Securing Your Journey to the Cloud

TARGETING THE SOURCE

FAKEAV AFFILIATE NETWORKS

Nart Villeneuve

A 2011 Trend Micro White Paper

Abstract

The underground ecosystem provides everything required to set up and to maintain a malware operation for a minimal investment. It enables those with limited technical skills and with a few underground connections to earn significant returns on their investment. The operators of malicious networks are increasingly monetizing their activities by propagating rogue security software that use scare tactics to trick unsuspecting users into installing and purchasing fake antivirus software, aka FAKEAV.

This research paper focuses on how FAKEAV affiliate networks operate, what propagation strategies they use, and how much they earn from their malicious activities. It explores the various underground connections among malicious actors, including the emergence of "meta" affiliate networks that act as mid-tier FAKEAV providers. These meta affiliates aggregate the malicious links and the malware provided by top-tier FAKEAV affiliates and make these available to those with limited underground connections. The complexity of these affiliate networks poses significant challenges to law enforcement agencies and to the security industry. Unlike direct fraud such as stealing sizable amounts of money from compromised bank accounts, the damage that results from FAKEAV infections is considerable in the aggregate, the amount of criminal activity conducted in any one jurisdiction and against any particular victim remains small. As a result, many smaller malicious operations connected with FAKEAV affiliates are able to avoid scrutiny.

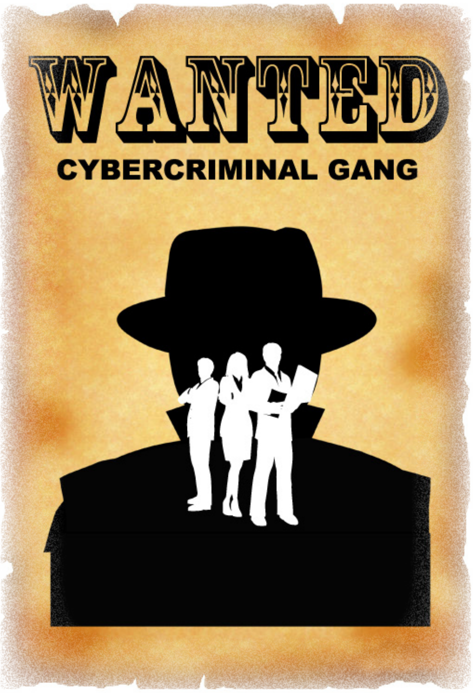
In order to mitigate the threats FAKEAV pose, we need to understand the environment in which related malicious activities occur. This is, after all, just as important as the technical details of the malware that cybercriminals use. Analyzing how affiliate networks operate provides an understanding of malicious actors' motivation, their capabilities, and their composition. Distinguishing between the affiliate networks that supply FAKEAV and the malicious networks (e.g., botnets) used to propagate these allows us to target their sources and not just their distributors. Infiltrating these affiliate networks allows us to acquire malicious URLs and malware in order to provide timely detection and blocking as FAKEAV providers supply them to their affiliates.

Introduction

Money is the primary driver of malicious online activities. There exists a malware ecosystem comprising a network of buyers and sellers that profit from all kinds of malicious online activity. This ecosystem provides opportunities for malicious software developers to sell their products to aspiring cybercriminals who, in turn, are provided a forum in which to sell to and to exchange the value they extract from their operations with others. A variety of services (e.g., VPN, “bulletproof” hosting, and “crypting” services) and antivirus checkers are available for purchase. These tools and services provide cybercriminals with the ability to counter the efforts of law enforcement agencies and of the security community.[1] Cybercriminals use distribution methods such as spamming and blackhat search engine optimization (BHSEO) techniques, often in conjunction with exploit packs that can take advantage of vulnerabilities in popular software in order to distribute malware to unsuspecting Internet users.[2] With limited technical skills and a few underground connections, anyone ready to invest can set up a botnet operation and can earn significant returns on that investment.

The rise of banking Trojans such as ZeuS and SpyEye variants provide cybercriminals with the ability to purchase malware that enable banking fraud and that excel at stealing users’ credentials. Stolen credentials such as FTP passwords can be packaged and can be sold in underground markets. Stolen banking and credit card information, on the other hand, can be used in conjunction with “mules” to commit fraud.[3]

In a recent case, cybercriminals used ZeuS malware, along with a network of money mules, in an attempt to steal US$200 million from victims’ compromised systems. However, the size and the scope of this type of operation can draw significant attention. In October 2010, the Federal Bureau of Investigation (FBI), along with law enforcement agencies from the United Kingdom, from the Netherlands, and from the Ukraine, arrested more than 100 people associated with this ZeuS operation.



