KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | North Korean Hackers deploying New MagicRAT

Tracker ID: TN0913 **Date:** 14/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

Background

The Lazarus APT, a North Korean state-sponsored attacker group, developed and is utilizing a new remote access trojan (RAT) called "MagicRAT." Lazarus launches MagicRAT after successfully attacking vulnerabilities in VMware Horizon systems. Despite having rather limited RAT capabilities, it was built with the Qt Framework with the primary intention of making automatic detection via machine learning and heuristics less likely and human analysis more challenging. It is known to target a wide range of entities worldwide, including government, defense, banking, media, and critical infrastructure.

Lazarus Group, also known as APT38, Dark Seoul, Hidden Cobra, and Zinc, is a group of cyber threat actors who are financially motivated and espionage-driven. Bluenoroff and Andariel are "spin-off" organizations of the state-sponsored hacking group that focus on similar attacks and targets as Winnti and MuddyWater. In contrast to the Bluenoroff faction, which is committed to attacking foreign financial institutions and conducting financial thievery, Andariel is steadfast in its pursuit of South Korean organizations and enterprises.

Lazarus develops its malware and attack tools, employs cutting-edge attack techniques, is careful, and is patient. The most recent addition to the group's extensive malware toolkit demonstrates the group's capacity to use a variety of methods and strategies depending on their targets and operational aims. MagicRAT, a C++-based implant, is intended to establish persistence by executing scheduled operations on the compromised machine. North Korean methods, in particular, try to prevent detection by security products and to remain hidden within infiltrated systems for as long as possible. Furthermore, it is "very simple" in that it grants the attacker access to a remote shell from which they may run arbitrary commands and manage files.

MagicRAT can also launch additional payloads obtained from a remote server on infected devices. Furthermore, TigerRAT, a backdoor originally credited to Andariel, meant to conduct commands, collect screenshots, log keystrokes, and gather system information, was discovered to be housed and provided by the C2 infrastructure related to MagicRAT. The most recent version now contains a USB Dump feature, which allows the opponent to search for files with extensions and provides the groundwork for camera video capture. MagicRAT's debut in the field demonstrates Lazarus' goals to quickly produce new, unique malware to be used in conjunction with previously known malware, such as TigerRAT, to attack enterprises all over the world.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | North Korean Hackers deploying New MagicRAT

Tracker ID: TN0913 **Date:** 14/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Command and Control, Execution.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Keep systems and products updated as soon as possible after the patches are released.
- Ensure latest patches are applied to internet-facing VMware Horizon servers.

References

- Jung soo An, Asheer Malhotra and Vitor Ventura, MagicRAT: Lazarus' latest gateway into victim networks, CISCO, 7th September 2022, External Link (blog.talosintelligence.com)
- Ravie Lakshmanan, North Korean Hackers Deploying New MagicRAT Malware in Targeted Campaigns, The Hacker News, 7th September 2022, External Link (thehackernews.com)
- Lucian Constantin, North Korean state-sponsored hacker group Lazarus adds new RAT to its malware toolset, CSO, 9th September 2022, External Link (www.csoonline.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | North Korean Hackers deploying New MagicRAT

Tracker ID: TN0913 **Date:** 14/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

*

SHA-256	URLs	IPs
f6827dc5af661fbb4bf64bc625c78283ef836c6985bb2bfb836bd0c8d5397332	hxxp[://]64[.]188[.]27[.]73/adm_bord/login_new_check[.]php	193[.]56[.]28[.]251
f78cabf7a0e7ed3ef2d1c976c1486281f56a6503354b87219b466f2f7a0b65c4	hxxp[://]gendoraduragonkgp126[.]com/board/index[.]php	52[.]202[.]193[.]124
1f8dcfaebbcd7e71c2872e0ba2fc6db81d651cf654a21d33c78eae6662e62392	hxxp[://]64[.]188[.]27[.]73/board/mfcom1.gif	64[.]188[.]27[.]73
bffe910904efd1f69544daa9b72f2a70fb29f73c51070bde4ea563de862ce4b1	hxxp[://]64[.]188[.]27[.]73/board/pct.gif	151[.]106[.]2[.]139
196fb1b6eff4e7a049cea323459cfd6c0e3900d8d69e1d80bffbaabd24c06eba	hxxp[://]64[.]188[.]27[.]73/board/logo_adm_org.gif	66[.]154[.]102[.]91
1c926fb3bd99f4a586ed476e4683163892f3958581bf8c24235cd2a415513b7f	hxxp[://]64[.]188[.]27[.]73/board/tour_upt.html	
f32f6b229913d68daad937cc72a57aa45291a9d623109ed48938815aa7b6005c		
23eff00dde0ee27dabad28c1f4ffb8b09e876f1e1a77c1e6fb735ab517d79b76		
ca932ccaa30955f2fffb1122234fb1524f7de3a8e0044de1ed4fe05cab8702a5		
d20959b615af699d8fff3f0087faade16ed4919355a458a32f5ae61badb5b0ca		