Trend Micro Forschungsbericht

Liebesgrüße aus Moskau

Trend Micro Honeypots im Experiment für NBC News

Autor: Kyle Wilhoit

Forward-Looking Threat Research Team

Inhalt

Einleitung

Kürzlich hatte NBC News den Autor zur Teilnahme an einem Versuch mit dem Auslandskorrespondenten des Senders Richard Engel in Moskau eingeladen. Dafür erstellte das Trend Micro-Team eine Honeypot-Umgebung als Emulation eines Nutzers, der während der Olympischen Spiele in Sotschi die üblichen Aktivitäten durchführt, etwa im Internet browsen, E-Mails abrufen und über Instant Messaging Nachrichten empfangen und senden. Die Versuchsteilnehmer wollten herausfinden, wie einfach bestimmte Geräte kompromittiert werden können, während ein Nutzer normale Online-Aktivitäten ausführt. Drei Geräte wurden aufgesetzt – ein Macbook Air®, ein Lenovo ThinkPad® mit Windows® 7 und ein Samsung Galaxy S Android™ Smartphone.

Angriffe, wie die im Versuch festgestellten, können von überall auf der Welt kommen, doch scheinen diejenigen, die mit Russland in Verbindung gebracht werden, häufiger zu sein. Dieses Forschungspapier zeigt im Detail, wie die Umgebung aufgesetzt war und was mit den drei Geräten geschah.

Obwohl die Infektionen scheinbar automatisch infolge des Editier-Prozesses im Fernsehen passierten (zeigte die Nutzerinteraktion nicht), wurden keine Zero-Day-Lücken ausgenutzt und alle Infektionen hatten als Voraussetzung eine Nutzerinteraktion und riskantes Verhalten.

Aufsetzen der Versuchsumgebung

Als Erstes musste die Konfiguration der Umgebung festgelegt werden. NBC News wollte den Versuch auf neuen Geräten durchführen, die keine Sicherheits- oder Software-Updates hatten. Die Entscheidung gegen Basisvorkehrungen sollte die realistische Situation normaler russischer Nutzer während der Olympischen Spiele in Sotschi abbilden. Sie wollten die Bedrohungen für diejenigen Teilnehmer verstehen, die keine entsprechenden Maßnahmen getroffen hatten. Es mussten Standardanwendungen auf den Geräten vorhanden sein, die zum „Lifestyle“ gehören oder auch so genannte „Produktivitäts“-Anwendungen wie Microsoft™ Office®, Adobe® Flash®, Java™ und andere zum Ansehen von Webseiten oder für die Dokumentenverarbeitung. Wegen der breiten Nutzerbasis wählte das Team Microsoft Office 2007 und lud dann die neueste Version von Flash und Java herunter.

Als Nächstes musste das Team überlegen, wie der Netzwerkverkehr gesammelt werden sollte, denn ohne diese Möglichkeit hätte sich der bösartige vom normalen Verkehr nicht unterscheiden lassen. Die Lösung bestand darin, einen eigenen WLAN Access Point zwischen dem Hotelnetz und den Geräten “einzuschleifen”. Dies erlaubte es, direkten Zugriff auf den Verkehr zu erhalten, der von den Geräten nach draußen geht. Um die Umgebung so sauber wie möglich zu halten, installierte das Team Logging- und Monitoring-Tools auf eine separate Linux-Maschine und eine virtuelle Maschine, die dazu verwendet wurden, um den Netzwerkverkehr abzufangen und zu analysieren. Sie nutzten eine Kombination aus Snort (eigene und Standard-Regeln), BroIDS, tcpdump, ntop und interne Trend Micro-Tools für die Identifizierung bekannter C&C-Server sowie von bösartigen Binaries, die die Geräte infizieren können.

