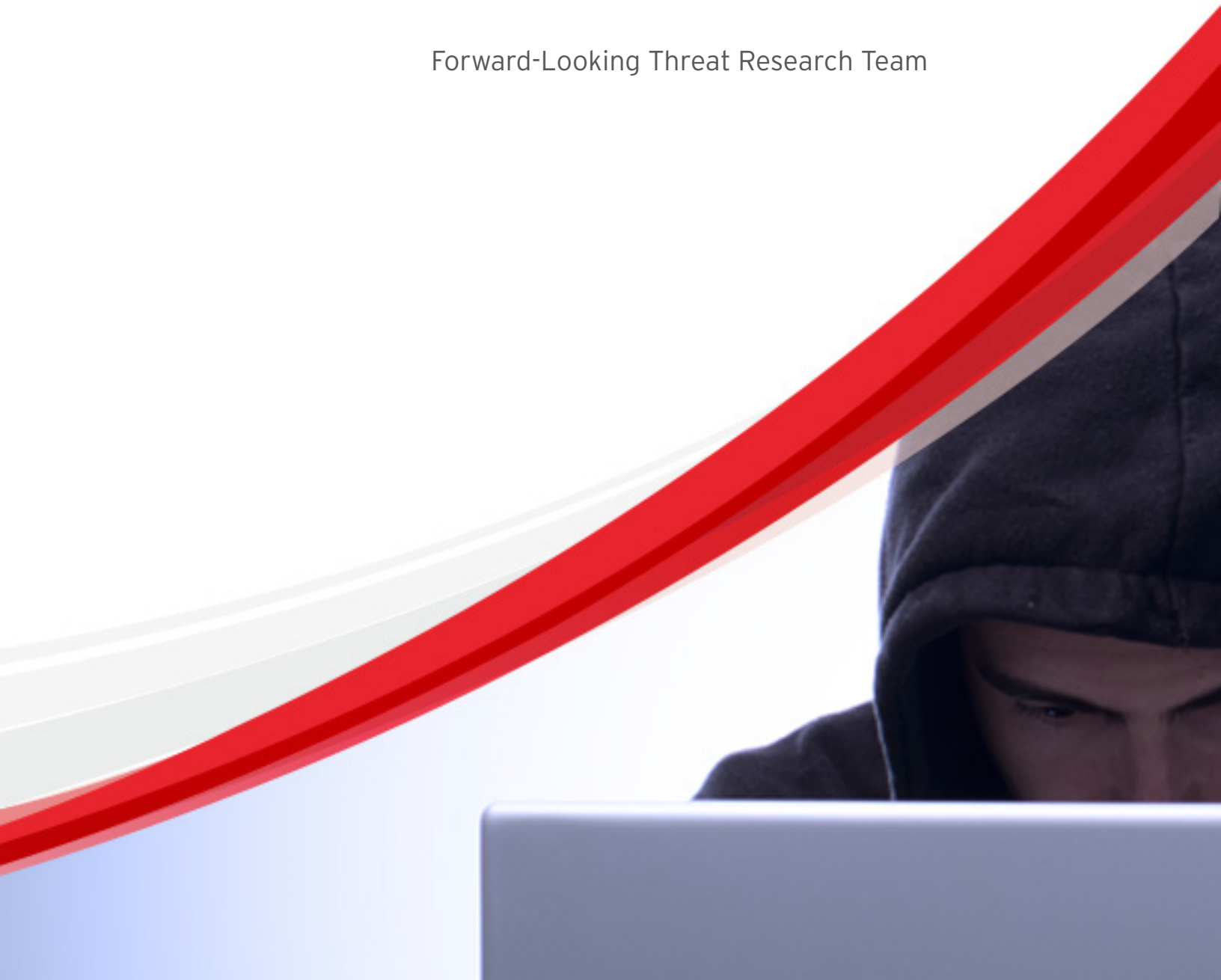


On the Actors Behind MEVADE/SEFNIT

Forward-Looking Threat Research Team



Contents

Introduction..... 1

Enormous Uptick in Tor Users in August 2013 2

Infection Vectors 5

InstallBrain Monetizes Nonbuyers 7

iBario Ukraine 11

Smoking Guns 12

 Antivirus Check System..... 13

 MEVADE/SEFNIT Code Repository 14

Conclusion..... 14

References 14

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

In 2013, an Israeli/Ukrainian adware company pushed additional click-fraud malware known as “MEVADE/SEFNIT” into the vast network of computers in which its adware have been installed. This was not an isolated incident; there is strong evidence showing that since early 2011, this adware company has been directly involved in the development of MEVADE/SEFNIT malware. This illustrates the great risk adware pose to Internet users. Adware are often regarded as low-risk threats, but in reality, adware companies can decide to discreetly load dangerous malware onto the computers on which their adware have been installed anytime.

The MEVADE/SEFNIT actors managed to keep a low profile for a long time until August 2013 when they chose to modify the way their bots communicated with the bot master. As soon as they did that, their network of millions of bots was noticed by the security industry and large corporations in the United States. Earlier in the year, Trend Micro had already commenced an investigation into MEVADE/SEFNIT malware and had learned the identity of some of the individuals responsible. MEVADE/SEFNIT malware were subsequently linked to an abrupt increase in the number of Tor users, which increased from 1 million to more than 5 million within a couple of weeks. This put the Tor network under a lot of stress, not so much because of increased bandwidth, but rather because of increased computing power that was needed to handle all requests from new users. The Tor network barely managed to stay up.

