Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 15 - 21, 2025

Report Summary:

- **New Threat Detection Added** – 3
  - CrushFTP - CVE-2025-31161
  - Totolink A3700R
  - D-Link DIR-605L/DIR

- **New Threat Protections - 244**

The following threats were added to Crystal Eye this week:

1. CrushFTP

CVE-2025-31161 is a critical severity vulnerability allowing attackers to control how user authentication is handled by CrushFTP managed file transfer (MFT) software. We strongly recommend patching immediately to avoid affected versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0. Successful exploitation of CVE-2025-31161 would give attackers admin-level access across the CrushFTP application for further compromise. This blog outlines our re-created proof-of-concept for CVE-2025-31161 and attackers' use of both legitimate and malicious RMM tooling for post-exploitation activities.

Threat 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: Trojan-activity

Kill Chain:

Tactic	Technique	Description
Initial Access	[T1190] Exploit Public-Facing Application	Exploited a race condition in CrushFTP's AWS4-HMAC authorisation to bypass authentication and gain admin access via HTTP(S).
Execution	[T1059.001] Command and Scripting Interpreter: PowerShell	Used PowerShell scripts for post-exploitation activities, including downloading and executing payloads.
	[T1203] Exploitation for Client Execution	Deployed MeshCentral agents and AnyDesk for remote code execution and persistence.
Persistence	[T1136.001] Create Account: Local Account	Created backdoor accounts within CrushFTP for persistent access.
	[T1547.001] Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder	Configured MeshCentral agents to start automatically upon system boot.
Privilege Escalation	[T1068] Exploitation for Privilege Escalation	Leveraged administrative access to escalate privileges within the system.
Defence Evasion	[T1036.005] Masquerading: Match Legitimate Name or Location	Used AnyDesk and MeshCentral, legitimate remote management tools, to avoid detection.
	[T1027] Obfuscated Files or Information	Employed obfuscated PowerShell commands to hinder analysis and detection.
Credential Access	[T1555.003] Credentials from Password Stores: Credentials from Web Browsers	Potentially accessed stored credentials through administrative privileges.
Discovery	[T1083] File and Directory Discovery	Enumerated files and directories to identify valuable data.
	[T1057] Process Discovery	Monitored running processes to understand the system environment.
Lateral Movement	[T1021.001] Remote Services: Remote Desktop Protocol	Utilised AnyDesk for lateral movement across systems.
Command-and-Control	[T1105] Ingress Tool Transfer	Transferred additional tools and malware to the compromised systems.
	[T1071.001] Application Layer Protocol: Web Protocols	Communicated with command-and-control servers over HTTP(S).
Exfiltration	[T1041] Exfiltration Over C2 Channel	Exfiltrated data through established command and control channels.
Impact	[T1486] Data Encrypted for Impact	Potential deployment of ransomware to encrypt data and disrupt operations.

2. Totolink A3700R

A protection mechanism failure in Windows BitLocker allows an unauthorised attacker to bypass a security feature with a physical attack.

Threat Protected: 03
Rule Set Type:

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

Class Type: Exploit Kit

- For CVE-2025-26637: Ensure physical security measures are in place to prevent unauthorised access to devices. Regularly update systems with the latest security patches provided by Microsoft.
- For CVE-2025-3668: Update the TOTOLINK A3700R router firmware to the latest version. If a patch is unavailable, consider replacing the router with a model that receives regular security updates.

Kill Chain:

Tactic	Technique	Description
Initial Access	[T1190] Exploit Public-Facing Application	The attacker exploits the vulnerable setScheduleCfg function via the router's web interface to gain unauthorised access.
Execution	[T1059.003] Command and Scripting Interpreter: Windows Command Shell	Post-exploitation, the attacker may execute arbitrary commands on the device.
Persistence	[T1136.001] Create Account: Local Account	The attacker may create new user accounts to maintain access.
Defence Evasion	[T1562.004] Impair Defences: Disable or Modify System Firewall	The attacker may alter firewall settings to allow further malicious activities.
Impact	[T1499] Endpoint Denial of Service	The attacker could disrupt network services by modifying router configurations.

