Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

GachiLoader Deployed via the YouTube Ghost Network

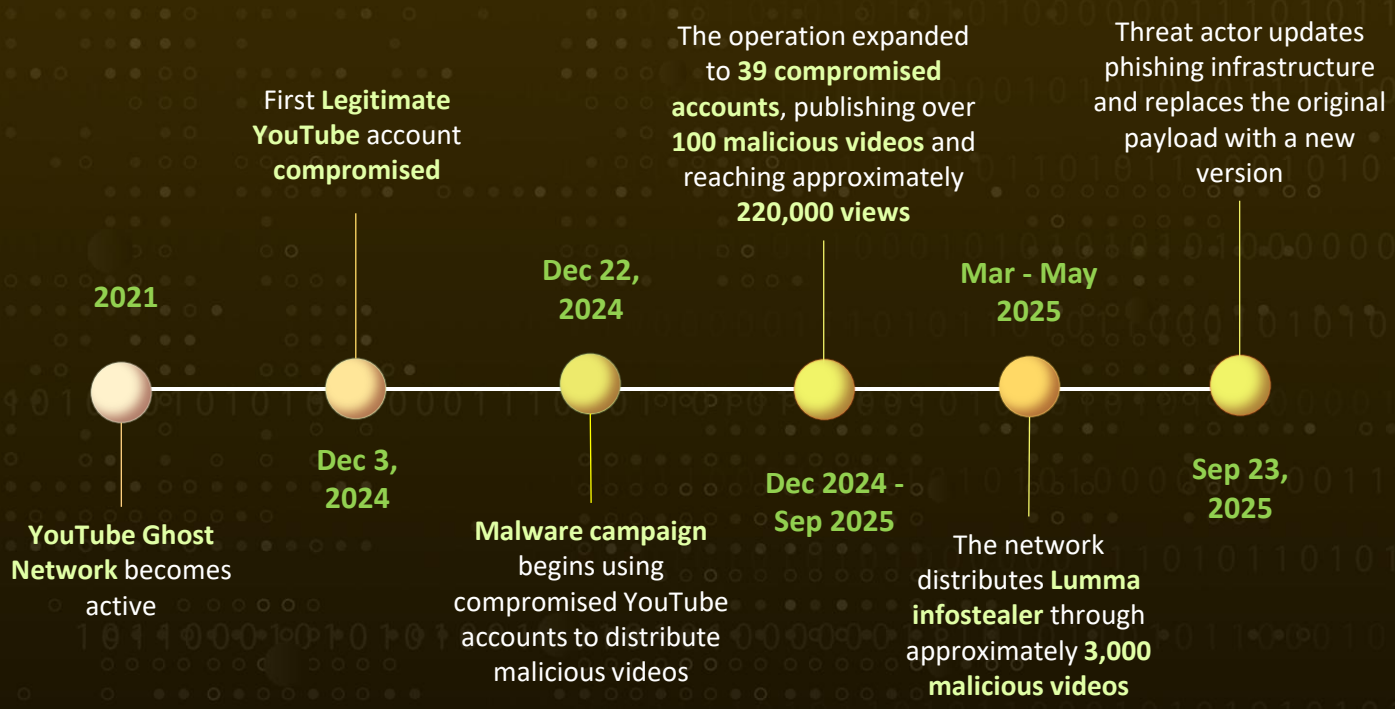
Date of Publication	Admiralty Code	TA Number
December 19, 2025	A1	TA2025386

