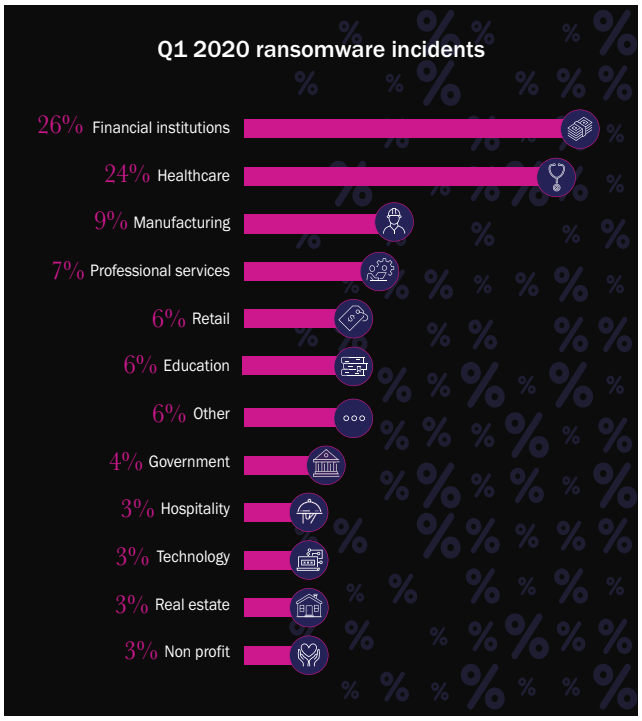
The enduring threat of ransomware

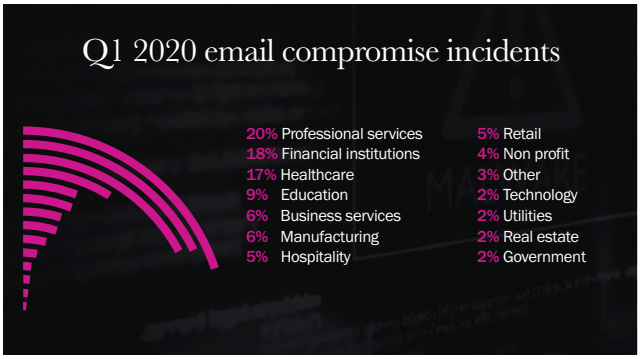
COVID-19-related phishing scams likely to dominate Q2



Ransomware attacks continue to blight organizations of all sizes and sectors. The number of incidents involving ransomware reported to Beazley Breach Response (BBR) Services in the first quarter of 2020 increased by 25% compared to Q4 2019. While no industry was immune, manufacturing experienced the steepest increase of all – up 156% quarter on quarter.

The growing number of attacks against vendors and managed service providers, as highlighted in a previous Insight, contributed significantly to the increase. When a vendor experiences a ransomware incident, many of their customers, often within the same industry, may experience downstream impacts. During Q1, BBR Services noted a particular spike in ransomware incidents at service providers for banks and credit unions as well as for healthcare organizations, which led to multiple notifications.

As threat actors increasingly exploited ransomware, business email compromise (BEC) eased somewhat in Q1; down 16% from the previous quarter, although it remains a problem across all industries. While the financial services, healthcare and retail sectors reported fewer BEC incidents than in Q4, this may prove to be a temporary reprieve tied to behavioral changes amid the response to COVID-19. Employees first adjusting to working from home may have been less responsive to emails generally, and organizations may have been more focused on quickly ramping up remote working capacity than on identifying and reporting BEC incidents.



Phishing scams soar during pandemic

What is clear in Q2 is that cybercriminals have seized on the opportunities presented by the pandemic and we are likely to see more employees falling victim as attacks accelerate. Research from security awareness training experts KnowBe4 reveals that COVID-19-related scams ranging from social media posts, smishing (text message phishing) and, above all, email phishing have skyrocketed during this time.

Social engineering relies on manipulating human emotions to bypass our critical thinking. Cybercriminals exploit uncertain or emotional situations to influence people into taking actions they would typically avoid. Therefore the spike in phishing tricks behind these attacks should not be a surprise given the drastic changes to working practices under lockdown.

During the pandemic, attackers are taking advantage of the fact that many employees have been working from home, without the technical protections that their corporate networks often provide. Furthermore, many employees are working from their personal computers, often shared with family members, processing sensitive and potentially personally identifiable information (PII) without the advantage of managed endpoint protection or even regular patching schedules that are also managed by the typical IT team. Many organizational policies are not designed to function in these distributed environments, leaving them less protected against wire transfer fraud and similar attacks.

