ransomware Report

The **Red Piranha Team** actively monitors the dark web and other sources to identify organisations globally affected by ransomware attacks. In the past week, we uncovered numerous ransomware incidents across various groups, highlighting the ongoing and pervasive nature of these cyber threats. Below is the breakdown of ransomware group activities for this period.

Ransomware Groups and Attack Coverage:

Name of Ransomware Group	Percentage of new Victims last week
RansomHub	16.81%
Black Suit	9.24%
Hunters	5.88%
Cicada3301	1.68%
Sarcoma	4.20%
Everest	2.52%
Arcus Media	3.36%
Killsec	5.04%
Monti	5.88%
Ransomhouse	0.84%
Fog	9.24%
Meow	2.52%
Space Bears	0.84%
Lynx	4.20%
Rhysida	1.68%
Bianlian	2.52%
Interlock	1.68%
Eraleign (APT73)	9.24%
3AM	2.52%
Cactus	0.84%
RA Group	2.52%
Play	4.20%
Nitrogen	0.84%
Team Underground	0.84%
Hellcat	0.84%

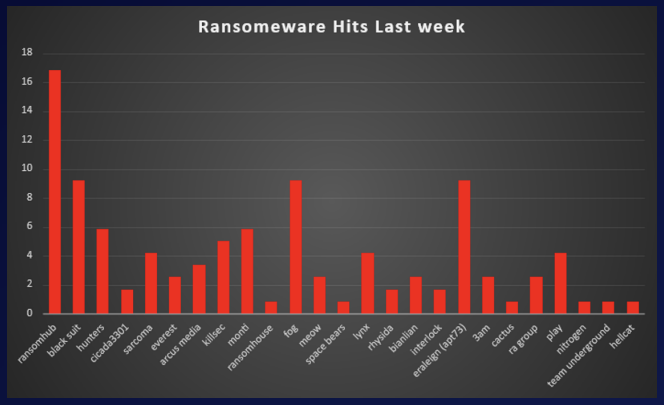

Figure 1: Ransomware Group Hits Last Week

APT73: Eraleign Ransomware

APT73, also known as Eraleign, marks itself as an "APT" (Advanced Persistent Threat), a designation it chose to align with notable groups like APT37. Originating as a spin-off from the LockBit group, APT73's operations mirror those of its predecessor, which is evident in its data leak site (DLS) setup. The group's hallmark is its ransomware DLS named "ERALEIGNEWS," located on the dark web and accessible via TOR, showcasing limited active operations compared to LockBit. APT73's first publicised target was TRIFECTA, a U.S.-based customer service platform focusing on Salesforce, suggesting a strategic selection of high-value targets. This group's DLS lacks the sophistication of LockBit's, with no active mirrors and only a single victim leak displayed, pointing to its nascent stage in the ransomware arena.

The unique aspect of APT73 is its lack of public promotion and its low-key operational style, hinting at either an early stage of victimisation or a strategy to stay under the radar until a significant number of victims are secured. Their operational base reflects a systematic approach to ransomware deployment, leveraging both direct system compromise and broader strategic data leaks to exert pressure on victims.

Detailed TTPs for APT73: Eraleign Ransomware

1. **Phishing and Exploitation**: APT73 initiates its attacks primarily through phishing, employing tactics to exploit public-facing applications, mirroring strategies used by its progenitor, LockBit.
2. **Website Cloning and Deception**: Their operational websites, including "Contact Us" and instructional pages, are clones of LockBit's, indicating shared tactics or possibly shared resources.
3. **Data Leak Site Operations**: The group's data leak site "ERALEIGNEWS" on the TOR network showcases a minimalistic operational footprint with scarce victim data, reflecting a strategic or developmental approach.
4. **TOR Network Anonymity**: They heavily rely on the TOR network for hosting and data leaks, ensuring anonymity in their operations and complicating efforts to trace their activities.
5. **Selective Targeting and Data Exfiltration**: Their targeting of specific high-value sectors like customer service platforms indicates a systematic selection process for maximum impact.
6. **Operational Security**: The lack of public promotion and low visibility in common forums suggests a cautious operational security strategy aimed at avoiding early detection by law enforcement and cybersecurity firms.

These TTPs highlight APT73's cautious yet strategic approach to establishing its presence in the ransomware landscape.

