THE INVISIBLE BECOMES VISIBLE
Trend Micro Security Predictions for 2015 and Beyond
A TrendLabs™ Report
TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.
PREDICTIONS

1. More cybercriminals will turn to darknets and exclusive-access forums to share and sell crimeware.

2. Increased cyber activity will translate to better, bigger, and more successful hacking tools and attempts.

3. Exploit kits will target Android, as mobile vulnerabilities play a bigger role in device infection.

4. Targeted attacks will become as prevalent as cybercrime.

5. New mobile payment methods will introduce new threats.

6. We will see more attempts to exploit vulnerabilities in open source apps.

7. Technological diversity will save IoE/IoT devices from mass attacks but the same won't be true for the data they process.

8. More severe online banking and other financially motivated threats will surface.
More cybercriminals will turn to darknets and exclusive-access forums to share and sell crimeware.
Several takedowns occurred this year, thanks to collaborative public-private partnerships and efforts. Trend Micro particularly aided in disrupting GameOver operations despite the malware’s resilience to takedown. We also provided threat intelligence and research findings to law enforcers, halting Citadel-related attacks against Japanese banks and contributing to the arrest of James Bayliss (Jam3s), Aleksandr Andreevich Panin (Gribodemon), and Hamza Bendelladj (bx1) who ran several SpyEye command-and-control (C&C) servers. These developments, however, will make anonymity a crucial requirement in committing cybercrime since security researchers and law enforcers now have quick access to the underground. Case in point—the celebrity photos tied to the iCloud hack that were first leaked on Reddit and 4chan ended up on the Deep Web as well.

Leveraging the Deep Web and darknet services or using untraceable and anonymous peer-to-peer (P2P) networks like Tor, I2P, and Freenet to exchange and sell tools and services is no longer new. We’ve seen cybercriminals use rogue top-level domains (TLDs) as alternative domains to further cloak underground markets like Silk Road, which was shut down by the Federal Bureau of Investigation (FBI) after two-and-a-half years of operation.

We’ve also seen cybercriminals adopt targeted attack techniques to better evade detection, just as we predicted in 2013. In Africa, this was manifested by the exploitation of vulnerabilities normally associated with targeted attacks via the distribution of typical cybercrime malware like ZeuS. Cybercriminals are also increasingly using remote access tools (RAT) like BlackShades in attacks.

It does not help that the prices of malicious wares in underground markets are decreasing as supplies increase. The average price of stolen U.S. credit card credentials has declined from US$3 in 2011 to US$1 in 2013. Compromised account credential prices have also dropped in the Russian underground. Stolen Facebook credentials that cost US$200 in 2011 only cost US$100 in 2013 while Gmail account credentials that were sold for US$117 in 2011 were only sold for US$100 in 2013. As more and more players enter the cybercriminal underground economy, ware prices will continue to decline. Before long, getting the greatest number of customers will depend on who can assure that buyers won’t be caught red-handed. Sellers will be pushed to go even deeper underground, particularly into the deep recesses of the Web.

As the bad guys move deeper into the Web, security firms and law enforcers need to extend their reach as well to cover the Deep Web and darknet services. This will require greater effort and investment. Public-private partnerships will be needed more than ever to disrupt and take down cybercriminal operations. Security firms should continue to provide threat intelligence to help law enforcers catch perpetrators. Lawmakers worldwide, meanwhile, need to agree on what constitutes cybercrime to aid enforcers, regardless of jurisdiction, to bring bad guys to justice.

A comparison of the prices of stolen credit card credentials from various countries in the Russian underground revealed a declining trend from 2011 to 2013.
Increased cyber activity will translate to better, bigger, and more successful hacking tools and attempts.
The constant growth of cyber activities worldwide means that individuals and organizations alike will continue to succumb to online threats and attacks. Cybercriminals will, however, set their sights on bigger targets rather than on individuals, as this translates to bigger gains.

