CyberGuard Technologies

Proactive Cyber Defence Report

September 2018

We have long since warned our users about the threat of Business Email Compromise (BEC), but worryingly we have seen a growing number of incidents coming through to our Incident Response (IR) teams.

Trend Micro reports Business Email Compromise attacks have expanded tremendously over the past few years, with a projected growth of over $9 billion in 2018. The combination of simplicity and effectiveness have ensured that BEC will continue to be one of the most popular attacks, especially for those who lack special tools and knowledge, to pull off more complicated schemes.

We can categorise BEC attacks into 2 main types:

- **Credential-Grabbing** – involves the use of keyloggers and phishing kits, to steal credentials and access the webmail of target organisations.
- **Email-Only** – involves an email sent to someone in the Finance Department (usually the CFO) of the target company. The attackers design the email to make it look as if a company executive sent it, typically instructing the target to transfer money. The transfer request is usually for payment to a supplier or contractor, or as a personal favour.

Once compromised, the cyber-criminals search the email inbox for anything of interest, passwords, banking or card details, documents and spreadsheets, or any other information that may have value to launch a new attack. Sometimes we see the cyber-criminals stay under the radar, writing rules to avoid detection, and then using that account to typically ask or change payment and financial details. Once they have the information required, the inbox is typically then used to target all the user's contacts, hoping to breach the next person.

To avoid being the next victim of BEC, we strongly recommend a strong complex password, especially if this is linked to your internal domain, and add two-factor authentication to your login. This is free with most Office 365 plans; these plans should also extend to all VPN and cloud-based applications.

Most Business Email Compromises start with a phishing email and phishing continues to be the largest attack tool used by cyber-criminals.

The Anti-Phishing Working Group (APWG) analyses phishing attack data from industry partners, and reports on its findings quarterly. Their latest, released on 31 July, covers the phishing trends found in Q1 of 2018.

While APWG's reports are probably a quarter behind in their timeliness, the data found remains valuable to demonstrate the trends we should continue to see throughout 2018.

The highlights of the report included:

- Over 11,000 phishing domains were created in Q1
- The total number of phishing sites increased 46% over Q4 2017
- The use of SSL certificates on phishing sites continues to increase to lull visitors into a false sense of security and site legitimacy

All three of these trends add up to one thing – the cyber-criminals are working on looking more and more legitimate. While the poorly-written HTML emails attempting to look like an email from FedEx and other well-known companies still exist today, cyber-criminals are working

diligently to improve their craft – the more legitimacy they can establish through great presentation, proper context, and intelligently targeted spear phishing, the more successful the campaign.

Notable breaches this month…

Timehop, an app that collects and reposts photographs and posts on social media sites such as Twitter, Facebook and Instagram, suffered a data breach. 21 million users were affected, having their names and email addresses stolen. Almost five million users may have also had their phone numbers stolen, although Timehop have said they have detected no unauthorised access to photos or posts at any point. The breach reportedly occurred from access to the company's cloud computing provider, using stolen credentials in December 2017 and early 2018, with the theft of data happening in a two-hour window on 4 July, before access was stopped. Timehop has made it clear that this breach was enabled by the lack of two-factor authentication (2FA) on one of their cloud computing accounts, which has now been added. If only they had read my Global Threat Report!

Remember most breaches will boil down to poor passwords, incomplete patching, or users clicking on phishing emails.

According to media reports, Spanish telecoms provider Telefónica, has suffered the largest data breach in Spanish telecommunications history. It has been widely reported that the breach exposed the personal and financial information of millions of Spanish users of the company's landline, broadband and television services, under the Movistar brand. It was revealed that anyone with an account could view other users' personal data by manipulating part of the URL within the customer portal. Telefónica reported that mitigation measures had been taken immediately, and the vulnerability had been resolved overnight. The Telefónica breach was reported to the Spanish Agency for Data Protection (AEPD), the national agency in charge of enforcing the new GDPR data protection rules. Under GDPR, Telefónica may face a fine between €10 million and €20 million, or a fine that's the equivalent of 2% to 4% of its annual turnover. This is not Telefonica's only problem with cyber-attacks. Media claims some 85% of Telefónica's computers were affected by the WannaCry ransomware attack in May 2017.

Sources:
Threat intelligence provided by Anomoli Labs and Recorded Future.
Content NCSC and Knowb4 and Kaspersky Labs.

Targeted Industries

Social network
Hits: 256 | Targets: Reddit, Google, Facebook, Twitter, LinkedIn
Finance
Hits: 164 | Targets: PayPal, Equifax Inc, Bank of Thailand, Western Union, HSBC Holdings PLC
Software
Hits: 114 | Targets: Google, Cambridge Analytica, Timehop, IBM Corporation, Facebook
Information Technology
Hits: 91 | Targets: Google, IBM Corporation, VMware Inc, Facebook, SAP SE
eCommerce
Hits: 89 | Targets: PayPal, LivingSocial, Under Armour, Amazon.com

Threat Actors

Inj3ct0r Team
Hits: 95 | Targets: WordPress, Joomla, Twitter, Symantec, SCADA and ICS Products and Technologies
FIN7
Hits: 64 | Targets: Saks Fifth Avenue, Lord & Taylor, United States, U.S. Securities and Exchange Commission, JScript
Carbanak
Hits: 9 | Targets: United States, SWIFT, Russia, Payment System, Oracle Corp
Shadow Brokers
Hits: 4 | Targets: Microsoft Windows, Microsoft, Cisco Systems Inc, Iran, China
APT22
Hits: 4 | Targets: Google, Adobe ColdFusion, RSA Security, Microsoft Internet Explorer, United States

Exploited Vulnerabilities

CVE-2016-7255
Hits: 32 | Related products: Microsoft Windows, Microsoft Windows 7, Microsoft Windows 10, Adobe Flash Player, Microsoft Windows 8
CVE-2017-0199
Hits: 8 | Related products: Microsoft Office, Microsoft Office Powerpoint, Microsoft Windows, Microsoft Office Word, WordPad
CVE-2018-2892
Hits: 8 | Related products: Solaris, Solaris 10, Solaris 11.3, OpenSolaris, CVSS 3.0
CVE-2018-8096
Hits: 8 | Related products: EMC Data Protection Advisor
CVE-2018-14777
Hits: 7

Malware

BigChurchSwitch
Hits: 17
Zegost
Hits: 16 | Targets: Microsoft Windows, Government of Nepal, Adobe, Microsoft Internet Explorer, Honeypot
Samsam
Hits: 15 | Targets: Atlanta, Bitcoin, Colorado Department of Transportation, Allscripts, LabCorp
Mirai
Hits: 14 | Targets: Internet of Things, Dynamic Network Services, Inc (Dyn), Deutsche Telekom, Germany, United States
Pegasus
Hits: 13 | Targets: Apple Mac Os X, Android, Mexico, Apple iPhone, iOS

Suspicious IP Addresses

206[.]189[.]61[.]126
Hits: 500 | First seen in Recorded Future on 11 Jul 2018 19:25:46
103[.]224[.]182[.]251
Hits: 155 | First seen in Recorded Future on 12 Apr 2015 07:12:10
71[.]244[.]60[.]231
Hits: 47 | First seen in Recorded Future on 04 Jan 2018 20:18:40
108[.]170[.]54[.]171
Hits: 44 | First seen in Recorded Future on 09 Jun 2018 01:55:51
93[.]89[.]226[.]17
Hits: 41 | First seen in Recorded Future on 12 Nov 2014 20:08:12