DARKOWL

DARK HORIZONS

Will the Top Threats of 2023 Continue into 2024?

Like the years before it, 2023 was busy in cyber security and the dark web with many attacks, emerging threats, and law enforcement activity. As we enter 2024 it is important to be aware of what we are likely to face.

Top Threats:

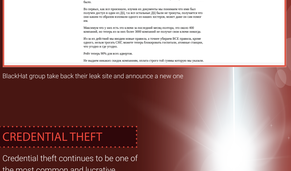
- Ransomware
- Credential Theft
- AI
- Islamic Extremism

RANSOMWARE

4671 ransomware attacks were reported in 2023. Although some groups were disrupted in 2024, new groups emerged with new methodologies and techniques, and some with less "rules" with healthcare and schools being "fair game". Ransomware will continue to be a threat, as double extortion is being conducted by more and more ransomware groups.

Header from CL0P leak site

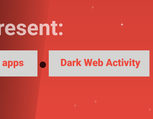
Lockbit 3.0 Leak site



BlackHat group take back their leak site and announce a new one

CREDENTIAL THEFT

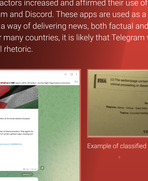
Credential theft continues to be one of the most common and lucrative methods of attack for threat actors. Selling and trading of Stealer Log information will raise in 2024 as these logs allow threat actors to capture credentials, cookies and user agents for victims which can be used to mount attacks and steal accounts.



Redline Stealer Log Header

AI

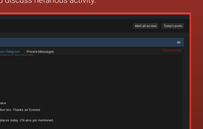
Like the rest of the world, threat actors began to adopt this technology to assist them in their attacks – selling access to AI accounts, providing training on how it can be used to conduct attacks, as well as generating images which can be used for fake IDs used to circumvent financial institutions policies. As the technology matures, we expect this to be used more extensively by threat actors in 2024.



Breach Forums users discuss jailbreaking ChatGPT

ISLAMIC EXTREMISM

Likely linked to the ongoing conflict in Gaza, we have begun to see an increase in material linked to Islamic Extremism. Although not strictly a cyber threat, ISIS and AQAP have previously utilized online methodologies to incite violence and attract and radicalize followers. This will continue with tensions rising in the Middle East.



Inspire Magazine Header

Always present:

- APT Groups
- Messaging apps
- Dark Web Activity

APT GROUPS

APT groups will always pose a threat. They tend to be well funded, sophisticated, and hard to detect and disrupt, with apparent periods of "inactivity". As geo-political tensions rise, Iran and Russia are likely to be very active in 2024. Elections will also likely illicit disinformation campaigns. China has been attributed to a high volume of attacks with a range of sophistication and it is likely to continue, posing the largest and most persistent threat.

MESSAGING APPS

Threat actors increased and affirmed their use of messaging apps such as Telegram and Discord. These apps are used as a means of communication as well as a way of delivering news, both factual and not. As we enter an election year for many countries, it is likely that Telegram will be extensively used to share political rhetoric.

Example of classified document shared on Discord

Telegram Channel for Mysterious Silent force a hacktivist group supporting Hamas

DARK WEB ACTIVITY

Several dark web marketplaces were taken down by law enforcement action and several threat actors arrested in 2023. In response, onion sites are increasing security and rules for participating – increasing captcha difficulty and requiring memberships. The dark web will continue to be a place where threat actors congregate to conduct and discuss nefarious activity.

BreachForums Shout Box

About DarkOwl

DarkOwl collects data continuously at scale from the darknet, and indexes and makes that data actionable for cybersecurity companies, organizations and governments seeking to mitigate risk from malicious actors. We collect and store data in near real-time, allowing it to be queried in a safe and secure manner without having to access the darknet itself.

For more information, visit www.darkowl.com

DARKOWL