Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

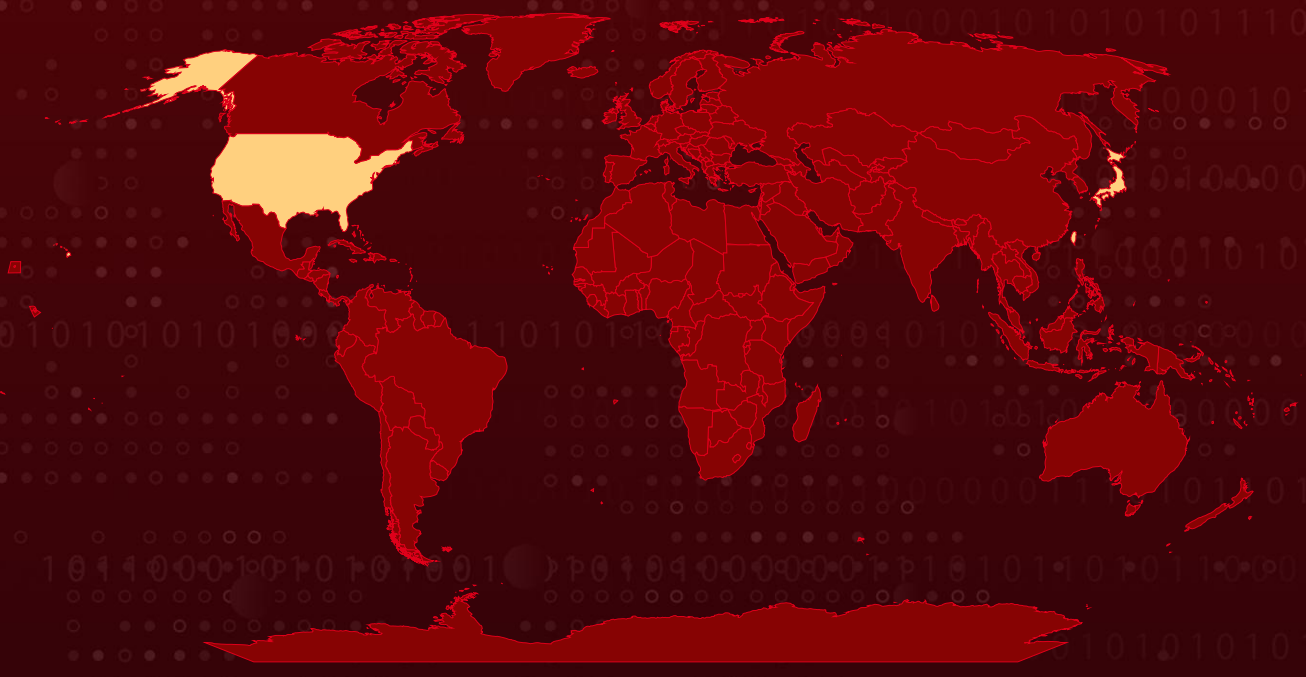
SocGholish and RansomHub: A Dangerous Cybercrime Alliance

Date of Publication	Admiralty Code	TA Number
March 17, 2025	A1	TA2025080

Summary

Attack Commenced: January 2025
Targeted Countries: United States, Japan, Taiwan
Malware: SocGholish, RansomHub
Targeted Industries: Government, Banking, Consulting
Targeted Platform: Windows
Attack: The Water Scylla attack exploits compromised websites and the Keitaro Traffic Distribution System (TDS) to distribute SocGholish malware, tricking users into downloading fake browser updates. Once executed, SocGholish facilitates data theft, persistence, and lateral movement within the network. Attackers leverage PowerShell scripts and credential theft tools to escalate privileges and gain deeper access. Ultimately, RansomHub ransomware is deployed, encrypting files and demanding payment. The campaign primarily targets organizations worldwide, with a focus on the US, Japan, and Taiwan.

Attack Regions



Attack Details

#1

The Water Scylla intrusion set is a multi-stage attack campaign that leverages compromised websites, malicious Keitaro Traffic Distribution System (TDS) instances, and SocGholish malware to facilitate ransomware deployment. SocGholish, also known as FakeUpdates, is a malware-as-a-service (MaaS) framework that primarily spreads through legitimate websites injected with malicious scripts. When users visit these sites, they are redirected to fake browser update pages, tricking them into downloading and executing a malicious JavaScript loader.

#2

Once executed, the SocGholish loader collects system information, evades detection through obfuscation techniques, and downloads additional payloads, including backdoors and credential stealers. The malware establishes persistent access, allowing attackers to exfiltrate sensitive data and execute arbitrary commands. Water Scylla collaborates with rogue Keitaro TDS operators to filter traffic and deliver the SocGholish payload only to intended targets while avoiding security researchers and automated defenses.