There was considerable speculation on the cause of this sudden increase but the Tor developers soon realized that the enormous uptick in users was actually caused by a botnet. This botnet was later confirmed to be MEVADE/SEFNIT. MEVADE/SEFNIT refer to malware that primarily commit click fraud and some Bitcoin mining. Since at least 2011, MEVADE/SEFNIT malware have been highly likely sponsored by an adware company operating in Israel with contractors from the Ukraine.

Enormous Uptick in Tor Users in August 2013

Around the middle of August 2013, the number of Tor users increased from about 1 million to more than 5 million.¹

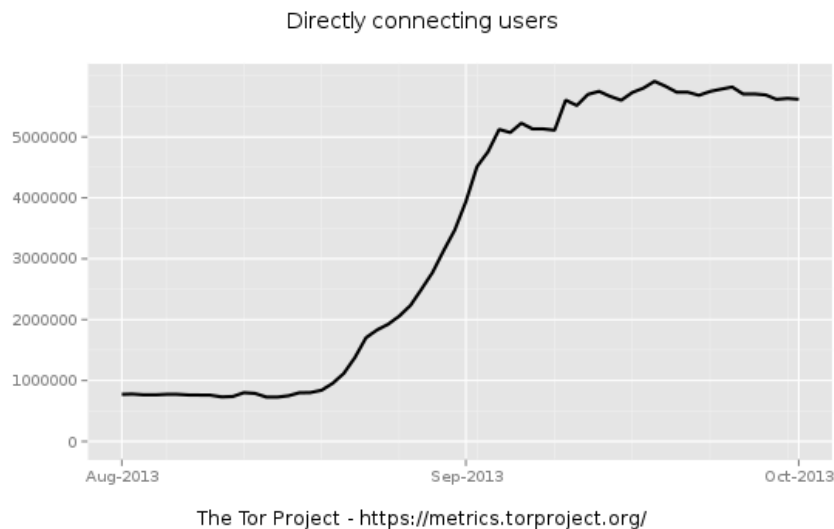


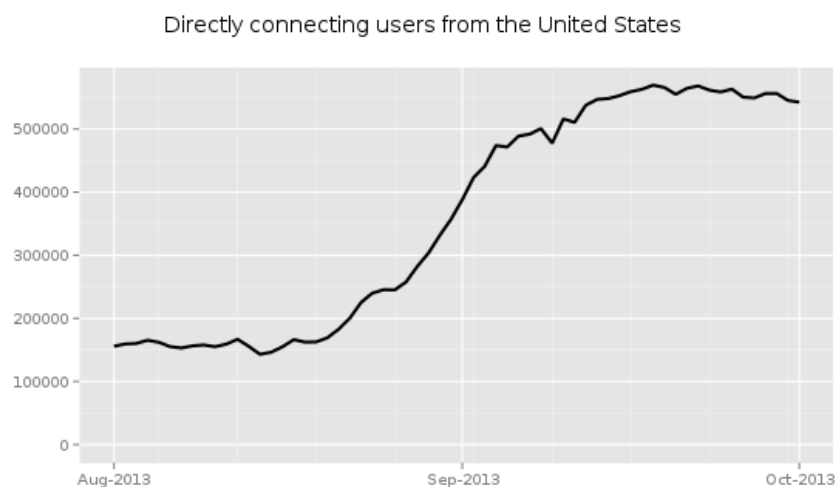
Figure 1: August 2013 saw a dramatic increase in Tor users

It soon became clear that a botnet was responsible for the dramatic increase in Tor users. Fox-IT was the first company to publish information on the cause of the dramatic uptick in Tor users—a botnet consisting of millions of infected computers called “MEVADE/SEFNIT.”² Smaller botnets have previously used Tor as a communication channel between infected nodes and their bot master, but these botnets were relatively small and did not lead to stability problems for the Tor network.

The Trend Micro Forward-Looking Threat Research (FTR) Team has been following MEVADE/SEFNIT since early 2013 and learned the identity of those behind this malware family.³ When we learned that the enormous uptick in Tor users was caused by MEVADE/SEFNIT malware, we disclosed some of the nicknames of those responsible for the threat.

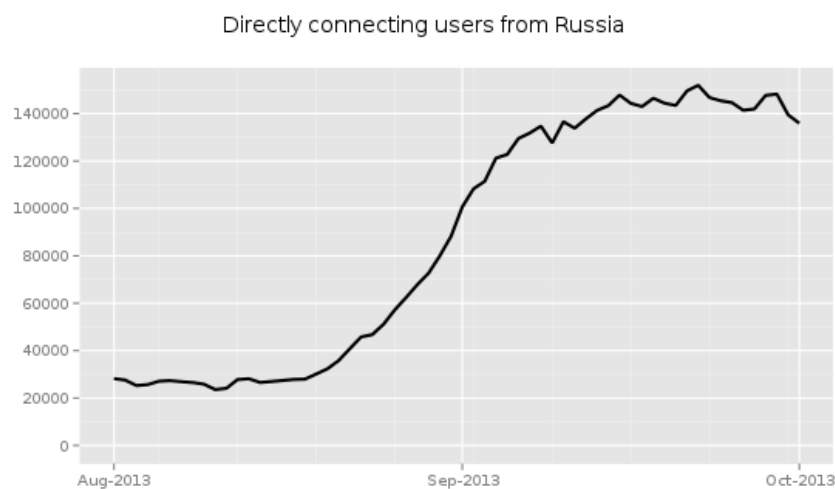
MEVADE/SEFNIT malware have been known for search engine result hijacking and click fraud since at least 2010.⁴ In August 2013, the actors behind MEVADE/SEFNIT malware experimented with Tor for the command and control of their bots.⁵ This move by the MEVADE/SEFNIT actors did not go unnoticed. Tor is not suitable for controlling millions of bots at the same time, particularly as its number of legitimate users is only around 1 million.

