KPMG Cyber Threat Intelligence Platform

Chaes Malware - Siphoning Data through Chrome DevTools

Chaes Malware emerged in November 2020, initially focusing on e-commerce customers in Latin America, expanded its operations in 2021. To propagate itself, the malware took advantage of approximately 800 compromised WordPress websites. In January 2023, an advanced Chaes variant dubbed Chae$4 emerged, targeting platforms like Mercado Libre, Mercado Pago, WhatsApp Web, Itau Bank, Caixa Bank, MetaMask, as well as various content management systems like WordPress and Joomla.

In its latest iteration, Chaes malware has integrated a customized Google DevTools protocol implementation, allowing direct access to a victim's browser capabilities for data theft via WebSockets. The infection begins with a deceptive MSI installer that poses as legitimate program, which downloads essential files. When the malicious installer is executed, the malware establishes a dedicated folder to deploy and retrieve its required files. Three base64 strings undergo decoding, with one activating ChaesCore module. ChaseCore operates in three phases: initialization, communication with the C2 server (beaconing), and the execution of additional modules. During initialization, it establishes persistence, and execution is moved to operate within the memory of legitimate processes. After initialization, ChaesCore connects to C2 server to download and load seven unique modules, each with specific functions. Additionally, instead of user-initiated actions, the module independently visits the service's website, using Google's DevTools Protocol to steal vital data. Utilizes WebSocket communication in one of the module to handle C2 communication & steals WhatsApp Web data via JavaScript injections.

Chae$4, the latest Chaes malware variant, poses a major threat to banking and logistics. It can bypass traditional security and target various services, necessitating vigilant security measures.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Chaes Malware - Siphoning Data through Chrome DevTools

Indicators of Compromise: IP Addresses	
45.15.27[.]216	91.208.184[.]164
176.123.7[.]135	

Indicators of Compromise: Domains	
4.q111[.]sbs	seriscojamais[.]live
awsgold[.]xyz	cleanupett.ddns[.]net
awsvirtual[.]xyz	gbviadinho.ddns[.]net
cnxtours.com[.]br	evolved-thief[.]online
farteresina[.]com	gilbertantonio.com[.]br

Indicators of Compromise: Hashes
6e7dcfd13260001c8fbfcc96b72e6e75
7affb9eb1472811a734eafdcec26aff8
4b44a2a657c208f72dce5f09f5a6838a
f9946a0868671bb90f05dd9d7b4335cf
9bcc9f4fafe710a2cef3c3192c1e3a98
ffe5e6e0beeba16fa36a2ba4b83fc103
af118ad39f767cddc4c47b28bba1b322
0d895da6e8f71bbea4dbb58adccd7b3b
9141839b2665a39dceebdc5fa4276ea3
3be41362b4f38377614bcb8286ac40d1
514d51218fa28d92ae3fbfb08750ff18
cb281ac4dcdf009a7761a5e8731c77dd
bc5bf281451078ca5838beb658cd23dd
c797fd0367e9b30bdede0d58ebb4b2be
b5fd6ecb788120fde3c04db8b2efe64e
ce0483adc969e35b93350a5fe302b218
9628880e03660d8fe97434c5af3fa901
8dbe59eae8006bd86ea0106918c49144
87f830f557eda5d683cb6a773e9e0afe
dc46afe76b104ebbdfcd9d4b726c7ae1
835c5b7ffda1bc64e1d8ce759a30e5af
725f2477306a9dd8c728dd33ed4fd19a

