TrendLabs ANNUAL SECURITY ROUNDUP

A Look Back at 2011

Information Is Currency

True to one of our predictions for the year, 2011 has been dubbed the "Year of Data Breaches," as we witnessed organizations worldwide succumb to targeted breach attacks and lose what we have come to know as the new digital currency—data. As individuals and organizations alike embark on the cloud journey, we at Trend Micro, along with our fellow cybercrimefighters in law enforcement and the security industry, will continue to serve our customers by providing data protection from, in, and for the cloud.

Proven 2011 Trend Micro Predictions

Trend Micro Security Wins

2011 was a particularly challenging year for the security industry, as several organizations succumbed to targeted data breach attacks that soiled their reputations via the loss of confidential information and caused them to spend huge sums of money on fixing the damage done. Two of the biggest targets—RSA[1] and Sony PlayStation[2]—were left with no other choice but to publicly disclose facts about the attacks against their infrastructure so their customers could ensure proper mitigation.

2011 has been dubbed the "Year of Data Breaches," marring organizations worldwide via huge information and financial losses.

2011 PREDICTION

We will see more targeted attacks and cyber espionage.

[1] http://www.rsa.com/node.aspx?id=3872

[2] http://arstechnica.com/gaming/news/2011/04/sony-admits-utter-psn-failure-your-personal-data-has-been-stolen.ars

RSA APT ATTACK

- RSA Executive Chairman, Arthur W. Covellio, Jr., issued an open letter to customers on the extent of the APT attack
- Certain information related to SecurID two-factor authentication products was extracted from RSA's systems
- RSA released best practices for victims and replaced tokens belonging to defense industry customers as remediation[3]
- Information stolen from RSA's systems was used in a broader attack on client, Lockheed Martin—the biggest IT provider to the U.S. government[4]

[3] http://www.rsa.com/node.aspx?id=3891

[4] http://uk.reuters.com/article/2011/05/26/us-lockheed-network-idUKTRE74P7U320110526

SONY PLAYSTATION DATA BREACH

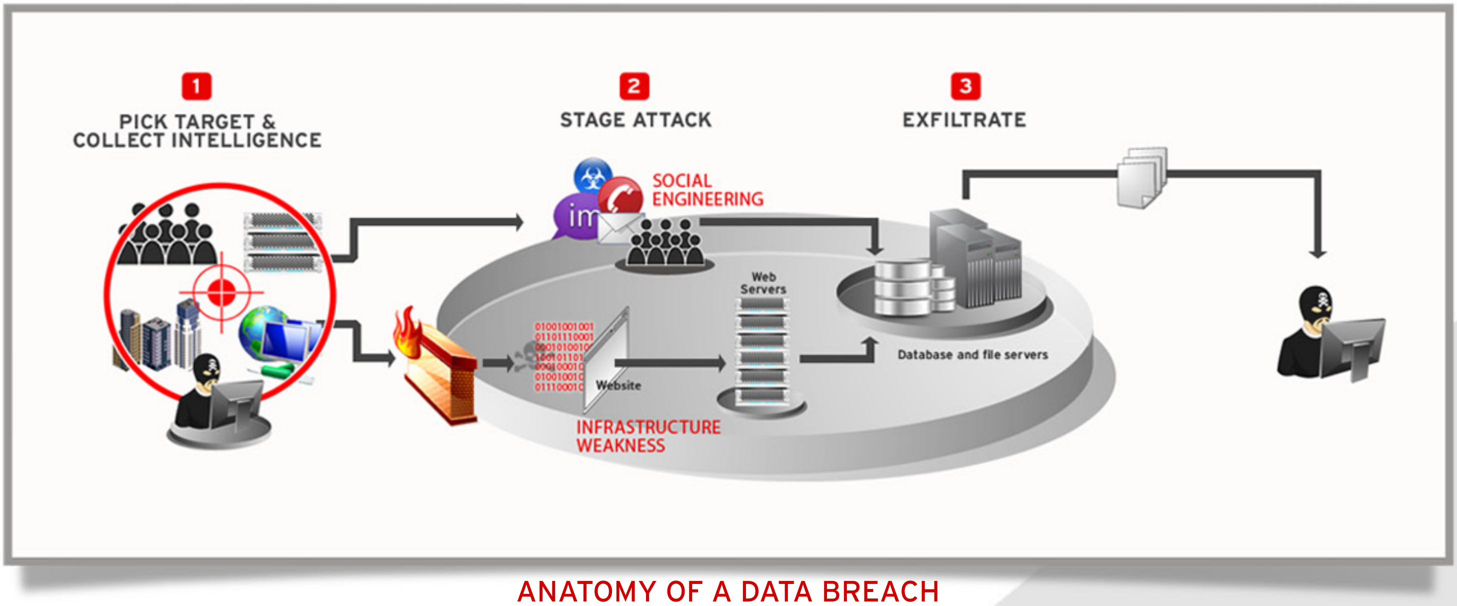
- Sony was forced to close down its *PlayStation Network* service after publicizing pertinent facts about a targeted attack
- Information on **~77M** *PlayStation Network* and *Qriocity* user accounts was stolen[5]
- Sony spent at least **US$171M** to fix the damage caused by the attack[6]

