September – December 2021

ESET Threat Intelligence Index

A look back at the key cyber trends and threats from the final third of 2021, and a look forward at what's to come in 2022

Executive Briefing

As you may know ESET, the largest cybersecurity vendor in Europe and the fourth largest in the world, releases three Threat Reports each year, providing in-depth technical analysis of cyber threats and trends from around the world.

However, when running a business or team, we often don't have time in our busy working day to digest the all of the information that comes across our desks. As a result, I felt it was important to summarise and highlight what are really important and serious trends facing organisations today. To that end, we have produced our inaugural ESET Threat Intelligence Index, highlighting the key trends impacting businesses and giving predictions and recommendations on how they can protect themselves going forward.

The ESET Threat Intelligence Index sheds light on the most frequent cyberattack vectors for UK businesses in the last third of 2021, and makes sobering reading.

Between September and December 2021, on average ESET blocked 4.8 million web threat and 400,000 unique URLs daily, a rise of 2.6% on May – August 2021. The most frequent external attack vector was brute-force attacks, which work to break into accounts through systematically trying all possible combinations to guess passwords. This was followed by exploitation of the ProxyLogon vulnerability on Microsoft Exchange Server that allows an attacker to bypass authentication by impersonating an admin.

The Remote Desktop Protocol (RDP) attacks that first emerged during the lockdowns of 2020, targeting employees using remote access tools to work remotely, continued to escalate. Similarly, ransomware attacks continued to be as aggressive than ever, with T3 seeing the highest ransom ultimatum of USD 240 million, more than triple the previous record.

There was also a 114% increase in ransomware threats on Android devices. However, we did see a 5.9% decline in threats to macOS devices. Interestingly, the "safest" days for devices was Tuesdays, where telemetry detected the lowest numbers of Android threats on average.

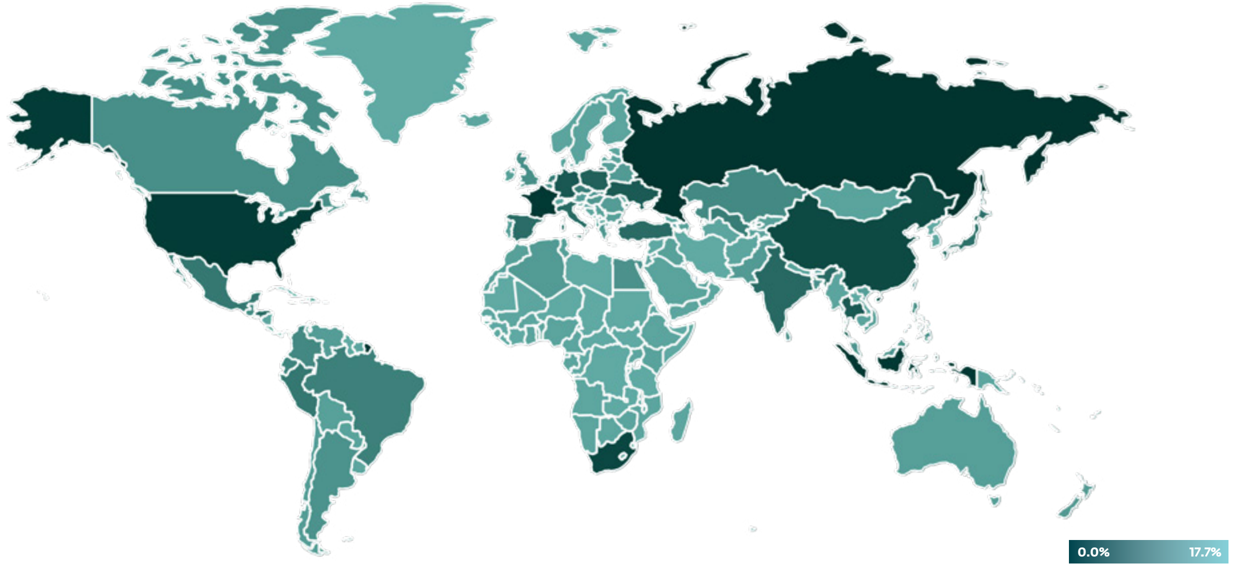
Email threats, often the route in for more serious attacks, saw their detection numbers more than double. This was mainly driven by a rise in phishing emails, with those using DHL and WeTransfer as lures being particularly popular.

As we move into 2022, we expect to see more opportunistic campaigns designed to harvest sensitive information from our increasingly connected world. And, as cybercriminals are always looking for new means of detection evasion, we can expect the attacks to become sneakier and sneakier.

