Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

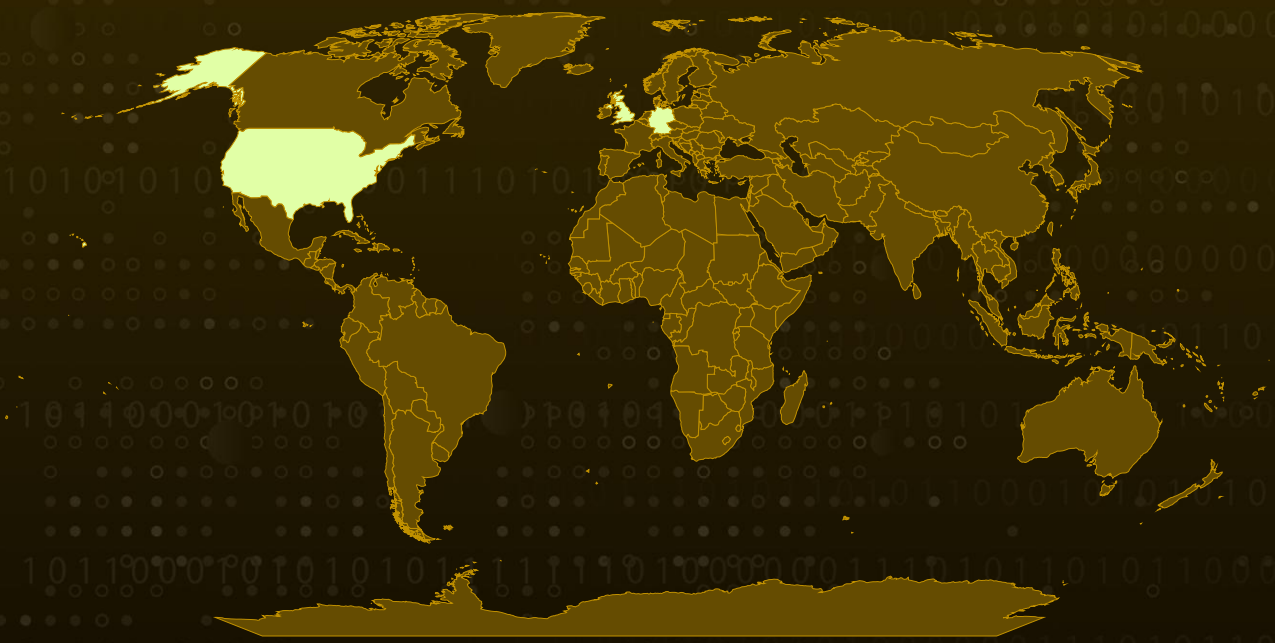
SERPENTINE#CLOUD: A New Benchmark for Malware Stealth

Date of Publication	Admiralty Code	TA Number
June 19, 2025	A1	TA2025194

Summary

Attack Commenced: 2025
Targeted Countries: United States, United Kingdom, Germany
Affected Platform: Windows
Malware: AsyncRAT, RevengeRAT
Campaign: SERPENTINE#CLOUD
Attack: The "SERPENTINE#CLOUD" campaign represents a highly sophisticated and stealthy malware operation that innovatively leverages legitimate Cloudflare Tunnel infrastructure to deliver malicious payloads. Initiated through phishing emails containing disguised Windows shortcut (.lnk) files, the attack unfolds in a multi-stage process involving obfuscated batch, VBScript, and Python scripts, designed for advanced evasion. This culminates in the memory-injection of Donut-packed payloads, enabling fileless execution that minimizes forensic traces and establishes full command and control over compromised systems, with observed final payloads including RATs such as AsyncRAT or RevengeRAT. By exploiting trusted cloud services and employing adaptive, multi-layered techniques, SERPENTINE#CLOUD highlights a significant evolution in cyber threats.

Attack Regions



Attack Details

#1 The "SERPENTINE#CLOUD" campaign marks a significant advancement in sophisticated malware delivery, expertly blending stealth, multi-stage execution, and the abuse of legitimate cloud infrastructure. The operation commences deceptively with highly targeted phishing emails, often themed around urgent invoices or payments, and has primarily been observed targeting entities in the US, UK, Germany, and other regions across Europe and Asia. These emails contain zipped attachments that, upon extraction, reveal malicious Windows shortcut (.lnk) files. These LNK files are meticulously disguised with PDF icons and friendly display names to trick unsuspecting users into execution.

