Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

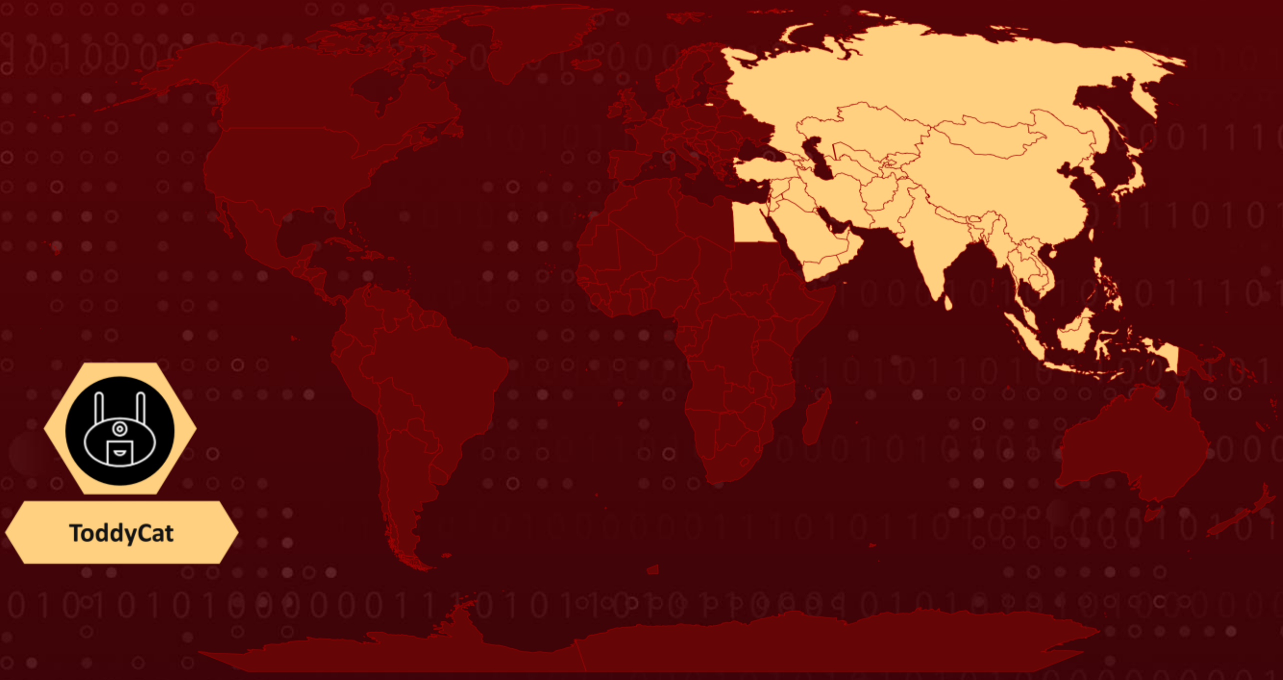
Unraveling the Intricate Arsenal of Stayin' Alive Campaign

Date of Publication	Admiralty Code	TA Number
October 12, 2023	A1	TA2023411

Summary

Active Since: 2021
Malware: CurKeep, CurLu, CurLog
Threat Actor: ToddyCat
Attack Region: Asia
Targeted Industries: Telecommunication, Government
Attack: The Stayin' Alive campaign, affiliated with the ToddyCat group, employs sophisticated tactics, including spear phishing and DLL sideloading, to target specific countries in Asia, particularly entities belonging to the Telecom industry and government.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-23748	Dante AV DLL sideloading vulnerability	mDNSResponder.exe v1.3.1 and earlier Dante Application Library for Windows v1.2.0 and earlier	✗	✗	✓

Attack Details

#1 The "Stayin' Alive" initiative, an enduring campaign in operation since at least 2021, strategically focuses its efforts primarily on the Telecom industry in Asia and government entities, with a specific emphasis on countries such as Kazakhstan, Uzbekistan, Pakistan, and Vietnam.

