Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 16 - 22, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Patchwork APT, Mustang Panda APT and Vidar Stealer)
- **New Threat Protections - 134**

Due to the recent significant outage at CrowdStrike, threat actors have leveraged this temporary gap in defences to execute phishing attacks. The IoCs below are recently created domains that are used by threat actors to conduct social engineering attacks. Threat actors use these domains to pose as legitimate Crowdstrike support representatives and take advantage of the urgency of the situation.

- crowdstrike-bsod[.]com
- crowdstrike0day[.]com
- crowdstrikebluescreen[.]com
- crowdstrikedoomsday[.]com
- crowdstrikedown[.]site
- crowdstrikefix[.]com
- crowdstriketoken[.]com
- crowdstuck[.]org
- fix-crowdstrike-apocalypse[.]com
- fix-crowdstrike-bsod[.]com
- microsoftcrowdstrike[.]com
- whatiscrowdstrike[.]com
- crowdfalcon-immed-update[.]com
- crowdstrikebsod[.]com
- crowdstrikeoutage[.]info
- crowdstrike-helpdesk[.]com
- crowdstrikeupdate[.]com
- crowdstrikeclaim[.]com
- crowdstrikefix[.]zip
- crowdstrikeoutage[.]com
- crowdstrikereport[.]com
- crowdstrike[.]fail
- crowdstrikebug[.]com
- crowdstrikedown[.]com
- crowdstrikefail[.]com
- crowdstrikeoopsie[.]com
- isitcrowdstrike[.]com

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

1. Patchwork APT

Patchwork APT, also known as Dropping Elephant or Quilted Tiger, is a cyber espionage group suspected to be of Indian origin. Active since at least 2014, they target high-profile entities in South and Southeast Asia, with a focus on government, defence, and diplomatic organisations. Their primary weapon is social engineering, launching spear phishing campaigns with emails tailored to deceive victims. Once a foothold is gained, Patchwork utilises custom-built tools to steal sensitive data, making them a significant threat in the cyber landscape. Their adaptability is concerning, as they've been observed expanding their targets to other regions and incorporating new techniques like watering hole attacks.

Threats Protected: 13
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and scripting Interpreter
	T1129	Shared Modules
Persistence	T1543	Create or modify system process
	T1543.003	Windows Services
Privilege Escalation	T1134	Access Token Manipulation
	T1543	Create or modify system process
	T1543.003	Windows Services
Defence Evasion	T1027	Obfuscated Files or Information
	T1036	Masquerading
	T1112	Modify Registry
Discovery	T1082	System Information Discovery
	T1016	System Network Configuration Discovery
	T1057	Process Discovery
	T1018	Remote System Discovery
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
	T1573	Encrypted Channel
Impact	T1489	Service Stop
	T1529	System Shutdown or Reboot

2. Mustang Panda APT

Mustang Panda APT, also known as TA416 or Bronze President, is a cyber espionage group believed to be China-based and active since at least 2012. They primarily target governments, NGOs, and religious organisations critical of the Chinese government, with a focus on Southeast Asia, Europe, and the US. Mustang Panda employs a mix of social engineering tactics like spear phishing emails with lures relevant to the target's interests. Once in, they deploy custom malware like PlugX variants to steal sensitive documents and maintain persistence on the system. Their attacks are known for exploiting vulnerabilities in popular software and leveraging legitimate tools for malicious purposes. By staying vigilant about suspicious emails, keeping software updated, and implementing strong password policies, organisations can help defend themselves against Mustang Panda's espionage.

Threats Protected: 17
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1106	Native API
Defence Evasion	T1027 T1497 T1497.001	Obfuscated Files or Information Virtualization/Sandbox Evasion System Checks
Credential Access	T1539 T1552	Steal Web Session Cookie Unsecured Credentials
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Lateral Movement	T1550 T1550.004	Use Alternate Authentication Material Web Session Cookies

3. Vidar Stealer

Vidar Stealer, lurking since 2018, is a nasty malware operating as Malware-as-a-Service (MaaS). This means it's readily available for purchase by cybercriminals on the dark web. Vidar targets a treasure trove of sensitive data, including login credentials, browsing history, cryptocurrency wallets, and even takes screenshots. Acting like a stealthy thief, it can also download additional malware, potentially ransomware, further compromising the infected system. This adaptability and focus on financial gain make Vidar a popular choice for cybercriminals. Be cautious of suspicious emails and downloads and keep your software up-to-date to avoid falling victim to Vidar's thievery.