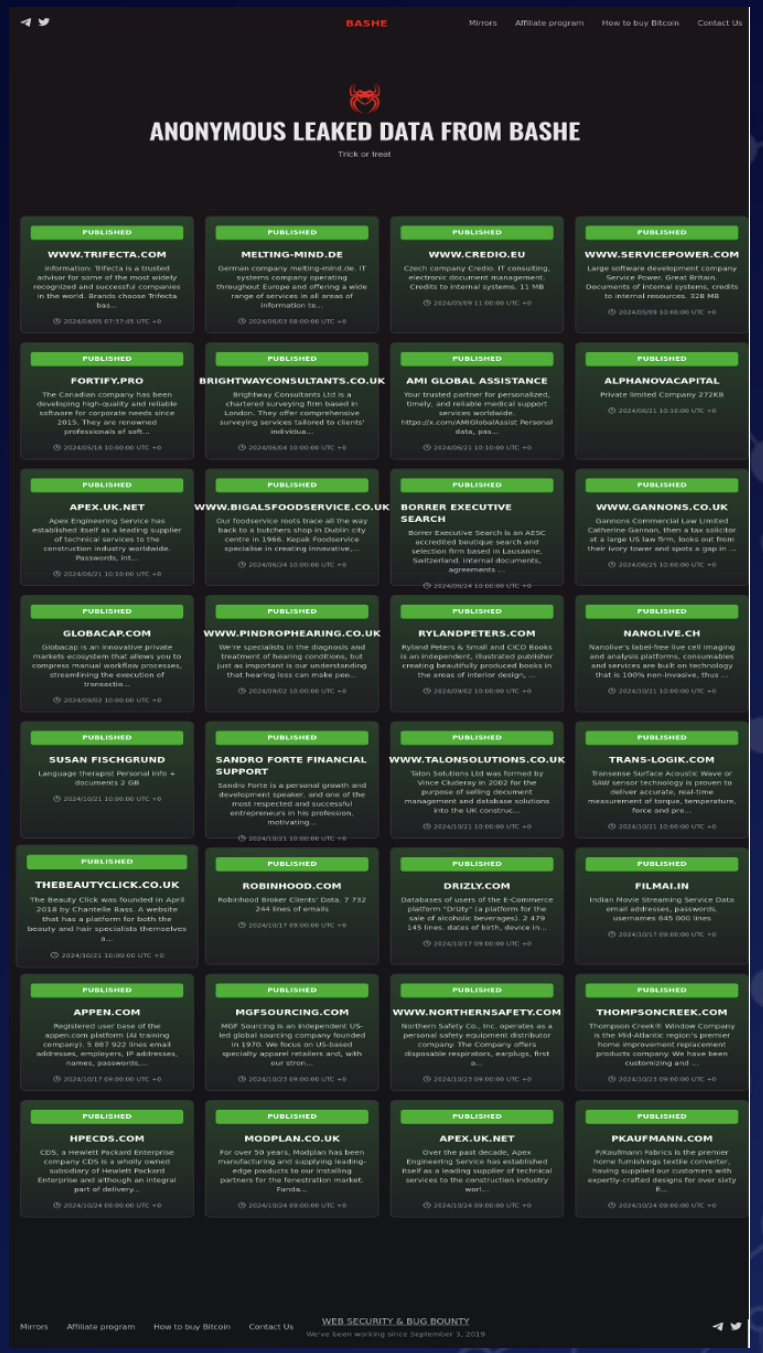

Figure 2: Screenshot of Leak Site used by APT73

Key Characteristics of APT73:

- Emergence: Surfaced in late 2023, quickly aligning itself with strategies commonly seen in LockBit and other prominent ransomware gangs.
- Use of a TOR-Based Data Leak Site (DLS): The group's data leak site (DLS), dubbed "ERALEIGNEWS," is hosted on the TOR network, making it challenging to trace their activities. While the group lacks active mirrors for their DLS, a feature typically seen in more mature ransomware operations, they are still effective in threatening victims with public exposure of stolen data.
- Ransomware Distribution: APT73 primarily employs phishing campaigns to gain an initial foothold within an organisation. From there, they compromise systems and deploy their ransomware. Their operations are opportunistic, meaning they appear to exploit unpatched systems and security weaknesses rather than leveraging more sophisticated zero-day exploits.

Modus Operandi:

- Phishing Attacks: The primary method of attack used by APT73 is phishing, likely via email with malicious attachments or links. This is a common initial access vector for ransomware groups, allowing them to gain unauthorised entry into targeted systems.
- Data Exfiltration: One of APT73's signature moves is the exfiltration of sensitive corporate data, which is later used as leverage in their extortion campaigns. The group focuses on compromising valuable files such as legal documents, client information, financial data, and internal agreements, making their threats particularly damaging to their victims.
- Threat to Leak Data: After encrypting the victim's systems, APT73 threatens to publish the stolen data on their TOR site (ERALEIGNEWS) if ransom demands are not met. This double extortion tactic increases the pressure on victims to pay the ransom.

