**INTRODUCTION TO INFORMATION SECURITY**

**ASSIGNMENT-1**

Name: **Manish Choudhary**

Major: **MS INFOSEC**

GTID: **902982487**

**Question1: The story mentions that a network of virus‐infected computers is used to deliver massive quantities of spam email. How are so many computers infected? What makes it a virus infection? Why do owners not know about these infections, and why is this infection not detected by anti-virus tools?**

**Answer:** The network of virus-infected computers, which is used to deliver massive quantities of spam mail, is basically a botnet named “Festi” which is also known as “Topol-Mailer” and “Spamnost**”.** A botnet is a collection of infected computers under the control of one or more attackers. Festi Botnet was also controlled using a Command and Control server to send spams using all the infected computers under it.

**How did so many computers get infected?**

The bot consists of two parts: the dropper and the main module, a kernel‐mode driver. The dropper is used to install into the system the kernel‐mode driver which implements the main logic of the bot. So, to infect some machine, this dropper has to reach to the victim machine so that it can install the driver. It is distributed as an executable Trojan.

To distribute this dropper to a large number of computer systems, PPI (Pay‐Per‐Install) scheme is used1. Under this scheme, the malware owners submit their malware (the dropper here) to the PPI service, which in turn charges rates from $7 to $180 per thousand successful installations, depending on the requested geographic location of the desired victims2. The PPI service provider set-up a pay-per-install website and then recruit affiliates signing up the website where they can get access to the malware. The affiliates install the malware onto the victims’ computers using a variety of methods, and then get paid for every successful install. The common methods used are3:

1. **File-Sharing Networks:** Distribution of the payload (malware) using torrents and other file sharing services.
2. **Infecting Web Sites:** Affiliates often hack into legitimate websites and add code to the website that exploits client-side vulnerabilities, such as vulnerabilities in Internet browsers or their plug-ins, secretly installing the pay-per-install malware.
3. **Search Result Poisoning:** Keywords related and other Search Engine optimization tricks leads to the affiliate’s malicious web site getting listed very high in popular search queries. When user visits these websites, social engineering tricks are used to fool the victim into downloading pay-per-install malware or exploit client side vulnerabilities in order to silently install the malware.
4. **Malvertisements:** Malicious ads—usually in the form of Flash, JavaScript, or DHTML, are used, clicking on which the user allows the malicious files to be installed on the system.
5. **Spam:** Sending spam through emails or forums to redirect the users to malicious code or executable.

Thus, the Festi-Botnet owners used the above discussed Pay-Per-install scheme to spread the virus which is actually the propagation of the dropper which installs the driver on the victim machine. As this scheme implements various ways of malware distribution by using public webpages/social media etc., it was successful to infect a large number of users.

**What makes it a virus infection?**

As discussed above, the scheme used for malware distribution was PPI. The techniques used for distribution make it a virus infection. The dropper propagates using this approach and is able to move to different victim machines. The infected victims actually fall into the trap designed by the affiliates and allow the installation of malicious code/executable (the dropper) on their systems unknowingly. Festi likely infects its victims via drive-by downloads. This is a malware/virus infection where the executable gets executed and thus, makes the system a compromised one. It propagates using different means over the internet. As it is attached to different software/installers/downloadable files etc. to propagate, it comes under the category of virus infection. Another point is, Festi has the capability to send the email spams from already compromised machines to new victims with the dropper attached which can lead these new machines to become a part of the zombie network.

**Why do owners not know about these infections?**

There are many reasons for the owners not knowing about the infection:

1. Most of the infected computers are in India, Brazil and other developing countries where users cannot afford virus protection4 (but, the malware is capable of going undetected even in the presence of an anti-virus).
2. It installs itself silently on the victim machine and doesn’t perform any activity which would directly harm the user or would catch his attention.
3. Users with anti-viruses on their systems, think that their security software would protect them against any kind of intrusion or malware activity. But, this malware is capable of evading AV software.
4. Once infected, software embedded on home and business computers can be used to send persistent e-mails. Thus, the owner usually never knows the system has been compromised.

**Why is this infection not detected by anti-virus tools?**

The malware implements following techniques because of which it is able to go undetected.

