Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

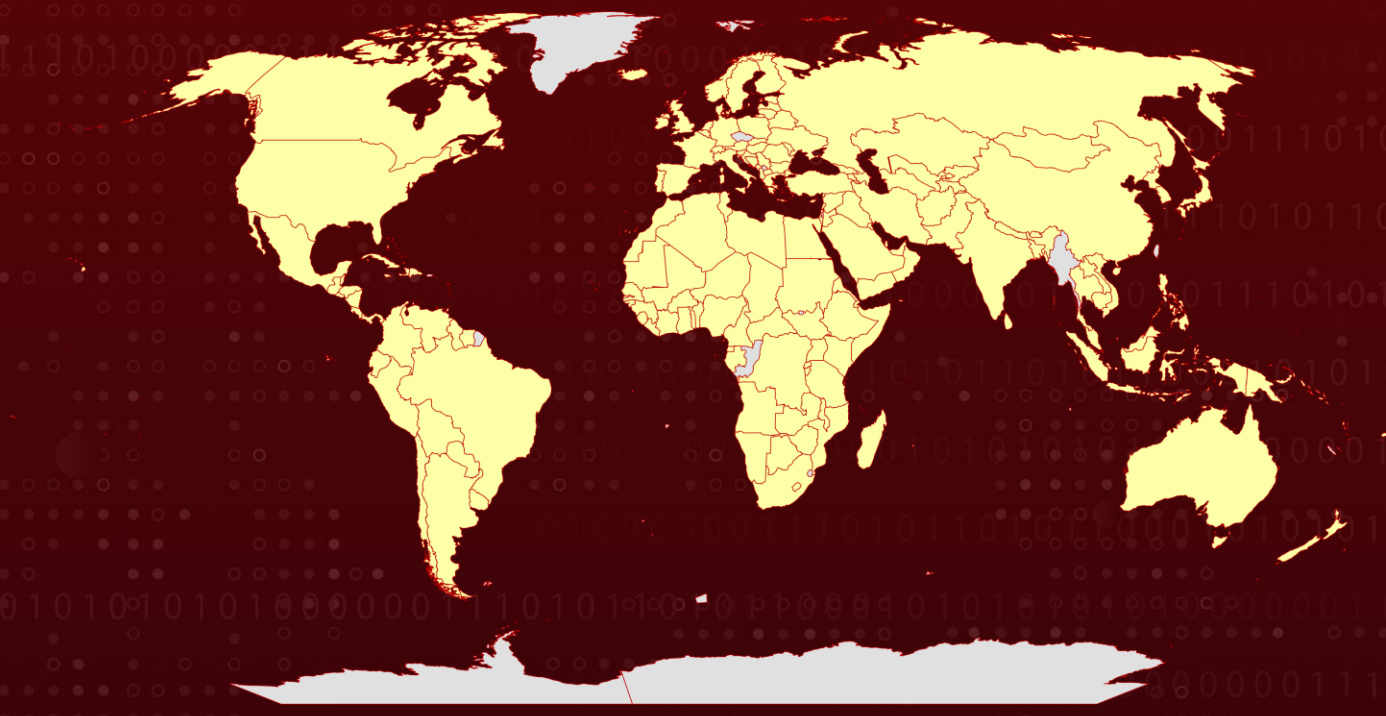
New Azov Ransomware can wipe 666 bytes data at a stretch

Date of Publication	Admiralty Code	TA Number
November 8, 2022	A1	TA2022247

Summary

Date: October 28, 2022
Attack Region: Worldwide
Attack: Dual encryption via Azov and STOP ransomware; corrupts 666 bytes at a stretch;

Attack Regions



Attack Details

#1 The threat actor appears to have purchased the SmokeLoader malware botnet in a fresh effort to deploy the new disruptive Azov wiper. The SmokeLoader is found in fake pirated software and crack sites. The initial ransomware executable is dropped and executed in Windows as a random file.

#2 The wiper will now analyze the directories on the compromised machine and dual encrypt, first with Azov and then with STOP ransomware, all files excluding .ini, .dll, or .exe extensions, and further append the .azov extension to the names of encrypted files.

