ZEROACCESS

THE MOST PROFITABLE BOTNET MALWARE IN THE WILD

A case study of the affiliate marketing and peer-to-peer (P2P) activities of ZeroAccess, one of the most profitable botnets operating today

Extracted from F-Secure's H2 2012 Threat Report

F-Secure

ZEROACCESS

THE MOST PROFITABLE BOTNET MALWARE IN THE WILD

ZeroAccess is one of today's most notable botnets. It was first discovered by researchers back in 2010, when it drew a lot of attention for its capability for terminating all processes related to security tools, including those belonging to anti-virus products. When too many researchers focused on this self-protection capability however, ZeroAccess' author decided to drop the feature and focus more on improving its custom peer-to-peer (P2P) network protocol, which is unique to ZeroAccess. After the change[1] , ZeroAccess became easier to spot by anti-virus products, yet it continued to spread like wildfire around the world due to the improved P2P technique[2]. This success can be largely attributed to its affiliate program.

Affiliate program: ZeroAccess success story

Affiliate programs are a well-known marketing strategy and are widely used by many e-commerce websites[3]. Essentially, a business owner with an e-commerce site to promote commissions other site owners to help drive customers to it (and hopefully eventually make a purchase). The website owners are then compensated for providing these customer leads.

The variety of distribution schemes and methods used by the numerous affiliates have contributed to the volume of trojan-dropper variants detected by antivirus products every day. All driven by the same motive which is to collect attractive revenue share from the gang.

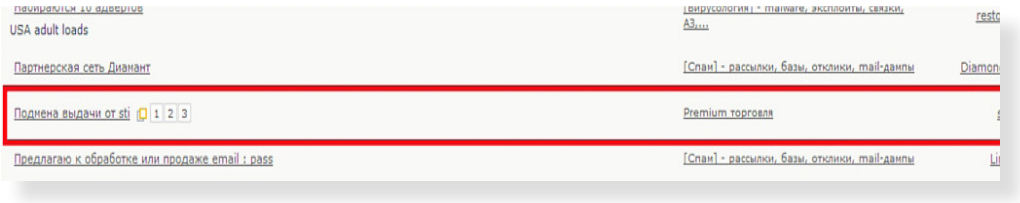


Figure 1: A botnet operator seeking partners in an underground forum

Adopting this concept, ZeroAccess's author or operator(s) has managed to distribute the program to a large number of machines with the help of its enlisted partners.

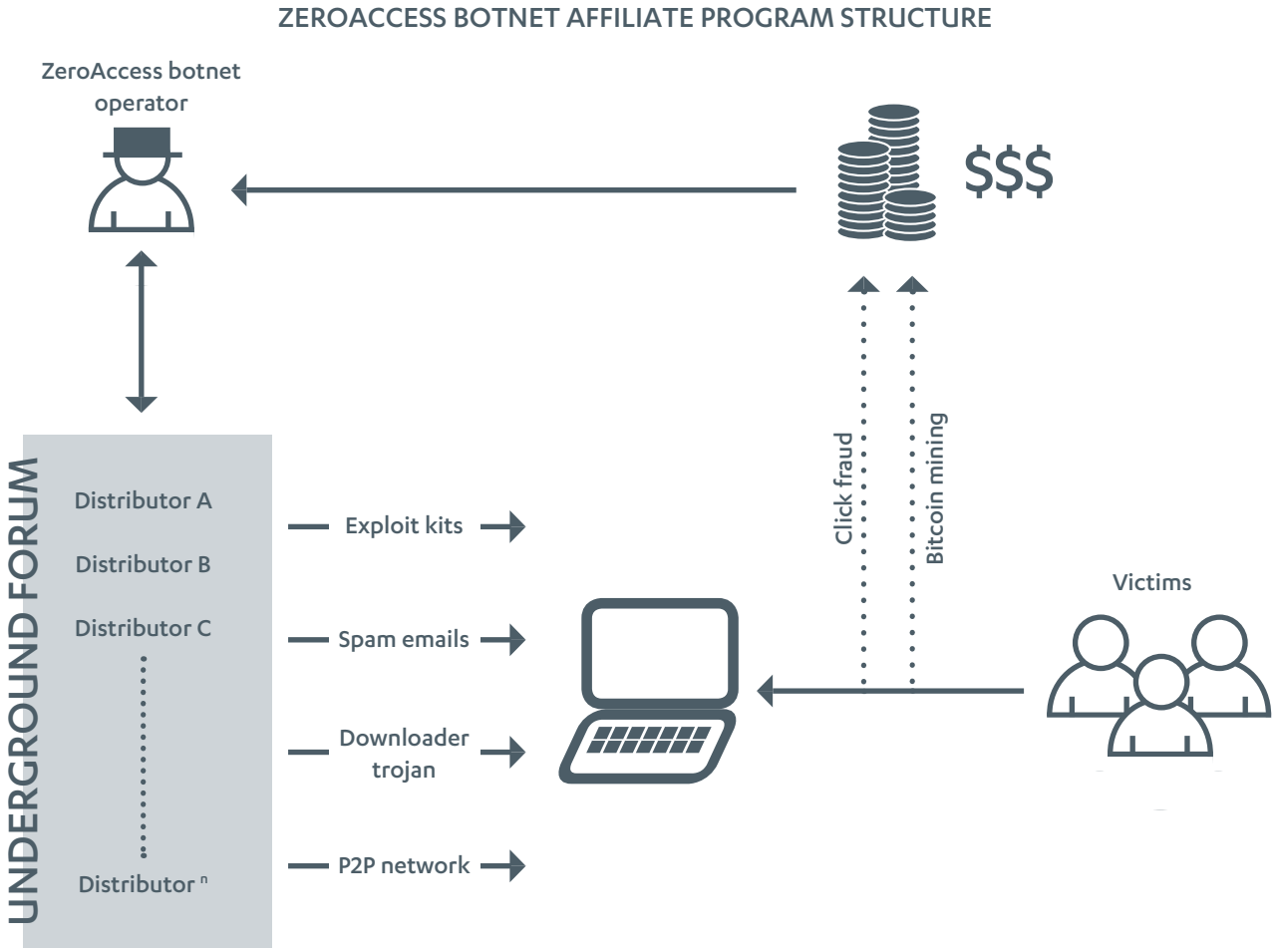
The ZeroAccess gang advertises the malware installer in Russian underground forums, actively looking for distributor partners. Their objective is to seek other cybercriminals who are more capable in distributing the malware and do so more efficiently.