#2 Upon execution of the malicious LNK file, a cascade of heavily obfuscated scripts written in batch, VBScript, and Python are deployed. This multi-layered approach is central to the campaign's design, with each script progressively downloading and executing subsequent components to build a robust and resilient infection process. The threat actors have evolved their initial access methods from simpler .url or basic .bat files, which were more easily flagged to the more deceptive .lnk files. They further enhance evasion by employing WebDAV protocols to fetch later stages directly from Cloudflare's tunneling service.

#3 A defining characteristic of SERPENTINE#CLOUD is its strategic abuse of Cloudflare Tunnel infrastructure. Attackers exploit subdomains to host and deliver their malicious payloads, enabling secure, outbound-only connections from compromised machines to their C2 infrastructure. This method effectively bypasses traditional firewall rules and network monitoring tools, as traffic routed through Cloudflare.

#4 The elaborate infection chain culminates in the delivery of sophisticated Python-based shellcode loader playing a pivotal role, executing Donut-packed payloads directly into the system's memory. The ultimate objective of these payloads is to establish full command and control over the compromised host, with observed final payloads including RATs such as AsyncRAT or RevengeRAT enabling attackers to conduct actions such as data exfiltration, surveillance, and potentially to deploy further malicious software or achieve lateral movement within the victim's network.

#5 Finally, the SERPENTINE#CLOUD campaign strongly prioritizes persistence on compromised systems. Threat actors deploy scripts to the user's startup folder to ensure re-execution upon system reboot, and multiple files are often configured to reinitialize the entire infection chain if any component is disrupted. The judicious use of PowerShell keeps these persistence mechanisms hidden during execution, and environmental checks are sometimes incorporated to refine subsequent attack stages. Notably, the use of **Cloudflare Tunnels** for deploying various RATs has been observed in previous campaigns leveraging similar tactics.

Recommendations

Strengthen Email Security Posture: Deploy advanced email security gateways equipped with robust attachment sandboxing, URL filtering, and threat intelligence capabilities. These solutions should be capable of deeply analyzing attachments like zipped LNK files and proactively blocking or flagging links to suspicious domains, particularly those hosted on free cloud services or dynamic DNS providers.

Restrict Unnecessary File Execution: Implement Group Policies or other technical controls to restrict the execution of specific file types, such as .lnk files or certain script interpreters (VBScript, Python), from user-writable directories or untrusted sources. Consider application whitelisting to allow only approved applications and scripts to run, significantly reducing the attack surface.

Monitor Cloudflare Tunnel Traffic with Caution: While Cloudflare Tunnel is a legitimate service, its increasing abuse by threat actors necessitates heightened scrutiny. Implement network monitoring solutions capable of analyzing outbound connections to trycloudflare.com or similar Cloudflare subdomains. Look for unusual traffic patterns, large data transfers, or connections from unexpected systems that might indicate malicious C2 or payload delivery.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0008 Lateral Movement	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel

T1132 Data Encoding	**T1572** Protocol Tunneling	**T1027** Obfuscated Files or Information	**T1027.010** Command Obfuscation
T1027.012 LNK Icon Smuggling	**T1027.013** Encrypted/Encoded File	**T1036** Masquerading	**T1218** System Binary Proxy Execution
T1564 Hide Artifacts	**T1564.006** Run Virtual Instance	**T1021** Remote Services	**T1021.007** Cloud Services
T1055 Process Injection	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1059.005 Visual Basic	**T1059.006** Python	**T1204** User Execution	**T1204.001** Malicious Link
T1204.002 Malicious File	**T1620** Reflective Code Loading	**T1072** Software Deployment Tools	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	nhvncpure[.]shop, nhvncpure[.]sbs, nhvncpure[.]click, nhvncpureybs[.]duckdns[.]org, nhvncpurekfl[.]duckdns[.]org, ncmomenthv[.]duckdns[.]org, hvncmomentpure[.]duckdns[.]org, nhvncpure.twilightparadox[.]com, nhvncpure1[.]strangled[.]net, nhvncpure2[.]mooo[.]com, nhvncpure[.]duckdns[.]org, lp145[.]ip-51-89-212[.]eu, trycloudflare[.]com, depot-arrange-zero-kai[.]trycloudflare[.]com, djksncb.duckdns[.]org, duckdns[.]org, twilightparadox[.]com, strangled[.]net, mooo[.]com

