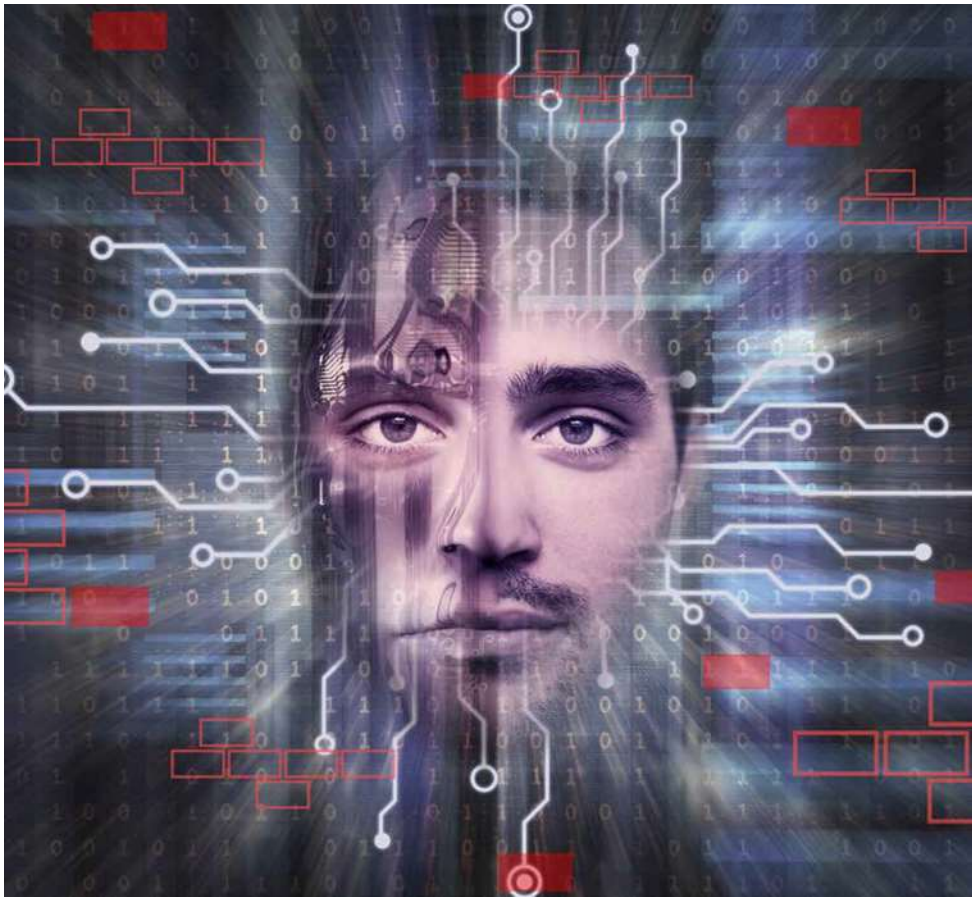
CYBERCRIME 2015

An Inside Look at the Changing Threat Landscape



RSA® Research remains at the forefront of threat detection and cybercrime intelligence, protecting global organizations with the shutdown of over a million cybercrime attacks. Based on its insight into cybercriminal activity, recovery of over a million actionable findings in 2014 and analysis of around 400,000 unique malware variants each week, RSA Research has identified the top cybercrime trends it expects to see evolving over the coming year.

April 2015

RSA WHITE PAPER

Copyright © 2015 EMC Corporation. All Rights Reserved.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided "as is." EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

EMC^2, EMC, the EMC logo, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is a registered trademark or trademark of VMware, Inc., in the United States and other jurisdictions. ©Copyright 2015 EMC Corporation. All rights reserved. Published in the USA 04/15 Cybercrime Trends White Paper H14146

