KPMG Cyber Threat Intelligence Platform

Nitrogen Ransomware - Rapidly Expanding Global Cyber Threat

TLP : Clear

KPMG. Make the Difference.

Nitrogen is a financially motivated ransomware group first identified in late 2023. The group has transitioned from malware development to a sophisticated double-extortion model. Nitrogen leverages advanced techniques such as malvertising and trojanized installers to target IT professionals within organizations. Primary targeted sectors include financial services, manufacturing, construction, and professional services across the United States, United Kingdom, Canada, and additional regions.

Initial access is obtained through poisoned search-engine ads that redirect victims to fake websites hosting trojanized installers for tools like WinSCP, AnyDesk, Advanced IP Scanner, and PuTTY. Once executed, these installers trigger DLL sideloading to deploy a staged loader (NitrogenStager) that reaches out to command-and-control infrastructure and downloads additional payloads for credential harvesting and lateral movement. For reconnaissance, the threat actor leverages embedded modules to map networks, enumerate accounts, and establish persistence through registry run-keys and scheduled tasks. Lateral movement and post-exploitation are achieved using frameworks such as Cobalt Strike and Meterpreter, enabling remote command execution and privilege escalation. To evade detection and maintain control, Nitrogen abuses a vulnerable 'truesight.sys' driver to disable antivirus and EDR processes, modifies boot configurations using 'bcdedit,' and clears security logs to remove forensic evidence. Data is staged locally and exfiltrated to attacker-controlled servers before encryption begins, ensuring leverage for extortion. The ransomware payload then encrypts files with the ".NBA" extension and drops ransom notes titled 'readme.txt' across affected directories.

Nitrogen's reliance on malvertising, legitimate tool abuse, staged loaders, and anti-detection techniques reflects its operational maturity, necessitating robust, multi-layered defenses.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it 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

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

Nitrogen Ransomware - Rapidly Expanding Global Cyber Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
1b637a43abca552acaee11c01913db18
b9e23af97d7215b3c45b5cc8b631b8c2
b580be9e58374b7c3a1e91922e982d3b
f4cba020d9746ea861267253454daca6
d919e343301c46db373a0694d25a0feb
7e043d880dcf7889c6767ab97764769c
3139c8e0d0dd9683ebfecdb2e4f1b6bb
b580be9e58374b7c3a1e91922e982d3b
3965999701c945a100241f1adaeff1e5
f53fa44c7b591a2be105344790543369
3dbd3c04b1acab0b70546e48d39247b7
834d94cf35d9417aa93a5cb350a756e9
3139c8e0d0dd9683ebfecdb2e4f1b6bb
a9297a8acbee74ba0169333ee38be2ef
3029954ac63d1c92601ba03ac8a59c66b386be21
43d29eca57784ae519f8076a02f4b2ab994f574f
bcb9455f82f17483a625e61b3cb52aa20835dc6e
0a037416725fdd23094dda0e89b4fc2e728ca414
ae92b5a4e618747b2d84cf39e826efb9fbaffefc
ba8ce2d5eceb73d3a24c2eba0871110596b27fe4
9d8189c1d66154b5f01b307748ba47ea589f91fc
bcb9455f82f17483a625e61b3cb52aa20835dc6e
5bad14d423c31bda3f6383dd1f04a8286611a92f
363068731e87bcee19ad5cb802e14f9248465d31
704a4c5c224a5d9120f2f21336e5f7347e4ccf85
5fbe4fef61314da6663b17b9120af20db0a2866f

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Nitrogen Ransomware - Rapidly Expanding Global Cyber Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
9d8189c1d66154b5f01b307748ba47ea589f91fc
013bcd831c2681c852b716055afb8dc2cd3f3f4b
c94b70dff50e69639b0ef1e828621c5fddcf144fea93e27520f48264ddd33273
ce8788e6ed0042010dd27a4fd79b9962d11385008b88485b8368fd666e5d38ec
55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be
f30198a8a62e189653bfbeaa7a2f303549b8042ddd84c980f132a4e889f9cb60
4e58629158a6c46ad420f729330030f5e0b0ef374e9bb24cd203c89ec3262669
779576719a9c400a7a4abed0386e2111eb331160572c91a2fd8eaa1a7d6e6c63
e6a498b89aa04d7c25cbfa96599a4cd9bdcc79e73bf7b09906e5ca85bda2bff6
55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be
fa3eca4d53a1b7c4cfcd14f642ed5f8a8a864f56a8a47acbf5cf11a6c5d2afa2
bfc2ef3b404294fe2fa05a8b71c7f786b58519175b7202a69fe30f45e607ff1c
ab366a7c4a343a798490c4451d1d8e42aea2b894cb3162b5c59e08d8507ffe2c
0db5c55ef52e89401a668f59bf4f69391f4632447c51483bb64749d7f2123916
e6a498b89aa04d7c25cbfa96599a4cd9bdcc79e73bf7b09906e5ca85bda2bff6
08c4e99a0bd2c88d0d96f0c688557fbb27c027ce3fbad861925961c86eb35ec1