

The image shows the top portion of a report cover. It features a dark teal background with abstract, glowing blue and white lines that suggest a digital or network environment. On the right side, there is a close-up, high-angle view of a hard drive's platters and spindle, rendered in a metallic, futuristic style with blue highlights. The text 'Global threat report' is overlaid in the lower-left area of this image in a bold, white, sans-serif font.

Global threat report

March 2012

Feature Article: Sizing Up the BYOD
Security Challenge



Table of Contents

Sizing Up the BYOD Security Challenge	3
Java Holes and Targeted Attacks	4
Gender and the Success of Suspicious Links	6
AMTSO, Testing, and ESET's Dutch Treat	7
The Top Ten Threats	8
Top Ten Threats at a Glance (graph)	11
About ESET	12
Additional resources	12

Sizing Up the BYOD Security Challenge

Stephen Cobb, ESET Security Evangelist

Do you let your employees use their own computers for work? How about smartphones, iPads and other tablet devices? If so, you are not alone. The phenomenon of allowing or encouraging employees to use their own devices for work—known as Bring Your Own Device, or BYOD—is now widespread in many countries. On the plus side, you may get more work from people when they can work in more places and at more times of the day (from the breakfast table in the morning to the kitchen table at night and the coffee shop in between). There can be cost savings too: equipment outlays can be reduced if employees use their own devices instead of the company buying them.

At the same time, IT security managers must weigh those benefits against the security risks that come with these devices, plus the cost of bringing them into line with existing security policies and compliance standards. For example, what are the legal ramifications of an employee's personal laptop going missing when it contains your customer list or sensitive internal correspondence?


To help companies get a handle on the scale and scope of these risks, ESET engaged Harris Interactive to survey some 1,300 adults in America who are currently employed. We found more than 80 percent of them “use some kind of personally owned electronic device for work-related functions.” Many of these devices are older technologies like laptop and desktop computers, but smartphones and tablets are already a significant part of the BYOD phenomenon.

Unfortunately, the survey paints a worrying picture of security

on these devices; for example, encryption of company data is only happening on about one third of them. One third of those surveyed responded that company data is not encrypted when it is on their personal devices and the remaining third did not know one way or the other, which is worrying in itself. You can see more of the findings in the accompanying infographic.



One particular area of concern is small devices—like tablets and



smartphones—that are easier to steal than laptops and desktops but pack tremendous processing, storage, and communication capabilities. Consider the Microsoft Word document in which the results of ESET’s BYOD survey were presented. This file takes up 170 kilobytes of storage space and contains 17 pages of charts, tables, and text that summarize the most important findings from this not inexpensive research. That means you could easily store more than 70,000 similar reports on 16 gigabyte smart phone or microSD card. A smartphone could transmit all 70,000 documents to the other side of the world in matter of minutes on a WiFi or 4G/LTE connection (the latter could prove costly, but the recipient might be happy to pay the data overage).

So it is not good news to learn that only 25 percent of smartphone users, and less than 10 percent of tablet users, say they have enabled auto-locking on these devices (the feature that locks the device after a period of inactivity and requires a password or code to unlock). Overall, we found that less than half of all devices in the BYOD category are protected by basic security measures. On the bright side, BYOD security could be boosted cheaply and quickly if companies did the following:

- Mandate auto-locking with password protection on all devices.
- Enable remote lock/wipe to protect data on any stolen devices.
- Enable encryption of company data on all devices.
- Make sure up-to-date anti-malware protection is active on all devices.

In summary, now would be a good time to check how your

company is handling BYOD security. With roughly two thirds of our survey respondents reporting that their employer had not yet implemented a BYOD policy, or provided any security training, those would be good places to start.

Java Holes and Targeted Attacks

March produced a number of important new insights into malware threats and ESET researchers around the world were hard at work bringing these to light. Here we highlight three threats, starting with the information stealing trojan that ESET dubbed Win32/Georbot.

