Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

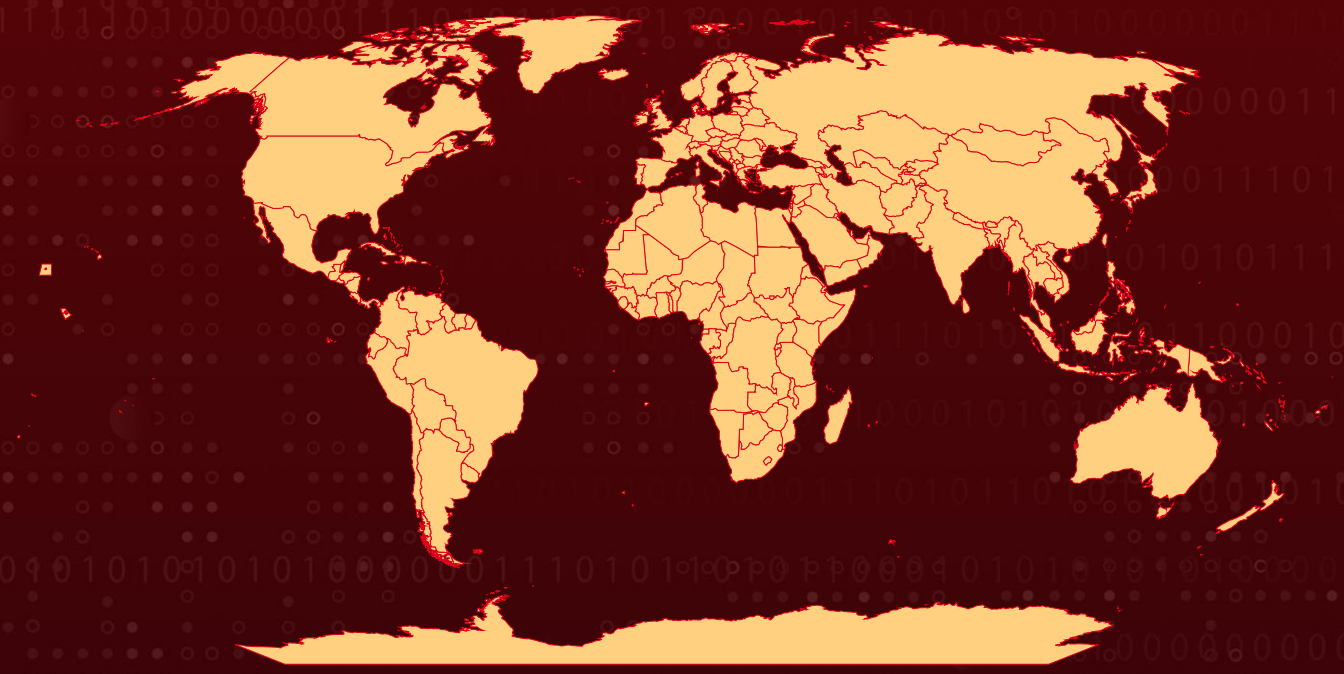
Abyss Locker Ransomware: A Growing Threat to Virtualized Environments

Date of Publication	Admiralty Code	TA Number
February 12, 2025	A1	TA2025038

Summary

First Appearance: 2023
Malware: Abyss Locker ransomware (aka AbyssLocker)
Targeted Region: Worldwide
Affected Platforms: Windows, Linux and VMware ESXi
Targeted Industries: Technology, Healthcare, Manufacturing, Business Services & Consulting, Agriculture, Retail, Food Service, Real Estate, Financial Services, Energy
Attack: Abyss Locker is a ransomware group mainly targeting VMware ESXi servers and corporate networks using vulnerabilities in VPN appliances and SSH exploits. The group exfiltrates data before encrypting systems, demanding ransom payments while leveraging double extortion tactics. Their latest attacks focus on critical network devices, making them a significant cybersecurity threat in 2025. Their expanding attacks highlight the need for strong cybersecurity measures, including regular patching, backup security, and network monitoring.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-20038	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability	SonicWall SMA 100 Appliances	✗	✓	✓

Attack Details

#1

Abyss Locker is a ransomware group that emerged in 2023, rapidly escalating its cyberattacks throughout 2024 and into 2025. The group employs sophisticated tactics to infiltrate corporate networks, exfiltrate sensitive data, and encrypt systems, primarily targeting critical network devices, including VMware ESXi servers.

#2

Abyss Locker initiates its attacks by exploiting vulnerabilities in edge devices, such as unpatched VPN appliances. Notably, the group has leveraged vulnerabilities like CVE-2021-20038 in SonicWall VPNs to gain initial access. Once inside the network, they deploy tunneling tools and malware on critical devices to maintain persistence and evade detection. Key targets include network-attached storage (NAS) systems and VMware ESXi servers.

