Stratecast | FROST & SULLIVAN

April 14, 2017

You've Been Phished, Again!

Solution: Eliminate the Click-it Temptation

Stratecast Analysis by

Michael P. Suby

Stratecast Perspectives & Insight for Executives (SPIE)

Volume 17, Number 13

You've Been Phished, Again!
Solution: Eliminate the Click-it Temptation

Introduction[1]

Who hasn't been phished? According to Symantec, there are not too many. *Based on a 2016 online survey of over 20,000 consumers, 86% said they experienced this electronic form of a confidence game; a game that is designed to trick targets into willingly sharing personal or sensitive information (e.g., log-in credentials), or clicking on a malware-laden attachment or a link to a fraudulent website or webpage.*[2] For the phishers, predominately financially-motivated cybercriminals, this high incident rate encourages them to continue.

Other stats add further encouragement. *From this same Symantec survey, three in 10 consumers state that they cannot detect a phishing attack, and another 13% make guesses between a real email message and a phishing email.* Not bad from a phisher's perspective: four in 10 online consumers are susceptible.

Receiving a phishing email, however, does not complete the game. The email recipients must take some type of compromising action; that is, provide personal information, click a link, or open an attachment. Symantec's survey reported that 13% of consumers that experienced a phishing incident did just that. This finding is similar to the outcomes from a set of 2015 sanctioned phishing tests curated and compiled by Verizon.[3] *Verizon reported that 30% of phishing emails were opened by the email recipients (up from 23% in 2014 phishing tests); and, in 12% of the opened emails, the recipients clicked on the malicious attachment or link (11% in 2014 tests).*

Phishing email recipients were also quick to respond to phishing attack campaigns (phishing emails sent to multiple recipients). Also, as reported by Verizon, *the median time for the first recipient to open a phishing email was 1 minute 40 seconds; and first to click on an email attachment was 3 minutes, 45 seconds.*

With stats like these, it is reasonable to conclude that phishing as a cyber-attack method will increase in frequency. In fact, this has been the case. *The Anti-Phishing Working Group (APWG) reports that the number of known phishing attacks in 2016—1,200,523—represents a 65% increase over 2015, and is the highest annual total since the APWG began monitoring phishing attacks in 2004.*[4]

As we peel back the onion further in the next section, phishing's sinister nature for enterprises becomes even more apparent. Consequently, enterprises are thirsting for effective approaches to mitigate their phishing exposure. Phishing awareness training has shown to reduce exposure, but provides no guarantee of elimination, as a single target responding in a compromising fashion could

---

[1] In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- Area 1 Security – Shalabh Mohan, VP of Product & Marketing
- IBM – Ayelet Avni, Offering Management Leader for IBM Trusteer Rapport

Please note that the insights and opinions expressed in this assessment are those of Stratecast, and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

[2] *2016 Norton Cyber Security Insights Report*

[3] *Verizon 2016 Data Breach Investigations Report*

[4] *APWG Phishing Activity Trends Report, 4th Quarter 2016*

be all the perpetrator needs. And with spear phishing, personalized phishing attacks, even the educated are vulnerable to phishers' social engineering tactics.

Stratecast's perspective is that the ultimate in phishing mitigation is to block all phishing attacks from ever reaching users' device screens. In essence, remove users from the role of defending against phishing attacks. Complete and immediate blocking, of course, is easier said than done; otherwise, it would have been accomplished already. Nevertheless, this does not stop cybersecurity vendors from making concerted headway in this direction.

In this SPIE, we shine a spotlight on the phishing prevention approaches of one start-up company, Area 1 Security; and one long-tenured cybersecurity vendor, IBM. Although complete elimination cannot be promised, each is taking steps that reduce the potential of their business clients (Area 1's Horizon) and their clients' clients (IBM Trusteer Rapport) from becoming victims. Secondarily, by removing the burden of phishing defense from employees and consumers, employees' productivity is positively affected, and consumers' trust in online activities is strengthened.