The name Win32/Georbot is derived from Georgia, the country in Eurasia, because ESET researchers found the malware was receiving updates from a domain belonging to the Georgian government. Of course, that does not mean the malware, or the botnet created with it, had anything to do with the Georgian government (in fact it should be noted that the Data Exchange Agency of the Ministry of Justice of Georgia and its national CERT cooperated with ESET on this matter). However, from our analysis of the code it appears that citizens of Georgia might be the intended target of the malware’s information stealing capabilities. A review of the stealing functionality of this malware is a reminder of how pernicious such threats can be. Once it infects a system, Win32/Georbot can:

- Send any file from the local hard drive to the remote server.
- Steal certificates
- Search the hard drive for Microsoft Word documents

- Search the hard drive for remote desktop configuration files
- Take screenshots
- Record audio using the microphone
- Record video using the webcam
- Scan the local network to identify other hosts on the same network
- Execute arbitrary commands on the infected system

And those are just the information stealing capabilities of this botnet. Interestingly, these commands are not automated but activated manually, sent to each host individually rather than being broadcast to all infected hosts. ESET researchers were able to gain access to the botnet's control panel and in doing so discovered lists of keywords used to search through Word files on infected machines. For more on this threat, you can find a summary of our analysis in a blog post cleverly titled [From Georgia With Love](#) and the full report is [available as a PDF file](#).

```
[ministr,service,secret,top,agent,contact,army,USA,
Russia,Georgia,major,colonel,FBI,CIA,phone,number,
east,program]
```

```
[ministr service secret Russia Geo Euro weapon USA
Americ top colonel major serg soldie contact telephone
Cauca FBI CIA FSB KGB army name surname important]
```

```
[ministry,secret,plan,scheme,fsb,fbi,cia,kgb,captain,
colonel,lieutenant,plan,phone,contact,number,russia,
georgia,usa,europe,major,general,top,interest,photo,
build,sphere]
```

The second recently discovered threat we want to highlight is great news for conspiracy theorists because it is a second information stealing botnet with manual controls and geopolitical targeting. This time the country is Tibet and the target appears to be NGOs (Non-Governmental Organizations). We published a detailed [analysis of the Mac OS X payload](#) delivered by this malware, dubbed OSX/Lamadai.A.

Although this code exploits a vulnerability that Apple patched some time ago (Java vulnerability CVE-2011-3544), we did see infections and our researchers were able to observe communications between a sacrificial test machine and the botnet's C&C (Command and Control, the software from which the botnet owner or botmaster, monitors and manages the infected machines). In fact, we observed the botmaster typing in commands as he or she looks for sensitive files on our machine.

```
sh-3.2# cd Keychain
sh: cd: Keychain: No such file or directory
sh-3.2# cd Keychains
sh-3.2# ls
login.keychain      metadata.keychain
sh-3.2# pwd
/Users/<username>/Library/Keychains
```

The third in our trio of highlighted threats continues the Java theme, a new exploit for the Java [CVE-2012-0507](#) vulnerability found in a new version of the Blackhole exploit kit. These days, Java vulnerabilities are the number one target for exploit kit developers because they are the most effective way of exploiting end-user systems and can sometimes be effective across [a variety of platforms](#). Our write-up of this latest example tracks many incidents involving the infection of popular and legitimate Russian sites where iFrames redirect victims to the [latest version of Blackhole](#). Yet again we are reminded that it is imperative to keep your patches current and your antivirus updated.

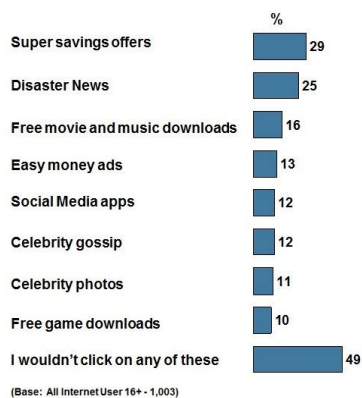
Gender and the Success of Suspicious Links

Urban Schrott, ESET Ireland

Sub-head or first sentence: A new ESET Ireland study reveals which online topics may be irresistible, compelling both men and women to click on links even if they seem suspicious.