TYPE	VALUE
IPv4	51[.]89[.]212[.]145, 192[.]169[.]69[.]26
URLs	hxxps[:]//vocabulary-bangladesh-designation-manhattan[.]trycloudflare[.]com, hxxps[:]//flour-riding-merit-refers[.]trycloudflare[.]com, hxxps[:]//agricultural-brooks-nevertheless-hawk[.]trycloudflare[.]com, hxxps[:]//departments-emperor-maximize-synopsis[.]trycloudflare[.]com, hxxps[:]//integration-previous-brilliant-true[.]trycloudflare[.]com, hxxps[:]//works-clubs-attendance-vi[.]trycloudflare[.]co, hxxps[:]//pop-incl-accountability-pharmacy[.]trycloudflare[.]com, hxxps[:]//bought-boulder-algeria-warned[.]trycloudflare[.]com, hxxps[:]//depot-arrange-zero-kai[.]trycloudflare[.]com, hxxps[:]//hobbies-gratis-literally-dry[.]trycloudflare[.]com, hxxps[:]//bold-accepts-wide-te[.]trycloudflare[.]com, hxxps[:]//lender-router-exclusively-fraction[.]trycloudflare[.]com, hxxps[:]//whatever-hearings-transmission-daisy[.]trycloudflare[.]com, hxxps[:]//catalogs-amounts-functions-chicago[.]trycloudflare[.]com, hxxps[:]//bold-accepts-wide-te[.]trycloudflare[.]com, hxxps[:]//superb-rotation-gourmet-frequently[.]trycloudflare[.]com, hxxps[:]//now-refer-several-tariff[.]trycloudflare[.]com, hxxps[:]//wizard-individual-intervals-franklin[.]trycloudflare[.]com, hxxps[:]//surprise-poly-longitude-populations[.]trycloudflare[.]com, hxxps[:]//travel-sagem-distant-potential[.]trycloudflare[.]com, hxxps[:]//obtaining-removing-blocking-effectiveness[.]trycloudflare[.]com, hxxps[:]//bought-boulder-algeria-warned[.]trycloudflare[.]com, hxxps[:]//uploaded-overall-seating-browser[.]trycloudflare[.]com, hxxps[:]//cold-neon-springfield-asset[.]trycloudflare[.]com, hxxps[:]//dolls-pet-bon-shirts[.]trycloudflare[.]com, hxxps[:]//shed-determination-conviction-herself[.]trycloudflare[.]com, hxxps[:]//works-clubs-attendance-vi[.]trycloudflare[.]com, hxxps[:]//archived-hungary-paxil-tubes[.]trycloudflare[.]com, hxxps[:]//reensboro-even-suburban-str[.]trycloudflare[.]com, hxxps[:]//greensboro-even-suburban-str[.]trycloudflare[.]com, hxxps[:]//vertical-pentium-b-dead[.]trycloudflare[.]com, hxxps[:]//violin-amendment-stranger-job[.]trycloudflare[.]com, hxxps[:]//diy-solution-warriors-workflow[.]trycloudflare[.]com, hxxps[:]//fy-golf-fraction-bath[.]trycloudflare[.]com, hxxps[:]//menu-conviction-given-not[.]trycloudflare[.]com, hxxps[:]//opportunities-choosing-non-torture[.]trycloudflare[.]com, hxxps[:]//flexibility-hawaiian-ever-bon[.]trycloudflare[.]com, hxxps[:]//hose-jerusalem-sure-older[.]trycloudflare[.]com, hxxps[:]//milton-smithsonian-raising-mind[.]trycloudflare[.]com, hxxps[:]//eastern-instructional-ant-jungle[.]trycloudflare[.]com/cam[.]zip