Phishing: Mechanism for a Bigger Heist

A key aspect of phishing is that it is a stepping-stone mechanism supporting cybercriminals' true objective of income generation. The reality is that pilfering of users' account credentials is not exceedingly valuable. However, the targeted use of those credentials to advance schemes that lead to monetary gain can be great; for example, in business email compromise schemes (described later). Similarly, the delivery of a malware-laden document file, either as an attachment in a phishing email or by enticing users to click on a link for a file download, masks the true threat. The true threat is the placement and denotation of malware on the receiving device and the system that device is connected to. Phishing, consequently, is a conduit for malware delivery, and a very effective conduit.

Analysis from various sources confirms the effectiveness of phishing as a stepping-stone scamming mechanism. For example, Verizon's investigations on data breaches demonstrate phishing as a frequent stepping stone in data breaches. *Based on 2015 data breach investigations, 40% of confirmed data disclosures involved phishing (916 of 2,260 security incidents with confirmed data disclosures)*.[5]

Pertaining just to malware delivery, Invincea and Malwarebytes noted the increasing use of phishing as a delivery vehicle. Invincea stated *". . . by the end of 2015 organizations were five times more likely to suffer a compromise from a spear-phishing delivered weaponized document than from a traditional malware delivery vehicle."*[6] More recently, Malwarebytes stated, *"One of the biggest changes in [malware] distribution in 2016 was the use of attached scripts to phishing emails. These scripts usually reside inside of a ZIP file and, once opened and launched, reach out to a remote server to download and install malicious software on the system."*[7] Malwarebytes further adds, *"Another method that became popular again in 2016 included the use of macros scripts inside of Microsoft Office documents (.docx, .xlsx, etc.), which would execute once the user opened the document and [enticed through social engineering tactics] enabled macros."*

Adding to the challenges of documents containing malware or scripts that download malware from external sources is that the malicious code can be hidden within the document structure, and that code is typically beyond the detection range of traditional anti-virus (AV) products. Glasswall

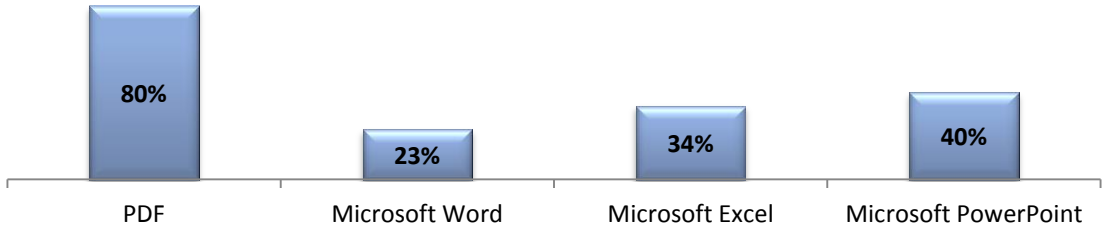
[5] *Verizon 2016 Data Breach Investigations Report*

[6] *Invincea Advanced Endpoint Threat Report, April 2016*

[7] *Malwarebytes State of Malware Report 2017*

Solutions, as shown in Figure 1, determined in an examination of over 300,000 electronic documents that material percentages of known malware (i.e., previously identified and signatures created) were not recognized by traditional AV products, because the malware was hidden within the document structure (i.e., document structure as opposed to content or a functional element such as a macro or JavaScript).[8] As cybercriminals are constantly seeking ways to improve the proficiency of their schemes, hiding malicious code deep in the document structure of a phishing email attachment or a downloaded file improves the potential that the code will land and be activated on user devices.

Figure 1: Percent of known malware undetected by anti-virus products due to being hidden within document structure



Source: Glasswall Solutions Ltd.

The Billion-Dollar Business Email Compromise Problem

Business email compromise (BEC) has become a serious cyber threat to businesses, as evidenced by the FBI ringing the alarm on BEC for several years. In its third Public Service Announcement on BEC, the FBI estimated that BEC dollar losses for the period of October 2013 – May 2016 totaled $3.1 billion.[9] Since this estimate is based on reported BEC incidents, the dollar losses are likely significantly higher if scams not reported or detected were also estimated. Even so, the financial toll on known BEC scams has been on a rapid upward trajectory. The FBI states that there has been a 1,300% increase in identified BEC exposed dollar losses since January 2015.