[5] http://www.flickr.com/photos/playstationblog/5686965323/in/set-72157626521862165/

[6] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Anatomy+of+a+Data+Breach

> "While targeted malware attacks are currently used to steal data, future attacks may aim to modify data."[7]
>
> —Nart Villeneuve,
> Trend Micro Senior
> Threat Researcher

[7] http://us.trendmicro.com/imperia/md/content/us/trendwatch/cloud/wp01_targetedattacks_111012us.pdf



ANATOMY OF A DATA BREACH

Mobile malware seemingly took the world by storm, catching users unaware with the whopping increase in the *Android* malware volume alone.[8] Mobile malware invaded device users' privacy by stealing personal and other kinds of confidential information. RuFraud[9] and DroidDreamLight[10]—just two of the most notorious *Android* malware variants—took much of the spotlight, causing millions of users a lot of grief from losing data and, at times, money.

[8] http://blog.trendmicro.com/a-snapshot-of-android-threats-infographic/
[9] http://blog.trendmicro.com/2011-in-review-mobile-malware/
[10] http://blog.trendmicro.com/massive-code-change-for-new-droiddreamlight-variant/

2011 saw the mobile threat landscape mature, as evidenced by the staggering spike in the mobile malware volume.

2011 PREDICTION

We will see more mobile device attacks.

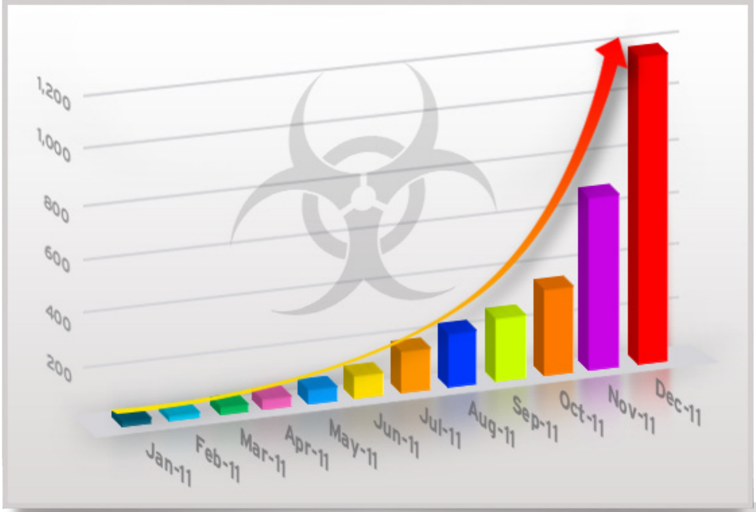
DROIDDREAMLIGHT VARIANTS

- Mostly found in China-based third-party app stores though some variants also plagued the *Android Market*
- Come in the guise of battery-monitoring, task-listing, installed app-identifying tools, among others
- Steals all sorts of device and personal information that is sent to a remote URL
- Secretly sends messages to affected users' contacts
- Checks if infected devices have been rooted and if so installs and uninstalls certain packages

51.9M	number of *Android*-based devices[12]
350+M	number of active *Facebook* users who access the site via mobile devices
475+	number of mobile operators worldwide that deploy and promote *Facebook's* mobile products[13]

[12] http://www.canalys.com/static/press_release/2011/canalys-press-release-010811-android-takes-almost-50-share-worldwide-smart-phone-market_0.pdf

[13] http://www.facebook.com/press/info.php?statistics



ANDROID MALWARE VOLUME GROWTH IN 2011

RUFRAUD VARIANTS

- Found in the *Android Market*
- Categorized as "premium-service abusers"
- Were taken off by Google from the *Android Market* soon after their discovery
- May have been downloaded by some users before being taken off Google's official app store, as these proliferated in time for the *Android Market's* celebration of reaching **10B** downloads[11]

[11] http://blog.trendmicro.com/checking-the-legitimacy-of-android-apps/

> "If current trends hold, we may be able to see more than 120,000 malicious *Android* apps by the end of 2012."[14]
>
> –Menard Oseña,
> Trend Micro Solutions
> Product Manager

[14] http://blog.trendmicro.com/how-big-will-the-android-malware-threat-be-in-2012/

ANDROID MALWARE TYPES

- Data stealers
- Premium-service abusers
- Click fraudsters
- Malicious downloaders
- Spying tools
- Rooters[15]

[15] http://blog.trendmicro.com/snapshot-of-android-threats

Survey scams and all kinds of spam leveraging every trending topic imaginable littered social networking sites throughout 2011. Armed with improved social engineering and hacking tactics and tools, spammers and scammers alike continued to wreak havoc among social networkers worldwide, all after the so-called "new currency"—data.[16] In light of the situation, regulators have started demanding that social networking sites implement policies and mechanisms to protect the privacy of their users.[17]

2011 was a good year for social media spammers and scammers but not such a good one for site administrators and regulators.

2011 PREDICTION

We will see more clever malware campaigning.