Technical Observations:

- Phishing and Social Engineering: APT73 is likely leveraging spear-phishing techniques to target employees at high-value organisations. These phishing campaigns may involve malicious documents or URLs disguised as legitimate business communications.
- Double Extortion: APT73 employs a two-pronged approach where they not only encrypt files but also exfiltrate data to increase the leverage over their victims. The stolen data is then posted or threatened to be posted on their DLS "ERALEIGNEWS" if ransom demands are not met.
- Data Leak Site (DLS): "ERALEIGNEWS" appears amateurish in some ways, with no active mirrors—a sign of a group that may still be evolving. Despite this, the use of a TOR-based site offers them protection against easy shutdown by law enforcement.

Mitigation Strategies:

- Phishing Protection: Organisations must implement robust phishing defences, including email filtering, user education, and multi-factor authentication (MFA) to limit the success of credential theft through phishing.
- Data Encryption and Backup: Encrypt sensitive data both at rest and in transit. Regular, isolated backups can help mitigate the effects of a ransomware attack.
- Endpoint Detection and Response (EDR): Deploying strong endpoint monitoring solutions can help detect the early stages of intrusion or lateral movement within a network.
- Patch Management: Ensure systems are up-to-date with the latest security patches to avoid exploitation of known vulnerabilities.
- Below is a detailed MITRE ATT&CK-based kill chain for APT73, illustrating each phase of their attack process along with the relevant tactic, technique IDs, and names.

APT73 Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
	T1190	Exploit Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1203	Exploitation for Client Execution
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task
	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys
Privilege Escalation	T1068	Exploitation for Privilege Escalation
	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control (UAC)
Defence Evasion	T1055	Process Injection
	T1562.001	Impair Defences: Disable or Modify Tools
	T1574.002	Hijack Execution Flow: DLL Side-Loading
Discovery	T1018	Remote System Discovery
	T1083	File and Directory Discovery
	T1057	Process Discovery
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares
Collection	T1005	Data from Local System
	T1074.001	Data Staged: Local Data Staging
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
	T1105	Ingress Tool Transfer
	T1573.002	Encrypted Channel: Asymmetric Cryptography
Exfiltration	T1041	Exfiltration Over C2 Channel
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery

A recent analysis of ransomware impacts across various countries highlights the United States as the most affected, with a significant 52.1% of incidents. Following are the United Kingdom and Canada, experiencing 8.4% of attacks each. India also saw a notable percentage of 7.56%, while Australia recorded 4.2%. Lesser affected countries include Italy and Germany at 2.52% each, and Switzerland, Peru, and Belgium each reported 1.68%. Several other nations such as Malaysia, Poland, and Japan observed minimal impacts at 0.84%. This distribution underscores the global reach and varied impact of ransomware attacks.

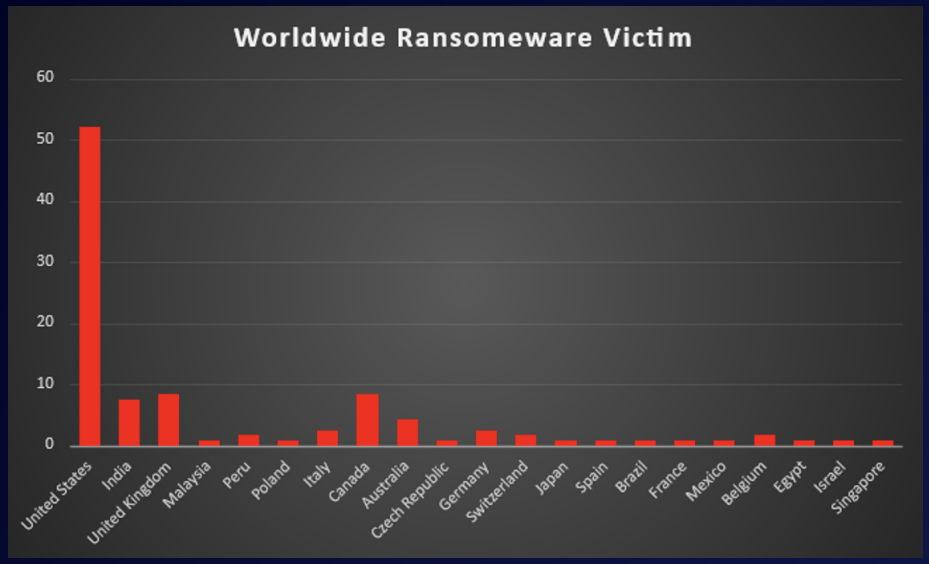

Figure 3: Ransomware Victims Worldwide

A refined analysis of recent ransomware attacks across diverse sectors shows significant impacts in Manufacturing and Construction, each accounting for 4.2% of total incidents. Business Services emerged as the most affected, with 8.4%, closely followed by Retail at 7.56%. Education and Healthcare sectors experienced 3.36% of attacks, reflecting the broad vulnerability spectrum. This data underscores the imperative for robust cybersecurity defences across all industries to mitigate the escalating threat of ransomware.

