KPMG Cyber Threat Intelligence Platform

NS Stealer : Leveraging Discord for Data Exfiltration

NS Stealer, a recently discovered information-stealing malware, gained attention in mid-November for its sophisticated Java-based architecture. This malicious tool employs a Discord bot as part of its strategy to gather sensitive data from compromised hosts. NS Stealer demonstrates advanced capabilities in swiftly extracting information from systems that utilize the Java Runtime Environment (JRE). The Discord bot channel functions as an EventListener, receiving the exfiltrated data from affected systems as using discord is cost - effective approach which makes it a potent tool for threat actors.

The initial access is achieved through spearphishing emails, distributing ZIP archives disguised as cracked software. Within the ZIP archive, a rogue Windows shortcut file (LNK file) named "Loader GAYve" serves as the initial trigger for the malware execution. Upon execution, a malicious JAR file is deployed, creating a folder with a name in the format "NS-<11-digit_random_number>" to store the harvested data. This folder acts as a repository for stolen information. The malware extensively collects data, including screenshots, cookies, credentials, autofill data from web browsers, system information, lists of installed programs, Discord tokens, and session data from platforms like Steam and Telegram. To enhance its capabilities, the malware utilizes features like X509Certificate for authentication support. The exfiltration process involves zipping the gathered information into a designated folder, followed by the deletion of the folder. In its final stage, the malware sends the zip file, containing all collected data, to a Discord bot channel with the message title "***@here NS-STEALER*** $$$".

NS stealer is a tricky malware, slipping through fake software, stealing valuable data. It is imperative for organizations to fortify defenses against NS-STEALER by consistently updating software's, promoting awareness of phishing risks, and implementing MFA.

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

NS Stealer : Leveraging Discord for Data Exfiltration

Indicators of Compromise: Hashes
7cfd37dad1fe552de49383d13a612fcd
2cc9658708d759082d8448ec5c059fde
100e880abfe77eae339d2c1cf769578f
794bf33c4834a68d5b3019981836a11c
7ee0206a78eb3670a3e827c4459bc681
57eb4b574f76a4066542a5834737023e
0457b3fcc77f1e3b22ce5c6fbf3813c4
02269d6946809df85bc4c466373407d3
3fd24ddd53999430eae7f76d36835a9b
be0e31e81f823a90b40650805f8fbbe4
4b58b2622ef53defc306e6631f51cd25
f2e28a1e67ff7673f3c6e57909f1cfe7
680bea8cc75aabdcf953a0a2df87ad0e
4cdff2e824a162bea68e5d18c458ab3c
fc4c2da35e3cf111b4650b2d05239da4
86620775ed463b38569d3b3ce7857ab7
307d82cb58114ec82f8fdd2df6a3ae43
87d60a21ed28979f2edd1891e07aec20
2840f08dd9753a5b13c60d6d1c165c9a
7a2bcc01232927019008d880a4c71426
92e6031c65dd0061d870907b8218117b
3e1b6aa1b37f02301b523f3ad81095bc
e86a0e9cf3a6d4f8fd69710f2ae3e81c
2b59fe0fec268a155ec478f53a523431
ae37a012afe51b3e8783c910890d9b7f
3de21de1b64a67255c6bae4d3f9bf6d8a4fcb397
685ade8015375b2eb586c67ea82225b31a270177
3669add3057cca24d62df1a5bf7f88d22a4a64cc
Fd58aa03d88f6b49409a50cf6f0396338524e4e2
E1d60b1e265aa2ff0210493cc5ab9838754b6207
A870cbce5747ea91652c0e532dd1f6a7ecb14ec7
Ddf731bc8510a5d414c6ff082c5bd8feaa3cb4c1
Da806688ed31fea9066da478218c897772e7ae94
318148808cc0df272b5725ce3d6a7c60a216cebf
B0fbe749a07ba2e1d414a14f9da5ec920ef18e5b

KPMG

KPMG Cyber Threat Intelligence Platform

NS Stealer : Leveraging Discord for Data Exfiltration

Indicators of Compromise: Hashes
32574676bcd96771550ac13239aa04aa664e1fe9
f893cb591eff1eba84be91f9e2b45d5b28d0650b
60fa70626910b79ecce984b196f6fd659bc9e515
2f1c41e3827e552255c62a2847b4abd8c4526f79
342ce9726fa89cf64fe6ca13dcdc422c1e122221
972f42f3d78ae159217a869eccd8f95aaff940e9
236a490b2f8c66374b3eeb405128a27b8a60825e
d89d98f8e960f7800fa597a52cfb74591118f10f
c89297e75b6813cf8950e278a5c390e2c5f9d9f6
50c3059c270839d1a5cd28aa2db71df69d0765e8
35ddfe601669ce521170b2896ca0698287a6261f
6088d119648da161e57d12bc4171c10f4e4da1f2
b7719d2a5ac760fd92ac965ed1e8d98bdd9fcc5b
d276e6ab3bcf1095b52240e23af1b8fa7c7cd116
9100c8c3df0a19c6bea88abbd37a1d2ba4c3b56b
f02496f4b9da09ae0fbf1b59fbdc4b2193cc9e03134ee4c5e71141bb618fdd0c
506b40e0f199b32a597bb44aa90343cc14830796f2bf3fd7c3fa281a52ce27c9
6d6c788c928c1408dd19de83b6dd1a12092c96b179fc17a66414886cf8d1daf0
90ba262acdb6fd1ead5167a7347a1d66ee0075c24ed18d5b4cb07933a4c42805
a8be7f50b0554e519a8c98ec39d2ba76e0655da133c8795a41d36dc29d9c7433
d5a528f524401a36a6366619f3b2d83efed740801128f527e9dce80e68060922
ded871d290ad309d228c00107d87e88dfadbc9d682ff3e04d9fb63f2c34aa256
ecb4b09bfd34adc671537c98d1b1cd6f662e66077904db0da9f88e2054ef9edd
85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10
3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4
3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f
9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113
3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83
eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224
89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e
bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1
9f92e618bc7a56f03f4906e80ea448d085161b1c4b3f324023b8903da5f043d0
90eee4cb163562bdb64e3947abf4702b00510a68930dd7be5278cab06f0f28f0
fefda850b69e007fceba644483c7616bc07e9f177fc634fb74e114f0d15b0db0
4587e1ce4290dd7ae65c9021145dfbd7b41a865f65011aef479228960aa710fb

KPMG

KPMG Cyber Threat Intelligence Platform

NS Stealer : Leveraging Discord for Data Exfiltration

Indicators of Compromise: Hashes
7c770181859c31bf75fc972850afc69a8d49fcffc699e8e5aa0e65cd15596975
fb49207c686fae355d292506cd2fc219725b8724ed4a2d0f2c45b2c86af3f3ea
1d353d5cb84a9d6cda7d6aca10348e719c75cbdd5cc4319ed45e9ee6562f5096
ccaa73d844c2476646eefceb4d0af3c44a86d6191d2794751538163c583eacfb
ef55db81c4296de2b1c72c8264cee499588214be2531662d16e61be1ab71b63d