3. D-Link DIR-605L/DIR

This vulnerability exists in the /goform/formAdvFirewall endpoint of the router's Firewall Service component. Due to improper access controls, an attacker on the local network can manipulate this endpoint to gain unauthorised access or modify firewall settings without authentication.

Threat Protected: 01

- CVE-2025-2546 – Improper Access Control in Firewall Service
  Affected Products: D-Link DIR-618 and DIR-605L routers, firmware versions 2.02 and 3.02
  Vulnerability Details: This vulnerability exists in the /goform/formAdvFirewall endpoint of the router's Firewall Service component. Due to improper access controls, an attacker on the local network can manipulate this endpoint to gain unauthorised access or modify firewall settings without authentication.
  - Impact: Exploitation can lead to unauthorised configuration changes, potentially compromising network security.
  - CVSS Scores:
    - CVSS v3.1: 4.3 (Medium)
    - CVSS v4.0: 5.3 (Medium)
  - CWE Identifiers:
    - CWE-266: Incorrect Privilege Assignment
    - CWE-284: Improper Access Control
  - Exploit Availability: A public proof-of-concept exploit has been disclosed, increasing the risk of exploitation.
  - Support Status: The affected router models are no longer supported by the manufacturer, and no official patches are available.
- CVE-2025-2553 – Improper Access Control in Virtual Server Configuration
  - Affected Products: D-Link DIR-618 and DIR-605L routers, firmware versions 2.02 and 3.02
  - Vulnerability Details: This issue is present in the /goform/formVirtualServ endpoint, responsible for virtual server configurations. Similar to CVE-2025-2546, improper access controls allow a local network attacker to manipulate this endpoint without proper authentication, leading to unauthorised changes in virtual server settings.
  - Impact: Attackers can alter virtual server configurations, potentially exposing internal services to external networks or disrupting existing services.
  - CVSS Scores:
    - CVSS v3.1: 4.3 (Medium)
    - CVSS v4.0: 5.3 (Medium)
  - CWE Identifiers:
    - CWE-266: Incorrect Privilege Assignment
    - CWE-284: Improper Access Control
  - Exploit Availability: A public proof-of-concept exploit has been released, posing a significant security risk.
  - Support Status: As with CVE-2025-2546, these router models are no longer supported, and no official fixes are provided.

Rule Set Type:

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

Class Type: Trojan activity

- CVE-2025-2546: Affects the /goform/formAdvFirewall endpoint in D-Link DIR-618 and DIR-605L routers (firmware versions 2.02/3.02). The vulnerability allows improper access controls, enabling unauthorised modifications to firewall settings.
- CVE-2025-2553: Targets the /goform/formVirtualServ endpoint in the same router models and firmware versions. Similar to CVE-2025-2546, it permits unauthorised access, allowing attackers to manipulate virtual server configurations.

Tactic	Technique	Description
Initial Access	[T1190] Exploit Public-Facing Application	Exploitation of improper access controls in the /goform/formAdvFirewall and /goform/formVirtualServ endpoints allow attackers on the local network to gain unauthorised access to the router's administrative functions.
Execution	[T1059] Command and Scripting Interpreter	Upon gaining access, attackers may execute arbitrary commands or scripts to manipulate router settings or deploy malicious payloads.
Persistence	[T1543] Modify System Configuration	Attackers can alter firewall rules or virtual server configurations to maintain persistent access or create backdoors.
Privilege Escalation	[T1548] Abuse Elevation Control Mechanism	By exploiting these vulnerabilities, attackers can escalate privileges, gaining administrative control over the router.
Defence Evasion	[T1027] Obfuscated Files or Information	Attackers may obfuscate configuration changes or malicious scripts to avoid detection.
Impact	[T1498] Network Denial of Service	Malicious modifications to firewall or virtual server settings can disrupt network services, leading to denial-of-service conditions.

