KPMG Cyber Threat Intelligence Platform

NodeStealer – Targeting your Digital Presence

NodeStealer malware first appeared in late 2022, now resurfaced itself as NodeStealer 2.0 in January 2023 with two different variants. It targets windows-based browsers to steals cookies/ stored login credentials, specifically from Facebook, Gmail, and Outlook accounts. This new updated python variant of the malware is capable of compromising Facebook business accounts and stealing cryptocurrency by avoiding any detection. It is suspected to have originated in Vietnam and is being distributed by threat actors located within the country.

Initially distributed through deceptive Facebook messages offering free templates for Excel and Google Sheets, luring users to download malicious executable. Post execution, it captures stored browser cookies/credentials of Facebook business accounts. By Bypassing the User Account Control, it downloads ZIP files from remote site and execute them through PowerShell scripts with admin rights. Downloaded ZIP files, 'Bat.zip' contains a script, deactivates security solutions such as Microsoft Defender & uses any anti-analysis techniques to evade detection. If found, terminates itself. 'Ratkyc.zip' contains three pieces of malware, 'BitRAT', 'hVNC RAT', 'XWorm' and sets persistence by adding them in registry run keys. It exploits 'MetaMask' extension to capture crypto wallets credential stored in web browsers such as Google Chrome, Cốc Cốc & Brave. Post access, it steal browser credentials, cryptocurrency wallets, & Outlook email data. Post collection, the stolen files are exfiltrated to a remote server using the Telegram API, and then delete footprints to eliminate traces.

NodeStealer targets for credentials & cryptocurrency by exploiting the Facebook business accounts, poses significant threat to organization as well as individual. Enable robust authentication measures and foster awareness about refraining from execution of malicious file.

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

NodeStealer – Targeting your Digital Presence

Indicators of Compromise: IP Addresses
15.235.187[.]170

Indicators of Compromise: Domains	
dongvanfb[.]net	adgowin66[.]site

Indicators of Compromise: Hashes
7b979b43eebeb4b9969312695601dab1
f135f1d24ad1cf2dd000a3eed2e7b681
2dc8f6c04d059348451cf38c798b5732
8d41f5eaac4acca0d1d675b28da1df58
c704c8a5400f353e4f232211ddedb0a3
6c4360a9e1b23995675a8599d70aa443
f160da34e4b707870c9e82007f062bf5
2d62aa427512ed47755fdf5749fe90a5
ed0fe734a63699d3fbf42f6251e4697a
a24a56622341bb722a0cffec3effd85b
f389693ff4e9863b712e80314bf4a6a8
5d2e313e2e2bae15b6e6fba89cadb237
a471fee01ea3a0606112e2096e22241b
6b6b00d3a98432335e5a751d3ab05ddd
1e6f756fb1cf0a6fa185d51496e28ba4
2537d96011fc12adbd3814700f73ba86
40f36aec03708148f2a0a6ad408ca64c
81451abb2acf809a66a2f9fc4e3c51b6
95b5957f1afc5ad1ecb186e9591ff4ded7c74be1
e86f3204cf919db10e6fa1609fb535e440d23bb5
b1c9b1f39c2af12b9eee533f04f12c5d4816e65e
da5bc554e66905c9c63d1dbd8b5f97854239227b
981896f72353def9cf649f7075338b68b85d15d2
9d6d6cdfdfa50c2fee43e4755581020df1e33cff
23bbad28c06450627e2dca9d7cf6cdd77d65b532
ecdc38d0f1835bf1b08637ddc05a99d4540ee92d
dce62b6589a66a450f0502915d6826c42607f403

KPMG

KPMG Cyber Threat Intelligence Platform

NodeStealer – Targeting your Digital Presence

Indicators of Compromise: Hashes
7f125adb5b64c8e083bb49b82414c9c307336f16
791947c1401a3073cbe146ebf8e3e5b83511f8cd
6ebfe9d8d53e678ea10301bd5d63fcf093ad03d6
ff3c8b40631b13cb4a02c431654d3075a1c5a7f0
79fab51fd030606d3eb6acb89711f7d2397ad590
417aadb24e0ce872d43cb0ddc1a81049ed38222a
b35bf69985f964f6cbfdef305ef7204ba99ce3b5
8487a6630487b0fe211fec10cc476a716d70dcc4
b613ddde6becb4f8d1fc1784433e6d3b02720a86
aa07f42e5f1a1e37eb72f44ca05c0ffc868c713e
a67b65e795f0d3490ab9e5a2739f1f0bcfe1fa7b
6dca4153c60128455561d7ac9eebecc8daf6401d
d1263040734f850d609372803c73170cffefe215
3352d74f33f03edff1516a1d8d75e5e6b91d4039
c34437ac4362777061fe626bb2fbf8ca16bf991e
f57f319528821c46037a28d7381c347e03cfcc00
533f44d4e196d9d7c7579c9c8b7092a1a959f971
f31fcc0596fb5c85900fedb1dcdc80801ff6a511
611892e2eb706145f0792cc0acacd08186cd19a0
3dce20bff60789038ba50884926c7de2427a1ec2
61a65a632e035738c5a854b91e78ed624cec18b8
f322a9d963f9af45705eaa0e554ab369e13bcd1f
88db5b36a9f20e2ff8113f4e054454caa978a593
b153b1d76dfd0e69d8a77d6a2503c38fabaf2856
c8d4f567e2162fce6b49c15ca0908f9e3171e6bb6acbfd2c7b129872053b025d
dccc95c28bbc1f049c06e7b3a9866a920c4c4081e3176b26fc6aea2cb59daed7
8582241f8e0163f6360486e9b59e54c91dd3219538e03619e9e999f90aa92f81
fab5abe774e1af199da4b85df87077e2e8f66c6f00f083b9074fd2186e455bfb
9dba2cef0e28a24b59eda107633528cd83257f033a5d4330cf3302943b3e07c2
440541d9e9c4d1fa8a1f33ce8c434ace11786e278278df7a600978290b33e93f
009827ab2624370ded2cb8240ca2fe82af36e3a94cff1f8a2eac574b4b928c4e
bfb4f44e8dd9c0a708df89f0f114b523c446baaee19205d62ad99bb53a8b5935
50b5ab35c1e78429fdcdd45e2a0ceacc140fbf4022f7c34bac4b5f296a17379a
bd16e9d3f730df6b88fff91485d3d27e544f3bb819347b0886806b1c14cbd575

