NOCTURNUS

THREAT ALERT: COVID-19 MALWARE



OVERVIEW

THREAT TYPE:
PHISHING ATTACK

TARGET INDUSTRY:
ACROSS ALL INDUSTRIES

ATTACK GOAL:
STEAL SENSITIVE DATA &
SPREAD RANSOMWARE

IMPACTED GEO:
ACROSS ALL GEOS

REMEDIATION STEPS

Consider social engineering awareness and training, which are key in preventing such attacks.

Disable macros and install an endpoint protection solution to help mitigate similar attacks.

EXPERIENCED A BREACH?
EMAIL US AT

INFO@CYBEREASON.COM

WHAT'S HAPPENING?

The Cybereason Nocturnus team is investigating multiple types of campaigns that specifically target regions most heavily impacted by the coronavirus with coronavirus-themed files and domains.

Attackers are abusing the pandemic for their benefit by manipulating people's anxiety over the virus to trick them into downloading malware.

KEY OBSERVATIONS & TTPS

» Taking Advantage of Remote Workers: Attackers are taking advantage of the shift to remote work by promoting malware masquerading as VPN installers. This is particularly dangerous as businesses make the transition to remote work and suggest best practices to employees, including the use of VPNs.

» Using Mobile Malware: Attackers are creating malicious mobile applications posing as legitimate apps developed by the World Health Organization to help individuals recover from coronavirus. Instead, the application downloads the Cerberus banking trojan to steal sensitive data.

» Targeting Healthcare Organizations: Attackers are using ransomware to target healthcare organizations, arguably the most vital and overworked among us at this time.

» Read the full length research here.

CYBEREASON CUSTOMERS

PREVENTED & 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.