The malware distributors generally consist of experienced affiliates, each of them employing their own methods of distributing the Zeroaccess installers, in order to fulfill the recruiter's requirements.

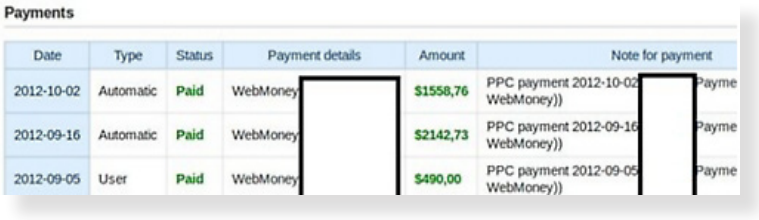
The most popular distribution methods we've seen involve exploit kits, spam e-mails, trojans-downloaders, and seeding fake media files on P2P file-sharing services and on video sites, though the specific details in each case depend on the distributor handling the operations.

METHODS USED BY ZEROACCESS DISTRIBUTORS

DISTRIBUTION METHODS	
Downloader trojan	Dropping a downloader trojan onto a machine, which proceeds to download and install the botnet
Exploit kit	Using an exploit kit (e.g., Blackhole) in a drive-by-download attack
Fake media file or keygen or crack	Hosting infected files in P2P file sharing services using enticing names, such as '*microsoft.office.2010.vl.editi.keygen.exe*'
P2P file sharing service	Abusing a P2P file sharing website to host the ZeroAccess installer
Spam email	Sending spam emails containing an attachment or a link that could enable further exploitation



The partners are compensated based on a Pay-Per-Install (PPI) service scheme[4] and the rate differs depending on the geographical location of the machine on which the malware was successfully installed. A successful installation in the United States will net the highest payout, with the gang willing to pay USD 500 per 1,000 installations in that location.


Payments

Date	Type	Status	Payment details	Amount	Note for payment
2012-10-02	Automatic	Paid	WebMoney	$1558,76	PPC payment 2012-10-02 WebMoney)) Payme
2012-09-16	Automatic	Paid	WebMoney	$2142,73	PPC payment 2012-09-16 WebMoney)) Payme
2012-09-05	User	Paid	WebMoney	$490,00	PPC payment 2012-09-05 WebMoney)) Payme

Figure 2: Proof of payments made by recruiter

Given the rate of pay, it is no surprise that ZeroAccess is widespread in the US alone[5]. After the US, the commission rate sorted from highest to lowest are Australia, Canada, Great Britain, and others. Some distributors even post screenshots of the payment they've received in underground forums to show the reliability of their recruiter.

The ZeroAccess gang can afford to pay such high incentives to its recruits because the army of bots created by the affiliate's efforts is able to generate even more revenue in return.

