KPMG Cyber Threat Intelligence Platform

PXA Stealer – Vietnamese Driven Infostealer Goes Global

TLP : Clear

KPMG. Make the Difference.

PXA Stealer is a Python-based information-stealing malware first identified in late 2024, attributed to a Vietnamese-speaking threat actor. It has evolved with advanced anti-analysis techniques and a robust command-and-control infrastructure. The malware primarily targets government and education sectors and is believed to have compromised thousands of unique IPs across 62 countries, with South Korea, the U.S., the Netherlands, Hungary, and Austria among the most impacted, highlighting its wide global reach.

Initial access is gained via phishing emails delivering ZIP attachments containing either a Rust-based loader with batch scripts and a decoy PDF, or a signed fake installer (PDF/Word) bundled with a malicious DLL for sideloading. These scripts or DLLs generate deceptive documents like fake invoices or copyright notices and use certutil[.]exe to decode hidden archives archives and extract malicious payloads from WinRAR files disguised as images to evade detection. Persistence is established via Registry Run entries, with optional decoy startup batch files to ensure execution upon reboot. Both variants ultimately deploy a portable Python interpreter disguised as svchost[.]exe which runs base64-encoded scripts to disable antivirus and launch PXA Stealer. Once active, PXA Stealer terminates processes tied to security tools, browsers, messengers, and crypto wallets. It decrypts browser master keys keys (both for Chromium and Firefox) to extract passwords, cookies, autofill data, credit card information, Discord tokens, and Facebook session cookies with AD account data via Graph API. All stolen data is archived with metadata like country code and victim IP, then exfiltrated through Telegram bots using intermediaries such as Cloudflare Workers.

PXA Stealer's deployment techniques and evasion capabilities highlight its growing complexity, demanding layered defenses and continuous monitoring to effectively mitigate its threat.

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.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

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

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

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

PXA Stealer – Vietnamese Driven Infostealer Goes Global

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Domains	
0x0[.]st	tvdseo[.]com
paste[.]rs	lp2tpju9yrz2fklj.lone-none-1807.workers[.]dev

Indicators of Compromise: Hashes
f23ea2bbd7d5b56a4a97805e57e01175
80664dd289f737e17c5280fb1af22494
3636854c14643ace9b56ab7da0ad4191
d475ce52dbd24457788bbf45ff177691
5a92f0559729261b6afa39fab2efa497
a0ae41d39744b2a1f93d9c9bc6aa9a6d
6510f6d274e03e177a0540d7307d7ac9
996d6590e680c8e029282fa5027fd604
c1ea9c7c799770e82625271a2b5b8979
a1de860115ebbef7f96b089bd61bbb75
1a4f20cd79079b18d410c43d87f1f0a6
39d66ca56cf219e34945df69ba0d9776
a26cdef223d3537bc80299171fb4e23b
fd5e8a1d11f06db561c38e898879e39b
fe06d9599a0877a5a0031598893b577b
ae180268e7507cfae8c0693a91ca2a94
b5169f555ac654bd551b2bf3791392ce
0a4e403cbe7adca4e966d17b1385606d
a1afa1799670cb59cbe11bc1f888538c
393ff5839c4ce9e06079c3e7adf1cc27
da3c285addbf66cacfd765f17bae0f3f

KPMG

KPMG Cyber Threat Intelligence Platform

PXA Stealer – Vietnamese Driven Infostealer Goes Global

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
76d9c664f9a8b8366f5ab659e2375d51
c713f8e94f6179be72f8ecbef71de771
ddc1539a1c7950b48b371920674874d9
68109761c23f703e6d527a2e38245802
48d6350afa5b92958fa13c86d61be30f08a3ff0c
4dcf4b2d07a2ce59515ed3633386addff227f7bd
5246e098dc625485b467edd036d86fd363d75aae
540227c86887eb4460c4d59b8dea2a2dd0e575b7
e27669cdf66a061c5b06fea9e4800aafdb8d4222
e9dfde8f8a44b1562bc5e77b965b915562f81202
f02ae732ee4aff1a629358cdc9f19b8038e72b7b
f5793ac244f0e51ba346d32435adb8eeac25250c
f7bb34c2d79163120c8ab18bff76f48e51195d35
f8f328916a890c1b1589b522c895314a8939399c
f91e1231115ffe1a01a27ea9ab3e01e8fac1a24f
faf033dc60fed4fc4d264d9fac1d1d8d641af5e0
ff920aee8199733258bb2a1f8f0584ccb3be5ec6
3d38abc7786a1b01e06cc46a8c660f48849b2b5f
08f517d4fb4428380d01d4dd7280b62042f9e863
1aa5a0e7bfb995fc2f3ba0e54b59e7877b5d8fd3
734738e7c3b9fef0fd674ea2bb8d7f3ffc80cd91
80e68d99034a9155252e2ec477e91da75ad4f868
ba56a3c404d1b4ed4c57a8240e7b53c42970a4b2
bd457c0d0a5776b43969ce28a9913261a74a4813
da210d89a797a2d84ba82e80b7a4ab73d48a07b1
dc6a62f0a174b251e0b71e62e7ded700027cc70b