KPMG

KPMG Cyber Threat Intelligence Platform

Chaes Malware - Siphoning Data through Chrome DevTools

Indicators of Compromise: Hashes
e3ad7116b107e607a9b3a5569bbd46a2
8ebeb3d1fdd8537bc3606d90e2a8d67d
0defdd5a4d3de2f94c69ae77e49031d3
562402e84b8ce85c03fbb027f58d40ac
e5f46320041e4c7441ded3f69710fa16
7a2a733c70f38ae3084ff44f04d482a0
c642779c7aa7a67624e8a14f9a16810f
c044d74485b31e31a9573506b2133d8b54ede250
47ef71675a2dfae56823d76f459021c023b6bbba
484a217993de2380c33a3690122e4df840d17c47
b78ae307865a5382a463da70c44447f349e06923
cf30d3b861a3648e26c2406c9f78564bb872ed81
69aff119d2504512bdc7dc9e0ed421843633bd38
7bc2950ccbfd20917071f782578673893dc5f1f5
f1f30ee4d7847a998f877ccdccfe299b6976189e
603595b5015c572067d62fced82522cd86f9b147
9d247cbb5b1fe3aea0d0a9974f7f535bec88a6fe
1440254bfa1df060600af3f00272d07be142eed0
5c9785af3c10a36183aab9d2204ed11746678f66
14e07dc3c21f4a3bd8aec01c03004d573c217b05
eade5d6b12a576d716f87ec5083d316b285161d4
4eefa2a413ccfeb66d2eec41a4f9e46e4d13b864
3fd6edcda997e45ff694f55c4f8870085b8a6350
92ccc0bc6294888ed1d044ed8d75e6b2026341d2
b574b7487b1b0aa27c9f6060601048206cb3bb13
ebefe6ba47093f6346ed1ec3eeb9fc6f7d9c6d62
b13d8214e6ce1be8292e7305c43a29404339e633
d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6
b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a
6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c
628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57
05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd
8a361ec47aa5f999e37ed08408c2d145d0d6e41d305f62865e6f5b40b6e0e9cb
3292fc7a815a01bfbcd7478b0bfc28f8fda425e9a33b2848315e5ad75168bc29

KPMG

KPMG Cyber Threat Intelligence Platform

Chaes Malware - Siphoning Data through Chrome DevTools

Indicators of Compromise: Hashes
0c5edb9b8b830ed35ccab57f49cab3218fcbebc5ef3127518ff2fcab64471c2d
a50e29d49df8bf6d0d6f9a8abffce8ef6158dd5a4c813bc2313344ebb468bc0b
6f4247f2b34a6e37173a5b8432f8a64e3e5b36ef3c329aa83cabe2036f97e779
dc19f7f5e7eea7cb23e30e73f55d7ec61c1b28d996085cc50a2dafdc33b3b0c7
9ddaa03d15f55099ce5d1dfc981431cd7074147c71aa094e43d4aa715b81df7b
1482f9506977e6ffc5510852d7fe02abdd394499ebbe2439475c3eb4193f5359
f844708b307e0b5259714feec25c32ffe188535798e8be517e0b13f0d5ab68a4
db932b0a50c16f281a0e4f4ca1943f6867dbbf19978ef48463c3c7913acc04ec
41a0f8cb7addac0d3d259fd8a1d72671f519afc8c47d1d80c4f495e0a2aa8c67
d353a3725adba02e2db889c86e8f53fef15b497538023689c70fd0269f269e22
cd32569498e325e8c44e15cb3317084b54e291aeff4165741ef0c3081ce4f845
0a409856f4fc32b62442163a630880a3bcb6e4169135fce194648a516e26fa6b
6c1ac7e0e87eb47c662b01ae46efe346d5c71c4ea29243b974734959222124ee
7700f5cc5eb3149b67e8c06d893fd9a85afbe9a5c582a6db9f88a784605866cc
67ed7e369dd34ab348b2cf0fa730076a6b735aa5007acc2e5f8221b19a8799c2
e051c9a186b9f84400a01b23e5cba63ed895d8fa753390239432638a983a6268
cf1928a26bec7fa0a08ec88584d55c354e7ae0053ca618cca95608f2bc2d34b2
4b6860d1d903064750af333a69ab2aa7c118c176d3aefbcb05a074d0f3684ec3
19831b8a02d57396525fab89922e6257ebdcff44ff7866e13536be30654c998a
65ef7f5d9c66798d937fa634b534090d7863c30886c9d4a500f57471e6965e85
091e8d85423440e18883461be6a85a8ff5b7c55c4b96261b835b2a0bc8871ba5
ee6b7792b855e4df34557022fcecb5e9f9c4fd35ccdddea2007b7f7fb811252e
181ef3dd877e67cf83b3712ffe6c5c2ac90abbe4f449bbee4c6080e526716fa4
51e31ef335b3fe52362a583ac02476bbec3c2a42eb0485867f978dbaaa74fd32
4896ba0c43ffb85e7bc1656115b5c0bea9d4a135677cd256d75f7ecab1c07ac1
859d46ca687205bcda73a84b9a890b853063e6be0ebc19ccd7218684f1979f2a
044c2af8e43f9a6c48207eca5ac37bd312a7ee0cff2b34d237916c151981fb9f
8da49aecb2cfaacd0e7bcc593c23659b0133d781fc008d20ba15d14b878a327f
47164f7775e6e66a751e118e8e77798c40d129f1c148eb4fd70fcf1f6a5c7297