There are several versions of BEC schemes, and phishing is used in the majority. Figure 2, below, depicts the steps involved in The Bogus Invoice Scheme. For this BEC scheme and others, there are two targets.[10] The first target is someone of high authority within the business. The scheme's objective with this target is to take control of his/her business email account, typically facilitated by a spear-phishing attack that convinces the target to divulge his/her credentials (e.g., "click on this link to change your password"). Or, with passwords frequently being reused by users across several accounts, the perpetrator could attempt email account takeover with credentials gathered from other accounts (e.g., personal email account, bank account), also possibly harvested from another phishing attack.

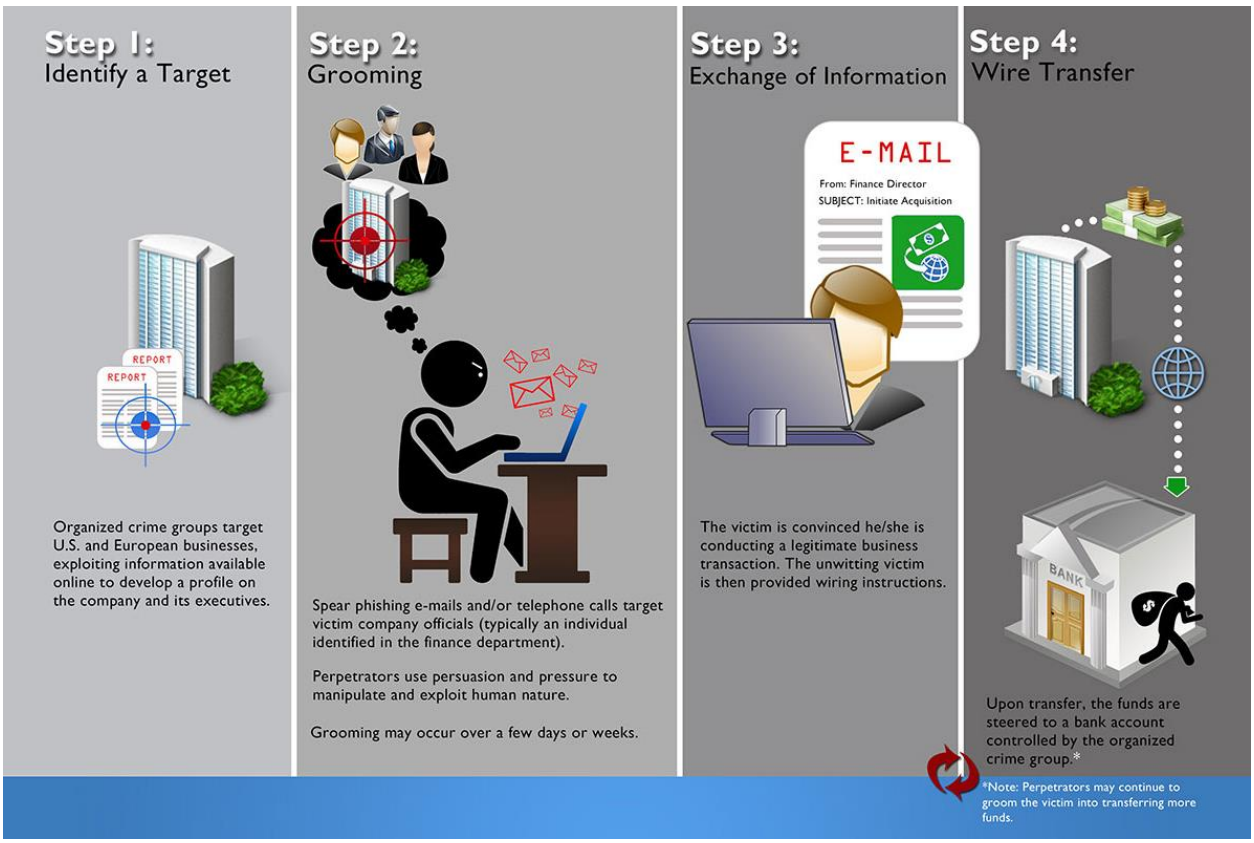
[8] Glasswall Solutions' document sanitization product deconstructs documents at the byte level; then, validates the file against the manufacturer's specification for the document type; and regenerates a fully sanitized 'known good' document in sub-seconds; https://www.glasswallsolutions.com/.

