expel

Top cybersecurity attack trend during COVID-19 pandemic: Phishing

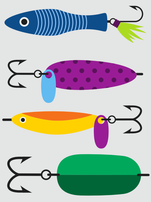
Between March 2020 and March 2021, Expel's SOC noticed a theme – an uptick in credential phishing attacks.

And we weren't the only ones who noticed that during the chaos of 2020, phishing remained a top threat.

In fact, phishing was the top cybersecurity related crime (by number of victims) according to The FBI's 2020 Internet Crime Report.

Why phishing?

Bad actors create phishing emails with links to credential harvesting sites that impersonate webmail login portals or user authentication sites. Once a victim enters their information, the attacker can use these compromised credentials to access email through legitimate web portals or gain access to data within cloud applications.



Phishing is appealing because of its low barrier to entry for attackers: it's cheap and phishing kits are readily available.

These phishing kits target different types of credentials but especially SaaS app credentials.

TOP PHISHING TACTIC IN 2020:

Business email compromise (BEC)

BEC accounts for the most losses as a result of cybercrime.

In 2020, the **IC3** reported **$1.8 billion in BEC losses**, a figure that ransomware pales in comparison to.

There was quite an uptick in ransomware activity, but BEC still reigns supreme (by a lot) as the most prevalent threat to orgs.

Incidents Expel responded to in 2020

Most common BEC attack spotted in Expel's SOC: credential harvesting against Office 365 (O365) users.

BEC incidents represented nearly 60% of all incidents Expel identified in 2020.

If we zoom in on just our cloud security signal, BEC accounts for a whopping 97% of our customer's cloud security incidents.

BEC attempts

MARCH 2020 vs. MARCH 2021

↑51% higher

29% of Expel customers **experienced at least one BEC attempt.**

69% of those customers **experienced more than one BEC attempt.**

Other phishing attacks during 2020

Okta phishing and multi-factor authorization (MFA) bypass

Many orgs migrated all of their SSO (SAML) authentication behind one gatekeeper, especially as people switched to remote work. Which means attackers had to get smarter about bypassing multi-factor authentication (MFA). We saw that Okta, a user authentication software, was a favorite target among attackers. **Getting access to Okta accounts provides a ton of access and it's an easy phishing tactic to pull off.** Expel saw attackers tricking end users into handing over their access credentials by creating fake Okta pages. They were then able to bypass MFA by intercepting session tokens from unsuspecting users.

In the Expel SOC during 2020

35% of the BEC attempts we've spotted **could have been prevented by enabling MFA.**

- 7% of BEC attempts Expel detected **could have been stopped by enforcing modern authentication**
- There was an **increase in targeting of Okta accounts vs. O365 mailboxes** at the end of the year

COVID related lures

Phishing attackers took advantage of the pandemic by **preying on people's fears and desire to help others during a public health crisis** that threatened lives and livelihoods. These attacks mimicked communications related to the CARES Act, unemployment insurance and, more recently, vaccine appointments (IC3 2020 Report).

In the Expel SOC during 2020

We saw email phishing attempts related to:

- Pandemic **relief** and food security **funds**
- Corporate-led **improvement projects**
- **Investments** in COVID-19 programs

Looking ahead: BEC and MFA bypass

So what's in store for the threat landscape in 2021?

While we don't have a crystal ball, it's likely BEC will continue at the same volume. Let's face it: it's an easy avenue for attackers.

In addition to BEC, we saw how session tokens were easily compromised because end users were quick to mash those MFA push notifications after accidentally handing over their credentials to phony authentication pages.

We can expect to see this trend continue as MFA becomes more standard and less "user friction." Which means attackers will find new and more sophisticated ways to defeat MFA.

See how Expel's Managed Phishing service works and what we look for when you report a phishing email.

www.expel.io

Our SOC-as-a-service capability offers 24x7 security monitoring and response for cloud, hybrid and on-premises environments. We use the security signals our customers already own so organizations can get more value from their existing security investments. We connect to customer tech remotely through APIs, not agents, so our SOC can start monitoring a customer's environment in a matter of hours, letting their internal teams get back to focusing on the most strategic security priorities that are unique to their business. Learn more at www.expel.io.