Summary

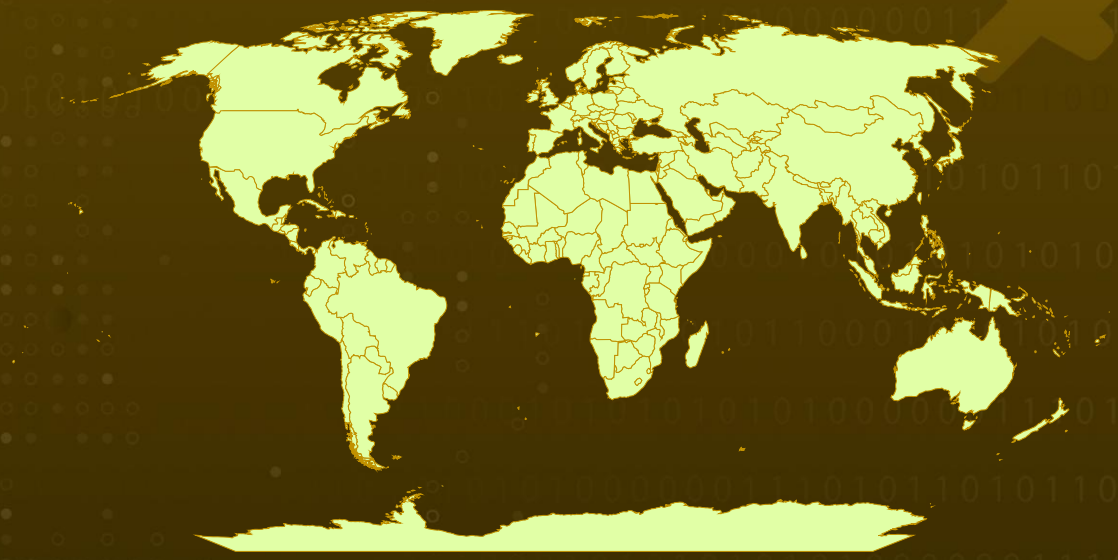
First Seen: 2021
Malware: GachiLoader, Kidkadi Dropper, Rhadamanthys Infostealer
Affected Platform: Windows
Targeted Region: Worldwide

Attack: GachiLoader is a Node.js–based malware loader used to deliver the Rhadamanthys infostealer through a large-scale campaign that abuses compromised YouTube accounts. The campaign highlights a growing trend toward unconventional malware development and refined distribution methods, underscoring the increasing abuse of trusted platforms like YouTube for scalable malware delivery.

Attack Timeline



Attack Regions



Attack Details

#1 GachiLoader is a newly identified, heavily obfuscated loader written in Node.js and designed to deploy multiple malicious payloads on compromised Windows systems. Its primary role in the observed campaign is the delivery of the Rhadamanthys infostealer. The loader is distributed through the YouTube Ghost Network, a large-scale malware delivery operation that hijacks legitimate YouTube accounts.

#2 These compromised channels promote fake game cheats and pirated software, exploiting user trust and platform visibility. Victims are lured through video descriptions containing links to password-protected archives hosted on common file-sharing services, often accompanied by instructions to disable Windows Defender before execution.

#3 Once launched, GachiLoader begins by profiling the host system. It collects information such as the operating system version and installed security products, then transmits this data via POST requests to the command-and-control infrastructure. This reconnaissance phase helps the malware evade sandbox environments and security analysis.

#4 Rhadamanthys payload delivery varies by campaign. In one case, GachiLoader retrieves the next-stage payload directly from its command-and-control server. In another, the payload is embedded within the loader itself and executed through a secondary component known as Kidkadi, which is dropped during runtime.

#5 GachiLoader reflects a broader shift in malware development toward unconventional technologies. By leveraging Node.js, threat actors complicate detection while expanding operational flexibility. Combined with the abuse of trusted platforms like YouTube and a novel executable injection technique referred to as "Vectored Overloading," which hides a malicious executable inside a legitimate DLL and abuses Windows exception handling to quietly trigger execution, this campaign demonstrates a refined and deliberate approach to modern malware distribution.

Recommendations

Endpoint Hardening and Execution Control: Reduce exposure by limiting script and runtime abuse on Windows systems. Node.js should not be present or executable on endpoints unless there is a clear business requirement. Enforce application allowlisting to prevent unauthorized loaders and secondary executables from running, particularly those launched from user-writable directories such as Downloads or Temp.

Detection and Behavioral Monitoring: Implement behavioral detection for abnormal process activity, including Node.js instances performing system reconnaissance or initiating outbound network connections. Monitor for suspicious artifacts such as randomly named .lock files in temporary directories, which may indicate execution control mechanisms used by loaders like GachiLoader.

