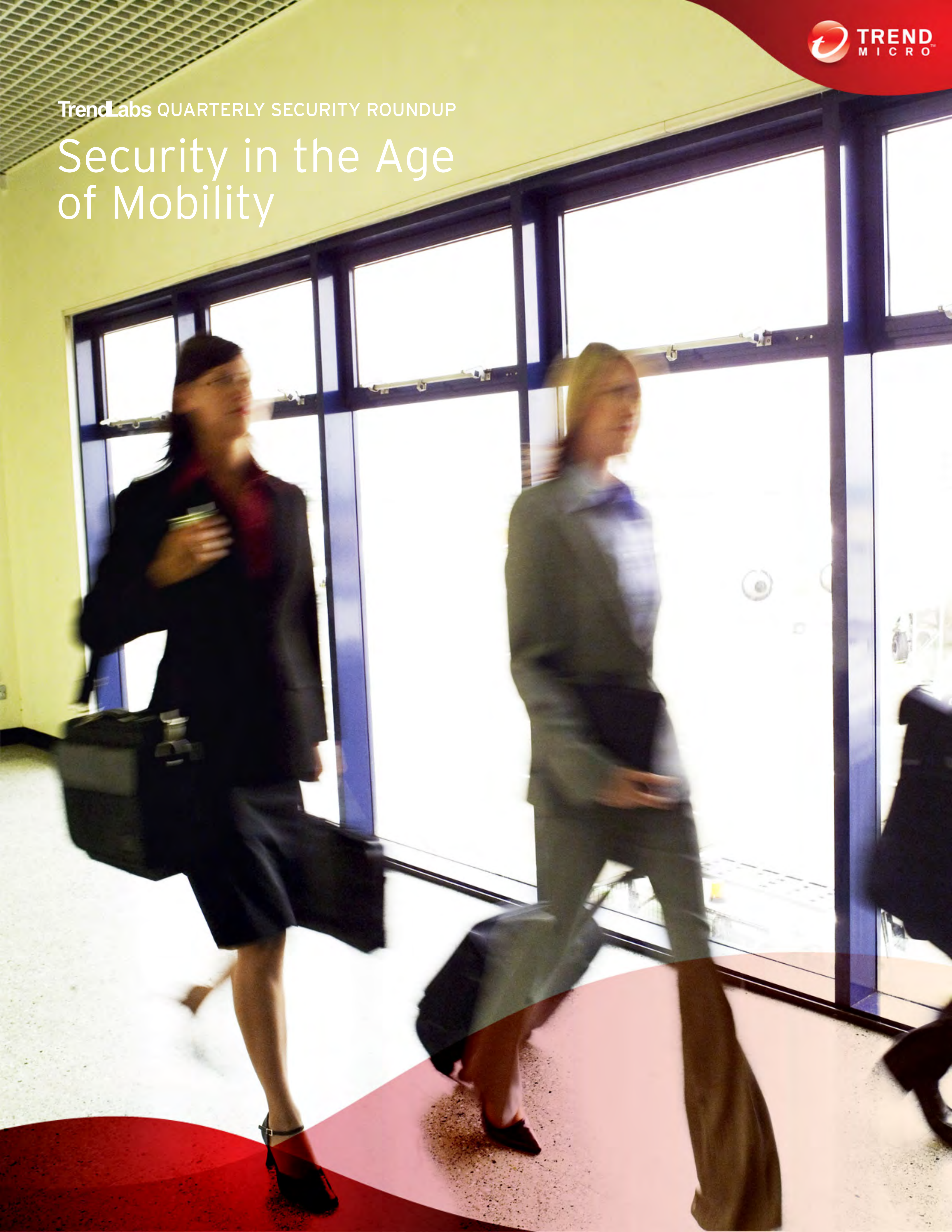
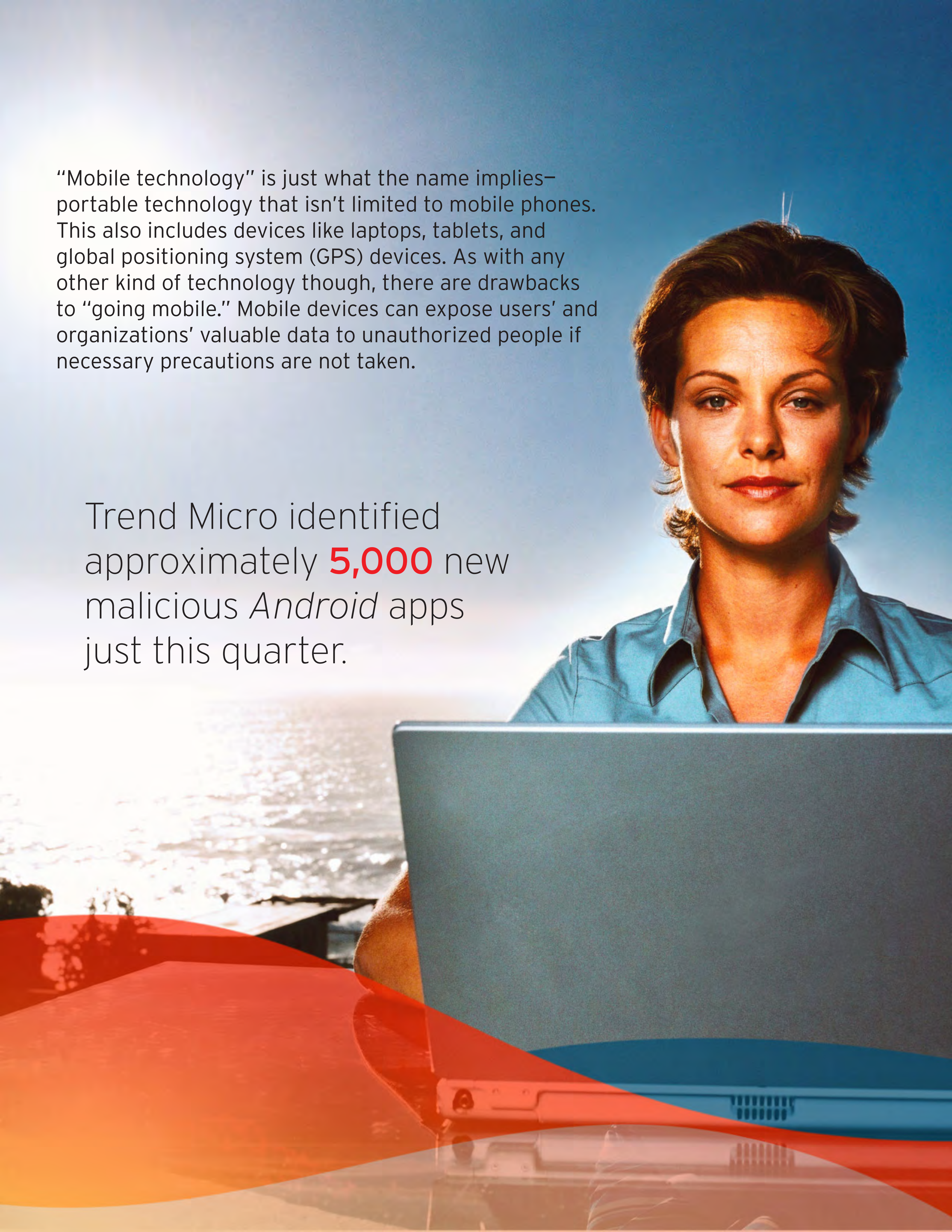
TrendLabs QUARTERLY SECURITY ROUNDUP