A hint as to who may be behind MEVADE/SEFNIT malware can be seen by observing the Tor usage in different countries in August and September 2013. The number of Tor users dramatically increased in August 2013 in countries such as the United States, Russia, and the Ukraine.



The Tor Project - <https://metrics.torproject.org/>

Figure 2: Number of Tor users in the United States



The Tor Project - <https://metrics.torproject.org/>

Figure 3: Number of Tor users in Russia

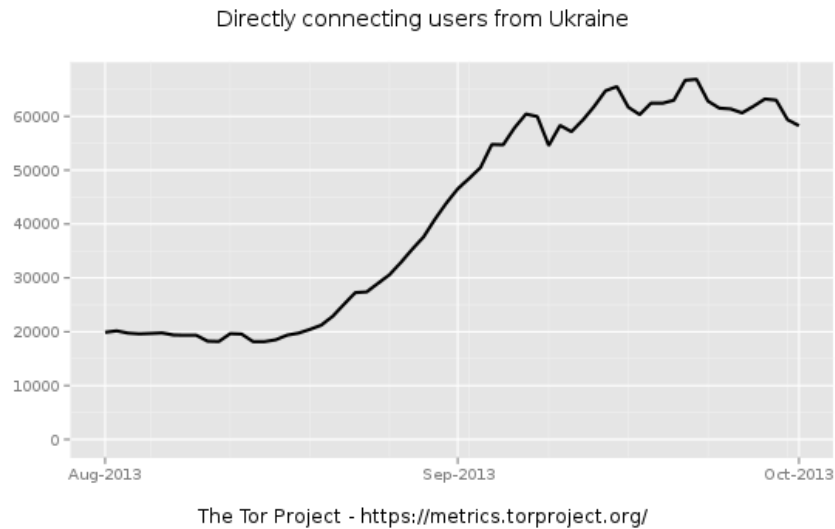


Figure 4: Number of Tor users in the Ukraine

Other countries also showed a dramatic increase in Tor users. There were a few exceptions though. Some of these were countries where Tor is actively blocked by the government. But there is one other country where the number of Tor users remained more or less flat—Israel.

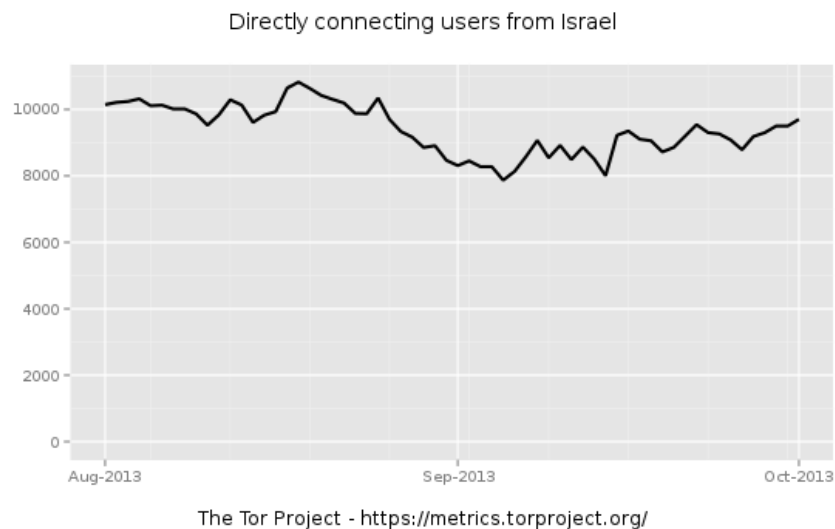


Figure 5: Number of Tor users in Israel

This may not be a coincidence. Using the Trend Micro™ Smart Protection Network™ infrastructure, we determined that the MEVADE/SEFNIT malware that downloaded an additional Tor component were widespread.⁶ There were infections in more than 68 countries, even in sparsely populated ones.