Recently ESET Ireland commissioned a survey to find out under what circumstances people would click on a suspicious link in social media, online ads or unsolicited email (spam). In other words, would they still click even if they were not sure it was safe to do so, knowing that it could be fake or malicious?

The good news is that 49 percent of those surveyed said they would not click, regardless of the type of "bait" such as an unbelievably low price on a popular product or news of a major disaster. Of course, everyone has heard the phrase: If it looks too good to be true, it probably is. Our Irish colleagues have been telling Irish computer users this for some time with regards to spam and various online offers that promise incredible deals. The fact that about half of all users can resist the urge to click dodgy links suggests that the message is getting through, but what about the other half?



The survey revealed that money saving offers were the most irresistible (29%) followed by disaster news (25%). Free movie and music downloads lured some people (16%) as did free game downloads (10%). Celebrity gossip and photos were an admitted weakness for some (12% and 11% respectively). Advertisements promising easy money tempted 13% while social media apps lured 12%.

Perhaps it is not surprising, but the survey also revealed interesting gender differences when it came to temptation. For example, satisfying the shopping urge was worth a risky click for one in three women, but only one in four men were tempted by shopping offers. However, the roles reverse when it comes to free downloads. There males are far ahead in recklessness, as 20% (even up to 23% in age group 15-24) of males and only 12% of females will engage in downloading music, films or computer games from dodgy websites which could cause malware infection in the process.

Disaster news appears to be equally interesting to females and males, but particularly interesting to youths (30% of age group 15-25). Our Irish colleagues found one more positive note; it seems the Irish have not yet succumbed to the celebrity obsessions of some other nations, because less than 12% appear susceptible to the dangers of suspicious links to celebrity photos or gossip.

What to do and how to know what to click on?

Of course, the point of the survey was to draw attention to the problems that can arise from giving into temptation when you see an alluring but suspicious link. A significant percentage of malware infections rely on this type of user interaction. So here are some tips to share with friends and family and colleagues in the workplace:

- Act responsible and don't just click on everything you find appealing. Internet fraudsters are counting on your curiosity to help them spread malware and lure people into financial scams.
- Do your online shopping on reputable websites and make sure they have the safety certifications for secure payments.
- Get your world news from known news websites, from your local TV or radio stations' websites, etc. Many scams are spread through email and social media by pretending to show "yet unseen footage" from some recent disaster.
- And, as always, think before you click!

AMTSO, Testing, and ESET's Dutch Treat

David Harley, ESET Senior Research Fellow

Righard Zwienenberg is not only an enormously respected security researcher but also an old friend (well, nowhere near as old as I am, but not many people are, though Stephen Cobb is getting there!), and I was very pleased to hear, after many years at Norman (and at Thunderbyte before that), that there was a possibility of his joining ESET. Since [he joined ESET](#) in February as a Senior Research Fellow (yes, we're replicating virally) in the Technology Division at ESET HQ in Bratislava, he's introduced himself with a volley of heavy-hitting blog articles:

- [Password management for non-obvious accounts](#)
- [SKYPE: \(S\)ecurely \(K\)eep \(P\)ersonal \(E\)-](#)


[communications](#)

- [The security of unlocking an Android based device, the future is near?](#)
- [From Georgia With Love: Win32/Georbot information stealing Trojan and botnet](#)

However, it turned out that there was a slight problem.

For most of the past three years, Righard and I have both been on the Board of Directors of AMTSO (the Anti-Malware Testing Standards Organization), of which Righard is the President, and two directors representing the same member entity is against the organization's bylaws. So I've stepped down from the Board a little earlier than anticipated (I wasn't planning to stand for re-election this year, so it was an easy decision). Rest assured (if you *do* find it reassuring!) that I still represent ESET N. America in AMTSO and will continue to engage with the organization, I still wholeheartedly support AMTSO's aim of raising testing standards, I will continue to do authoring jobs on behalf of AMTSO when I can find time, and I have every intention of commenting even more regularly on testing issues. In fact, I'll be presenting a paper on "After AMTSO: a Funny Thing Happened on the Way to the Forum" at [EICAR](#) in May (and, by way of a complete contrast, another on PIN selection strategies).