[16] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Spam%2c+Scams+and+Other+Social+Media+Threats

[17] http://dataprotection.ie/viewdoc.asp?DocID=1175&m=f

SOCIAL MEDIA SPAM

- Use practically every trending topic possible such as Lady Gaga's supposed death to lure victims
- Drop big media companies' names such as the British Broadcasting Corporation (BBC) as senders
- Make use of links to phishing pages and fake sites that serve as malware hosts or site redirectors
- Spread via automatic reposting on victims' *Walls* or retweets[18]
- Take advantage of even the most unfortunate event such as Hurricane Irene to gain as many victims as possible, most likely for financial gain[19]
- Ride on popular gadget or application releases to get user clicks[20]

SURVEY SCAMS

- Use newsworthy events and tempting offers such as premiere movie tickets to trick users into clicking links to survey pages[21]
- Victims of which end up with stolen personal data or, worse, thinner wallets[22]

> "With or without *Facebook*, unenlightened users will make a mistake and divulge private information no matter what social network you drop them in to."
>
> –Jamz Yaneza,
> Trend Micro Threat
> Research Manager

TOP 3 PUBLICLY AVAILABLE INFORMATION ON SOCIAL MEDIA

- Email addresses
- Hometown
- High school

3 MOST COMMON *FACEBOOK* ATTACK TYPES

- Likejacking attacks
- Rogue application propagation attacks
- Spam campaigns

TOP 3 SOCIAL MEDIA SECURITY RISKS

- Malware infection
- Data leakage
- Unwilling attack participation

[18] http://blog.trendmicro.com/facebook-scam-leverages-lady-gagas-death-bypasses-https/
[19] http://blog.trendmicro.com/hurricane-irene-scam-hits-facebook/
[20] http://blog.trendmicro.com/seasons-warnings-iphone-4s-scam-and-other-holiday-threats/

[21] http://blog.trendmicro.com/free-breaking-dawn-part-2-tickets-scam-spreads-in-facebook/
[22] http://blog.trendmicro.com/survey-scams-as-cross-platform-threats/

Even though the number of publicly reported vulnerabilities decreased from 4,651 in 2010 to 4,155 in 2011,[23] exploit attacks improved in terms of both complexity and sophistication. The exploit attacks we saw in 2011 were targeted, original, and well controlled, the most notable of which set their sights on *CVE-2011-3402, CVE-2011-3544*, and *CVE-2011-3414,*[24] along with a couple of Adobe product zero-day vulnerabilities that were exploited in the wild.[25]

2011 continued to be a bad one in terms of exploits despite the decline in the number of publicly reported vulnerabilities.

2011 PREDICTION

We will see the use of vulnerabilities and exploits evolve.

[23] http://cvedetails.com/browse-by-date.php

[24] http://blog.trendmicro.com/microsoft-releases-out-of-band-update-before-year-ends/

[25] http://blog.trendmicro.com/2011-in-review-exploits-and-vulnerabilities/

CVE-2011-3402

- A vulnerability in a *Microsoft Windows* component that may allow an attacker to execute code on vulnerable systems
- Exploited by DUQU malware[26]

[26] http://about-threats.trendmicro.com/Vulnerability.aspx?language=us&name=Vulnerability+in+TrueType+Font+Parsing+Could+Allow+Elevation+of+Privilege+(2639658)

CVE-2011-3544

- An unspecified vulnerability in the *Java Runtime Environment (JRE)* component of *Oracle Java SE Java Development Kit (JDK)* and *JRE*
- Allows remote *Java Web Start* applications and *Java* applets to affect the confidentiality, integrity, and availability of systems via unknown vectors related to scripting[27]

[27] http://about-threats.trendmicro.com/vulnerability.aspx?language=us&name=Unspecified%20vulnerability%20in%20the%20Java%20Runtime%20Environment

37% percentage of users who browse the web with unsecured *Java* versions[30]

56% percentage of enterprise users that utilize vulnerable *Adobe Reader* versions[31]

[30] http://www.csis.dk/en/csis/news/3321

[31] http://www.zscaler.com/pdf/Zscaler-Labs-State-of-the-Web-2011Q2.pdf

WORST MASS SQL INJECTION ATTACKS

8M number of pages infected during the *willysy.com* attack[32]

1M number of pages infected during an attack targeting *ASP.NET* sites[33]

[32] http://blog.armorize.com/2011/07/willysycom-mass-injection-ongoing.html

[33] http://www.zdnet.com/blog/security/over-a-million-web-sites-affected-in-mass-sql-injection-attack/9662?tag=mantle_skin;content

CVE-2011-3414

- A vulnerability that may lead to elevation of privilege if a potential attacker sends a maliciously crafted web request to a target
- Can lead to the execution of arbitrary commands via existing accounts on the *ASP.NET* site
- The vulnerability that Microsoft released an out-of-band patch for before 2011 ended[28]

[28] http://about-threats.trendmicro.com/vulnerability.aspx?language=us&name=Vulnerabilities%20in%20.NET%20Framework%20Could%20Allow%20Elevation%20of%20Privilege%20(2638420)

