Cybersecurity White Paper on Business Email Compromise

TLP:GREEN

Business Email Compromise (BEC) is a form of cybercrime threat that has become more prevalent in recent years, prompting the attention and concern of businesses and organizations worldwide. More than US$195.3 million was defrauded from companies in Hong Kong and overseas in the first 10 months of 2018, and the trend will likely keep growing in 2019.
The most common path for the stolen money is through a wire transfer to Hong Kong or China, so unless there is quick intervention by domestic law enforcement, foreign victims will find it almost impossible to recover their money swiftly.
As a quick reference guide to help Hong Kong organizations select their anti-phishing or BEC solutions, Dragon Advance Tech reviewed several common commercial solutions to defend against BEC threats.

Background

After publishing our Cybersecurity Alert on Business Email Compromise (BEC) in January 2019,[1] we received some enquiries from our clients on how to deploy technological solutions to mitigate such attacks. In this white paper, we summarize our extended research on this type of cybercrime threat and how Hong Kong is affected, and we review several commercial solutions for defending against BEC threats.

BEC in Hong Kong

In August 2017, Andy Robinson of University of Portsmouth – Institute of Criminal Justice Studies published an in-depth study of BEC attacks entitled "Hacking the Boardroom: Business Email Compromise More than CEO Fraud," in which he evaluates the UK Government "4-P's" approach to cybercrime, how this is currently applied to BEC threats, threat mitigation, and future threat predictions. The research also examines the cybersecurity practices of those targeted by BEC cybercriminals and how those at the top of the organizations can be the biggest weakness.

The research also examines the complex money laundering methodologies adopted by BEC cybercriminals, akin to those used to finance the 9/11 terrorist attacks, and how law enforcement agencies and the private sector can work together to disrupt the organized criminal groups behind these cybercrimes. The paper also created a threat intelligence term for BEC: - ***"Financial Fraud Kill Chain" (FFKC).***

Under the Money Laundering chapter, Robinson discloses an alarming phenomenon that Hong Kong is the "ground zero" or preferred destination of the stolen funds obtained by BEC. The paper even discusses BEC cases in which BEC victims are faced with tremendous difficulty when attempting to recover funds through the Hong Kong Police and courts. We have been approached by a BEC expert/victim to assist in recovering defrauded money with the help of a local bank. However, we were told by a bank in Hong Kong that they could not provide direct help to the victim unless the victim was based in Hong Kong. The bank informed us that they are handling many cases

[1] https://www.scmp.com/news/hong-kong/law-and-crime/article/2180879/more-us1953-million-defrauded-companies-hong-kong-and#comments

every day and they could not halt any transactions or temporarily suspend the suspected BEC accounts. They also could not entertain ad hoc direct requests from foreign victims.

Preliminary review of some technological solutions

We have found one free option that can be used to mitigate BEC threats, called DMARC[2] (Domain-based Message Authentication, Reporting and Conformance). DMARC is an email authentication, policy, and reporting protocol. It is the simple, trusted, free solution that brings together email authentication protocols, and adds reporting and compliance. The functionalities of DMARC can be illustrated in the attack tree model of phishing. (Fig. 1)

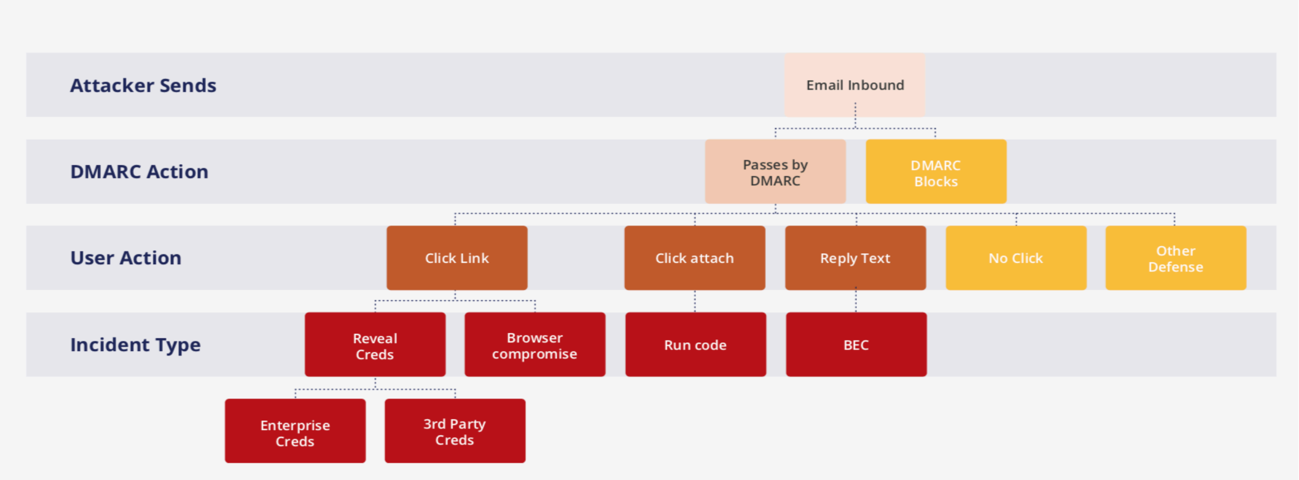

Fig. 1 Attack Tree Model of Phishing by Global Cyber Alliance

There is growing support for DMARC. In June 2016, the U.K. government mandated that all U.K. government departments adopt DMARC, and the EU-CERT has also made a recommendation for the use of DMARC. In October 2017, the U.S. Department of Homeland Security issued Binding Operational Directive 18-01, which requires the adoption of DMARC by federal civilian domains.

