OPEN SOURCE SUMMARY OF CYBER THREAT LANDSCAPE FOR 30 MAR 2020

Hackers Begin Exploiting Zoom’s Overnight Success to Spread Malware

The recent telecommuting shift to web conferencing app Zoom has led to a sharp rise in new domains and users over the last few days. Hackers have recognized this change and created multiple malicious coronavirus-related domains in an effort to profit off the global pandemic. From these domains they’ve staged a variety of malware attacks, phishing campaigns, create scam sites, and malicious tracker apps. Since the outbreak 1,700 new domains have been registered and roughly 25% of them have been created in the last seven days. This is part of a growing trend targeting online platforms for government, schools, video conferencing, and employers.

https://thehackernews.com/2020/03/zoom-video-coronavirus.html?m=1

Coronavirus phishing lures continue to dominate threat landscape

While the volume of cybercrime hasn’t gone up during the COVID-19 pandemic the focus of the phishing attacks has become the primary and effective threat. The lures used in these crimes are sent to the general public, and even with a low success rate are still highly effective. For example, these scams pose as medical providers that invite people to join an “online conference” related to the latest coronavirus information. This tactic would generally fail in normal circumstances, but due to general fears in the public people are more desperate for information and thinking less critically.

https://searchsecurity.techtarget.com/news/252480848/Coronavirus-phishing-lures-continue-to-dominate-threat-landscape

Zeus Sphinx Banking Trojan Arises Amid COVID-19

The Zeus Sphinx banking Trojan has resurfaced after three years, and is taking advantage of the government relief payments.

Sphinx’s core capability is to harvest online account credentials for online banking sites (and some other services). When infected users land on a targeted online banking portal, Sphinx dynamically fetches web injections from its command-and-control (C2) server to modify the page that the user sees, so that the information that the user enters into the log-in fields is sent to the cybercriminals.

https://threatpost.com/zeus-sphinx-banking-trojan-covid-19/154274/