KPMG

KPMG Cyber Threat Intelligence Platform

PXA Stealer – Vietnamese Driven Infostealer Goes Global

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
533960d38e6fee7546cdea74254bccd1af8cbb65
c5688fc4c282f9a0dc62cf738089b3076162e8c6
c9a1ddf30c5c7e2697bc637001601dfa5435dc66
4ab9c1565f740743a9d93ca4dd51c5d6b8b8a5b6
fdad95329954e0085d992cba78188a26abd718797f4a83347ec402f70fe65269
7db49da15fd159146fe869d049e030a4ecd0d605a762bea4cc4eb702a6ce9ee6
707004559c8d625f2d4b296ede702def1f9f52cadf4c52dadc41f3077531d04f
bc15114841e39203b4e0f5d2cdeef11cc4eceba99eb0c3074a1c6d7b3968404a
a9e3f6b9047b5320434bc7b64f4ba6c799d2b6919d41ed32e9815742f3c10194
782da8904a729971fab86286dd1f44e8de686b7bc66b855079381e1c9e97f6da
e689601d502cc0cd8017f9d6953ce7e201b2dad42f679dc33afa673249ea1aa4
331708ab439736db2e64d94db49d3bd00de872471afbcbd31b9816677fa04c75
4ab71fd27d9794d32e5d0f7f6ae6c7591ce4dca40c09e4f59fee1c25a7d701b2
8e32c904ba3e66f0acfd29e601c9957ca44ce84bea460ab138a5cbca8577fc0f
a6235b27b77155ad8866a63211cef92a196476a08b09457f9a5c8f8dee692a3b
04d7cbb4a6f4152a59fba1c83b53815716f7008db0b2a4514166bfa9c4413895
f10e48d4afe61688e121652e16f70bca8483ef8d3cce1ab900fc7a95cfcebc98
5bca90172085e52de0543c6d8dae1a335289995f8a91f7debe034bdc5196985f
a044238378236213f1cb3d446ca1509fcfc253fc3d7cc9cfb3327add8311a487
45e375173feb23bd0da71a321a5c847c12335961ebf8878935104bd0259aa0e4
3e8b370b8f499f5de89bf20bce2f0890c4731b4972943cfb82691ed370d9f62a
86fb906de0aa88d4638f5820a275a580b5bdbe6512604ed7d1091f9ba21f1e97
1e8242ee0dd9a26d3e3558c6d753fe66d30c0ff8091982d9fdfb31fbca3d32b0
3b47893c0ca67b9faa00a86caf2d50eda55d1a1169500c9efaa9c4fda9a48432
11b7dca543c3fcc2b0283c337954bc0bb7d181bd290b3313419f59928dd5b6ac
e4adc3bbc1235b57a733c42a33acdb42e75462a6b752ca5d7b91463021e68200

KPMG

KPMG Cyber Threat Intelligence Platform

PXA Stealer – Vietnamese Driven Infostealer Goes Global

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
bc6dc9ba1f1f3d10c04c807181efce8db2d3cc240484e848f4502a0f83f0ec63
7775d00a82ec44a718d7ee5417d6097bc4315d3513303bcb9340266cc0c87f73
fc4d76fc8f7a8d73f56a01fdfb5da52ed1e2f4b4cd8a307e2e4dc2b675f0afd6
6e0df3d6ed4499e652844699be35e1443131546ecd9e57db0349cb0bc5f6f6ea
9b60153787a0b5481eeeec7d2f4bd7a6b04d415d24fa7b275171982c4d2e7b22
ecd3e17b6cdf422b68ef2aac160ebff53295e294092460560f03477240b92084
af10870a0088752f96dc5571b847f307ae49e364d6d8f4c1046ec14823c4dbf9
69d31aa172fec64071dfbe6f6104f560422ec5966274953f6473f379f9123e78
0cd9f10a8e644754d1c3ed624e7a3d79c738d446e3b5d1f645c4ee2d855ee4ca
8c6f78eba426c0709010e21169a2e7d63d98d06a36796c9cf59e06775da1cfd8
f3ba1f89aa4543ad00a6586add0ef0d4db05daaa271fdf5a38ad752240c2b3b4
99cfc0d8da609b0cab35b9b17b1a3b3817cbe52ba398e7c1c15bd38f60c4e10a
0414a4264abe75ed2619eddf1daf981f756c6ff367af01e5011df44d066edede
0002962e7557e8cef69bcd28e23f4398d56e9d25a27089ba999d9e2d2f71b859
a0a4bd9e25d13b317755c082dbd74c499606cb1001d2bbe1f6dfdac2371cb933
849ef4df070208640e2c8a3a3f720b581610f89f1de15ae1b327307e77a25cfd
67a94ef73216041c98460756946488 51e100d2ca6ae30433e853708c86dfeff8
421322c787a5d6a68587530004c8d014966cdffd1ba2ccb623c9c72e4066e6e2
9cba3837c483659604b282ffff8581ef069080435fecaa3bb8d53b8548502fc2
5d2636003dd928b17bca33dc79f32b26f2929198a708741f5d71d585ed7ad30f
8dcf1b4029fd388e2f025a303edb99936ce0b2eedb06ffab0c29e66f15003f00
a27f9a274c3a779bccbd80b4a5a3067c358488c38d19164bd8e45f15ec8b3da0
8e911de1cf39b90c4bfccf9f48d36f5ec456dcff4539925847ccde6c73f3abdf
a3ae96de3604ba872af9941be785e53b319dca656326fa19398d5ccedb178e72
997e5c1305971b478c580b7213b96a7248e853c722fd9499e4f5f90b3867df63
1dc43e348a2f39bb8a0d8205a91be2882dfbf6db759b24de01ed7f279613823b