Once the malware is successfully installed on the victim machines, ZeroAccess will begin downloading and installing additional malware onto the machines, which will generate profit for the botnet operators through click fraud and Bitcoin mining operations.

Botnet operators prefer the click fraud payload because since 2006 [6], it has been a proven way to generate income from the pay-per-click (PPC) or the cost-per-click advertising.

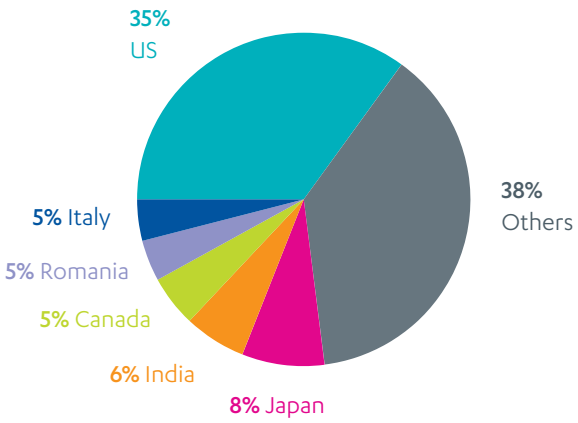
Bitcoin mining has too many constraints. For instance, the success of generating a bitcoin depends on the difficulty level of the target specified in the Bitcoin network and might even require some luck[7]. Furthermore, the victim's machine needs to run on a decent CPU power, preferably with GPU or FPGA hardware, in a reasonable amount of time[8]. Even with a large number of botnets, the difficulty factors in solving Bitcoin blocks hinder Bitcoin mining operation from performing as well as click fraud which only requires the victims to have an internet connection and a web browser.

Despite the difficulties in Bitcoin mining, the fact that the ZeroAccess botnet was modified to drop its problematic self-protection feature and introduce the Bitcoin mining operations indicates that ZeroAccess's operators are very ambitious to keep the botnet growing and are not afraid of taking risks.

Conclusion

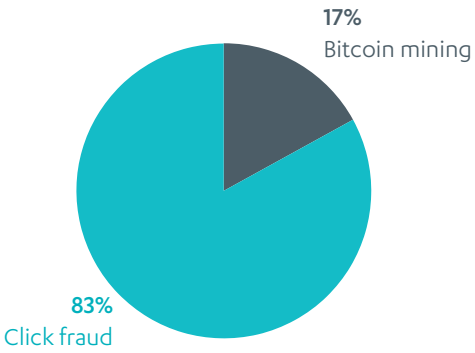
Given ZeroAccess's current success as a huge, fully functional profit-generating 'machine', it's unlikely that we'll see it going away anytime soon. The ZeroAccess malware - which poses the most direct threat to the users - will continue to exist as a hidden danger on malicious or boobytrapped websites. The affiliate program that encourages the spread of malware will continue to attract more cybercriminals due to the botnet operators' established reputation for reliably paying its affiliates and adjusting commission rates to maintain their attractiveness. And finally, the criminal organization behind the botnet have demonstrated that they're willing to experiment and modify their 'product' in order to increase their ability to make money. As such, we expect the ZeroAccess botnet to grow and evolve, with new features or feature updates being introduced in the near future.

ZEROACCESS INFECTIONS, TOP COUNTRIES BY PERCENTAGE (%)



*Based on statistics gathered from national ASN-registered networks.

