

Trend Micro Incorporated
TrendLabs 2012 ANNUAL SECURITY ROUNDUP

Evolved Threats in a “Post-PC” World

Mobile.....2

Android malware followed the footsteps of Windows threats in terms of history, but at a much faster rate.

Targeted Attacks and Data Breaches4

Data breaches have become typical. Threat actors closely respond to their target's environment by using both old and new tools and techniques.

Cybercrime.....7

Threats evolved to become more effective and platform-agnostic, responding to the changing digital landscape.

Software Vulnerabilities11

Java exploits were seen, along with several zero-days for other programs.

Social Media and Online Services.....13

Social media threats flatlined in terms of creative use of technology, privacy concerns made headlines, and cloud services were abused by the bad guys.

Experts have been predicting the coming “post PC” era for a few years. So the question has been, “when will we know that it’s really here?” A simple answer is, we’ll know it’s really here when cybercriminals move beyond the PC. By that measure, 2012 is truly the year we entered the post-PC era as cybercriminals moved to embrace Android, social media platforms, and even Macs with their attacks.

Most notable for 2012 is that it took Android less than three years to reach the volume of malware threats that it took 14 years for the PC to reach. If that wasn’t enough proof, attackers moved their tried-and-true attacks to social media platforms like Pinterest and Tumblr for a broader reach. Attackers have even embraced social media for command and control, opting for Twitter over IRC in some cases.

In seeking out vulnerabilities to attack, attackers continued this trend by focusing on a technology whose very name is synonymous with multiplatform development—Java. 2012 was the year when Java supplanted pure Windows-based threats in the attackers’ crosshairs leading, among other things, to the first widespread attack against Macs.

Beyond this move away from the PC, 2012 saw attackers focus on refining their attacks and adopting more professional software development practices rather than introducing new attack means. The Black Hole Exploit Kit, automatic transfer systems (ATs), and ransomware were all refined and improved in ways that would make any commercial software vendor proud.

Most worrisome for enterprises and organizations though is that data breaches and targeted attacks continued at an alarming rate with staggering consequences. In one incident alone—the Global Payments data breach—the cost has already reached US\$94 million and is still climbing. Targeted attacks are being helped along by the “children of Stuxnet”—attack code and kits like Flame, Duqu, and Gauss that were derived from the Stuxnet attack of three years ago.

Overall, 2012 unfolded much like our chief technology officer, Raimund Genes, predicted in our [“12 Security Predictions for 2012,”](#) particularly around post-PC threats—the sophistication of attacks and targeted attacks. As he noted then, “our hope that new OSs make the world a safer place didn’t work out.” 2012 has clearly shown that to be the case. The post-PC era is here—and it’s already looking to be a more dangerous era with higher stakes at risk.

Growth of Android OS Threats Like PC Malware but Faster

2012 erased any doubt that the malware threat for mobile devices is real. The number of Android malware shot up from 1,000 at the start of the year to 350,000 by year's end.

This explosive malware growth mirrors the growth of the Android OS itself. IDC estimates that as many as three-fourths of all smartphones shipped in the third quarter ran the Android OS.¹ Since cybercriminals go after the most commonly used OS, Android has attracted the bulk of cybercriminal attention on mobile platforms to date.

Two major mobile malware types dominated 2012. First, we saw premium service abusers, which subscribe users to various

"services" that add to their bills. Second, we saw many high-risk apps, which violate user privacy by acquiring sensitive data without asking for explicit consent.

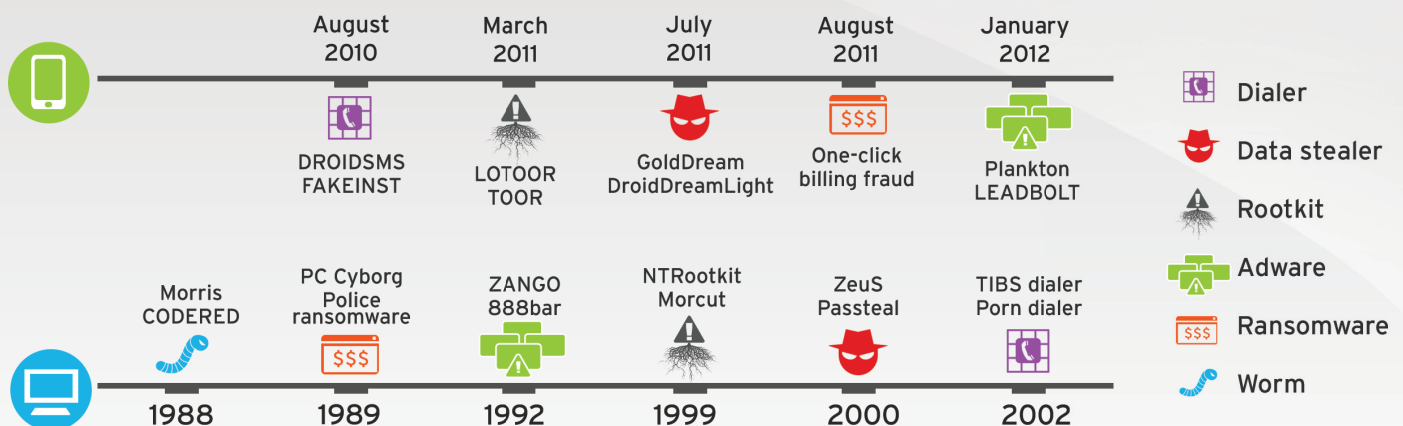
Android is well on its way to becoming the Windows of the mobile space. The popularity of Windows means that it has faced the lion's share of desktop threats for years. Similarly, the large Android market was the target of most mobile threats, but their rate of volume growth and complexity swelled at a much faster pace compared with PC malware.

For Android, it is no longer a case of directly installing malicious apps in smartphones. Now, URLs are able to either wipe data from phones² or take over devices.³ Smartphones are now facing the same kinds of threats previously seen on their PC cousins, all in roughly three years.

TrendLabsSM also released the "2012 Annual Mobile Threat and Security Roundup: Repeating History," which goes into more detail about the mobile threat landscape last year.

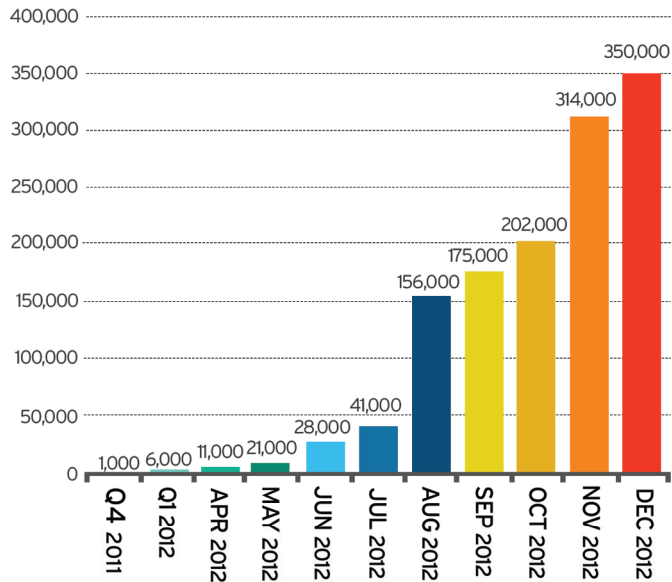
- **Android was the target of most mobile threats, but their rate of volume growth and complexity swelled at a much faster pace compared with PC malware.**