However, there are several less conspicuous methods to monetize botnet operations. While not as profitable in the short term, cybercriminals can still earn significant profits over long periods of time. These methods do not require vast human networks of mules that are possible causes of leakage and that present considerable risks of getting arrested.

[1] VPN services allow malicious actors to disguise the true origin of network traffic, making it more difficult to track its actual location. Bulletproof hosting service providers do not respond to abuse notifications or to takedown requests from the security community and ensure that their malicious operations stay online. Crypting and “packing” services modify malicious binaries in order to prevent antivirus detection.

[2] BHSEO tactics are malicious techniques used to promote a website so that it appears as a top result when users search with particular keywords in popular search engines. Exploit packs are software packages available for purchase that attempt to determine the OS and browser versions of visitors to a Web page then serve an appropriate exploit designed to execute malware on their systems.

[3] Mules are individuals that agree to act as middlemen for fraudulent transactions.

Cybercriminals leverage affiliate networks as a mode of organization. Also known as *partnerkas,* these affiliate networks use a model that distributes the responsibility for the development and distribution of malicious campaigns across several people or across various groups. In effect, the affiliate network model delegates advertising responsibilities to clients that aggressively promote products such as online pharmacies, dating sites, casino sites, counterfeit luxury product sites, and FAKEAV download sites that are supplied by various providers.

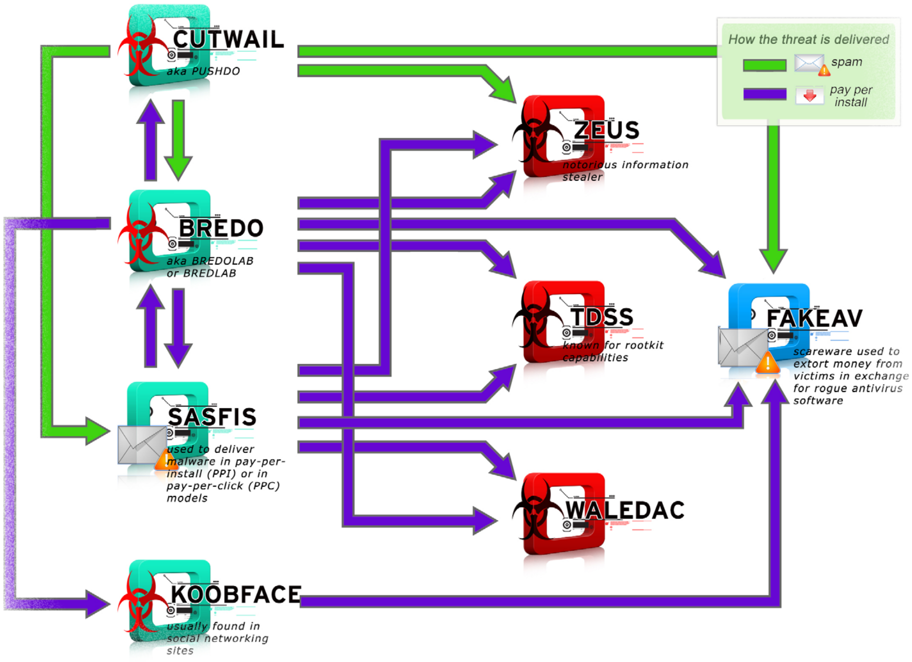
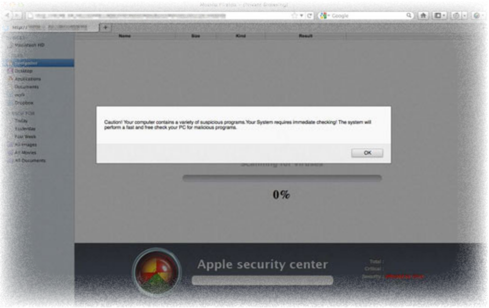

CUTWAIL
aka PUSHDO
BREDO
aka BREDOLAB or BREDLAB
SASFIS
used to deliver malware in pay-per-install (PPI) or in pay-per-click (PPC) models
KOOBFACE
usually found in social networking sites
ZEUS
notorious information stealer
TDSS
known for rootkit capabilities
WALEDAC
FAKEAV
scareware used to extort money from victims in exchange for rogue antivirus software
How the threat is delivered
🟩 spam
🟪 pay per install

Figure 1. *Pay-per-install (PPI) business model*

Cybercriminals leverage the pay-per-install (PPI) business model to monetize their operations. This model allows affiliates to earn income whenever they get Internet users to install software supplied by PPI providers. While the PPI model has legitimate uses, it is frequently adopted by malicious actors to spread malware. A recent study found that 12 of the top 20 malware families were heavily distributed through PPI affiliate networks. The PPI model is based on the relationship between clients that develop malicious software and providers that act as middlemen who, in turn, outsource distribution to affiliates. In practice, however, these roles are not always distinct. PPI providers may also be the developers and, at times, may also engage in direct distribution.