TABLE OF CONTENTS

CYBERCRIME 2015: AN INSIDE LOOK AT THE CHANGING THREAT LANDSCAPE

CYBERCRIME TRENDS 2015

TREND#1
THE CYBERCRIME-AS-A-SERVICE MARKETPLACE CONTINUES TO MATURE

TREND#2
MOBILE PROVIDES A LARGER ATTACK SURFACE

TREND#3
CYBERCRIMINALS SEEK MORE BANG FOR THE BUCK AND INCREASE LARGE-SCALE RETAIL AND FINANCIAL ATTACKS

TREND#4
THREATS CONTINUE TO GROW MORE TARGETED AND MORE ADVANCED

The cybercrime landscape continues to evolve as criminals look to adopt more efficient and profitable attack tactics. At the same time, the market for cybercrime-as-a-service is advancing rapidly, with competition among malware vendors leading to increased innovation. And as smartphone penetration reaches record levels globally, cybercriminals are starting to switch their focus to standalone attacks on mobile devices.

RSA Research remains at the forefront of threat detection and cybercrime intelligence, protecting global organizations with the shutdown of over a million cybercrime attacks. In 2014 the RSA Anti-Fraud Command Center identified nearly 500,000 cyberattacks – an 11% increase year over year.

Based on its insight into cybercriminal activity, recovery of over a million actionable findings in 2014 and analysis of around 400,000 unique malware variants each week, RSA Research has identified the top cybercrime trends it expects to see evolving over the coming year.

TREND#1: THE CYBERCRIME-AS-A-SERVICE MARKETPLACE CONTINUES TO MATURE

The criminal underworld continues to develop its as-a-service model, enabling more fraudsters to cash in without needing to understand the chain of fraud, how to phish or spam, or the IT infrastructure requirements. It's a trend we observed last year that shows no sign of abating. In fact, the marketplace is growing so fast that it's becoming fiercely competitive and cybercrime 'service providers' must work harder than ever before to win and keep 'customers.’

Cybercrime-as-a-service providers are therefore focused on delivering great customer service and innovative products. Examples include 'try before you buy' options and money-back guarantees for fraud services. Similarly, when it comes to the #1 commodity in the marketplace — stolen credit cards — vendors are offering more choices to attract and retain customers. For example:

- Replacement of ‘damaged’ goods. If a purchased payment card has been canceled by the victim, the buyer will get a replacement or refund.
- Mobile apps that make the purchase of compromised payment cards all the more convenient on buyers' mobile phones.

The other outcome of strong competition in the marketplace is innovation, as providers and vendors try to stand out from the crowd by offering more advanced, differentiated and stealthier services and to earn more revenues from the expertise they offer to accompany these services. This is critical, as many types of attack are fundamentally simple and low cost, such as phishing attacks, where 500,000 email addresses can cost as little as $30, hosting a phishing site can be more or less free, and thousands of credit cards can be stolen in return for around $100.

One example of innovation we've seen recently is providers capitalizing on the increasing popularity of ransomware. They're attempting to differentiate their offerings with more sophisticated capabilities, such as enabling interaction with the victim, or providing control panel options for extending the lock period.