Network Visibility and Command and Control Detection: Inspect outbound traffic for unexpected POST requests to unfamiliar infrastructure originating from non-browser processes. Early-stage beaconing used for host profiling and payload retrieval can often be detected through network monitoring and anomaly-based alerts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**T1566** Phishing	**T1059** Command and Scripting Interpreter	**T1547** Boot or Logon Autostart Execution
T1548 Abuse Elevation Control Mechanism	**T1562** Impair Defenses	**T1497** Virtualization/Sandbox Evasion	**T1055** Process Injection
T1027 Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1574** Hijack Execution Flow	**T1082** System Information Discovery
T1057 Process Discovery	**T1005** Data from Local System	**T1071** Application Layer Protocol	**T1573** Encrypted Channel
T1041 Exfiltration Over C2 Channel	**T1566.002** Spearphishing Link	**T1059.007** JavaScript	**T1059.001** PowerShell
T1548.002 Bypass User Account Control	**T1562.001** Disable or Modify Tools	**T1497.001** System Checks	**T1055.012** Process Hollowing
T1027.002 Software Packing	**T1574.002** DLL Side-Loading	**T1071.001** Web Protocols	**T1573.002** Asymmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	062d342f59136c3bbc729e0c412d2c2589b6f9058912583eeb9b61d7916db00e, 34e1cd959c0c586fcd495225803061e6e2a19e7818c47a46a47822ba6726500d, 434fc84cc190bb0c8af86d3566d6517672fed9c171eb0df5c7541f0dce679c8b, 606eca698d0d4a67b21428b0812a261daab36598fded60b189106b0b27992225, 775b05b8cc8d03751828986727cd1929caf6868e1df9cd21e9366c48ce161c5e, 872fde8128f3a0f074975b6ca0d83fa56a8289b2063351f298bbf0c9025948d3, 99f4755fd9b25aadae4e154d661ccceecbbb3d4343dc6c81e04aa81516be81d0, a4e2c0ffb93103db23777c12b48a31816b83b0799c9bc71e92bb576e884d76d4, b48f3e7e6c67bfb3c73c85a33a377f9bb840e1b7b09871ab29a19cdb7965d5d1, c4266da90d6c655388ae8d64aebf5f9178adbbe486b2249e6bb7d18451f28a3b, cc95609cc375263129b8f425800a9bb462055b11dbf0d8aef2b3312aa2e90daf, f0de35ff0b889c7e93a89e918488a33aa21e4b6e7743ae87f1993ea77b237ecf, 00bcfecad4b679f72c50cbdcd883caf55b6a1f641258a636317871c7b8940156, 00db4aa911e95ecfafa6f10ebfeb9f0a8051ee63de51ea1d9515ece5be2a294b, 01a3da42f74578c0b7c1146f30eceb2a2bc26c2d814a48fcf29ae527a1048aff, 028711c1b435c773ba600a863f4d4a2d1218860de799a1275d15d4ea93f0cbef, 02c0de5116d9b05d930e4858cd9768cc2ba70e91be62690439537fdf0f52de53, 032a297bfbdc94226f0d88c77ab27148c54ebde6bfa2750fed09b1d8667ddcd6, 03d55245ef2766943813c0d1eaa3859d3918ee6fed2705bb5eeb38f4f87a5643, 079a180eeed0f4fc84c2412ba0398a79c5262efa1d9e8fd53290cd001b5abf9f,

TYPE	VALUE
SHA256	094240cd298de1121da36adb96b3cdd632f866837f27e3951b6a0a544e5437f6, 0a6d41411ef3c65540a525dc5c3ab0964cd595aa73c3a477a8a96ec986277660, 0bd44592e75854a1c763384bf9dcea6dfe1174f6f45df342ebd9dfaa3a27dc85, 0c03845b9e2ff5ddac56f6e75b8e9dadf1a7bd1681d074e732478596b3173922, 0f81656ce724b65c230c4d63259c3a0edff20cc664de964f16451417eda60005, 14bfaf75b5c7ffac451f41352f8e94b6cc060efe7d645189795fa921f4e602bc, 16b2f7d9d4ace9e3004bd47f97c252a7fea21662656ec6b906d30a6b21900fc4, 18649874ab887ab613a3ccdd7cddc683e2b21f7cbe0762d2ce8201fc7e57540c, 1d28c23b271eb2156bf2780cb0dd042573f38f4758ef61877a7347bbbc756c8b, 1ebeca5dc62d759904c47597ebeb67865017a99892081c94d7647206b78a6cd2, 1f35a5ee4ead5c286f3e0d3ddecaf8789f12da7b8b7422b0511af619353284b7, 2038f38ccd42cd1df84abfb5915e3a6eb9c976b8d822768068343716f46a09f1, b429a3e21a3ee5ac7be86739985009647f570548b4f04d4256139bc280a6c68f, da36e5ec2a8872af6e2f7e8f4d9fdf48a9c4aa12f8f3b3d1b052120d3f932f01, b41fb6e936eae7bcd364c5b79dac7eb34ef1c301834681fbd841d334662dbd1d, 7d9e36250ce402643e03ac7d67cf2a9ac648b03b42127caee13ea4915ff1a524, ad81b2f47eefcdce16dfa85d8d04f5f8b3b619ca31a14273da6773847347bec8, 19b6bb806978e687bc6a638343b8a1d0fbd93e543a7a6a6ace4a2e7d8d9a900b, 270121041684eab38188e4999cc876057fd7057ec4255a63f8f66bd8103ae9f2, ed0cbb7b137a10493319473610209016f2c1a8b9560876bc32999b472a32e18f, ee363c5bdc5e786b0b47840d8fe69a5bd71f3684a9eec5d9e49b9ab68c64c793, ee752ce83f645fe4d3db0b1d8c41428d7b9adf37e72a9c21c153450862d30906,