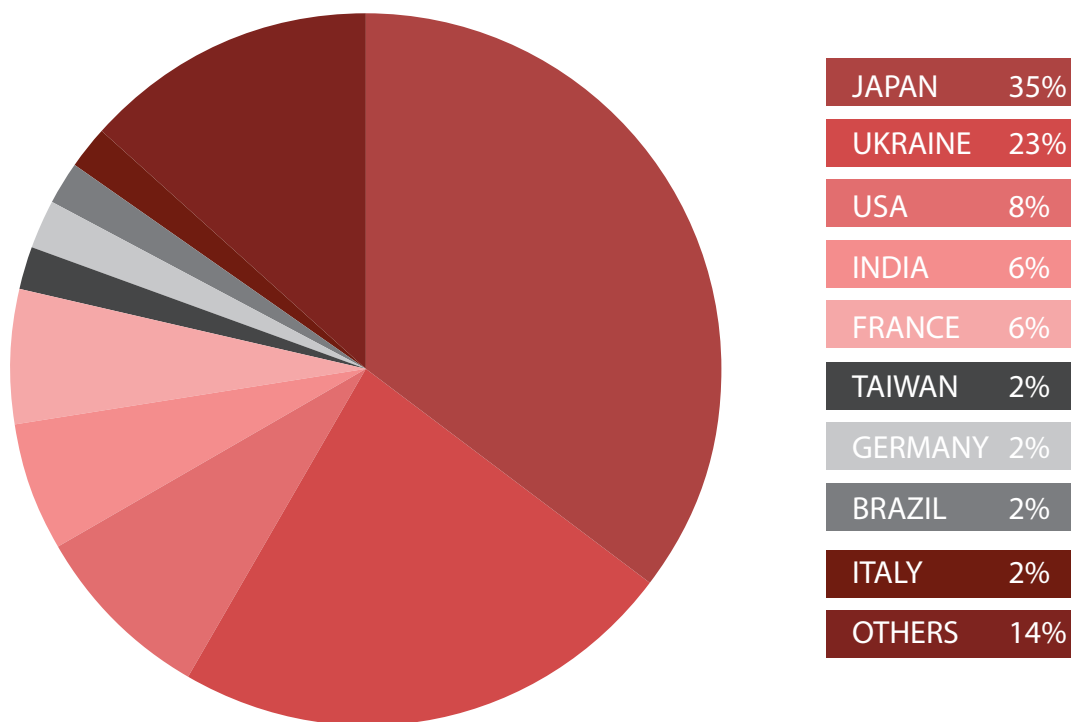


Figure 6: BKDR.MEVADE.C was seen in 68 countries but not in Israel⁷

But in one developed country—Israel—the number of infections was virtually zero. The actors appeared to want to avoid Israel and chose not to infect users there. It is possible that the actors did not want to have problems with Israeli law enforcement agencies. This would make sense if the actors operated from Israel. As it turns out, MEVADE/SEFNIT malware are most likely sponsored by an adware company located in Israel since at least early 2011. This adware company has an office in a suburb of Tel Aviv and appears to have contractors located in the Ukraine.

Infection Vectors

MEVADE/SEFNIT malware can be installed on victims' computers in various ways. One notable way is via adware called "InstallBrain."⁸ Other adware such as Bprotect and File Scout can also install MEVADE/SEFNIT malware. Microsoft has published a couple of very useful posts on this topic.

InstallBrain has been installed on millions of computers. There are more than 5 million different InstallBrain adware variants in the wild. There have been InstallBrain detections in around 150 countries, which shows how widespread the adware are. It also confirms the dangers that adware can pose, particularly when developers decide to install malware into their massive network of computers containing their adware.

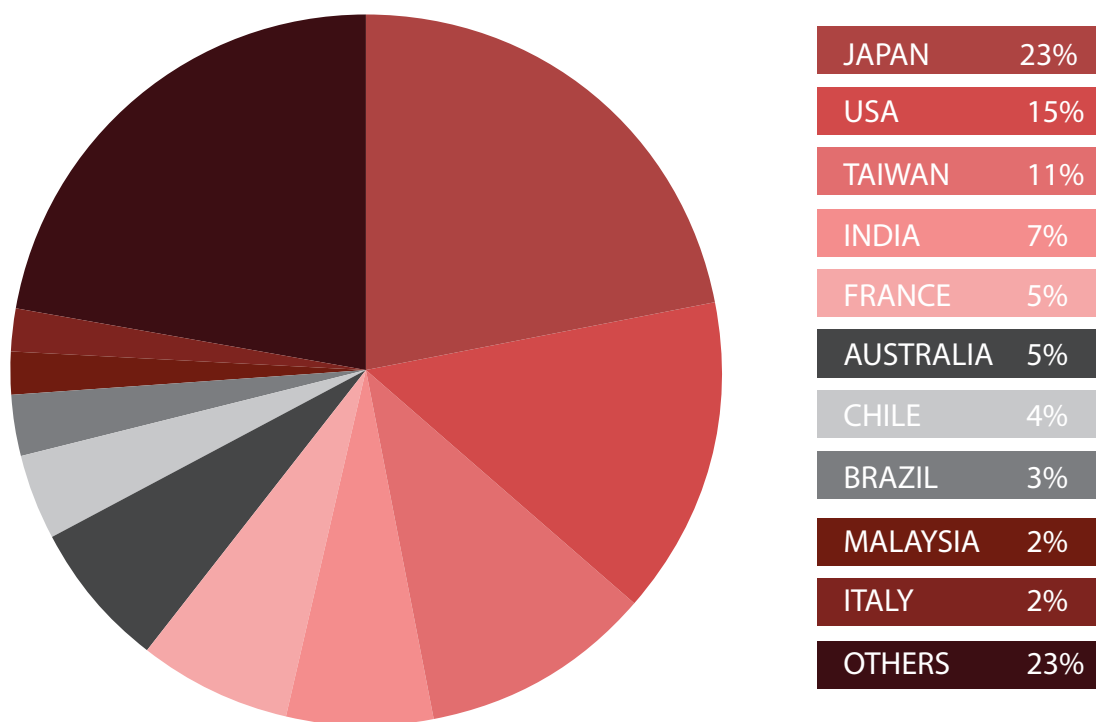


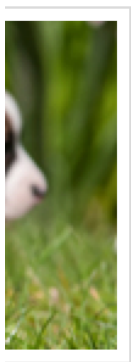
Figure 7: InstallBrain was detected in around 150 countries worldwide

As noted in a Microsoft blog post, InstallBrain and MEVADE/SEFNIT malware bear some similarities in their code and in their way of contacting command-and-control (C&C) servers.^{9, 10, 11} Microsoft also described in a post that Rotbrow—its detection name for Bprotect—is a MEVADE/SEFNIT malware distributor.¹²

InstallBrain and Bprotect appear to have originated from an adware company called iBario, Ltd. located in Israel.

InstallBrain Monetizes Nonbuyers

One of the mottos on the website of InstallBrain is “Monetize On Non-buyers.” This is a rather bold motto and may suggest the type of adware company iBario is—one that wants to make money at all costs.



