Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

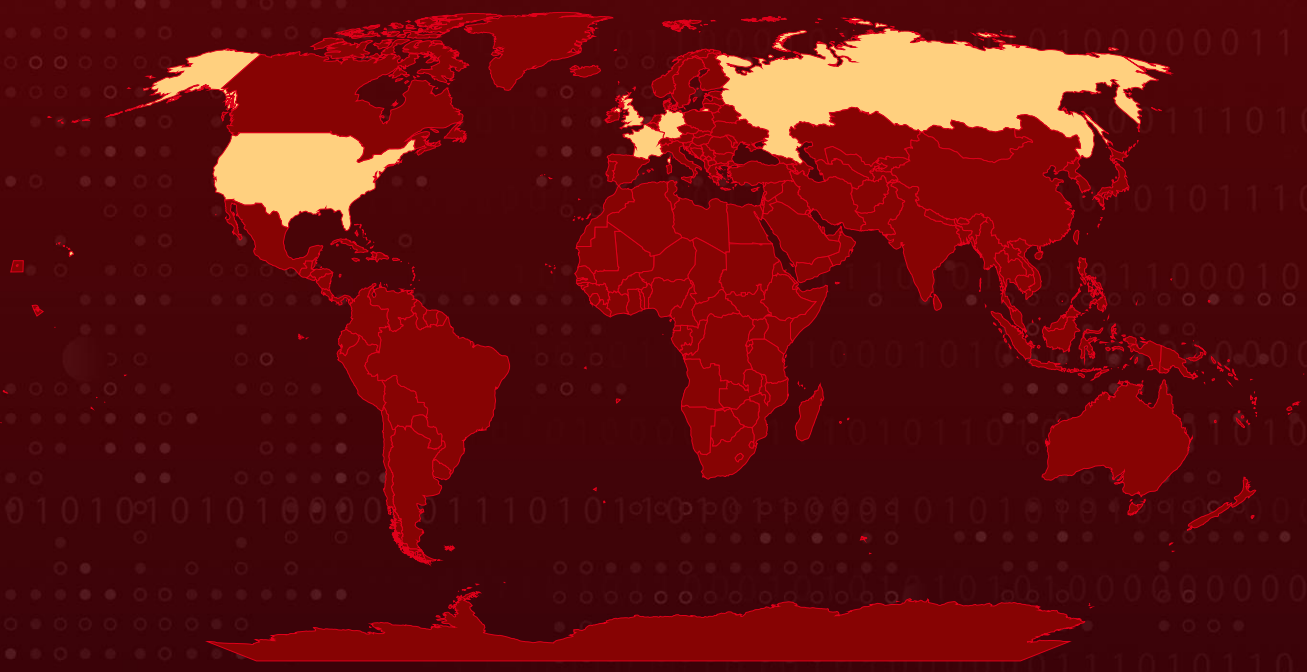
New Helldown Ransomware: A Growing Threat Across Cross-Platform Systems

Date of Publication	Admiralty Code	TA Number
November 21, 2024	A1	TA2024438

Summary

First Appearance: August 2024
Malware: Helldown ransomware
Targeted Countries: United States and Europe
Affected Platforms: Windows and Linux
Targeted Sectors: Manufacturing, Healthcare, IT services, Telecommunications
Attack: Helldown ransomware is a rising cyber threat targeting Windows and Linux systems, particularly VMware infrastructures, with a double extortion strategy of encrypting data and threatening to leak it. Exploiting vulnerabilities like CVE-2024-42057 in Zyxel firewalls, it has impacted over 30 organizations in sectors such as IT, healthcare, telecommunications and manufacturing. Helldown shares code similarities with LockBit 3.0 but remains distinct and under active development. Its evolution highlights the growing sophistication and platform diversification of ransomware threats.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-42057	Zyxel ATP series Command Injection Vulnerability	Zyxel ATP series	✗	✗	✓

Attack Details

#1 Helldown ransomware has emerged as a significant cybersecurity threat, recently expanding its focus from Windows systems to Linux environments, with a particular emphasis on VMware infrastructures. First identified in August 2024, Helldown has rapidly gained notoriety for its aggressive tactics and has been linked to attacks across various sectors, including IT services, telecommunications, manufacturing, and healthcare.

#2 This ransomware employs a double extortion strategy, encrypting data while simultaneously threatening to leak sensitive information if the ransom is not paid. This approach has reportedly impacted over 30 companies within a short period, underscoring the urgent need for organizations to bolster their defenses.

#3 Helldown's attack sequence typically begins with the exploitation of vulnerabilities in Zyxel firewalls, such as CVE-2024-42057, which allows attackers to execute commands without authentication. Once access is gained, the attackers engage in credential harvesting and lateral movement within the network, compromising additional systems in the process.

#4 After establishing a foothold, the ransomware is deployed to scan for files to encrypt. A notable feature of the Linux variant is its ability to terminate active virtual machines before encryption, although this capability appears underutilized in its current implementation. This calculated approach enables attackers to maximize damage while minimizing the chances of early detection.

#5 Helldown shares code lineage with LockBit 3.0 and exhibits behavioral similarities with other ransomware strains like DarkRace and DoNex, although definitive links remain unconfirmed. The rise of Helldown highlights the increasing diversification of ransomware threats across platforms. Its ongoing development and adaptive strategies make it a growing global concern for organizations of all sizes.