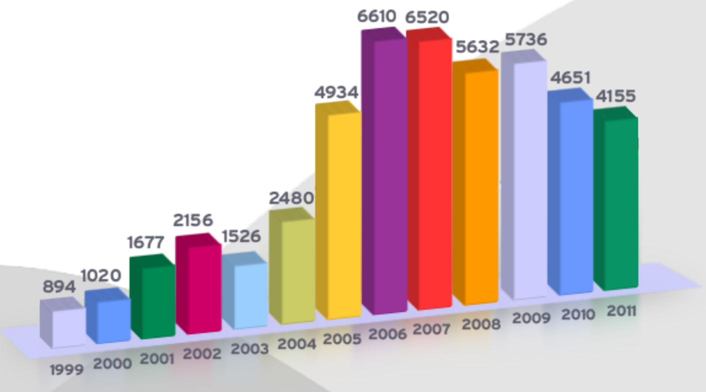
TOP 5 VENDORS BY DISTINCT NUMBER OF VULNERABILITIES

- Google
- Microsoft
- Apple
- Oracle
- Adobe[29]

[29] http://cvedetails.com/top-50-vendors.php?year=2011

> "The trends that we saw in 2011 are going to continue in 2012. We will just see attacks become more complicated."[34]
>
> —Pawan Kinger,
> Trend Micro Vulnerability
> Research Manager

[34] http://blog.trendmicro.com/2011-in-review-exploits-and-vulnerabilities/



VOLUME OF REPORTED VULNERABILITIES, 1999–2011

Malware, spam, and malicious links continued to cause users grief, wreaking havoc in innumerable ways. Malware such as SpyEye,[35] KOOBFACE,[36] FAKEAV,[37] and other variants underwent further enhancements in order to spread more malice while evading detection. Spam sporting malicious links, meanwhile, have become multiplatform threats, invading not just users' systems but also their mobile devices.[38] Malicious links leading to all kinds of web threats continued to riddle direct messages and posts in various social networking sites. Whether utilized as separate infection tools or combined to form more powerful multipronged threats, malware, spam, and malicious links lived on as part of the threat landscape's white noise, allowing cybercriminals to profit from selling stolen data.

[35] http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/from_russia_to_hollywood-turning_the_tables_on_a_spyeye_cybercrime_ring.pdf

[36] http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/more_traffic__more_money-koobface_draws_more_blood.pdf

[37] http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/targeting_the_source-fakeav_affiliate_networks.pdf

[38] http://us.trendmicro.com/imperia/md/content/us/pdf/trendwatch/spam_trends_in_today_s_business_world.pdf

2011 continued to be plagued by attacks that made use of traditional vectors, which refused to quietly fade into the background.

2011 PREDICTION

We will see old malware reinfections and consolidation in the cybercriminal underground.

CREDIT CARD NUMBER VALUE IN THE CYBERCRIMINAL UNDERGROUND

US$1–3	per U.S.-based number
US$3–8	per Central America-, Australia-, and Europe-based number
US$6–10	per number in Asia, the Middle East, and other countries

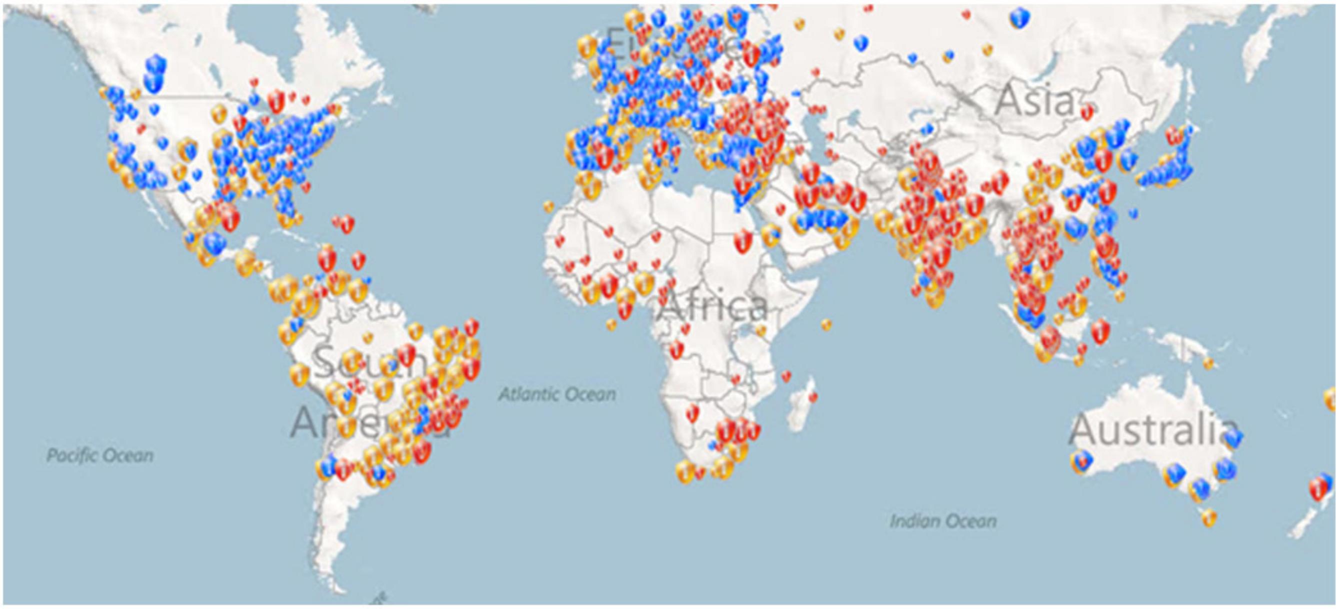
The KOOBFACE botnet creates **~7,900** tweets, **2,200** *AOL Lifestream* posts, **1,700** *FriendFeed* posts in just **1** hour.

