



2Q THREAT ROUNDUP

TrendLabsSM



The **Trend Micro Quarterly Roundup** reports present key security highlights and developing trends in the current threat landscape.

A Quarterly Trend Micro Report | 2011



The second quarter of 2011 was marked by a spate of data breaches, vulnerability exploit attacks, the proliferation of new *Android* malware, improvements in social networking scams, as well as notable developments in traditional system infectors. Closely resembling the first quarter, albeit some improvements and enhancements in tools, targets, tactics, and scale, cybercriminals continued to instigate a myriad of malicious schemes.

IN THIS ISSUE

The second quarter of 2011 was marked by a spate of data breaches, vulnerability exploit attacks, the proliferation of new *Android* malware, improvements in social networking scams, as well as notable developments in traditional system infectors. Closely resembling the first quarter, albeit some improvements and enhancements in tools, targets, tactics, and scale, cybercriminals continued to instigate a myriad of malicious schemes.

As Trend Micro security experts predicted, the beginning of enterprises' journey to the cloud indeed ushered in data breaches of never-before-seen magnitude. This spelled disaster not only for attack targets such as Epsilon but for clients and customers as well. At the rate cybercriminals are launching attacks—targeted or not—there is no telling how many more companies and users will succumb to the dangers these pose before the year ends.

In line with the rapid shifts in the threat landscape and the never-ending slew of technological developments, we revamped our Threat Roundup reports. Instead of publishing these every month, succeeding issues will now be released on a quarterly basis. This change will allow us to give you a more in-depth view of the ever-evolving threat landscape as the shifts occur and even more valuable insights direct from our experts on what these mean for you.

DATA BREACHES AND HIGHLY TARGETED ATTACKS

Epsilon Data Breach

The recent spate of data breaches that our security experts have been seeing in the past months have been hogging the threat spotlight. In one of the most-talked-about incidents, cybercriminals hacked into Epsilon's email system, allowing them to obtain customer-related information such as clients' names and email addresses. This put 50 of the vendor's clients at risk not only of data theft but also of even more damaging spear-phishing attacks, prompting Epsilon to put up a warning on its official site and to release a tool that will supposedly help clients determine if their personal information was among those disclosed.

As usual, cybercriminals found a way to use Epsilon's solution to their advantage, most probably because they found it lucrative to exploit the vendor's over 2,000 global clients. Shortly after the tool's release, TrendLabsSM engineers were alerted to the presence of a Web page spoofing that from which the *Epsilon Secure Connect Tool* may be downloaded. As expected, the fake tool detected as TROJ_MSPOSER.ASM allowed cybercriminals to steal personally identifiable information (PII) from infected systems via a backdoor application, aka BKDR_MSPOSER.KAX.

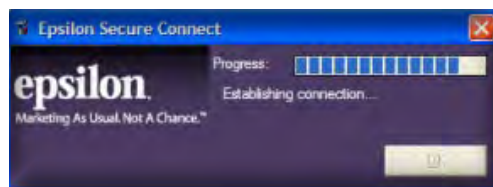


Figure 1. Graphical user interface (GUI) of the fake Epsilon Secure Connect Tool

VULNERABILITY EXPLOITS

Adobe Flash Player, Reader, and Acrobat Zero-Day Exploit

Adobe Flash Player, Reader, and Acrobat users who fell prey to the exploitation of [CVE-2011-0609](#) were again put at risk with the discovery of yet another critical vulnerability in the software. Identified as [APSA11-02](#), users who have been tricked into downloading malicious .SWF files detected as [SWF_EXPLOIT.WMP](#) embedded in specially crafted Microsoft Word documents, aka [TROJ_MDROP.WMP](#), were put at grave risk of data theft. Successful exploitation of the said zero-day vulnerability leads to the dropping and consequent execution of a backdoor application detected as [BKDR_SHARK.WMP](#), which stole PII.