#3

Post-compromise, SocGholish operators deploy reconnaissance and credential theft tools to escalate privileges and move laterally within the victim's network. Data exfiltration is a key component, with stolen credentials and other sensitive information sent to command-and-control (C&C) servers. The attackers also use PowerShell scripts and Python-based backdoors to maintain control, enabling follow-up attacks, including ransomware deployment.

#4

RansomHub, a ransomware-as-a-service (RaaS) group, is the final stage of the attack, using SocGholish as an entry point for its affiliates. The attackers deploy reverse shells and establish SMB-based persistence, allowing them to encrypt files and extort victims. Trend Micro telemetry has identified thousands of compromised websites facilitating these attacks, with government organizations, banks, and consulting firms being among the most affected. The widespread nature and evasiveness of SocGholish make it a critical enabler of ransomware campaigns.

Recommendations

Strengthen Endpoint Security: Deploy advanced endpoint detection and response (EDR) solutions to identify and block malicious scripts and payloads. Enable application whitelisting to prevent unauthorized execution of JavaScript files and other suspicious executables. Keep all software, including browsers and plugins, updated to reduce the risk of exploitation.

Enhance Web and Email Security: Implement web filtering solutions to block known malicious domains associated with Keitaro TDS and SocGholish campaigns. Use browser extensions or security tools that detect and block fake update prompts. Train users to recognize phishing attempts and avoid downloading software updates from unverified sources.

Improve Network Defenses: Monitor network traffic for suspicious activity, such as unexpected PowerShell execution or abnormal SMB connections. Implement network segmentation to limit lateral movement if an endpoint is compromised. Use intrusion detection/prevention systems (IDS/IPS) to detect command-and-control (C&C) communications.

Strengthen Access Controls and Authentication: Enforce multi-factor authentication (MFA) for all remote access and privileged accounts.Regularly audit user accounts and disable unused or unnecessary administrative privileges.Rotate credentials regularly and monitor for leaked or stolen credentials.

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	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access

TA0010 Exfiltration	T1053 Scheduled Task/Job	T1095 Non-Application Layer Protocol	T1572 Protocol Tunneling
T1608.004 Drive-by Target	T1204 User Execution	T1059.007 JavaScript	T1059 Command and Scripting Interpreter
T1059.003 Windows Command Shell	T1204.002 Malicious File	T1059.001 PowerShell	T1059.006 Python
T1027.013 Encrypted/Encoded File	T1070.004 File Deletion	T1006 Direct Volume Access	T1074.001 Local Data Staging
T1069.001 Local Groups	T1087.002 Domain Account	T1082 System Information Discovery	T1482 Domain Trust Discovery
T1069.002 Domain Groups	T1135 Network Share Discovery	T1016 System Network Configuration Discovery	T1083 File and Directory Discovery
T1003 OS Credential Dumping	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1552.001 Credentials In Files
T1105 Ingress Tool Transfer	T1555 Credentials from Password Stores		T1003.002 Security Account Manager
T1041 Exfiltration Over C2 Channel	T1021.002 SMB/Windows Admin Shares	T1608 Stage Capabilities	T1053.005 Scheduled Task

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	nevada[.]mandros[.]us, cpanel[.]kreativelife[.]net, exclusive[.]nobogoods[.]com, whcms[.]greendreamcannabis[.]com, windows[.]envisionfonddulac[.]net,

TYPE	VALUE
Domains	round[.]micha[.]ai, mail[.]aestheticfina[.]com, cluster[.]buydoorlitesandlouvers[.]com, software[.]adx-crm[.]com, sponsor[.]sewacanada[.]org, certificate[.]hypnotherapy-training[.]co[.]nz, estate[.]envisionfonddulac[.]org, seminary[.]envisionfonddulac[.]com, exchange[.]tuckx[.]com, dashboard[.]nzlifecoaching[.]com, programs[.]edlester[.]com, academy[.]entrepreneurwealthhub[.]com, portal[.]miaariacademy[.]com, preview[.]jpainting[.]ca, hub[.]unlimitedcashflowevent[.]com, ceo[.]cowholesaling[.]com, support[.]myfirstdealplaybook[.]com, newsite[.]iapmd[.]org, cpanel[.]buyjlindustriesonline[.]com, btctrading[.]crestlinesolutions[.]work, webmail[.]ebuildingsource[.]com, subscribe[.]bigeznola[.]com, gemini[.]1stpagegold[.]com, customer[.]aaddigitalstrategies[.]com, regular[.]ptbaconsulting[.]com, crm[.]bestintownpro[.]com, trial[.]buyintercomsonline[.]com, order[.]buyanemostatonline[.]com, static[.]buyweatherstriponline[.]com, zone[.]ebuilderssource[.]com, slot[.]buyaiphoneonline[.]com, rednosehorse[.]com, apiexplorerzone[.]com, smthwentwrong[.]com, newgoodfoodmarket[.]com, foundedbrounded[.]org, packedbrick[.]com, newgreenvibes[.]com, rapiddevapi[.]com, digdonger[.]org, blackshelter[.]org, blacksaltys[.]com, brickedpack[.]com, blessedwirrow[.]org