Known exploited vulnerabilities (Week 3 - April 2025)

CISA (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

Vulnerability	CVSS	Description
CVE-2025-31200	7.5 (High)	Apple iOS, iPadOS, macOS, and other Apple products contain a memory corruption vulnerability that allows for code execution when processing an audio stream in a maliciously crafted media file.
CVE-2025-31201	6.8 (Medium)	Apple iOS, iPadOS, macOS, and other Apple products contain an arbitrary read-and-write vulnerability that allows an attacker to bypass Pointer Authentication.
CVE-2025-24054	6.5 (Medium)	Microsoft Windows NTLM contains an external control of file name or path vulnerability that allows an unauthorised attacker to perform spoofing over a network.

Updated Malware Signatures (Week 3 - April 2025)

Threat	Description
Gholoader	Gholoader is a JavaScript-based malware loader associated with the SocGholish campaign, which utilises fake browser update prompts to deceive users into downloading malicious files. This malware is typically delivered through compromised legitimate websites that have been injected with malicious JavaScript code.
SonicWall Command Injection	The SonicWall SMA Post-Auth sitecustomisation CGI Command Injection vulnerability refers to a remote command injection flaw affecting SonicWall Secure Mobile Access (SMA) appliances. This vulnerability exists in the sitecustomisation CGI component and requires authentication (i.e., the attacker must be logged in or have valid session credentials).
Lumma Stealer	The alert “Win32/Lumma Stealer Related CnC Domain in DNS Lookup (shiftvc[.]digital)” indicates that a system on your network attempted to resolve a domain known to be associated with the Lumma Stealer malware family. Specifically, it attempted a DNS lookup for shiftvc.digital, which is a command-and-control (C2) or exfiltration domain used by Lumma Stealer.

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	Overall Percentage of total attack coverage
Inc ransom	4.26%
Leaked Data	5.67%
Lockbit3.0	4.96%
Qilin	10.64%
Crypto24	0.71%
Rhysida	1.42%
Lynx	7.8%
Termite	0.71%
NightSpire	4.96%
Devman	0.71%
Akira	9.93%
Medusa	4.26%
Dragonforce	8.51%
Play	7.8%
RAlord	2.84%
WikiLeaksv2	0.71%
Chaos	0.71%
Nitrogen	1.42%
Team Underground	0.71%
Clop	0.71%
SafePay	8.51%
Kairos	0.71%
Sarcoma	3.55%
Space Bears	1.42%
Hunters	0.71%
Money Message	0.71%
Cloak	3.55%
RansomHouse	0.71%
Skira Team	0.71%

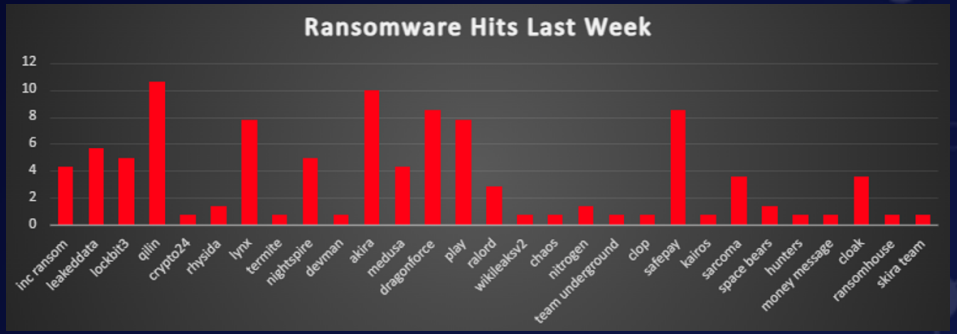

Figure 1: Ransomware Group Hits Last Week

Maui Ransomware Group

Maui is a manually operated ransomware strain first identified in early 2021 and attributed to North Korean state-sponsored threat actors. Unlike ransomware-as-a-service (RaaS) models, Maui does not automatically display ransom notes or exfiltrate data. Instead, it is designed for targeted attacks against critical infrastructure, particularly within the healthcare sector. Its operations are human-driven at every stage—from deployment to ransom negotiation—reflecting a highly curated approach.