Threats Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
	T1129	Shared Module
Persistence	T1547	Boot or Logon Autostart Execution
Privilege Escalation	T1547.009	Shortcut Modification
Defence Evasion	T1027	Obfuscated Files or Information
	T1112	Modify Registry
Credential Access	T1056	Input Capture
	T1056.001	Keylogging
Discovery	T1010	Application Window Discovery
	T1012	Query Registry
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1056	Input Capture
	T1056.001	Keylogging
	T1115	Clipboard Data
	T1125	Video Capture
Impact	T1529	System Shutdown/Reboot

Known exploited vulnerabilities (Week 3 July 2024):

Vulnerability	CVSS	Description
CVE-2024-36401	9.8 (Critical)	OSGeo GeoServer GeoTools Eval Injection Vulnerability
CVE-2022-22948	6.5 (Medium)	VMware vCenter Server Incorrect Default File Permissions Vulnerability
CVE-2024-28995	8.6 (High)	SolarWinds Serv-U Path Traversal Vulnerability
CVE-2024-34102	9.8 (Critical)	Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-july-2024/488

Updated Malware Signatures (Week 3 July 2024)

Threat	Description
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.
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 actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered new ransomware victims and updates on previous victims across 18 industries spanning 23 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

LockBit3.0 ransomware group stands out as the most prolific, having updated a significant number of victims (18%) distributed across multiple countries. In comparison, Ransomhub ransomware updated 10% of victims, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

Name of Ransomware Group	Percentage of new Victims last week
Abyss-Data	0.96%
Akira	1.92%
Arcus Media	0.96%
Bianlian	1.92%
Black Suit	1.92%
Blackbasta	3.85%
Blackbyte	0.96%
Blackout	0.96%
Cactus	1.92%
Cicada3301	0.96 %
Donutleaks	2.88%
Dragonforce	0.96%
Dunghill	0.96%
Everest	1.92%
Fog	6.73%
Handala	1.92%
Hunters	8.65%
Inc Ransom	3.85%
Lockbit3	18.27%
Mad Liberator	4.81%
Mallox	1.92%
Meow	7.69%
Nullbulge	2.88%
Play	1.92%
Qilin	0.96%
Ransomcortex	0.96%
Ransomexx	0.96%
Ransomhouse	0.96%
Ransomhub	10.58%
Rhysida	2.88%
Space Bears	0.96%

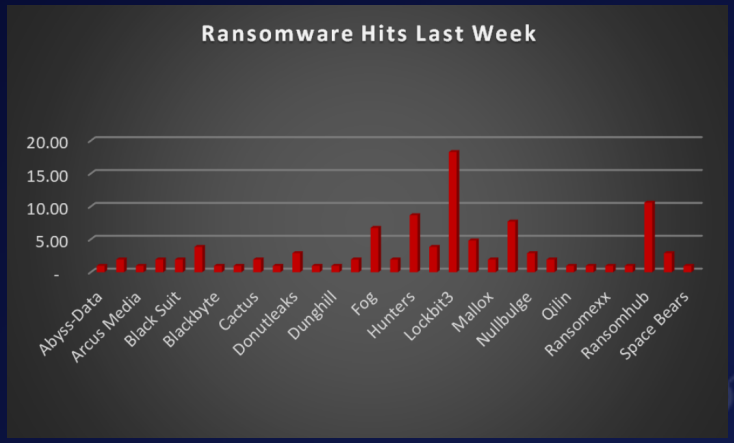


Figure 1: Ransomware Group Hits Last Week

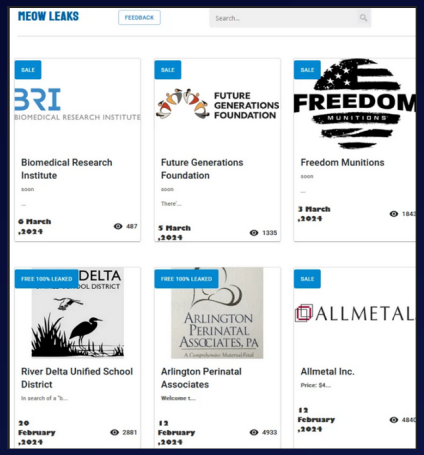
Meow Ransomware

First detected in the wild around August 2022, Meow Ransomware quickly established itself as a cunning adversary in the cybercrime landscape. This feline-themed malware utilises a double extortion tactic, crippling victims by encrypting their data and threatening to leak it on the dark web if ransom demands aren't met. While the exact origins of Meow Ransomware remain shrouded in some mystery, security researchers believe it may be linked to a cybercriminal group previously operating under names like MeowCorp, MeowLeaks, or simply Meow. This group initially leveraged the LockBit ransomware strain, but Meow Ransomware itself appears to be a distinct evolution with its own set of characteristics.