[9] FBI Public Service Announcement, *Business E-Mail Compromise: The 3.1 Billion Dollar Scam*, (June 14, 2016)

[10] This article prepared and posted by Trend Micro, *Billion-Dollar Scams: The Numbers Behind Business Email Compromise*, (June 9, 2016), provides illustrative explanations on five versions of BEC schemes: The Bonus Invoice Scheme, CEO Fraud, Account Compromise, Attorney Impersonation, and Data Theft.

With the credentials to access the first target's business email account, the perpetrator can now impersonate via email this high-ranking individual. Leveraging social engineering techniques, and information gathered on the first target and the business he/she represents, an email is sent to the second target. The second target in BEC schemes frequently includes employees with financial authority (e.g., can authorize a wire transfer or change transfer location) or that have access to personally identifiable information (e.g., employee W-2s). The objective with the second target is to complete the scam; that is, transferring money to the perpetrator's account, or using PII for fraudulent, income-generating purposes. For example with stolen W-2s, they become the fodder for preparing and submitting fraudulent refund-generating income tax filings; with the refunds electronically deposited to a bank account fronted by the perpetrator.

Figure 2: Business e-mail compromise steps and timeline (example: Bogus Invoice Scheme)



Source: FBI

Phishing Attacks Evolve

Successful cybercriminals actively evolve their schemes in order to sustain and grow their income streams, and to counter efforts by businesses and government to thwart them. In phishing, the expanding variations in BEC schemes, and the packing of malicious code into the structure of frequently exchanged document types, are two examples of evolution. But, evolution does not end with these. Phishers are taking measures to complicate efforts to detect and block access to their online traps.

In an examination of over 800 phishing sites detected in September and October 2016, Webroot identified two ominous trends complicating the detection of phishing sites.[11] Those trends are:

- **Shortening the time phishing sites are active** – Rather than maintain a phishing site for weeks, or even months, to support an attack campaign, sites have much shorter durations. In Webroot's phishing site sample, the average time a site is online is less than 15 hours, with the longest in the sample being 44 hours (less than two days). This trend is disconcerting for anti-phishing solutions that rely on post day-one blacklisting, unless they can accelerate their pace of phishing site identification, and propagation of list updates to site-blocking platforms. This is a non-trivial task in consideration of the next trend.
- **Using existing benign domain names in phishing attacks** – Rather than establish a new domain name to host a phishing site, phishers surgically insert one or more webpages in legitimate and benign websites and domain names. Consequently, detection is more challenging as it is not triggered by the launch of a new domain name or website, but by subtle changes to existing websites. Based on Webroot's sample, this is not just a trend but has quickly become an established practice: almost 100% of phishing URLs pointed to malicious pages or sites within benign domains.

Phishing Prevention

Once phishing attacks appear on user devices, as history has shown, nearly one in 10 users take the bait, and take the bait quickly. Viewed in another way, phishing attacks are successful 90% of the time when 10 or more users are targeted. Also, it is reasonable to assume that targeted or spear phishing attacks would have even higher user take-rates, as they have the extra element of personalization to manipulate the targets. And with cybercriminals' phishing success and the prominent use of phishing in BEC schemes, it is also reasonable to conclude that existing anti-phishing approaches are insufficiently "anti." Phishing attacks continue to land on user devices, relegating users as the final arbitrator on whether to click or not.

Despite inadequacies in current approaches to slam the door on phishing attacks, prevention should still be the objective, as prevention reduces reliance on users for phishing defense, and reduces the reliance on post-compromise, reactive activities (e.g., threat detection and response, and data breach damage control). In this remaining section, we outline the recently introduced phishing prevention solutions offered by Area 1 Security and IBM.

Area 1 Security

Distinctive with Area 1's approach to phishing prevention is its preemptive discovery and action. Rather than react to the launch of targeted phishing attacks (e.g., phishing emails or URLs reaching users), Area 1 built ActiveSensor™, a combination of globally distributed physical sensors and online sensors crawling the web continuously, to discover phishers in their pre-attack, preparatory stages of phishing. The collected material is then ingested into SPARSE™, the company's small pattern analytics engine.

