Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

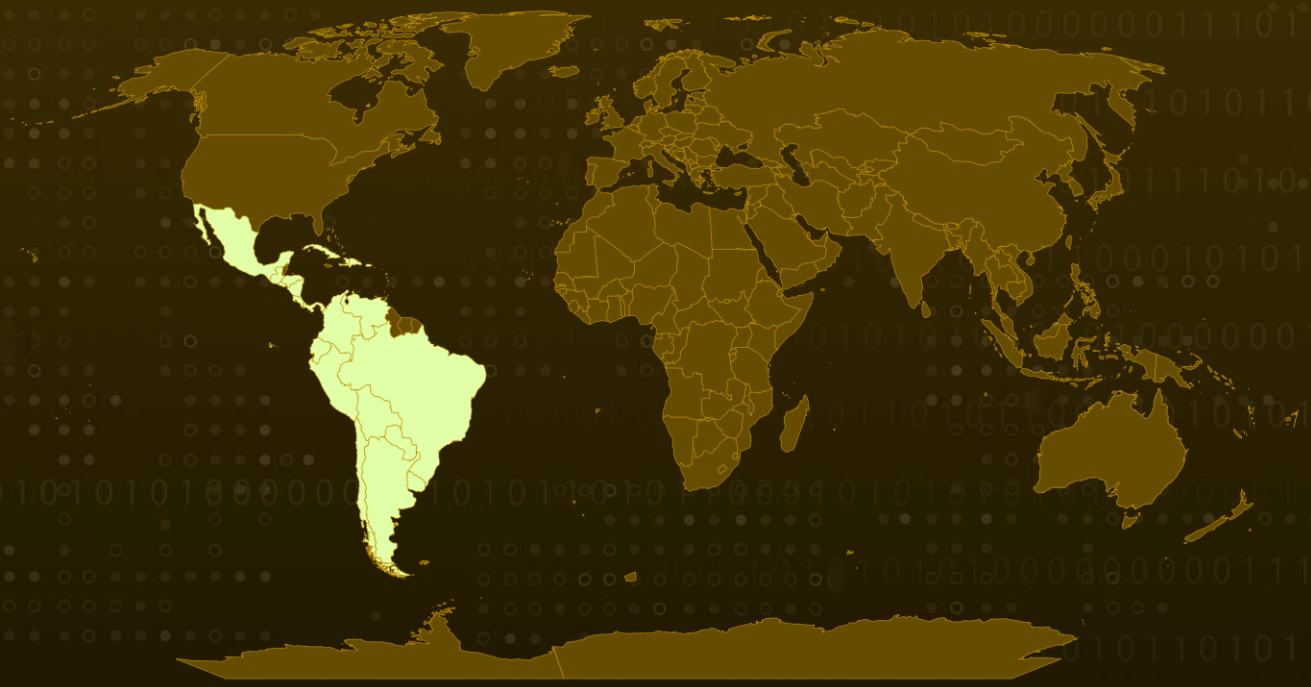
ParaSiteSnatcher A Silent Threat to Latin America

Date of Publication	Admiralty Code	TA Number
November 29, 2023	A1	TA2023481

Summary

Active Since: October 2023
Malware: ParaSiteSnatcher
Attack Region: Latin America
Attack: ParaSiteSnatcher is a malicious Google Chrome extension designed to target users in Latin America, particularly Brazil. It specifically focuses on Chromium-based browsers like Microsoft Edge, Brave, and Opera, with potential compatibility with Firefox and Safari.

Attack Regions



Attack Details

#1 A malicious Google Chrome extension, ParaSiteSnatcher, operates within a framework that enables threat actors to surreptitiously observe, manipulate, and extract highly sensitive information from diverse sources. This nefarious extension is meticulously crafted to target users in Latin America, with a particular focus on Brazil.

#2 ParaSiteSnatcher infiltrates systems through a VBScript downloader hosted on both Dropbox and Google Cloud, subsequently embedding itself in the compromised infrastructure. Once successfully installed, the extension materializes with the aid of extensive permissions granted through the Chrome extension.

#3 These permissions enable it to control web sessions, manipulate web requests, and monitor user interactions across multiple tabs, leveraging the Chrome tabs API. The malware boasts various components that facilitate its covert operations, including content scripts that enable the injection of malicious code into web pages, monitoring of Chrome tabs, and interception of user input and browser communication.

#4 In its initial stages, the malware utilizes the Windows Management Instrumentation (WMI) service to extract intricate details about the operating system. Subsequently, this information is relayed to the malevolent command and control (C&C) server operated by the attacker. It is crucial to highlight that ParaSiteSnatcher is specifically tailored to target Chromium-based browsers, encompassing newer versions of Microsoft Edge, Brave, and Opera. Notably, there is the potential for compatibility with Firefox and Safari as well.