Security in the Age of Mobility



“Mobile technology” is just what the name implies–portable technology that isn’t limited to mobile phones. This also includes devices like laptops, tablets, and global positioning system (GPS) devices. As with any other kind of technology though, there are drawbacks to “going mobile.” Mobile devices can expose users’ and organizations’ valuable data to unauthorized people if necessary precautions are not taken.

Trend Micro identified approximately **5,000** new malicious *Android* apps just this quarter.



CONTENTS

True to one of our mobile threat predictions, *Android*-based smartphones suffered from more cybercriminal attacks this quarter. A Google/Ipsos poll found that users are increasingly using their smartphones to surf the web.[1] Germany, in particular, recorded the biggest jump from 39% to 49%. With the increased use of smartphones for Internet access and the huge *Android* user base, the increase in attacks targeting the platform is thus not surprising.

[1] http://googlemobileads.blogspot.com/2012/01/new-research-global-surge-in-smartphone.html

As predicted...

- Smartphone and tablet platforms, especially *Android*, will suffer from more cybercriminal attacks.
- Security vulnerabilities will be found in legitimate mobile apps, making data extraction easier for cybercriminals.

* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp_12-security-predictions-for-2012.pdf

> "One big reason for the popularity of apps is their ease of use. Browsing the net on your mobile phone is not the same experience as doing it on a laptop... The key thing to remember is to think before you give an app access to your data... If you have any doubts about giving oversensitive information, just don't do it."
>
> – Robert McArdle, Trend Micro
> Senior Threat Researcher

* http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Mobile+Apps%3a+New+Frontier+for+Cybercrime

ONE-CLICK BILLING FRAUD SCHEMES

- Target users who go to video-sharing sites or blogs with adult content[2]
- Charge victims higher fees amounting to as much as ¥99,800 (approximately US$1,300) compared with scareware and FAKEAV in Japan[3]
- Now target *Android*-based smartphone users, too[4]

[2] http://blog.trendmicro.com/the-ins-and-outs-of-one-click-billing-fraud/
[3] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=One-Click+Billing+Fraud+Tricks
[4] http://blog.trendmicro.com/one-click-billing-fraud-scheme-through-android-app-found/

