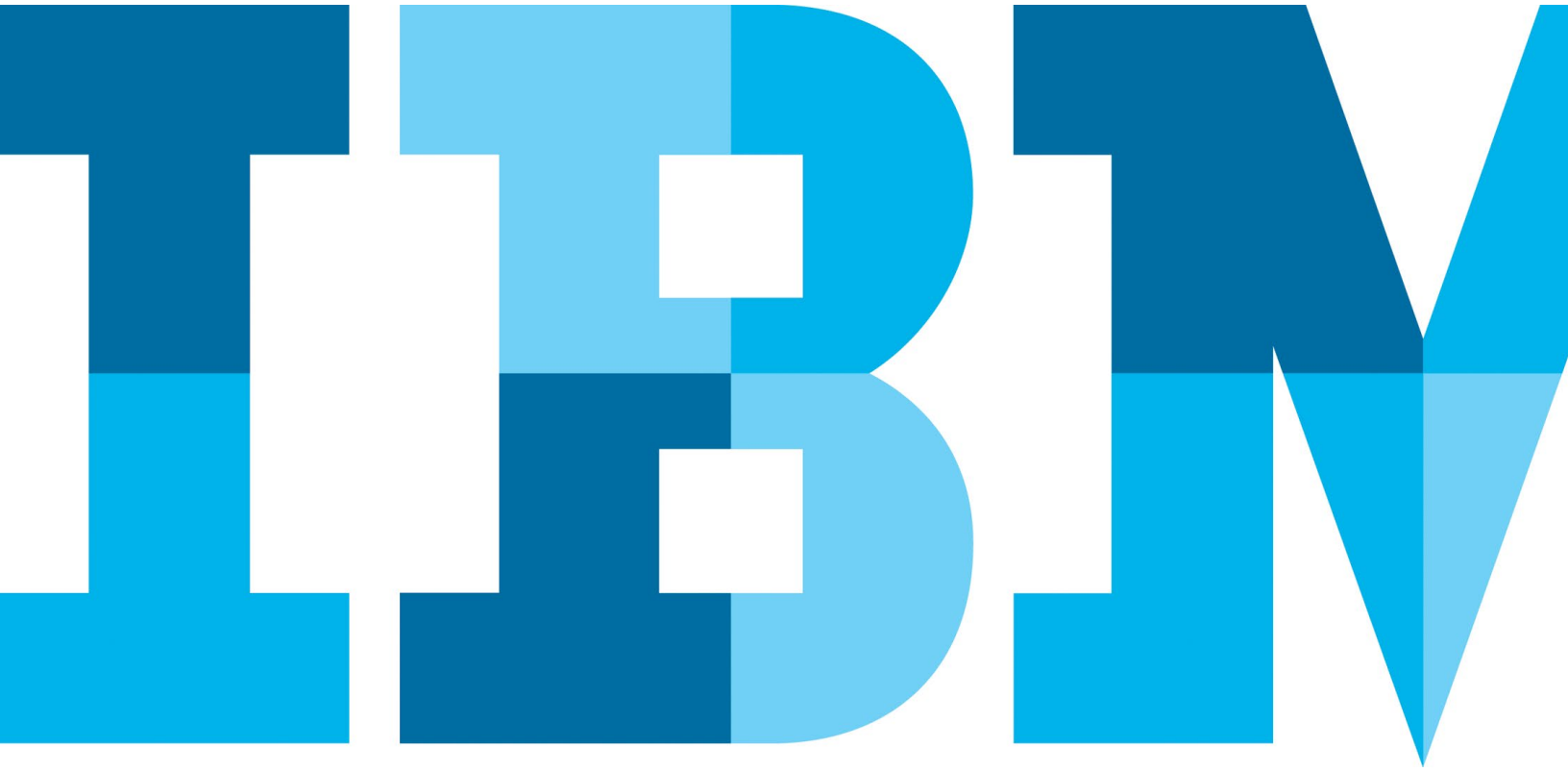
Security

Thought Leadership White Paper

March 2017

Transforming the approach to phishing detection and protection



IBM

Contents

Introduction

A new phishing site pops up targeting your online banking customers. Many of the end users who land on the page won't realize they're about to disclose their login or payment card information and help fraudsters conduct both online and cross-channel fraud.

