THE CURRENT STATE OF CYBERCRIME 2014: GLOBAL MALWARE OUTLOOK

April 2014

APT ATTACKS REMAIN UNABATED AND POS MALWARE ATTACKS BECOME COMMON

Cybercriminals are finding sophisticated new ways to make botnets stealthier and more durable, and to shield the data stolen during attacks. At the same time, they're also generating significant returns from unsophisticated hit-and-run POS malware attacks. Cyber-espionage attacks continue to occur with tactics that are largely unchanged and new players in the space being identified.

Stealthier, more durable botnets

Botnets are used by fraudsters, cybercriminals and hacktivists to host their infrastructure and launch attacks such as DDoS to bring down the websites of banks, government agencies and other high-profile organizations. The large number of zombie computers in a typical botnet means an attack will move around, making it difficult to find the source and shut the attack down. Even so, cybercriminals are developing even more robust botnets that can remain active for longer before being discovered.

- Botnets are being created that behave as similarly as possible to legitimate software and take considerable time and effort to detect. This has changed the way defenders focus their efforts, such as detecting when an infected computer communicates with a domain that's been used for cybercrime in the past.
- Hosting a botnet's command-and-control center in a Tor-based network (where each node adds a layer of encryption as traffic passes) obfuscates the server's location and makes it much harder to take it down.

– Cybercriminals are building more resilient peer-to-peer botnets, populated by bots that talk to each other, with no central control point. If one bot (or peer) in a peer-to-peer botnet goes down, another will take over, extending the life of the botnet using business continuity techniques.

– An alternative business continuity–led approach involves controlling a botnet from a mobile device using SMS messages. For example, some have speculated that the cyber attack on South Korean banks in early 2013 may have been a multi-vector attack that involved Android phones located in China, Korea or both[1]. With this type of botnet, if the primary command-and-control center gets shut down, the cybercriminal can redirect the botnet to an alternative center via SMS.

Attackers shield stolen data

The cybercrime world is like an arms race: cybercriminals pursue a course of action until the defenders work out how to combat it, at which point the cybercriminals change tack. An example of this is the use of password-protected zip files by APT attackers to exfiltrate stolen data. The challenge for the defender is to crack the password on the zip file to see what was taken. Because attackers tend to work from a script or within a structured framework, they will often reuse a password, enabling the defender to link attacks and open subsequent zip files with ease.

Once the attacker realizes they've been rumbled, they'll change something about their process in order to regain the upper hand — for example, switching from zip files to rar files (which are more difficult to crack), or using asymmetric encryption algorithms that are harder for defenders to reverse engineer. This results in the defender losing the ability to identify the stolen data and establish relationships between attacks, until he or she manages to crack the next one.

Cyber espionage attacks

Cyber espionage attacks have continued unabated in the last, with attack methodology largely centering around spear phishing attacks, in which specific internal personnel are targeted with documents containing malicious Trojans to allow the attacker to establish a foothold in the network. Also popular last year were "Watering Hole[2]" attacks, or strategic web compromise, in which the attacker compromises a website that is of business interest to a target and uses it as an exploit platform to intrude into the target network. Attacker malware varies in sophistication, but simple methods continue to be successful for the most part.

While the frequency of reported incidents appears to have increased, this is likely due to a move towards intelligence-driven detection, rather than an actual increase in attacks. Additionally, new nation-state players such as the "Hangover" campaign[3] out of India and the "Snake" campaign[4] in Russia have made recent headlines and caused a shift in viewing cyber espionage as a threat originating from specific regions to a more global one.

Hit-and-run POS malware attacks

Hit-and-run attacks are carried out against retailers using point-of-sale (POS) malware, much of which is based on the free-to-use leaked code for Dexter and Alina malware. ChewBacca, which was uncovered by RSA in January 2014, and BlackPOS are other well-known examples of POS malware. This type of malware infects POS terminals, scraping the terminals' memory for the payment card and personal data — customers' names, card numbers, expiration dates and card verification value (CVV) information — that can be used to clone cards.

---

1 Source: RSA Firstwatch blog "Tales From the Darkside: Mobile Malware Brings Down Korean Banks", March 2013 (https://community.emc.com/community/connect/rsaxchange/netwitness/blog/2013/03/21/tales-from-the-darkside-mobile-malware-brings-down-korean-banks)

2 https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/

3 http://normanshark.com/wp-content/uploads/2013/08/NS-Unveiling-an-Indian-Cyberattack-Infrastructure_FINAL_Web.pdf

4 http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

POS malware does this by searching for simple regular expressions for card magnetic stripe data. When a card number is found, it is extracted and logged. Even when a retailer is compliant with PCI DSS, unless data is encrypted or tokenized at the moment of capture at the POS terminal, there's a short window of opportunity during which it can be stolen in readable form.