FAKE "TEMPLE RUN" AND OTHER BOGUS *ANDROID* APPS

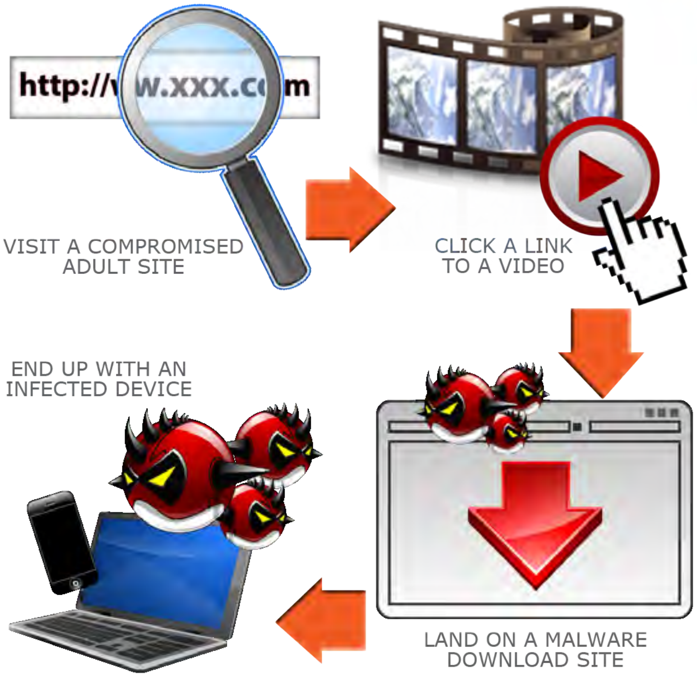
- Seen in *Google Play* (formerly the *Android Market*), the fake "Temple Run" app displayed bothersome ads via notifications[5]
- Fake "Temple Run" app also created shortcuts on infected devices' home screens[6]
- Fake Russian *Google Play* site also hosted a premium mobile service abuser that left victims with unwanted phone charges[7]
- Fake smartphone optimizer apps for *Android* and *Symbian* were also found hosted on a German server[8]
- A PLANKTON variant was found embedded in various *Android* apps, which led to the "largest *Android* malware outbreak ever"
- Apps categorized as "adware" installed shortcuts that triggered ad serving in infected phones[9]

[5] http://blog.trendmicro.com/fake-version-of-temple-run-unearthed-in-the-wild/
[6] http://blog.trendmicro.com/fan-apps-now-spreading-on-the-android-market/
[7] http://blog.trendmicro.com/fake-google-play-site-leads-to-rogue-apk-app/
[8] http://blog.trendmicro.com/malicious-mobile-apps-found-hosted-in-german-ip-address/
[9] http://blog.trendmicro.com/search-monetization-as-a-new-threat-to-the-mobile-platform/

Japanese police arrested **6** suspects in relation to a one-click billing fraud campaign that netted **¥12M** (around **US$148,800**).

* http://www.theregister.co.uk/2012/01/19/japanese_cops_cuff_smut_trojan_suspects/

TYPICAL ONE-CLICK BILLING FRAUD SCHEME INFECTION DIAGRAM


http://www.xxx.com
VISIT A COMPROMISED ADULT SITE
CLICK A LINK TO A VIDEO
LAND ON A MALWARE DOWNLOAD SITE
END UP WITH AN INFECTED DEVICE

When installing apps in your smartphone...

- Be ready to give out some personal information.
- Know that a third-party will gain access to your information.
- Know the app developer's reputation.

* http://blog.trendmicro.com/3-truths-about-mobile-applications/

As the name suggests, advanced persistent threats (APTs) typically exhibit persistent behavior.[10] These are normally considered "campaigns" rather than "smash-and-grab incidents," as attackers need to go deep into a target's network to get what they want. The very act of doing business these days prompted by trends like consumerization and outsourcing as well as interacting with new technologies, platforms, and entities can only further broaden the attack surface.

[10] http://www.trendmicro.com/cloud-content/us/pdfs/about/wp_trends-in-targeted-attacks.pdf

As predicted...

- Though many organizations are still uncomfortable with consumerization, security and data breach incidents in 2012 will force them to face bring-your-own-device (BYOD)-related challenges.
- More high-profile data loss incidents via malware infection and hacking will occur in 2012.

> "It is more useful to think of highly targeted attacks as campaigns—a series of failed and successful attempts to compromise a target's network over a certain period of time... As the attackers learn more about their targets from open source research—relying on publicly available information as well as previous attacks, the specificity of the attacks may sharply increase."
>
> — Trend Micro Forward-Looking Threat Research Team

* http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Luckycat+Leads+to+Attacks+Against+Several+Industries

LUCKYCAT CAMPAIGN

- Active since at least June 2011
- Linked to 90 attacks targeting several industries in Japan and India as well as Tibetan activists
- Exploited several vulnerabilities in *Microsoft Office* as well as *Adobe Reader, Acrobat,* and *Flash Player* via specially crafted email attachments
- Heavily used free web-hosting services for command-and-control (C&C) servers, allowing the attackers to cover their tracks
- Managed to compromise 233 computers, from which confidential data was stolen[11]

[11] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf

The Luckycat campaign targeted the following industries and/or communities:

- Aerospace
- Energy
- Engineering
- Military research
- Shipping
- Tibetan activists

* http://blog.trendmicro.com/luckycat-redux-inside-an-apt-campaign/

>174M records were compromised in 855 data breach incidents in 2011.

* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

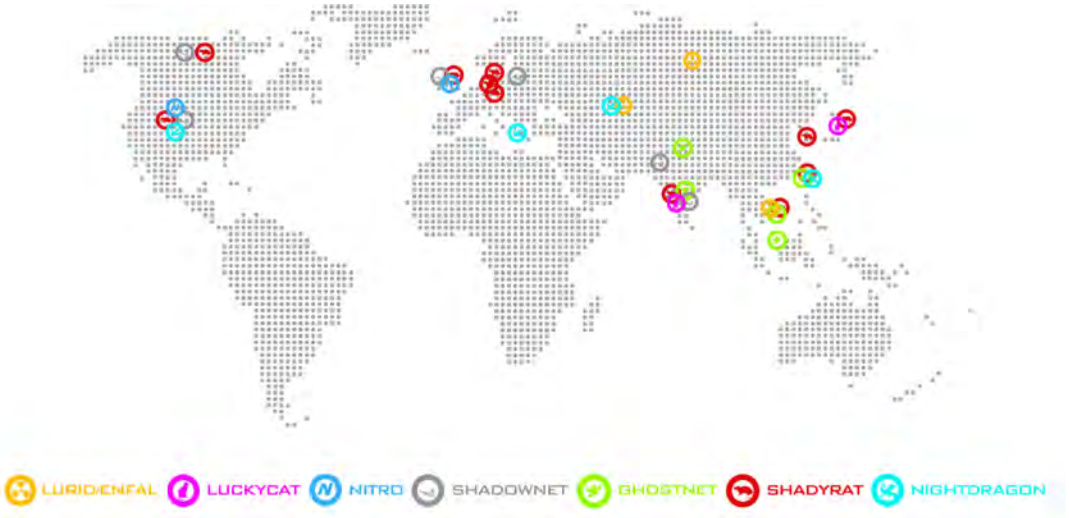
LINSANITY AND SOCIOPOLITICAL EVENTS AS TARGETED ATTACK LURES

- NBA superstar Jeremy Lin's name was recently used as a social engineering lure for the LURID/Enfal campaign[12]
- An email on the Tibetan protests supposedly from the German Chancellor came with a malicious .DOC file attachment that exploited a *Microsoft Word* vulnerability[13]

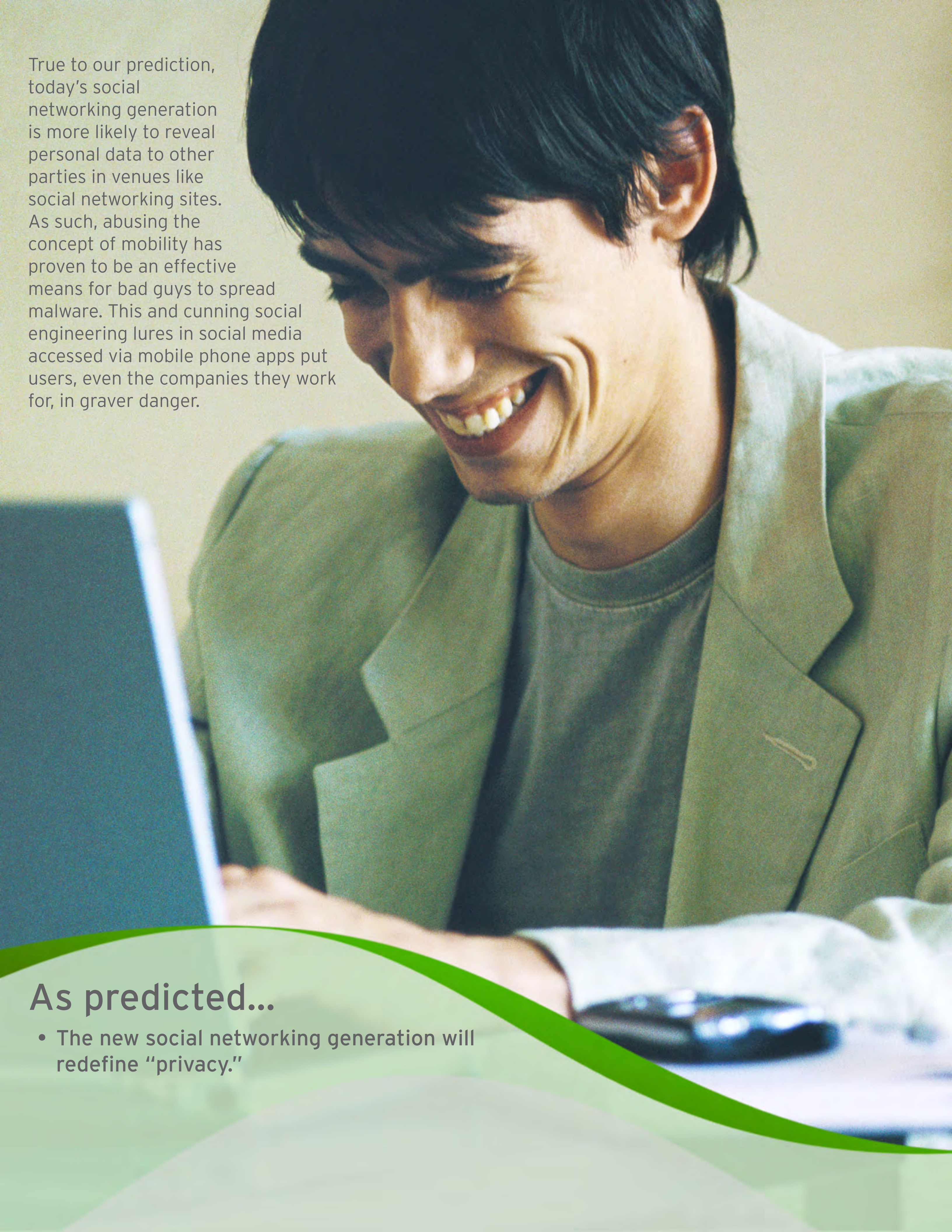
[12] http://blog.trendmicro.com/linsanity-leads-to-targeted-malware-attacks/

[13] http://blog.trendmicro.com/malicious-email-campaign-uses-current-socio-political-events-as-lure-for-targeted-attack/

APT CAMPAIGN TARGET COUNTRIES



* Shows countries infected with malware used in publicly reported APT campaigns featured in http://blog.trendmicro.com/global-targets-infographic/



True to our prediction, today's social networking generation is more likely to reveal personal data to other parties in venues like social networking sites. As such, abusing the concept of mobility has proven to be an effective means for bad guys to spread malware. This and cunning social engineering lures in social media accessed via mobile phone apps put users, even the companies they work for, in graver danger.

