Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

DJVU Ransomware's Variant Emerges Disguised as Cracked Software

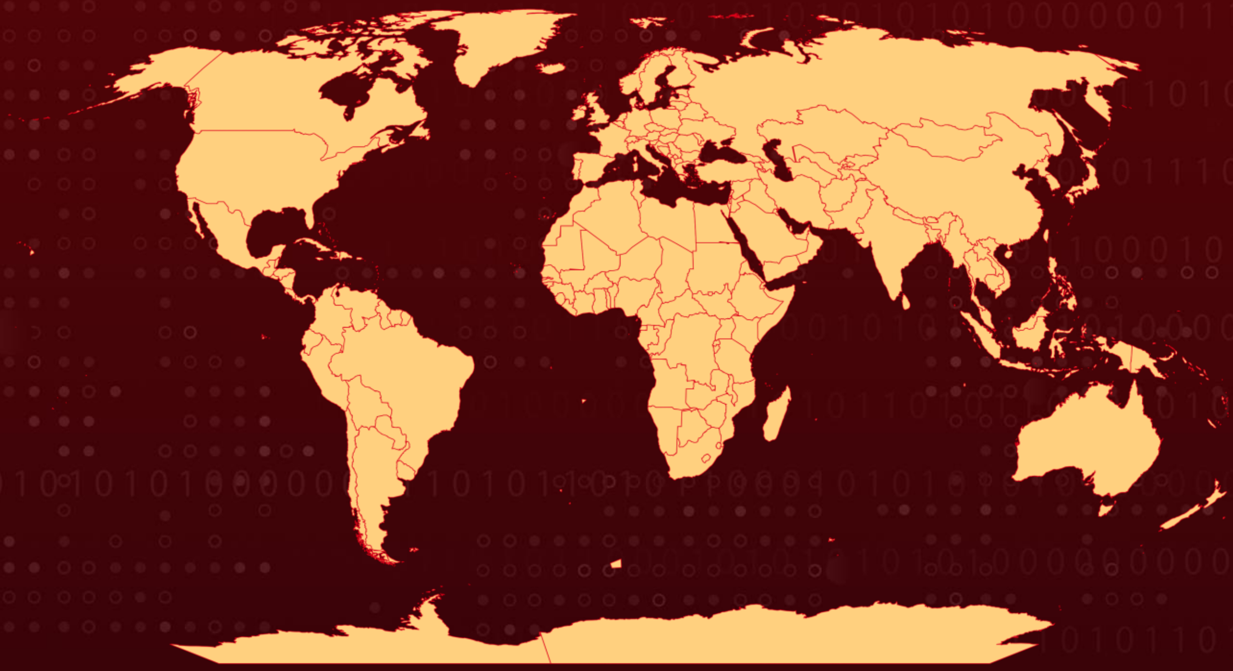
Date of Publication	Admiralty Code	TA Number
November 30, 2023	A1	TA2023483

Summary

Attack Began: November 2023
Malware: Djvu, PrivateLoader
Ransom: $490 - $980
Attack Region: Worldwide

Attack: A variant of the DJVU ransomware, disguising itself as cracked software, has emerged and is demanding a ransom of $980 for decryption. These incidents involve the infiltration of systems by various commodity loaders and infostealers, with the adversary's primary objectives being data exfiltration and information theft.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 A variant of the DJVU ransomware strain has been identified and distributed under the disguise of cracked software. This specific DJVU variant appends the .xaro extension to compromised files and demands ransom for a decryptor. These incidents involve the infiltration of systems by various commodity loaders and infostealers. The primary objectives of the adversary include data exfiltration, information theft, and file encryption, ultimately aiming to extort a ransom from the victim.

#2 DJVU, a derivative of the STOP ransomware, typically enters the scene disguised as legitimate services or applications. Notably, DJVU attacks are characterized by the deployment of supplementary malware, such as information stealers like RedLine Stealer and Vidar, intensifying the overall impact of the attacks.

#3 In the latest attack sequence, the infection initiates with users downloading the DJVU variant named Xaro. This variant is propagated as an archive file from a dubious source posing as a site offering legitimate freeware. The archive file leads to the execution of what appears to be an installer binary for a PDF writing software called CutePDF. However, this installer is a pay-per-install malware downloader service known as PrivateLoader.

#4 PrivateLoader establishes communication with a command-and-control (C2) server to retrieve various stealer and loader malware families. The objective seems to be the collection and exfiltration of sensitive information for double extortion, while also ensuring the success of the attack, even if one of the payloads is blocked by security software. The threat actor sets the ransom at $980 for the private key and the decryptor tool, with a 50% reduction to $490 if the victim responds within 72 hours.

Recommendations

Application Whitelisting: Enforce application whitelisting to allow only authorized applications to run, preventing the execution of unauthorized or malicious programs on endpoints.

File System Auditing: Enable file system auditing to track and log file access and modification events. This can aid in the early detection of suspicious activities associated with ransomware.

Zero Trust Architecture: Adopt a Zero Trust Architecture, where trust is never assumed, and verification is required from everyone trying to access resources within the network, minimizing the risk of lateral movement by attackers.

