

From Russia with Love

Behind the Trend Micro-NBC News Honeypots

Kyle Wilhoit

Forward-Looking Threat Research Team



Contents

Introduction.....	1
Environment Setup.....	1
User Activity.....	2
Samsung Galaxy S4.....	2
Lenovo ThinkPad.....	3
Macbook Air.....	4
Conclusion.....	6

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



Introduction

I was recently invited by NBC News to take part in an experiment with their chief foreign correspondent, Richard Engel, that took place in Moscow, Russia. For this experiment, we created a honeypot environment to emulate a user currently in Russia for the Sochi Olympics performing basic tasks such as browsing the Internet, checking email, and sending and receiving instant messages. The experiment primarily aimed to gauge how quickly certain devices can be compromised while their user engages in normal online activities. We set up three devices—a Macbook Air®, a Lenovo ThinkPad® running Windows® 7, and a Samsung Galaxy S Android™ smartphone.

While attacks identical to the ones observed can and do originate in nearly every country in the world, attacks originating from and/or tied to Russia may be more prevalent. This research paper covers in greater technical detail the environment setup and what happened to the above-mentioned devices.

Environment Setup

The first thing we had to consider was how the environment was going to be configured. NBC News wanted the experiment to be performed on new gadgets with no security or software updates. The decision to not put basic precautions in place was made because we were supposed to be regular users in Russia for the Sochi Olympics and wanted to understand the threats attendees who do not take proper precautions faced. We did, however, need to install standard software that were considered “lifestyle” or “productivity” applications such as Microsoft™ Office®, Adobe® Flash®, Java™, and others that aid in viewing websites or processing documents. We chose Microsoft Office 2007 because of its perceived user base. I then downloaded the most recent version of Flash and Java since they were the most readily available on their vendors’ websites.

We then needed to consider how to collect network traffic. Without having this ability, we would not be able to differentiate malicious from normal network traffic. To solve the problem, we tethered our own Wi-Fi access point off the physical connection within the hotel room. We then used a network tap to gain direct access to the traffic coming from our devices to the outside world. To keep the environment as clean as possible, we installed logging and monitoring tools on a separate Linux box and a virtual machine. We used these to capture and analyze network traffic. We used a combination of Snort (custom and standard rules), BroIDS, tcpdump, ntop, and internal Trend Micro tools to help identify known command-and-control (C&C) servers and malicious binaries that can affect the devices.

In addition to setting up a logging solution, we also connected an email account emulating Richard’s real inbox to the phone. The email address we used resided within the NBC News domain and was very similar to Richard’s true email address to help convince any would-be attacker it was the real thing. We used the same email account on each device.

User Activity

As in most malware attacks, user activity of one form or another is required for an infection to affect devices. The case studies presented in this paper do not differ in that the user has to do something because no compromise automatically occurs. Throughout the testing period of 72 hours, we started visiting websites that any regular traveler would.

Samsung Galaxy S4

Compromises can occur in Russia just as quickly as in any other country. We unboxed the Samsung Galaxy S4 running Android when we arrived in Russia. We left all of its security settings in the default state. We then plugged in a local subscriber identity module (SIM) card from the Russian cellular service provider, MTS. After establishing a working line, we then connected it to an open Wi-Fi access point in a local coffee shop. We started visiting websites that any traveler would. Many of them primarily featured content on the Sochi Olympics.

We visited a Sochi-Olympic-themed site and were redirected to another, which prompted us to download an app (*avito.apk*) that seemed to have relevant travel information. After downloading the .APK file (MD5: *6d6cb42286c3c19f642a087c9a545943*), we were prompted to install it. We clicked “Accept” because we believe that’s what typical users would do. The app was then installed on the phone though we didn’t see its icon. After a while, it (a piece of malware) started communicating with *http://<REDACTED>/getTask.php/imei=<VALUE>&balance=0* and *http://<REDACTED>/reg.php/country=us&phone=<VALUE>&op=Android&balance=0&imei=<VALUE>*.



Figure 1: Image seen while the site drops the malicious .APK file (screenshot was taken on the Macbook Air, which shares the email address with the Samsung Galaxy S4 smartphone)

Executing *avito.apk* fills in the “country,” “phone,” “balance,” and “imei” fields with values pulled from the infected phone. This allowed the attacker to read the emails on it, gain access to external media connected to it, collect contact data stored in it, record calls made on it, and perform several other tasks. After beaconing to *uploader.ru*, we saw encrypted traffic leave the phone via port 443 to the said domain. The malicious app appears to be part of the SMSSEND malware family, which has infected more than 200,000 Android phones to date.¹

Trend Micro has been detecting variants of the SMSSEND malware family since April 2010. Trend Micro™ Mobile Security blocks access to all related URLs and binaries.

