ESET Threat Report T2 2022

Issued by ESET

28 Nov 2022

ESET released its T2 2022 Threat Report in October, summarising key statistics from ESET detection systems, and highlighting notable examples of ESET's cybersecurity research.

Steve Flynn, sales and marketing director, at ESET Southern Africa.

The latest issue of the ESET Threat Report (covering May to August 2022) sheds light on the changes in ideologically motivated ransomware, Emotet activity, the most-used phishing lures, how the plummeting cryptocurrency exchange rates affected online threats, and the continuation of the 89% sharp decline of Remote Desktop Protocol (RDP) since the T 1 Threat Report. ESET analysts think these attacks continued to lose their steam due to the Russia-Ukraine war, along with the post-Covid return to offices and overall improved security of corporate environments.

Even with declining numbers, Russian IP addresses continued to be responsible for the largest portion of RDP attacks. “In T1 2022, Russia was also the country that was most targeted by ransomware, with some of the attacks being politically or ideologically motivated by the war. However, ESET Threat Report T2 2022 shows that this hacktivism wave has declined in T2, and ransomware operators turned their attention towards the United States, China, and Israel,” explains Steve Flynn, sales and marketing director, at ESET Southern Africa.

According to ESET telemetry, August was a vacation month for the operators of Emotet, the most influential downloader

strain. The gang behind it also adapted to Microsoft's decision to disable VBA macros in documents originating from the internet and focused on campaigns based on weaponised Microsoft Office files and LNK files.

The report also examines threats mostly impacting home users. ESET phishing feeds showed a sixfold increase in shipping-themed phishing lures, most of the time presenting the victims with fake DHL and USPS requests to verify shipping addresses. "In terms of threats directly affecting virtual and physical currencies, a web skimmer known as Magecart remains the leading threat going after online shoppers' credit card details. We also saw a twofold increase in cryptocurrency-themed phishing lures and a rising number of cryptostealers," says Flynn.

The ESET T2 2022 Threat Report also reviews the most important findings and achievements by ESET researchers. They uncovered a previously unknown macOS backdoor, and later attributed it to ScarCruft, discovered an updated version of the Sandworm APT group's ArguePatch malware loader, uncovered Lazarus payloads in trojanised apps, and analysed an instance of the Lazarus Operation In(ter)ception campaign targeting macOS devices while spearphishing in crypto-waters. ESET researchers also discovered buffer overflow vulnerabilities in Lenovo UEFI firmware and a new campaign using a fake Salesforce update as a lure.

Besides these findings, the report also summarises the many presentations given by ESET researchers in recent months, and shares planned presentations for AVAR, Ekoparty, and many other conferences.

For more information on the ESET Threat Report, please refer to the ESET Threat Report T2 2022 on WeLiveSecurity. Make sure to follow Research on Twitter for the latest news from ESET Research.

Threat Report - summarised

- Politically motivated ransomware declined; operators turned their attention from Russia back to their usual targets such as the United States, China, and Israel.
- Emotet continued to be active, with detections seen mainly in Japan and Italy; according to ESET telemetry, its operators took time off in August.
- ESET phishing feeds showed a sixfold increase in shipping-themed phishing URLs, with the most commonly impersonated brands being USPS and DHL.
- Web skimmer known as Magecart constituted three-fourths of all banking malware detections, leaving far behind the rest of the malware strains in the category.
- Cryptocurrency threats went down along with the price of bitcoin; however, the previously declining category of Cryptostealers grew by almost 50%.

- **Eset launches solution to address SOHO security concerns** 15 Apr 2024
- **Don't gamble with your cybersecurity** 29 Feb 2024
- **Avoiding job scams, and finding a job you love** 9 Feb 2024
- **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024
- **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET

ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.
Profile | News | Contact | Twitter | Facebook | RSS Feed