Fortify Your Data Defense: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0040 Impact	T1566 Phishing	T1598 Phishing for Information
T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1055 Process Injection	T1059.001 PowerShell
T1070.001 Clear Windows Event Logs	T1083 File and Directory Discovery	T1082 System Information Discovery	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1490 Inhibit System Recovery	T1486 Data Encrypted for Impact	T1659 Content Injection
T1657 Financial Theft	T1018 Remote System Discovery	T1033 System Owner/User Discovery	T1059 Command and Scripting Interpreter
T1112 Modify Registry	T1482 Domain Trust Discovery	T1564.003 Hidden Window	T1078.002 Domain Accounts

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	10ef30b7c8b32a4c91d6f6fee738e39dc02233d71ecf4857bec6e70520d0f5c1, 83546201db335f52721ed313b9078de267eaf1c5d58168b99e35b2836bf4f0fc, 3d9cf227ef3c29b9ca22c66359fdd61d9b3d3f2bb197ec3df42d49ff22b989a4, 8d7f0e6b6877bdfb9f4531afafd0451f7d17f0ac24e2f2427e9b4ecc5452b9f0, 1bb689e95fd5ed5f70fd3ac60cf28d7aace52fea6b1bacc0a257e19cbf50a71d, a4b3953a8fdbee6fccaa3c25847c3da85e78d33377e73e6bebe3fe9d00a4de84, 3802d96292e6a2968272841a8d9e360e1358d4cd58db35ef04a08da70ce3c329, d5d2f7a0d0ec8cbba0f3f3ad7f4eebdb0e82bb54e0edb6356eccb84b8d9d5736, e833b7fc4bf14527edb120ee4e691a660b21f93b1ec22bf15881bdcee4c5bb8d, a0e32603876c3035d76a78e35d5f89576ded2475451b4d27e19331bf9e6abfc3, 9ded335a6f346de4aafbc4f8c08e90dce1f064820b13d6580f01731c9837d7a8, 7c9bc6a878b6cb355bb2a5c70170aa48b1e8f369dd64ee47df3ac9ea9e213b02, 1da3193c52b5ec3a14b36acbc9c92266a2a531399e33c1e3a209e828eda7a0a5, aa8c5d42026ac9a483f1984f762441d7f5805ef914819b473f9e15353995cc99, 672488666b68b99cef16ff0c1acfd3aa009df3f6d3f18897c5ecee77b77a57c7, 8a4214d3c69df6a10e057fe1071e6bbb2ebd463bf3e73b9c66c3cbf3f31839b2, 0708f648422765beec57de76dba43e18175da0304bd38b805b12b4f18ba435b3
Domains	api.2ip[.]ua, colisumy[.]com, zexeq[.]com
Registry	software\microsoft\windows\currentversion\run\syshelper

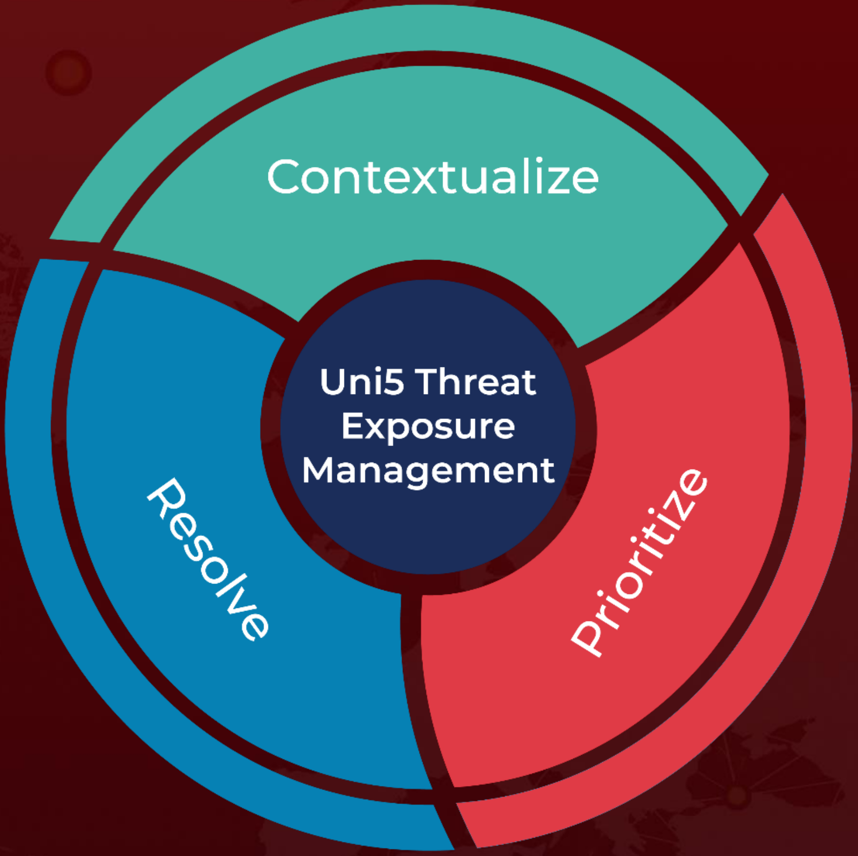
References

https://www.cybereason.com/hubfs/dam/collateral/reports/threat-alert-DJvu-variant.pdf

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 30, 2023 • 05:30 AM

More at www.hivepro.com