Furthermore, since it is likely that geopolitical tensions will remain high for some time, countries whose governments are actively supporting either Ukraine or Russia will likely also be targeted with cyberattacks intended to disrupt, cause damage, and steal information. We already see hacker groups choosing sides and entering the cyber-battlefield guided by their sympathies. Threats will continue to evolve in volume and sophistication, so it is important to remain vigilant.

Malcolm Tuck
Managing Director at ESET UK

Global distribution of Remote Desktop Protocol password guessing attack attempts in 2021



ESET's Cyber Threat Predictions for 2022

Ransomware

The professionalism of ransomware attacks will continue to improve in 2022, meaning the victim will have less opportunity to decrypt their data without paying the ransom.

RDP

2022 will bring further growth of RDP brute-force attacks. The Log4Shell exploit is here to stay and – together with ProxyLogon or EternalBlue – will become a key part of security testing suites.

Downloaders

In 2022, we expect Emotet's malicious macros in email attachments to surge again as its botnet expands rapidly, returning it to a leading position among downloader families.

Phishing

Rates of phishing attacks will continue to grow, leveraging big brand names, as well as current trends.

Cryptocurrencies

Cryptocurrencies and Non-Fungible Tokens (NFTs) are both likely to lead to an increase in cryptostealers looking to rob users of their funds.

Android

We expect malware developers to focus even more on malicious apps that offer them a high return on investment, such as ransomware, banking malware and threats mining cryptocurrencies on victims' devices.

macOS and iOS

Adware, a type of malware that displays unwanted advertisements on devices, will continue to be the most common threat to the macOS platform, as it is relatively cheap to acquire and does not depend on focused targeting.

IoT

Many threat actors will continue to target IoT devices, such as smart speakers and connected security systems in 2022 – some utilising older malware and vulnerabilities, while others will try to exploit freshly reported flaws.

Key Global Stats

ESET blocked **4.8 million** web threats and **400,000** unique URLs daily

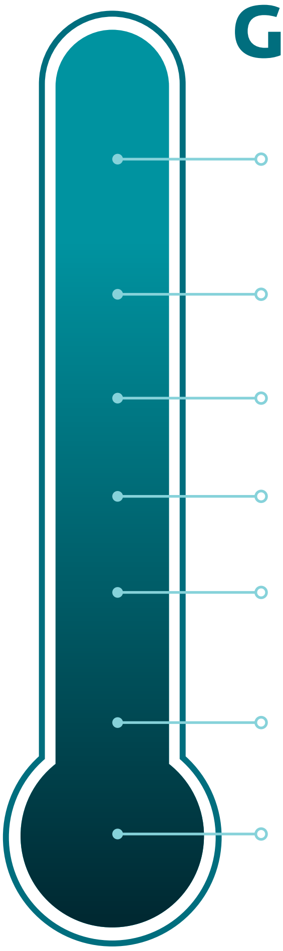
Attempts to exploit MS Exchange and password guessing were the **most frequent** intrusion vectors

There was a record-breaking **206 billion** RDP password guessing attacks

There was also a **114% increase** in ransomware threats on Android devices

Email threats **continued to grow**

Getting hotter



- The highest ever ransom of **$240 million** was seen
- RDP attacks increased by **274%**
- Downloaders increased by **46.1%**
- Email threats rose by **8.5%**
- Cryptocurrency threats increased by **7.7%**
- Overall threat detections rose by **7.2%**
- Android threats advanced by **2.8%**

How to protect your business

The myriad of threats outlined in this document, prove just how potent the issue of cybersecurity is for modern businesses today. Whilst there is no silver bullet, there are several things that businesses can do to mitigate the risk.

Educate staff on the attack vectors cybercriminals commonly use. There is a reason why they continue to use compromised links and infected attachments within emails. It works. Share this document and get teams to undertake regular Cybersecurity Awareness Training, to add a vital layer of protection for the business.

Timely **patching** of applications and operating systems closes off potential avenues of attack. An intelligent, multi-platform patch management solution is recommended.

It is important to create fire breaks within the network. There are several approaches to implementing such a strategy, but the most common is network **segmentation**. It is particularly relevant in the cloud, which has become a fertile hunting ground for cybercriminals.

A properly managed **backup and recovery** program provides a safety net. An all-in approach is needed, though. It is important to backup data and system state on all endpoints, servers, mailboxes, network drives, mobile devices, and virtual machines.

To access the full T3 2021 Threat Report please visit WeLiveSecurity.