Android Versus PC Threat Type Timeline Comparison



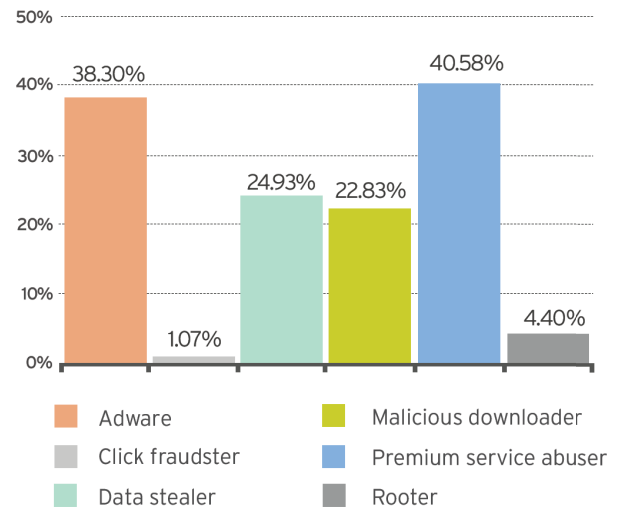
We've seen the same kinds of threats in the early web threat days of PC malware appear in the Android malware landscape—all in roughly three years.

Growth of Android Malware

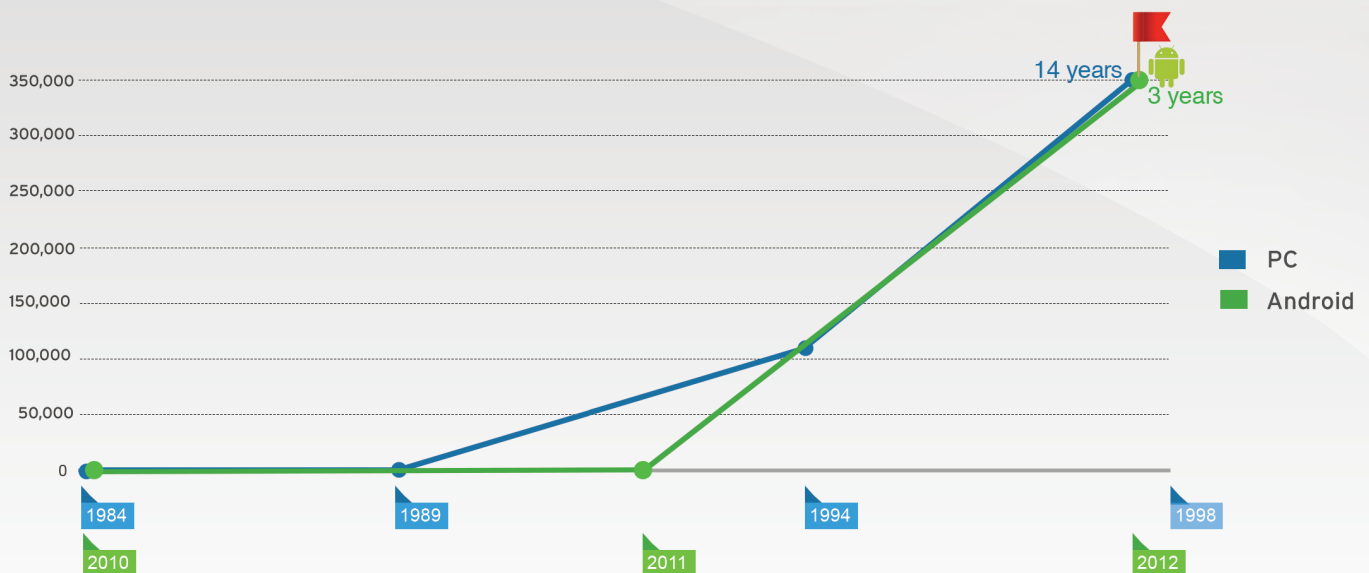


The staggering increase in the Android malware volume was partially due to the volume of premium service abusers and high-risk apps seen in the latter months of 2012.

Threat Type Classification of the Top 10 Android Malware Families



More than 70% of all Android malware belongs to a few malware families, most of which were either premium service abusers or high-risk apps.



It took Android less than 3 years to reach 350,000 malware while it took PC malware 14 years to reach the same volume of threats.

Data Breaches and APT Campaigns

The New Normal

2012 saw the continuation of the previous year's pattern of data breaches and targeted attacks. Payment processing company, Global Payments;⁴ the South Carolina Department of Revenue;⁵ and online shoe store, Zappos,⁶ for instance, all suffered breaches that affected millions of users and had a considerable financial impact. In the case of the Global Payments breach, the expenses reached US\$94 million. The question is no longer if a system will suffer a security breach, but when.

Despite heightened awareness of APTs and targeted attacks, we have seen several ongoing campaigns against various

organizations and companies. Among the campaigns we closely investigated were LURID, Luckycat, Taidoor, and IXESHE. We observed that attackers were good at “customizing” attacks as necessary—threat actors were able to use the attack vector most suitable to their purposes.

Spear-phishing emails were still the primary means of delivering malware in targeted attacks. Stealth and persistence were achieved through a wide variety of means, making network traffic analysis critical for security defenders. We have

seen remote access Trojans (RATs) like PoisonIvy, PlugX, Xtreme, JACKSBOT, and DRAT used in targeted attacks. These readily available RATs, including unsophisticated ones, made it easier for threat actors to carry out targeted attacks.

We also saw indications that mobile devices were becoming of interest to threat actors. Mobile malware with information theft capabilities—similar to those used in a targeted attack—were found on servers related to the Luckycat campaign.⁷

