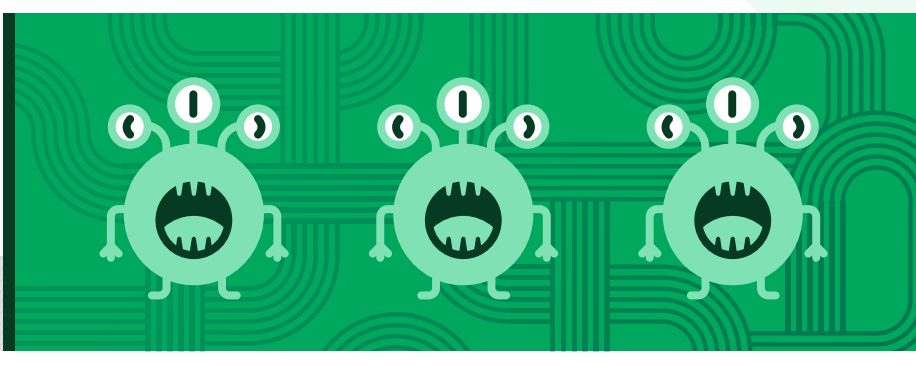
expel

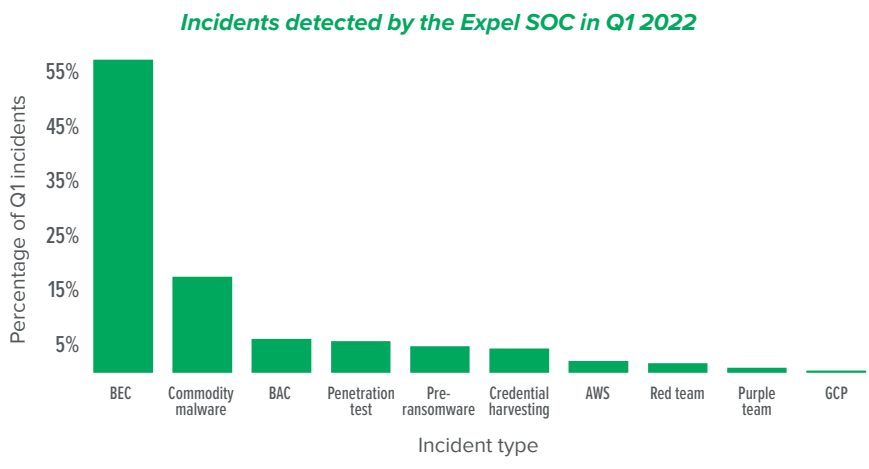
SOC SNAPSHOT #1: Q1/2022

What we're seeing:

Business email compromise (BEC) trends

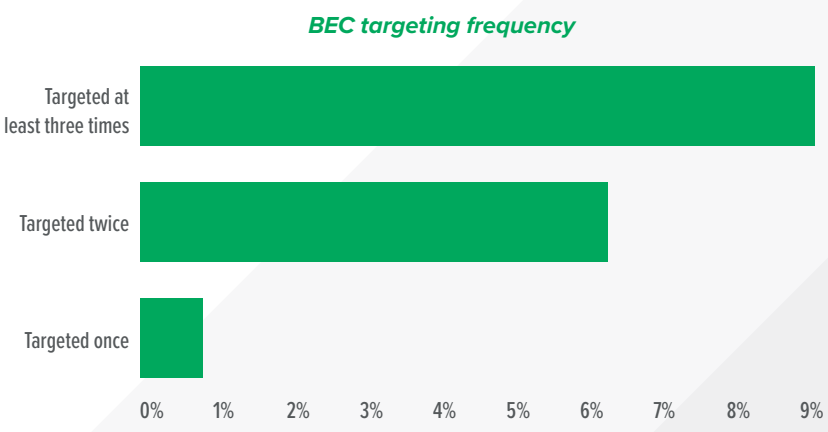


What did our SOC see?



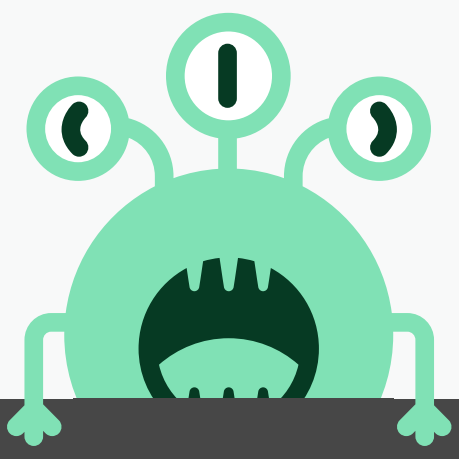
57% of all Q1 incidents were BEC attempts in Microsoft Office 365 (O365). None of the BEC incidents we identified were in Google Workspaces or involved accounts with FIDO security keys.

How many customers were affected?