As predicted...

- The new social networking generation will redefine "privacy."

> "Social networking accounts are even more useful for cybercriminals because besides plundering your friends' email addresses, the bad guys can also send bad links around and try to steal the social networking credentials of your friends. There is a reason why there is a price for stolen social networking accounts."
>
> – David Sancho, Trend Micro
> Senior Threat Researcher

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

EMAIL HOAXES AND SCAMS

- Free "iPad 3" giveaway promos stirred up interest in the product even before its launch and infected systems with malware[14]
- *Twitter* spam touting free McDonald's gift cards redirected users to adult dating sites[15]
- Tax season was also used as a social engineering bait to distribute malware and instigate phishing attacks[16]
- Whitney Houston's sudden demise was the talk of the town, much to cybercriminals' delight, as this allowed them to spread malice[17]

[14] http://blog.trendmicro.com/free-ipad-3-scam-steer-users-to-bad-sites/
[15] http://blog.trendmicro.com/mcdonalds-gift-card-spam-on-twitter/
[16] http://blog.trendmicro.com/tax-season-opens-tax-spam-follows/
[17] http://blog.trendmicro.com/cybercriminals-leverage-whitney-houstons-death/

PINTEREST

- New social networking site, *Pinterest,* gained not just popularity but also notoriety
- Site users were drawn into "re-pinning" a Starbucks logo to get supposed gift cards but instead got malware[18]

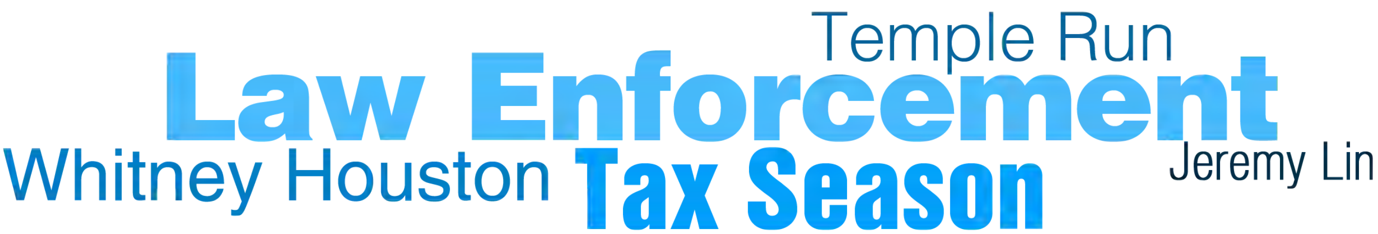
[18] http://blog.trendmicro.com/survey-scams-find-their-way-into-pinterest/

SOCIAL NETWORKING BY NUMBERS

- *Facebook*
  - **845M** active users per month
  - **483M** active users per day
- *Twitter*
  - **140M** active users
  - **340M** Tweets a day
- *Pinterest*
  - **11.7M** unique visitors per month
- *LinkedIn*
  - **>150M** users
- *Google+*
  - **>100M** active users

* http://newsroom.fb.com/content/default.aspx?NewsAreaId=22; http://blog.twitter.com/2012/03/twitter-turns-six.html; http://techcrunch.com/2012/02/07/pinterest-monthly-uniques/; http://press.linkedin.com/about; http://investor.google.com/corporate/2012/ceo-letter.html

TOP 5 SOCIAL ENGINEERING LURES



* Based on Trend Micro noteworthy incident tracking

Exploitable vulnerabilities continued to be the bane of every IT administrator. The number of reported vulnerabilities this quarter showed that threats can easily spread among systems and possibly even mobile devices. The most notable of the publicly disclosed vulnerabilities, *MS12-020*, shows that target devices are susceptible to attacks anytime, anywhere when remotely accessed.[19]

[19] http://technet.microsoft.com/en-us/security/bulletin/MS12-020

As predicted...

- Though many organizations are still uncomfortable with consumerization, security and data breach incidents in 2012 will force them to face BYOD-related challenges.

> "While this is not enabled by default on *Windows* systems, Remote Desktop Protocol (RDP) provides remote access functionality that many environments utilize, thus potentially putting them at risk."
>
> – Pawan Kinger, Trend Micro Operations Manager on the *MS12-020* vulnerability

* http://blog.trendmicro.com/a-deeper-look-into-the-critical-flaw-in-windows-remote-desktop-protocol-server/

MS12-020 (CVE-2012-0002)

- Exploits a *Microsoft Windows* RDP vulnerability that allows remote code execution
- Has been rated "critical" because it can be exploited even by unauthenticated users
- Affects all *Windows* versions[20]
- Has been patched last March 13[21]

[20] http://about-threats.trendmicro.com/vulnerability.aspx?language=us&name=(MS12-020)%20Vulnerabilities%20in%20Remote%20Desktop%20Could%20Allow%20Remote%20Code%20Execution%20(2671387)

[21] http://blog.trendmicro.com/march-2012-patch-tuesday-includes-fix-for-critical-rdp-vulnerability/

Apart from posting the highest number of reported vulnerabilities, Apple also issued a record-breaking number of patches last March.