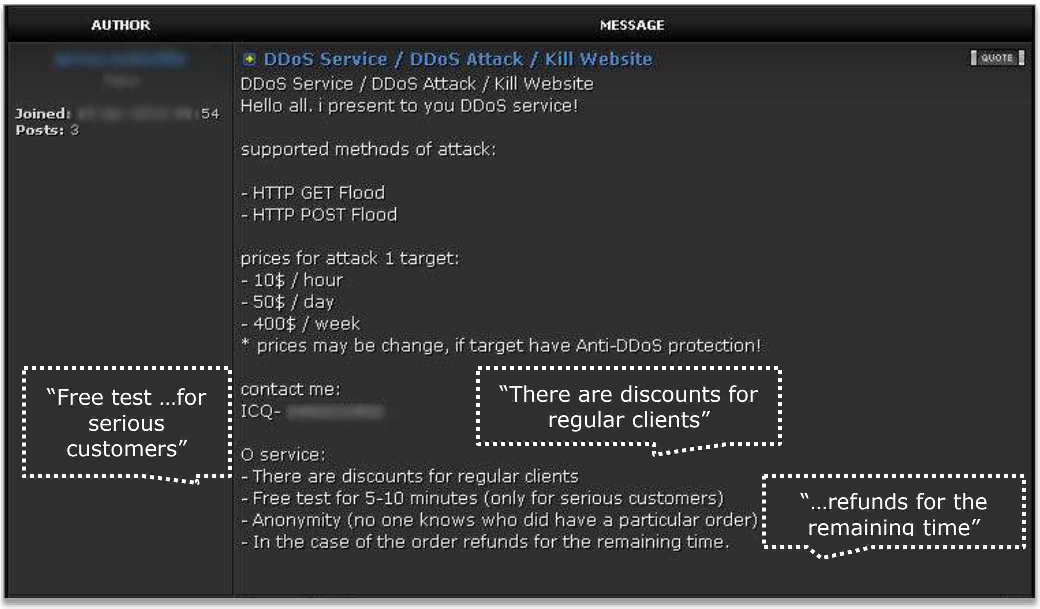
2015 OUTLOOK: CYBERCRIME-AS-A-SERVICE

The cybercrime marketplace has evolved tremendously over the past two years and that evolution looks set to continue through 2015 and beyond.

Innovation among cybercrime-as-a-service providers will continue to be driven by a competitive marketplace, leading to a generalized increase in the quality of malware produced, and enabling a much larger pool of bad actors with no technical knowledge to profit from cybercrime.

In contrast, providers of poor-quality malware soon lose their reputation and get kicked off the marketplace forums — especially now that forums increasingly enable buyers to rate sellers and their services, leave comments and report 'rippers,’ or vendors who rip their customers off.

The upshot is that the quality of malware is rising as vendors compete hard to keep existing customers and win



[redacted]
Joined: [redacted]:54
Posts: 3

DDoS Service / DDoS Attack / Kill Website

DDoS Service / DDoS Attack / Kill Website
Hello all. i present to you DDoS service!

supported methods of attack:

- HTTP GET Flood
- HTTP POST Flood

prices for attack 1 target:
- 10$ / hour
- 50$ / day
- 400$ / week
* prices may be change, if target have Anti-DDoS protection!

contact me:
ICQ- [redacted]

O service:
- There are discounts for regular clients
- Free test for 5-10 minutes (only for serious customers)
- Anonymity (no one knows who did have a particular order)
- In the case of the order refunds for the remaining time.

"Free test …for serious customers"

"There are discounts for regular clients"

"…refunds for the remaining time"

TREND#2: MOBILE PROVIDES A LARGER ATTACK SURFACE

In 2013, when the worldwide smartphone market reached over a billion units shipped in a single year for the first time[1], mobile malware started to become a serious issue. Last year, 1.3 billion smartphones were shipped, and 1.5 billion units are forecast for 2015.[2]

As well as adapting to the demands of the criminal marketplace, it's well known that criminals also adapt quickly to the evolving technology landscape. Given the rate of smartphone adoption around the world, we're seeing more focus on mobile threats and fraud than ever before.

The vast majority of mobile malware is still focused on the Android platform. Not only is it an open platform, but Android phones tend to be manufactured and distributed using less tightly controlled supply chains than, say, Apple's. And because Android is the most widely used platform, there's a big attack surface to exploit.

Banking Trojans, used with SMS sniffers on mobiles, have seen increased adoption over the past couple of years. In this scenario, a user is persuaded through social engineering to download mobile malware from their PC. For example, during an online banking session, a screen will pop up inviting the user to download a mobile app, often masquerading as a security feature, which is actually an SMS sniffer. When the user's bank detects an unusual activity, such as a high-value wire transfer, and sends an out-of-band one-time password to the user's mobile that must be entered to authorize the transaction, the criminal can intercept it and complete the transfer to their own account.

During 2014, however, we started to see more mobile-only attack vectors, which don't require the victim's PC to be infected. These include:

- Premium rate scams. Scammers persuade the user to send SMSs or make calls to premium-rate numbers from their mobile, with the scammers collecting the cash that results.

- Data stealers and spying apps. These apps switch on a phone's camera or audio, so that a criminal can watch the user's face to see whether he or she is being convinced by a social engineering attempt; or record what the user says during calls to their bank. They can also steal address book data, lift photos from the phone and get the device's geo location.