Although not equipped with automated features such as lateral movement or backup deletion, Maui's encryption mechanisms are sophisticated and highly disruptive. The ransomware is typically executed with command-line arguments, targeting specific directories and encrypting data using a hybrid AES-RSA scheme. Its selective and stealthy behaviour, coupled with the absence of widespread campaigns, signals a strategic focus on high-value targets.

Detailed TTPs

Initial Access
North Korean actors gain entry via spear-phishing campaigns or exposed RDP services. The FBI and CISA have highlighted that, although no universal initial access vector has been confirmed, phishing and RDP exploitation remain consistent with previous nation-state tactics.

Persistence & Lateral Movement
Once inside, attackers establish persistence using valid credentials or by creating local accounts. Tools like Cobalt Strike, Empire, and Metasploit are employed for post-exploitation control, lateral movement, and privilege escalation.

Execution
Maui is launched manually using command-line instructions (maui.exe <target directory>). Operators specify parameters such as thread count and logging directories, confirming hands-on execution.

Encryption Behaviour
Maui uses:

- AES-128 (CBC mode) for per-file encryption
- RSA encryption for AES keys
- XOR obfuscation of key files
  It writes encrypted data to .tmp files before renaming them and generates an execution log (maui.log), which is exfiltrated along with the RSA private keys for later decryption post-payment.

Command & Control
Maui does not feature built-in C2 communication. Instead, attackers leverage external tools like Cobalt Strike to maintain remote control, often communicating over HTTPS to blend in with normal traffic.

Impact
The impact centres on data encryption (T1486) and disruption of services, particularly healthcare operations. Maui does not delete backups but may disable or remove them manually. The lack of data exfiltration shifts the focus from double-extortion to targeted ransom demands.

Tactic	Technique (ID)	Description
Initial Access	Spearphishing Attachment (T1566.001)	Phishing emails with malicious attachments or links.
Initial Access	External Remote Services – RDP (T1133)	Use of weak or stolen RDP credentials to gain access.
Execution	Command & Scripting Interpreter (T1059.003)	Manual CLI-based execution of maui.exe
Persistence	Valid Accounts (T1078)	Attackers reuse or steal legitimate user credentials.
Persistence	Create Account (T1136) (possible)	Potential creation of new accounts for persistent access.
Defence Evasion	Masquerading (T1036)	Executable renamed to evade detection (e.g. aui.exe).
Defence Evasion	Obfuscated Files or Information (T1027)	XOR encoding of RSA keys.
Credential Access	Credentials from Password Stores (T1555) (suspected)	Likely use of credential dumping tools like Mimikatz.
Discovery	Network Share Discovery (T1135)	Manual identification of valuable file shares.
C2	Ingress Tool Transfer (T1105)	Uploading of Maui or other tools via SMB.
C2	Application Layer Protocol (T1071.001)	Cobalt Strike beacons over HTTPS.
Impact	Data Encrypted for Impact (T1486)	Strong AES-RSA encryption renders files inaccessible.
Impact	Inhibit System Recovery (T1490) (partial)	Backup deletion is manual, not automated.

IOCs
c90d3b0d0a8751edc16e3e8e16ce5e1167e195e1245783c36b3f4517f611077b
e5734713f2d7dd70aa7a3e0cb4c30e937e1a4a72e76126bc828c5b68205e8d2a
d8f0835e3c0cebc2a0d7f26dfcae3d43c54f3d5a9a8e6314ff861f1ce56fe3d0

Filenames:
maui.exe
aui.exe
maui.key
maui.evd
maui.log
*.tmp - Temporary files created during the encryption process