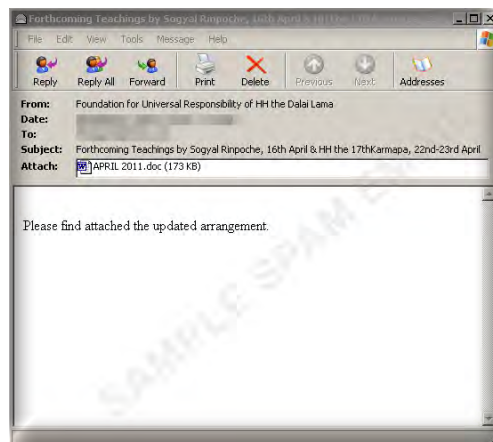


Figure 2. Spam carrying the .SWF exploit

Hotmail Vulnerability Exploit

A targeted attack put [Hotmail users](#) at risk of losing PII with the simple act of previewing a spammed message that prompted the download of [JS_AGENT.SMJ](#) from a remote URL. Upon further investigation, TrendLabs engineers discovered that the attack was made possible by a previously unpatched Hotmail bug, aka [CVE-2011-1252](#). The spammed message used in the attack, aka [HTML_AGENT.SMJ](#), triggers a request to the Hotmail server that sends all of the affected users' email messages to certain addresses. Email message forwarding, however, will only work within the session when the script was executed and will stop once users log off.

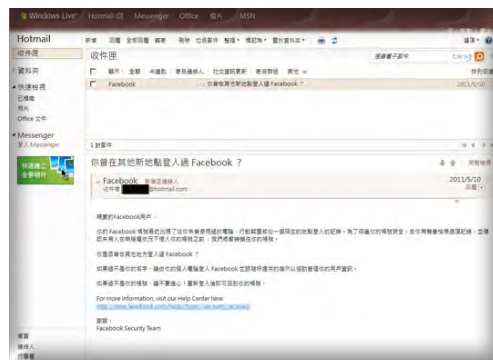


Figure 3. Hotmail spam sample

Vulnerability Statistics

The first quarter's top vendor target—Apple—was ousted by Microsoft this quarter, which is not surprising since despite the greater attention Apple's products have been getting, the number of Windows-based system users still hugely outnumber that of Mac users. The previous quarter's second and third placers—Google and Adobe—however, retained their posts.





The number of exploit attacks in the first six months of the year has been dropping. If this trend continues, we can probably expect the months of the third and of the fourth quarters to post even smaller numbers.

Rank	1Q 2011		2Q 2011	
	Target Vendor	Number of Exploit Attacks	Target Vendor	Number of Exploit Attacks
1	Apple	89	Microsoft	96
2	Google	84	Google	65
3	Adobe	72	Adobe	62
4	Cisco	67	HP	57
5	IBM	59	Oracle	50
6	Oracle	49	IBM	48
7	Sun	46	Mozilla	38
8	Microsoft	41	Linux	31
9	Linux	35	Cisco	30
10	HP	29	Sun	29

Table 1. Top 10 vendor exploit attack targets by distinct vulnerability

The number of exploit attacks in the first six months of the year has been dropping. If this trend continues, we can probably expect the months of the third and of the fourth quarters to post even smaller numbers.

	1Q 2011		2Q 2011	
	Month	Number of Exploit Attacks	Month	Number of Exploit Attacks
1	January	396	April	312
2	February	378	May	295
3	March	356	June	294

Table 2. Overall number of exploit attacks by month

MOBILE ATTACKS

Notable Android Malware Attacks

Due to *Android OS*'s increasing popularity, it has been the subject of at least three attacks via ANDROIDOS_ADSMS.A, ANDROIDOS_DORDRAE.L, and ANDROIDOS_CRUSEWIN.A in the past three months. Like previously discovered *Android* malware, all three posed as either fake apps or updates to trick users into executing them, albeit varying targets.

ANDROIDOS_ADSMS.A specifically targeted China Mobile subscribers while the latter two—ANDROIDOS_DORDRAE.L, aka DroidDreamLight, and ANDROIDOS_CRUSEWIN.A, which can turn infected devices into SMS relays, were less discriminating. All three steal a variety of PII despite varying arrival means. Unlike ANDROIDOS_ADSMS.A and ANDROIDOS_CRUSEWIN.A, which arrived via SMS, DroidDreamLight-Trojanized apps may be downloaded from the *Android Market* or from any third-party app store. These will, however, not be the last *Android* malware, especially due to the OS's more "open nature" compared with competing mobile platforms.



