BIZCOMMUNITY

Eset Threat Report: Ransomware and password-guessing top cybersecurity threats

Issued by ESET

23 Feb 2022

- Ransomware surpassed the worst expectations in 2021, with attacks against critical infrastructure, outrageous ransom demands and over USD 5 billion worth of potential bitcoin transactions in the first half of the year alone.
- RDP (Remote Desktop Protocol) attack numbers from the last weeks of T3 2021 broke all previous records, amounting to a staggering yearly growth of 897%.
- Android banking malware detections rose by 428% in 2021 compared to 2020.
- ProxyLogon vulnerability was the second-most frequent external attack vector in ESET's 2021 statistics, right after password-guessing attacks.
- Attacks exploiting the Log4Shell vulnerability were the fifth-most common external intrusion vector in 2021.

Eset Research has released its T3 Threat Report for the fourth quarter of 2021, summarising the key statistics from Eset detection systems between September to December 2021.

The research reveals a rising scourge of email threats towards the end of 2021 and a marked increase in threats exploiting customer excitement around cryptocurrency's bull run at the end of the year. But it was, the nearly 900% increase year on year of Remote Desktop Protocol (RDP) attacks, and a critical flaw in the Log4j utility, that was a great cause for concern in the latter part of the year.

IT teams everywhere were sent scrambling, again, to locate and patch the Log4j flaw in their systems. "This vulnerability, scoring a 10 on the Common Vulnerability Scoring System, put countless servers at risk of a complete takeover – so it came as no surprise that cybercriminals instantly started exploiting it. Despite only being known for the last three weeks of the year, Log4j attacks were the fifth most common external intrusion vector in 2021 in our statistics, showing just how quickly threat actors are at taking advantage of newly emerging critical vulnerabilities," explains Roman Kováč, chief research officer at Eset's Slovakia-based research lab.

According to Eset telemetry, the end of the year was also turbulent for RDP attacks, which escalated throughout 2020 and 2021. RDP attacks exploit the fact that many work from home environments leave enterprise networks vulnerable if organisations fail to secure end-points due to the rapid adoption of work from home working policies.

Numbers from the final weeks of 2021 broke all previous records, amounting to a staggering yearly growth of 897% in total attack attempts blocked.

Ransomware threats continue unabated

But it has been a monumental rise in ransomware attacks that continues to be one of the most significant concerns even into 2022. "Since 2020, ransomware threats have been more aggressive than ever," says Steve Flynn, sales and marketing director for Eset Southern Africa.

"Ransomware surpassed the worst expectations in 2021 with attacks on critical infrastructure, even here in South Africa, crippling many institutions both public and private," he says.

Ransom demands and over USD 5 billion worth of bitcoin transactions tied to potential ransomware payments were identified in the first half of 2021 alone. As the bitcoin exchange rate reached its highest point in November, Eset experts observed an influx of cryptocurrency-targeting threats, further boosted by the popularity of non-fungible tokens (NFTs).

Steve Flynn - Sales and marketing director for ESET Southern Africa

Android banking malware shows an alarming increase

In the world of mobile, Eset noted an alarming upsurge in Android banking malware detections, which rose by 428% in 2021 compared to 2020. Banking malware threats are almost as prevalent as adware, a common nuisance on the Android platform.

Phishing remains a problem

Email threats, the door to a myriad of attacks, saw their yearly detection numbers more than double. This trend was mainly driven by a rise in phishing emails, which more than compensated for the rapid decline in Emotet's signature malicious macros in email attachments. Emotet, an infamous trojan inactive for most of the year, as illustrated in the report, came back in the last quarter of the year.

No platform is immune to threats.

The Eset T3 2021 Threat Report also reviews the most important research findings, with Eset Research uncovering: FontOnLake, a new malware family targeting Linux; a previously undocumented real-world UEFI bootkit named ESPecter; FamousSparrow, a cyberespionage group targeting hotels, governments, and private companies worldwide; and many others. The full report contains an analysis from Eset researchers on all 17 malicious frameworks known to have been used to attack air-gapped networks.

Rounding out the report is news that ProxyLogon vulnerability was the second-most frequent external attack vector in Eset's 2021 statistics, right after password-guessing attacks.

Microsoft Exchange servers fell under siege again in August 2021, with ProxyLogon's "younger sibling", named ProxyShell, which has been exploited worldwide by several threat groups.

"The move online has made everyone's life much easier during the pandemic. Organisations and their people have been quick to adapt, but this brought levels of threats we have never seen before. Cybercriminals are more determined than ever to exploit any vulnerability, and users are going to have to take cybersecurity seriously if we are to get on top of these threats in any meaningful way in the future," concludes Flynn.

For more information, check out Eset Threat Report T3 2021 on WeLiveSecurity or follow Eset's social media pages: LinkedIn, Facebook, and Instagram.

About Eset

For more than 30 years, Eset® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, encryption and multifactor authentication, Eset's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defences in real-time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by Eset's R&D centres worldwide, working in support of our shared future. For more information, visit www.eset.com/za or follow us on LinkedIn, Facebook, and Instagram.

- **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