We think all Hong Kong organizations, ISP and email service providers should consider adopting DMARC[3] as their email security standard. DMARC is an effective way to limit the spoofing of email from protected domains, and therefore can help organizations defend against BEC threats.

We have also reviewed some commercial Anti-Phishing and BEC solutions (but not on the Secure Email Gateway[4] functions) that are now available to Hong Kong organizations. Below is a quick and short reference on the technical terms, but please note that this review does not represent a complete product evaluation on all aspects of the selected solutions but only a study of the functionalities of each product from a technical perspective. Each organization should exercise their judgement when selecting their suitable anti-phishing or BEC solutions. The following table summarizes our findings:

[2] https://dmarc.org
[3] https://www.globalcyberalliance.org/dmarc/
[4] https://www.forcepoint.com/cyber-edu/secure-email-gateway

	[Solution A]	[Solution B]	[Solution C]	[Solution D]
Purpose	Anti-Spam/Phishing & Phasing Awareness Training	Anti-Spam/Phishing/Secure Email Gateway	Phishing Simulation and Awareness Training	Anti-phishing, Email Fraud & BEC prevention
Deployment Method	MX record forwarding	MX record forwarding	Office365 Add-in, Gmail Chrome Extension	[MX record forwarding]
Deployed Location	Cloud (AWS) or On-premises (Appliance)	Cloud	Cloud	Cloud
Supported Platform	O365, G Suite, Exchange 2003+	O365 & G Suite	Outlook, O365, G Suite	O365, MS Exchange, G Suite
Mobile devices support	Partial	Partial	No	[to be clarified]
Inbound Message Scan	Yes	Yes	No	Yes
Outbound Message Scan	Yes	No Information	No	Yes
Customize Policies	Yes	No	No	[to be clarified]
Admin and User Quarantine	Yes	Yes	No	[to be clarified]
Quarantine Summary Email	Yes	Yes	No	[to be clarified]
Admin Allow / Block Lists	Yes	No	No	[to be clarified]
Anti-Spam Filters	Yes	Yes	No	Yes
Inbound SPF, DKIM and DMARC	Yes (Customize on Portal)	Yes	No	Yes
Anti-Virus Filters	Yes	Yes	No	[to be clarified]
URL Click Protection	Yes (Advanced Edition)	Yes (Enterprise Edition)	No	[to be clarified]
Sandboxing	Yes (Advanced Edition)	Yes (Process all attachments)	No	[to be clarified]
Phishing Awareness	Yes	N/A	Yes	[to be clarified]
Syslog Export		No	No	[to be clarified]
Minimum user	5	10	Not available	[to be clarified]
Price per user per month	Not available	Not available	Not available	Not available

	Pros	Cons
[Solution A]	• Basically all-rounded solution. Company can choose appliance which is an on-premises deployment. • Company need not worry about cloud security. • It provides a portal that allow users to do some customization. Supports the most popular platforms. • It allows the company to do phishing awareness training. • All emails are scanned before they reach the inbox.	• Cloud security and availability may be a concern. (Sandbox feature is a cloud service) • Not a BEC solution or it can only partially detect BEC threats.

[Solution B]	• Supports the most popular platforms. • It has anti-spam filters and sandbox. • The sandbox is hosted in the cloud and managed by the service provider to provide managed detection response (MDR) services to address optional email security needs. • All emails are scanned before they reach the inbox. • URLs and attachments will be opened in a contained environment. • It offers threat hunting services together with the Endpoint Detection and Response (EDR)-type functions which is not validated in this review. • Launched with a very competitive pricing model; especially good choice for SMEs.	• Cloud security and availability may be a concern. • Lack of transparency and customization. • It will modify the URLs in the email. • Not a BEC solution or it can only partially detect BEC threats.
[Solution C]	• Helps the organization to identify Indicator of Compromise (IoC) of phishing attacks. • It allows the company to do phishing awareness training.	• Not an anti-phishing or a BEC solution; or it can only partially detect BEC threats.
[Solution D]	• Claims to protect user against consumer phishing, spear phishing, account takeover, data breach, ransomware, CEO email fraud and BEC. • Quick response with automated investigation and remediation workflows that reduce phishing incident response time. • Delivers detailed impact analysis—including URL, attachment and sender forensics. • Uses security orchestration, automation and response (SOAR) tools that claim to address false positive challenge	• No domestic support • [to be clarified]

Additional note for [Solution C]:
[Solution C] is a phishing identification, analysis, and simulation solution. [Solution C] enables the organization to report suspected phishing attacks and lets the organization's security team simulate internal phishing campaigns to improve resiliency. The solution claims to help the organization learn to identify the key indicators of a phishing attack so that instead of interacting with phishing messages, the users report them. Streamlined reporting and analysis tools enable the organization to quickly identify and respond to reported campaigns that are underway.

Additional note for [Solution D]:
Modern and sophisticated identity-based email attacks easily bypass security controls such as Secure Email Gateways, attachment sandboxing, URL rewriting, and imposter classifiers. These technologies are predicated on a failed security paradigm of attempting to model known bad signals, whether by volume, sender identity, or content. [Solution D] takes a new approach to stopping email attacks, enabled by the [Solution D]'s intelligence on a consistent set of codified terms or email threats taxonomy on different challenges (such as: look-alike domain and domain spoofing, display name deception, compromised account attacks, etc) of the email scam.