Figure 4. Malicious service DroidDreamLight starts

SOCIAL NETWORKING SCAMS

Notable Facebook-Related Threats

Like any other high-ranking platform such as the *Android OS*, *Facebook*—one of the most popular social networking sites worldwide—was also plagued by several notable attacks this quarter. Arriving in the form of spammed malicious links through various *Facebook* tools or as "copy-and-paste" scripts, all these led to data theft. Note that even the site's recent addition of security features to minimize the dangers that copy-and-paste scripts pose did not deter cybercriminals from launching these campaigns and from succeeding with their attempts.

A recent trend is the use of various *Facebook* features and tools to spread malicious links or scripts in order to infect systems, as the recent attacks used the site's Events, Chat, and Notes functions apart from the usual malicious wall posts.

One particular incident also used a slew of spammed messages to convince users to do various things, including to install a so-called *Facebook Messenger*, aka BKDR_QUEJOB.EVL, and to check if their passwords were secure by opening a malicious .DOC file attachment detected as TROJ_DOFOIL.VI that asks recipients to run JS_OBFUSCAT.SME.

These attacks used enticing come-ons such as allowing recipients to see how they will look after 20 years and helping keep spam at bay via several malicious JavaScripts, including JS_MALAGENT.PB, JS_DOOLF.SPM, and JS_FBJACK.B.



Figure 5. Facebook threats timeline

It should be noted that all of the *Facebook*-related malware identified above put users at risk of losing PII that cybercriminals can use for more nefarious schemes in the future.

TOP SYSTEM INFECTORS

Notable Spam Runs

Three spam runs related to separate events were noted by TrendLabs engineers this quarter, the first of which was political in nature. In this incident, recipients—mostly users from China—were asked to join the so-called Jasmine Revolution, aka the Tunisian Revolution. It made use of a malicious .RTF file attachment detected as TROJ_ARTIEF.KER, which exploits the CVE-2010-3333 vulnerability. The Trojan has been embedded with BKDR_IRCBOT.KER, which triggers the opening of a .DOC file that contains complaints and grievances related to the said revolution.

Similar to previously reported spam runs, the second to fourth attacks leveraged enticing news bits and promotions such as Osama bin Laden's death, the upcoming "London 2012 Olympics," and a so-called "Free Supper Day" despite varying social engineering techniques. The latter two used more traditional email messages with malicious file attachments such as TROJ_INJECTOR.VI, which downloads two more malware—TROJ_CTGOG.VI and TSPY_KARAGNY.VI—apart from embedded links. The former, however, added *Facebook* to its list of infection vectors with the help of JS_OBFUS.AB and JS_FBJACK.C.

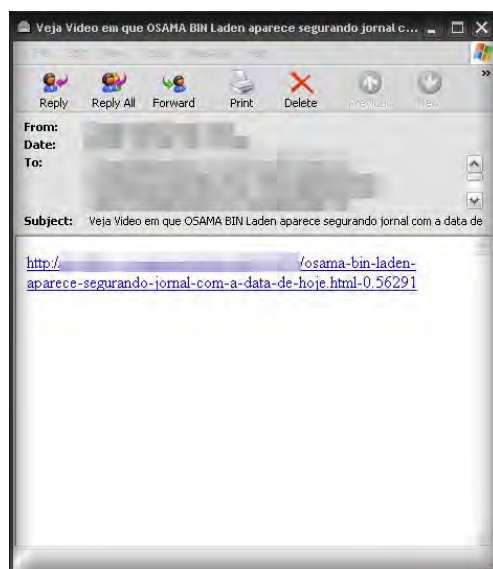


Figure 6. Spam promoting a video of bin Laden's death



Recent events showed that spammers are still up to no good and will continue to scam users through whatever means possible, hence the addition of various social networking sites to their list of infection routes.

Recent events showed that spammers are still up to no good and will continue to scam users through whatever means possible, hence the addition of various social networking sites to their list of infection routes.