Monetize On Non-buyers

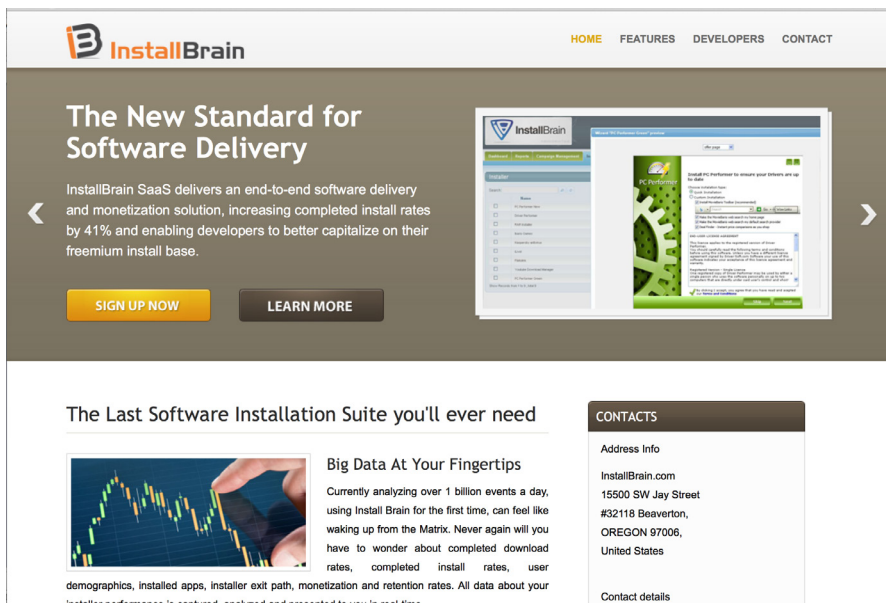
No matter how great your products are, chances are a large percentage of the users who download your product are not going to convert into paying customers. Thanks to InstallBrain, you no longer have to think of

es with dozens of monetization channels, letting you extract

s. Your InstallBrain account manager will custom tailor the

Figure 8: Motto taken from the InstallBrain website
(<http://www.installbrain.com>) on July 3, 2014

However, there is a big difference between iBario and other adware companies that operate in the gray zone. iBario—the owner of InstallBrain—went one step further by spreading MEVADE/SEFNIT malware across its vast network of InstallBrain-infected computers.¹³



The New Standard for Software Delivery

InstallBrain SaaS delivers an end-to-end software delivery and monetization solution, increasing completed install rates by 41% and enabling developers to better capitalize on their freemium install base.

SIGN UP NOW **LEARN MORE**

The Last Software Installation Suite you'll ever need

Big Data At Your Fingertips

Currently analyzing over 1 billion events a day, using Install Brain for the first time, can feel like waking up from the Matrix. Never again will you have to wonder about completed download rates, completed install rates, user demographics, installed apps, installer exit path, monetization and retention rates. All data about your installer performance is monitored, analyzed and presented to you in real time.

CONTACTS

Address Info

InstallBrain.com
15500 SW Jay Street
#32118 Beaverton,
OREGON 97006,
United States

Contact details

Figure 9: InstallBrain website (<http://www.installbrain.com>) screenshot taken on June 27, 2014

InstallBrain is a brand name of iBario. It appeared on the website of iBario until at least January 2014.

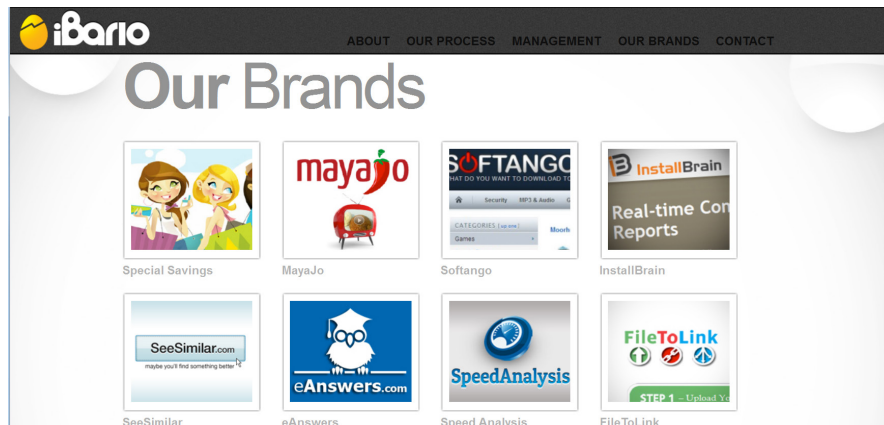


Figure 10: InstallBrain was featured in the “Brands” section of the iBario website (<http://www.ibario.com>); screenshot taken on January 20, 2014

InstallBrain was subsequently removed from the iBario corporate website. This may have been in response to Microsoft calling out InstallBrain about installing MEVADE/SEFNIT malware.¹⁴ iBario replaced the logo of InstallBrain with that of UnknownFile.

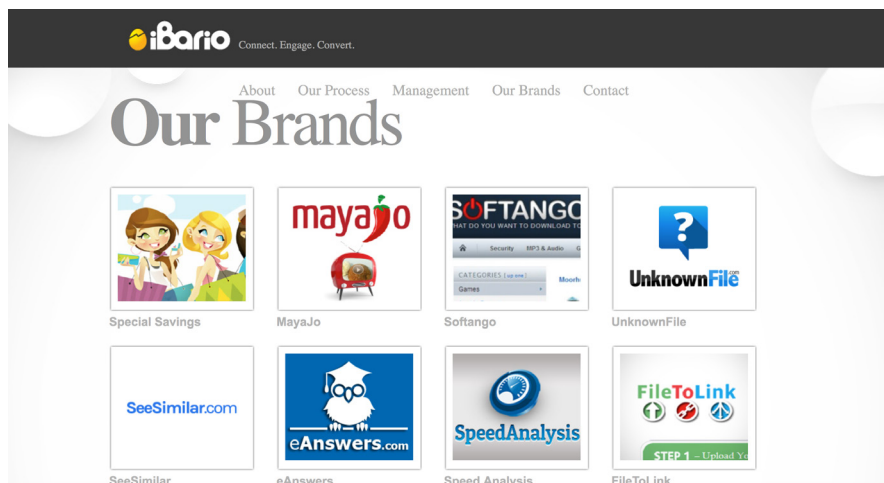


Figure 11: InstallBrain was replaced with UnknownFile on the iBario website; the UnknownFile logo can still be seen on the iBario website as of June 25, 2014

However, it appears that UnknownFile is just another name for InstallBrain. On the unknownfile.com website, people can search for and download programs that can supposedly read files with specific file extensions.