Recommendations

Behavioral Analysis: Utilize advanced threat detection solutions that employ behavioral analysis to identify abnormal patterns of behavior in real time. This can help detect and mitigate emerging threats like ParaSiteSnatcher that may not be identified by traditional signature-based methods.

Endpoint Detection and Response (EDR): Deploy EDR solutions on endpoints to continuously monitor and respond to advanced threats. EDR can provide insights into the behavior of ParaSiteSnatcher on individual systems and aid in its quick identification and removal.

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
T1659 Content Injection	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1047** Windows Management Instrumentation
T1176 Browser Extensions	**T1543** Create or Modify System Process	**T1574** Hijack Execution Flow	**T1211** Exploitation for Defense Evasion
T1083 File and Directory Discovery	**T1185** Browser Session Hijacking	**T1001** Data Obfuscation	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	webgoalarm[.]online, backmnk[.]online, nonbrowm[.]com, mnksystem[.]online
URLs	hxxps[://]storage[.]googleapis[.]com/98jk3m5azb, hxxps[://]uccbf6a90286e6acc2a790729260[.]dl[.]dropboxusercontent[.]com/cd/0/get/CGqsvrqOuB4FhGVeZWMyQmSofO8uNJ8EV_sB9CypG92ekXY38jFAv9xQxx7QHpViLjUiEO7JzJ_eQurMhVA9ptRY0qTFFHQC0PkKvO64jHHju7RjYSIJo9vkJkoN7l5HPojdhpe-rLIy1U_oZboMSkgH/file?dl=1, hxxps[://]uc8bf39dfd51f19eca022ff937cc[.]dl[.]dropboxusercontent[.]com/cd/0/get/CGra8cbuRwTG62ccNRWQK3CHk96XzuTfm16q2nC1og5CiCXTPrwXZtf0TTJ3u6QelROuT3GllV05RL60fow_mvq9BpmNUeM0f6c1tUpdVEVYS3KaTHf-At7aLzI6ET-6MxKFT2NlOE9tgzXNEMIy3Ouy/file?dl=1,

TYPE	VALUE
URLs	hxxps[://]ucee667c79a6c55d864febd411be[.]dl[.]dropboxusercontent[.]com/cd/0/get/CGJ3qwC1u0jLr4CMzA6xZ77B9wEwh0nsM6QbQmwau3W0r-QUrhwEOFMEtcKTaPiNvaz-wngORZmw9w_Bc0ljndJu1OFJJa-1qoI66JNdBmu8fa9dNvM64fbOYZohfqjDQpHDQbkFXU7ffTWOXkk8ZlEk/file?dl=1, hxxps[://]www[.]dropbox[.]com/scl/fi/cx975utps1os4gw38q73b/1698022264[.]zip?rlkey=tqmsmhjonobx8ise21lp35601&dl=1, hxxps[://]www[.]dropbox[.]com/scl/fi/8otjw9dhf4kpb7s5vzxdu/1698746809[.]zip?rlkey=1w2k81ure5hm9ut5owezxa2gg&dl=1
SHA256	6822817419e5f0656f5d32cb1fcf2c03217ff7444e865d35e0d5405f3305b5a6, 445728f32c78f4a73b2a5c043aba674e5be14ffeb41a518fc774bbf4d7b408ba, 584ae99d672da18528a2c4d6c0506a83b55503a650ea1aafd5419f62afcee761, 887c167569c786b1639d87e0f624ce4af939baf67e1113bedde7226c744dbb38, bbd86446018a0d956794965a6b9f2da1402decb630f247529cd975a0cdfc3875, 0665989cd37454b2a1e83d0f930b471635fd993135facba20cc4c724682e64f1, 0371d28b45d13847504685a1baa360ce8e2e97301dfdc37de93f403b17484e98, 417323d076f7a3fc74fcb1534e39a7c55b6c9cb2a27120369634fd1c32d60f94, a70f323549ec1ce2d31814a8f0852f23b62cade04011058c247a1e55ba049bfd, c216989a7101e8849d4bd392377859c90772344289719519d5808ead81ae42e9, 0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4, e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807, 96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f, b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250, 6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4, 9e882594b497f6bc99f6da26211c54d5005064423b1f93059406332e36ae3eba, 1ebfe73932122e898c30098be4384a0fc9150565c3a340750b37b121ea7a55fa,