Spam Statistics

As in the previous quarter, India and the Russian Federation remained two of the top 3 spam-sending countries this quarter. Former top-ranking spam-sending country—the United States—was, however, ousted by South Korea.

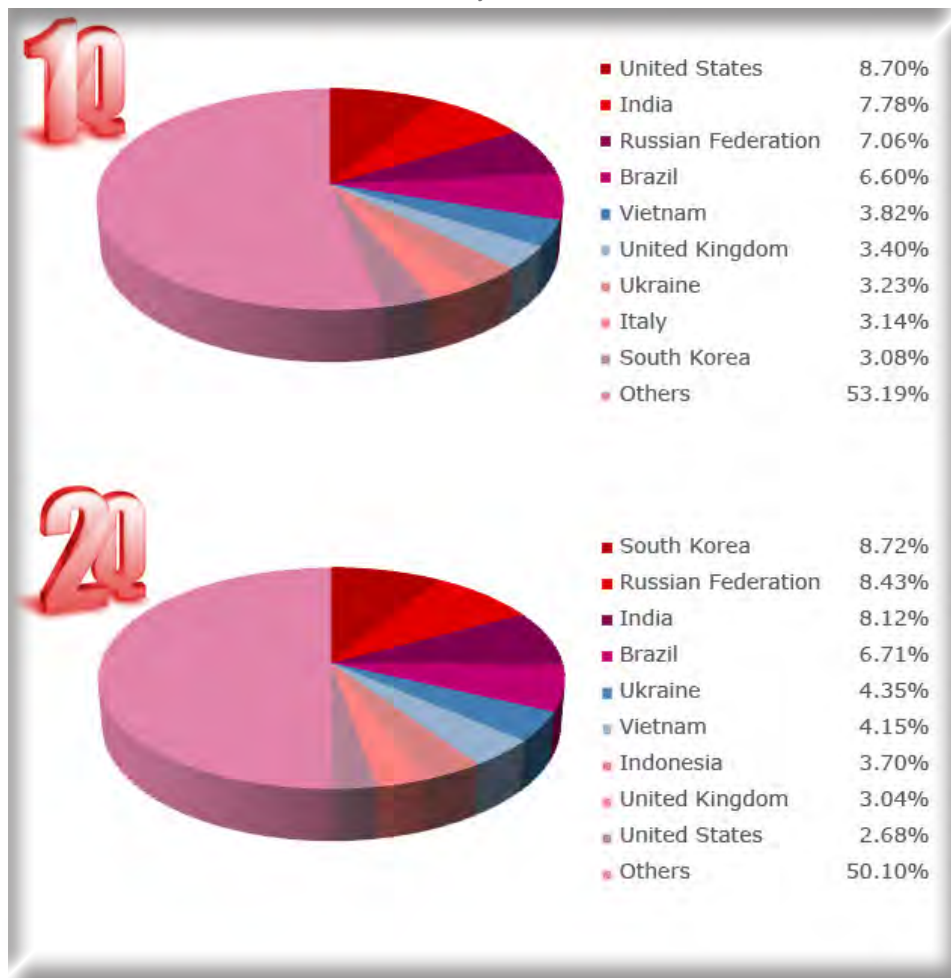


Figure 7. Top 9 spam-sending countries

Unlike the list of top spam-sending countries, however, the top 3 spam languages—English, Russian, and German—maintained their ranking.





Figure 8. Top 10 spam languages

NOTABLE MALWARE ATTACKS

FAKEAV Malware Do Not Discriminate in Terms of Platform

FAKEAV malware are no longer just common for *Windows*-based systems. These are also increasingly being used to attack Macs. Just this quarter, we saw several FAKEAV for Macs variants sporting names such as *Mac Security*, aka `OSX_FAKEAV.A`, and *MACDefender*, aka `OSX_FAKEDEF.M` or `OSX_DEFMA.B`, infect Macs via different means. One variant arrived via malicious landing pages to which Mac users utilizing Google Images's search function were taken to. The other two variants, on the other hand, arrived via malicious sites or via malicious links spammed in *Facebook*.