[1] IDC Worldwide Quarterly Mobile Phone Tracker
[2] IDC Worldwide Smart Phone 2015-2019 Forecast and Analysis

2015 OUTLOOK: MOBILE THREATS

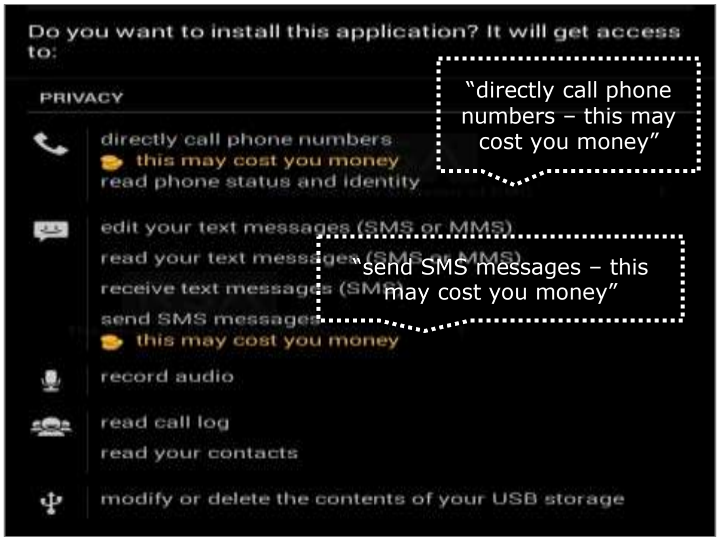
In 2014 the volume of mobile malware and rogue mobile apps increased and we expect to see the same thing happening in 2015. Today, about half the world's adult population owns a smartphone: they're becoming the go-to device over the computer, and the one to which we're always connected.

Cybercriminals will increasingly look to exploit this change in user device preference by switching an expanding proportion of their attacks to mobiles. So we expect to see more standalone attacks on mobile devices over the coming year. In addition, we expect to see attacks against mobile payment systems, such as Apple Pay, in 2015, as their popularity looks set to take off.

The Android platform will once again to bear the brunt of attacks, as it continues to maintain its very high market share of approximately 79%, with iOS grabbing around 15%, and the remaining 5% being split among other platforms, including Windows.[4] Not only does Apple iOS have a much smaller market share than Android, attacking iOS requires very advanced skills. However, we are already starting to see a few attacks that target both iOS and the Windows platform.

[4] IDC Worldwide Quarterly Mobile Phone Tracker

Strictly speaking, many of these attacks are initiated by rogue mobile apps rather than malware, as they misuse trust to steal information and money by persuading users to give them permissions during the installation process. Many users simply click 'Next' without reading each screen, and fail to notice, for example, that the app has gained super-user privileges which provide full access to the phone's features and may even make the app impossible to uninstall.



Do you want to install this application? It will get access to:

PRIVACY

directly call phone numbers
this may cost you money
read phone status and identity

edit your text messages (SMS or MMS)
read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
this may cost you money

record audio

read call log
read your contacts

modify or delete the contents of your USB storage

"directly call phone numbers – this may cost you money"

"send SMS messages – this may cost you money"

Ransomware, such as Police Locker, which has recently jumped to mobile, takes advantage of this typical user behavior during installation to gain the privileges needed to lock the device. Just as with PC ransomware, the user will be instructed to pay a ransom to unlock their files (or to 'pay a fine' because the phone supposedly contains 'illegal content'). Ransoms generally have to be paid via an online payment system, such as Bitcoin, or prepaid cash cards — both of which are untraceable and non-reversible. A lot of victims do pay up, especially if they have no backup copies of the information stored on their phones, so criminals are making good money from ransomware.

TREND#3: CYBERCRIMINALS SEEK MORE BANG FOR THE BUCK AND INCREASE LARGE-SCALE RETAIL AND FINANCIAL ATTACKS

2015 OUTLOOK: EVOLVING THREAT TACTICS

The hacking of POS devices has shifted rapidly from being a premium attack to a commodity. Some vendors in the criminal marketplace even offer POS malware for free when they're starting out and want to build their reputation. The barriers to entry are low and some old code is even free, so almost anyone who can code can produce this malware (and will continue to do so).

