Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 05 - 11, 2024

Report Summary:

- **New Threat Detection Added** – 2 (PTZOptics CVE-2024-8956 and Mirai Variant for IoT Exploits)
- **New Threat Protections - 140**

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

1. PTZOptics CVE-2024-8956

PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40 is vulnerable to an insufficient authentication issue. The camera does not properly enforce authentication to /cgi-bin/param.cgi when requests are sent without an HTTP Authorisation header. The result is a remote and unauthenticated attacker can leak sensitive data such as usernames, password hashes, and configuration details. Additionally, the attacker can update individual configuration values or overwrite the whole file.

Threats Protected: 02
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

2. Mirai Variant for IoT Exploits

A new variant of the Mirai botnet has emerged, exploiting multiple vulnerabilities in Internet of Things (IoT) devices to expand its botnet network. This variant incorporates several known exploits, including:

- CVE-2023-27076: Tenda G103 command injection vulnerability
- CVE-2023-26801: LB-Link command injection vulnerability
- CVE-2023-26802: DCN DCBI-Netlog-LAB remote code execution vulnerability
- Zyxel remote code execution vulnerability

By leveraging these vulnerabilities, the botnet gains unauthorised access to devices, integrating them into its network for potential malicious activities such as distributed denial-of-service (DDoS) attacks.

Threats Protected: 02
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Impact	T1499	Endpoint Denial-of-Service

Known exploited vulnerabilities (Week 1 November 2024):

Vulnerability	CVSS	Description
CVE-2024-8956	9.1 (Critical)	PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability
CVE-2024-8957	9.8 (Critical)	PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability
CVE-2019-16278	9.8 (Critical)	Nostromo nhttpd Directory Traversal Vulnerability
CVE-2024-43093	N/A – undergoing analysis	Android Framework Privilege Escalation Vulnerability
CVE-2024-5910	9.3 (Critical)	Palo Alto Expedition Missing Authentication Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-november-2024/522

Updated Malware Signatures (Week 1 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.
njRAT	A remote access trojan typically spreads using phishing emails or social engineering tactics. It allows a threat actor to steal sensitive information, install additional malware, and control the victim's machine remotely.

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	26.53%
Qilin	3.06%
Hunters	2.04%
Killsec3	9.18%
Embargo	3.06%
Bianlian	4.08%
Lynx	5.1%
INC Ransom	3.06%
Rhysida	1.02%
Meow	3.06%
Dispossessor	1.02%
Fog	2.04%
Helldown	12.24%
Clop	2.04%
Medusa	10.2%
Play	5.1%
Darkvault	1.02%
Interlock	1.02%
Space bears	1.02%
Everest	1.02%
Eraleign (APT73)	2.04%
Cactus	1.02%

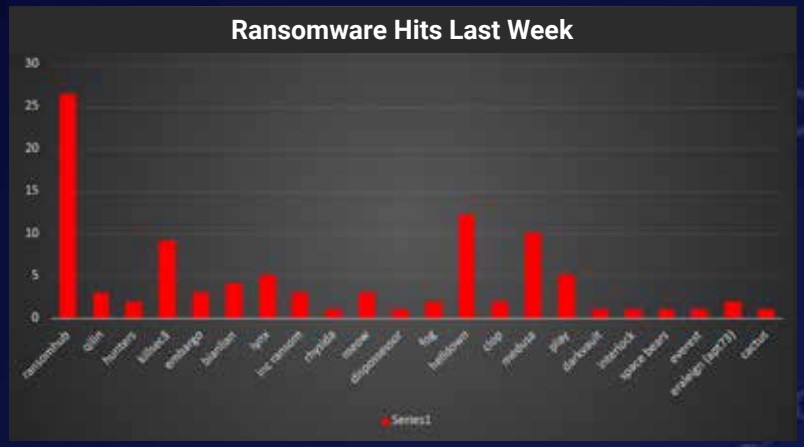

Figure 1: Ransomware Group Hits Last Week

Helldown Ransomware Group Report

The Helldown Ransomware Group is an emerging threat actor specialising in ransomware attacks across various sectors. Their operations have expanded globally, targeting multiple industries and countries. This report provides detailed insights into their activities based on recent findings.

Key Findings

- New Domain Discovered: A new domain linked to Helldown has been identified, indicating active development and expansion.
- Indicators of Compromise (IOCs): Multiple file hashes, IP addresses, and domains have been associated with the group's malicious activities.
- Targeted Industries and Countries: The group targets a wide range of industries and countries, suggesting a broad attack surface.
- Attack Techniques: Utilisation of exploitation for privilege escalation and spear phishing attachments as primary attack vectors.