TYPE	VALUE
SHA256	eed231bda3ad5a946a254d06865610e50b05eabaece8f09f84323d9fb23e2742, ef4d2a7ca4306626ff90e53ebad63e243a50dff63f34eb0eeaeb4acb2f39c42b, f0269f2b26534acc3ef8bee5b243c54b14812769249a974b2e2b7eba9734a967, f1de30fa0eeedc1f1a7d97736cf751c88fb01456a182f97ede7294bc89bf69af, f4f18af4acee36826b8e2162749250ffb96fc7f8f154d181dd1b8179cf4da68d, f73e65f624f15d967951a6795c712daf31363ab1602485c164549b04989caaaf, f9648d34727738abe86310378929ab7a8d5c8f2698c913bc84dee9be49e3b96a, f98ce437118aeca437a43612858068f4ea6099bb93c63f1b4ffc4d4335e8eaed, fbae3424943aec7aea7ce380c7a83c89ca9c6ff243bfac5186edba6e560f5b66, fd06caf741fd4e5fc9f00c575cc22c00f1a7fd55e826a16dbabc8b3436ed64c4, 2ac4f1a2e22c99a823f18dba8ad5aafde0de98966d5534d5af61650d1f47997c, f87b964e6a619cae6bb8852822d70bee93d708da98214e3b2381ff0774ee8e62, 0e0a094e2d27a0e3583ff528296f784d29e139bed9ba41fdc6788169c83698b4, 72eb1f7a418def9d64aaadc556f9350d2a8c444eb7ab56fc59324c5d5f4d76f9, 33bba47346c03968977688bddbdd245210c06fb7686b4dfc78789c70e2a95219, f9ab9fc5f1e092ace1dcea7610f4643040a85a5385e3eab3c3666bfe09dc8d6b, 90fa0da74389a302edd4cdb641f280bf95b9f73ed7145f0f9c1728c576cfc0df, 1d405b03bc5913b6b43c06550ef0b9b02196b270625e4dc5fa0c37e8a424be25, ded68a8f5d0765740d469c08bd66270097f3474eab92ee1e65ddcdd6d15fca6e, 92c26a15336f96325e4a3a96d4206d6a5844e6a735af663ba81cf3f39fd6bdfe,
Domains	davpniktonevidit[.]cfd, nupogodi[.]cfd, nexus-cloud-360[.]com, globalmarket247online[.]com, vault-360-nexus[.]com, iietrich[.]cfd,

TYPE	VALUE
Domains	mceenzie[.]sbs, digitalservice365cloud[.]com, cxbnqdytjgrxutmzawczv[.]cg/gateway/0f4m3h8r[.]trz19, jfbcrmphnnikoktsmcpzirlplkwp[.]zl/gateway/8pv47lge[.]93qfg
Hostname	b30f0242-1c6a-4, xc64zb, server1, desktop-b0t93d6, wileypc, ralphs-pc, desktop-5oy9s0o, archibaldpc, comname_5076, tdt-eff-2w11wss, desktop-vrsqlag, desktop-d019gdm, lisa-pc, desktop-1pypk29, wok, desktop-wg3myjs, qarzhrdbj, julia-pc, work, q9itrkphr, desktop-wi8clet, john-pc, desktop-1y2433r, 6c4e733f-c2d9-4, desktop-7xc6gez, orelee pc, d1b_coursek, desktop-vkeons4, q9iatrkphr
IPv4	94[.]154[.]35[.]99, 176[.]46[.]152[.]18, 213[.]209[.]150[.]104, 62[.]60[.]226[.]233, 66[.]63[.]187[.]72, 178[.]16[.]52[.]231, 3[.]126[.]43
URLs	hxxp[:]//176[.]46[.]152[.]18[:]8181/gDatFeDway/r26ggaap[.]dssde, hxxp[:]//178[.]16[.]53[.]193/mK2k20ajW7kairt1mg88vT1aT9vwU5AZN9AkYYs2QBNbnXV3ph/YEr2KP0jEBhSDdVcS9cWNhbKUgDxcEm9kqxLwFAdHgmKyw7FZq[.]exe, hxxp[:]//180[.]178[.]189[.]34[:]8181/gDatFeDway/mh3af5md[.]wg4ja, hxxp[:]//180[.]178[.]189[.]34[:]8181/gDatFeDway/ujp8k5q9[.]kbtsk,