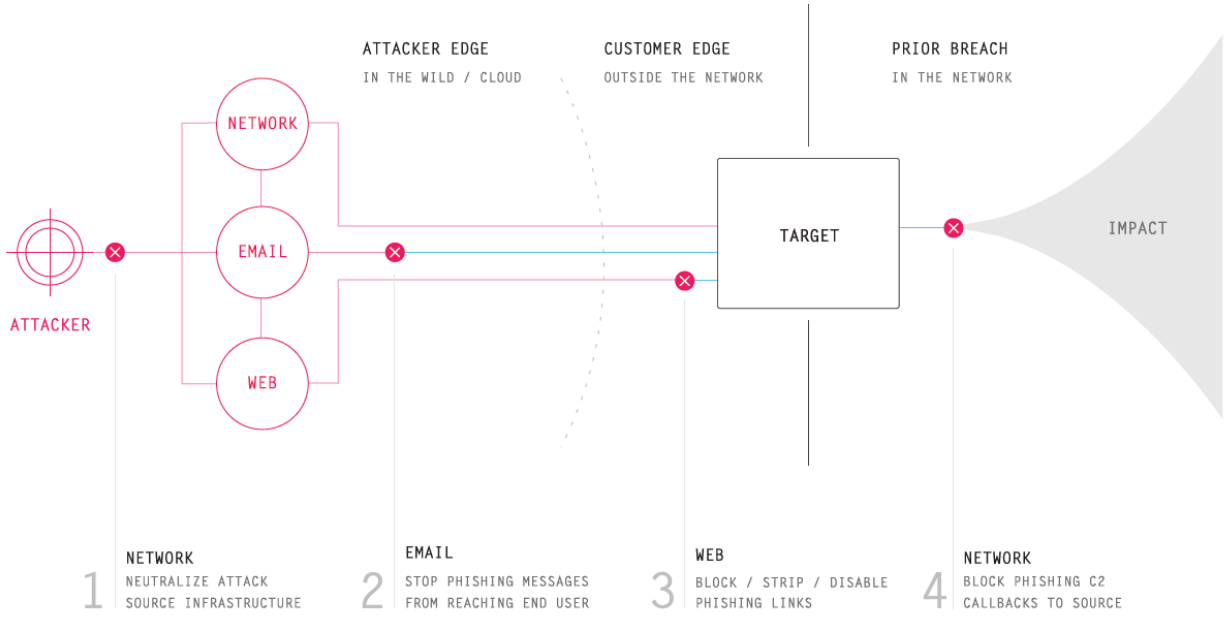
Each ActiveSensor component is described below:

[11] *2017 Webroot Threat Report*

- **Physical Sensors** – Owing to an internet reality that protection and monitoring of internet-connected servers varies, cybercriminals compromise lightly protected servers, and use them as their supporting infrastructure. Undetected by their hosts, cybercriminals build and launch their phishing attacks, and/or use these servers as command posts while the host's commercial operations are on-going. If detected, or sensing the potential of being detected, the cybercriminals simply relocate to other compromised servers. Recognizing this shadow aspect of the internet, Area 1 is co-located in 50 globally distributed servers, owned and operated by assorted businesses. From these silent listening posts, Area 1 spies on cybercriminals; gaining insights on their phishing methods, targets, tools, and sites.
- **Online Sensors (Web Crawlers)** – Further feeding Area 1's insights is its army of high-speed web crawlers. Whereas the physical sensors go deep into infrastructure, the web crawlers go far and wide in the internet to collect additional information on cybercriminals' activities, properties, and tactics. Operational processes are essential in maximizing intelligence-gathering efficacy, while minimizing detection potential. To reach an optimal balance, the company continuously refines its web crawlers along three vectors: 1) frontier management (where to crawl); 2) static and dynamic assessments (what to look for); 3) human-like crawling (project a human-like behavioral appearance to cybercriminals, rather than that of a more readily detected and circumvented robot). According to the company, the web crawlers examine over 3 billion webpages each week.
- **SPARSE Engine** – The continuously gathered information from the physical and online sensors are fed into a data warehouse hosted in Google Cloud Platform. Now exceeding 4 petabytes, Area 1 crunches the data through a 500+ small pattern analytics engine (SPARSE) to detail targeted phishing attacks (what, where, how, and who); and, from that, prepare preventive actions (countermeasures, rulesets, and blacklists). Through the combination of its sensors and SPARSE, the company states it identifies over 400,000 unique targeted phishing sites annually (slightly more than 1 thousand per day). From a "finding the needle in a haystack" perspective, that's one targeted phishing site identified per 390,000 webpages examined.