We’ve seen cybercriminals use point-of-sale (PoS) RAM scrapers to steal millions of customer data records from some of the biggest retailers worldwide. Before 2013 ended, Target lost the credit card information of 70 million of its customers to cybercriminals in a PoS malware attack. Target wasn’t alone, however, as other organizations like P.F. Chang’s suffered the same fate. And months before 2014 is set to end, Home Depot took Target’s place as the biggest breach victim to date. The breached organizations lost customer data, which damaged their brands and cost them dearly.

Though majority of breaches result from external attacks, some, like the Amtrak breach, are caused by insider threats. Reports revealed that an Amtrak employee has been selling rail passengers’ personally identifiable information (PII) for two decades before getting found out.

That said, individuals and organizations alike will do well to assume that all of the data they reveal online will land in cybercriminals’ hands. We'll see two or more major data breach incidents each month. Banks and financial institutions, along with customer data holders, will always be attractive breach targets. As a result, we will continue to see changes in victims’ upper management every time they succumb to attacks.

So how should organizations and individuals respond? It’s best to assume compromise. Individuals should regularly change passwords while organizations should constantly monitor their networks for all kinds of threats and exploitable vulnerabilities.

Waiting for solutions like more secure payment systems and legal sanctions, though already in the works, is no longer enough. Awareness of threats is a must and so are ever-ready mitigation and remediation plans because no one is safe from compromise.

The number of recorded cyber attacks against all sorts of organizations that handle customer data has been steadily increasing from 2011 to the present.

http://www.idtheftcenter.org/images/breach/20052013UPDATEDSummary.jpg
Exploit kits will target Android, as mobile vulnerabilities play a bigger role in device infection.
Apart from twice the current number of Android™ threats foreseen in 2015, the number of vulnerabilities in mobile devices, platforms, and apps will pose more serious security risks. Data stored in mobile devices will land in cybercriminals’ hands for use in attacks or selling underground.

The cumulative Android threat volume has steadily been increasing since 2012. We are likely to see the 2014 total to double in 2015.

The vulnerabilities we’ve seen so far did not only reside on devices but also on platforms and apps. Platform threats like the master key vulnerability allowed cybercrooks to replace legitimate apps with fake or malicious versions. When exploited, a certain Chinese third-party payment app vulnerability, meanwhile, allowed bad guys to phish information from infected devices.

We will see mobile attackers use tools similar to the Blackhole Exploit Kit (BHEK) to take advantage of problems like Android OS fragmentation. The success of BHEK and similar tools in infecting computers running different OSs will serve cybercrooks well in attacking Android devices since most users either don’t or can’t regularly update their systems and software. Bad guys can point vulnerable device users to malicious websites, for instance. Successful exploitation can then give them access to any or all of the information stored in affected devices. Worse, because exploit kits are known for affecting multiple platforms, should such a kit be made to target even mobile devices, who’s to say that the threats infected smartphones carry won’t spread to any device they have access to?

A steady rise in the number of mobile banking malware will be seen as well. Earlier this year, we saw the cybercriminals behind Operational Emmental prod a European bank’s customers to install a malicious Android app to gain access to their accounts. We will see more such attacks amid the rise in mobile banking popularity.

Traditional computer threats like ransomware and tactics like darknet service use will also figure in the mobile landscape. We already saw the first mobile ransomware in the form of REVETON rear its ugly head this year, along with another malware that used Tor to better evade detection.

Installing malicious apps and visiting malicious websites will no longer be the sole mobile infection vectors. Vulnerability exploitation across platforms will become even bigger mobile threats. Security vendors should extend vulnerability shielding and exploit-prevention technologies to include protection for mobile devices. Finally, mobile device manufacturers and service providers should work more closely with one another to come up with scalable vulnerability-patching solutions to prevent infection and data theft.
Targeted attacks will become as prevalent as cybercrime.
Successful high-profile and widely talked-about targeted attack campaigns led to the realization that cyber attacks are effective means to gather intelligence. Targeted attacks will no longer just be associated with countries like the United States or Russia. We’ve seen such attacks originate from other countries like Vietnam, India, and the United Kingdom. We’ve seen threat actors set their sights on countries like Indonesia and Malaysia as well.