Industries	Overall Percentage
Construction	4.20%
Software	0.84%
Insurance	1.68%
Education	3.36%
Hospitals	0.84%
Elderly Care Services	0.84%
Legal Services	1.68%
Manufacturing	2.52%
Engineering & Design	1.68%
Electricity, Oil & Gas	0.84%
Hospitality	2.52%
Telecommunications	0.84%
Healthcare Services	0.84%
Business Services	8.4%
Hospitals	0.84%
Building Materials	0.84%
Retail	7.56%
Defence	0.84%
Banking	0.84%
Food & Beverage	0.84%
Industrial Machinery & Equipment	2.52%
Automotive Parts	0.84%
Chemicals	0.84%
Commercial	0.84%
Industrial Machinery	1.68%
Finance	0.84%
Transportation	0.84%
Consumer Services	0.84%
Media & Internet	0.84%
Content & Collaboration Software	0.84%
Energy, Utilities & Waste	0.84%
Chemicals & Related Products	0.84%
Non-Profit & Charitable Organisations	0.84%
Airlines Services	1.68%
Internet Services	1.68%
Architecture	0.84%
Architecture, Engineering & Design	0.84%
Hospitals & Physicians Clinics	3.36%
Furniture	0.84%
Building Materials	3.36%
Retail	1.68%
Business Services	1.68%
Financial Software	0.84%
Freight & Logistics Services	0.84%
Talon Solutions	0.84%
Manufacturing	4.20%
Household Goods	0.84%
Appliances	0.84%
Law Firms & Legal Services	2.52%
Education	2.52%
Commercial & Residential Construction	4.20%
Real Estate	0.84%
Industrial Machinery & Equipment	0.84%
Energy, Utilities & Waste	1.68%

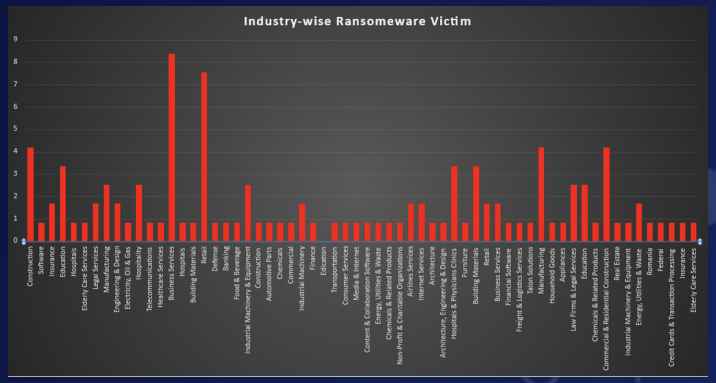

Figure 4: Industry-wise Ransomware Victims

Here are essential measures to mitigate the risk of APT73 ransomware and similar threats:

1. **Third-Party Risk Management**: Establish a comprehensive program to monitor and evaluate the security practices of third-party vendors, as ransomware often exploits weaknesses in the supply chain.
2. **Enhanced Web Security**: Implement robust web application firewalls and conduct regular vulnerability assessments, especially since APT73 has shown capabilities in website defacement.
3. **Data Backup and Recovery**: Maintain regular, encrypted, and offline backups of critical data, ensuring they are tested periodically for integrity.
4. **Patch Management**: Regularly update and patch all software and systems to close security gaps that could be exploited by ransomware.
5. **Employee Training on Phishing**: Educate employees about the dangers of phishing, which is commonly used by APT73, through regular training and simulations.
6. **Endpoint Detection and Response (EDR)**: Deploy advanced EDR systems to detect and neutralise threats at the endpoint level before they can cause damage.
7. **Network Segmentation**: Divide your network into segments to contain and limit the spread of ransomware if an intrusion occurs.
8. **Incident Response Planning**: Develop and routinely test an incident response plan tailored to ransomware threats to ensure quick and effective action when needed.

These strategies provide a layered defence approach, crucial for protecting against sophisticated ransomware operations like those conducted by APT73.