#2 Affiliated with Chinese APTs renowned for their sophistication, the "ToddyCat" group distinguishes itself by deviating from established patterns, showcasing its distinctive approach since at least 2020. Commencing its operation through spear-phishing emails containing archive files, the Stayin' Alive campaign employs a sophisticated tactic by exploiting CVE-2022-23748, a DLL sideloading vulnerability within Dante AV systems software.

#3 ToddyCat adeptly utilizes DLL sideloading, a technique popular among Chinese threat actors, deploying loaders and downloaders onto targeted devices. The attack unfolds by launching a legitimate executable, signed by Zoom, which in turn loads dal_keepalives.dll, triggering a simple backdoor known as CurKeep.

#4 Upon execution, the payload engages the report functionality, transmitting basic reconnaissance information to the C&C server. Further analysis of the newly identified infrastructure unveils additional samples, predominantly loaders like CurLu and CurLog, employed in targeted attacks within the same geographical region.

#5 Another noteworthy payload, CurCore, is a compact, restricted backdoor that, when activated, loads and resolves functions associated with HTTP requests. The array of tools mentioned is bespoke and likely designed for easy disposal. While the commonalities between these tools do not definitively establish a direct link between the "Stayin' Alive" campaign and ToddyCat, there is a strong indication of a shared nexus and infrastructure. Additionally, it is noteworthy that ToddyCat has been documented operating in the same geographical regions as the "Stayin' Alive" campaign.

Recommendations

Patch Management: Ensure that software, especially critical systems like Dante AV systems, is promptly updated with the latest security patches to mitigate vulnerabilities such as CVE-2022-23748.

Enable Audit Logging: Activate audit logging for DLL loading events on Windows endpoints. This allows for the collection of detailed information about DLL loads, helping security teams identify anomalous behavior.

Vendor Risk Management: Assess and monitor the security practices of third-party vendors, especially those providing critical software or services, to ensure they meet security standards and do not introduce additional risks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**T1588.006** Vulnerabilities
T1566 Phishing	**T1598.002** Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1053** Scheduled Task/Job
T1543 Create or Modify System Process	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1055** Process Injection
T1083 File and Directory Discovery	**T1570** Lateral Tool Transfer	**T1105** Ingress Tool Transfer	**T1071** Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6eaa33812365865512044020bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746, 78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd, 295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719, 409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c, 462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a, 4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6, 437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a, c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac, da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9, 451f87134438fa7e5735a865989072e7bab4858ca0b1e921224ed27dea0226b0, 93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347, 482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651, 877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697, c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0, d94ed414dbfb9bbcba42e3bf2db3b76eb8172b03133d1745d6abcde6f9edbaa7, 732621aa53683c16edf3959dfe9d93de5359c431c130784b31d4a598fbbd80a9, 12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc, a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172, 60030b970491bced72a56c9dde09a1d2260becfbf80a2b0d217a0b913e781c3a, 36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652, b3fc497f94ac04abc4c9a6f23ab142fdc2387c520ce5c6fdae1b511793bc6ba2,

TYPE	VALUE
SHA256	caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1, 4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d, d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30, 47de9bf5f60504c229fe9f727aa59ba5c34d173a23af70822541a9e485abe391, 1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6, 2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed, d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4, 6f3de35c531993aa307729e2046ff7aa672f5058b7e0fc6557bbd4c500fb46e7, 2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782, 1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a, a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9, 778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e, 7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e
IPv4	70[.]34[.]201[.]229, 185[.]136[.]163[.]129, 45[.]77[.]171[.]170, 167[.]179[.]91[.]150, 185[.]243[.]112[.]223, 207[.]148[.]69[.]74, 139[.]180[.]145[.]121, 77[.]91[.]75[.]232, 178[.]23[.]190[.]206, 136[.]244[.]111[.]25, 185[.]242[.]85[.]124, 45[.]159[.]250[.]179, 178[.]23[.]190[.]206, 65[.]20[.]68[.]126
Domains	ns01[.]nayatel[.]orinafz[.]com, eaq[.]machineaccountquota[.]com, qaq2[.]machineaccountquota[.]com, imap[.]774b884034c450b[.]com, admit[.]pkigoscorp[.]com,