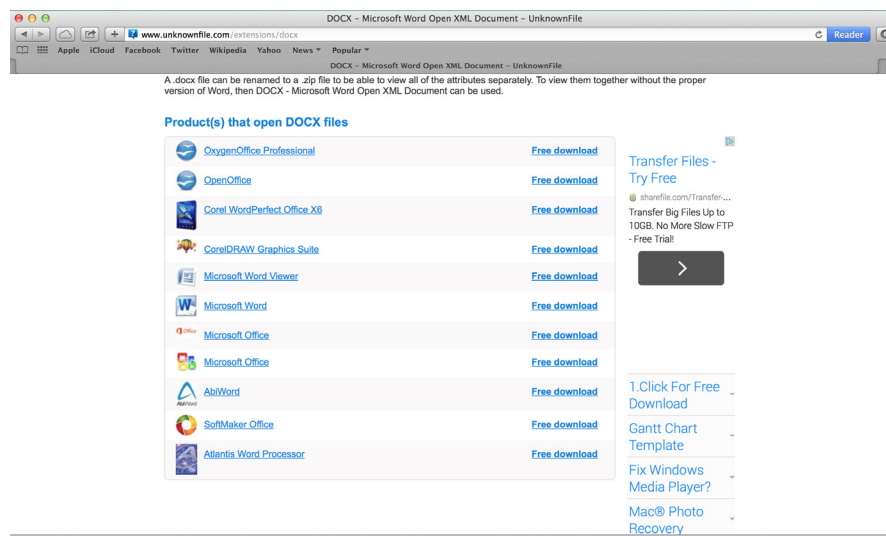


Figure 12: Screenshot of a page on the UnknownFile website (<http://unknownfile.com>) taken on June 25, 2014

If one searches for .DOCX—the well-known extension for Microsoft™ Word® documents—the UnknownFile website provides basic information on the file extension and prompts the user to download OpenOffice or Microsoft Office® to open .DOCX files. When downloaded, the user receives a file (SHA1 hash: e83cae08441b360936594e2a59814b4fe3bdad0c) that is not OpenOffice but instead one of the many variants of InstallBrain. This is at least misleading because it tricks Internet users into installing unwanted software, which is not an uncommon practice by adware companies.

iBario allegedly offers free downloads of Microsoft Office and other copyrighted software through the UnknownFile website. At the same time, iBario appears to have issued four requests to be removed from Google search results in 2012 and 2013 because of alleged copyright infringement. All removal requests were for websites that explained how to remove the adware of iBario. Of course, all four requests were declined by Google because it was not concerned with copyright infringement.

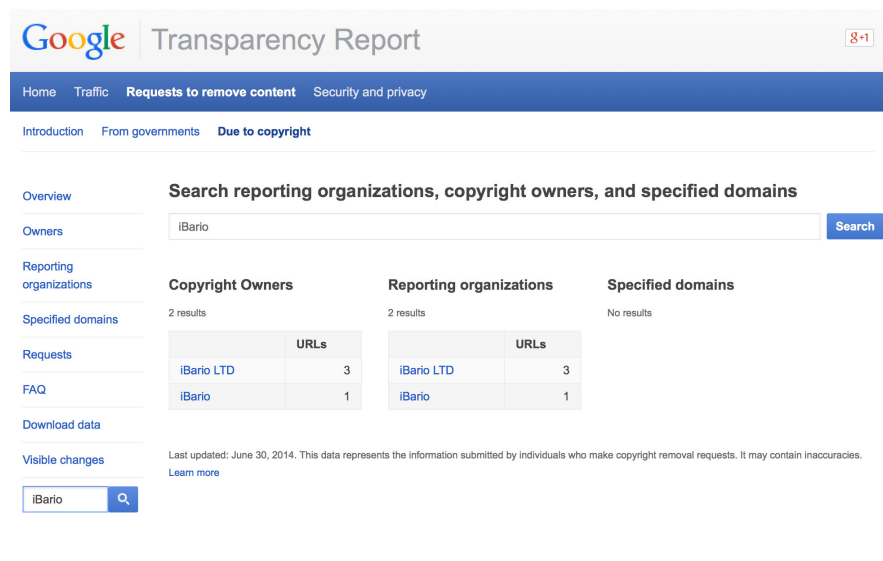


Figure 13: Requests filed by iBario as seen in a Google Transparency Report screenshot taken on June 30, 2014

Microsoft has been explicit in saying it has seen InstallBrain (Brantall) and Bprotect (Rotbrow) install MEVADE/SEFNIT malware. We have seen similar evidence. Ukrainian individuals working for iBario have been constantly tweaking InstallBrain to specifically evade anti-malware detection. They have been working on a project called "Antivirus Check System (ACS)," which checks for anti-malware detection rates before new malware are used in the wild. It is one of the key points iBario has been working on with contractors in the Ukraine to constantly develop new versions of InstallBrain with low anti-malware detection rates. This shows that the Ukrainian individuals who developed InstallBrain and MEVADE/SEFNIT malware actually worked for iBario.

iBario Ukraine

In recent interviews, an iBario executive claimed that iBario is an entirely Israeli company that does not outsource any work abroad.¹⁵ However, there is evidence on the Internet that proves otherwise.