This type of POS malware was used during the very high-profile attack against several large retailers late last year that affected tens of millions of card holders. The cost to financial institutions has so far been estimated at over $200m, and that only takes into consideration expenses for actions such as notification and card reissuance. That still does not account for fraudulent purchases making it a figure that is likely to increase in the long term. These attacks have mainly been confined to countries such as the U.S., where EMV technology is not yet in widespread use.

Referral abuse malware

Some common breeds of malware were on the rise for inciting referral abuse in 2013. The malware is custom-designed to target corporations that pay cash to affiliate referrers for each installation of the target's software. This type of customized malware is written specifically to install software on a victim PC under a referrer's identity, make the infected machine click on ads that pay pennies per click, and direct it to purchase "likes" on social media.

In August 2013, RSA Research discovered a variant of the Zbot Trojan being used in referral abuse[5]. The typical charter of Zbot has been to attempt to swipe passwords, but this variant was also programmed to check for availability of Instagram usernames – likely in an effort to create an army of fake Instagram users that can be sold as followers to help individual users or businesses create an image of popularity. The same Zbot variant was also capable of SEO poisoning to help boost keyword rankings, likely in an effort to push its own content to the top of search engine results. These rank-abuse promoted pages often contain malicious content to spread additional malware.

2014 OUTLOOK: Malware Continues to Spawn New Waves of Attacks

From POS malware to referral abuse, cybercriminals are continually in search of new approaches to monetize their bots. At the same time they seek to spawn new attacks, they are also creating more bulletproof infrastructure on the backend. They are moving their infrastructure to P2P and Tor-based networks to evade detection. They are changing the methods they use to mask stolen data, making it more difficult for researchers to reverse engineer and understand the methods being used behind prominent cyber attacks. Advancements in cybercrime technology and infrastructure will only continue. For example, given the computing power contained in a smartphone and criminals' willingness to adopt new technology, it is likely we will witness more mobile-phone-based botnets and command-and-control centers over the coming year.

Also, with the scale of several high-profile data breaches, we are likely to see a shift in the U.S. market towards adoption of EMV payment cards. It will be slow, but 2014 will be a pivotal year in making the move. Regulations such as PCI-DSS will be re-evaluated and lead to stricter guidance for retailers to implement encryption or tokenization at the point of sale. Until there is a major industry change, there is little reason to expect criminals to stop using POS malware–based attacks against retailers, given the enormous returns that are possible from this relatively unsophisticated, easy-to-obtain malware.

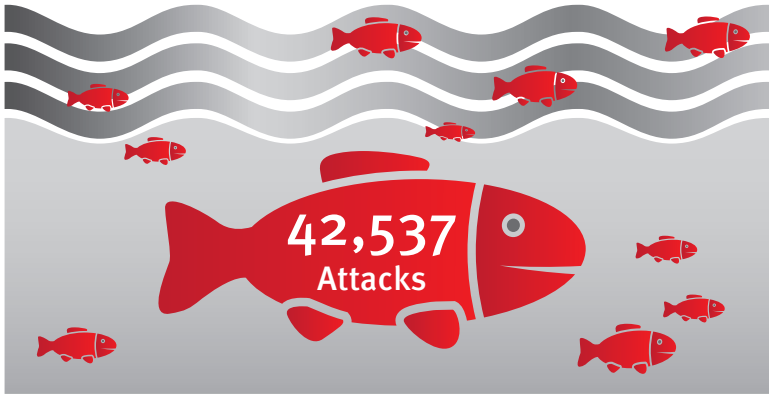
5 https://blogs.rsa.com/new-zbot-variant-builds-instagram-army/

APRIL 2014

Source: RSA Anti-Fraud Command Center

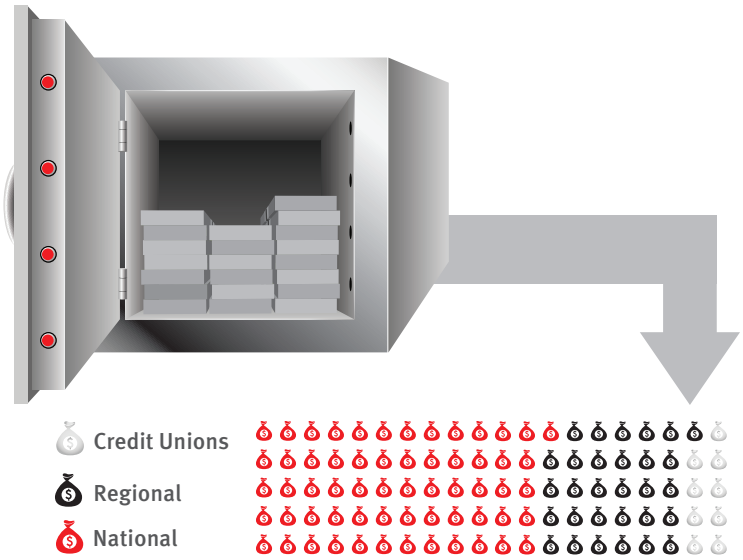
Phishing Attacks per Month

RSA identified 42,537 phishing attacks in March, marking a 15% increase from February's attack numbers. This also represents a 75% increase from the number of attacks a year ago.