Zusätzlich zum Aufsetzen einer Logging-Lösung verband das Team auch ein E-Mail-Konto, das Richard Engels tatsächliche Inbox emulierte, mit dem Telefon. Die genutzte E-Mail-Adresse stammte aus der NBC News-Domäne und war der richtigen E-Mail-Adresse von Engel sehr ähnlich. Dies sollte einen möglichen Angreifer glauben lassen, die Adresse sei echt. Dasselbe E-Mail-Konto wurde auf jedem Gerät genutzt.

Nutzeraktivitäten

Für die meisten Schadsoftware-Angriffe ist eine wie auch immer geartete Nutzeraktivität erforderlich, damit eine Infektion stattfindet. Während der Testperiode von 72 Stunden besuchten die Versuchsteilnehmer Websites, die auch ein normaler Tourist aufgerufen hätte.

Samsung Galaxy S4

Eine Kompromittierung kann in Russland genauso schnell passieren wie in jedem anderen Land. Alle Sicherheitseinstellungen auf dem Samsung Galaxy S4 auf Android-Basis wurden bei der Ankunft im Land unverändert im Default-Zustand belassen. Dann erhielt das Gerät eine SIM-Karte eines russischen Mobilfunk-Providers, MTS. Das Gerät wurde mit einem offenen WLAN-Zugangspunkt in einem Café verbunden. Der Versuchsteilnehmer begann im Internet zu surfen wie jeder andere Reisende. Viele der besuchten Websites hatten mit den Olympischen Spielen zu tun.

Der Autor besuchte eine Sotschi-Site und wurde zu einer anderen weitergeleitet, wo er aufgefordert wurde, eine App *(avito.apk)* herunterzuladen, die angeblich wichtige Reiseinformationen lieferte. Nach dem Download der .APK-Datei *(*MD5: *6d6cb42286c3c19f642a087c9a545943)* kam die Aufforderung, diese zu installieren. Dies wurde vom Autor mit „Akzeptieren“ angenommen, gemäß der Annahme, dass ein normaler Nutzer das auch tun würde. Die App installierte sich auf das Smartphone, ohne dass ein Icon zu sehen war. Nach einer Weile begann sie (eine Schadsoftware) mit *http://<REDACTED>/ getTask.php/imei=<VALUE>&balance=0* und *http://<REDACTED>/reg.php/country=us& phone=<VALUE>&op=Android&balance=0&imei=<VALUE>* zu kommunizieren.

Bild 1: Dieses Bild wird angezeigt, während die Site die bösartige .APK-Datei ablegt (Der Screenshot stammt vom Macbook Air, das eine gemeinsame E-Mail-Adresse mit dem Samsung Galaxy S4 Smartphone hat)

Beim Ausführen füllt *avito.apk* die Felder “Country,” “Phone,” “Balance” und “imei” mit Werten vom verseuchten Telefon aus. Dadurch konnte der Angreifer darauf die E-Mails lesen, auf damit verbundene, externe Medien zugreifen, Kontaktinformationen sammeln, Anrufe mitschneiden und verschiedene weitere Aktivitäten ausführen. Auf *apploader.ru* sah das Team, dass verschlüsselter Verkehr zu besagter Domäne über Port 443 floss. Die bösartige App scheint Teil der SMSSEND Malware-Familie zu sein. Diese hat bis heute mehr als 200.000 Android-Telefone infiziert.[1]

Trend Micro hat seit April 2010 bereits Varianten der SMSSEND-Familie identifiziert. Trend Micro™ Mobile Security blockiert den Zugriff auf alle damit in Verbindung stehenden URLs und Binaries.

Lenovo ThinkPad

Das Team installierte Windows 7 auf dem Lenovo ThinkPad, weil dies das weltweit am häufigsten genutzte Microsoft-Betriebssystem ist.[2] Auch hier wurden die Default-Sicherheitseinstellungen beibehalten.

Nach etwa 30 Stunden erhielt Richard Engels gefälschtes Konto eine Spear-Phishing-Mail. Die Nachricht kam von *quentorn1971@gmail.com* (MD5: *85a97e1550be413b850f76a5a3a36272*), von jemand, der angeblich Informationen für Engel hatte, und zwar in Form eines Links auf ein Olympia-bezogenes Dokument.