The combination of PPI affiliate networks and botnet operators results in cybercriminal activity that spreads across multiple jurisdictions. While the damage that results is considerable in the aggregate, the amount of criminal activity conducted in any one jurisdiction and against any particular victim remains small. This poses considerable challenges for law enforcement agencies, as they seek to identify victims, to determine the crimes committed, and to measure the impact relative to numerous other crimes conducted within their jurisdiction. In addition, inter-jurisdictional investigations require significant resources and international cooperation remains challenging. Many smaller botnet operations, therefore, are able to stay under the radar of law enforcement.



Caution! Your computer contains a variety of suspicious programs.Your System requires immediate checking! The system will perform a fast and free check your PC for malicious programs.

Figure 2. *FAKEAV for Macs graphical user interface (GUI)*

Internet users face the challenge of distinguishing between legitimate and malicious content. Malicious links are often spread through poisoned search engine results or through popular social networking sites—sometimes from the compromised accounts of people that users know and trust. Cybercriminals use social engineering techniques to trick users into installing malicious software or use exploit packs that take advantage of vulnerabilities in popular software to force malicious software onto users' systems. FAKEAV providers develop landing pages that detect which specific version of *Windows OS* a user is running and deliver a "scanning" page with the corresponding "look and feel." FAKEAV providers even recently developed versions of FAKEAV that imitate the look and feel of *Mac OS X* in order to target its users as well. In a recently reported case, a BHSEO campaign poisoned the search results of *Google Images* using nearly 5,000 compromised servers that redirected users to FAKEAV landing pages. In total, the campaign generated 300 million hits from 113 million visitors in just one month of operation.

The security community continues to face significant challenges as well. Each day, malware distributors produce modified binaries that are checked against popular antivirus products to ensure low or even no detection. Some operations dynamically produce malware so that each potential victim receives a uniquely modified version of the malware in an effort to counter antivirus detection. Each day, numerous new domain names are registered and are used to host malware, exploit packs, and landing pages designed to trick users into installing malicious software. One FAKEAV provider registers an average of 20 new domains per day and uses a variety of email addresses and domain registrars to disguise its activities. The domain names FAKEAV providers register are often checked against security industry blocking lists and are replaced as needed. As a result, a constant stream of malicious software and of domain names propagate throughout the Internet.

FAKEAV Affiliate Networks

In order to monetize their operations, malicious actors create accounts with FAKEAV PPI providers. FAKEAV affiliate networks comprise a specific type of PPI network that somewhat differently operate from traditional malware PPI networks. Traditional malware PPI providers use affiliates to distribute "downloaders" that push whatever malware the PPI providers' clients supply them with. The affiliates are paid each time the downloader is installed. However, FAKEAV affiliates are usually not paid for installations but only when users actually purchase FAKEAV.

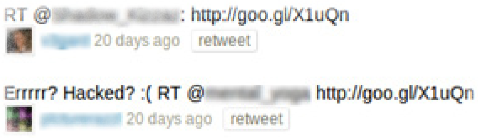
In a recent study, researchers from the University of California in Santa Barbara were able to acquire copies of the backend databases of three FAKEAV providers. These FAKEAV providers earned a combined total of US$130 million. The researchers found that these FAKEAV providers maintained extensive affiliate programs. One of the FAKEAV providers paid a top affiliate US$3.86 million while the top affiliate of another was paid US$1.8 million. They also found that affiliate members often held accounts with multiple FAKEAV providers.

While FAKEAV providers may supply affiliates with malware, they also typically supply URLs to landing pages that display false antivirus scanners and that attempt to scare users into installing rogue antivirus software. Botnet operators and other malicious actors spread the links to these landing pages and, if any user installs and purchases the rogue antivirus software, the affiliates receive a portion of the income generated.

A variety of FAKEAV providers compete with one another to provide similar services. Cybercriminals often maintain relationships with several affiliate networks. In addition, meta affiliate networks that provide access to the FAKEAV malware provided by multiple providers have emerged through one common interface. The affiliate model of distribution combined with countermeasures against the security community enables these operations to convert their malicious activities into profit.

Common FAKEAV Propagation Methods

In January 2011, a malicious campaign used compromised *Twitter* accounts to spread FAKEAV. The compromised *Twitter* accounts were used to Tweet links that were shortened using Google's URL-shortening service.

