Secureworks®

CYBERSECURITY PREDICTIONS FOR 2024

24 HOUR DWELL TIME

RANSOMWARE

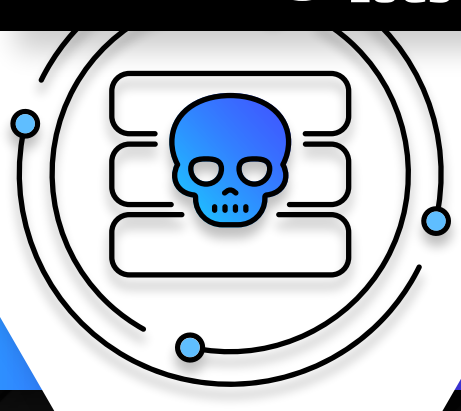
Dwell times will remain low, in line with the median figure for 2023 of less than 24 hours, as ransomware and data theft actors prioritize speed to evade detection.

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) attack figures will continue to rise in 2024, with estimated losses since 2013 now reaching $51 billion USD. We expect to see ongoing innovation in the methods BEC actors use to evade security defenses and deceive end users. Current tactics include QR code phishing, multi-factor authentication (MFA) fatigue attacks, and the use of proxies for adversary-in-the-middle (AitM) attacks.

$51 BILLION IN LOSSES[1]

141% INCREASE IN INFOSTEALER LOGS



MALWARE DISTRIBUTION

2024 will likely mark a shift in how threat actors deliver their payloads. Opting to use multiple smaller botnets helps cybercriminals avoid the widespread disruption caused by law enforcement takedowns of large botnets like Qakbot and Emotet. The use of infostealers will remain high, but it will be interesting to see whether stolen remote access credentials mean infostealers win out as the biggest ransomware precursor compared to scan and exploit.

NORTH KOREA

North Korean threat groups will continue to attack crypto organizations to steal cryptocurrency to fund the North Korean economic and military budgets. To support these efforts, they will further expand their macOS and Linux capabilities to target operating systems that are popularly used in the financial, crypto, and related industries.

RUSSIA

The Ukraine conflict will remain a primary focus for Russian state-sponsored cyber campaigns as they seek to gather intelligence, disrupt critical services and shape the perception of war in the information landscape. Ukraine's allies, both in Europe and abroad, will run a higher risk of attacks. Russian influence operations will likely seek to exploit existing social and political fissures related to foreign support for Ukraine and the 2024 U.S. Presidential elections.

CHINA

Chinese state-sponsored threat groups will increase their emphasis on stealthy tradecraft to conduct cyberespionage attacks undetected. This will include using proxy infrastructure, living off the land via native operating system tools, and adapting their approach to cloud-based environments. The scope of their targeting will remain broad: near neighbors in Asia, and other targets of geopolitical interest, especially the U.S. and Europe.

IRAN

Iran will continue to target political opponents domestically and abroad, in some case using cyber capabilities to inform and guide real-world operations to abduct or harass individuals. We expect Iran will research and develop capabilities to target physical infrastructure via attacks on operational technology (OT) systems. These attacks are likely to focus on Israel.

READ THE STATE OF THE THREAT REPORT

[1] FBI Public Service Announcement (June, 2023) https://www.ic3.gov/Media/Y2023/PSA230609

Secureworks®