In fact, the speed of success is staggering. It only takes about 82 seconds from when a phishing attack is launched for the first person to become a victim.[1] PhishMe found in its surveys that people clicked on phishing links for a variety of reasons, with curiosity, fear and urgency serving as the leading causes.[2]

Fraudsters know that it is only a matter of time from when their phishing sites are detected to when they are blocked, so the duration of attacks has decreased. Typically, a phishing site remains active for an average of 15 hours, highlighting the efficiency and effectiveness of these nefarious campaigns.[3]

Moreover, fraudsters maintain a keen watch on the market to learn how their sites are detected, and then quickly change their tactics so they can bypass phishing detection altogether.

As a result, the year 2016 saw on average more than 400,000 phishing sites each month, and more than 13,000 new phishing sites appearing daily.[4] An average of 85 percent of organizations have experienced phishing attacks, many of which are highly sophisticated and were personalized to their targets.[5]

If you're like most financial organizations, you probably believe there's no easy way to stop an end user from accessing a phishing site, and that there's no easy way to keep pace with the growing number of phishing attacks against your organization.

But that's no longer true.

How can you better prevent financial fraud due to phishing attacks?

The answer lies in your organization's ability to protect your end users at the moment they're most vulnerable—when they're about to disclose their credentials or payment card data.

In this whitepaper, you'll learn how client-side phishing protections combined with new advanced phishing detection capabilities offer an adaptive approach that can help your organization better prevent phishing success, even as phishing tactics continue to evolve.

Using a cognitive approach to phishing detection and protection

In the past decade, phishing has undergone a radical transformation that has helped fuel its continued success and enabled fraudsters to compromise online banking accounts and conduct financial fraud.

Unprecedented sophistication in email content, advanced tactics and compelling lures have helped give phishing campaigns tremendous credibility, and enabled fraudsters to trick even the savviest end users.

Additionally, fraudsters have developed many different approaches to help drive their success. For example, one common brute force technique that fraudsters use is to compromise thousands of systems to host a phishing site. They will typically only launch a select few at any given time, and then regularly switch sites—creating a virtual cat-and-mouse game for anti-phishing investigators. Not only can the fraudsters constantly change sites, they can rapidly change the DNS and IP addresses of those sites to help create confusion.

In its trends report for the second quarter of 2016, APWG reported a continued increase in the number of phishing emails and phishing sites.[6]

Clearly, the challenge is only growing. So how can you keep up?

IBM is tackling the challenge head on by using patented machine learning and advanced analytics for phishing detection.

These advanced phishing detection capabilities use machine learning to analyze unstructured website data—including links, images, forms, text, scripts, DOM (document object model) data, URLs and more. Coupling these new capabilities with IBM® Trusteer® robust analytics and other global security intelligence data can help financial institutions protect their customers at a speed and scale like never before.

Sophisticated algorithms intelligently evaluate different variables and generate a highly accurate threat score that separates legitimate sites from phishing sites.

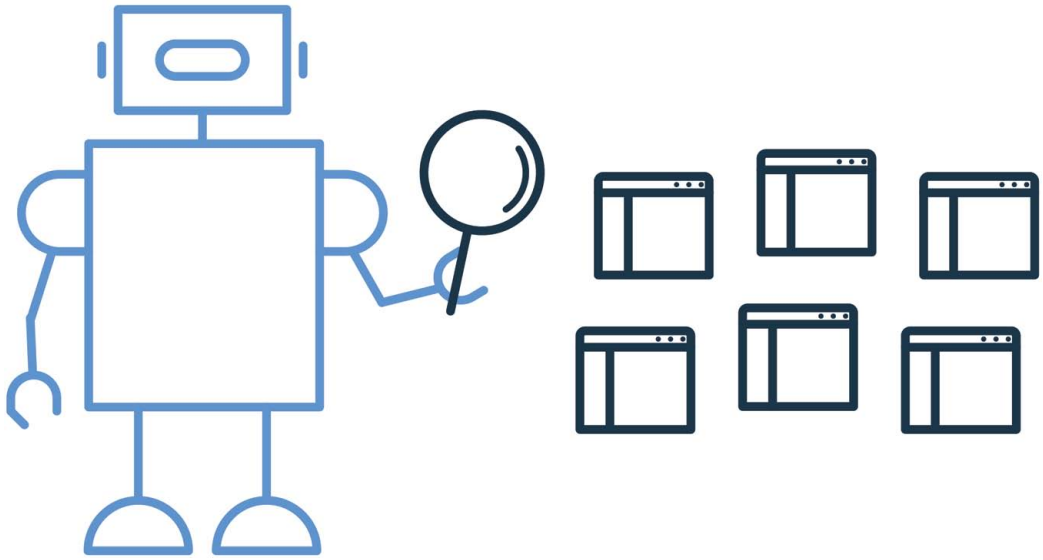
As a result, these advanced phishing detection capabilities offer a huge leap forward in the speed of phishing detection and help organizations rapidly adapt as new phishing tactics are introduced.