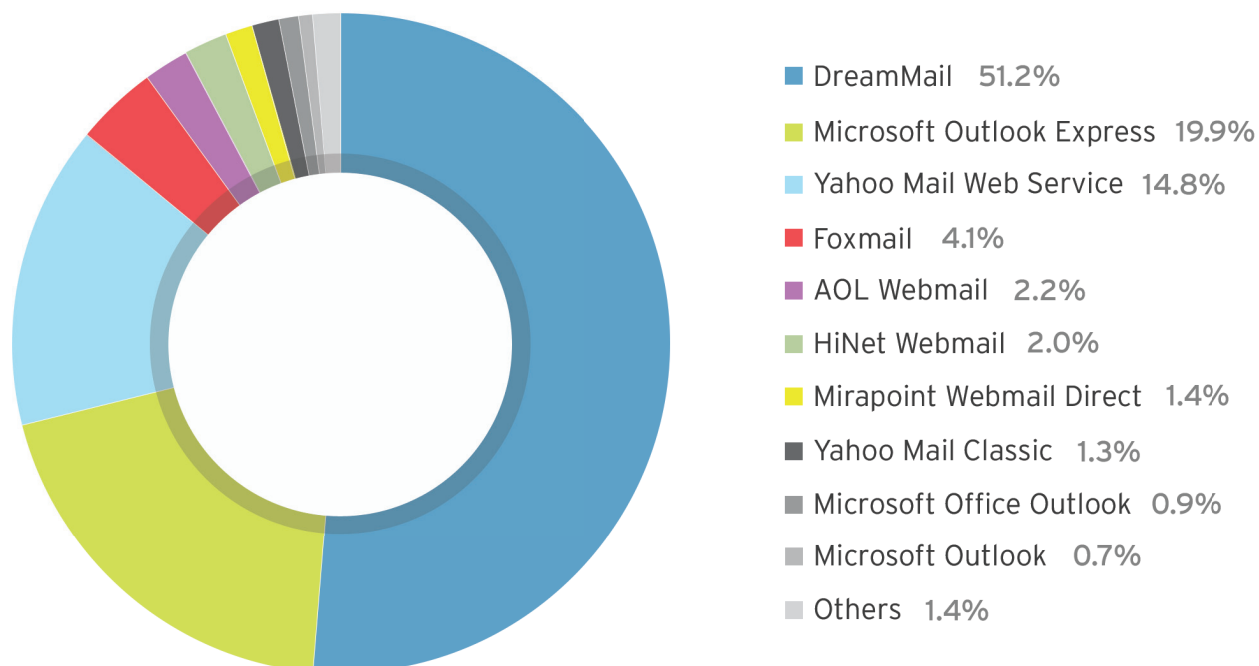
• **The question is no longer if a system will suffer a security breach, but when.**

APT FAST FACTS

- An experiment found that 87% of organizations clicked a link related to a social engineering lure.
- Targets of the Luckycat campaign included those in the aerospace, energy, military research, engineering, and shipping industries and Tibetan activists.
- A modified version of ENFAL—a malware used in the Lurid campaign—was able to compromise 874 computers in 33 countries in 2012..
- A survey found that 67% of organizations believed their security activities weren't enough to stop advanced persistent threats (APTs) or hackers.
- The IXESHE campaign has been actively staging targeted attacks since at least July 2009.
- The first stage of launching an APT campaign is intelligence gathering.

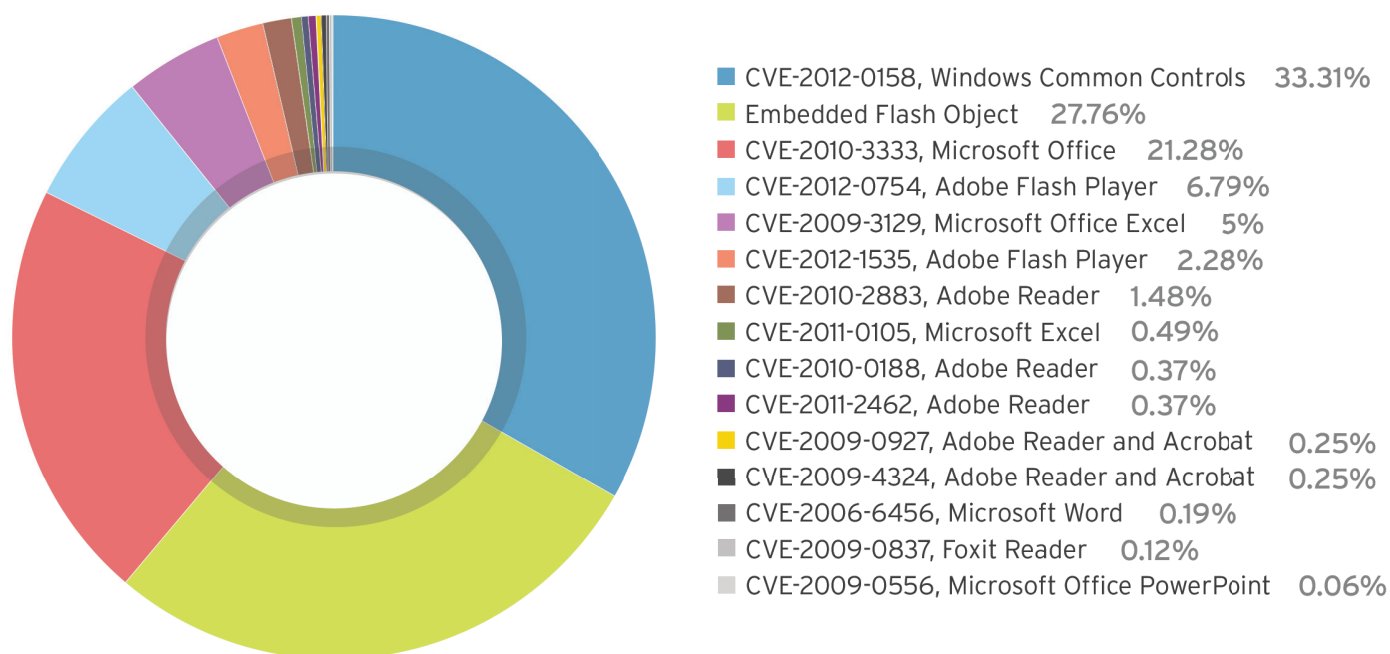


Email and Webmail Services Used in Targeted Attacks



Attackers still largely used emails, the most popular mode of business communication, to get in to target networks. DreamMail is an email client that supports several protocols, including SMTP, eSMTP, POP3, Hotmail, and Yahoo and a remote mailbox access function.

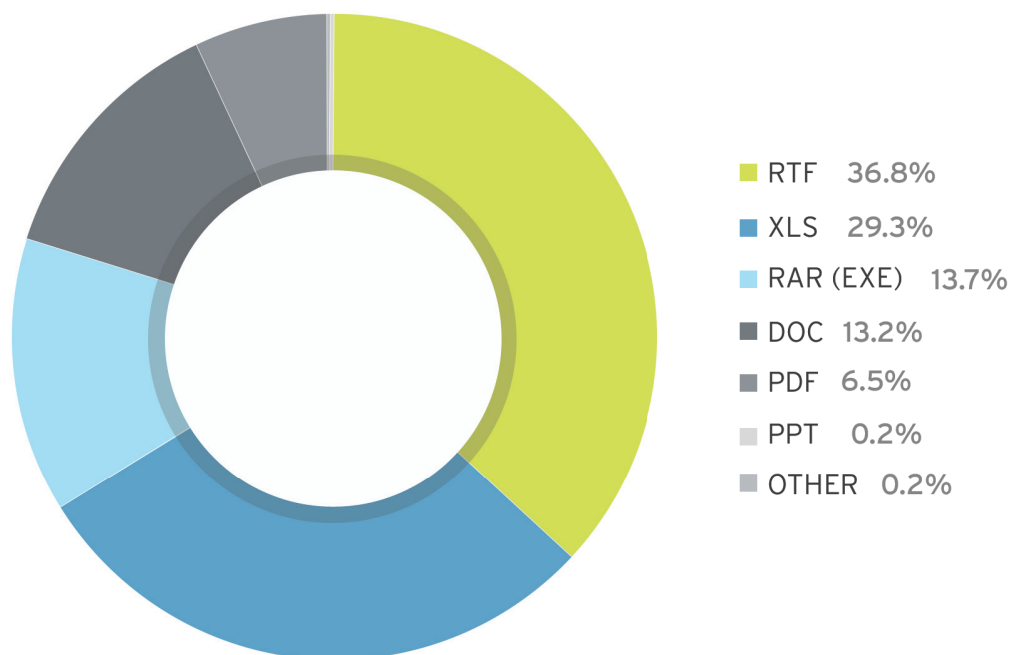
Vulnerabilities Used in Targeted Attacks



Note: The data in this figure is based on the targeted attacks Trend Micro monitored in 2012.