Mitigation Strategies

- Endpoint Detection & Response (EDR): Use behaviour-based EDRs like SentinelOne or CrowdStrike to catch CLI encryption behaviours and automatically roll back changes.
- Patch Management: Regularly patch VPN/RDP services and internal applications to prevent exploitation.
- Network Segmentation: Isolate critical systems and implement strict access controls to hinder lateral movement.
- Multi-Factor Authentication (MFA): Enforce MFA for all administrative and remote access accounts.
- User Awareness Training: Train staff to detect and report phishing attempts to reduce the risk of initial access.
- Credential Hygiene: Regularly audit and disable unused accounts. Use strong, unique credentials.
- Backup and Disaster Recovery: Maintain offline, immutable backups and test restore procedures frequently.
- Monitoring and Incident Response: Deploy SIEMs and threat-hunting tools. Monitor for the presence of maui.exe, maui.log, or related indicators.

Ransomware Victims Worldwide

A recent analysis of the global ransomware threat landscape indicates that the United States continues to be the most heavily impacted nation, accounting for a staggering 58.16% of all reported ransomware incidents. This reinforces the country's position as a prime target for financially and politically motivated threat actors.

Germany ranks second, experiencing 9.22% of global attacks — a sharp indication of the country's exposure within the European economic and industrial sphere. Canada follows with 4.96%, while the United Kingdom reports 4.26%, reflecting persistent threats across North American and Western European nations.

Several other countries also show notable ransomware activity. Spain and Italy each report 2.84% of incidents, while Portugal is close behind at 2.13%, highlighting a broader European trend. Australia, Norway, Brazil, and Switzerland each recorded 1.42%, suggesting ransomware groups are diversifying their target selection across regions and verticals.

A range of countries reported moderate to low levels of incidents, each contributing 0.71% of global ransomware cases. These include Vietnam, Chile, Argentina, Luxemburg, Indonesia, Saudi Arabia, India, Bolivia, China, Taiwan, Netherlands, Czech Republic, Ireland, and Greece. While smaller in share, these nations' inclusion underscores the increasingly global footprint of ransomware operations.

This widespread distribution of ransomware victims emphasises the transnational nature of modern cybercrime. It calls for urgent international collaboration in intelligence sharing, the adoption of advanced threat detection mechanisms, and the strengthening of cyber resilience programs across both public and private sectors.

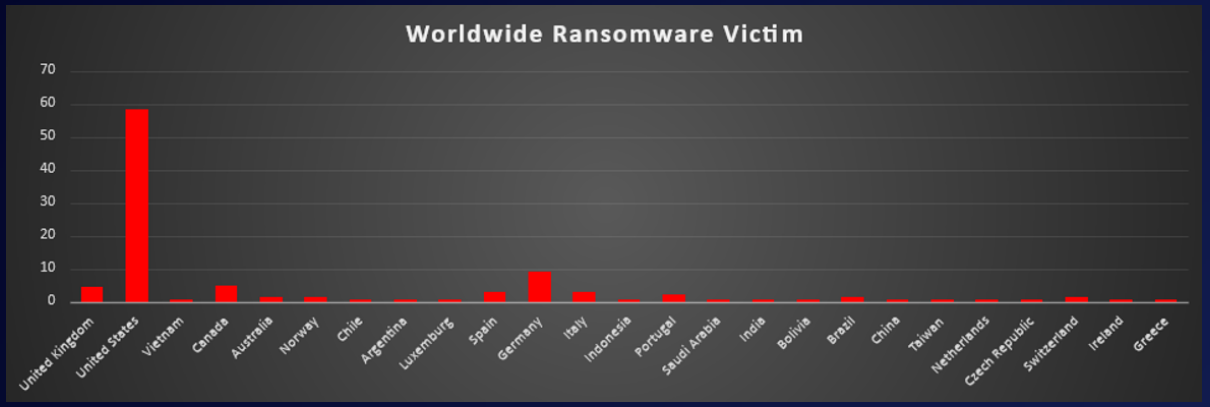

Figure 2: Ransomware Victims Worldwide

Ransomware Victims by Industry

In the most recent industry-specific analysis of ransomware activity, the Construction sector has emerged as the most targeted, accounting for 16.31% of global incidents. This sharp rise underscores persistent vulnerabilities in infrastructure development, engineering operations, and supply chain integration within the sector.