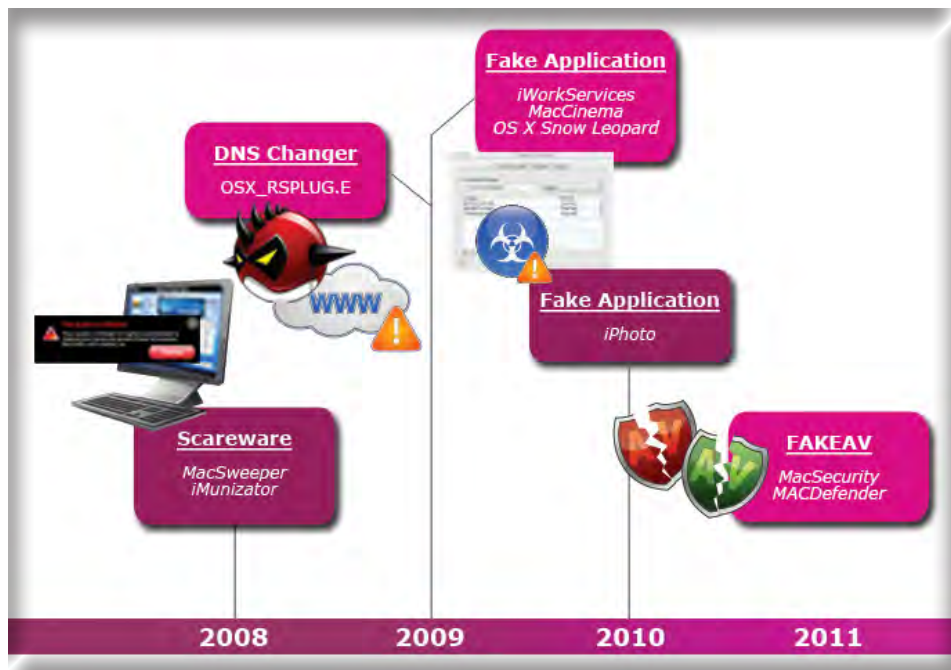


Figure 9. Mac malware timeline

The recent spate of FAKEAV for Macs attacks garnered so much attention that Apple had to immediately release [a security update](#) to try to mitigate the issue. This resurgence of Mac malware also prompted Trend Micro senior threat researcher Joey Costoya to take the [TrendLabs Malware Blog](#) readers to [a walk-through](#) of a typical FAKEAV for Macs infection as well as to provide [more information](#) on how cybercriminals went about their so-called FAKEAV business.

Despite crossing borders, however, we still came across several FAKEAV variants targeting *Windows*-based systems, one of which was a [fourth-generation variant](#) detected as [TROJ_FAKEAV.BTV](#). The second malware, aka [TROJ_FAKEAV.HKZ](#), rode on the increasing attention on [iCloud's upcoming release](#).

Malware Statistics

Last quarter's top 2 malware instances—[WORM_DOWNAD.AD](#) and [CRCK_AGENT](#)—maintained their posts this quarter. Meanwhile, the first quarter's top 3—[HKTL_KEYGEN](#)—was ousted by [ADW_SAHAGENT](#).