Common scams

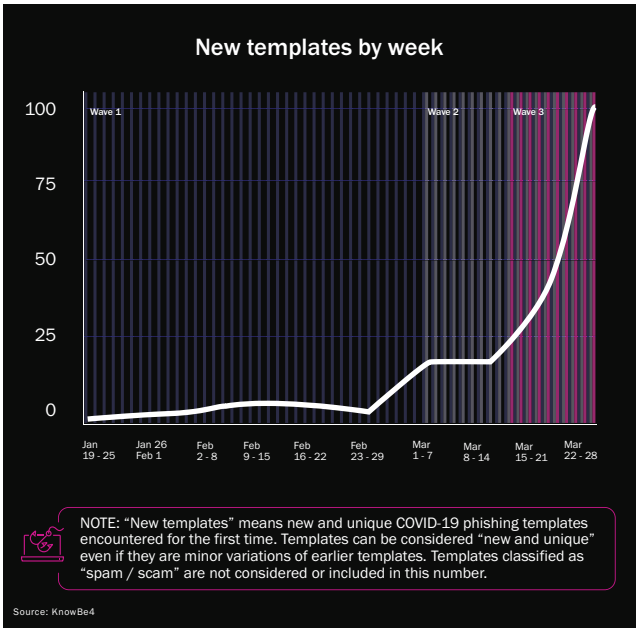
Some of the most common scams in the US that are on the radar of KnowBe4 are The Coronavirus Aid, Relief, and Economic Security Act. These involve scammers sending phishing emails and text messages telling people they need to register on a website to receive the payment. A typical example would involve the victim following a link, where they are asked for bank account information and a social security number for the deposit, as well as other sensitive information.

Another widespread phishing scam is a message designed to look like it comes from the White House with the most recent federal guidance about the outbreak. The attacker supplies a link to a website that looks like an official government page with another link that downloads an infected Word document to the victim's computer.

Even social media is seeing a huge rise in pandemic-related scams. A very prolific one is where the bad actors set-up a fake Facebook page to look like a legitimate company. Here they post that they will be giving a limited number of families one hour to shop for free in their store. All the person needs to do is like and share the post. The scammers start by posting these in local "For Sale" groups in cities using fake or hijacked accounts. Along with the post are instructions to follow a link to confirm their entry into the giveaway. This link is used to send the victim to a website hosting malware or a questionnaire that promises hundreds of dollars in coupons if they fill out a survey. One scam page had almost 5,500 followers after less than 14 hours of being created.

KnowBe4 has highlighted three waves of common scam templates:

1. Spoofs of authoritative sources of information such as the Centers for Disease Control and Prevention, World Health Organization and Department of Health & Human Services and company human resources departments, purportedly offering information and updates on the outbreak.
2. New and novel templates designed exclusively for COVID-19 that move beyond merely offering new information on the outbreak.
3. Repurposed older templates and social engineering schemes modified and updated to include a COVID-19 theme or angle.



As we move into Q2 and the economic fallout of the pandemic response worsens, cyber criminals will seek to exploit fear of financial insecurity and a natural desire for things to return to normal as powerful motivations for phishing campaigns. Organizations that have quickly expanded their remote workforce and now have a larger attack surface will need to be more vigilant than ever to protect against BEC, credential theft, and phishing that opens the door to ransomware and other malware.

BBR Services – a dedicated team of experts

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage cyber incidents successfully. This in-house team of experts works closely with cyber policyholders on all aspects of incident investigation and breach response and coordinates the expert services that insureds need to satisfy legal requirements and maintain customer confidence.

In addition to managing data breach response, BBR Services provides a full range of resources to help mitigate risks before an incident occurs. BBR Services develops and maintains Beazley's risk management portal as well as coordinates newsletters and live expert webinars and pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops.

Seven ways that IT teams can help to protect their organization

1. Use a virtual private network (VPN). Whenever possible, have employees connect from company managed computers and devices through a VPN to the corporate network. Ensure that all traffic is tunneled through this connection. This will allow many of the protections to apply to the traffic being generated from home.
2. Require multi-factor authentication (MFA). Turn on MFA for external access to all applications, particularly sensitive ones such as email, remote desktop protocol (RDP) and VPNs, as well as for administrative accounts.
3. Lock down RDP. The RDP attack vector is regularly targeted by ransomware attacks. Disable RDP where not required. Apply secure configurations where RDP is enabled, including use of strong passwords (at least 16 characters in length) and MFA.
4. Secure personal devices. Implement mobile device management (MDM) for personal devices used to access to the corporate network to manage configuration, ensure scheduled updates, and allow remote wiping of lost or stolen devices.
5. Log and monitor access. Identify and monitor successful and failed login attempts, and restrict logins from regions where employees are unlikely to be connecting from.
6. Patch systems. Allow automatic patching of the operating system and internet browsers. If possible, allow IT staff to help home users ensure their patching is up to date and provide a quality endpoint protection product for them to use. Stay on top of anti-virus software updates to detect new or emerging threats that can go unnoticed in a system if the anti-virus program is out of date.
7. Conduct security awareness training. Train employees on how to recognize common threats and scams and how to report any suspicious security incident. Conduct phishing exercises periodically to enhance security awareness and prepare employees for responding to cyber attacks.

beazley

www.beazley.com

BZCER037_US_06/20