For example, this approach can rapidly detect new phishing trends, such as "image-based phishing," that many traditional tools might not detect. With image-based phishing, fraudsters create a screenshot of a targeted online banking site, just adding the text and forms required for end users to provide their login credentials or credit card information.

Preventing and adapting to new phishing tactics

Detecting new fraudulent online banking sites is only half the battle. Once identified, how do you prevent your end users from inputting their login credentials onto the site? No matter how knowledgeable end users are, they are human and they make mistakes.

Detect



Machine learning and advanced analytics help identify phishing sites at a speed and scale like never before.

Many financial institutions today use anti-phishing services to detect and shut down phishing sites. However, due to the nature of these attacks, the fraudsters launching the sites know detection is imminent and are strengthening their attack methods.

This gap in time from when an anti-phishing service detects a phishing site to when it can block it is one of the reasons that phishing remains a well-used and successful attack method.

The IBM Trusteer Rapport® solution offers a different approach—one that is designed to protect banking customers from phishing attacks when they navigate to a phishing site.

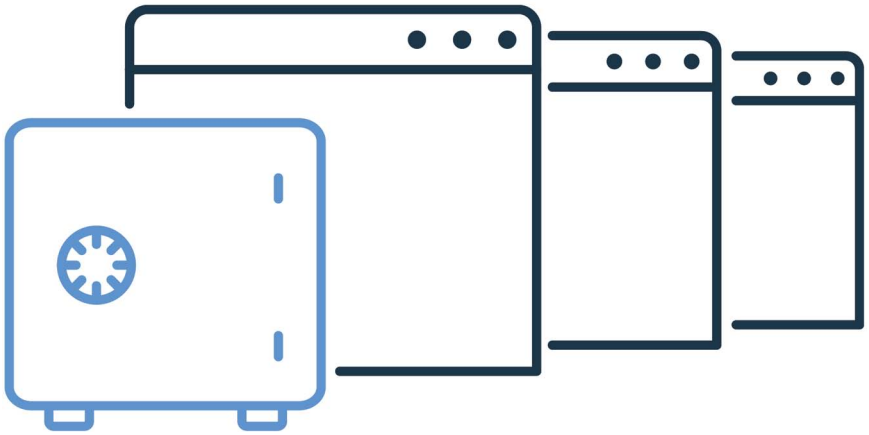
It's an important distinction, and one that can help financial institutions reduce the cost of phishing attacks, which Ponemon Institute estimates at nearly USD3.7 million per attack for the average 10,000 employee company.[7]

As an end user navigates to a website, the Trusteer Rapport solution identifies suspicious sites and uses machine learning and advanced analytics to provide near-real-time analysis of the site. If it confirms the site is a phishing site, the solution can notify or block the end user. By alerting the end user of a phishing attempt, the Trusteer Rapport solution can help prevent the theft of end user credentials and payment card data, and help stop the subsequent fraud that follows.

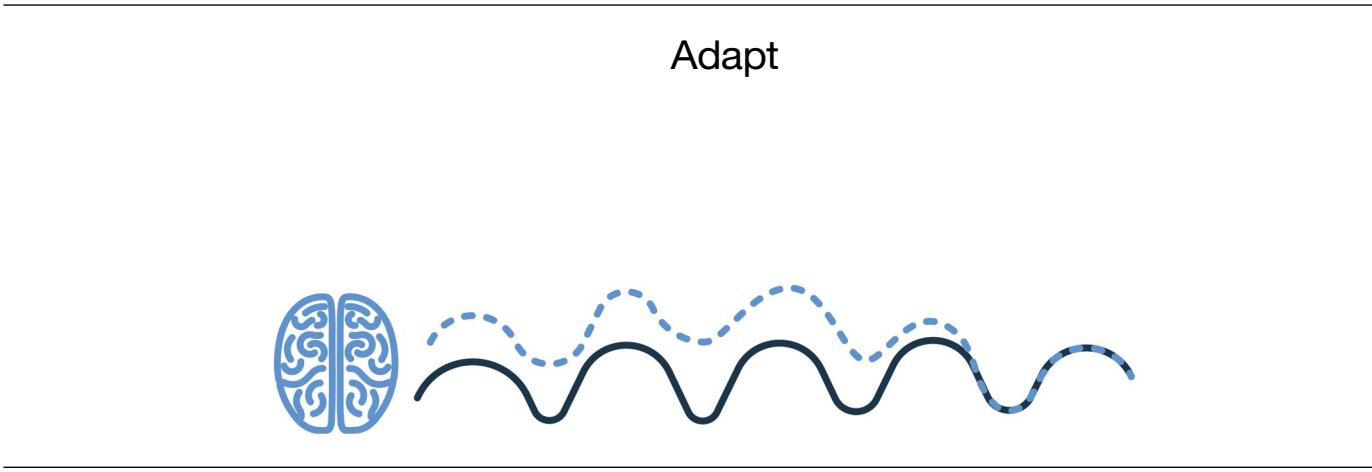
Because the Trusteer Rapport solution resides on the endpoint, it acts as a private security guard for end users—blocking malware threats and preventing end users from accessing identified phishing sites.

