NOCTURNUS | THREAT ALERTS

HACKING THE HACKERS

OVERVIEW

THREAT TYPE:
REMOTE ACCESS TROJAN

TARGET INDUSTRY:
ANY

ATTACK GOAL:
TOTAL CONTROL
& PROLIFERATION

IMPACTED GEO:
WORLDWIDE

REMEDIATION STEPS

Be careful to avoid installing tools downloaded from untrusted sources.

Periodically proactively hunt in your environment for potential attacks on sensitive assets.

EXPERIENCED A BREACH?
EMAIL US AT

INFO@CYBEREASON.COM

WHAT'S HAPPENING?

Cybereason Nocturnus is investigating a campaign where attackers are trojanizing multiple hacking tools with njRat, a well known RAT. The campaign ultimately gives attackers total access to the target machine.

In this writeup, the Nocturnus team presents an analysis of the attacker TTPs and indicators of compromise. During this investigation, we uncovered hundreds of trojanized files and information about the threat actors infrastructure.

KEY OBSERVATIONS & TTPS

- **A Widespread Campaign:** The Nocturnus team has found a widespread hacking campaign that uses the njRat trojan to hijack the victim's machine, giving the threat actors complete access that can be used for anything from conducting DDoS attacks to stealing sensitive data.
- **Baiting Hackers:** The malware is spreading by turning various hacking tools and other installers into trojans. The threat actors are posting the maliciously modified files on various forums and websites to bait other hackers.
- **Using Vulnerable Wordpress Sites:** The threat actors are hacking vulnerable WordPress installations to host their malicious njRat payloads.
- **Creating a "Malware Factory":** It seems as if the threat actors behind this campaign are building new iterations of their hacking tools on a daily basis.
- **Read the full length research here.**

CYBEREASON CUSTOMERS

DETECTED BY THE
CYBEREASON DEFENSE PLATFORM

We highly recommend every customer enable the following features:

- If you do not have Cybereason NGAV activated, consider doing so to prevent against threats like these.
- **For Cybereason MDR customers, the Cybereason team will monitor and triage as well as assist in the mitigation of potential infections.**