TYPE	VALUE
URLs	hxxp[:]//185[.]141[.]216[.]120[:]1888/gateway/st2jdbg8[.]gsg45, hxxp[:]//78[.]16[.]53[.]193/mK2k20ajW7kairt1mg88vT1aT9vwU5AZN9AkYYs2QBNbnXV3ph/YEr2KP0jEBhSDdVcS9cWNhbKUgDxcEm9kqxLwFAdHgmKyw7FZq[.]exe, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/el3tkioe[.]xcg4w, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/mbw0n34s[.]gibis, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/wwpac3ey[.]q23nf, hxxps[:]//94[.]74[.]164[.]157[:]8888/gateway/6xomjoww[.]1hj7n, hxxps[:]//openai-pidor-with-ai[.]com[:]6343/gateway/pqnrojhl[.]adc7k, hxxps[:]//178[.]16[.]53[.]236[:]6343/gateway/pqnrojhl[.]adc7k, hxxps[:]//5[.]252[.]155[.]99/gateway/r2sh55wm[.]a56d3, hxxps[:]//5[.]252[.]155[.]231/gateway/3jw9q65j[.]b3tit

References

https://research.checkpoint.com/2025/gachiloader-node-js-malware-with-api-tracing/

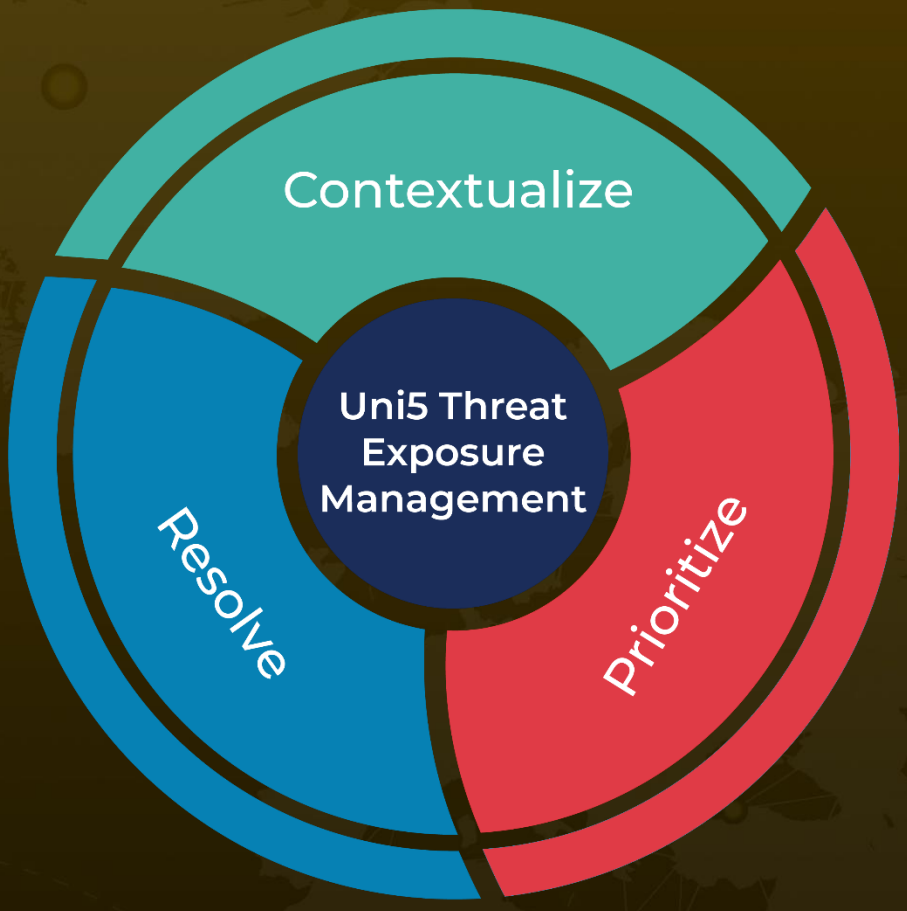
https://research.checkpoint.com/2025/youtube-ghost-network/

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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

December 19, 2025 • 8:00 AM

More at www.hivepro.com