As illustrated below in Figure 3, the company prevents targeted phishing attacks in the network, email, and web. Aligned with our promotion of prevention before attacks reach users' devices, three of the four attack-prevention actions occur before inbound traffic hits user devices.

Figure 3: Area 1's multi-vector targeted phishing prevention



Source: Area 1 Security

Offered as a cloud-delivered service, Area 1's service, Horizon, is available in three combinable modules:

- **View** – Pre-attack phishing campaign discovery, attack visualization, and context.
- **Fortify** – API-based integration with customers' edge platforms (web proxies, email gateways, and network perimeter defenses) for automated prevention. One such integration is with Symantec's Blue Coat ProxySG, a web security gateway.
- **Extend** – Area 1 cloud-based disablement and neutralization of phishing attacks; that is, before phishing attacks reach the network edge of Area 1's customers (i.e., at position #1, Network, in Figure 3).

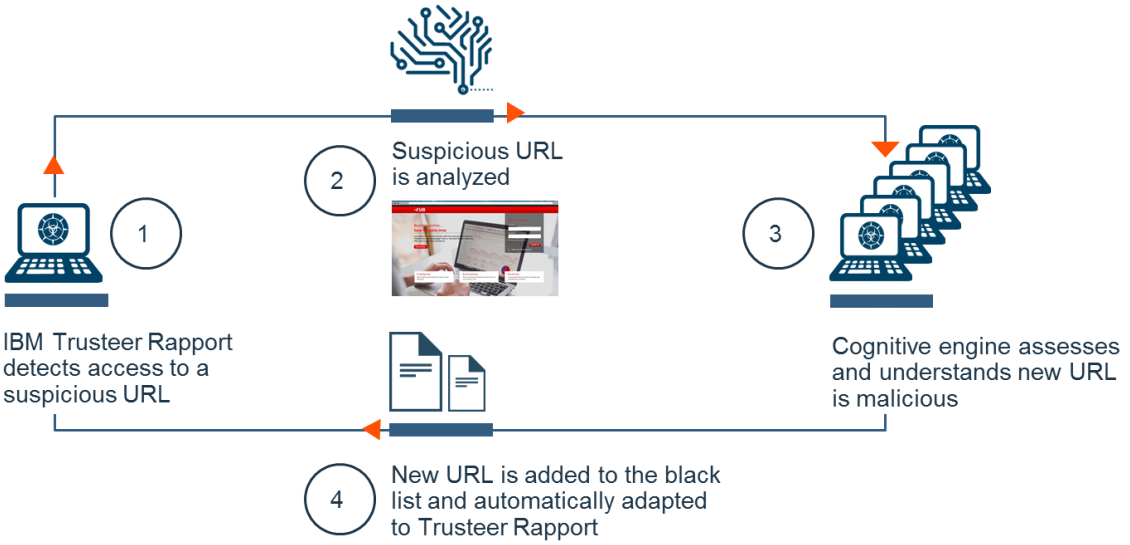
As an entirely cloud-delivered service, Area 1's customers make no infrastructure investments or install any software, either on user devices or in their edge platforms.

IBM

For phishing detection and protection, IBM® leverages its distributed base of IBM Trusteer® Rapport® fraud detecting and prevention endpoint agents (millions worldwide). Trusteer is a fraud protection suite, of which Rapport is one module. Rapport is designed to protect users from malware and phishing attacks. IBM Trusteer customers are primarily in the financial sector. They use IBM Trusteer to protect their customers from online financial fraud.

This recently added feature to Rapport, as shown in Figure 4, follows a four-step approach.