Tactics, Techniques, and Procedures (TTPs):

Meow Ransomware doesn't rely on brute force alone. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems, showcasing a level of planning and strategy. Here's a glimpse into its malicious toolkit:

- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a common entry point. These emails may appear to be playful or lighthearted, leveraging the "Meow" theme to disguise their malicious intent. They can appear to be from colleagues, delivery companies, or even greetings for special occasions.
- Exploiting Unpatched Vulnerabilities: Meow actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This underscores the importance of keeping all software and systems updated with the latest security patches.
- Remote Desktop Protocol (RDP) Exploitation: Similar to other ransomware strains, Meow can exploit weaknesses in RDP configurations to gain access to a system. RDP allows remote access to a computer, and misconfigured settings can create a vulnerability for attackers.
- Living-off-the-Land Techniques: Like many malware strains, Meow can utilise legitimate system administration tools for malicious purposes. This makes detection more challenging as these tools may appear as normal system activity. Read more on LOTL Techniques.
- Data Exfiltration: Before encryption, Meow often exfiltrates sensitive data like financial records, personal information, and intellectual property. This stolen data serves as additional leverage in extortion attempts, putting pressure on victims to pay the ransom.
- Strong Encryption: The malware utilises robust encryption algorithms to render files inaccessible. Decrypting them without the attacker's key is extremely difficult, if not impossible. This effectively cripples a victim's operations until a decision is made.
- Data Leak Site: Meow maintains a data leak site on the dark web where they list victims who haven't paid the ransom. This serves as a public shaming tactic and adds pressure on compromised organisations.



A Global Reach with Focused Targets

Meow Ransomware demonstrates a global reach, targeting victims worldwide. Here are some examples of its operations and the impact it has caused:

- Focus on Small and Medium Businesses (SMBs): Security researchers have observed a trend of Meow targeting SMBs. These organisations may have less robust cybersecurity measures compared to larger enterprises, making them more vulnerable to attack.
- Critical Infrastructure Concerns: Despite its playful facade, there have been concerns about Meow targeting critical infrastructure sectors like power grids or transportation systems. A successful attack on such infrastructure could have devastating consequences.

Ransom Note: The encrypted files bore the ".MEOW" extension, and the ransom note was named "readme.txt.

```
MEOW! MEOW! MEOW!

Your files has been encrypted!

Need decrypt?  Write to e-mail:

meowcorp2022@aol.com

meowcorp2022@proton.me

meowcorp@msgsafe.io

meowcorp@onionmail.org

or Telegram:

@meowcorp2022

@meowcorp123

Uniq ID: eabc2ef6-246a-482c-8c20-
c306d0adad06
```

The emergence of Meow Ransomware underscores the ever-evolving threat landscape of cybercrime. Its use of social engineering tactics with a playful theme, combined with its focus on data exfiltration and a dedicated data leak site, highlights the need for organisations to prioritise robust cybersecurity measures and user awareness training. Here are some crucial steps organisations can take to mitigate the risk of Meow Ransomware and similar threats:

- **Security Awareness Training**: Educate employees on identifying phishing attempts, particularly those that use social engineering tactics that may seem lighthearted or playful.
- **Phishing Simulations**: Conduct simulated phishing attacks to identify vulnerabilities in employee awareness and response.
- Multi-Factor Authentication (MFA): Enable MFA for all user accounts wherever possible. MFA adds an extra layer of security by requiring a second verification factor beyond just a username and password.
- Endpoint Security Solutions: Deploy endpoint security solutions that can detect and prevent malware infections at the device level. These solutions can act as a first line of defence against Meow and other malware threats.