#3

On ESXi servers, the attackers exploit administrative credentials or known vulnerabilities to enable SSH access if disabled. They utilize the native SSH binary to establish reverse SSH tunnels to their command-and-control (C2) servers, allowing them to pivot within the network and conduct reconnaissance while avoiding detection. The resilience of ESXi appliances makes them ideal for maintaining semi-persistent backdoors.

#4

Before deploying the ransomware, Abyss Locker exfiltrates sensitive corporate data to leverage in double extortion tactics. The group primarily uses Rclone, a powerful open-source cloud storage utility, renaming its binary to evade detection. This tool enables targeted data theft, selectively exfiltrating files matching specific extensions and uploading them to cloud storage services such as Amazon Web Services (AWS) and BackBlaze.

#5

After securing complete control over the environment, Abyss Locker launches its final destructive phase encrypting all accessible data. It uses the file extension ‘.Abyss’ on Windows systems and ‘.crypt’ on ESXi hosts. The ransomware creates ransom notes named ‘WhatHappened.txt’ on compromised systems and attempts to delete volume shadow copies to hinder data recovery. As of February 2025, Abyss Locker continues to pose a significant threat to organizations worldwide.

Recommendations

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 Abyss Locker ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Update all edge devices (e.g., VPN appliances, firewalls, and ESXi servers) with the latest security patches. Prioritize patching vulnerabilities exploited by Abyss Locker, such as CVE-2021-20038 in SonicWall VPNs. Disable unnecessary services and restrict remote access to prevent initial compromise.

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 an Abyss Locker ransomware attack, up-to-date backups enable recovery without paying the ransom.

Network Security & Access Control: Limit SSH access to trusted IPs and disable root login on ESXi servers. Use multi-factor authentication (MFA) for all privileged accounts, including ESXi management consoles. Separate critical infrastructure (e.g., ESXi hosts, backup systems) from user endpoints and public-facing services. Deploy Intrusion Detection/Prevention Systems (IDS/IPS) to detect suspicious SSH tunnels and lateral movement.

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

TA0010 Exfiltration	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	T1567 Exfiltration Over Web Service
T1133 External Remote Services	T1190 Exploit Public-Facing Application	T1059.004 Unix Shell	T1059 Command and Scripting Interpreter

T1003 OS Credential Dumping	T1543 Create or Modify System Process	T1543.003 Windows Service	T1136.001 Local Account
T1136 Create Account	T1078 Valid Accounts	T1068 Exploitation for Privilege Escalation	T1562.001 Disable or Modify Tools
T1562 Impair Defenses	T1036.005 Match Legitimate Name or Location	T1036 Masquerading	T1555 Credentials from Password Stores
T1003.002 Security Account Manager	T1046 Network Service Discovery	T1021.001 Remote Desktop Protocol	T1021.004 SSH
T1570 Lateral Tool Transfer	T1005 Data from Local System	T1039 Data from Network Shared Drive	T1071.001 Web Protocols
T1071 Application Layer Protocol	T1219 Remote Access Software	T1567.002 Exfiltration to Cloud Storage	T1486 Data Encrypted for Impact
T1490 Inhibit System Recovery	T1586 Compromise Accounts		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	59a97f9d7c1d6e10fa41ea9339568fb25ec55e27, 3f90fd241e9422cc447b5ccdcb87d72507f37e6f, 23873bf2670cf64c2440058130548d4e4da412dd, e44ec82d0d80c754afcd7ed149c263c55d158259, 13112e672d807fa7c7f8a383ecfa31e85b880e5a, f24ca204af2237a714e8b41d54043da7bbe5393b, 17d9200843fe0eb224644a61f0d1982fac54d844, 82780c0c1c0e04d994c770a3b3e73727528b0451
SHA256	05b82d46ad331cc16bdc00de5c6332c1ef818df8ceefcd49c726553209b3a0da, 6042a84529958a04a2d46384139da3ef016bf9498e791cd5e34dfecec2baa1d2,