In the next few years, we will see even more diverse attack origins and targets. Threat actors’ motivations will continue to vary. They will, however, continue to go after top-secret government data, financial information, intellectual property, industry blueprints, and the like.

Although majority of targeted attacks seen to date are initiated by spear-phishing emails or watering hole tactics, social media will increasingly be abused as infection vectors in the future. Threat actors will also explore the viability of exploiting router vulnerabilities as a means of getting in to target networks. Organizations that have been targeted in the past should not be complacent. Just because they’ve been breached before doesn’t mean they’re safe from future attacks. Threat actors can still use them to get to even bigger targets, likely their partners or customers.

The demand for portable or proxy in-the-cloud solutions that offer self-defense for security risks will rise. The popularity of network solutions such as firewalls and unified threat management (UTM) software, meanwhile, will decline. Better security analytics will become crucial to combat targeted attacks. Organizations should know what is normal for them and set this as a baseline when monitoring for threats. Network visualization and heuristic or behavior detection will also help them avoid becoming victims. Traditional or conventional security technologies will no longer be sufficient.
New mobile payment methods will introduce new threats.
The recent iPhone® 6 release came with the introduction of Apple’s version of digital payment—Apple Pay™. This, along with the increasing use of Google Wallet™ and other similar payment modes will act as catalyst for mobile payment to become mainstream. We will see new threats specifically target mobile payment platforms in the next few months akin to the Android FakeID vulnerability, which allowed cybercriminals to steal affected users’ Google Wallet credentials.

This year, apps like WeChat also started allowing users to purchase goods sold by certain retailers with so-called “credits.” If this becomes big, we will see cybercriminals take advantage of vulnerabilities in similar apps to steal money from users.

Although we have yet to see actual attacks and attempts to breach the Apple Pay ecosystem comprising NFC and Passbook, which holds users’ card information, cybercriminals used the latest iPhone models as social engineering bait two months before they were even launched. It’s safe to assume that as early as now, the bad guys are already looking for vulnerabilities to exploit in Apple Pay. They will continue to scrutinize NFC as well.

To stay safe from emerging threats, users would do well to practice safe computing habits, particularly those related to NFC use. Individuals who use NFC readers via their mobile devices should turn these off when they’re not in use. Locking their devices will help them avoid becoming a cybercrime victim. Organizations that accept mobile payments, meanwhile, should install and use security solutions that protect from NFC-related and similar security threats.
We will see more attempts to exploit vulnerabilities in open source apps.
Vulnerabilities in open source protocols like Heartbleed\(^{33}\) and command processors like Shellshock\(^{34}\) that remained undetected for years were heavily exploited this year, leading to serious repercussions. Just hours after the initial discovery of Shellshock, we saw several malware payloads\(^{35}\) in the wild. Distributed denial-of-service (DDoS) attacks and Internet Relay Chat (IRC) bots\(^{36}\) related to the vulnerability’s exploitation, which can disrupt business operations, were also spotted. More than Web surface attacks, however, Shellshock also put users of all Linux-based\(^{37}\) OSs and apps, which depended on protocols like HTTP, File Transfer Protocol (FTP), and Dynamic Host Configuration Protocol (DHCP) at risk.

Shellshock reminded the World Wide Web of Heartbleed, which put a lot of websites and mobile apps that used Open SSL at risk earlier this year. A quick scan of the top 1 million TLDs according to Alexa\(^{38}\), in fact, revealed that 5% were vulnerable to Heartbleed. When exploited, Heartbleed allows attackers to read parts of affected computers’ memory, which may contain confidential information.

Attacker will continue their search for seemingly dormant vulnerabilities like Heartbleed and Shellshock in the coming years. They will keep tabs on oft-forgotten platforms, protocols, and software and rely on irresponsible coding practices to get to their targets. As in 2013\(^{39}\), we will see even more injection, cross-site-scripting (XSS), and other attacks against Web apps to steal confidential information. Attacks such as that on JPMorgan Chase & Co.\(^{40}\), which put over 70 million customers’ personal data at risk, will continue to surface.