24% of our customers experienced at least one BEC attempt in O365. Eight percent of our customers were targeted more than three times.

How'd they get in?



2% of BEC attempts in O365 bypassed MFA by abusing OAuth applications.

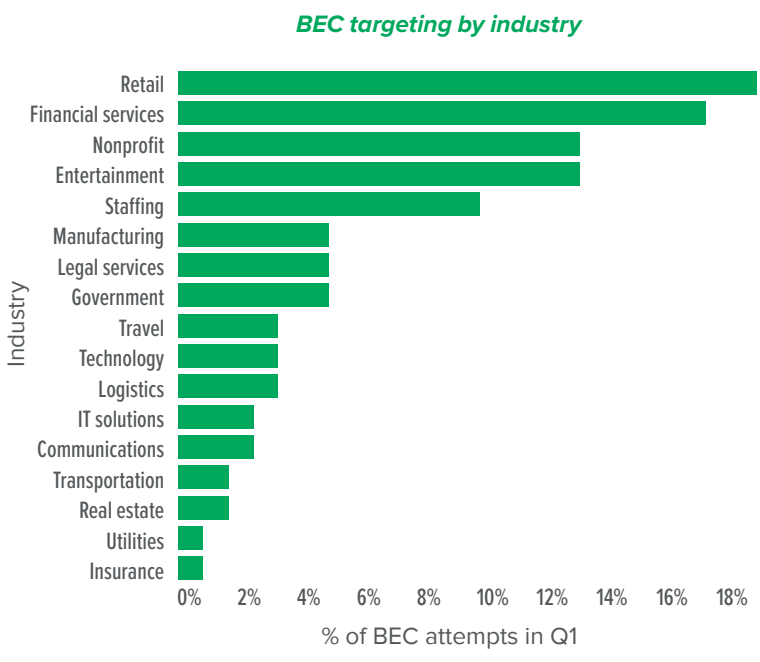
Typical remediation steps of clearing sessions, resetting the victim's password and MFA token **don't work here** — you must remove the malicious OAuth application and its permissions.

Reduce risks associated with malicious OAuth applications by restricting users from registering new applications to Azure AD.

When were attackers most persistent?

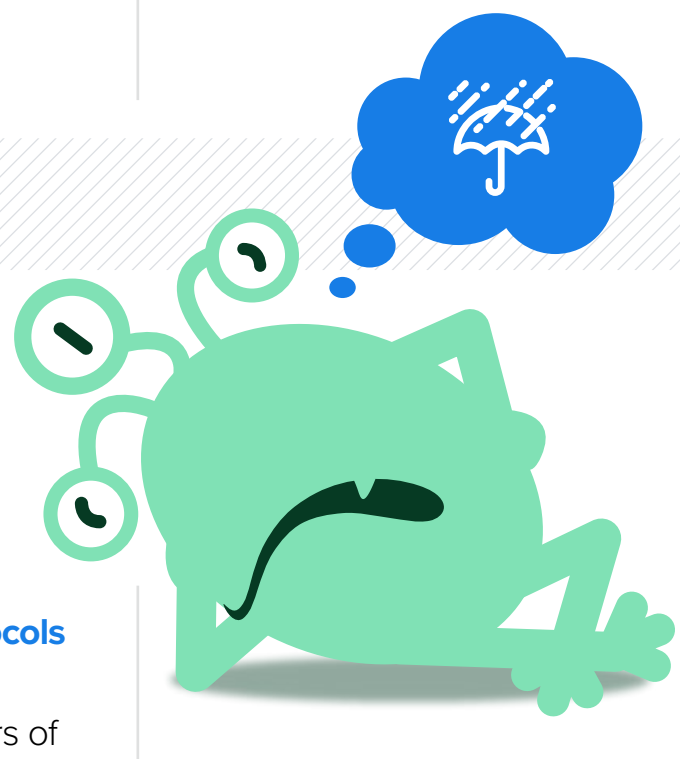
Holidays! Our data showed a spike in BEC targeting the week of Valentine's Day. During this period, our Expel Phishing service identified campaigns to harvest email credentials using Valentine's Day themed lures — preying on people's hearts.

Were specific industries targeted?



Threat actors targeted **retail firms** the most, followed by financial services.

BUT, our data shows that **BEC fraud isn't an industry-specific problem** nor a predictable insofar as revenue. BEC fraud attempts can happen anywhere, to anyone.



How can you help protect your organization?

Run MFA wherever possible using phish-resistant FIDO security keys.

Disable legacy protocols like IMAP and POP3. Implement extra layers of conditional access for your riskier user base (such as executives or employees with access to sensitive data) and high-risk applications.

Consider using Azure AD Identity Protection or Microsoft Defender for Cloud Apps.

Want more deets?
Check out the full Q1 2022 Threat Report

Download report

www.expel.com