TYPE	VALUE
SHA256	3C2FE308C0A563E06263BBACF793BBE9B2259D795FCC36B953793A7E499E7F71, 5fba25759423f9efc92592977f6c9ff77d47a20aa8ec8e9cd17d5cfa786a1852, cd9d88cccd85209966c5a35aba7751b962bcc021a4216d6addfc0c3462ce80da, f9ab649acfe76d6ac088461b471e5d981bdc8b71d940e94c63bc1988a2ed4678, 5f9dfd9557cf3ca96a4c7f190fc598c10f8871b1313112c9aea45dc8443017a2, d48c7f13db60ef615e59773c442485e84acef09343375d0d8a462b285e959baa, d76c74fc7a00a939985ae515991b80afa0524bf0a4feaec3e5e58e52630bd717, 0d9089efe2a28630bc21d8db451ec14dc856c2d40444292c42e7cca218c7029e
File Paths	C:\users\<USER>\appdata\roaming\microsoft\wmi\wmihelper.exe, C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\Microsoft\Wmi\wmihelper.exe, /bin/apache2, C:\Windows\uFmAnlZR.exe, /tmp/e.elf, C:\Users\<USER>\Desktop\e\e.exe, C:\Windows\System32\rclone, C:\Windows\System32\LTSVC.exe, C:\Windows\System32\filter.txt, C:\Windows\Temp\SophosAV.exe, C:\ProgramData\USOShared\auSophos.exe, C:\ProgramData\USOShared\UpdateSvc.exe, C:\programdata\pr.exe, C:\ProgramData\deploy443.ps1, C:\ProgramData\USOShared\UpdateDrv.sys
TOR Address	3ev4metjirohtdpshsqlkrqcmxq6zu3d7obrdhglpy5jpbr7whmlfgqd[.]onion
File Names	wmihelper.xml, wmihelper.key, veeam11.ps1, ped.sys, 3ware.sys
Host Names	DESKTOP-VM4QKN6, ADMINIS-F69E5L3
IPv4	139[.]180[.]135[.]191, 67[.]217[.]228[.]101, 64[.]95[.]12[.]57, 64[.]95[.]12[.]70, 149[.]137[.]142[.]15

Patch Links

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026

Recent Breaches

https://jpcgroupinc.com
https://fourcornerseye.com
https://envirosep.com
https://kingpower.com
https://berkotfoods.com
https://bataviacontainer.com
https://pez.com
https://glts.net

References

https://www.sygnia.co/blog/abyss-locker-ransomware-attack-analysis/

https://www.sentinelone.com/anthology/abyss-locker/

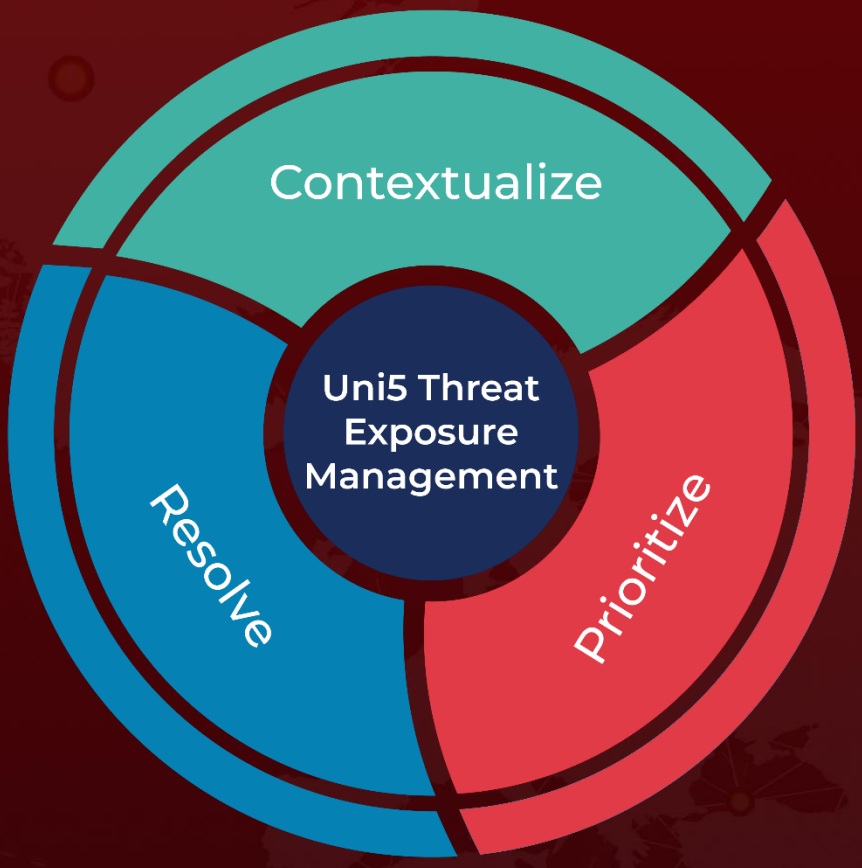
https://cyberint.com/blog/research/into-the-depths-of-abyss-locker/

https://www.hivepro.com/threat-advisory/abyss-lockers-substantial-threat-explored/

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

February 12, 2025 • 11:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com