PayPal and *eBay* are **2** of the most commonly phished sites.[41]

1 verified *PayPal* account (i.e., attached to a credit card or bank account) costs **US$1–6** when sold underground.[39]

> "3.5 new threats are created every second. As more and more businesses and home users take the inevitable journey to the cloud, risks of data and financial loss are greater than ever."[40]
>
> –Trend Micro

~3 of 4 spam attachments are malicious in nature.



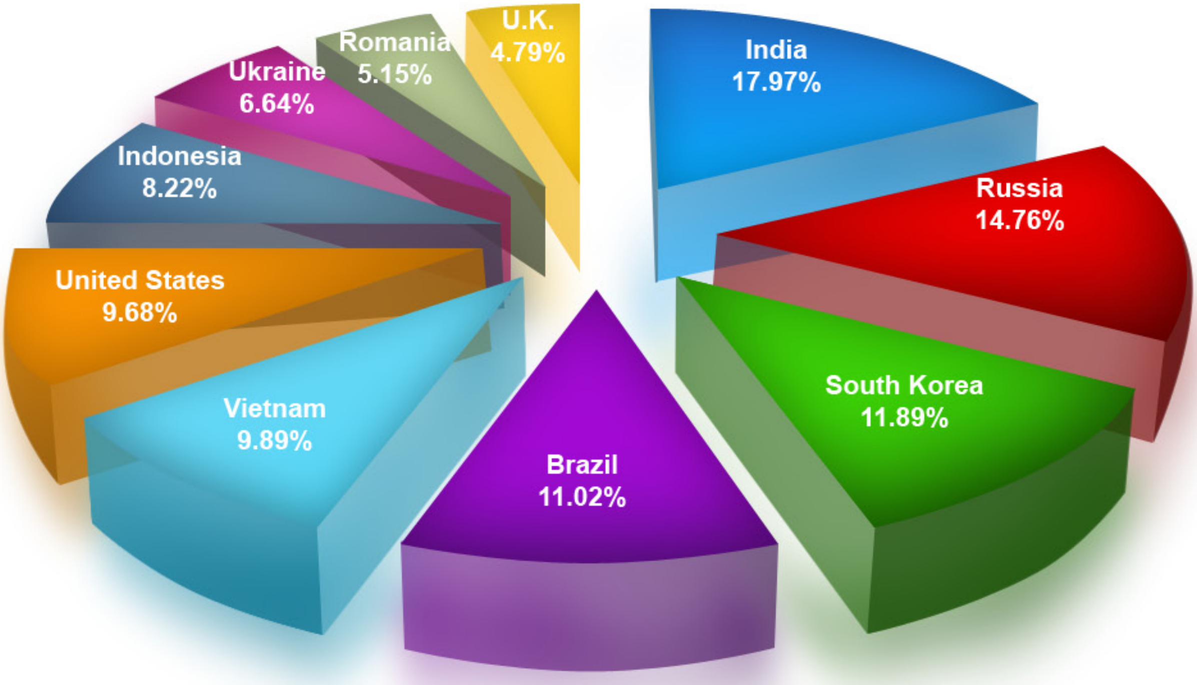
Legend: Yellow - DOWNAD; blue – KEYGEN; red – SALITY

* Shows the top 3 malware volume Trend Micro protected customers all over the world from

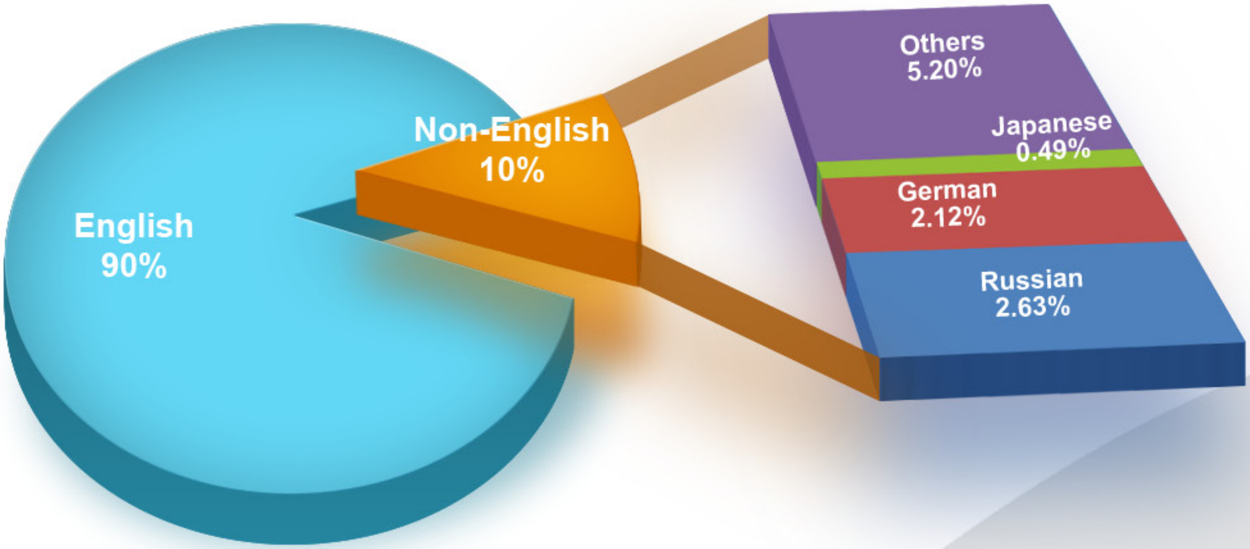
[39] http://blog.trendmicro.com/tricks-and-threats/

