Hive Pro®

Threat Level

Red

CISA: AA23-263A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

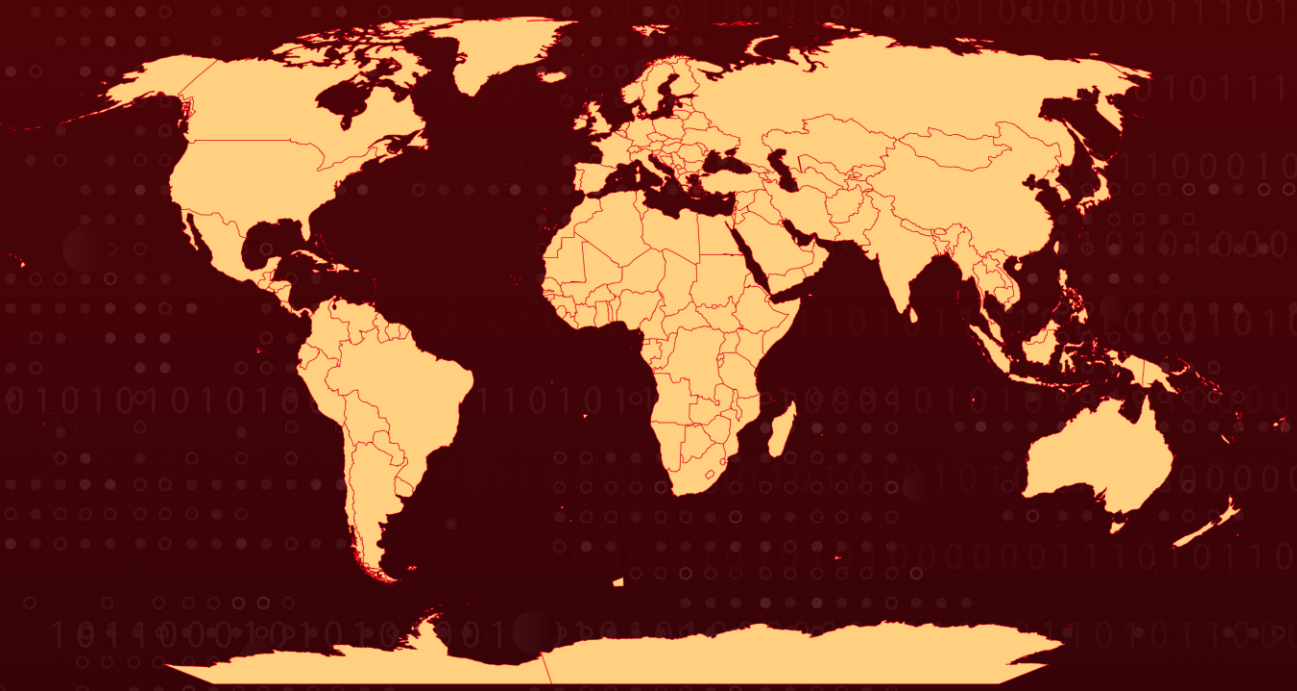
Snatch Ransomware: Evolving Threat and Defense Strategies

Date of Publication	Admiralty Code	TA Number
September 21, 2023	A1	TA2023382

Summary

First Appearance: 2018
Attack Region: Worldwide
Affected Platform: Windows
Targeted Industries: Defense Industrial Base (DIB), Food and Agriculture, Information Technology (IT)
Malware: Snatch ransomware
Attack: Snatch ransomware is a ransomware-as-a-service (RaaS) variant that was first discovered in 2018. It is known for its ability to reboot devices into Safe Mode, where many security protections are disabled, before encrypting files. Snatch also uses double extortion tactics, threatening to publish stolen data on the internet if the victim does not pay the ransom.

Attack Regions



Attack Details

#1

Snatch ransomware has evolved since 2018, using a ransomware-as-a-service model and unique tactics like rebooting devices into Safe Mode to avoid detection. They target critical infrastructure sectors, engage in data exfiltration, and threaten double extortion, posting victim data on their extortion blog if the ransom is not paid.

#2

The advisory encourages organizations to implement mitigation recommendations to reduce ransomware risks. Snatch actors gain initial access through RDP exploits and maintain persistence via compromised admin accounts. They use various tools for lateral movement and data discovery.

#3

Snatch disables antivirus, runs executables, modifies registries, and removes shadow copies during ransomware deployment. Each victim's encrypted files have a unique identifier, and communication with victims occurs via email, Tox, and their extortion blog. Some victims have received spoofed calls and ransom notes from Snatch, even if another ransomware variant was deployed.

Recommendations

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Implement Multi-Factor Authentication (MFA): Ensure that all user accounts are protected by multi-factor authentication, especially those with access to critical systems or sensitive data. This additional layer of security can significantly reduce the risk of unauthorized access, even if passwords are compromised.