Threat actors used a mix of old—up to three-year-old—and relatively new vulnerabilities.

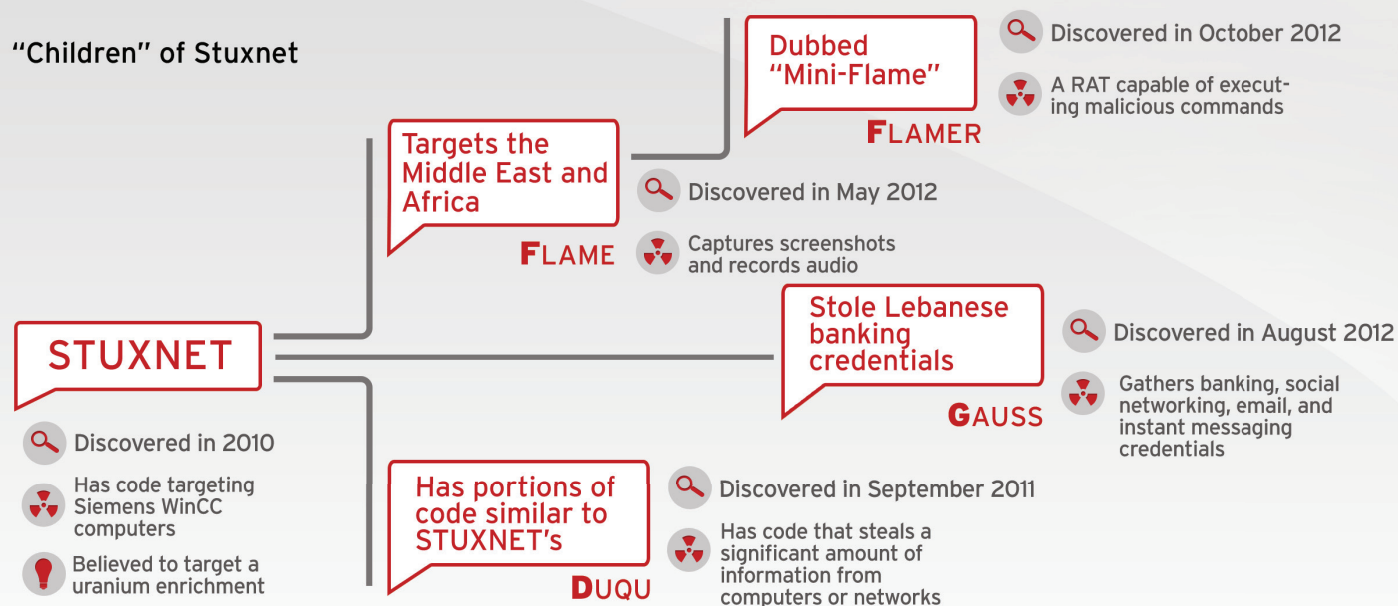
Email Attachment File Types Used in Targeted Attacks



Note: The data in this figure is based on the targeted attacks Trend Micro monitored in 2012.

Rich Text Format (.RTF) files were the most common kind of files used in targeted attacks, Microsoft® Excel® files, a close second. However, this data does not entirely reflect the actual vulnerabilities used, as it is relatively easy to embed different kinds of exploits into different file types.

"Children" of Stuxnet



The diagram above shows the connections between the heavily reported malware said to have close ties with Stuxnet.

Cybercrime

Fine-Tuning Attack Methods

Cybercriminals continued to enhance and improve their tools in 2012. The three most notable developments in the year had to do with ransomware, ATSS, and the Blackhole Exploit Kit.

Ransomware have been a problem for some time, but 2012 saw a particular tactic that came into common usage. Ransomware claimed that law enforcement groups “suspended” users’ systems due to violations of the law. In order to unlock their computers, users had to pay a fine using online vouchers.

Ransomware can be considered the successor of fake antivirus malware as the leading cybercrime threat facing consumers. Both threats cause users to worry about something (i.e., losing important data or downloading malicious files) and asks them to pay up to make the “problem” go away.

Similarly, ATSS became a key threat facing smaller businesses. ATSS remove middlemen, usually a keylogger or a WebInject file, when siphoning funds. Instead of passively stealing information, ATSS automatically transfer

funds from the victims’ to the cybercriminals’ accounts.⁸ This makes fraud more difficult to detect on the part of banks, as the transaction appears to be made by the user and not a potentially fraudulent third party. By contrast, traditional banking malware require human intervention to transfer funds, which is a slower process and may easily be detected by banks.

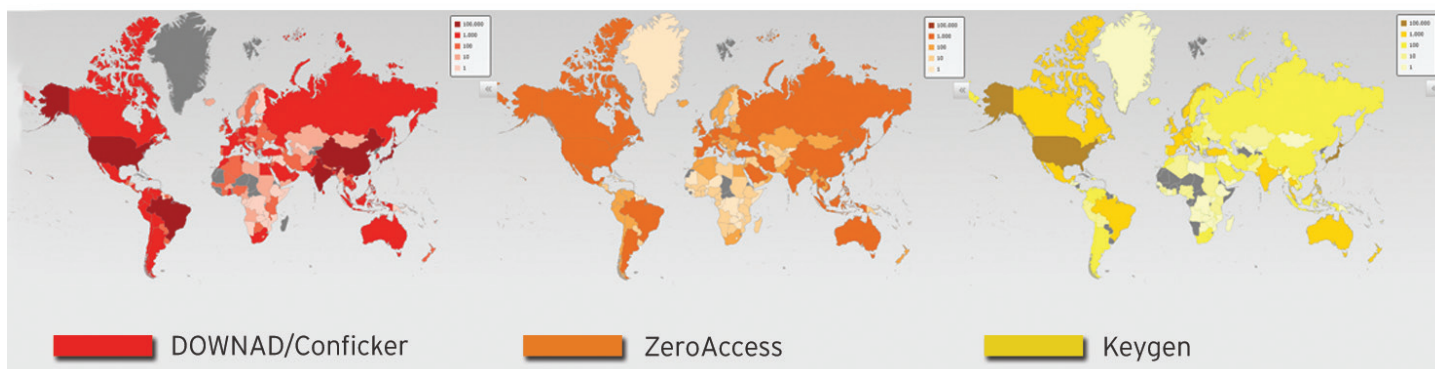
The Blackhole Exploit Kit spent 2012 in the limelight, as it was utilized in a number of phishing campaigns. It saw a major upgrade in the second half of the year with the release of version 2.0 in the underground—a response to increased security vendor efforts to shut down 1.x versions.⁹ These phishing campaigns also changed the way phishing was conducted—subtle emails made it difficult even for tech-savvy users to distinguish real from fake messages.