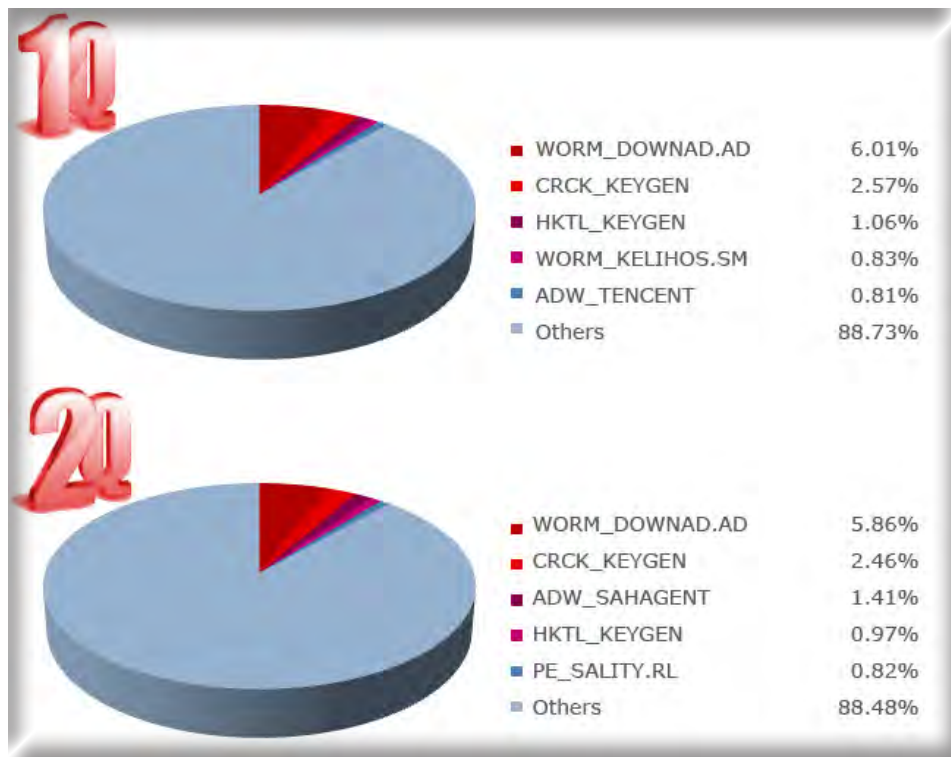


Figure 10. Top 5 malware

HOW HAS THE THREAT LANDSCAPE CHANGED?

TDL4 Malware Attack

Probably one of the most complex malware, **TDL4**—a variant of the well-known TDSS family—reared its ugly head this quarter. TDSS malware have been known to evade detection by residing in infected systems’ boot sector. Due to their complexity, Microsoft, as part of its April 2011 Patch Tuesday release, even included [a solution](#) specifically for TDL4 malware infections.

TrendLabs engineers found [a way to detect](#) the malware’s worm component, aka **WORM_OTORUN.ASH**, which gave the TDL4 malware the ability to spread. Detecting this component, according to Trend Micro threats analyst Brian Cortes, was “crucial to stopping the cybercriminals behind the attack from expanding their botnet.”





Figure 11. WORM_OTORUN.ASH's infection map

More SpyEye Modifications

SpyEye 1.3.4.x's release may spell even greater doom for users worldwide, as its control panels—CN1 and SYN1—now come with even more helpful features for bot masters or herders. Among the many modifications made to the toolkit were the following:

- Apart from changes to some of the buttons' names, a so-called *Logs* button was added, which allowed bot masters or herders to view or clear logs.
- The *Create Task* panel allowed users to create tasks by selecting files and by choosing any of the following types of action, depending on the file type they want to use:
 - **Update bot body:** Used to update the SPYEYE binary itself.
 - **Update bot config:** Used to update the configuration file if the users want to change how their bots are configured.
 - **Load exe:** Used to spread other malware such as ZBOT, TDSS, and FAKEAV variants.
- The *Files* option allowed users to only upload an .EXE or a .BIN file and no other file types, as in previous SpyEye versions, most probably to prevent a known security hole in the panel from uploading any other kind of file. This security check, however, is only applicable for file extension names and does not extend to file types.



Figure 12. Some notable SpyEye 1.3.4.x modifications



NOTABLE TAKEDOWNS AND OTHER SECURITY WINS



The past quarter was marked by a couple of notable takedowns and wins for the security industry, topped by the takedown of a CARBERP C&C server, which involved some of our very own top threat experts.

Trend Micro Wins

The past quarter was marked by a couple of notable takedowns and wins for the security industry. Topping our list was the takedown of a CARBERP command-and-control (C&C) server, which involved some of our very own top threat experts. In this exercise, our researchers redirected the identification of the malicious C&C server to their own analysis server, which allowed them to slow down the botnet. This represented a significant security win, especially since the botnet has been stealing PII from users worldwide for several months now since it was first deployed in the early part of 2010.

A blog entry published this May also showed how instrumental Trend Micro was in blocking malicious URLs, which prevented users from suffering from various system infections. In this particular entry, Trend Micro director for threat research Martin Roesler discussed how our efforts to conscientiously block access to malicious links put the company up on Microsoft's leader board for the seventh straight month in a row.

