KPMG Cyber Threat Intelligence Platform

BlueNoroff – AI-Enhanced Operations Targeting Crypto and Financial Sectors

TLP : Clear

KPMG. Make the Difference.

BlueNoroff, a financially motivated subgroup of North Korea's Lazarus Group active since 2010, recently launched GhostCall and GhostHire campaigns. GhostCall targeted macOS users mainly tech and venture capitalists via Telegram social engineering and phishing sites mimicking Zoom. GhostHire focused on Web3 developers, posing as recruiters and spreading malware through GitHub. Primary targets include cryptocurrency, Web3, and financial institutions across Japan, Italy, France, Singapore, Turkey, Spain, Sweden, India, and Australia.

For initial access attackers impersonate venture capitalists or use compromised entrepreneur accounts to lure victims to fake Zoom calls via Telegram or phishing emails. In other cases, they pose as senior recruiters. On the call, victims encounter an error prompting download of a disguised AppleScript update, which installs scripts to fetch a fake Zoom client and DownTroy malware. Recruiter-based attacks add targets to a Telegram bot and deliver a ZIP file with a coding project executing it triggers a GitHub package that drops an OS-specific payload. Persistence is achieved via a plist file for auto-start. Credential prompts harvest system passwords for privilege escalation ,while attackers manipulate macOS TCC.db and bypass Windows UAC for broader access. Malware includes launchers, loaders, injectors, and droppers, signed ad-hoc and disguised as system files, with some scripts using blank-line obfuscation. Stealer suites and bash scripts extract credentials from browsers, password managers, and blockchain wallets. Modular payloads gather system and user metadata. Remote control is maintained via encrypted WSS, and exfiltrated data is compressed and sent using cURL and bash scripts.

BlueNoroff's use of customized tooling and multi-stage payloads underscores its modular and dynamic capabilities, reinforcing the need for proactive and layered defense.

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

BlueNoroff – AI-Enhanced Operations Targeting Crypto and Financial Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Domains	
safefor[.]xyz	api.flashstore[.]sbs
safeup[.]store	cloud-server[.]store
writeup[.]live	support.ms-live[.]us
signsafe[.]xyz	firstfromsep[.]online
web071zoom[.]us	pre.alwayswait[.]site
readysafe[.]xyz	root.chkstate[.]online
signsafe[.]site	web.commoncome[.]online
api.clearit[.]sbs	instant-update[.]online
real-update[.]xyz	bots.autoupdate[.]online
chkactive[.]online	first.system-update[.]xyz
dataupload[.]store	first.longlastfor[.]online
filedrive[.]online	root.security-update[.]xyz
flashserve[.]store	system.updatecheck[.]store
secondshop[.]store	second.awaitingfor[.]online
file-server[.]store	second.systemupdate[.]cloud
safeupload[.]online	download.face-online[.]world
image-support[.]xyz	check.datatabletemplate[.]shop
secondshop[.]online	download.datatabletemplate[.]xyz

Indicators of Compromise: Hashes
00dd47af3db45548d2722fe8a4489508
01d3ed1c228f09d8e56bfbc5f5622a6c
0af11f610da1f691e43173d44643283f
0ca37675d75af0e7def0025cd564d6c5
10cd1ef394bc2a2d8d8f2558b73ac7b8
7581854ff6c890684823f3aed03c210f

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BlueNoroff – AI-Enhanced Operations Targeting Crypto and Financial Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
76ace3a6892c25512b17ed42ac2ebd05
7e50c3f301dd045eb189ba1644ded155
7f94ed2d5f566c12de5ebe4b5e3d8aa3
8006efb8dd703073197e5a27682b35bf
8f8942cd14f646f59729f83cbd4c357b
931cec3c80c78d233e3602a042a2e71b
9551b4af789b2db563f9452eaf46b6aa
963f473f1734d8b3fbb8c9a227c06d07
a070b77c5028d7a5d2895f1c9d35016f
a0eb7e480752d494709c63aa35ccf36c
a26f2b97ca4e2b4b5d58933900f02131
a6ce961f487b4cbdfe68d0a249647c48
ab1e8693931f8c694247d96cf5a85197
b2e9a6412fd7c068a5d7c38d0afd946f
b567bfdaac131a2d8a23ad8fd450a31d
c42c7a2ea1c2f00dddb0cc4c8bfb5bcf
c446682f33641cff21083ac2ce477dbe
c6f0c8d41b9ad4f079161548d2435d80
d63805e89053716b6ab93ce6decf8450
d8529855fab4b4aa6c2b34449cb3b9fb
de93e85199240de761a8ba0a56f0088d
e33f942cf1479ca8530a916868bad954
e8680d17fba6425e4a9bb552fb8db2b1
e9fdd703e60b31eb803b1b59985cabec
eda0525c078f5a216a977bc64e86160a
f1bad0efbd3bd5a4202fe740756f977a