TYPE	VALUE
SHA256	8915b71a1c7a4da5c1cf73cdfa1d24c5546ed203e2a2d17f997ec31398bf85cc, 8603b20b548270423fb03c2138c16f5f863ead4c48eb0999167df869e2eef8a6, bcba29cd571b58e7f0bbf9d72105e50f1eddf915207e9147c554b18922c5adf7, ec22d946dc9538100875b86d2f6035f3541f5e3f08698304b9591efeea7d09a2, 1a3c5f97e7915b70c1371dd9a0265565fe86f7f347e303e7a6d8eaad573d339b, 3f033626d5f4b0cb69e4e902d80d1c3c4de647562e359a0d8904485799483e3b, 71b9d8721defee1f8f1694ce4e2ae8b1a99b78baa8e7fc9dd11364e97c390ff8, 21f4b82b120d84a2b21f95d75a583f36d7116cc3768785a3d0f213b50e86b240, c08a6db547b833244dd93aca9441059efe65428c588f0db591bcc8157fe4b43f, 5d813c849a79c60440ae2a36117e29da1da6c7649c00156b5cfe6222322e4cd6, 049a80a962618d9b89fb0a2cf03ef2c3ee00975c5b424e209f073e3c7a491f2c, b5e07008f50ff56ffd0389340a037da43b6398d57bf345dda3e0661098bf5ae4, e59e36d652f454aab543722501ac23258d295ef0f1ecf7c97cad7720ceee6123, a21356a2294036d2b573e3f6350a198cd0c4e98d5c2e7ecc9d37089250a6c0c0, 260b650de3977580a86c63c7f13b0aaee606fe16feff552936eed8e3ad652627, e195d0548c52a7cdb142c6c5acda2af40e350bd9d606ae4e1c03c6aa246572b3, 77e314975b4d26998a6384c9cb0deda88b8fa5ea059e3fe7b48edd8a541f2315, 72f327f62710f60f43569741c2cb391b833b44c4dafe1f5d5c085a39c485b5df

References

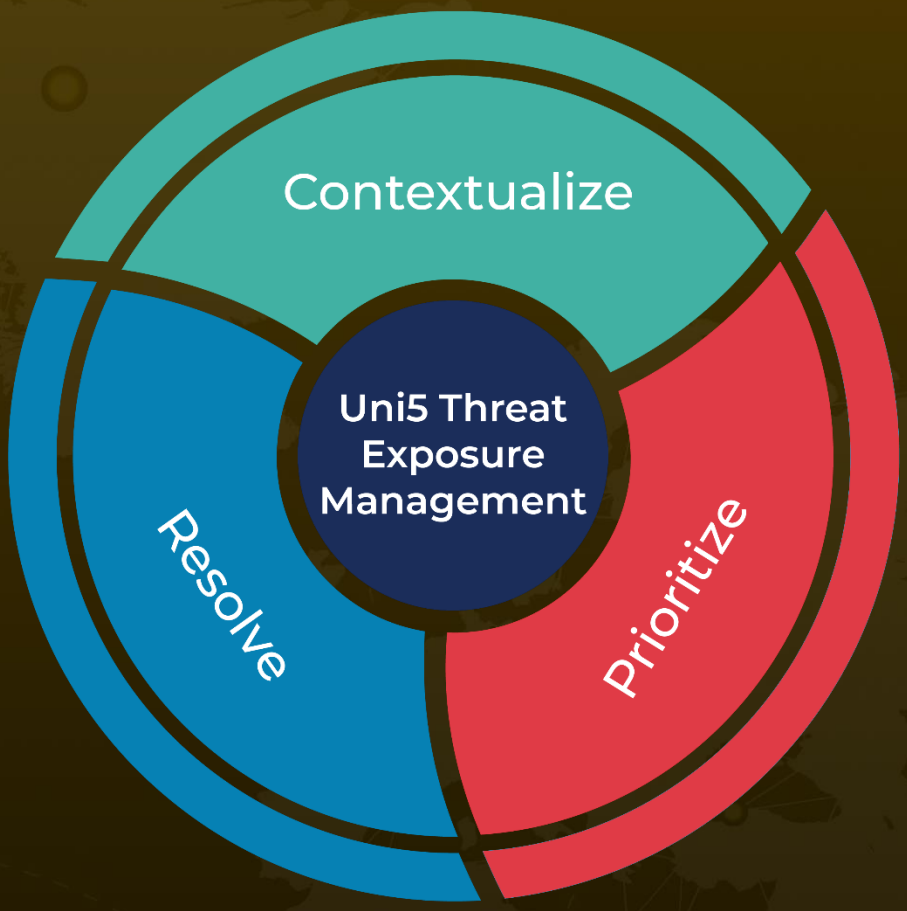
https://www.trendmicro.com/en_us/research/23/k/parasitesnatcher-how-malicious-chrome-extensions-target-brazil-.html

https://documents.trendmicro.com/assets/txt/20231121_ParaSiteSnatcher_IoCsl7nn42H.txt

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

November 29, 2023 . 5:30 AM

More at www.hivepro.com