Detailed Tactics and Techniques

1. Spearphishing Attachment (T1193): The group uses targeted phishing emails with malicious attachments to gain initial access to victim networks. These attachments may contain malware or exploit code that, when opened, executes malicious payloads.
2. User Execution (T1204): Requires the user to perform an action to execute the malicious code, such as opening a file or enabling macros.
3. Boot or Logon AutoStart Execution (T1547): The malware may install itself to run automatically upon system startup or user logon.
4. Exploitation for Privilege Escalation (T1068): Exploiting vulnerabilities in the operating system or installed applications to gain higher-level permissions.
5. Obfuscated Files or Information (T1027): The malware may use obfuscation techniques to hide its code and evade detection.
6. Disable Security Tools (T1562): Attempting to disable antivirus and other security solutions
7. Credential Dumping (T1003): Obtaining account credentials to move laterally within the network.
8. Network Service Scanning (T1046): Scanning the network to identify open services and potential targets.
9. Remote Service Execution (T1021): Moving between systems within the network using remote services.
10. Data from Local System (T1005): Collecting files and sensitive information from the infected system.
11. Exfiltration Over C2 Channel (T1041): Sending collected data back to the attacker over established Command-and-Control channels.

Infrastructure

- Domains and IP Addresses:
  - Domains:
    - helldown.org (surface web)
    - onyxcb44xvqra35m3lp3z26kf2pxrlbn64nbzvyvzjyc3uykzrwcjdid.onion (dark web)
  - IP Addresses:
    - Multiple IPs associated with their C2 infrastructure (e.g., 20.190.159.68, 51.11.168.232).
  - Usage:
    - Hosting Command-and-Control servers.
    - Data exfiltration points.
    - Hosting victim payment portals on the dark web.

Indicators of Compromise

FileHash-MD5	140aad1f823157222af3da2d23de8789
FileHash-MD5	5e7f5bb24a7cdaabcf3d2e77ed31fa4e
IPv4	162.255.119.18
IPv4	20.190.159.68
IPv4	20.223.35.26
IPv4	51.11.168.232
IPv4	52.168.112.66
IPv4	63.250.36.235
domain	helldown.org
domain	onyxcb44xvqra35m3lp3z26kf2pxrlbn64nbzvyvzjyc3uykzrwcjdid.onion
domain	onyxcgfg4pjevvp5h34zvhaj45kbft3dg5r33j5vu3nyp7xic3vrzvad.onion
domain	onyxcym4mjilrsptk5uo2dhesbwntuban55mvww2olk5ygqafhu3i3yd.onion
IPv4	192.229.221.95
IPv4	199.232.210.172