TYPE	VALUE
IPv4	207[.]174[.]31[.]215, 185[.]72[.]8[.]129, 38[.]180[.]137[.]245, 38[.]180[.]137[.]141, 45[.]76[.]228[.]18, 140[.]82[.]4[.]20, 149[.]28[.]125[.]75, 172[.]96[.]15[.]104, 193[.]124[.]24[.]117, 207[.]90[.]236[.]231, 155[.]138[.]226[.]179, 172[.]96[.]15[.]103, 85[.]209[.]85[.]206, 207[.]174[.]31[.]92, 166[.]88[.]182[.]126, 23[.]146[.]184[.]221, 194[.]135[.]104[.]251, 23[.]133[.]88[.]96, 166[.]1[.]173[.]65, 38[.]180[.]244[.]209, 91[.]149[.]239[.]242, 155[.]138[.]211[.]27, 128[.]254[.]146[.]183, 166[.]88[.]182[.]65, 85[.]209[.]85[.]199, 82[.]153[.]134[.]38, 194[.]135[.]104[.]175, 38[.]180[.]81[.]153, 108[.]181[.]115[.]171, 38[.]180[.]195[.]187, 185[.]174[.]101[.]240, 194[.]36[.]209[.]227, 92[.]118[.]112[.]143, 185[.]174[.]101[.]69, 92[.]118[.]112[.]208, 108[.]181[.]182[.]143, 173[.]44[.]141[.]226, 162[.]252[.]173[.]12, 23[.]227[.]193[.]172, 185[.]33[.]86[.]15, 45[.]66[.]248[.]150, 5[.]8[.]63[.]178, 88[.]119[.]175[.]70,

TYPE	VALUE
IPv4	185[.]219[.]220[.]175, 45[.]82[.]85[.]50, 104[.]238[.]61[.]144, 193[.]203[.]49[.]90, 38[.]146[.]28[.]93, 88[.]119[.]175[.]65, 37[.]1[.]212[.]18

References

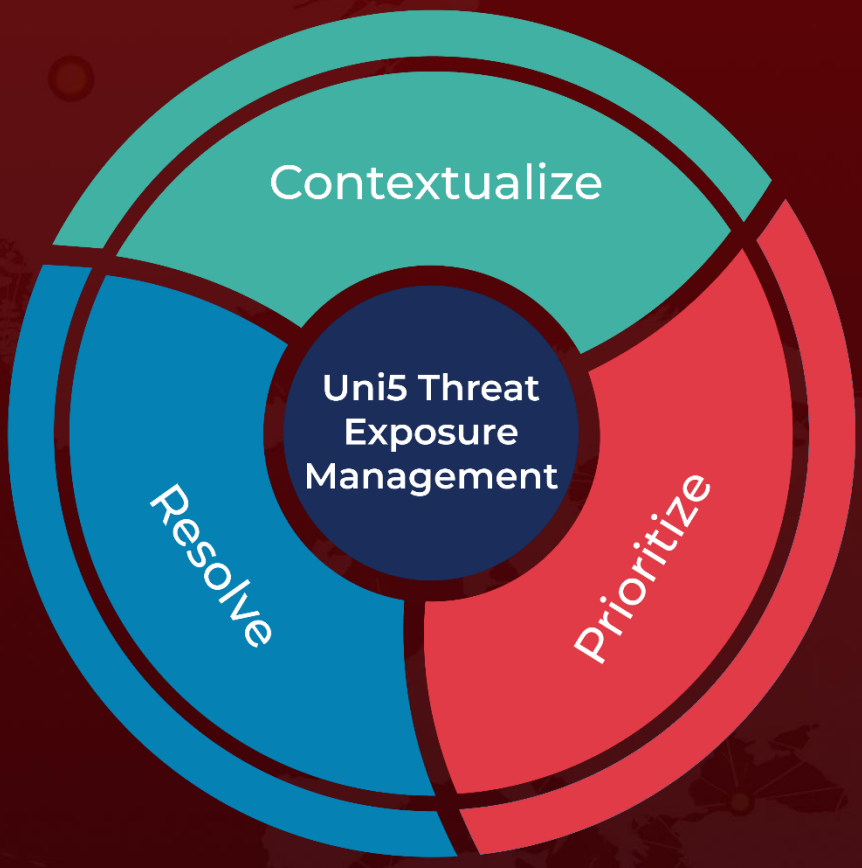
https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html

https://hivepro.com/threat-advisory/ransomhub-the-raas-powerhouse-exploiting-200-victims/

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

March 17, 2025 • 8:30 AM

More at www.hivepro.com