Cybercriminals eye passwords and cloud vulnerabilities with a sharp rise in attacks expected in 2023

Issued by ESET

12 Jan 2023

The cybercriminal is relentless, often sophisticated, and extremely persistent. In a constantly evolving threat landscape in which cloud adoption continues to grow and passwords are highly coveted by nefarious actors, attacks are expected to increase sharply in the coming year. However, this is being met with incredible advancement and innovation from the cybersecurity industry, says Carey van Vlaanderen, CEO of ESET South Africa.

Carey van Vlaanderen: CEO of ESET SA

Microsoft published its Digital Defense Report for 2022 which found a 74% increase in password attacks, resulting in approximately 921 attacks per second. “Passwords remain an easy win for threat actors but that is often down to users lending this attack vector to them on a plate. Attackers are cleverly compromising business networks prior to their phishing campaigns in order to look authentic and even when victims believe they are carrying out their due diligence on a site, they can still be duped into believing they are in communication with the real deal,” van Vlaanderen explains.

While nearly 1,000 attacks per second is an astonishing amount, there is much more people and businesses can do to reduce this number. “Passwords continue to be something of an inconvenience in people’s lives, which is often down to not knowing or even trusting the free security layers on offer. Implementing password managers on personal and work devices can help force unique and strong passwords for all accounts applicable. Most importantly, introducing two-factor authentication on every account will help reduce the impact of phishing campaigns hugely,” she adds.

The past year has seen a tremendous increase in businesses and consumers embracing cloud and in 2023 this space will yet again be the target of cybercriminals. Van Vlaanderen says the seismic shift from traditional on-prem to cloud hosting applications and infrastructure elevates cybersecurity risk.

While cloud services offer incredible benefits, it’s imperative that from a risk mitigation perspective, to assign thought and attention to:

- Using a reputable cloud service provider – a fundamental first step.
- Optimising and configuration using best practices.
- Making use of best-of-breed cybersecurity software.
- Multi-factor authentication (which should be standard).
- Encryption (which should be employed wherever possible).
- Strong password policies.
- Assigning credentials and rights only to those that require access.
- Redundancy is essential, backup and a disaster recovery plan should be enforced.
- Test for vulnerabilities timeously.

In 2022 spoof emails and ransomware defined the year and look set to remain a leading concern for people, businesses, and cybersecurity teams in 2023. “The damage caused by emails sent by cybercriminals that convincingly look like they originate from people within an organisation is real and extensive. These types of fraud usually try to create a sense of urgency or employ scare tactics to coerce the victim into complying with the attacker’s requests. Emails with requests for

quick payment should be handled with caution using as emails can be spoofed with legitimate invoices but with cybercriminal banking details," says Van Vlaanderen.

Despite ransomware reaching record levels this year, van Vlaanderen says many organisations still do not understand where their most valuable data and systems lie, and therefore have inadequate data and protection. "A good place to start then is to build an understanding of exactly all the data points that exists in your business, enabling a clear strategy to be formulated on the data that is collected and stored. Irrespective of the size of your organisation, data protection is a must and can be in the form of staff training, following compliance guidelines, utilising appropriate software, as well as ensuring data storage is secure and backed up, and that there is a data or disaster recovery strategy in place."

Van Vlaanderen predicts the continued innovation and adoption of smart technologies, IOT devices, car connectivity and infotainment, will also present new attack vectors for cybercriminals in 2023. "Given the reality of attacks becoming more sophisticated and personalised, people and organisations can't afford to be without some form of a protective solution in place, regardless of where the infrastructure is located or what device it is on."

- **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