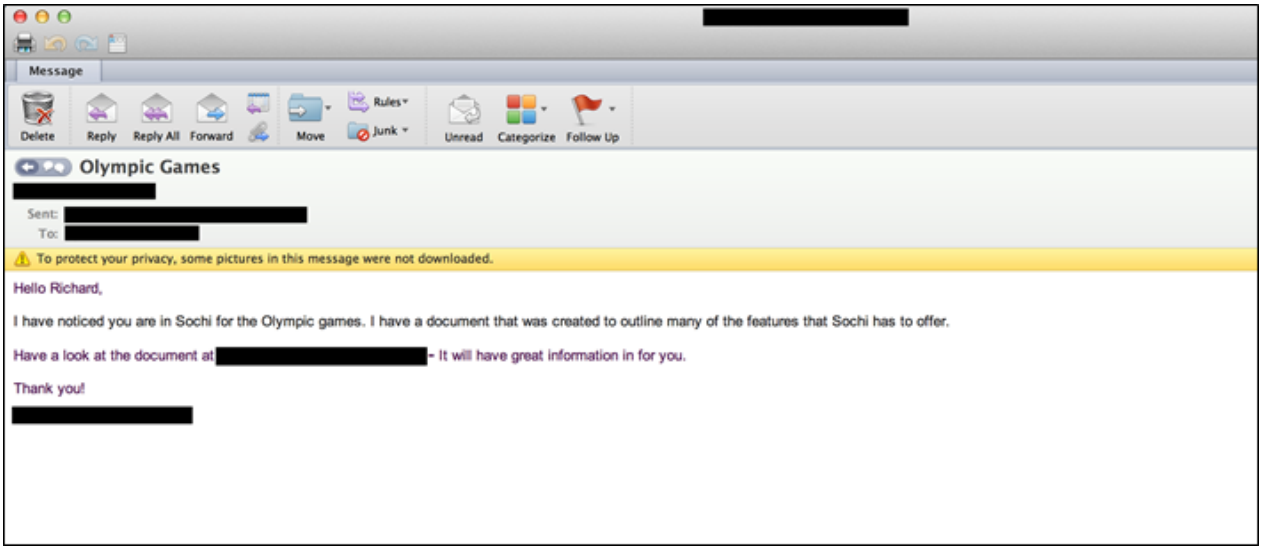

Bild 2: Spear-Phishing-E-Mail an Engel, nachdem seine vorher erzeugte E-Mail-Adresse mit allen Geräten verbunden wurde (der Screenshot stammt vom Macbook Air mit der gemeinsamen E-Mail-Adresse mit dem Lenovo ThinkPad)

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). NetMarketshareSM. “Desktop Operating System Market Share.”Last accessed February 7, 2014, http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0.

Anscheinend wurde Engels E-Mail-Adresse vom infizierten Samsung Galaxy S4 Smartphone weitergegeben. Möglicherweise dachte der Angreifer, der sich Zugang zum Smartphone verschafft hatte, dass Engel ein wertvolles Ziel sei und schickte deshalb die Spear-Phishing-Mail.

Der eingebettete Link führt zum Download eines Microsoft Word®-Dokuments namens *Olympics.doc* (MD5: *09326cec312ff356dde41d2e007fd009*). Beim Öffnen des Dokuments wird ein einfaches Signal an *whatsappload.ru* geschickt. Innerhalb einer Minute öffnete eine Schadsoftware einen Backdoor, der mit derselben Site über Port 443 in Verbindung stand. So konnte der Angreifer auf die infizierte Maschine zugreifen und sogar mehrere bösartige Aufgaben durchführen, so etwa Bankinformationen stehlen oder wichtige Dokumente abziehen.