That sounds a bit as if I'm predicting the death of AMTSO at EICAR. Well, no, I'm not sending for the undertakers yet. However, part way through the second day of the recent workshop in San Mateo, a major shift in direction *was* proposed. AMTSO's initial attempts to make testers and reviewers more accountable for the accuracy of their tests and test reports through a 'review of reviews' analysis, attempting



to assess whether a review was compliant with the organization's '[Fundamental Principles of Testing](#)', attracted a great deal of (mostly [negative](#)) attention. The new proposal covers too much ground to summarize in a short article, but a key component is the revival of the idea of tester accountability in a different form: primarily, a more general review of the testing landscape commissioned from academia.

I expect that proposal to excite a great deal of debate at the next AMTSO meeting in May, and I'm not going to attempt to predict what the final outcome will be. Personally, I have no problem with the principle of tester accountability. And it seems to me that there is an undercurrent of admission here that AMTSO has failed to convince the world that it's an impartial commentator on testing issues rather than simply a mouthpiece for companies selling a [frequently denigrated technology](#): it needs to channel the undoubted expertise of its participants (vendors *and* testers) via a credible, trusted third party. The success of this proposal, if adopted, may well depend on how consistently both testers and vendors within the AMTSO community (both members and subscribers) can put the well-being of the community ahead of their own vested interests as commercial organizations.

It's all too easy to write off security researcher concerns about the standard of testing as 'vendor whining': a lot of media comment is based on the assumption that vendors hype and testers expose weaknesses. However, it's worth remembering that testers (the professionals, at any rate) also have a commercial agenda, and it's not always easy to detect bias in a comparative test report.

The major certification testers are in a state of ongoing negotiation with the vendors who are their customers, trying to strike a balance between maintaining their independence and keeping the vendors who are their customers, and the same

principles are maintained by good vendor-sponsored comparatives, though not always with [due credit](#). And that's not a bad thing: those checks and balances help to keep everyone honest. But sometimes the business relationship between a particular vendor and an apparently impartial report is far from transparent. Sometimes an apparently independent tester is underwritten by a single AV company, and may even be covertly hosted by such a company.

Don't get me wrong: there are many honourable instances of information resources that are not only open about their association with a particular vendor, but whose independence is nevertheless generally unquestioned ([Virus Bulletin](#) testing is, perhaps, the star example). However, there are always going to be doubts when a testing organization isn't open about such links (or, come to that, its methodology), however good its tests may be. Or when it describes its test as 'sponsor-independent' tester while requiring large consultancy fees from companies whose products it tests before discussing verification of its testing, (And don't get me started on the 'we'll let you see the samples – or in some cases, the simulated attack – but only if you sign a form that stops you talking about it in public' gambit.)

The Top Ten Threats

1. HTML/ScrInject.B

Previous Ranking: 1

Percentage Detected: 5.60%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 5.19%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (<http://blog.eset.com/?p=94> ; <http://blog.eset.com/?p=828>) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at <http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun> useful, too.

3. HTML/Iframe.B

Previous Ranking: 3

Percentage Detected: 3.95%

Type of infiltration: Virus

HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.


4. Win32/Conficker

Previous Ranking: 4
Percentage Detected: 3.44%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC subsystem and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: <http://blog.eset.com/?cat=145>



It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

5. JS/Agent

Previous Ranking: 90
Percentage Detected: 2.30%

The trojan displays dialogs that ask the user to purchase a specific product/service. After purchasing the product/service, the malware removes itself from the computer. Trojan is probably a part of other malware.

6. JS/Iframe.AS

Previous Ranking: 66
Percentage Detected: 2.04%

JS/Iframe.AS is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

7. Win32/Sirefef

Previous Ranking:
Percentage Detected: 1.76%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

8. Win32/Sality

Previous Ranking: 8
Percentage Detected: 1.72%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:

http://www.eset.eu/encyclopaedia/sality_nar_virus_sality_aa_sality_am_sality_ah

9. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.68%

Win32/Dorkbot.A is a worm that spreads via removable media.