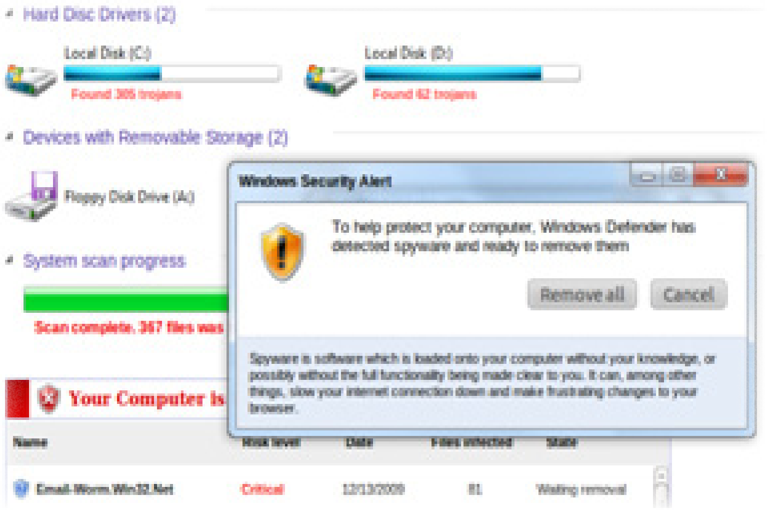


RT @[redacted]: http://goo.gl/X1uQn
[redacted] 20 days ago retweet

Errrr? Hacked? :(RT @[redacted] http://goo.gl/X1uQn
[redacted] 20 days ago retweet

Figure 3. *Tweets with a link to a FAKEAV download page*

These links redirected users to Web pages *(m28sx.html)* placed on compromised sites. These pages then redirected users to a server under the control of malicious actors *(gdfgdfgdgdfgdfg.in.ua/undo/red.php)* that, in turn, redirected users to FAKEAV landing pages.



Hard Disc Drivers (2)
Local Disk (C:)
Found 305 trojans
Local Disk (D:)
Found 62 trojans
Devices with Removable Storage (2)
Floppy Disk Drive (A:)
System scan progress
Scan complete. 367 files was
Your Computer is

Windows Security Alert

To help protect your computer, Windows Defender has detected spyware and ready to remove them

Remove all Cancel

Spyware is software which is loaded onto your computer without your knowledge, or possibly without the full functionality being made clear to you. It can, among other things, slow your internet connection down and make frustrating changes to your browser.

Name Risk level Date Files infected State
Email-Worm.Win32.Net Critical 12/13/2009 81 Waiting removal

Figure 4. *FAKEAV landing page*

The rogue antivirus software was hosted on a server with the IP address *93.104.208.72.* Every instance of FAKEAV downloaded from this site was slightly modified in an attempt to avoid antivirus detection.

At exactly the same time as the previously mentioned *Twitter* campaign, the KOOBFACE botnet also delivered FAKEAV landing pages hosted on the same IP address supplied by the same FAKEAV provider. KOOBFACE was one of the first botnets to successfully leverage social networking platforms in order to propagate. Those behind the KOOBFACE botnet monetize their operations through the use of PPI and pay-per-click (PPC) affiliate networks. This allowed them to earn US$2 million in a single year. Half of their income was generated through the propagation of FAKEAV.

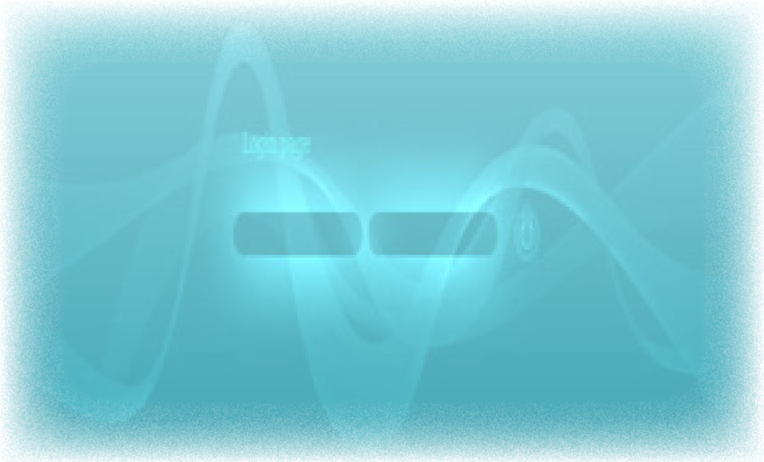


Figure 5. *PrivatCoin's FAKEAV affiliate login page*

The FAKEAV provider that supplied the landing pages and the malware used in the previously cited case is known as PrivatCoin—a private affiliate network that requires underground connections to join. Once accepted, PrivatCoin provides members with a special URL that is used to retrieve new FAKEAV landing pages. Affiliates can then propagate these links through any means at their disposal. According to records obtained from a KOOBFACE command-and-control (C&C) server last year, the gang earned US$278,585 from this affiliate alone between June 2009 and June 2010.