We expect to see more large-scale retail and banking breaches in 2015, as cybercriminals seek more efficient and profitable types of attack.

During 2014 RSA observed a number of developments in attack tactics as cybercriminals looked for new ways to steal credit cards and gain fraudulent access to money. We also saw banking botnets become more resilient and, at the same time, observed a move away from attacks on individuals to mass attacks on retailers and financial institutions.

Banking Botnets

In 2014 we observed banking botnets becoming more resilient and harder to take down, with criminals using the deep web and untraceable peer-to-peer networks, such as TOR and I2P, to increase resilience and anonymity, and hide their infrastructure from law enforcement agencies

We also saw an increasing trend towards private botnets. Instead of being 'commercially available' on the criminal underground, some botnets are being written specifically for an individual gang, which makes them harder to trace and analyze. In some cases, these private botnets can also be hired as a 'premium service' — another example of how vendors in the criminal marketplace are attempting to differentiate the services they offer.

Large-scale Retail and Financial Breaches

A number of large-scale breaches that took place in 2014 show that criminals are looking for more efficient, less time-consuming and more profitable ways to steal a large number of credit cards or large sums of money.

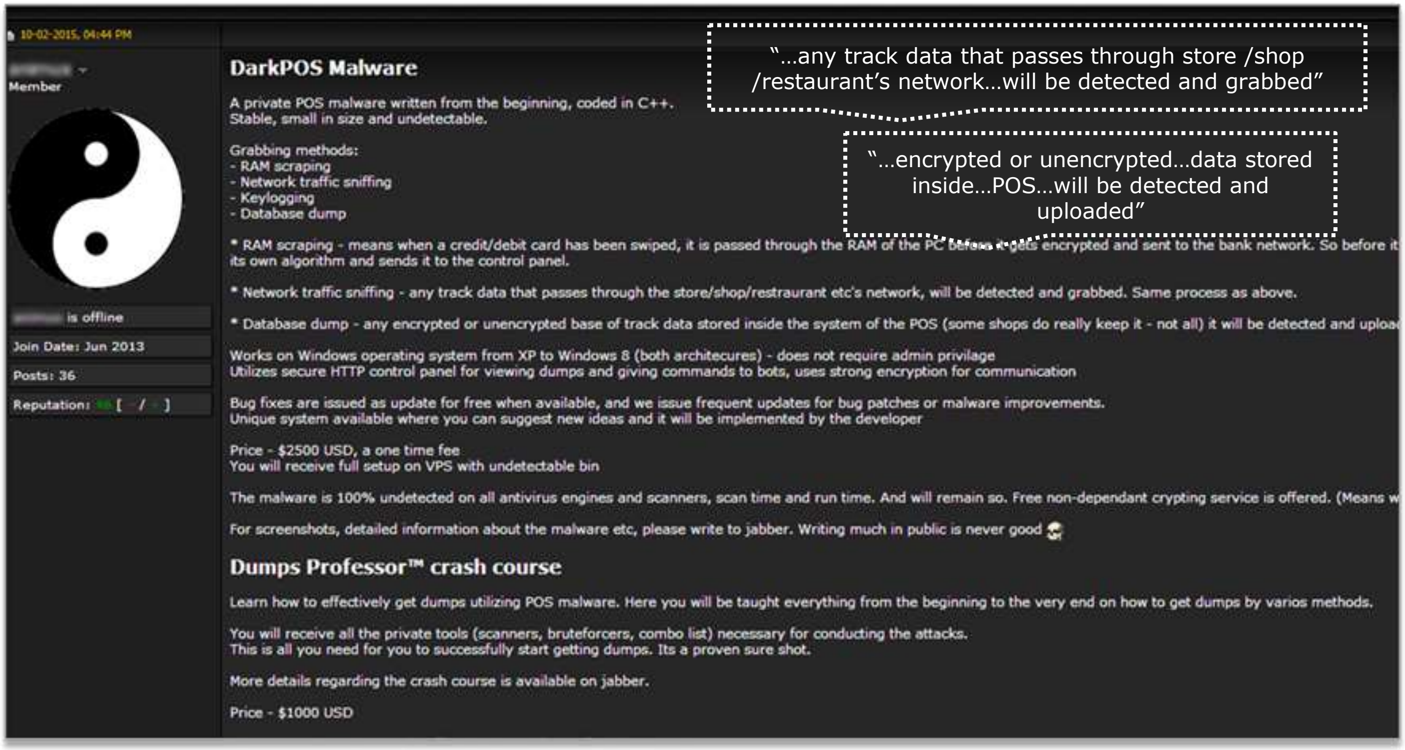
Instead of spending time phishing and using social engineering on individuals, cybercriminals are penetrating retailers’ systems and stealing data as the card is swiped. The most common type of point of sale (POS) malware used, RAM scrapers, tends to be a US phenomenon, because chip-and-pin cards aren't widely used in the United States.