Manufacturing follows closely at 15.6%, continuing to be a major target due to its reliance on industrial control systems and just-in-time production workflows. Business Services ranks third with 12.77%, highlighting sustained targeting of consulting, outsourcing, and professional service firms that manage sensitive client data.

Retail accounts for 9.22% of incidents, signalling that consumer-facing sectors remain highly attractive to ransomware actors due to the potential for high-impact disruptions and large-scale data exposure. Law Firms reported 8.51%, reaffirming the value attackers place on confidential legal information and litigation assets.

Other significantly impacted sectors include Transportation (5.67%), Hospitality (4.26%), Consumer Services (4.26%), and Education (4.26%). These industries represent a mix of critical logistics infrastructure, customer-centric services, and institutions handling vast amounts of personally identifiable information.

Finance (3.55%), Healthcare (2.13%), Insurance (2.13%), and Agriculture (2.13%) also faced considerable ransomware threats, further reflecting attackers' focus on sectors with high-value data and operational continuity requirements.

A range of industries experienced moderate levels of targeting, including Telecommunications (1.42%), Electronics (1.42%), Energy (1.42%), Media & Internet (1.42%), and Federal (1.42%) entities. These sectors present strategic interest to attackers due to their technological or governmental relevance.

Lower yet still notable levels of ransomware activity were observed in IT (0.71%), Organisations (0.71%), and Minerals & Mining (0.71%), suggesting that even smaller or niche industries are not immune to opportunistic targeting.

This comprehensive distribution highlights ransomware's pervasive reach across all industrial domains. It reinforces the urgency for sector-specific threat models, proactive defence mechanisms, and continuous risk assessments to combat the evolving ransomware ecosystem.

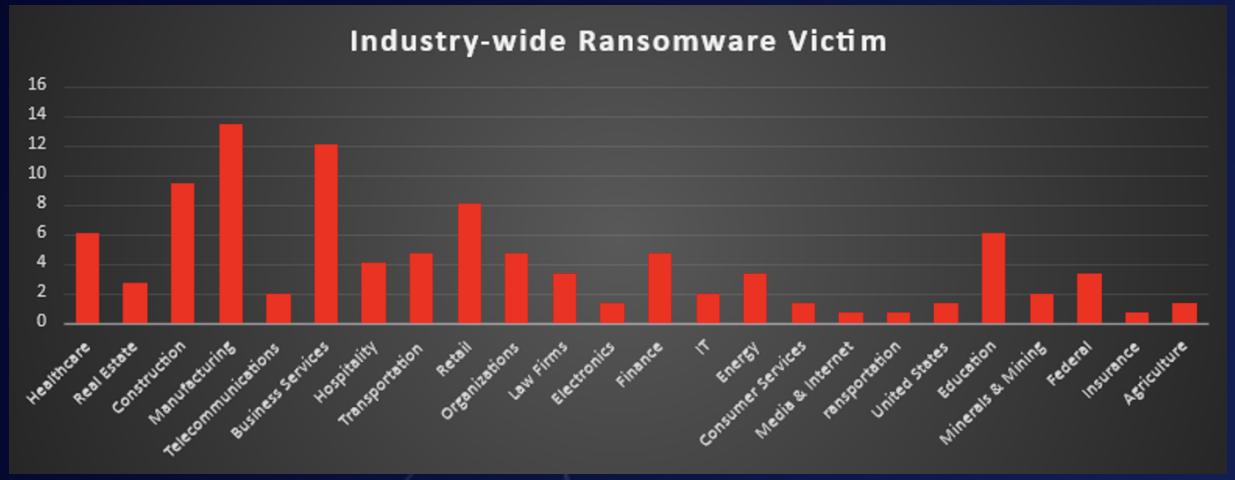

Figure 3: Industry-wide Ransomware Victims