While the KOOBFACE botnet does have components that leverage *Twitter* to propagate, the previously discussed campaign does not appear to have any connection to the botnet, apart from a common FAKEAV provider. The common FAKEAV provider—PrivatCoin—leverages the propagation of these two malware campaigns and probably many more malicious operations. Given that the payout PrivatCoin made to KOOBFACE was considerable, the provider must be generating a significant amount of income while essentially keeping their distance from efforts that tend to draw the most attention from the security industry and from law enforcement agencies.

Another case that illustrates a common propagation means among unrelated malicious actors concerns a well-known BHSEO operation and the KOOBFACE botnet. Both are clients of the same FAKEAV provider known as pro or inddec.

In January 2010, Trend Micro began tracking a BHSEO operation that was abusing searches for free printable items. SEO is a term that refers to efforts to increase the ranking of a website so that it appears as a top result when searching with particular keywords in a search engine. BHSEO, on the other hand, refers to malicious SEO techniques often used to promote rogue antivirus software and other PPC advertising schemes. This typically involves the use of thousands of compromised websites to manipulate search engine results.

Within a period of five months, this particular BHSEO campaign was able to generate over 9 million page views from over 5 million unique IP addresses. The malicious actors behind the campaign acquired compromised FTP credentials for over 11,000 legitimate websites and used BHSEO techniques to poison search engine results. They then redirected a significant amount of traffic using their own malicious infrastructure to their PPC and FAKEAV providers.

Figure 6. Administration panel of a BHSEO operation

This particular operation maintains several custom scripts that allow its operators to maintain proxy servers, to check FTP credentials, and to manage the scripts and search terms that are uploaded to compromised servers. This campaign currently sends non-*Windows* traffic to Riva Click—a PPC provider—and *Windows* traffic to FAKEAV landing pages. It constantly monitors and records search terms that users key in to search engines and automatically begins building related SEO pages. In addition to gathering search terms related to the term "printable," it also maintains records for keywords such as "coupons," "weather," and those related to holidays such as "Christmas."

This BHSEO operation uses a variety of FAKEAV providers, including one that was also used by KOOBFACE. Those behind the KOOBFACE botnet labeled this affiliate "pro" and "inddec," which are associated with the now-defunct *inddecsoft.com.* Last year, this provider supplied the rogue antivirus software known as *Internet AntiVirus Pro.* Both KOOBFACE and this BHSEO operation now spread the URLs supplied by different FAKEAV providers.

Complex relationships exist between malware (e.g., FAKEAV) distributors and their suppliers. Security researchers seek to link the operations of malicious networks in order to better understand them. Often, malicious operations such as botnets are linked through a common infrastructure such as hosting providers or the malicious executable files or the malicious links botnets distribute. Rather than simply bundling all of these activities together, it is important to distinguish between the common infrastructure of botnets and the infrastructure of the affiliate networks themselves. Distinguishing between the source and distribution layers allows researchers to gain a more complete understanding of the underground economy.

Meta Affiliates

BeeCoin is a FAKEAV provider that openly advertises on publicly accessible underground forums such as *damagelab.org.* Malicious actors who wish to monetize their operations simply create an account in order to become an affiliate. The affiliates are given access to a page from which they can retrieve new links to FAKEAV landing pages. The affiliates can choose to distribute these links through any means at their disposal. BeeCoin even provides new affiliates with some sample codes to get them started. In addition to supplying standard FAKEAV scanning pages, BeeCoin also provides "adult" landing pages. Each time a user purchases FAKEAV, the affiliate that distributed the malware earns US$25.

Figure 7. BeeCoin's FAKEAV affiliate login page

Records recovered from BeeCoin's server show that from January to June 2011, its affiliates were able to install FAKEAV in more than 214,000 systems. Moreover, one in every 44 people that installed the malware actually purchased the full version of the rogue software, which allowed BeeCoin to generate US$123,475 in profit. BeeCoin maintained a 2.2 percent conversion ratio, which is comparable to recent research findings that involve much higher installation numbers. When analyzing three FAKEAV providers, researchers from the University of California in Santa Barbara found that three FAKEAV providers accounted for 106,333,156 installations and for US$22,96,514 in sales, resulting in a 2.1 percent conversion rate.

Installations	Sales	Ratio	Profit
214,972	4,939	1:44	US$123,475

Table 1. *BeeCoin's installation and sales statistics from January 17–June 10, 2011*

BeeCoin itself is actually an affiliate of a very well-known FAKEAV provider—Baka Software. In 2008, Baka Software provided the rogue antivirus software, *Antivirus XP 2008*, that was actively propagated by a variety of affiliates. Knowledge of the scale of Baka Software's activities emerged after its servers were compromised and after information from the compromised servers was posted on the Internet. Records revealed that Baka Software's affiliates earned large sums of money. One affiliate, in particular, earned US$146,525.25 in just 10 days.