TYPE	VALUE
Domains	update[.]certexvpn[.]com, cyberguard[.]certexvpn[.]com, gist[.]gitbusercontent[.]com, git[.]gitbusercontent[.]com, raw[.]gitbusercontent[.]com, cert[.]qform3d[.]in, admit[.]pkigoscorp[.]com, sslvpn[.]pkigoscorp[.]com, cdn[.]pkigoscorp[.]com, idp[.]pkigoscorp[.]com, ad[.]fopingu[.]com, proxy[.]rtmcsync[.]com, pic[.]rtmcsync[.]com, backend[.]rtmcsync[.]com

Patch Link

https://www.audinate.com/learning/faqs/audinate-response-to-dante-discovery-mdnsresponder-exe-security-issue-cve-2022-23748

References

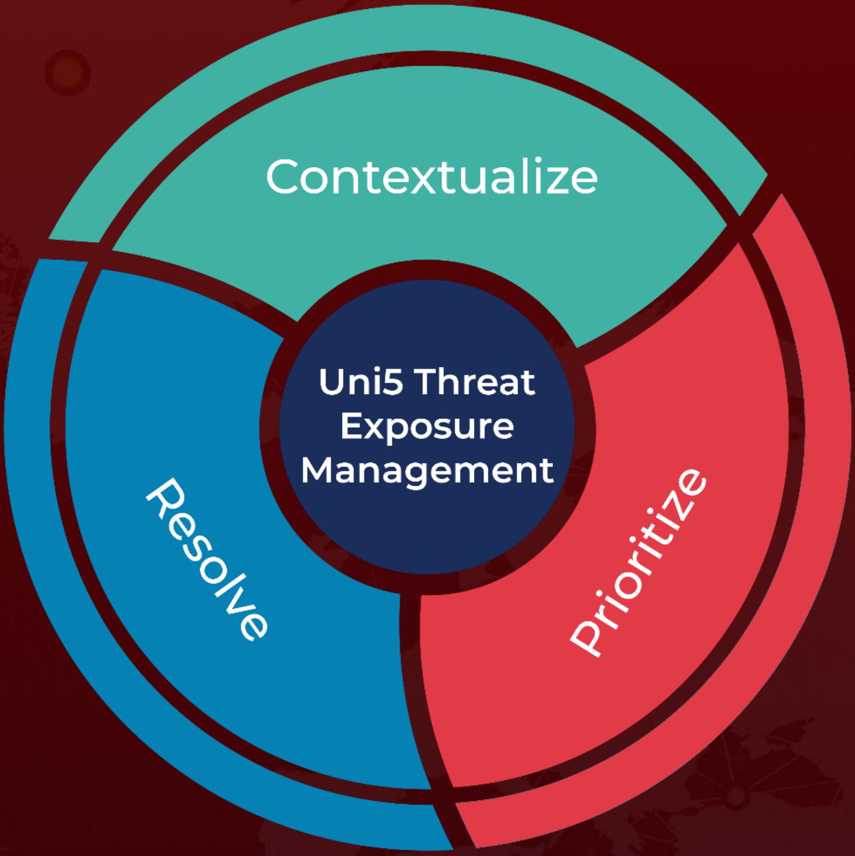
https://research.checkpoint.com/2023/stayin-alive-targeted-attacks-against-telecoms-and-government-ministries-in-asia/

https://www.hivepro.com/toddycat-exploits-unknown-vulnerability-in-microsoft-exchange-servers-to-targets-entities-in-europe-and-asia/

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

October 12, 2023 • 4:00 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com