Report: Nearly 100% of Email Attacks Due to End Users Clicking Links

Devolutions

END USERS ARE BY FAR THE WEAKEST LINK IN THE SECURITY DEFENSE CHAIN

A new report by cybersecurity firm Proofpoint is echoing what IT and InfoSec professionals have been earnestly saying for years: end users are by far the weakest link in the security defense chain.

Just how bad have things become? According to the report, more than 99% of email attacks are triggered by end users who click on malicious links, open documents, accept security warnings, and perform other unsafe behaviors. The remaining attacks — which represent a tiny fraction — use exploit kits (EKs) and software vulnerabilities to breach systems. Here are some other key insights from the report:

Phishing Lures

The 10 most common methods (a.k.a. "phishing lures") that hackers use to carry out attacks are:

1. Generic email credential harvesting
2. Office 365 account phishing
3. Financial institution phishing
4. Microsoft OWA phishing
5. OneDrive phishing
6. American Express phishing
7. Chalbhai generic phishing (more on this below)
8. Adobe account phishing
9. DocuSign phishing
10. Netflix phishing

Chalbhai Generic Phishing

In case you're unfamiliar with this type of threat, it involves sending emails that encourage end users to visit various common websites — such as Bank of America, OneDrive, Outlook, Wells Fargo, LinkedIn, Comcast, Yahoo, Chase, and many others — and enter their credentials. Once they do, hackers drain funds and get direct access to their infrastructure services. Chalbhai phishing refers to a range of campaigns associated with templates created and sold by a group collectively referred to as Chalbhai based on artifacts in the templates.

Email Subject Lines

How are hackers enticing victims to pay attention to phony emails vs. trashing them? Here are the 10 most common imposter email subject line categories:

1. Other
2. Payment
3. Request
4. Urgent
5. Greeting

6. Where Are You?
7. W2
8. FYI
9. Gift
10. Document

Targeted Industries

While businesses in all sectors are on the radar screen, hackers are especially interested in these targets:

- Finance
- Manufacturing
- Technology (not IT)
- Healthcare
- Retail
- Construction
- Automotive
- IT
- Industry
- Education

"Very Attacked People"

The report also highlighted VAPs — or "Very Attacked People" — which are end users who represent high areas of risk in their respective organizations. Such users often have easily discoverable identities through corporate websites, social media, government or educational websites, news or published media, Google search, web leaks, breached data, etc. However, VAPs are not necessarily high-profile end users like executives or C-suite. Hackers are targeting employees at all levels, including entry and mid-level staff.

Best Practices for Closing the Human Factor Gap

To be fair, not all end users who inappropriately follow links, open documents, accept security warnings, or perform other behaviors are negligent. As highlighted in our September poll, it is getting increasingly difficult to spot fake emails and websites. Some are surprisingly genuine-looking, with only slight variances between

the real thing and the fake. Furthermore, these variances are often only revealed when hovering over a link, or by contacting the sender directly and confirming authenticity.

To close the human factor gap and minimize the risk of a hack, Proofpoint advises businesses to implement the following best practices:

- Adopt a people-centered security posture that provides visibility into who has been attacked, how they were attacked, and if they clicked on a link or an attachment.
- Use simulated attacks and other methods to train end users so they can identify malicious/potentially-malicious emails, and then rapidly and appropriately report end user concerns.
- Deploy technology that: detects and stops inbound threats before they reach an end user's email inbox; isolates unverified or suspicious URLs in email; blocks threats that use an organization's domain to target customers; and provides strong email fraud defense capabilities.
- Deploy a social media security tool that scans all social networks and accounts, and that identifies fraudulent activity.
- Work with a threat intelligence vendor that combines dynamic and static techniques to find new attack tools, targets and tactics, and which constantly learns from them to get smarter and stronger in the future.

In addition to the above best practices, we recommend implementing a password management solution such as Devolutions Password Server, which enforces robust and compliant Privileged Account Management (PAM) and supports sensitive/confidential data storage and sharing. We also suggest implementing a cloud-based solution like Devolutions Password Hub for non-technical business users — many of whom qualify as Very Attacked People, and are therefore key targets for hackers looking to breach endpoints and infect networks.

From the Desk of Our CSO Martin Lemay:

"I am surprised the report does not mention the very important Multi-Factor Authentication (MFA) control as a mitigation point against phishing. Assuming breach, you need to take into account that credentials may have been compromised by attackers. Your users might not advise your IT or security department when it happens, because they might not even be able to identify the deception in the first place. MFA will protect your accounts against stolen credentials.

"Again, assuming compromise, you need controls deployed at the endpoint level to detect, contain and report threats to your response team. LAPS (Local Administrator Password Solution) technology from Microsoft can help prevent lateral movement using stolen credentials if a user downloads and executes malware. Endpoint detection and response technologies can be leveraged to better respond to this kind

of threat too. These are basic controls that should've been in the report's recommendations, since these controls should happen way before you 'Deploy a social media security tool that scans all social networks and accounts, and identifies fraudulent activity.' Don't hunt for witches: assume breach and protect your environment accordingly."