Lenovo ThinkPad

We installed Windows 7 on the Lenovo ThinkPad because it is the most used Microsoft OS worldwide.² This is what a standard user would likely do. We kept all of the default security settings as well.

After roughly 30 hours, Richard’s fake account received a spear-phishing email. The email came from *quentorn1971@gmail.com* (MD5: *85a97e1550be413b850f76a5a3a36272*), someone who supposedly had some information to share with Richard in the form of a link to a Sochi-Olympic-related document.

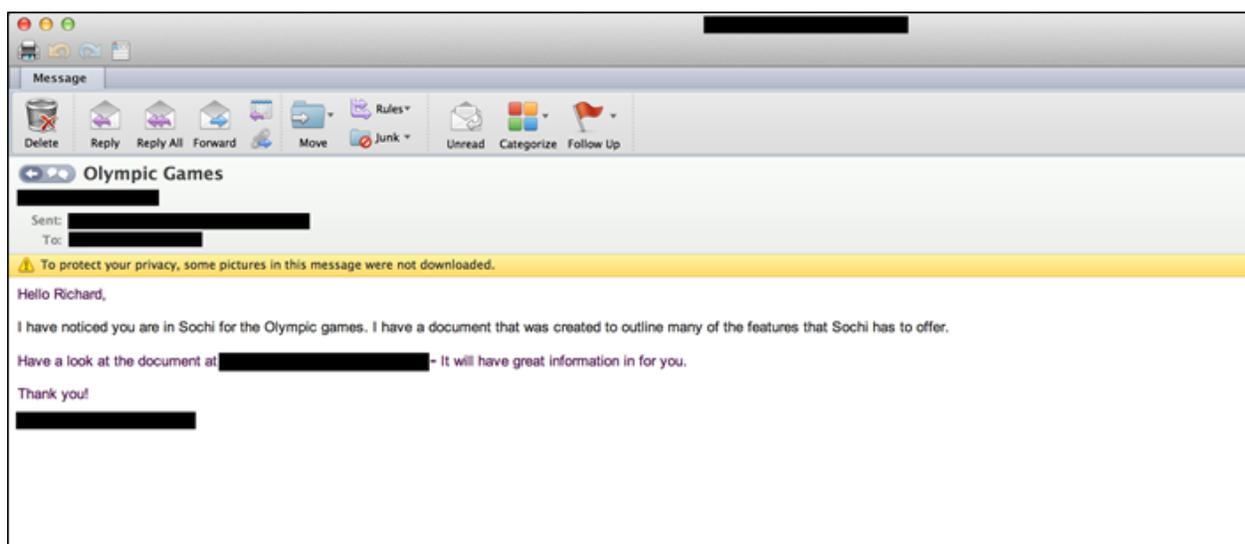


Figure 2: Spear-phishing email sent to Richard after linking the email address we created earlier to all devices (screenshot was taken on the Macbook Air, which shares the email address with the Lenovo ThinkPad)

1 Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “SMSSEND.” Last accessed February 7, 2014, <http://about-threats.trendmicro.com/us/search.aspx?p=SMSSEND>.

2 NetApplications.com. (2014). *NetMarketshare*™. “Desktop Operating System Market Share.” Last accessed February 7, 2014, <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>.

Richard's email address appears to have been obtained from the compromised Samsung Galaxy S4 smartphone we used. It is possible that the attacker who gained access to the phone realized that Richard was a high-value target and so sent him a spear-phishing email.

Clicking the link embedded in the email leads to the download of a Microsoft Word® document named *Olympics.doc* (MD5: *09326cec312ff356dde41d2e007fd009*). Opening the document sends a simple beacon to *whatsappload.ru*. Within a minute, the piece of malware opened a back door connected to the same site via port 443. This allowed the attacker to gain access to the infected machine. He can even perform several malicious tasks such as stealing banking information or exfiltrating important documents.

Further research on the domain revealed that it has been actively distributing Android malware, none of which, however, infected our phone during the experiment. It appears to exploit the common CVE-2012-0158 vulnerability, which works against unpatched versions of Microsoft Office 2003, 2007, and 2010.³ Had the document been opened in Microsoft Office 2010, depending on its patch level, the attack would have likely succeeded as well.

As in the smartphone's case, a Trend Micro product built for Windows PCs such as Trend Micro Titanium™ Security, would almost certainly have been able to prevent the bug exploitation. Patching the OS to the latest level would have also helped prevent the exploit from properly executing.