Taken together, these three developments represent an evolutionary upgrade to existing threats, demonstrating how malware development has become increasingly professional in rigor, discipline, and methodology. None of the developments constituted a completely new threat, but the updated versions appeared more dangerous in the threat environment.

This doesn’t mean that the rest of the threat landscape was stagnant. 2012 saw the significant rise of the ZeroAccess malware family¹⁰ while major file infectors like XPAJ¹¹ and VOFBUS¹² returned to prominence. Our analysis of the Chinese¹³ and Russian¹⁴ underground economies revealed that the business of stealing information like email and social networking account logins, credit card numbers, and personal data remains as brisk as ever.

- None of the developments constituted a
- completely new threat, but the updated
- versions appeared more dangerous in the
- threat environment.

Top 3 Malware



Infections: DOWNAD/Conficker - 2,564,618; ZeroAccess - 1,197,870; Keygen - 789,931

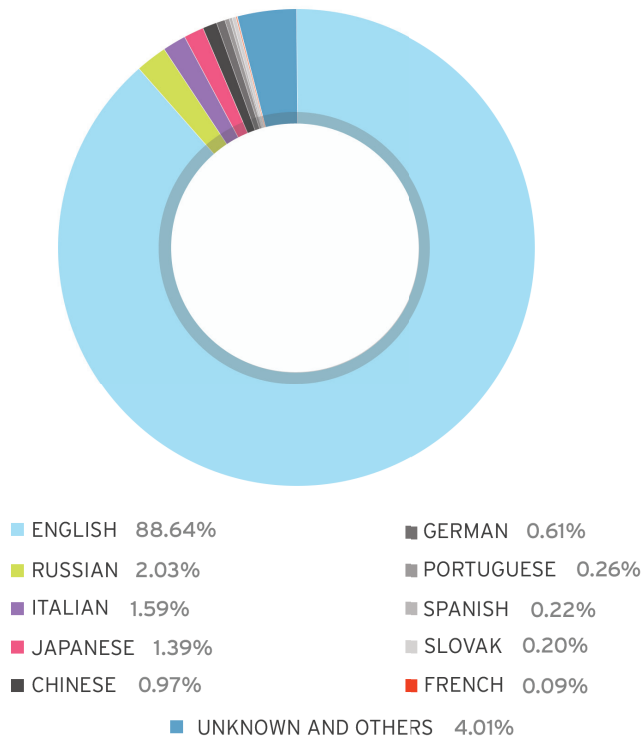
The DOWNAD worm has been around since 2008, spreading throughout networks using a now-patched vulnerability in Microsoft's Server Service. ZeroAccess piggybacks on cracked applications or poses as a required codec in peer-to-peer (P2P) applications. Crack or keygen programs generate serial numbers to enable the use of pirated applications.

Top Malicious Domains Blocked

Domain	Reason
trafficconverter.biz	Distributes malware, particularly DOWNAD variants
info.ejianlong.com	Downloads malware
deepspacer.com	Hosts malicious URLs, the registrant of which is a known spammer
mmi.explabs.net	Page DROPPER Trojans request access to
www.funad.co.kr	Poses security risks for compromised systems and/or networks
www.trafficholder.com	Traffic site known for distributing malware
serw.clicksor.com	Associated with the proliferation of pirated applications and other threats; posts annoying pop-up messages
install.ticno.com	Engaged in malware distribution
172.168.6.21	Distributes X97M_LAROUX.BK, XF_HELPOPY.AW, XF_NETSNAKE.A, X97M_LAROUX.CO, and X97M_LAROUX.CE

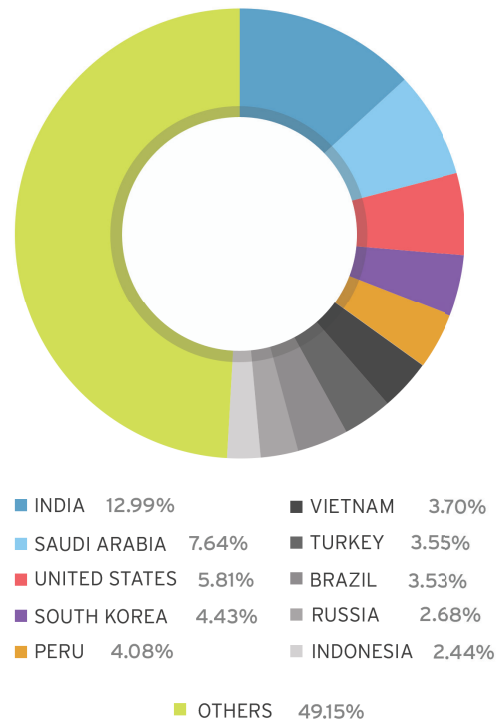
The proliferation of DOWNAD malware was partially aided by malware-hosting URLs. Some of these, however, are not necessarily malicious but have been compromised to perform malicious routines.

Top 10 Spam Languages



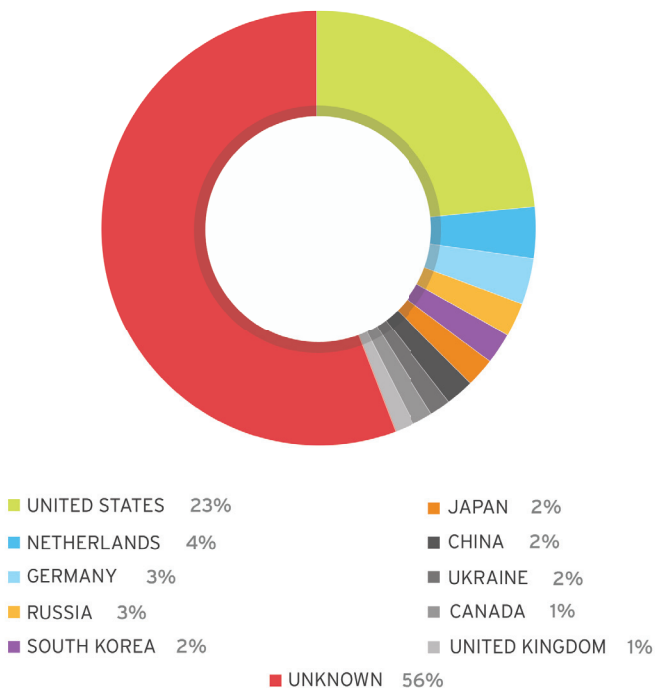
Almost all spam are still written in English, similar to previous years.

Top 10 Spam-Sending Countries

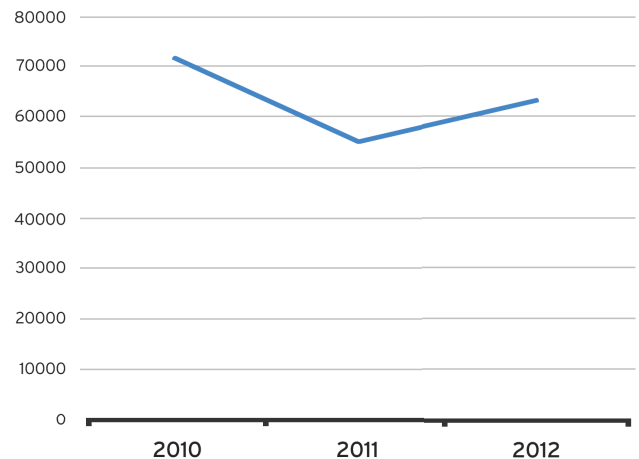


India was the top spam-sending country in 2012 while Saudi Arabia sent the most number of spam in the third quarter.