[40] http://blog.trendmicro.com/threat-morphosis/

[41] http://blog.trendmicro.com/online-shopping-safety-tips-infographic/

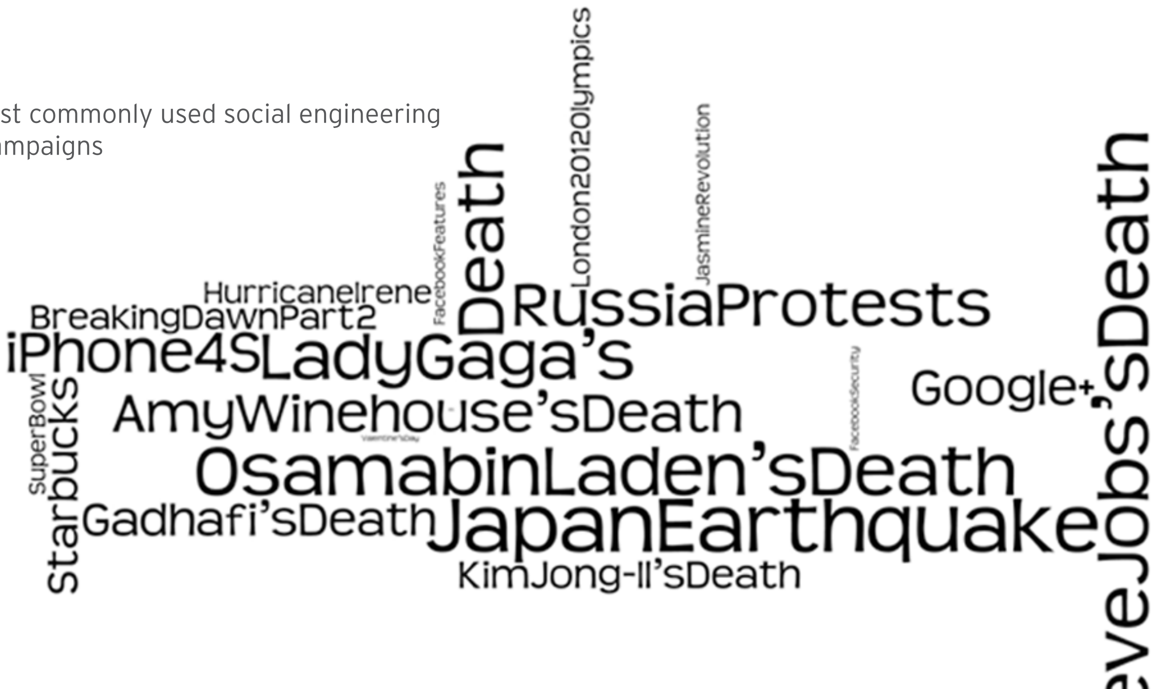


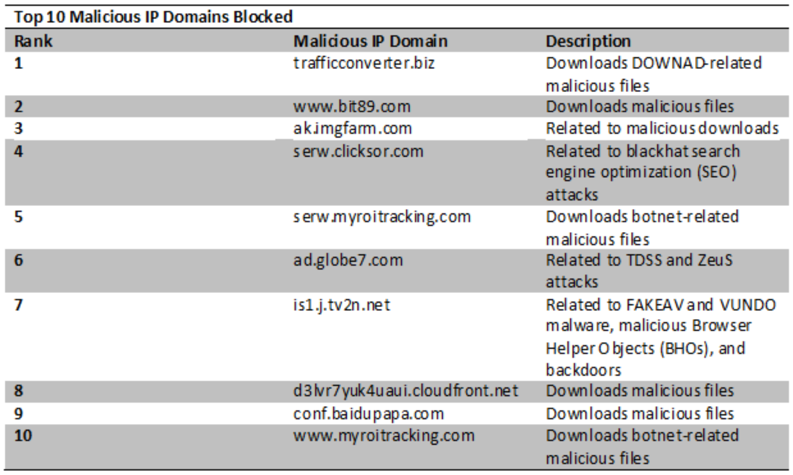
* Shows the top 10 spamming countries Trend Micro protected customers against



* Shows the proportion of English to non-English spam Trend Micro protected customers against

* Shows 20 of the most commonly used social engineering lures for 2011 spam campaigns