Figure 8. *BakaVIP's FAKEAV affiliate login page*

The Washington Post revealed that when users purchased Baka Software's rogue antivirus software, the credit card payments were processed by a Russian company known as ChronoPay. After ChronoPay's servers were compromised, details of its operations began to emerge in a series of articles by Brian Krebs. According to these reports, ChronoPay provided payment-processing services for a variety of FAKEAV providers, including Baka Software. It also provided payment-processing services to pharmaceutical affiliate networks.[4] Krebs analyzed ChronoPay's records, which revealed the scale of the income generated from FAKEAV:

> *... One of the documents apparently stolen from ChronoPay lists more than 75 pages of credit card transactions that the company processed from Americans who paid anywhere from US$50 to US$150 to rid their computers of imaginary threats found by scareware...*[5]

BeeCoin maintains a number of relationships with FAKEAV providers. In addition to Baka Software, BeeCoin provides FAKEAV that originates from two additional FAKEAV providers—PrivatCoin and SoftCash. As previously discussed, PrivatCoin supplies FAKEAV to a number of malicious operations, including KOOBFACE and BHSEO campaigns. SoftCash is a particularly interesting affiliate because in addition to *Windows* versions of rogue antivirus software, it also provides versions that run on *Mac OS X*.

Top-tier affiliate networks such as Baka Software and payment processors such as ChronoPay provide botnet operators and other malicious actors with the infrastructure and capability to monetize their activities. Intermediary providers such as BeeCoin further shield the activities of these malicious actors while allowing them to further "crowdsource" the propagation of malicious software.

The emergence of meta affiliate networks continues. We were able to uncover the operations of an aspiring FAKEAV affiliate network known as MoneyBeat. We recovered a compressed archive file that contains the FAKEAV provider's source code and database, which allowed us to recreate its setup and to analyze its operation.

MoneyBeat provides an interface for its affiliates to check statistics and to retrieve new URLs to FAKEAV landing pages that they can propagate. This is a typical setup for FAKEAV affiliate networks. MoneyBeat also has an administrative panel that lists its users, its payment rates, and its payment records. While little information is contained within the database, it still provides an interesting snapshot of the FAKEAV affiliate's activities.

Figure 9. *MoneyBeat's FAKEAV affiliate statistics page*

[4] Pharmaceutical affiliate networks serve as another means to monetize malware by promoting and by selling pharmaceutical products such as Viagra. See http://www.nartv.org/2010/12/23/rx-promotion-a-pharma-shop/.
[5] From Brian Krebs' *Krebs on Security* blog. See http://krebsonsecurity.com/2011/03/chronopays-scareware-diaries/.

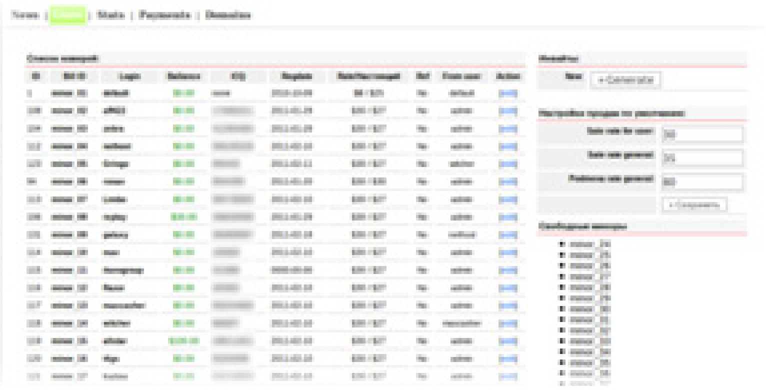


__Figure 10.__ MoneyBeat's FAKEAV affiliate administrative page

MoneyBeat is an interesting affiliate because it is an intermediary affiliate that receives FAKEAV from three upstream providers, including the previously discussed PrivatCoin. MoneyBeat retrieves malware from the upstream affiliate then generates domain names and landing pages. It then supplies these landing pages to its users. The landing page generation script has four themes—*default, default_xp, firefox,* and *IE6.* Landing pages that contain obfuscated JavaScripts are created for each theme and users are redirected to one of the themes, depending on what browsers they use.

MoneyBeat's main upstream FAKEAV provider is known as Gamesoftcash. This provider supplies its affiliates, including MoneyBeat, with FAKEAV executable files. Gamesoftcash scans its malware with a variety of antivirus products to ensure low detection rates. One interesting function of the FAKEAV Gamesoftcash supplies is that if compromised users do not purchase the software within four days, it is replaced with a click fraud application.