TYPE	VALUE
SHA256	193218243C54D7903C65F5E7BE9B865DDB286DA9005C69E6E955E31EC3EFA1A7, 3B97A79ED920A508B4CD91240D0795713C559C36862C75EC6C9A41B4EC05D279, 32253D3EA50927D0FD79F5BFDD6EE93C46AA26126CE4360D9915FABD2E5F562F, 81C47E749E8A3376294DE8593C2387A0642080303BB17D902BABFF1DE561E743, 017FD2003F8EAA65FF85131322F5FAEC1E33851178832843802084 8EDF3DFD8D, 22DE5FFC9BFFE49C4713113AC171B95E016ED0F09065BFEE1394A579174E8DD6, E78FF6F51A3FAECF4D20CD5B71B2396B7C2FEC74AF19122B1E1EEE432C13B773, 100970B2EB83E3A80CB463126845619A05C979D235B07ECA4B1C2027772334EC, 63FFC2B66E32111CD5BE311AD499BD15DA5D28EDC05B7F3DA43DFE77F3E2C7F8, F6B403D719D770FFB6CC310E2F97889998224A563A1A629BE5B7F8642B5F00BA, 0484DE293F2C125132CAA585229A8702AF00CB645AA27684C2EE6F9F4F3EDB6F, FCAD11819FCA303372182C881397E0B607C0DA64ECDA1CF9B2C87CF5F8F5957A, B57F591866A0D5A68B76382476087310A6F96C34B9449D070619DF6B763E6A1D, 139B2B11B1C0D9697A78C1A9535A7A4E4F41D4833B247C1CDDC91ABE3BEBE3E4, E78FF6F51A3FAECF4D20CD5B71B2396B7C2FEC74AF19122B1E1EEE432C13B773, 3CF0E84EA719B026AA6EF04EE7396974AEB3EC3480823FD0BB1867043C6D2BF9, F0F7276C54E6D6B41732D51FB1B61366AA49C6992A54D13FFD24AEE572FFAF95, 7B4931E498CE8B3A15BFF5FDFD3A547397E85296462DE3D2D322B4B3FE52F26C, CDD097329D2C539A3C67C278530D951964F593A4FFB90A31B0EFAD4C3E0ED5BA, 13A8150B68A3FAD30C48778B80BAA7C97C1A813F37688CBE14B1D3F5AB69AC72, 9DC84272D11E273B6B4DEFEABB7E3DD6EBE0E418FB96F9386DD7F1F695636384, 715CEF51FFCFAEC05A080A0E0DB4D88BB5123E2ADE4A1C72FD8C10F412310C1D, 35DB935E80BEDA545577A5F7FF6DE7C8A8B1376C363B0D5C704DC14EBC1D2F93,

TYPE	VALUE
SHA256	AECE8FA3B8EA803E9CA9BF06B6FD147B54CD3A00207AAD36871DA424A9CA4748, 3D3A6D7905CA1387F3EC7A637CB672D6B6EFA0F8EFDBF819F756A8E5F92BC960, DF9ECDE8058CB9756BDE3DE1A2A2727A3709F238885165B7FEB747EB10DE1502, 6134BAC7A6215A158DFEE2F6824B9E648DE073EEB0499A325C8EF2EA43DAB84C, 45BABDCBD661450B3643A14DC960DAF7FAFAEA2876FEE249A2A2417B15272A4B, 049A576A5BC77AF51065D28A711656BD93FF6BD5FE74D54064A66A802D14E438, CDCD71A62CD579B8AA01792769B99961CDE2D34419E066C4A45943559E0C4029, 7AA7406147E1365A78412BA44ADECEE8C5F5B8365C61A2BC4DE3BC2C37C0E1DD, 36F02254BF8631E5E4CDB83FFB4621C85AB5E41FB20983C7B1E2B2292EF02D0A, 1A15C4D654D88DC3F1943361CB69BB5DEA90C758A6FE4E8B72E683BA9354C480, 5710A67E4A3A633A8B3446A9E94B8CDD11B00E922A5585802A94BD91FA2A5D82, 427FA98FC638D1EC0D8C6863D9B2E7E58642287BEF11404089B45024564B54F4, A6F04F0C7B2827F4C102B1B1E3978805A628DB1EE83FB61E640FF215BA732262, D70B2EC135B1DC4D0BE8E029574D9E686B29C0225022FC65D0AF0811FDF88CE7, E8DAB17006948378B94183226F8E2D345A6AEB6688BE02E4EE578D4618D9FB43, 0172CA7C07D1D52DC163090886D5F32A5DCF528506D19203E4C405495F51C60B, 36D05B8CA1B6E629BFCCC2342DB331EB88D21EBCE773CA266F664CD606BC31B7, F626A8E8E1EB51A23B56B69060A76B9F566944C1B4DF044B8B4B68861FB8A761, 9096D706D90598BA0DD6473A1CF0529AB7AB486E753B2EBF6B180D2BEBF68990, DEF421B838A43054AB8336AB4DB6BF8F973E1BBABC2C38E278C3FA4EA459F961, 408A7C9B1AFCC367A086C1386DA621D532632E2B54C47F7061161105BD63A37E, 547250102B3B779CFEAB6F9FF4B67FFD577D83D9E8027DF90697B01E24256D67, 850FB460F68AB1B5810F96DB1FF16954CD1B590B921968FCBC3203135B40ACC0,