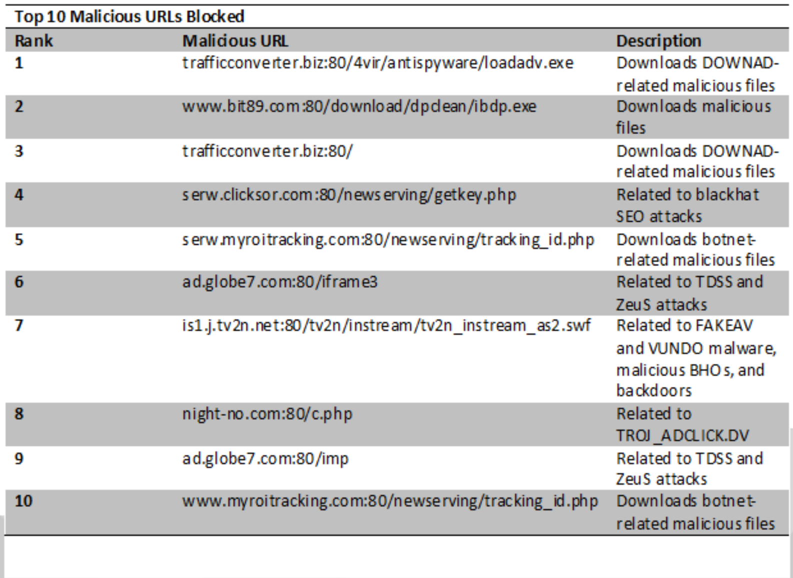




Top 10 Malicious IP Domains Blocked

Rank	Malicious IP Domain	Description
1	trafficconverter.biz	Downloads DOWNAD-related malicious files
2	www.bit89.com	Downloads malicious files
3	ak.imgfarm.com	Related to malicious downloads
4	serw.clicksor.com	Related to blackhat search engine optimization (SEO) attacks
5	serw.myroitracking.com	Downloads botnet-related malicious files
6	ad.globe7.com	Related to TDSS and ZeuS attacks
7	is1.j.tv2n.net	Related to FAKEAV and VUNDO malware, malicious Browser Helper Objects (BHOs), and backdoors
8	d3lvr7yuk4uaui.cloudfront.net	Downloads malicious files
9	conf.baidupapa.com	Downloads malicious files
10	www.myroitracking.com	Downloads botnet-related malicious files

* Shows the top 10 malicious IP domains Trend Micro blocked customer access to



Top 10 Malicious URLs Blocked

Rank	Malicious URL	Description
1	trafficconverter.biz:80/4vir/antispyware/loadadv.exe	Downloads DOWNAD-related malicious files
2	www.bit89.com:80/download/dpclean/ibdp.exe	Downloads malicious files
3	trafficconverter.biz:80/	Downloads DOWNAD-related malicious files
4	serw.clicksor.com:80/newserving/getkey.php	Related to blackhat SEO attacks
5	serw.myroitracking.com:80/newserving/tracking_id.php	Downloads botnet-related malicious files
6	ad.globe7.com:80/iframe3	Related to TDSS and ZeuS attacks
7	is1.j.tv2n.net:80/tv2n/instream/tv2n_instream_as2.swf	Related to FAKEAV and VUNDO malware, malicious BHOs, and backdoors
8	night-no.com:80/c.php	Related to TROJ_ADCLICK.DV
9	ad.globe7.com:80/imp	Related to TDSS and ZeuS attacks
10	www.myroitracking.com:80/newserving/tracking_id.php	Downloads botnet-related malicious files

* Shows the top 10 malicious URLs Trend Micro blocked customer access to

Hacktivist groups such as Anonymous, under the Operation AntiSec banner, and LulzSec, as in years past, continued to cast their nasty nets over Internet users. Disgruntled with various political issues, members of hacktivist groups worldwide launched a plethora of attacks against carefully chosen targets. In 2011, hacktivists who used to focus on launching distributed denial-of-service (DDoS) attacks instead trailed their targets on stealing data. Despite news of LulzSec's disbandment, attacks continued to ensue, partly owing to the decentralized nature of hactivist groups.[42]

2011 witnessed the emergence of new threat actors with politically charged agendas.

[42] http://blog.trendmicro.com/lulzsec-disbands-now-what/

STRATFOR HACKTIVIST ATTACK

- Some of the organization's members' personally identifiable information (PII), including credit card data, was publicly disclosed on December 24, 2011
- A list of the organization's members, classified as "private clients," was also released to the public[43]
- Anonymous, which was believed to have been behind the attack, denied its involvement[44]
- LulzSec's supposed leader, Sabu, claimed to have been responsible for the attack[45]

[43] https://www.facebook.com/stratfor/posts/10150456418503429
[44] http://pastebin.com/8yrwyNkt
[45] https://twitter.com/#!/anonymouSabu/status/151141501492137986

PII STOLEN DURING THE STRATFOR HACKTIVIST ATTACK

68,063	unique credit card numbers, **~36,000** of which had yet to expire
859,311	unique email addresses
50,569	phone numbers
860,160	hashed passwords, **~11.8%** could be easily cracked
7.2	average number of characters in passwords
50,618	email addresses that belonged to U.S.-based victims[47]

[47] http://www.identityfinder.com/blog/post/Update-Identity-Finder-Releases-New-Analysis-of-StratforAnonymous-Breach3b-Warns-Victims-to-Beware-of-Phishing-and-Change-Passwords.aspx

> "We don't believe that the people behind LulzSec have stopped their activities. Instead, they disbanded due to the attention they were getting from law enforcement and other hackers less approving of their activities."[46]
>
> —Kevin Stevens,
> Trend Micro Senior
> Threat Researcher

[46] http://blog.trendmicro.com/lulzsec-disbands-now-what/

750,000	number of users affected by the hactivist attack against Stratfor[48]

[48] http://news.hitb.org/content/lulzsecs-topiary-had-750000-passwords-his-posession

Despite being another challenging year, 2011 also proved to be a successful one for both the security industry and its fellow cybercrimefighters. Before 2011 drew to a close, we saw various cybercriminal operations close down as well. Trend Micro, for its part, fought side by side with its industry partners and law enforcement agencies worldwide in bringing down what has been dubbed the "Biggest Cybercriminal Takedown in History."[49]

2011 marked significant wins for Trend Micro, along with its industry partners and law enforcement authorities, in the fight against cybercrime.