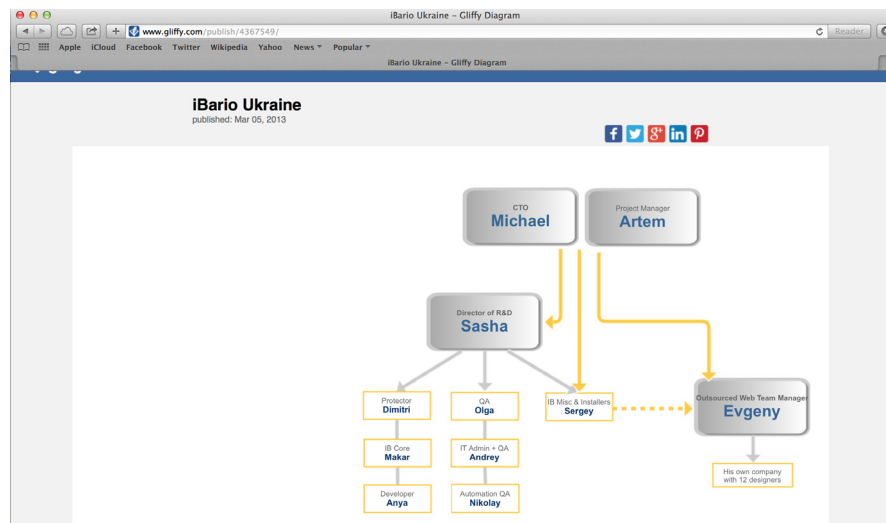


Figure 14: Organizational chart for iBario Ukraine; screenshot taken on June 20, 2014

The author of this document is unknown and the organizational chart only shows first names. The chart is likely authentic, however, as it is consistent with other known data. “Michael” probably refers to the former CTO of InstallBrain who moved to San Francisco, California; he previously lived in the Ukraine and in Israel. “Artem,” who is listed as a “project manager,” holds a PhD from the Kharkov National University of Radio Electronics. “Makar” has used the nickname, “jeday,” online and is apparently responsible for the core of InstallBrain.

Though iBario claims that all of its development takes place in Israel, a significant portion of the work is performed in the Ukraine. Online pictures of visits to tourist spots in Israel only confirms that these Ukrainian contractors visited Israel. For example, one contractor who uses the nickname, “Bisovman,” posted pictures in tourist spots in Jerusalem and near a hotel in Tel Aviv in 2013. These pictures are consistent with other known data.



Figure 15: Bisovman visiting Jerusalem; image taken from vk.com on July 4, 2014



Figure 16: Bisovman in Tel Aviv; screenshot taken from vk.com on July 3, 2014

Smoking Guns

One of the Ukrainian contractors of iBario, Denis R., also known as “Scorpion,” used his domain, *codeconst.com*, to host a source code management system and a project management system for iBario. Parts of these systems were available to the public for a time.

Antivirus Check System

Figure 17 below shows the project plan for ACS on *dev.codeconst.com*. We do not know if this system was ever completed but its intention is very clear—evading anti-malware detection. Bad actors often check first whether security companies already detect their malware or not before they launch them in the wild.

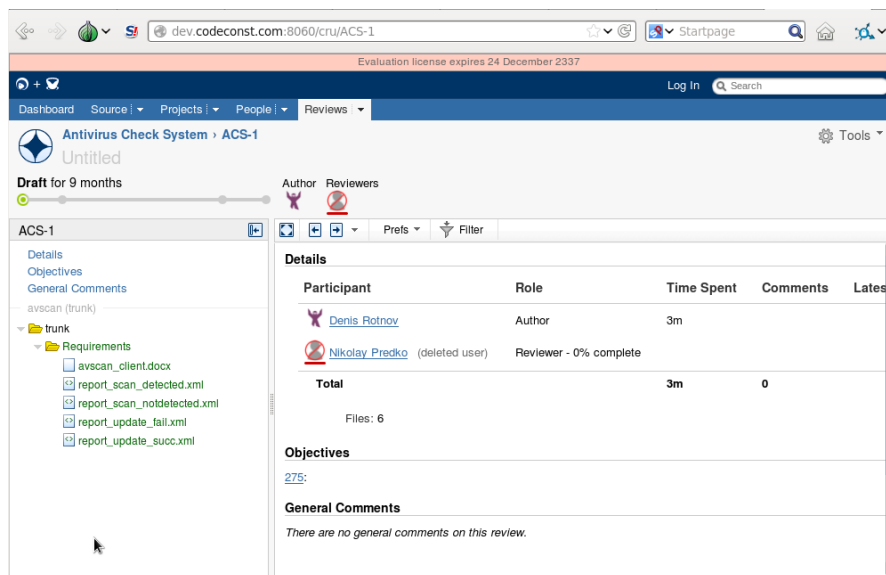


Figure 17: Plans for ACS; screenshot taken on August 29, 2013

ACS was probably developed to evade anti-malware detection for iBario adware. There are millions of unique InstallBrain files in the wild.

A list of all of the users on the project management system was available on *dev.codeconst.com*, including the names of several Ukrainian iBario contractors as well as the CTO of InstallBrain, Michael F.