Cybercriminals have been known to launch these attacks by penetrating insecure systems belonging to a third party in the retailer's supply chain. Another method we saw during 2014 was used in stores whose points of sale are under video surveillance. The criminal scans hosts for open ports which indicate a remote access connection to the POS (left open to enable easy access to check balances and so on) and IP video (which lets the attacker know where the cameras, and therefore the points of sale, are). Attackers will brute-force the remote access connection until they get in to the system, at which point they can install the POS malware and start stealing card details.

Attackers monetize the credit card details stolen during these large breaches in the usual way, either by selling the card details or using them to buy goods online which are then resold.

Fraudsters who attack financial institutions are targeting the corporate network and going straight to where the money or the information is. Some of these financially motivated attacks are on the same scale as APTs launched by nation states. Attack types include:

- Transferring cash from a bank's system to criminals' own accounts
- ATM attacks — directly cashing out an ATM
- Ransom requests — extorting money based on locking private information about a bank's customers



“…any track data that passes through store /shop /restaurant’s network…will be detected and grabbed”

“…encrypted or unencrypted…data stored inside…POS…will be detected and uploaded”

10-02-2015, 04:44 PM

[redacted]
Member

[redacted] is offline

Join Date: Jun 2013

Posts: 36

Reputation: [redacted] [[redacted] / [redacted]]

DarkPOS Malware

A private POS malware written from the beginning, coded in C++.
Stable, small in size and undetectable.

Grabbing methods:
- RAM scraping
- Network traffic sniffing
- Keylogging
- Database dump

* RAM scraping - means when a credit/debit card has been swiped, it is passed through the RAM of the PC before it gets encrypted and sent to the bank network. So before it
its own algorithm and sends it to the control panel.

* Network traffic sniffing - any track data that passes through the store/shop/restraurant etc's network, will be detected and grabbed. Same process as above.

* Database dump - any encrypted or unencrypted base of track data stored inside the system of the POS (some shops do really keep it - not all) it will be detected and uploa

Works on Windows operating system from XP to Windows 8 (both architecures) - does not require admin privilage
Utilizes secure HTTP control panel for viewing dumps and giving commands to bots, uses strong encryption for communication

Bug fixes are issued as update for free when available, and we issue frequent updates for bug patches or malware improvements.
Unique system available where you can suggest new ideas and it will be implemented by the developer

Price - $2500 USD, a one time fee
You will receive full setup on VPS with undetectable bin

The malware is 100% undetected on all antivirus engines and scanners, scan time and run time. And will remain so. Free non-dependant crypting service is offered. (Means w

For screenshots, detailed information about the malware etc, please write to jabber. Writing much in public is never good

Dumps Professor™ crash course

Learn how to effectively get dumps utilizing POS malware. Here you will be taught everything from the beginning to the very end on how to get dumps by varios methods.

You will receive all the private tools (scanners, bruteforcers, combo list) necessary for conducting the attacks.
This is all you need for you to successfully start getting dumps. Its a proven sure shot.

More details regarding the crash course is available on jabber.