Continuous security improvements in Microsoft\(^{\text{TM}}\) Windows® and other big-name OSs will lead to a decline in their number of vulnerabilities. This will push attackers to instead focus on finding vulnerabilities in open source platforms and apps such as Open SSL v3 as well as OS kernels. Individuals and organizations can, however, stay protected by regularly patching and updating their systems and software. Organizations are also advised to invest in more intelligence-based security solutions backed by trusted global threat information sources, which can thwart exploitation attempts even if patches for vulnerabilities have yet to be issued.
Technological diversity will save IoE/IoT devices from mass attacks but the same won’t be true for the data they process.
Attackers will find IoE/IoT devices viable attack targets because of the endless possibilities their use presents. We are bound to see greater adoption of smart devices like smart cameras and TVs in the next few years, along with attacks against their users. As factors like market pressure push device manufacturers to launch more and more smart devices sans security in mind to meet the rising demand, so will attackers increasingly find vulnerabilities to exploit for their own gain.

Despite mass smartification, however, the first attacks we’ll see on smart appliances as well as wearable and other IoE/IoT devices will not be financially motivated. They will be more whitehat hacks to highlight security risks and weaknesses so manufacturers can improve their products, particularly the way they handle data. If and when these devices are hacked for purposes other than to bring vulnerabilities to light, cybercriminals will likely launch sniffer, denial-of-service (DoS), and man-in-the middle (MiTM) attacks.

Since IoE/IoT devices remain too diverse and a “killer app” has yet to emerge, bad guys will not be able to truly launch attacks against them. Attackers are more likely to go after the data that resides in these devices. In 2015, we expect attackers to hack smart device makers’ databases to steal information for traditional cyber attacks.

Later on, however, aided by the formation of the Open Interconnect Consortium (IOC) and the launch of HomeKit, we expect a shift in tides, as common protocols and platforms slowly emerge. As attackers begin to better understand the IoE/IoT ecosystem, they will employ scarier tactics akin to ransomware and scareware to extort money from or blackmail device users. They can, for instance, hold smart car drivers hostage until they pay up when said vehicles officially hit the road come 2015. As such, smart car manufacturers should incorporate network segmentation in their smart car designs to adequately shield users from such threats.
More severe online banking and other financially motivated threats will surface.
Weak security practices even in developed countries like the United States such as not enforcing the use of two-factor authentication and adoption of chip-and-pin technology will contribute to the rise in online banking and other financially motivated threats.

We’ve seen the online banking malware volume steadily rise throughout the first half of 2014\textsuperscript{46,47}. Apart from data-stealing ZeuS malware, VAWTRAK\textsuperscript{48} also affected a multitude of online banking customers specifically in Japan, contributing to the overall volume growth in the second quarter of the year. Complex operations like Emmental\textsuperscript{49}, which proved that even the two-factor authentication measures that banks employed could be flawed, also figured in the threat landscape.

In the next few years, cybercriminals will no longer just launch financially motivated threats against computer users, they will increasingly go after mobile device users as well. They are likely to use fake apps and Domain Name System (DNS) changers and launch mobile phishing\textsuperscript{50} attacks similar to those we’ve already seen in the past. They won’t stop at just gaining access to victims’ online banking accounts, they will even go so far as stealing their identities\textsuperscript{51}. And to come up with even stealthier mobile threats, we will see the emergence of packers akin to those used on computer malware.

The success of targeted attacks in obtaining user data will also inspire cybercriminals to better employ reconnaissance to make more money from their malicious schemes. Cybercrooks will use proven targeted attack methodologies for short-selling and front-running schemes.

The growing risks online banking threats pose should motivate individuals and organizations alike to use the two-factor authentication measures and hardware or session tokens that banks and other financial institutions provide. Payment card providers in the United States and other countries, meanwhile, should put data security at the forefront by making the use of chip-and-PIN cards and PoS terminals mandatory, especially amid the breaches hitting big-name companies left and right.

*We continued to see a steady rise in the online banking malware infections throughout the first half of 2014.*

**NOTE:** “Infection” refers to instances when threats were found on users’ computers and subsequently blocked by any Trend Micro security software.
REFERENCES