* http://www.computerworld.com/s/article/9225130/Apple_patches_record_number_of_Safari_5_bugs_with_monster_update

CVE-2012-0002 was given the highest rating on Microsoft's exploitability index, as the vulnerability is an "attractive target for attackers" because they "could consistently exploit it."

* http://www.networkworld.com/news/2012/031312-microsoft-patch-tuesday-257244.html

MIDI REMOTE CODE EXECUTION VULNERABILITY *(CVE-2012-0003)*

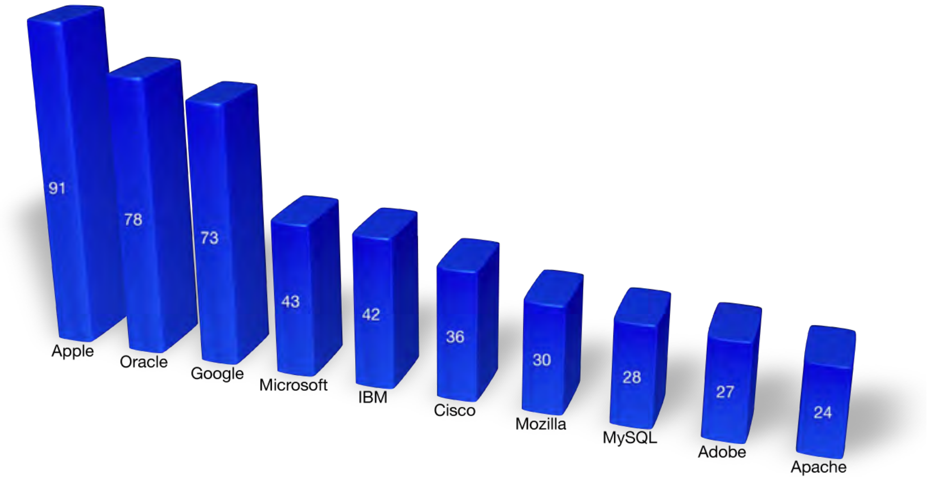
- Is triggered when the Windows Multimedia Library in *Windows Media Player (WMP)* fails to handle a specially crafted .MIDI file[22]
- Allows remote attackers to execute arbitrary code on vulnerable systems[23]
- Allows malicious users to steal information from infected systems[24]

[22] http://blog.trendmicro.com/malware-leveraging-midi-remote-code-execution-vulnerability-found/

[23] http://technet.microsoft.com/en-us/security/bulletin/ms12-004

[24] http://about-threats.trendmicro.com/Vulnerability.aspx?language=us&name=(MS12-004)+Vulnerabilities+in+Windows+Media+Could+Allow+Remote+Code+Execution+(2636391)

TOP 10 VENDORS BY DISTINCT NUMBER OF VULNERABILITIES



* Shows the vendors of the most vulnerable OS/software from January to March 2012 based on data available in http://cve.mitre.org/

Blended threats are cybercriminals' answer to wreaking greater havoc among users. Developments like the reemergence of ransomware or the proliferation of spam campaigns allow the bad guys to profit off stolen data.[25] Whether on desktops or mobile devices, blended threats remained just as prominent.

[25] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Dwindling+FAKEAV+Business+Spurs+Ransomware+Infections+in+Europe

As predicted...

- Cybercriminals will find more creative ways to hide from law enforcement.
- More high-profile data loss incidents via malware infection and hacking will occur in 2012.

> "The Trend Micro Smart Protection Network processes over 4TB of data daily, including daily analyses of over 8 billion URLs, 50 million email samples, 430,000 file samples, and 200,000 IP addresses."
>
> – Trend Micro

RANSOMWARE

- Refers to a class of malware that holds systems and/or files "hostage" unless victims pay up
- Sometimes encrypt files on infected systems' hard drives
- Force victims to pay up because infection renders their systems useless[26]
- Previously concentrated in Russia but now also targets other European countries[27]