Top 10 Sources of Malicious URLs



More than 20% of the malicious URLs identified in 2012 were hosted in the United States or used hosting services located in the same region.



Blackhole Exploit Kit URLs related to renewed phishing attacks were a primary contributor to the resurgence of the phishing URL volume in 2012 after dipping in 2011.

Cybercrime Technique Improvements Seen



Typical phishing

- Contains typographical or grammatical errors
- Uses an alarmist tone
- Leads to sites that ask for personal information



Recent, Blackhole Exploit Kit-aided phishing

- Directly copies the content of legitimate corporate communications
- Leads to an exploit kit that downloads banking Trojans, among others



Old banking Trojans

- Use WebInjects, which insert fields to banking site forms
- Collect information users enter for later use



ATSS

- Run a script that initiates unauthorized withdrawals from victims' accounts
- Modify displayed account balances to hide unauthorized transactions



FAKEAV malware

- Show infection warnings and fake scanning results
- Prompt victims to pay for the software's full version to remove an "infection"

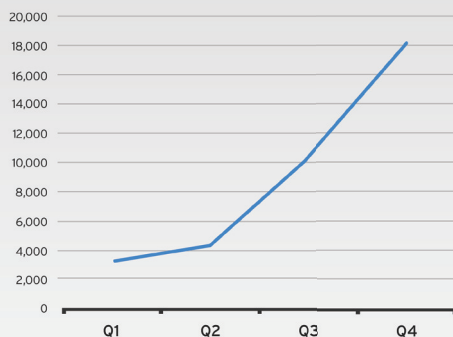


Ransomware

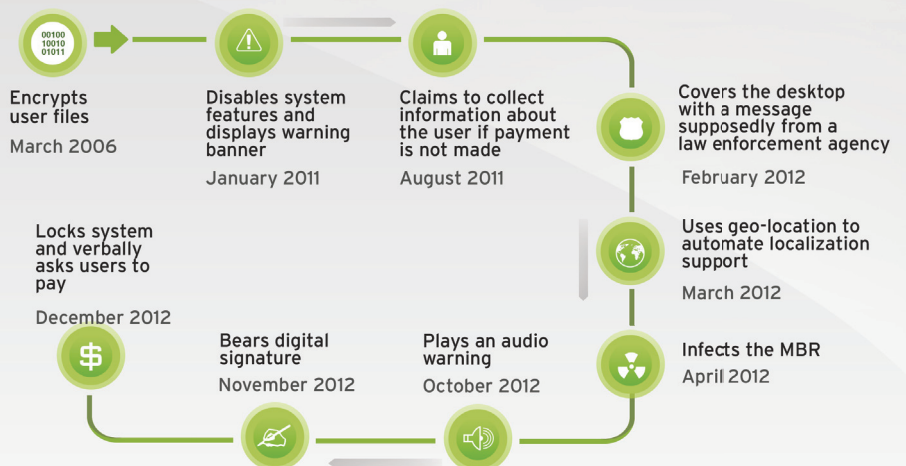
- Display warning messages and restrict access to affected computers, encrypt files
- Display law-enforcement agency logos
- Ask victims to pay a ransom to regain control of their computers or as fine for "violations"

The Blackhole Exploit Kit has changed the way phishing attacks are carried out. ATSS, meanwhile, have seen developments compared with traditional banking Trojans that made them prominent in 2012.

Ransomware Developments



Ransomware infections increased throughout 2012.



Ransomware have changed throughout the years.

Vulnerabilities

Old but Reliable Exploits and Some Zero-Days

Zero-day vulnerabilities continued to affect users in 2012. In August, the Blackhole Exploit Kit¹⁵ made use of a zero-day vulnerability in Java 7.¹⁶ In September, a zero-day use-after-free vulnerability in Internet Explorer¹⁷ was patched, but was previously used in attacks that led to RATs.¹⁸ Just before the year ended, older versions of the browser were found with another zero-day flaw.¹⁹ Taking a peek ahead this year, we saw yet another Java zero-day vulnerability abused by the Blackhole Exploit Kit.²⁰

Attackers did not need to seek out new vulnerabilities, as most users failed to patch their systems anyway, which means that old vulnerabilities still worked. The VOBFUS worm, which hit a number of computers in the latter part of 2012, uses the same vulnerability that Stuxnet originally used as far back as 2010.²¹ Targeted attacks are known to make use of vulnerabilities in Microsoft® Office® applications that date back to 2009.²² In fact, a

three-year-old vulnerability, CVE-2009-3129 or MS09-067, was the third most exploited vulnerability in targeted attacks in April 2012.²³

An exploit kit—a combination of exploits designed to compromise a user's computer—is a key part of today's threat environment. One of the most prominent exploit kits today is the Blackhole Exploit Kit, which is commonly used in phishing campaigns to target computers.²⁴

The applications most targeted by exploit kits are browsers or technologies that expose functionality through browser plug-ins, particularly Internet Explorer; Adobe Acrobat, Reader, and Flash Player; and Java. However, developers have taken steps to make the bugs in their products more difficult to exploit. For example, Adobe highlighted

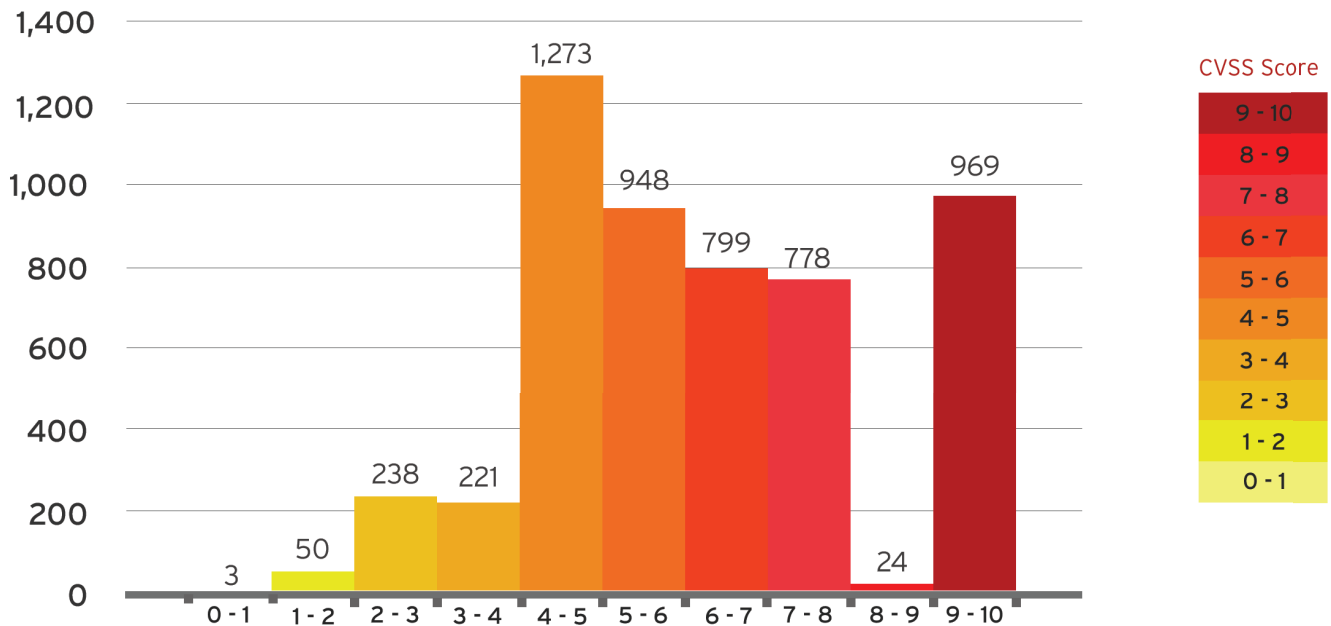
Acrobat and Reader's improved sandboxing feature with the release of version 11.²⁵ Adobe Flash Player received a new background updater²⁶ to help users who still run older versions. Browsers received constant updates throughout the year to patch existing holes and strengthen their defenses against exploits.

