CHRONOLOGY OF CORONAVIRUS (COVID-19) RELATED CYBER ACTIVITY [CONDENSED]

Since at least January 2020, threat actors have seized on the media attention surrounding the 2019 Novel Coronavirus (COVID-19) global pandemic to launch phishing campaigns designed to distribute malware to unsuspecting users.

AS OF MARCH 23RD, OUR RESEARCH HAS YIELDED:

threat actors or groups

over Indicators of Compromise

malware families

at least

distinct campaigns

various MITRE ATT&CK techniques employed

THREAT OVERVIEW

JANUARY 31

TA542 (MUMMY SPIDER)



JANUARY 31

TA542 (MUMMY SPIDER) PHISHING/LOKIBOT MALWARE



UNATTRIBUTED 💂 EARLY SPEAR PHISHING 🚒 **FEBRUARY** UNATTRIBUTED 🙎 **FEBRUARY 11** PHISHING/PARALLAX RAT 🚒

UNATTRIBUTED (RUSSIA/EASTERN EUROPE) 🙇 🔵 FEBRUARY 13 PHISHING/ AZORULT MALWARE 撫

HADES APT 🖳 **FEBRUARY 20** SPEAR PHISHING / KOPOHABIPYCHA MALWARE

MUSTANG PANDA 🚇 🌘 FEBRUARY 27 PHISHING / COBALT STRIKE MALWARE

> BABYSHARK 💂 🌑 FEBRUARY 27 VB SCRIPT MALWARE 奪

EARLY MARCH

MUSTANG PANDA

MEDITY DOCUMENTS / PLUGX RAT

MARCH 9

UNATTRIBUTED (RUSSIA) **PHISHING / REDLINE STEALER MALWARE**

MARCH 10

UNATTRIBUTED

🐲 WINDOWS APP DOWNLOAD / AZORULT MALWARE

MID MARCH 🔵 💂 HIGAISA MALICIOUS LNK FILE / PLUGX MALWARE

MARCH 12 🔴 🙎 VICIOUS PANDA PHISHING / ROYAL ROAD RTF WEAPONIZER

MARCH 12

MARCH 12

MARCH 12 🚒 RANSOMWARE / NETWALKER MALWARE

MARCH 14

MARCH 14

MARCH 14

MARCH 15
APT36

RANSOMWARE

MALICIOUS DOCUMENT / CRIMSON RAT

MARCH 16 • 🔎 🙉 TA505 AND TA564

MALWARE

Check out the blog and full research report.

Disclaimer: The information contained in this document is provided "AS IS", without warranties of any kind (including, without limitation, with respect to accuracy). It is provided for informational use only. Anomali Incorporated will have no liability, of any kind, with respect to use of such information.