Figure 4: IBM Trusteer Rapport's cognitive approach to phishing detection and protection



Source: IBM

Steps

1. In this step, as a user clicks on a URL (i.e., a webpage), the URL is compared to Trusteer's list of known static and dynamic phishing URLs. If on the list, Rapport customers can customize responses that their users experience (e.g., alert, redirect to a legitimate site, or block access to the phishing site). If the user is alerted, and the user continues to engage with the phishing site, the Rapport customer will be informed of this access, and also whether the user submits his/her credentials (i.e., compromising action).
2. Locally within the Rapport endpoint agent, logic is run on new URLs to detect indicators of phishing. Although light-weight logic, so as not to slow down local processing, this logic is dynamically updated based on changes in phishing tactics (e.g., message has an image file of a legitimate website and very limited script), and aligned with the user's location. On the latter, global-operating cybercriminals modulate their tactics based on cultural norms and past effectiveness, in order to maximize the targets' response rates. Leading to the next step: if a new URL is deemed suspicious, the URL is automatically, and transparently to the user, shuttled to the IBM Trusteer Cloud.
3. In this step, deep analytics are conducted on the phishing-suspect URL in the IBM Trusteer Cloud, to determine, in a matter of minutes, if the site is malicious. As part of the analysis, unstructured website data is examined, including links, images, forms, texts, scripts, DOM data, and URLs. In addition to understanding how the phishing attack is conducted, the compromised brand (e.g., banks, financial institutions, and popular online destinations such as Google, Yahoo, Apple, and PayPal) used as part of the phishing lure (i.e., playing to users' recognition and trust in a brand) is also automatically determined. Like the endpoint agent logic, the cognitive engines in Trusteer Cloud adapt to changes in phishers' strategies and techniques.

4. At this final step, the confirmed malicious URL is added to the IBM Trusteer's blacklist, which extends immediate protection to all endpoints running IBM Trusteer Rapport (step 1).

With the shortening of average duration time for phishing sites (on average, less than 15 hours), and users' quick-to-click propensity (a few minutes), IBM Trusteer Rapport must be built for speed in order to be effective in shielding users from phishing sites. By using cloud-scalable processing and adaptive cognitive technology, IBM states that Trusteer Rapport can examine hundreds of URLs in minutes. Conditionally, in cases where the Rapport's cognitive engines cannot determine with certainty if the site is phishing, the examination defaults to human analysts.

Although Rapport will not stop all users from being victimized by phishing attacks (e.g., the first, fast-responding recipient to a zero-day phishing attack), the community effect of updated and automated protection for all users served by Rapport's customers contains the exposure.

Stratecast
The Last Word

Phishing attacks produce multiple tiers of pain. The first tier is the phishing targets. They include consumers whose identities were stolen and finances pinched; and businesses that had their users' endpoints infected with malware, systems hacked, and employees duped into transferring money to fraudulent accounts. Real pain incurred by real people and real businesses.

Unfortunately, the pain and victims include another tier. This second tier occurs because effective technologies have not existed to thoroughly mitigate the risk of phishing attacks. Instead, there is a reliance on users, whether in their work roles or as consumers, to think before they act. They form a compensating defensive layer for what anti-phishing technological defenses could not completely accomplish: blocking phishing attacks before they reach users. Consequently, businesses lose employee time that otherwise would have been spent on productive activities.

This time loss occurs in several areas. Time spent on phishing awareness training is certainly one area. Another, more subtle, is the time creep of extra seconds spent triaging emails, thinking twice about clicking on a URL, and, although an advisable security practice, using two-factor authentication. Potentially more time consuming and disruptive to the cadence of established workflows is extra authorization procedures. For example, to combat BEC schemes, employees are directed to re-confirm their superiors' requests for sensitive information, or to alter a payment, and confirm through a communication channel other than email (an email reply to the original email may be a reply to a fraudulent party).

For banks, financial institutions, governmental agencies, and health services, trust in online business-to-consumer (B2C) operations allows them to offer more services, more affordably and conveniently, to more of their customers, citizenry, and patients. Yet, if trust in the authenticity of a link or the source of an email is weakened by the continuous onslaught of phishing attacks, adoption and use of B2C online services are likely impacted. Moreover, the very operations that B2C online operations were designed to supplement or replace may need to remain; undermining the full extent of benefits these online B2C operations were to deliver.

This is why the anti-phishing innovations developed by companies like Area 1 Security and IBM take on extra meaning. They, in a manner of speaking, work to protect the trustworthiness of internet-enabled B2B and B2C operations and communications.

Michael P. Suby

VP of Research

Stratecast | Frost & Sullivan

msuby@stratecast.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.