KPMG

KPMG Cyber Threat Intelligence Platform

NodeStealer – Targeting your Digital Presence

Indicators of Compromise: Hashes
9b1dcde16f34ac3d5abc15510060cd1692591054988416167dae3c4643e5796c
57c234dc3a210467b990c16092fbd3af2dc0aaf8aabbdfa1b566138b2abc5e82
2cabb8e10c5ad57788d99f5218a1248e0ada9a5bdbd5f976d9523b2e4a47aacf
a62acb65022abbd849e0a741a17485156333fbfe26f32c50654b3818335c1d0d
989f62528b32d47e50f1bd61cc7dc2e9cb25f54514374902d8a9ce41fcfcd779
a45ff2f03d88abfb949b8c8f40fa08fa7e72d22e756716f8dc18e2f34376b722
7072dbc19da9713c997cdbcacbc68ca709e900d44bb3572bc34fb3c91ecbea9f
ce6314bfe207e4106df4249452b654ffa892a1bd45bc7ff9d6871b1dbe8e3e3b
d3e1060a003f6a8073dea4f6c976f552372cd4ab9251953c0932be22c6f6605f
41a09e66c24953c7cb19f4a09b0779c8e9bcb39f0e544d0bdc9760c9b3d56e03
9282f4b1fa8ecf1273ddf3291abcc8fc073b2e99a00f70985077197112a46c4c
a41b170f554a752a23769b28f3fa93703fa160b74897a8f35078d1e8923b91b0
4316a560734e68303860899d0f2b07a9ef4618647da2e8ad38bab70a4e532f88
fe434fff6becc2d829bbfed6ba9bf88154028d0327e7c6aa870ad050235fc334
b87ead56ff364a052619c373b8c06d2150561196f87e584590f67a341ba78abc
92eba1a137918f99fbe15651568b8b76ad5f59788b1bce9076bfb33bbc3484de
1ada42adb9ee65aa02d5eb9d24d3455df61c85f69e84f310b9630d62ca83a518
6777bbf5fd14eb1a7e81de33c477ac5ba4f446699df447995e8d362a8438a0a3
d12196087135b9383a4e9820d27625c059511c4776593a4d2eb83409a96af3a5
ea96973f3d71cccad26bce7f106f5800fcb007cf33d82fa00f5d564994397153
f31e2c430d4a8b17b45591bf68e5c4c7f7c28e4ccbd4cabcd10c33ba14b388c3
f80700c220246238507cf5eedcb2e1397c32b3646bb90ad990e7fb69199752b5
415d70be7a2e3ae8fd2babc929c3110fce7ce66d23ec32c473c6aab73c5c00f8
4932514acfad25c7b2a1631706aef8d91a415315e5207e1bc9a24791298e6319
9ecba5aa60b9c202b1c69aade1edabb1c04072471a3618a5d714aa8833d570f4
38cbccea7c9f3032a8348e54bb94871b26279a7cca64f5b79c3fa54c240960d2
4f91fdf024b54ad650c13f7ffe1a7f3eb6cad66eb457e8a7fe494cf9bdb6f42a
cdcaf4ecae94421503364d28ef72eb65a83f300980cd1a8ba02bea1c29e193ec
b78a980b66327c4e45f95f2e0fc2dbaffebcac00107cd16ac2d2c2a42618e645
f2548fd9d622dae1b21e18323a2d8dca2f7670789dfbb5f6d32320f4fd289039
65669e873a3732f1617c9c80667a1c3efda5f72538b5abd475e80a25efc0e5e2
3984a025b7fb7c5ada86da0b4fa32bef88eb2a01fb337a7f73619cb716c859ab
0d313ad0b46218acfc25fae744b53eb539169e56f9976eec47f37d99ebce510c
834215c7226d28be513562991cacd7f56f4914b8ae1e27ff3ae85ca82e208605