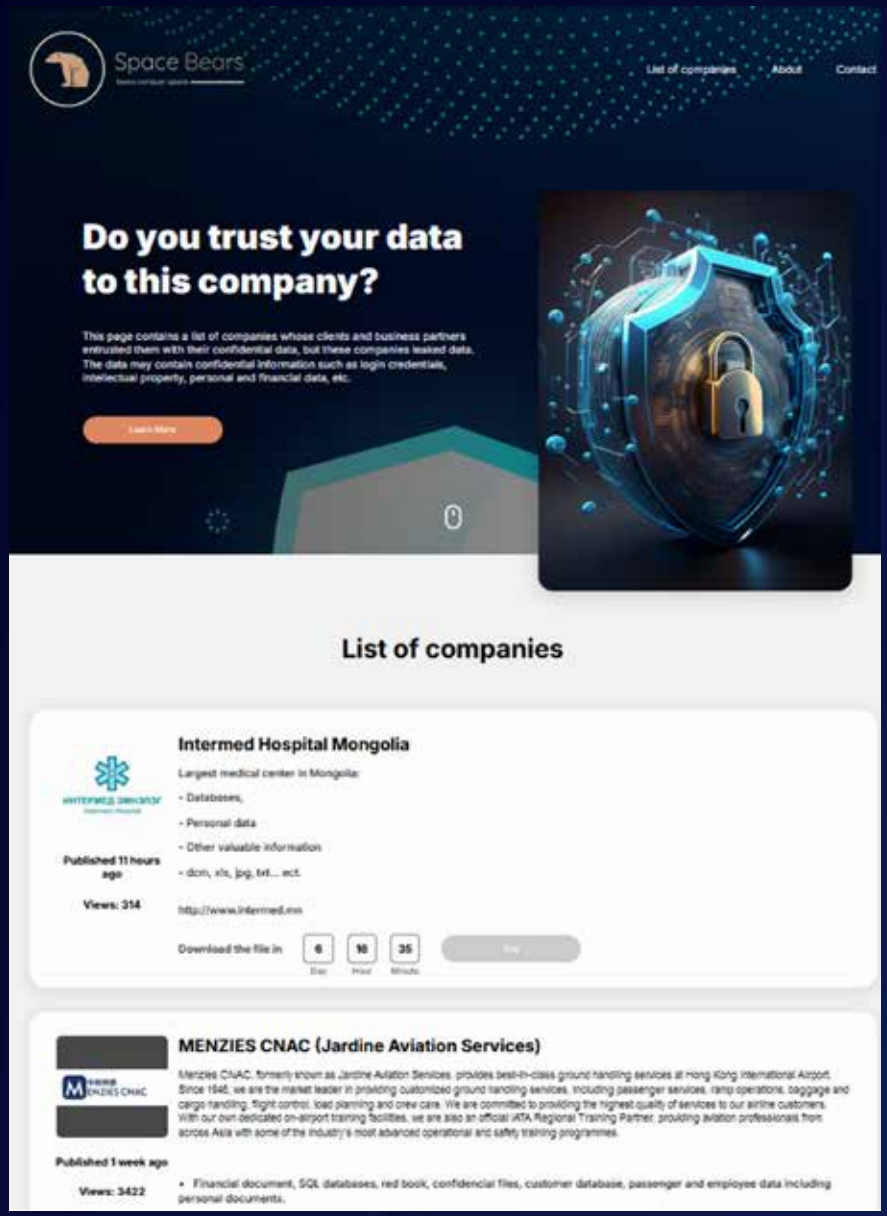

Figure 2: Screenshot of Leak Site used by Helldown

A recent analysis of ransomware impacts across various countries highlights the United States as the most affected, with a dominant 62.24% of incidents. Following are the United Kingdom, which had 6.12% of the total attacks, and India, which had 4.08%. Canada, France, and the United Arab Emirates each recorded 2.04% of total incidents. Several other nations including Taiwan, Lebanon, Argentina, Chile, Netherlands, Brazil, South Africa, Peru, Luxembourg, Germany, Switzerland, Qatar, Czech Republic, Italy, Bosnia and Herzegovina, Ireland, El Salvador, Dominican Republic, Spain, Australia, and Uruguay observed minimal impacts at 1.02% each. This distribution underscores the global reach and varied impact of ransomware attacks, with a clear concentration in North America, particularly the United States.

Figure 3: Ransomware Victims Worldwide

Analysis of ransomware impacts across various industries reveals that Manufacturing is the most affected sector, accounting for 11.22% of incidents. Close behind are the Education and Construction industries, each experiencing 10.2% of attacks. The Finance sector also faces significant risk, comprising 9.18% of incidents, while Healthcare represents 7.14%.

Other notable sectors include Business Services at 4.08%, and industries like Automotive, Electricity, Government, Real Estate, Architecture, and Chemicals, each with 3.06% of incidents. Sectors such as Retail, Law Firms, Hospitality, Technology, Legal Services, Associations, and Engineering each account for 2.04% of attacks.

A variety of other industries—including Accounting Services, Logistics Services, Non-Profits, Corporate Services, Energy, Media & Marketing, Construction Materials, and Insurance—each experienced 1.02% of incidents. This data highlights the extensive reach of ransomware attacks across multiple sectors, with particularly heavy impacts on the Manufacturing, Education, and Construction industries.

Industries	Overall Percentage
Finance	9.18%
Automotive	3.06%
Electricity	3.06%
Government	3.06%
Education	10.2%
Real Estate	3.06%
Retail	2.04%
Construction	10.2%
Law Firms	2.04%
Business Services	4.08%
Hospitality	2.04%
Healthcare	7.14%
Manufacturing	11.22%
Michigan	1.02%
Accounting Services	1.02%
Logistics Services	1.02%
Technology	2.04%
Architecture	3.06%
Non-Profit	1.02%
Legal Services	2.04%
Associations	2.04%
Chemicals	3.06%
Engineering	2.04%
Corporate Services	1.02%
Energy	1.02%
Logistics	1.02%
Media & Marketing	1.02%
Construction Materials	1.02%
Insurance	1.02%

Figure 4: Industry-wise Ransomware Victims

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

1. Email Security
   - Enhance Email Filters: Upgrade your email security to automatically detect and block phishing emails that might contain malicious attachments or links.
2. Keep Everything Updated
   - Regular Software Updates: Always keep your operating systems and software up to date. Installing the latest updates and patches fixes security vulnerabilities that hackers could exploit.
3. Protect Your Devices
   - Install Antivirus Programs: Use trusted antivirus and endpoint protection software on all devices to detect and remove malware.
   - Monitor for Threats: Keep an eye out for known signs of compromise, such as specific malicious files or unusual network activity related to Helldown.
4. Secure Your Network
   - Divide Your Network (Segmentation): Break your network into smaller, isolated sections. This way, if one part is compromised, the attacker can't easily access the rest.
   - Control Access to Sensitive Data: Limit who can access important information. Only grant permissions to those who absolutely need it for their job.
5. Strengthen Access Controls
   - Least Privilege Principle: Give employees the minimum level of access necessary to perform their duties. This reduces potential damage if an account is breached.
   - Enable Multi-Factor Authentication (MFA)
6. 6. Regular Backups
   - Backup Important Data: Consistently back up your essential data and store copies offline or in a secure cloud service that's not constantly connected to your network.
   - Test Your Backups
7. Prepare for Incidents
   - Develop an Incident Response Plan: Create a clear plan outlining the steps to take if a ransomware attack occurs. Include roles, responsibilities, and communication strategies.