Using the threat intelligence generated via IBM's advanced phishing detection capabilities as well as by IBM security experts, the platform continuously adapts to evolving phishing threats.

Prevent



Trusteer Rapport helps prevent end users from accessing known phishing sites.



Protections are rapidly adapted as new phishing tactics are introduced.

From the end user's perspective, the solution can be easily downloaded and respects their privacy—so they can easily go about their online activity, knowing their protected.

Conclusion

A new phishing site just popped up online targeting your online banking customers. Many of your end users who land on the page won't realize they're about to disclose their login or payment card information to fraudsters.

With traditional approaches, you likely won't be able to shut down the site before many of your customers disclose their credentials.

By combining advanced phishing detection capabilities with client-based fraud protection, IBM offers a huge leap forward in the speed and accuracy of phishing detection.

IBM's approach provides rapid protections for end users who have the Trusteer Rapport solution installed on their devices, so they're protected when they're most vulnerable and before the phishing site is shut down.

In addition, it continuously adapts so it can detect when fraudsters change their strategy and techniques, and adjust protections accordingly.

With IBM, there's an easier, faster and effective way to combat financial fraud due to phishing.

IBM Trusteer Rapport—Highlights

 Compact software agent for PC and Mac	• One click web-based deployment • No hardware to install • Minimal impact on end-user's machine
 Malware protection	• Helps protect user credentials & website interactions transparently • Helps prevent malware infections from malicious sites • Removes existing infections, upon installation • Alerts security teams of malware infections
 Phishing protection	• Alerts user & security teams of potentials phishing sites and credentials loss • Blocks access to known phishing sites
 Adaptive protection	• Gathers intelligence from hundreds of millions of endpoints • Adapts protection automatically, without customer interaction

For more information

To learn more about transforming your approach to phishing detection and protection, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/trusteer

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

Please Recycle

[1] Marlo Aguilar, "The Number of People Who Fall for Phishing Emails Is Staggering," Gizmodo, April 14, 2015. Retrieved from: http://gizmodo.com/the-number-of-people-who-fall-for-phishing-emails-is-st-1697725476

[2] Steve Zurier, "91% of Cyberattacks Start With A Phishing Email," Dark Reading, December 13, 2016. Retrieved from: http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704?_mc=NL_DR_EDT_DR_daily_20161214&cid=NL_DR_EDT_DR_daily_20161214&elqTrackId=a66534266dff45aea858b9f0a66ad75b&elq=f95350c3de284618b8c9ab9f4f4257c8&elqaid=75468&elqat=1&elqCampaignId=24738

[3] Marika Samarati, "4 eye-opening facts about phishing," IT Governance (Blog), December 14, 2016. Retrieved from: http://www.itgovernance.co.uk/blog/4-eye-opening-facts-about-phishing/

[4] Tara Seals, "84% of Phishing Sites Last for Less Than 24 Hours," Infosecurity Magazine, December 12, 2016. Retrieved from: http://www.infosecurity-magazine.com/news/84-of-phishing-sites-last-for-less/

[5] Jonathan Crowe, "Phishing by the Numbers: Must-Know Phishing Statistics 2016," (Blog). Retrieved from: https://blog.barkly.com/phishing-statistics-2016

[6] APWG. (October 3, 2016). APWG Phishing Trends Activity Report: 2nd Quarter 2016 [Trend Report]. Retrieved from: https://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

[7] Maria Korolov, "Phishing is a $3.7-million annual cost for average large company," CSO Online, August 26, 2015. Retrieved from: http://www.csoonline.com/article/2975807/cyber-attacks-espionage/phishing-is-a-37-million-annual-cost-for-average-large-company.html

WGW03271-USEN-01