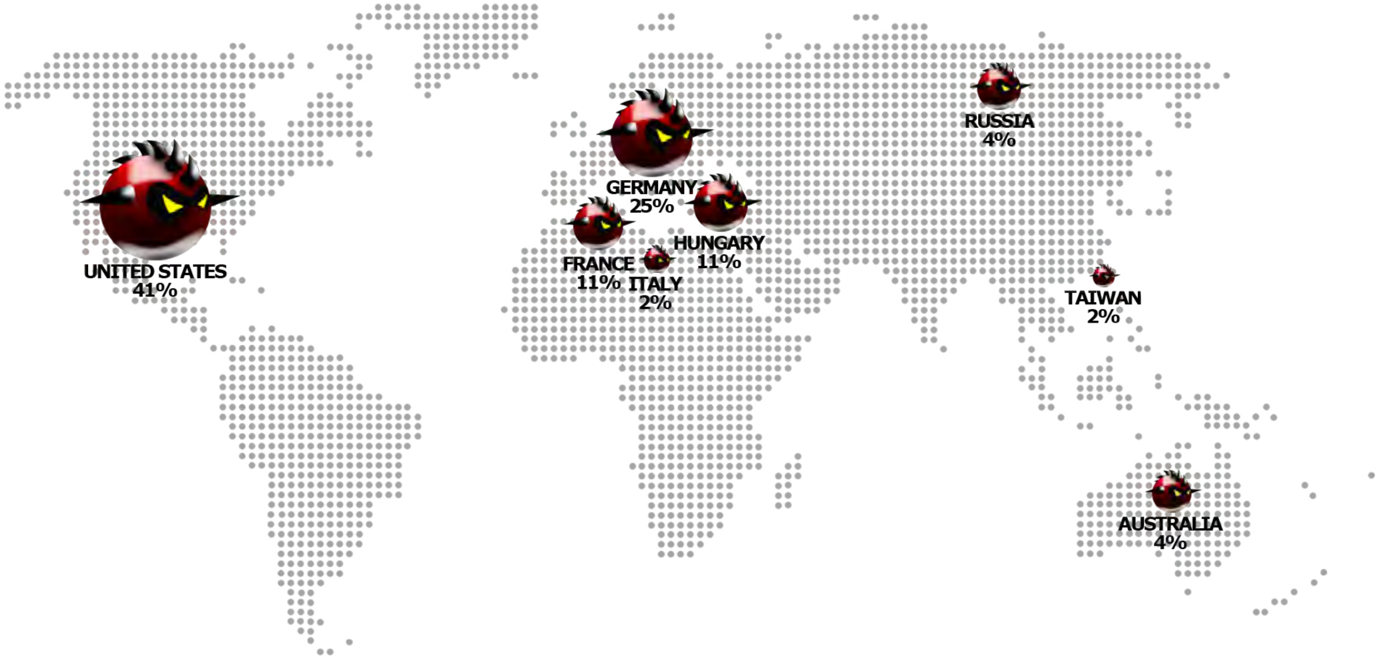
In several "Police Trojan" ransomware attacks, affected users were presented with what appears to be a police force splash screen demanding a **€100** fine for accessing Internet porn or violent materials.

* http://www.pcadvisor.co.uk/news/security/3349716/police-ransom-trojans-work-of-single-russian-gang-trend-finds/

This quarter, the Trend Micro™ Smart Protection Network™ protected product users against a total of:

- **15.3B** spam
- **338.4M** malware
- **1.3B** malicious URLs

TOP 8 RANSOMWARE-INFECTED COUNTRIES



* Trend Micro Smart Protection Network data

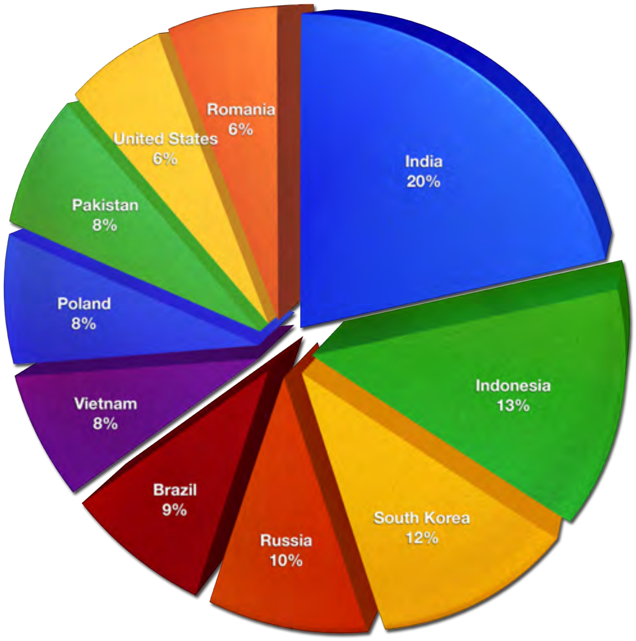
[26] http://blog.trendmicro.com/compromised-website-for-luxury-cakes-and-pastries-spreads-ransomware/

[27] http://blog.trendmicro.com/ransomware-attacks-continue-to-spread-across-europe/

SINOWAL

- Dutch site compromise loaded a malicious iframe that infected visitors' systems with a SINOWAL variant
- System information like hard disk serial number, running processes, and registered software landed on cybercriminals' eagerly waiting laps[28]

TOP 10 SPAM-SENDING COUNTRIES



* The percentage shares in this chart were computed based on the total number of spam from the top 10 countries, which account for 47.41% of the overall spam volume.
* Trend Micro Smart Protection Network data

MORE NOTABLE WEB THREATS

- Spoofed email warned recipients of a malicious campaign but instead downloaded a malicious JavaScript onto users' systems[29]
- Compromised human rights organization's site visitors' systems were infected by a backdoor that stole pertinent system information[30]
- Discovery of PoisonIvy backdoor stealth mechanism proves that the malware continues to persist[31]