Recommendations

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Helldown ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Helldown ransomware attack, up-to-date backups enable recovery without paying the ransom.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Network Segmentation: Divide the network into segments to limit the spread of ransomware. This can help contain the damage and protect sensitive data.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0010 Exfiltration	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0040 Impact	T1556 Modify Authentication Process
T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1490 Inhibit System Recovery	T1070 Indicator Removal

T1529 System Shutdown/Reboot	T1486 Data Encrypted for Impact	T1569.002 Service Execution	T1569 System Services
T1190 Exploit Public-Facing Application	T1136.001 Local Account	T1136 Create Account	T1059 Command and Scripting Interpreter
T1556.001 Domain Controller Authentication	T1027 Obfuscated Files or Information	T1588.006 Vulnerabilities	T1588 Obtain Capabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbbdcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7, 7731d73e048a351205615821b90ed4f2507abc65acf4d6fe30ecdb211f0b0872, 3e3fad9888856ce195c9c239ad014074f687ba288c78ef26660be93ddd97289e, 2621c5c7e1c12560c6062fdf2eeeb815de4ce3856376022a1a9f8421b4bae8e1, 47635e2cf9d41cab4b73f2a37e6a59a7de29428b75a7b4481205aee4330d4d19, cb48e4298b216ae532cfd3c89c8f2cbd1e32bb402866d2c81682c6671aa4f8ea, 67aea3de7ab23b72e02347cbf6514f28fb726d313e62934b5de6d154215ee733, 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0, 6ef9a0b6301d737763f6c59ae6d5b3be4cf38941a69517be0f069d0a35f394dd, 9ab19741ac36e198fb2fd912620bf320aa7fdeeeb8d4a9e956f3eb3d2092c92c, ccd78d3eba6c53959835c6407d81262d3094e8d06bf2712fefa4b04baadd4bfe

Recent Breaches

http://www.smarts-engineering.de
http://www.qualiform.cz
http://www.nightnurse.ch
http://www.knoxlawcenter.com
http://www.csikitchenandbath.com
http://www.compassfs.net
http://www.co.san-jacinto.tx.us
http://valleyfirm.com
http://tivoli-33.org
http://lacliniqueducoureur.com
http://klinik-am-kurpark.de
http://hausdesstiftens.org
http://generaldentistryforchildren.com
http://fuelco-us.com
http://americanventures.com
http://www.jewishharrisburg.org
http://www.barryavenueplating.com
http://www.rsk-immobilien.de
http://www.cincinnatipainphysicians.com
http://kbosecurity.co.uk
http://khonaysser.com
http://Zyxel.eu
http://atpsassari.it
http://XPERT Business Solutions GmbH
http://MyFreightWorld
http://cbmm.org
http://AZIENDA TRASPORTI PUBBLICI S.P.A.
http://briju.pl
http://vindix.pl
http://Albatros S.r.l.
http://SCHLATTNER.de
http://deganis.fr
http://hugwi.ch

Patch Details

Upgrade Zyxel ATP series to V5.39

Link: https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024

References

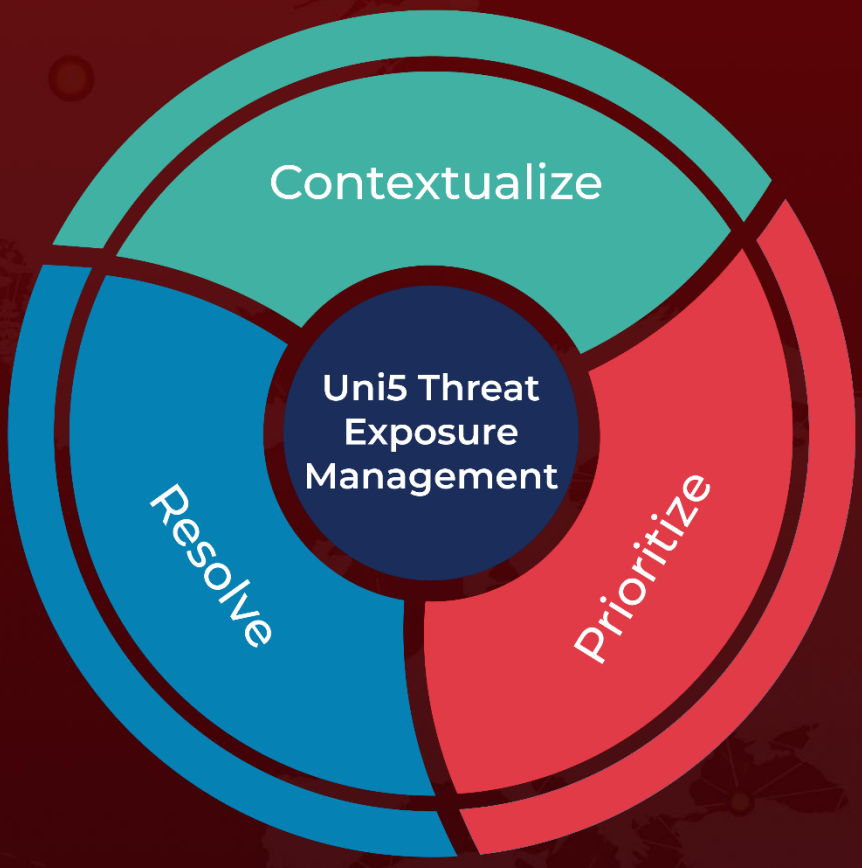
https://blog.sekoia.io/helldown-ransomware-an-overview-of-this-emerging-threat/#h-encryption

https://www.halcyon.ai/attacks/helldown-ransomware-hits-vindix-23-gb-data-breach-analysis

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 21, 2024 . 01:30 AM

More at www.hivepro.com