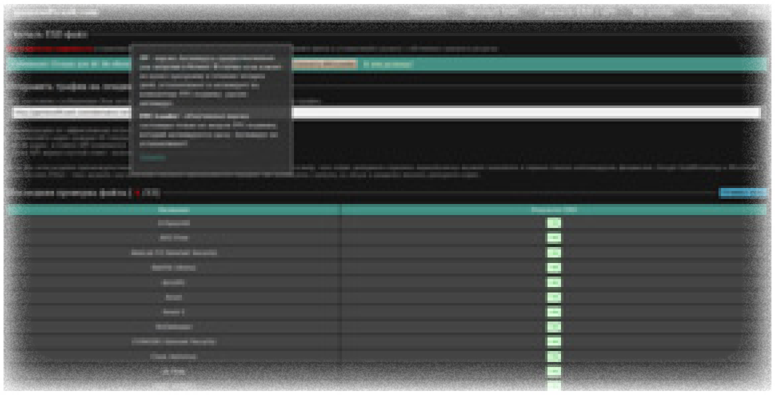


__Figure 11.__ Gamesoftcash's FAKEAV affiliate page

The emergence of meta FAKEAV affiliates makes access to rogue antivirus software easier for cybercriminals with fewer underground connections and further obscures the operations of high-level FAKEAV affiliate networks. It also demonstrates that the propagation of FAKEAV is so profitable that there is room for yet another middleman in the operation.

Conclusion

FAKEAV are successfully used to monetize malicious online operations. Users are scared into installing FAKEAV through the use of social engineering techniques and are then bullied or tricked into paying for useless software. FAKEAV are not botnet specific; these are distributed through affiliate networks. As a result, multiple malicious operations from botnets to BHSEO to spam campaigns can spread the same malicious links and binaries. Apart from possessing a common supplier, however, there are no other links among these malicious operations.

The success of the FAKEAV affiliate model spurred the emergence of meta affiliates—the affiliates of top-tier FAKEAV providers. These midtier FAKEAV providers aggregate the malicious links and the malware of top-tier FAKEAV affiliates and act as middlemen to those without the necessary underground connections to top-tier FAKEAV affiliates. This structure further obfuscates the malicious activities of the top FAKEAV affiliates and creates challenges for the security industry, as this makes it increasingly difficult to both link and separate the activities of specific malicious actors.

Given that the aggregate amount of damage within a specific jurisdiction is limited, many of the smaller FAKEAV operations are able to escape significant scrutiny from law enforcement agencies and from the security industry. In addition, investigating the complex layers of cybercriminal links within the affiliate model is expensive both in terms of cost and of the required leverages for successful international cooperation. As a result, monetizing malicious activities, particularly botnet operations, through the PPI model used by FAKEAV affiliate networks remains an attractive cybercriminal strategy.

Despite the distributed nature of the affiliate model, points of centralization can be uncovered. By discovering and by infiltrating top-tier FAKEAV affiliates, we can mitigate threats by detecting malicious software and by blocking access to scanning pages, as FAKEAV are distributed to affiliates for propagation.

In addition, recent research findings on spam campaigns revealed that there are "payment bottlenecks" that can be subjected to intervention. Researchers purchased a variety of products advertised via spam and found that only a limited number of banks processed these transactions. The concentration in payment infrastructure provides avenues to apply pressure on banks that serve malicious operations. While these operations can switch to new payment-processing services, that takes time and can be costly. Such intervention can negatively affect the operations of rogue pharmacies and of FAKEAV providers.

Researchers from the University of California in Santa Barbara, however, found evidence of collusion between payment processors and FAKEAV providers. In fact, one payment processor provided advice to a FAKEAV provider, which allowed it to set up multiple "high-risk merchant accounts" in order to rotate its transactions across multiple accounts so as to avoid fraud detection.

Researchers found that there are patterns in the relationship between "charge-backs" (i.e., when the credit card company refunds the buyer) and refunds (i.e., when the FAKEAV provider refunds the buyer). They found that FAKEAV providers altered their refund patterns in response to charge-back requests. Further research focusing on institutions that provide payment-processing services to FAKEAV affiliates is important, as this may uncover additional methods to detect and to reduce the payment flow to FAKEAV affiliate networks.

Through the exposure of the relationships among FAKEAV affiliate networks, botnets, and other malicious activities, we hope that the security community and that law enforcement agencies can better understand the challenges that this malicious monetization strategy poses for traditional defenses and investigations.

References

- Brett Stone-Grossx, Ryan Abmanz, Richard A. Kemmererx, Christopher Kruegelx, Douglas G. Steigerwaldz, and Giovanni Vigna. “The Underground Economy of Fake Antivirus Software.” http://www.econ.ucsb.edu/~doug/researchpapers/Underground%20Economy%20of%20Fake%20AV%20Software.pdf (Retrieved August 2011).