Macbook Air

Like the smartphone and the Windows-based laptop, we unboxed the Macbook Air as well and left all of the installed OS's default settings in place.

Once connected to a hotel Wi-Fi access point, we started browsing the Internet the same way any user would. We landed on a fake media site *<REDACTED>.ru/files/synboz/*, which then redirected us to *http://phimx.<REDACTED>.net/files/*. While being redirected, a file called *av.app* (MD5: *00c5ed370509b21e675d42096e883190*) was dropped onto the machine. The same hash has been seen elsewhere as early as December 10, 2013.⁴ We saw the following displayed on the redirect page as all of the above were going on in the background.

³ The MITRE Corporation. (2014). CVE. "CVE-2012-0158." Last accessed February 7, 2014, <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158>.

⁴ *VirusTotal*. (2014). Last accessed February 7, 2014, <https://www.virustotal.com/intelligence/search/?query=00c5ed370509b21e675d42096e883190>.



Figure 3: Prompt to right-click and open the file seen after redirection

We proceeded to right-click and choose “Open.” Had we not right-clicked and opened the file, Macintosh® Gatekeeper running on OS X® 10.8.5 would have caught and prevented the file from running. Once executed, *std.app* also created a back door and communicated with the IP address, *146.185.128.92*, for subsequent access.

The application may be considered a piece of malware, specifically a “valid” keylogger. Even if it serves a “legitimate” purpose, it can also be easily repurposed to log keystrokes, pull out saved browser passwords, and perform a variety of other nefarious acts.

Aobo Software
Aobo Keylogger for Mac – Records Passwords

877-882-8905 (Toll Free)

Aobo Mac Products Windows Products Mobile Products Purchase Download Support

Ultimate Keylogger for Mac that Records Passwords

Aobo Keylogger for Mac is the only invisible Keylogger for Mac OS X with Password Recording ability. In figuring out what people are doing on the Mac, Aobo Mac Keylogger gives full play to its logging features to monitor, record almost everything include keystrokes and Passwords typed, web history, chat messages, screen snapshots, and send logs to you by email or FTP automatically. [View all features](#)

- ✓ **Record user activities on Mac**
Record keystrokes, passwords(Pro only), websites visited in Safari, Chrome, Firefox, chat logs, social networking activity, email sent, and take screenshots.
- ✓ **Invisible and reliable monitoring tool**
Run in **Hidden** background on Mac, no trace to show its existence, and provide password protection. Aobo Keylogger offers you invisible and reliable monitoring solution.

Record Any activity

Free Trial

Purchase Now

Parental Control Spy on Mac computers Monitor Home Mac Employee Monitoring

Figure 4: Website of a legitimate software, Aobo Keylogger for Mac, which was maliciously used by the attacker

The techniques used to exploit the Macbook Air do not differ that much from those used against those browsing the Web on Windows machines, which shows that the attack was not targeted. All it required to succeed were an unpatched system and unsafe online behavior on the user's part.

Had the application not been executed or had the machine been running a reliable security solution such as Trend Micro Titanium Security for Mac, the Macbook Air is not likely to have been infected. As it turns out, we already detect the file as TROJ_GEN.F47V1210.

Conclusion

Attacks occur worldwide everyday in many countries. Of course, some do originate from Russia. Attacks can occur while you are sitting in a coffee shop in Berlin, Tokyo, or Philadelphia but in this case, Richard was sitting in a Russian café so his Google search returned several local results. The combination of default security settings, unpatched software, and risky behavior, not zero-days, was the reason the devices he used got infected.

While the infections appeared to have automatically occurred due to the editing process on TV (which did not show the user interaction), no zero-days were used and all infections required user interaction and several risky behaviors to succeed.

The experiment results featured in this paper revealed that the following general best practices should help protect devices and the data they contain from similar attacks:

- **Update software.** When using a new laptop, immediately update it from a trusted source and on a secure Internet connection.
- **Don't rely on default security settings.** Install a multilayered security solution that relies not just on malware detection but also on Web reputation, behavior monitoring, and email scanning.
- **Trust your instinct.** If you find an email from a random person suspicious, don't click links embedded in or open files attached to it. Or better yet, don't even open it.
- **Go straight to the source.** Rely only on trusted sites when looking for information on any much-discussed event such as the Sochi Olympics. Keep in mind that the more hype and attention an event gets, the more likely that attackers will abuse it.

Following the recommendations above can help prevent attacks like those we encountered in Moscow from succeeding.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2014 by Trend Micro, Incorporated. All rights reserved. Trend Micro and 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.



Securing Your Journey
to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900