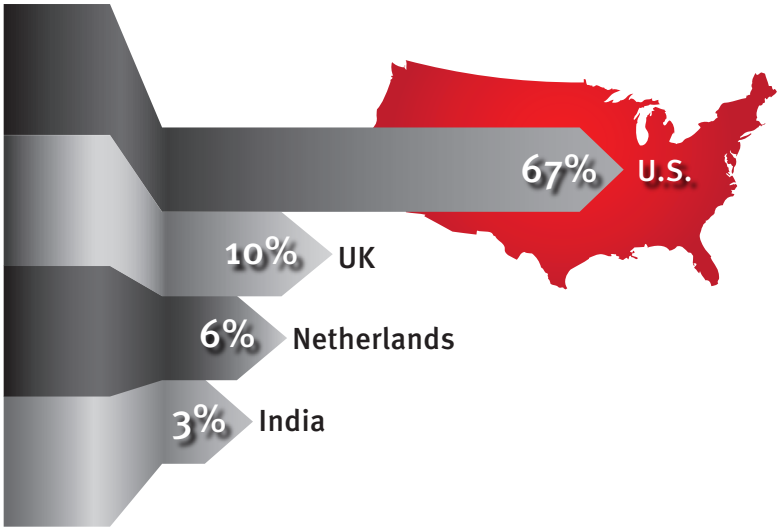
US Bank Types Attacked

Nationwide banks continued to be the most targeted by phishing with 61% of total volume in March, while regional banks saw a sharp spike in attacks – jumping from 5% to 30% compared to February.



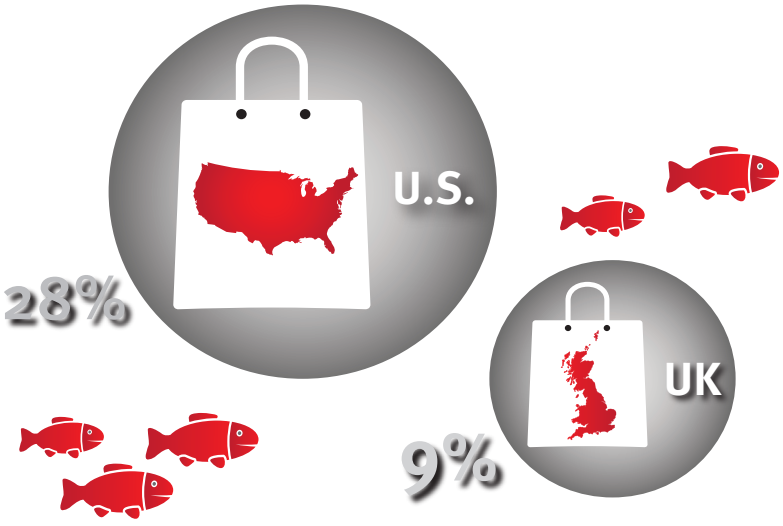
Top Countries by Attack Volume

The U.S. remained the most targeted country in March with an overwhelming 67% of global phishing volume, followed by the UK, the Netherlands, and India.



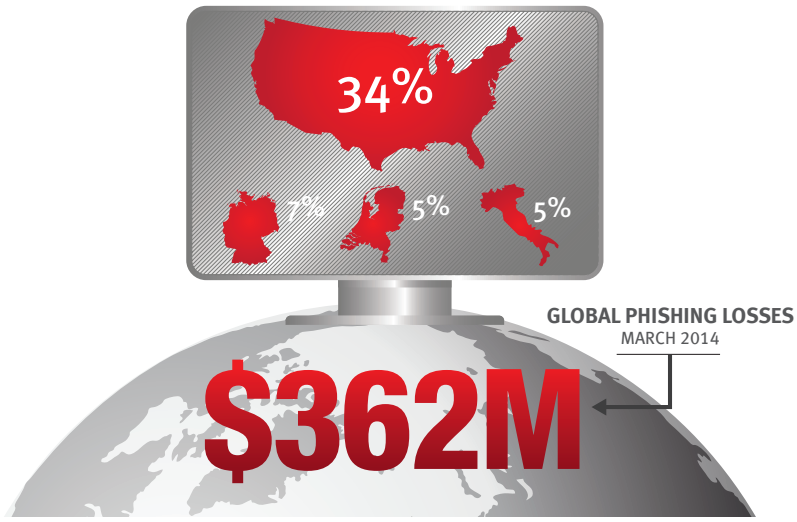
Top Countries by Attacked Brands

Over 50% of phishing attacks in March were targeted at brands in the U.S., UK, India, Australia and Canada.



Top Hosting Countries

The U.S. hosted 34% of global phishing attacks in March, followed by Germany, the Netherlands, Italy and Turkey.



CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.emc.com/rsa