- Brian Krebs. (July 31, 2009). *The Washington Post.* “Following the Money: Rogue Antivirus Software.” http://voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html (Retrieved August 2011).

- Brian Krebs. (December 29, 2010). *Krebs on Security.* “Russian e-Payment Giant ChronoPay Hacked.” http://krebsonsecurity.com/2010/12/russian-e-payment-giant-chronopay-hacked/ (Retrieved August 2011).

- Brian Krebs. (February 25, 2011). *Krebs on Security.* “Pharma Wars.” http://krebsonsecurity.com/2011/02/pharma-wars/ (Retrieved August 2011).

- Brian Krebs. (March 3, 2011). *Krebs on Security.* “ChronoPay’s Scareware Diaries.” http://krebsonsecurity.com/2011/03/chronopays-scareware-diaries/ (Retrieved August 2011).

- Brian Krebs. (June 28, 2011). *Krebs on Security.* “Banks Hold Key to Killing Rogue Pharmacies.” http://krebsonsecurity.com/2011/06/banks-hold-key-to-killing-rogue-pharmacies/ (Retrieved August 2011).

- Dmitry Samosseiko. (September 2009). “The Partnerka—What Is It and Why Should You Care?” (A paper presented at the “Virus Bulletin Conference 2009.”) http://www.sophos.com/security/technical-papers/samosseiko-vb2009-paper.pdf (Retrieved August 2011).

- FBI. (October 1, 2010). *The FBI.* “Cyberbanking Fraud: Global Partnerships Lead to Major Arrests.” http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud (Retrieved August 2011).

- JM Hipolito. (January 26, 2010). *TrendLabs Malware Blog.* “Searches for Free Printable Items Lead to Malicious Domains.” http://blog.trendmicro.com/searches-for-free-printable-items-lead-to-mal-domains/ (Retrieved August 2011).

- Joe Stewart. (October 22, 2008). *Dell SecureWorks.* “Rogue Antivirus Dissected—Part 2.” http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2 (Retrieved August 2011).

- Joey Costoya. (June 8, 2011). *TrendLabs Malware Blog.* “A Walk-Through of a FAKEAV Infection in *Mac OS X.”* http://blog.trendmicro.com/a-walkthrough-of-a-fakeav-infection-in-mac-os-x/ (Retrieved August 2011).

- Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. “Measuring Pay per Install: The Commoditization of Malware Distribution.” http://www.icir.org/vern/papers/ppi-usesec11.pdf (Retrieved August 2011).

- Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyháziz, Chris Griery, Tristan Halvorson, Chris Kanich, Christian Kreibichy, He Liu, Damon McCoy, Nicholas Weavery, Vern Paxsony, Geoffrey M. Voelker, and Stefan Savage. “Click Trajectories: End-to-End Analysis of the Spam Value Chain.” http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf (Retrieved August 2011).

- Macky Cruz. (September 15, 2008). *TrendLabs Malware Blog.* “Rogue AV Theatrics on Extended Run.” http://blog.trendmicro.com/rogue-av-theatrics-on-extended-run/ (Retrieved August 2011).

- Nart Villeneuve. (April 2010). “KOOBFACE: Inside a Crimeware Network.” http://www.nartv.org/mirror/koobface.pdf (Retrieved August 2011).

- Nart Villeneuve. (August 24, 2010). *Nart Villeneuve: Malware Explorer.* “Blackhat SEO, PPC, & Rogue AV.” http://www.nartv.org/2010/08/24/black-hat-seo-ppc-rogueav/ (Retrieved August 2011).

- Nart Villeneuve. (October 8, 2010). *Nart Villeneuve: Malware Explorer.* “Blackhat SEO, PPC, & Rogue AV Part 2.” http://www.nartv.org/2010/10/08/black-hat-seo-ppc-rogueav-part-2/ (Retrieved August 2011).

- Nart Villeneuve. (December 23, 2010). *Nart Villeneuve: Malware Explorer.* “RX-promotion: A Pharma Shop.” http://www.nartv.org/2010/12/23/rx-promotion-a-pharma-shop/ (Retrieved August 2011).

- Nart Villeneuve. (May 5, 2011). *TrendLabs Malware Blog.* “Targeting the Source: FAKEAV and Malicious Domains.” http://blog.trendmicro.com/targeting-the-source-fakeav-and-malicious-domains/ (Retrieved August 2011).

- Nart Villeneuve. (May 11, 2011). *TrendLabs Malware Blog.* “Blackhat SEO Attack Uses Google’s *Image Search* to Reach 300 Million Hits.” http://blog.trendmicro.com/blackhat-seo-attack-uses-google’s-image-search/ (Retrieved August 2011).