Weitere Nachforschungen auf der Domäne zeigten, dass die Malware aktiv Android-Schadsoftware verteilt hatte, welche jedoch das Telefon während des Experiments nicht infizierte. Sie scheint die bekannte Sicherheitslücke CVE-2012-0158 auszunützen, die in ungepatchten Versionen von Microsoft Office 2003, 2007 und 2010 vorhanden ist.[3] Wäre das Dokument in Microsoft Office 2010 geöffnet worden, so hätte der Angriff je nach Patch-Level ebenfalls Erfolg gehabt.

Wie schon im Fall des Smartphones hätte ein Trend Micro-Produkt, das auf Windows-PCs zugeschnitten ist, wie Trend Micro Titanium™ Security, bestimmt den Missbrauch der Lücke verhindert. Auch die Aktualisierung des Betriebssystems hätte geholfen.

Macbook Air

Auch im Fall des Macbook Air blieben die Einstellungen unverändert.

Nach der Verbindung mit einem WLAN-Zugang im Hotel startete das Team die gleichen Aktivitäten wie ein normaler Nutzer, also Browsen im Internet. Dabei landete der Autor auf einer gefälschten Media Site *<REDACTED>.ru/files/synboz/*, die ihn zu *http://phimx.<REDACTED>.net/files/* umleitete. Dabei wurde eine Datei namens *av.app* (MD5: *00c5ed370509b21e675d42096e883190*) auf der Maschine abgelegt. Dieselbe Hash-Summe war bereits am 10. Dezember 2013 gesichtet worden.[4] Folgendes erschien auf der Seite, alles andere passierte im Hintergrund:

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.

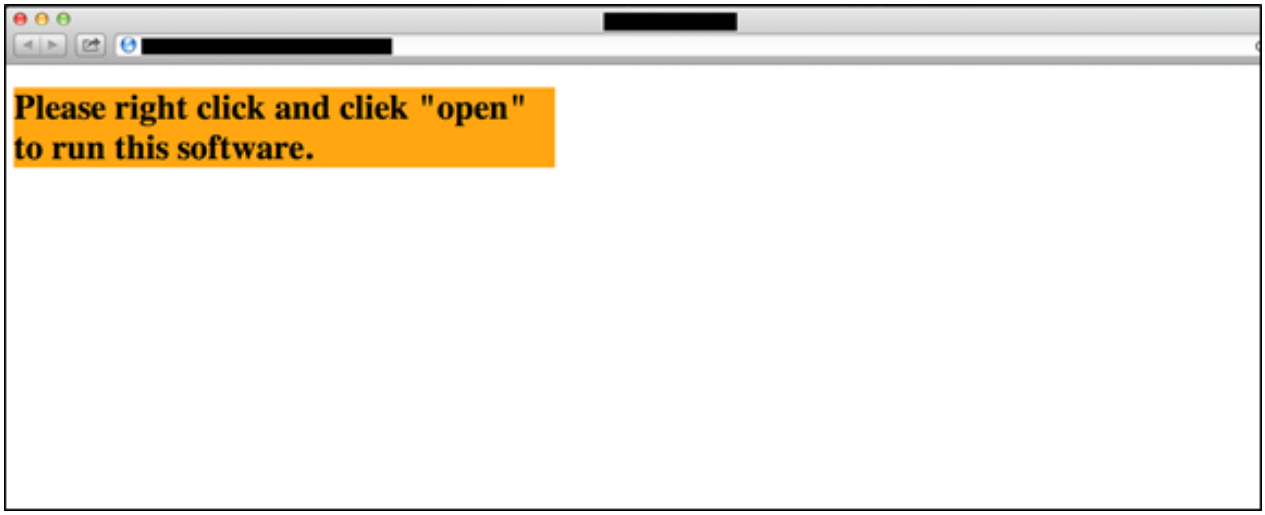

Bild 3: Aufforderung, die Datei nach der Umleitung zu öffnen

Das Team kam der Aufforderung nach: Hätte der Autor nicht mit einem rechten Mausklick die Datei geöffnet, hätte der Macintosh® Gatekeeper unter OS X® 10.8.5 die Datei abgefangen und an der Ausführung gehindert. std.app erzeugte beim Ausführen ebenfalls einen Backdoor und kommunizierte mit der IP-Addresse *146.185.128.92.*