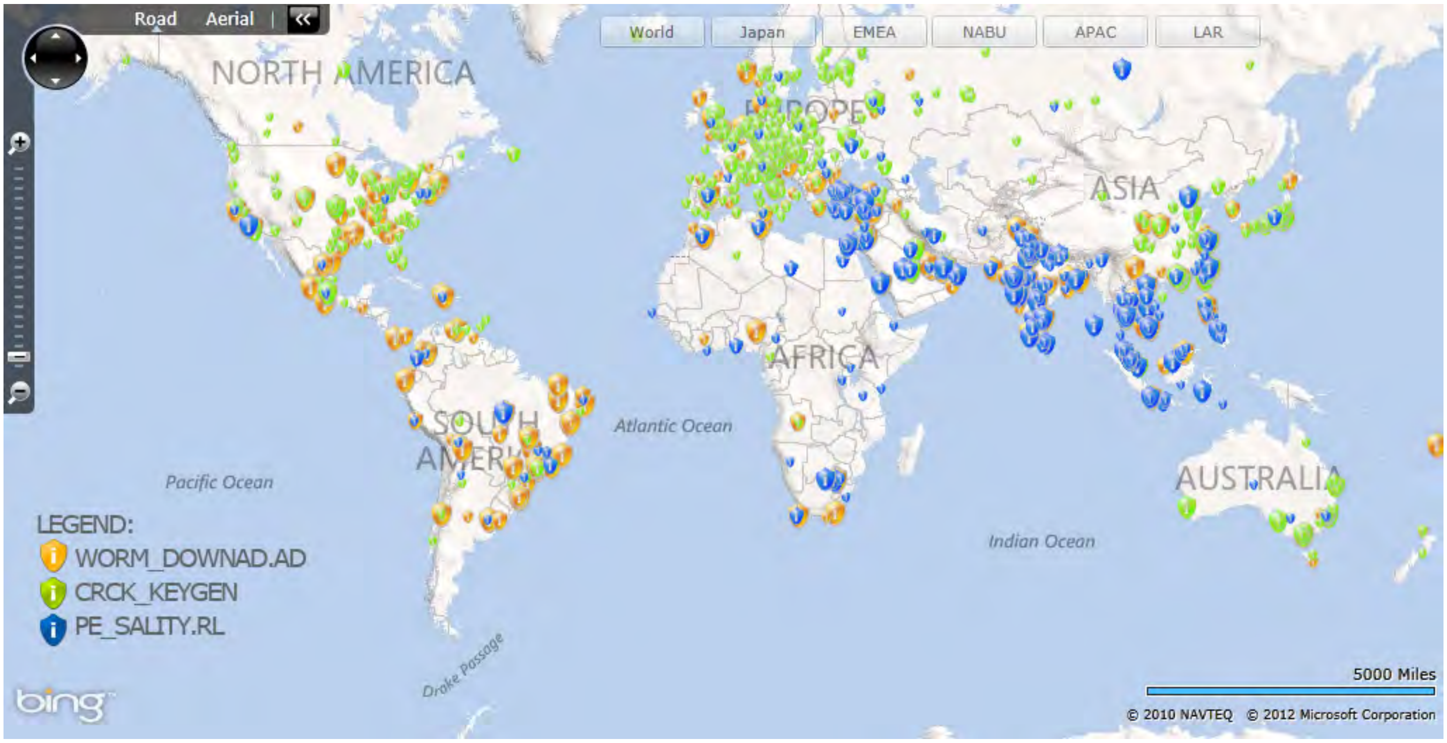
[28] http://blog.trendmicro.com/dutch-users-served-sinowal-for-lunch/

[29] http://blog.trendmicro.com/news-of-malicious-email-campaign-used-as-social-engineering-bait/

[30] http://blog.trendmicro.com/human-rights-organizations-possible-new-targets/

[31] http://blog.trendmicro.com/bkdr_poison-more-challenges-ahead/

TOP 3 MALWARE



* Exact numbers: WORM_DOWNAD.AD - 740,977; CRCK_KEYGEN - 197,330; and PE_SALITY.RL - 83,916 based on Trend Micro Smart Protection Network data

TOP 10 MALICIOUS URLS BLOCKED

MALICIOUS URL	DESCRIPTION
trafficconverter.biz:80/4vir/antispyware/loadadv.exe	Distributes malware, particularly DOWNAD variants
serw.clicksor.com:80/newserving/getkey.php	Associated with the proliferation of pirated applications and other threats
irs01.com:80/irt	Downloads malware
serw.myroitracking.com:80/newserving/tracking_id.php	Contacts various servers to download and aggressively display pop-up ads
trafficconverter.biz:80/4vir/antispyware/loadadv.ex	Distributes malware, particularly DOWNAD variants
172.168.6.21:80/c6/jhsoft.web.workflat/	Downloads malware
install.ticno.com:80/service/friendometer.php	Downloads malware
trafficconverter.biz:80/	Distributes malware, particularly DOWNAD variants
click.icetraffic.com:80/ice.php	Downloads malware
securesignupoffers.net:80/index.php	Downloads malware

* Trend Micro Smart Protection Network data

TOP 10 MALICIOUS IP DOMAINS BLOCKED

MALICIOUS IP DOMAIN	DESCRIPTION
trafficconverter.biz	Distributes malware, particularly DOWNAD variants
info.ejianlong.com	Downloads malware
serw.clicksor.com	Associated with the proliferation of pirated applications and other threats
x-web.in	Downloads malware
www.bit89.com	Downloads malware
down.game.2366.com	Downloads malware
cdn.feeds.videosz.com	Downloads malware
install.ticno.com	Downloads malware
img001.com	Downloads malware
irs01.com	Downloads malware

* Trend Micro Smart Protection Network data

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.

Securing Your Journey to the Cloud

Global Technical Support and R&D Center of TREND MICRO