#3 The wiper will create text files named RESTORE_FILES.txt in each analyzed folder containing a ransom message from the threat actor. Azov wiper shreds victims' data and infects other applications on purpose. Victims infected with Azov Ransomware will be unable to restore their files as additional executables are contaminated Windows should be reinstalled.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0040 Impact	T1190 Exploit Public-Facing Application	T1547 Boot or Logon Autostart Execution
T1055 Process Injection	T1562 Impair Defenses	T1036 Masquerading	T1112 Modify Registry
T1027 Obfuscated Files or Information	T1003 OS Credential Dumping	T1552 Unsecured Credentials	T1083 File and Directory Discovery
T1082 System Information Discovery	T1080 Taint Shared Content	T1560 Archive Collected Data	T1105 Ingress Tool Transfer
T1486 Data Encrypted for Impact			

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	650f0d694c0928d88aeeed649cf629fc8a7bec604563bca716b1688227e0cc7e,a041839327295fde3df12ea61374abd19c4499b87e211757c593179d6a6870d1,5fe41e533a89cbf6c659eb78b221f24c4827b834a877f72c0ee34a5a0fd80b84,b102ed1018de0b7faea37ca86f27ba3025c0c70f28417ac3e9ef09d32617f801,650f0d694c0928d88aeeed649cf629fc8a7bec604563bca716b1688227e0cc7e,848f2b8fdb3285f040310988e2c0d26c5644296c97e7d1ce39e379b04ce66824,9435b7a2b884676ec7e109ed28a9164cea5f5f6d4a18e1b2cebaff1de4c186db,848f2b8fdb3285f040310988e2c0d26c5644296c97e7d1ce39e379b04ce66824
MD5	7fdba86bba0508054fd1f058a6a2d134, 28097ef38e5b2bbcad21becaa9b232ca, 6468ee100d88c71d55dfdcf4e30f991e, 7129291fc3d97377200f8a24ad06930a,
SHA-1	131aa6889c55b9348a452fdf369fe54c2f05ba48, 0daaddbd5e25c88534652819cd8ae3d75955faf3, 5c520d2d7dc4c9e5d536d3aff998185657d40ac8

References

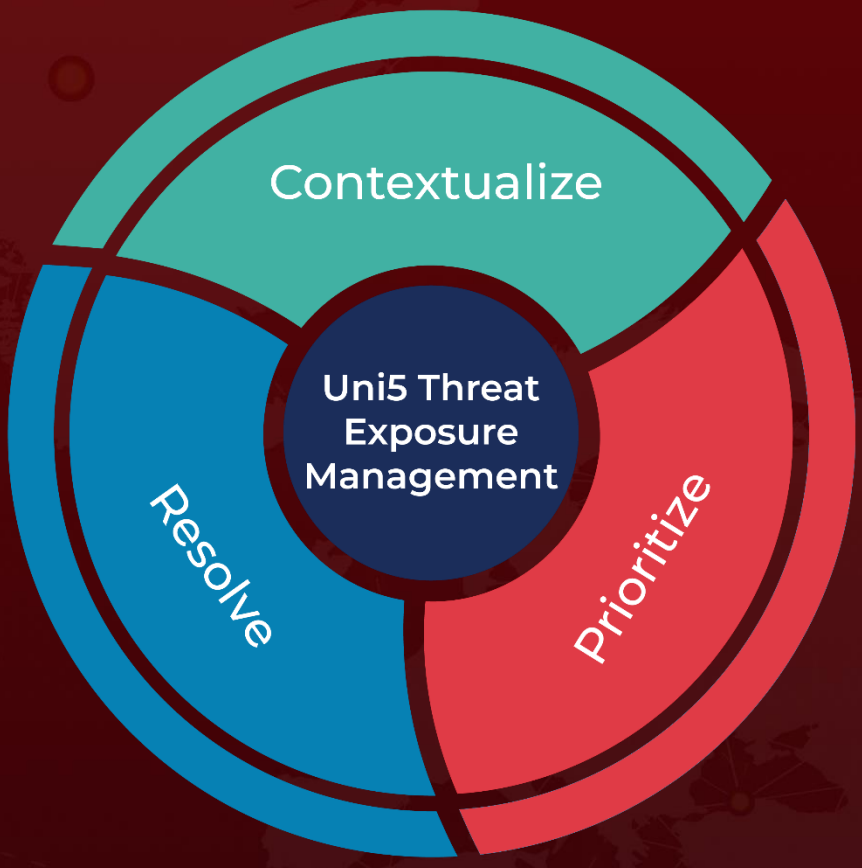
https://www.bleepingcomputer.com/news/security/azov-ransomware-is-a-wiper-destroying-data-666-bytes-at-a-time/

https://www.bleepingcomputer.com/news/security/new-azov-data-wiper-tries-to-frame-researchers-and-bleepingcomputer/#azov_note

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 8, 2022 • 5:45 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com