Die Anwendung lässt sich als Schadsoftware einstufen, und zwar als Keylogger. Auch wenn sie einem legitimen Zweck dient, kann sie auch einfach zum Aufzeichnen von Tastenanschlägen, zum Stehlen von Browser-Passwörtern und weiteren bösartigen Aktionen zweckentfremdet werden.

Bild 4: Website der legitimen Software Aobo Keylogger for Mac, die vom Angreifer für seine Zwecke missbraucht wird

Die Techniken, die für die Angriffe auf das Macbook Air verwendet wurden, unterscheiden sich kaum von denen gegen Windows-Maschinen. Das zeigt, dass der Angriff nicht gezielt war. Alles, was es für den Erfolg brauchte, war ein ungepatchtes System und das riskante Online-Verhalten des Nutzers.

Wäre die Anwendung nicht ausgeführt worden oder hätte es eine zuverlässige Sicherheitslösung auf der Maschine (wie Trend Micro Titanium Security for Mac) gegeben, so wäre es nicht zur Infektion des Macbooks gekommen. Trend Micro erkennt die Datei bereits als TROJ_GEN.F47V1210.

Schlussfolgerung

Angriffe passieren weltweit jeden Tag. Natürlich nehmen einige ihren Anfang in Russland. Doch können Nutzer auch angegriffen werden, während sie in Berlin, Tokio oder Philadelphia im Café sitzen. In diesem Fall jedoch saß Engel in einem russischen Café, sodass seine Google-Suche mehrere lokale Ergebnisse lieferte. Die Kombination aus Standard-Sicherheitseinstellungen, nicht gepatchter Software und riskantem Verhalten war der Grund für die Infektion seiner Geräte – und nicht Zero-Day-Lücken.

Obwohl die Infektionen scheinbar automatisch infolge des Editier-Prozesses im Fernsehen passierten (zeigte die Nutzerinteraktion nicht), wurden keine Zero-Day-Lücken ausgenutzt und alle Infektionen hatten als Voraussetzung eine Nutzerinteraktion und riskantes Verhalten.

Die Ergebnisse des Versuchs zeigen, dass folgende Best Practices den Schutz von Geräten und der darauf gespeicherten Daten vor ähnlichen Angriffen erhöhen können:

- **Update der Software.** Jeder neue Laptop sollte sofort aus einer vertrauenswürdigen Quelle und über eine sichere Internet-Verbindung aktualisiert werden.
- **Keine voreingestellten Sicherheits-Settings.** Nutzer müssen eine mehrschichtige Sicherheitslösung installieren, die nicht nur auf Malware-Entdeckung baut, sondern auch Web-Reputation, Monitoring des Verhaltens und E-Mail-Scanning bietet.
- **Der Intuition vertrauen.** Scheint eine E-Mail von einem zufälligen Absender verdächtig, so sollten keine Links darin angeklickt und auch keine Dateien im Anhang geöffnet werden. Idealerweise sollte die Mail gar nicht geöffnet werden.
- **Direkt zur Quelle.** Nutzer sollten sich nur auf vertrauenswürdige Sites verlassen, wenn sie Informationen zu so aktuellen Ereignissen wie die Olympischen Spiele suchen. Je mehr Hype sich um etwas rankt, desto wahrscheinlicher ist es, dass Angreifer diese Öffentlichkeit ausnützen.

Über TREND MICRO

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als zwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.

http://www.trendmicro.de/
http://blog.trendmicro.de/
http://www.twitter.com/TrendMicroDE

Securing Your Journey
to the Cloud

TREND MICRO DEUTSCHLAND GMBH

Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799
www.trendmicro.com