[49] http://blog.trendmicro.com/esthost-taken-down-biggest-cybercriminal-takedown-in-history/

RUSTOCK BOTNET TAKEDOWN

- The Rustock botnet was taken down by Microsoft on March 16, 2011
- TrendLabs data showed a **>95%** decrease in Rustock spam on March 16, at around the same time the botnet was taken down[50]
- Microsoft published ads in Russian newspapers that offered a **US$250,000** reward to anyone who gave information that led to the identification, arrest, and conviction of the Rustock gang members
- Microsoft's lawyers used novel legal arguments to convince a federal court in Seattle that it had the right to seize Rustock's servers, which set an important legal precedent for future cases

[50] http://blog.trendmicro.com/the-final-nail-on-rustock's-coffin–or-is-it/

KELIHOS BOTNET TAKEDOWN

- Microsoft convinced a federal judge to allow it to block all of Kelihos's command-and-control (C&C) servers' IP addresses in September 2011 without first informing their owners
- The *cz.cc* domain owner was explicitly named in the complaint
- The *cz.cc* domain takedown took hundreds of thousands Kelihos's subdomains offline, setting an example for all other rogue second-level domains (SLDs) to be more accountable for abuse incidents

> "2011 proved that collaboration between law-enforcement authorities and the security industry can have a major impact. For major cybercriminals, it is no longer a question of ever getting arrested but when."
>
> –Feike Hacquebord,
> Trend Micro Senior
> Threat Researcher

COREFLOOD TAKEDOWN

- The takedown was facilitated by the U.S. Department of Justice (DOJ) and by the Federal Bureau of Investigation (FBI)[51]
- The FBI took over CoreFlood's C&C servers and operated these until mid-June 2011
- The FBI sent a stop command to the bots in the United States, causing the malware to exit systems
- Marked the first time the U.S. government took over a botnet's C&C infrastructure and pushed a command to its bots so these became unreachable to botmasters

[51] http://blog.trendmicro.com/a-win-for-the-good-guys-the-coreflood-takedown/

OPERATION GHOST CLICK

- Trend Micro and its industry partners, along with the FBI and the Estonian Police Force, took down **>4M** bots on November 8, 2011
- The FBI raided two data centers in New York City and Chicago as well as took down Rove Digital's C&C infrastructure, which comprised **>100** servers
- **6** suspects were arrested in Estonia, including Rove Digital CEO, Vladimir Tsastsin, and spokesperson, Konstantin Poltev
- Banking accounts with millions of cash were frozen and other assets were confiscated

CHRONOPAY TAKEDOWN

- Co-founder and CEO of credit card clearinghouse Chronopay, Pavel Vrublevsky, was arrested in Russia for an alleged cyber attack against a competitor in June 2011
- Another major Chronopay shareholder—Rove Digital CEO, Vladimir Tsastsin—was arrested as part of Operation Ghost Click

OPERATION TRIDENT BREACH

- The Security Service of the Ukraine (SBU) detained key members of the Trident Breach gang on September 30, 2010
- **8** search warrants were executed by **~50** SBU officers and its elite tactical operations teams
- Targeting small and medium-sized businesses (SMBs), municipalities, churches, and individuals as well as infecting their systems with ZeuS malware, the gang's scheme resulted in the attempted theft of **US$220M,** with actual losses of **US$70M** from victims' bank accounts
- The FBI, the New York Money Mule Working Group, the Newark Cybercrime Task Force, the Omaha Cybercrime Task Force, the Netherlands Police Agency, the SBU, and the United Kingdom's Metropolitan Police Service participated in Operation Trident Breach[52]

[52] http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring

This year, as we look ahead, we've come up with 12 predictions for 2012 that fall into four main categories:

Big IT trends

Mobile landscape

Threat landscape

Data leaks and breaches

In looking at these predictions, what we see in common are trends toward ever more sophisticated attackers and away from the PC-centric desktop. Our hope that new OSs make the world a safer place didn't work out. This means that our customers in 2012 will need to continue moving toward a more data-centric model for effective security and privacy as they embrace consumerization, virtualization, and the cloud. And we here at Trend Micro need to continue our work in these key areas to help enable our customers to meet and protect against these threat trends in 2012.[53]

Raimund

Raimund Genes,
Trend Micro CTO

[53] http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/12_security_predictions_for_2012.pdf

TREND MICRO™

Trend Micro Incorporated, 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 Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 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.

TREND MICRO™

Securing Your Journey
to the Cloud

TrendLabs
Global Technical Support & R&D Center of TREND MICRO