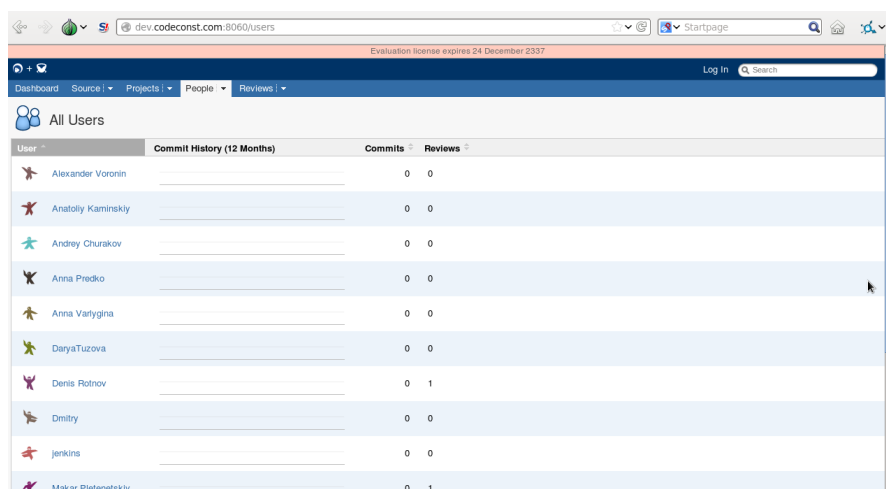


Figure 18: InstallBrain's CTO is included in the list of ACS users as seen in the Fisheye project management tool; screenshot taken on August 29, 2013

MEVADE/SEFNIT Code Repository

Since 2011, the corporate network of iBario appears to have been maintaining MEVADE/SEFNIT malware in a code repository system hosted on *master.codeconst.com*. This host name pointed to the IP address, 37.58.66.234, which belongs to an IP block owned by iBario in Israel.

Facts such as iBario having MEVADE/SEFNIT malware in a code repository system in 2011 and that iBario's InstallBrain and Bprotect were seen installing MEVADE/SEFNIT malware in 2013 are strong evidence that iBario has been directly involved in developing and spreading MEVADE/SEFNIT malware since at least 2011.

Conclusion

The history of MEVADE/SEFNIT demonstrates that adware can pose great risks to end users. Internet users are often misled to install stuff they do not want to. At any point in time, an adware company can decide to install more dangerous malware in users' computers. iBario appears to be one such example.

MEVADE/SEFNIT malware have been existing under the radar for several years. The MEVADE/SEFNIT actors made a decision in August 2013 to update their botnet with a Tor component, which changed bots' C&C mechanism to use hidden Tor services. However, Tor could barely handle the additional load of 4 million MEVADE/SEFNIT bots, which caused MEVADE/SEFNIT malware and those responsible for them to be exposed.

References

- [1] arma. (September 5, 2013). *Tor*. "How to Handle Millions of New Tor Clients." Last accessed July 6, 2014, <https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients>.
- [2] Fox-IT. (September 5, 2013). "Large Botnet Cause of Recent Tor Network Overload." Last accessed, July 6, 2014, <http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/>.
- [3] Feike Hacquebord. (September 5, 2013). *TrendLabs Security Intelligence Blog*. "The Mysterious MEVADE Malware." Last accessed July 6, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-mysterious-mevade-malware/>.
- [4] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "SEFNIT." Last accessed July 6, 2014, <http://about-threats.trendmicro.com/us/search.aspx?p=SEFNIT>.
- [5] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "MEVADE Serves Adware, Hides Using SSH and Tor." Last accessed July 6, 2014, <http://about-threats.trendmicro.com/us/webattack/130/MEVADE+Serves+Adware+Hides+Using+SSH+and+Tor>.
- [6] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "MEVADE." Last accessed July 6, 2014, <http://about-threats.trendmicro.com/us/search.aspx?p=MEVADE>.

- [7] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “BKDR_MEVADE.C.” Last accessed July 6, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_MEVADE.C.
- [8] Microsoft. (2014). *Microsoft Malware Protection Center*. “Win32/Sefnit.” Last accessed July 6, 2014, <http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32/Sefnit#tab=2>.
- [9] msft-mmpc. (September 25, 2013). *Microsoft Malware Protection Center*. “Mevade and Sefnit: Stealthy Click Fraud.” Last accessed July 6, 2014, <http://blogs.technet.com/b/mmpc/archive/2013/09/25/mevade-and-sefnit-stealthy-click-fraud.aspx>.
- [10] msft-mmpc. (January 9, 2014). *Microsoft Malware Protection Center*. “Tackling the Sefnit Botnet Tor Hazard.” Last accessed July 6, 2014, <http://blogs.technet.com/b/mmpc/archive/2014/01/09/tackling-the-sefnit-botnet-tor-hazard.aspx>.
- [11] msft-mmpc. (March 5, 2014). *Microsoft Malware Protection Center*. “Sefnit’s Tor Botnet C&C Details.” Last accessed July 6, 2014, <http://blogs.technet.com/b/mmpc/archive/2014/03/05/sefnit-s-tor-botnet-c-amp-c-details.aspx>.
- [12] msft-mmpc. (December 10, 2013). *Microsoft Malware Protection Center*. “Rotbrow: The Sefnit Distributor.” Last accessed July 6, 2014, <http://blogs.technet.com/b/mmpc/archive/2013/12/10/rotbrow-the-sefnit-distributor.aspx>.
- [13] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “ADW_BRANTALL.” Last accessed July 6, 2014, http://about-threats.trendmicro.com/us/malware/ADW_BRANTALL.
- [14] Microsoft. (2014). *Microsoft Malware Protection Center*. “Win32/Brantall.” Last accessed July 6, 2014, <http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Brantall>.
- [15] David Shamah. (May 19, 2014). *The Times of Israel*. “Meet iBario, Israel’s \$100-Million Internet Empire.” Last accessed July 6, 2014, <http://www.timesofisrael.com/meet-ibario-israels-100-million-internet-empire/>.

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