computerweekly.com

Social engineering a factor in virtually all cyber attacks, report claims

Alex Scroxton

4–5 minutes

natali_mis - stock.adobe.com

natali_mis - stock.adobe.com

Almost every single cyber attack will, at some stage, require a human to be tricked into doing something, according to research by Proofpoint

-
-

The exploitation of human failings to attack enterprises using so-called social engineering attacks through cloud applications, email or social media, is a factor in up to 99% of cyber attacks, according to Proofpoint's latest annual *Human factor* report.

Based on 18 months of data analysis collated from across Proofpoint's global customer base, the report set out to highlight how bad actors target people by getting them to enable a macro, open a file or follow a link, rather than attacking systems and infrastructure, as they attempt to gain access to enterprises and other organisations.

"Sending fraudulent emails, stealing credentials and uploading malicious attachments to cloud applications is easier and far more profitable than creating an expensive, time-consuming exploit that has a high probability of failure," said Kevin Epstein, vice-president of threat operations at

Proofpoint.

“More than 99% of cyber attacks rely on human interaction to work – making individual users the last line of defence.

“Organisations need a holistic people-centric cyber security approach that includes effective security awareness training and layered defences that provide visibility into their most attacked users.”

Proofpoint highlighted the existence of what it terms “very attacked people”, or VAP, as the most often approached targets. These individuals tend to be located deep within a target organisation, to have access to either funds or sensitive data, and, crucially, to have identities that can be gleaned via corporate websites, social media, trade publications, or even Google searches.

Impostor email messages closely mimic standard business routines, following legitimate email traffic patterns, with downtime at the weekends and spikes on Mondays, except in the case of malware actors, which tend to be distributed more evenly over the first three days of the working week.

Click times also show significant regional differences, said Proofpoint, with victims in Asia-Pacific and North America far more likely to read and click early in the day, while attacks in the Middle East and Europe are more likely to succeed after lunch.

The verticals most likely to be hit by such attacks were found to be education, finance, and advertising and marketing. As previously reported, Proofpoint noted that the education sector in particular seemed to attract the highest-severity attacks, and had the highest average number of VAPs.

Impostor attacks, meanwhile, were at their highest levels in the engineering, automotive and education industries, probably because of supply-chain complexities in engineering and automotive, and high-value VAPs and large student populations in education.

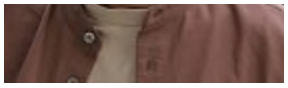
The report also found that given Microsoft's dominance in software estates, nearly a quarter of phishing emails sent during 2018 targeted its

products, with a notable shift towards its cloud services platforms in terms of effectiveness. Most lures were focused on credential theft to create feedback loops that pave the way for future attacks, lateral movement within the victims' networks, or internal phishing.

Threat actors are also refining their tools and techniques, moving from one-to-one and one-to-many attacks to attacks using multiple – often more than five – identities against more than five individuals in their target organisations.

Read more on Hackers and cybercrime prevention

- **UK boardrooms and CISOs increasingly aligned on cyber risks**



By: Alex Scroxton

- 

Red team tool developer slams ‘irresponsible’ disclosure

By: Alex Scroxton

-

Fraudsters adapt phishing scams to exploit cost-of-living crisis

By: Sebastian Klovig Skelton

- **How hostile government APTs target journalists for cyber intrusions**

By: Alex Scroxton