TYPE	VALUE
SHA256	759D6929E4456668A93D92B2AEA311D9B7590EBAB4A4DA3CD8602B8C0B8111D5, AC6EB3435CEC6058FFEA590AC51507B3313A74EA07893B984F2D87BE12E17027, 5D932BFDA0FFD31715700DE2FD43FC89C0F1D89EEABAC92081EBE2062DA84152, AC6EB3435CEC6058FFEA590AC51507B3313A74EA07893B984F2D87BE12E17027, 4D2FCCAD69BB02305948814F1AA6EF76C85423EB780EC5F3751B7FFBF8B74CA3C, 5022CD6152998D31B55E5770A7B334068CE8264876C5D6017FD37BEB28E585CA, 6211E469524A4BD7D3FA9C59A11A2F5BC6EAC34D839A5BA0BA8A616B82A098C8, 3AD13C59CEBDF654D2F04C26C4A0726F2E1BB3B1682BC9810A3B99FBD17D59C0, C2C8F3A7A7B07FC4F62B943011EF4239FF938077FDE2CC248B406616254F44D5, C2C8F3A7A7B07FC4F62B943011EF4239FF938077FDE2CC248B406616254F44D5, 1534D21DDD3A58B076EF49682E0CF7009ABFB4248FA70426B5436C02CAEAF82F, 6912F9484886EC8B8837AC3E2E63397A9C4FD499407DBAB92F730F0D6B4315FC, 8164643B2EFDCFEDAFAFB61919CF93C496375002F6AD806725C85A7C871C34EA, 1CACC0E005A506572B26D859579840188758C37377B19F33BBD084D7EF2956A8, 821F0956D3F52819C90035041C0F4C0EC644924AF46222C5913E05DE1C385B04, 521982A864B3B40B2627CF2067546ACCF346E2C97924A73DBC767907071C4029

References

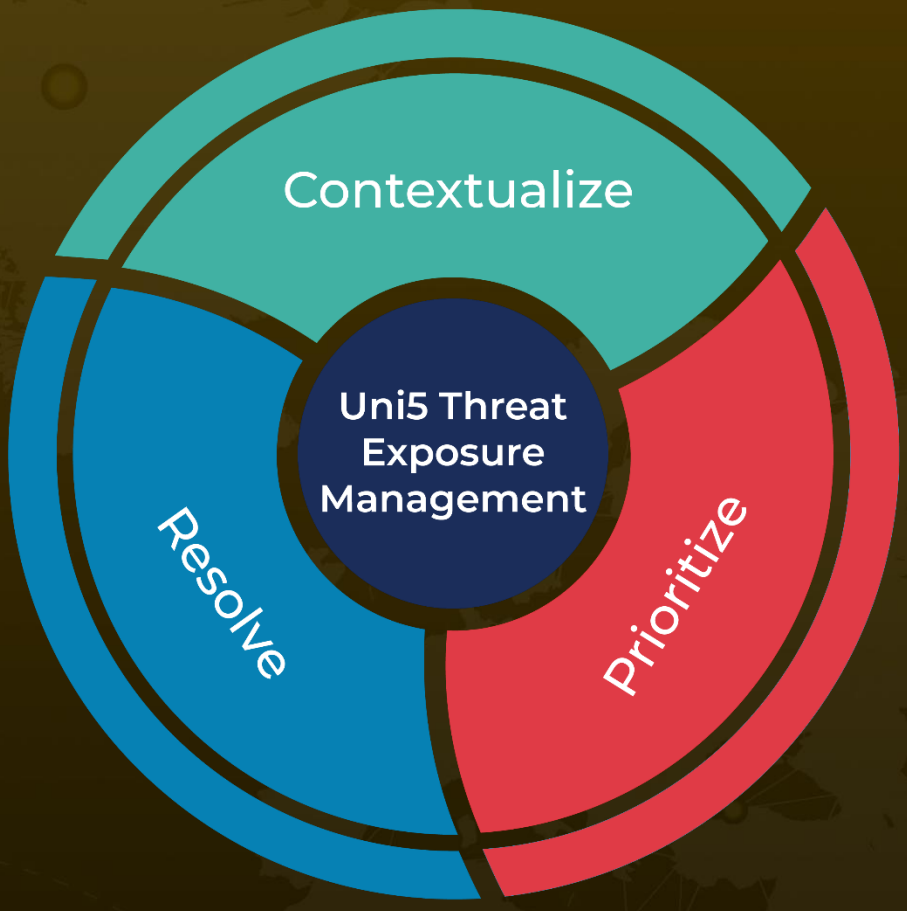
https://www.securonix.com/blog/analyzing_serpentinecloud-threat-actors-abuse-cloudflare-tunnels-threat-research/

https://hivepro.com/threat-advisory/rats-on-the-loose-through-abused-cloudflare-tunnels/

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

June 19, 2025 • 6:15 AM

More at www.hivepro.com