Other Security Wins

Apart from the wins above, we also witnessed the success of two more takedowns led by law enforcement officials, particularly in the United States and in Japan.

The U.S. Department of Justice and the Federal Bureau of Investigation (FBI) headed the CoreFlood takedown, which represented a huge victory for all of the good guys fighting against cybercrime. As Trend Micro senior threat researcher David Sancho said, "One less big botnet means that, at the very least, cybercriminals will think twice about setting up a server in the United States from now on."

Meanwhile, on June 17, the Japanese Parliament approved the revised *Cybercriminal Law*, which will start penalizing malware writers who create malicious wares without legitimate reasons and/or for the purpose of running these on others' systems without their consent.

The implementation of the *Cybercrime Law* put Japan in a much better position to collaborate with other governments in order to combat cybercrime. Trend Micro, as a security company, welcomes this move, as it reiterates the fact that creating, distributing, owning, and keeping malware for malicious purposes is a crime. Trend Micro security evangelist Masayoshi Someya added that "this is a huge step toward tackling cybercrime that will certainly continue to happen for many years to come."





To keep up with the rapid changes in the security industry as well as with the continuous enhancements made to systems and to devices, cybercriminals constantly improve their tools and tactics in order to continue profiting from their malicious schemes.

WHAT THE FUTURE SPELLS

To keep up with the rapid changes in the security industry as well as with the continuous enhancements made to systems and to devices, cybercriminals constantly improve their tools and tactics in order to continue profiting from their malicious schemes.

The following describe what our security analysts and researchers think users should look out for at present and in the near future.



- The Epsilon breach last April opened everyone's eyes to the consequences of having their email accounts compromised as well as to how such instances can lead to information and identity theft. This prompted Trend Micro senior threat researcher David Sancho to list down some useful tips for keeping email accounts safe, especially in light of today's highly targeted attacks.
- The spate of FAKEAV malware attacks this quarter renewed public interest in what makes the notorious family persistent. Trend Micro senior threat researcher Nart Villeneuve discussed how malicious domains and ISP registrars can contribute to the malware family's success, leading him to conclude that "identifying the source of the FAKEAV domains and not just the botnets that distribute these is important in combating this threat."
- Despite being an oft-ignored infection vector, Webmail again proved just how important it is to limit access to or to impose stricter rules when accessing personal email accounts at work. The recent Hotmail-related incident showed how this simple practice can lead to the leakage of sensitive corporate information and how even an old application bug can lead to disastrous endings.
- Italian security researcher Rosario Valotta recently described a zero-day attack on Microsoft's *Internet Explorer (IE)* browser, which he dubbed "cookiejacking," better known as sidejacking or session hijacking. The main idea behind which has actually been around for several years now though Valotta discovered a new attack delivery based on social engineering users to help exploit the said *IE* bug.

Trend Micro senior threat researcher Robert McArdle opined that "Microsoft's statement that this issue should not be taken seriously and does not pose high risk is misguided, especially since the vast majority of attacks are now hidden from view."

- Trend Micro senior threat researcher Loucif Kharouni believes that the changes the *SpyEye* author made to the toolkit can only bring the rumored Zeus-SpyEye merger closer to fruition should this indeed occur. If and when this happens, we may just see even graver data, identity, and financial theft consequences.

To stay abreast of developing threat trends and to constantly keep employees' systems and your corporate networks safe from the impending doom that can spell disastrous results for your organization, watch out for the release of the "3Q 2011 Threat Roundup" this coming October.



APPENDIX A: MALICIOUS URL STATISTICS

The following tables show the top 10 malicious URLs and IP domain addresses blocked by the Trend Micro™ Smart Protection Network™ in the first and second quarters of 2011.