The worm contains a backdoor. It can be controlled remotely.

The file is run-time compressed using UPX.

The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

10. JS/Redirector

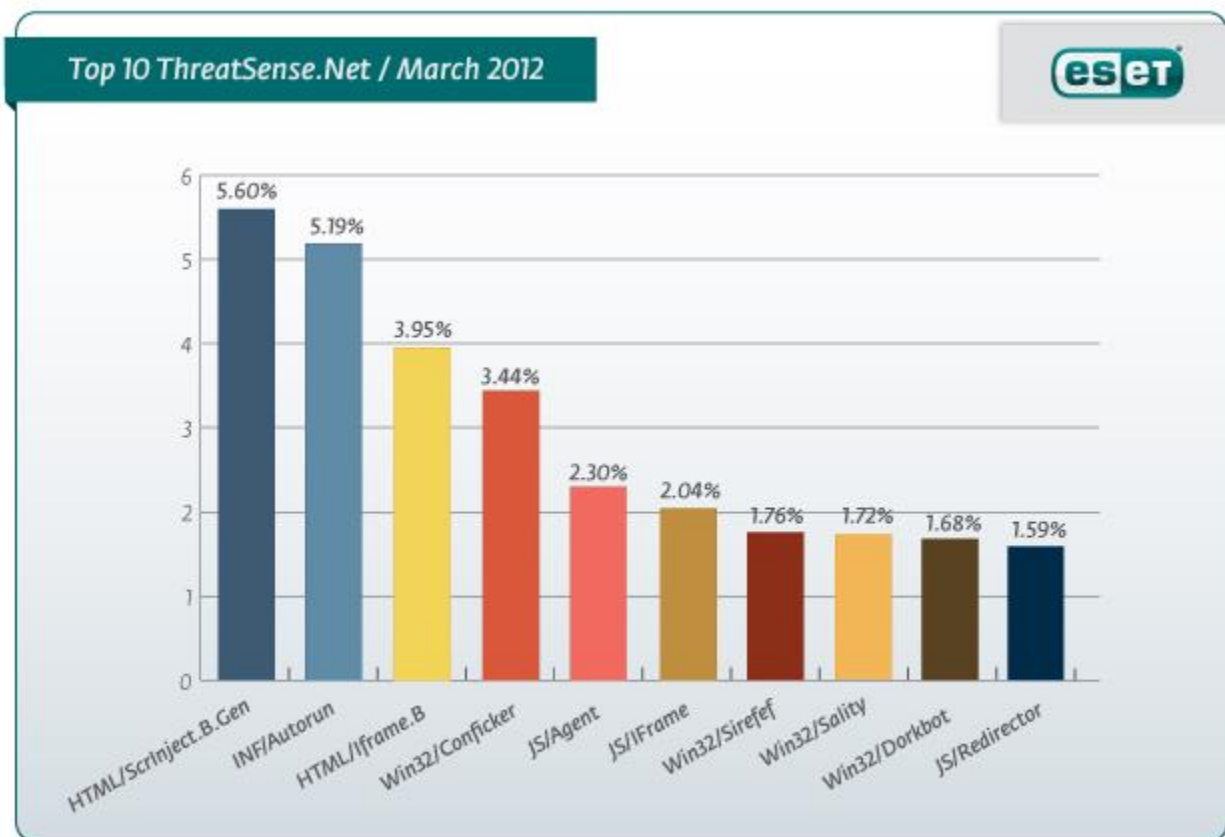
Previous Ranking: 47
Percentage Detected: 1.59%

JS/Redirector is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

Top Ten Threats at a Glance

(graph)

Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 5.60% of the total, was scored by the HTML/Scrinject.B class of threat.





About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the [ESET Threat Center](#) to view the latest:

- [ESET White Papers](#)
- [ESET Blog](#)
- [ESET Podcasts](#)
- [Independent Benchmark Test Results](#)
- [Anti-Malware Testing and Evaluation](#)