Java, however, has not seen a similar development. Instead, there have been moves to reduce the use of Java. Apple went so far as to remove Java from browsers on OS X computers.²⁷ A December update to Java allowed users to disable Java content in browsers.²⁸

The relatively unsecured state of Java, combined with its popularity with users, resulted in growth in its popularity among cybercriminals.

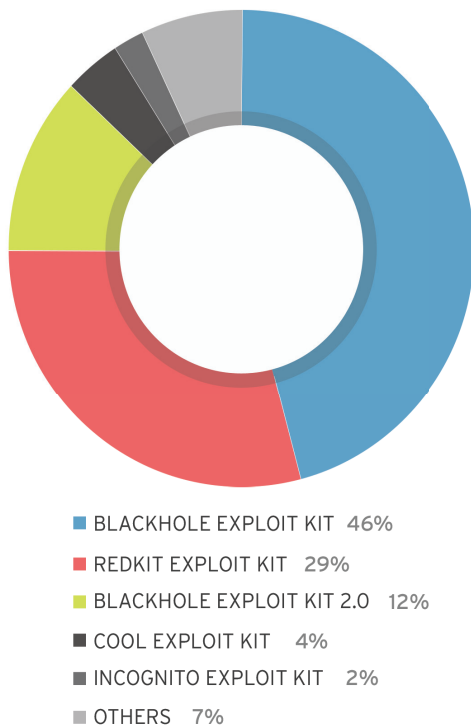
- **The relatively unsecured state of Java,**
- **combined with its popularity with users,**
- **resulted in growth in its popularity among**
- **cybercriminals.**

CVSS Score Distribution for Vulnerabilities Addressed



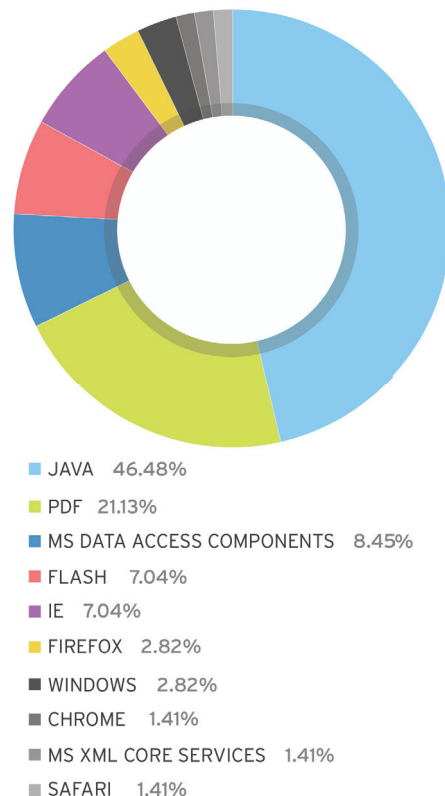
Of the vulnerabilities addressed in 2012, the majority were rated “medium” (4.0 to 6.9) in severity while a third were given a “high” (7.0 to 10.0) severity rating.

Top 5 Exploit Kits Using Browser Exploits



The majority of browser exploits we monitored in 2012 came from the Blackhole Exploit Kit 1.0, while a third came from RedKit.

Top 10 Browser Exploit Kit Targets



Java was the most targeted program by exploit kits based on the browser exploits we monitored.

Social Media and Online Services Recycled Threats

While social media threats did not change much in 2012, attackers did not remain idle in exploiting new opportunities.

In 2012, Pinterest²⁹ and Tumblr³⁰ became popular among users and attracted the attention of various scammers. As expected, cybercriminals go where the audience is, so malicious links in Pinterest and Tumblr pointed to survey scams.

However, much of the discussion surrounding social media has been about privacy. Decisions made by social networking sites about user privacy called into question how these sites handle personal information. The question of

whether or not users trusted their social networks came up again³¹ and again³² in 2012.

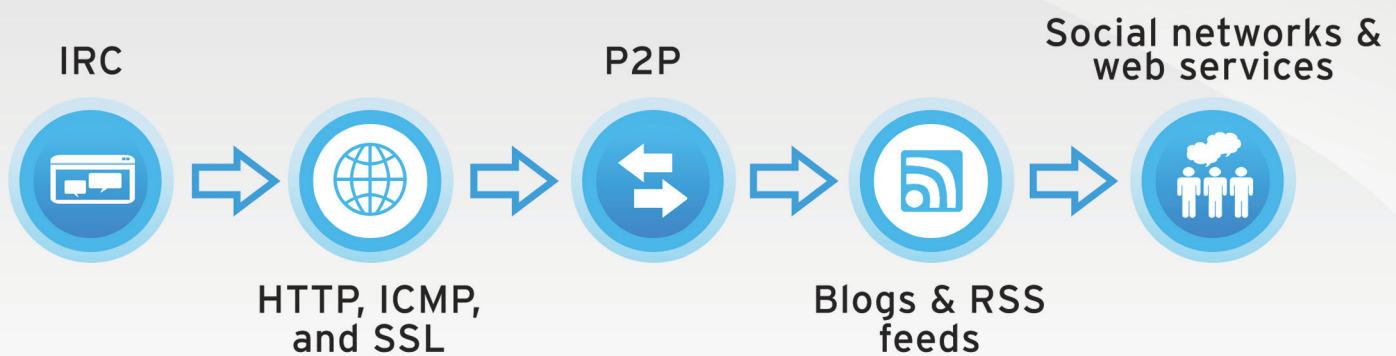
In addition, users continued to inadvertently share confidential information online. They posted their credit card details and IDs without realizing the consequences of doing so. Unfortunately, these incidents just represent the worst case of oversharing online.³³

Legitimate online services were also used with increasing frequency for malicious purposes.

Pastebin saw much use as a dumping ground for all sorts of stolen information. Blog comments and Twitter accounts became common means to control botnets, as an alternative to central command-and-control servers, which can be found and blocked far more easily than legitimate services.

- **Decisions made by social networking sites**
- **about user privacy called into question how**
- **these sites handle personal information.**

Evolution of Cybercriminal Tools for Command-and-Control Communication



The switch from basic IRC to other new tools for command and control is one example of how cybercriminals abuse legitimate online services for their own operations.

