# ESET Threat Report T3 2022


DUBAI, UNITED ARAB EMIRATES, February 9, 2023 /EINPresswire.com/ -- Roman Kovac, Chief Research Officer at ESET shares a view of the T3 2022 threat landscape as seen by ESET telemetry and from the perspective of ESET threat detection and research experts

In 2022, an unprovoked and unjustified attack on Ukraine shocked the world, bringing devastating effects on the country and its population. The war continues to impact everything from energy prices and inflation to cyberspace, which ESET researchers and analysts have monitored extensively throughout the year.

Among the effects seen in cyberspace, the ransomware scene experienced some of the biggest shifts. From the beginning of the invasion, we've seen a divide among ransomware operators, with some supporting and others opposing this aggression. The attackers have also been using increasingly destructive tactics, such as deploying wipers that mimic ransomware and encrypt the victim's data with no intention of providing the decryption key.

As you will read in the ESET Threat Report T3 2022, the war also affected brute-force attacks against exposed RDP services, with these attacks nose-diving in 2022. Other factors that might have contributed to this slump, besides the war, are a decline in remote work, improved setup and countermeasures by company IT departments, and a new brute-force blocking feature built into Windows 11. Most of the RDP attacks detected in 2022 originated from Russian IP addresses.

Even with the decline in RDP attacks, password guessing was still the most favored network attack vector in T3 2022. And despite remedies being available for the Log4J vulnerability since December 2021, it still placed second in the external intrusion vector ranking. Various crypto-threats were impacted by plummeting cryptocurrency exchange rates on one side and soaring energy prices on the other. While traditional crimeware such as cryptostealers and cryptominers

declined, cryptocurrency-related scams have been going through a renaissance: cryptocurrency-themed phishing websites blocked by ESET products increased by 62% in T3, and the FBI recently issued a warning about a surge in new crypto-investment schemes.

Numerous holidays celebrated in December led to increased phishing activity impersonating online shops, as people buying gifts online represent a very lucrative target for cybercrooks. And when mobile game developers rolled out new releases before the Christmas season, attackers exploited the hype by uploading their modified malicious versions to third-party app stores. In turn, we've observed a significant increase in Android adware detections in T3 2022.

The Android platform also saw an increase in spyware throughout the year, due to easy-to-access spyware kits available on various online forums and used by amateur attackers. And although overall infostealer detections trended down in both T3 and the whole of 2022, banking malware was an exception, with detections doubling in a year-on-year comparison.

The final months of 2022 were bustling with interesting ESET research findings. Our researchers discovered a MirrorFace spearphishing campaign against high-profile Japanese political entities, and new ransomware named RansomBoggs that targets multiple organizations in Ukraine and has Sandworm's fingerprints all over it. ESET researchers also discovered a campaign conducted by the infamous Lazarus group that targets its victims with spearphishing emails containing documents with fake job offers; one of the lures was sent to an aerospace company employee. As for supply-chain attacks, we found a new wiper and its execution tool, both of which we attribute to the Agrius APT group, aiming at users of an Israeli software suite used in the diamond industry.

As always, ESET researchers took multiple opportunities to share their expertise at various conferences, appearing at AVAR, Ekoparty and others, where they took deep dives into technical aspects of most of the aforementioned ESET Research discoveries. For the upcoming months, we are happy to invite you to ESET talks at Botconf, RSA Conference and others.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here