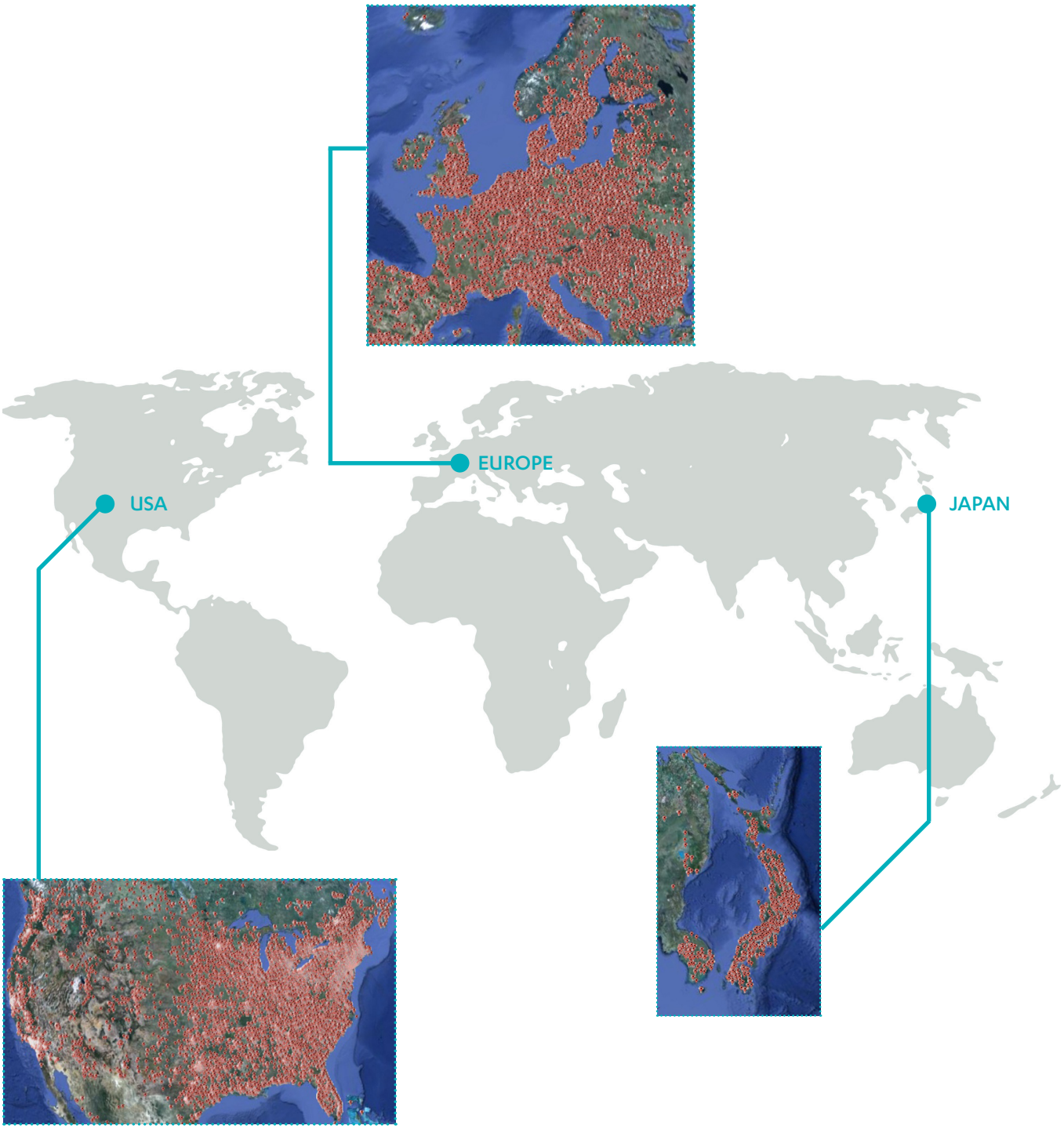
ZEROACCESS'S PROFIT-GENERATING ACTIVITIES, BY PERCENTAGE (%)



SOURCES

[1] F-Secure Weblog; Threat Research; *ZeroAccess's Way of Self-Deletion*; published 13 June 2012;
http://www.f-secure.com/weblog/archives/00002385.html
[2] F-Secure Weblog; Sean Sullivan; *ZeroAccess: We're Gonna Need a Bigger Planet*; published 17 September 2012;
http://www.f-secure.com/weblog/archives/00002428.html
[3] Wikipedia; *Affiliate Marketing;*
http://en.wikipedia.org/wiki/Affiliate_marketing
[4] Wikipedia; *Compensation Methods;*
http://en.wikipedia.org/wiki/Compensation_methods#Pay-per-install_.28PPI.29
[5] F-Secure Weblog; Sean Sullivan; *The United States of ZeroAccess*, published 20 September 2012;
http://www.f-secure.com/weblog/archives/00002430.html
[6] MSNBC; Associated Press; *Google settles advertising suit for $90 million*; published 8 March 2006;
http://www.msnbc.msn.com/id/11734026/#.ULiDyN2sHvA
[7] Bitcoin Wiki; Target;
http://en.bitcoin.it/wiki/Target
[8] Wikipedia; *Bitcoin;*
http://en.wikipedia.org/wiki/Bitcoin

ZEROACCESS INFECTIONS IN THE USA, JAPAN, AND EUROPE*



*Red markers indicate an infected unique IP address or cluster of IP addresses.

F-Secure in Brief

F-Secure has been protecting the digital lives of consumers and businesses for over 20 years. Our Internet security and content cloud services are available through over 200 operators in more than 40 countries around the world and are trusted in millions of homes and businesses.

In 2011, the company's revenues were EUR 146 million and it has over 900 employees inmore than 20 offices worldwide. F-Secure Corporation is listed on the NASDAQ OMX Helsinki Ltd. since 1999.

Protecting the Irreplaceable

F-Secure