Q1

Law Tax season
Enforcement
Whitney Houston
Temple Run Jeremy Lin

Q2

London 2012
Tibet Olympics
Instagram Android
Angy BirdsDiablo 3
Space

Q3

World of Warcraft
iPhone 5 Obama
Olympics 2012 London
2012

Q4

Christmas
Windows 8 **Thanksgiving**
Black Friday sale Obama
Cyber Monday sale
Holiday Bad Piggies

Cybercriminals used all kinds of lures to reel in victims throughout 2012.

What This Means for Users and Businesses

Mobile Threats

For Home Users

- Use your smartphone's built-in security features.
- Avoid using free but unsecured Wi-Fi access.
- Scrutinize every app you download regardless of source.
- Understand permissions before accepting them.
- Consider investing in a mobile security app for Android like Trend Micro™ Mobile Security Personal Edition.

For Security Groups

On top of educating employees on consumer tips to secure their mobile devices, enterprises should embrace consumerization via this three-step plan with the help of mobile device management and security products like Trend Micro™ Mobile Security:

- **Step 1:** Have a plan.
- **Step 2:** Say yes... but not to everything... and not to everyone.
- **Step 3:** Put the right infrastructure in place.

Targeted Attacks and Data Breaches

For Home Users

Enterprises and organizations are the common targets of APTs and highly targeted attacks. But attacks often enter target networks via employee inboxes in the form of spear-phishing emails. Employees must delete or ignore emails from unknown sources.

For Security Groups

- Develop local and external threat intelligence.
- Test and educate employees against social engineering attacks.
- Formulate mitigation and cleanup strategies in case of an attack.
- Deploy custom defense solutions like Trend Micro™ Deep Discovery to protect against APTs.
- Protect company data through data protection and management solutions.

Cybercrime

For Home Users

- Regularly check your bank, credit, and debit card statements to ensure that all of the transactions in them are legitimate.
- When conducting financial transactions online, make sure the website address contains an **s** as in **<https://www.bank.com>**.
- Invest in a comprehensive security suite like Trend Micro™ Titanium Security.

For Security Groups

- Install effective security solutions in computers or devices that contain or have access to sensitive information.
- Deploy a defense-in-depth security practice.
- Block threats at their source using web, IP, and domain reputation technologies.
- Invest in sandbox technologies to identify advanced malware.

Software Vulnerabilities

For Home Users

- Apply the latest security updates and patches to your software programs and OSs.
- Enable automatic updates where possible.

For Security Groups

Deploy solutions that allow vulnerability shielding to help immediately protect networks from exploits like Trend Micro™ Deep Security.

Social Media Threats

For Home Users

- Use random but memorable phrases as passwords.
- Avoid using the same password across online accounts.
- Change your password every few months.
- Consider using password managers like Trend Micro™ DirectPass™.
- A good rule of thumb on giving out information on social networking sites is to ask, “Would I give this information to a stranger over the phone?”

For Security Groups

- Monitor employees' social networking usage.
- Create easy-to-follow guidelines on social media use regarding sharing of information and representing your company's brand and image.
- Clearly define what's confidential.

References

- 1 <http://www.idc.com/getdoc.jsp?containerId=prUS23771812>
- 2 <http://blog.trendmicro.com/trendlabs-security-intelligence/dirty-ussds-and-the-android-update-problem/>
- 3 <http://blog.trendmicro.com/trendlabs-security-intelligence/exynos-based-android-devices-suffer-from-vulnerability/>
- 4 <http://money.cnn.com/2012/04/02/technology/global-payments-breach/index.htm>
- 5 <http://www.forbes.com/sites/anthonykosner/2012/10/27/cyber-security-fails-as-3-6-million-social-security-numbers-breached-in-south-carolina/>
- 6 http://news.cnet.com/8301-1009_3-57359536-83/zappos-customer-data-accessed-in-security-breach/
- 7 <http://blog.trendmicro.com/trendlabs-security-intelligence/defcon-2012-android-malware-in-luckycat-servers/>
- 8 <http://blog.trendmicro.com/trendlabs-security-intelligence/evolved-banking-fraud-malware-automatic-transfer-systems/>
- 9 <http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-2-0-beta-tests-in-the-wild/>
- 10 http://blog.trendmicro.com/trendlabs-security-intelligence/under-the-hood-of-bkdr_zaccess/
- 11 http://blog.trendmicro.com/trendlabs-security-intelligence/pe_xpaj-persistent-file-infector/
- 12 http://blog.trendmicro.com/trendlabs-security-intelligence/watch-out-for-worm_vobfus/
- 13 <http://blog.trendmicro.com/trendlabs-security-intelligence/the-chinese-underground-part-1-introduction/>
- 14 <http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-russian-underground/>
- 15 <http://blog.trendmicro.com/trendlabs-security-intelligence/java-zero-days-and-the-blackhole-exploit-kit/>
- 16 <http://blog.trendmicro.com/trendlabs-security-intelligence/java-runtime-environment-1-7-zero-day-exploit-delivers-backdoor/>
- 17 <http://blog.trendmicro.com/trendlabs-security-intelligence/microsoft-releases-out-of-cycle-patch-for-ie/>
- 18 <http://blog.trendmicro.com/trendlabs-security-intelligence/new-ie-zero-day-exploit-leads-to-poisonivy>
- 19 <http://blog.trendmicro.com/trendlabs-security-intelligence/why-is-the-watering-hole-technique-effective/>
- 20 <http://blog.trendmicro.com/trendlabs-security-intelligence/java-zero-day-exploit-and-ruby-on-rails-vulnerabilities/>
- 21 <http://technet.microsoft.com/en-us/security/bulletin/MS10-046>
- 22 <http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2012-0158-exploitation-seen-in-various-global-campaigns/>
- 23 <http://blog.trendmicro.com/trendlabs-security-intelligence/snapshot-of-exploit-documents-for-april-2012/>
- 24 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf
- 25 <http://blogs.adobe.com/asset/2012/10/new-security-capabilities-in-adobe-reader-and-acrobat-xi-now-available.html>
- 26 <http://blogs.adobe.com/asset/2012/03/an-update-for-the-flash-player-updater.html>
- 27 <http://arstechnica.com/apple/2012/10/apple-removes-java-from-all-os-x-web-browsers/>
- 28 <http://www.infoworld.com/d/security/java-7-update-10-allows-users-restrict-java-in-browsers-209423>
- 29 <http://blog.trendmicro.com/trendlabs-security-intelligence/survey-scams-find-their-way-into-pinterest/>
- 30 <http://blog.trendmicro.com/trendlabs-security-intelligence/tumviewer-and-online-income-survey-scams-hit-tumblr/>
- 31 <http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-public-or-private-the-risks-of-posting-in-social-networks/>
- 32 <http://blog.trendmicro.com/trendlabs-security-intelligence/privacy-worries-hound-facebook-yet-again/>
- 33 <http://blog.trendmicro.com/trendlabs-security-intelligence/the-dangers-of-posting-credit-cards-ids-on-instagram-and-twitter/>

TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.



Securing Your Journey
to the Cloud

TRENDLABSSM

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