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
	T1133	External Remote Services
	T1566	Phishing
Execution	T1129	Shared Modules
Defence Evasion	T1027	Obfuscated Files or Information
	T1027.005	Indicator Removal from Tools
	T1036	Masquerading
	T1497	Virtualization/Sandbox Evasion
Credential Access	T1056	Input Capture
Discovery	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1497	Virtualization/Sandbox Evasion
	T1518.001	Security Software Discovery
Lateral Movement	T1080	Taint Shared Content
Collection	T1056	Input Capture
Command-and-Control	T1071	Application Layer Protocol
	T1573	Encrypted Channel
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://meow6xanhzfci2gbkn3lmbqq7xjjufskkdfocqdngt3ltvzgqpsg5mid.onion/ hxxp://totos7fquprkecvcsl2jwy72v32glgkp2ejeqlnx5ynnxvbebgnletqd.onion	URLs (Onion)	Leak Site
8f154ca4a8ee50dc448181afbc95cfd7 4dd2b61e0ccf633e008359ad989de2ed 3eff7826b6eea73b0206f11d08073a68 1d70020ddf6f29638b22887947dd5b9c 033acf3b0f699a39becdc71d3e2dddcc 0bbb9b0d573a9c6027ca7e0b1f5478bf	Hash	Malicious File

In a comprehensive analysis of ransomware victims across 23 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 58% of victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

Industry	Victims Count (%)
Australia	3.85%
Bolivia	0.96%
Brazil	1.92%
Canada	5.77%
Egypt	0.96%
France	1.92%
Germany	2.88%
Greece	1.92%
India	0.96%
Israel	0.96%
Italy	2.88%
Kenya	0.96%
Malaysia	0.96%
Netherlands	2.88%
Oman	0.96%
Poland	0.96%
Singapore	0.96%
South Africa	0.96%
Spain	1.92%
Switzerland	0.96%
UK	4.81%
USA	57.69%
Zimbabwe	0.96%

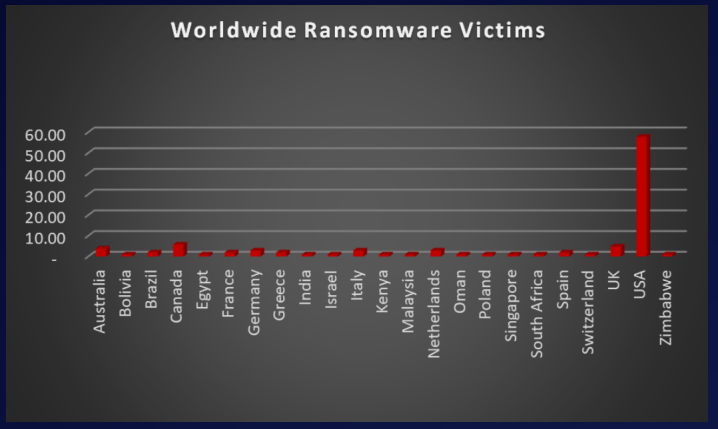


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 18 different industries worldwide. Notably, Manufacturing and Business Services bore the brunt of the attacks in the past week, accounting for 17% of victims each.

Industry	Victims Count (%)
Business Services	17.31%
Construction	3.85%
Consumer Services	2.88%
Education	7.69%
Energy, Utilities & Waste Treatment	2.88%
Finance	2.88%
Government	6.73%
Healthcare	6.73%
Hospitality	2.88%
IT	5.77%
Legal Services	6.73%
Manufacturing	17.31%
Media & Internet	1.92%
Organisations	1.92%
Real Estate	0.96%
Retail	6.73%
Telecom	3.85%
Transportation	0.96%

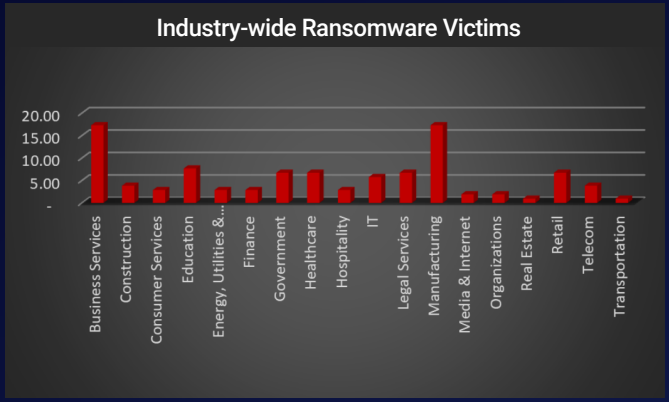


Figure 5: Industry-wide Ransomware Victims