Rank	1Q 2011		2Q 2011	
	Malicious URL Blocked	Description	Malicious URL Blocked	Description
1	ad.globe7.com:80/iframe3	Related to malicious ads and to a cross-site scripting (XSS) vulnerability	trafficconverter.biz:80/4vir/antispysware/loadadv.exe	Distributes malware, particularly DOWNAD variants
2	is1.j.tv2n.net:80/tv2n/instream/tv2n_instream_as2.swf	Already inaccessible during verification but reportedly downloads FAKEAV and VUNDO variants, Browser Helper Objects (BHOs), and backdoor agents	ad.harrenmedianetwork.com:80/iframe3	Distributes malware
3	trafficconverter.biz:80/	Distributes malware, particularly DOWNAD variants	trafficconverter.biz:80/	Distributes malware, particularly DOWNAD variants
4	trafficconverter.biz:80/4vir/antispysware/loadadv.exe	Distributes malware, particularly DOWNAD variants	www.myroittracking.com:80/newsserving/tracking_id.php	Contacts various servers to download and to aggressively display pop-up ads
5	links.gamevance.com:80/acttr.php	Displays ads and tracks anonymous usage information in exchange for free online games	d.gameplaylabs.com:80/conduit/loader.php	Distributes malware found in various folders on the site
6	ads.clicksor.com:80/showad.php	Hosts malicious files that may infect systems	gchp.sagac.info:80/pic.php	Part of a proxy site
7	stats.buysellads.com:80/imp.gif	Known phishing site	cdn.performersoft.com:80/download/installer/ibario-silent-us.exe	Engages in software downloads and at one time was tagged "malicious"
8	img.livejasmin.com:80/flash/sowriter.swf	Distributes malware when downloaded	cdn.performersoft.com:80/download/startnow/ibario-driverperformer-silent-us.exe	Engages in software downloads and at one time was tagged "malicious"

Rank	1Q 2011		2Q 2011	
	Malicious URL Blocked	Description	Malicious URL Blocked	Description
9	www.trafficholder.com:80/in/in.php	Traffic site known for distributing malware	www.trafficholder.com:80/in/in.php	Traffic site known for distributing malware
10	182.50.135.160:80/pic.php	Already inaccessible during verification	serw.clicksor.com:80/newserving/getkey.php	Included in the list of domains associated with pirated applications, <i>Android</i> malware, rogue antivirus, and other malicious activities

Source: Trend Micro Smart Protection Network data

Table A-1. Top 10 malicious URLs blocked in 1Q and in 2Q 2011

Rank	1Q 2011		2Q 2011	
	Malicious Domain IP Address Blocked	Description	Malicious Domain IP Address Blocked	Description
1	ak.imgfarm.com	Known for malicious download activities	trafficconverter.biz	Pay-per-install (PPI) affiliate site
2	trafficconverter.biz	PPI affiliate site	ad.harrenmedianetwork.com	Distributes malware
3	ad.globe7.com	Related to malicious ads and to an XSS vulnerability	cdn.performersoft.com	Engages in software downloads
4	is1.j.tv2n.net	Already inaccessible during verification but reportedly downloads FAKEAV and VUNDO variants, BHOs, and backdoor agents	d.gameplaylabs.com	Distributes malware found in various folders on the site
5	z0gyali0.com	Already inaccessible during verification but known for distributing TDSS and FAKEAV variants	www.myroittracking.com	Contacts various servers to download and to aggressively display pop-up ads
6	img.livejasmin.com	Adult video chat community	gchp.sagac.info	Part of a proxy site



Rank	1Q 2011		2Q 2011	
	Malicious Domain IP Address Blocked	Description	Malicious Domain IP Address Blocked	Description
7	ads.clicksor.com	Displays advertising campaigns	serw.clicksor.com	Included in the list of domains associated with pirated applications, <i>Android</i> malware, rogue antivirus, and other malicious activities
8	links.gamevance.com	Displays ads and tracks anonymous usage information in exchange for free online games	clicktrace.info	Distributes malware
9	stats.buysellads.com	Known phishing site	l4.zedo.com	Uses ad-tracking services but has already been de-listed in some domain block lists
10	www.trafficholder.com	Hosts malicious files that may infect systems	www.trafficholder.com	Hosts malicious files that may infect systems

Source: Trend Micro Smart Protection Network data

Table A-2. Top 10 malicious domain IP addresses blocked in 1Q and in 2Q 2011



TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TRENDLABS™

TrendLabs is Trend Micro's global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.

©2011 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.