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0040 Impact	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	T1071.001 Web Protocols	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery
T1590 Gather Victim Network Information	T1583.003 Virtual Private Server	T1078 Valid Accounts	T1133 External Remote Services
T1059.003 Windows Command Shell	T1059.002 AppleScript	T1078.002 Domain Accounts	T1036 Masquerading
T1070.004 File Deletion	T1112 Modify Registry	T1562.001 Disable or Modify Tools	T1562.009 Safe Mode Boot
T1110.001 Password Guessing	T1012 Query Registry	T1057 Process Discovery	T1021.001 Remote Desktop Protocol
T1005 Data from Local System			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	seznam[.]cz, cock[.]li, airmail[.]cc,

TYPE	VALUE
Domains	tutanota[.]com / tutamail[.]com / tuta[.]io, mail[.]fr, keemail[.]me, protonmail[.]com / proton[.]me, swisscows[.]email, sn.tchnews.top@protonmail[.]me
Emails	sn.tchnews.top@protonmail[.]me, funny385@swisscows[.]email, funny385@proton[.]me, russellrspeck@seznam[.]cz, russellrspeck@protonmail[.]com, Mailz13MoraleS@proton[.]me, datasto100@tutanota[.]com, snatch.vip@protonmail[.]com
TOX Messaging IDs	CAB3D74D1DADE95B52928E4D9DFC003FF5ADB2E082F59377D049A91952E8BB3B419DB2FA9D3F, 7229828E766B9058D329B2B4BC0EDDD11612CBCCFA4811532CABC76ACF703074E0D1501F8418, 83E6E3CFEC0E4C8E7F7B6E01F6E86CF70AE8D4E75A59126A2C52FE9F568B4072CA78EF2B3C97, 0FF26770BFAEAD95194506E6970CC1C395B04159038D785DE316F05CE6DE67324C6038727A58
SHA256	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd, 7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3, 28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c, fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066, a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae, 6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0, 510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1, ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d, 2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57,

TYPE	VALUE
SHA256	251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d, 3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924, 6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7, 84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5, a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84, b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
Filenames	qesbdksdvnotrjnexutx[.]bat, eqbglqcngblqnl[.]bat, safe[.]exe, DefenderControl[.]exe, PRETTYOCEANApplicationdrs[.]bi, Setup[.]exe, WRSA[.]exe, ghnhfglwaplf[.]bat, nllraq[.]bat, ygariiwfenmqteiwcr[.]bat, bsfyqgqeauegwyfvtp[.]bat, rgibdcghzwpk[.]bat, pxyicmajjlqrtgcnhi[.]bat, evhgpp[.]bat, eqbglqcngblqnl[.]bat, qesbdksdvnotrjnexutx[.]bat,
SHA1	c8a0060290715f266c89a21480fed08133ea2614
Registry Keys	HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\D8B548F0-E306-4B2B-BD82-25DAC3208786\FriendlyName, HKU\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{ED50FC29-B964-, 48A9-AFB3-15EBB9B97F36} {ADD8BA80-002B-11D0-8F0F-00C04FD7D062} 0xFFFF

TYPE	VALUE
Mutexes	\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-fc_key, \Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-sjlj_once, \Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-use_fc_key, gcc-shmem-tdm2-fc_key, gcc-hmem-tdm2-sjlj_once, gcc-shmem-tdm2-use_fc_key

References

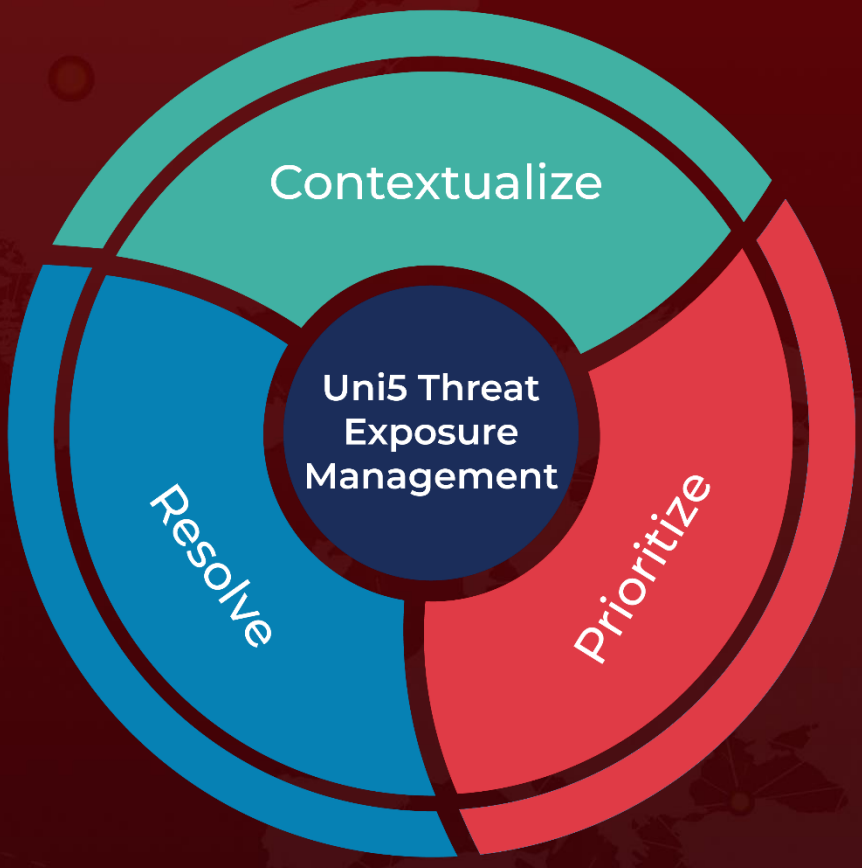
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a

https://www.cisa.gov/news-events/alerts/2023/09/20/fbi-and-cisa-release-advisory-snatch-ransomware

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

September 21, 2023 . 11:00 PM

More at www.hivepro.com