Price - $1000 USD

TREND#4: THREATS CONTINUE TO GROW MORE TARGETED AND MORE ADVANCED

2015 OUTLOOK: TARGETED AND ADVANCED THREATS

APTs and similar attacks by nation states are likely to ramp up in 2015, with regional conflicts driving the perpetrators and their victim selection.

Criminal groups will also continue to adopt nation-state tactics. Large enterprises and other organizations will still be vulnerable through their use of commodity equipment, which attackers quickly learn how to bypass, so defending against these attacks will still be challenging.

In the past, Advanced Persistent Threats (APTs) and other similar advanced attacks centered mainly on spear phishing, in which individuals in an organization are targeted with documents containing malicious Trojans. Once downloaded by the unsuspecting employee, the Trojans allow the attacker to establish a foothold in the network. Now, however, we're seeing a migration towards watering-hole attacks, in which the criminal compromises an organization that's of business interest to the primary target organization. This makes individual phishing attempts more convincing and increases the likelihood of introducing malware into the target organization's systems.

For example, an attacker could steal personal information from a healthcare organization, and use it to send the target organization's employees more personalized emails and links. The level of personalization — such as including a relevant health condition or medical practitioner's name — will make it more likely an employee will click on a link and so unwittingly download the Trojan.

Where we expect to see continued improvement, however, is in the detection of these advanced attacks, which will be helped in part by improved intelligence gathering and increased sharing of intelligence — an approach that RSA has long championed. We note, for example, that Facebook has launched an intelligence-sharing platform. And during his State of the Union address in January 2015, President Obama spoke about the critical role of intelligence in combating cyber threats and the need for legislation in this area, saying:

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids.

So we're making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism… I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyberattacks, combat identity theft, and protect our children's information."[3]

[3] President Obama's State of the Union Address 2015

AN INTELLIGENCE-DRIVEN, RISK-BASED APPROACH COMBATS CYBERTHREATS ACROSS MULTIPLE CHANNELS

Organizations are challenged on many fronts in their efforts to protect themselves, and their customers, partners and suppliers, from cyberthreats. Through constant innovation, cybercriminals are developing increasingly sophisticated malware and rogue mobile apps and more resilient botnets. And with the rapidly expanding cybercrime-as-a-service marketplace, all these products are becoming much more widely available — and more exploitable by criminals with little or no technical knowledge.

Advanced threats continue to evolve, too, with watering-hole attacks helping to make them more efficient and successful; and criminal gangs increasingly adopting APT-type techniques that were previously the preserve of nation states.

To combat these trends, organizations and law enforcement agencies are tending to favor intelligence-driven security and fraud prevention approaches which can operate in mobile and cloud environments, make greater use of behavioral analytics, and take advantage of smart device capabilities to protect users and data. Even if attacks can't be blocked completely, having access to the right intelligence makes it possible to detect an attack more quickly, significantly reducing the attacker's window of opportunity and minimizing the potential for loss or damage.

An intelligence-driven approach provides a layered security model that protects identities and assets across multiple channels, while providing three essential attributes that enable a balance to be struck between risk, costs, and end-user convenience:

- Immediate external visibility and context into cybercrime threats across all online and digital channels
- Extended analysis capabilities, enabling detection of anomalies that indicate threats based on an organization's unique risk profile, and immediate assessment of which threats are the most damaging
- Designation of the right corrective action to mitigate the specific threat at hand, quickly and efficiently

Criminals have long shared their knowledge and expertise in order to drive their success, and defenders must take the same approach — after all, a team is stronger than the individuals in it. RSA is pleased to note a generally increased propensity to share intelligence about threats and attacks with peers, government agencies and the security industry, in order to increase knowledge across the board.

The security industry continues to press for more open sharing of the intelligence which is critical to driving improvements in best-practice approaches to combating cybercrime and cyber threats. In February 2015, President Obama signed an Executive Order relating to cyber security; and in March 2015 the leaders of the House of Representatives Intelligence Committee introduced legislation to make it easier for companies to share information about cyber security threats with the government, without fear of being sued.

These are significant steps which encourage us to believe that a scenario in which threat intelligence is shared openly in the fight against cybercrime is closer to becoming a reality.