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BlueNoroff – AI-Enhanced Operations Targeting Crypto and Financial Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
f1d2af27b13cd3424556b18dfd3cf83f
f8bb2528bf35f8c11fbc4369e68c4038
df9894ceaf81945a771b4c230fc730b5b72c5ea2
a4933676e28dd47d685edeb8dd5be4533cd0f77d
decb44a5361e336ee5e576355f86c4fc17edd2b1
1269e7279b701777a660c7fa982f480cd1ffa43b
4fc1a0ea8dfab79fb95c1bef71295ba2b78dea6b
7e07765bf8ee2d0b2233039623016d6dfb610a6d
3f4c2532f57d56cde608b9606f05927cf1fdc81b
d3609d97f3cd1bba378210aa5526989b943117a8
4818af3d199ec7d59ca8671df05d4938f2570cff
5474451c25e8070d872102e88e65967f5f039290
4d101f0ca2bd81c23f0e68dbf34b3cd6625188b7
5b16e9d6e92be2124ba496bf82d38fb35681c7ad
132b79aa68b0843f1166ed46c0b5363d04951475
c91d54b555f14002a07667dc094eea44262a92e1
416ef3352638e2fe5815fca722df4e9ec70b550f
57973754f9d98bdb9b5682953234a1a8da15e74d
de3f83af6897a124d1e85a65818a80570b33c47c
177ddf491fb66c87f17570b50890e0c0fbcafc21
06566eabf54caafe36ebe94430d392b9cf3426ba
1793c038d3ec1986a767b15379a8b218c64c7df2
1e76f497051829fa804e72b9d14f44da5a531df8
945fcd3e08854a081c04c06eeb95ad6e0d9cdc19
023a15ac687e2d2e187d03e9976a89ef5f6c1617
79f37e0b728de2c5a4bfe8fcf292941d54e121b8

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BlueNoroff – AI-Enhanced Operations Targeting Crypto and Financial Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
0602a5b8f089f957eeda51f81ac0f9ad4e336b87
ad01beb19f5b8c7155ee5415781761d4c7d85a31bb90b618c3f5d9f737f2d320
14e9bb6df4906691fc7754cf7906c3470a54475c663bd2514446afad41fa1527
5c83daca1be2c9997550a95f23133ee096deb7548e87b4232a8f965aee3af449
81612cab25c707a4c5d12bb21ff5f87386fb52dcd0a12bbd063a9b4b11f2df14
69d23457d837d4d7fa5be2c853d54420c25792a3d4fba690b41d97ee12a7d17c
bd2aa5805b76f272b43a595b3d73e29d0fc4647e15e87950b8f904ea26dcf053
a1a09c0b98a69681707ccd054b480afe07ce1d7fc07fbaf84a51b312ec33d5aa
d21e88f255d49476bad526796cfadaf14c4ceb1c5cba08bc9d8bf7c7d8146e84
29f68201b878ccf21c41d9dc6a060961d49c55a6c2d32e2c205915320aff7bbe
45224b7d4b44833a4853729205e539b41b101381ab3b3d1e8dbe3e5efa936fb9
ccf7f7678965105142f6878d7b1f1f1c6f31fdbc45b0e50b8e70d0441f0b7472
41660a23e5db77597994e17f9f773d02976f767276faf3b5bac0510807a9a36f
2b0758b36ccefaf5f126e2eac16637249c1b5f27b89b791a716c96ff4b319f1f
5f4063e3a5583e62ddec2f84ca88eb97fbcfbee31d9269742ab438f441f0cd58
c24bb2b28d322faee5a0162675c0c579a5224149874742acdd0bdf0157359756
236e9e6fa09e309c3412fa4aa616ffd41dae8159f27e2bdfb44aac45fcb687fe
65b98ddc821212d13e0e64265353725f0adf6bcf3f4129c18d9d6327b8a69e11
4f0083f6a6796c327adba24b9e80c2d71203074e038bfcbce8bca45803a1d9ec
0d1e3a9e6f3211b7e3072d736e9a2e6be363fc7c100b90bf7e1e9bee121e30df
3315e5a4590e430550a4d85d0caf5f521d421a2966b23416fcfc275a5fd2629a
d5f41ea8dbf1ed159a0a4cfce563a917c1df32bb8ac8d321b4d3dcf67271dd25
74cbec210ba601caeb063d44e510fc012075b65a0482d3fa2d2d08837649356a
7ffc83877389ebb86d201749d73b5e3706490070015522805696c9b94fa95ccb
ebaaf177e746f9f0e16c906f1ffea95af771252b07136ca6a13995508fce34aa
bcef50a375c8b4edbe7c80e220c1bb52f572ce379768fec3527d31c1d51138fc