1. The previous versions of the bot communicated with C&C servers over HTTP (Hypertext Transfer Protocol) by encrypting POST requests. An updated version of the bot employed a new communication protocol which is protected against eavesdropping and is capable of bypassing IPS and IDS systems operating at the network layer1.
2. The strings used by the malware to perform various system‐specific operations are Encrypted which helps the bot to evade AV software.
3. Instead of using a system implementation of the ZwCreateFile system service, Festi implements its own, with almost the same functionality as the original.
4. In order to send/receive packets, the malware opens ‘\Device\Tcp’ or ‘\Device\Udp’ devices. Most personal firewalls and HIPS systems attach to these devices and intercept IRP\_MJ\_CREATE\_FILE requests sent to the transport driver on opening these devices. Festi manually creates a file object to communicate with the device being opened and sends an IRP\_MJ\_CREATE request directly to the transport driver. Thus, all the devices attached to ‘\Device\Tcp’ or ‘\Device\Udp’ will miss the request and as a result this operation is unnoticed by security software.
5. It implements some anti-VM techniques using which it can detect whether it is running in a virtual environment (which is commonly used for malware trapping and analysis).
6. Festi also checks for the presence of a kernel debugger in the system by examining the KdDebuggerEnabled symbol. It also periodically zeroes debugging registers so as to remove the hardware breakpoints.
7. To send the packets the plugin employs network sockets implemented by the main module of the bot. As a result the attack is performed in kernel‐mode, which makes it quite stealthy.

Reasons which make the forensic analysis difficult:

1. The plugins are kernel‐mode drivers which aren’t saved on any storage device in the system and are volatile in memory. This makes forensic analysis of the malware significantly harder since the only file stored on the hard drive is the main kernel‐mode driver, and this contains neither the payload nor information regarding which sites to attack or target with spam.
2. The botnet periodically migrates to new hosting and domain names in order to decrease the rate at which it is detected using C&C URLs and corresponding IP addresses. There are only C&C domain names inside the bot’s binary with no IP addresses.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Question 2:** **What is Festi and what makes it a botnet?**

**Answer:**

**What is Festi?**

Festi is currently one of the most powerful and active botnets for sending spam and performing DDoS attacks1. Festi is basically a network of compromised computers (zombie computers) which have been infected with the virus using Pay-Per-Install scheme. The bot consists of two parts, a dropper and a kernel-mode driver (the main module). As a part of infection, the dropper gets propagated to the victim machine and installs into the system the kernel-mode driver which implements the main logic of the bot. The network is controlled using Command and Control servers.

The kernel‐mode driver implements backdoor functionality and is capable of:

1) Updating configuration data from C&C;

2) Downloading additional dedicated plugins.

The kernel‐mode driver periodically contacts the C&C server and requests plugins and configuration information. The downloaded plugins perform the bot’s main tasks, such as sending spam. The plugins are kernel‐mode drivers which aren’t saved on any storage device in the system and are volatile in memory. Thus, the plugins can be used and updated to perform tasks like sending spams, launching DDoS attacks.

The botnet has been used to attack **Assis**t (a popular payments firm), to attack several rogue pharmacy programs that were competing with **Rx-Promotion, to send email spams** to promote the counterfeited male sexual enhancement and other drugs, and for other such illegal activities.

**Why Festi is a Botnet?**

|  |  |
| --- | --- |
| **GENERAL BOTNET5** | **FESTI BOTNET** |
| Botnets consist of a group of infected computers known as "zombie" computers that have been compromised by drive-by-downloads of software. | Festi is also a network of compromised computers which are infected by drive-by-downloads using Pay-Per-Install Scheme. |
| A botnet is generally controlled by a Botmaster (the attacker who builds and uses the Botnet for some purpose). | Festi has also been controlled by a Botmaster named **Igor Artimovich who is also the curator of same and used it to assist people to achieve specific goals.** |
| To control the botnet, Command and Control servers are used. | Festi also has command and control servers to send the updates and action commands to the compromised zombie computers. These servers’ domain names have been identified as Russian domain names. |
| Bot connects to C&C server. This could be done using HTTP, IRC or any other protocol. | Initially, Bots used to communicate with C&C servers over HTTP (Hypertext Transfer  Protocol) by encrypting POST requests. Later, an updated version of the bot employed a new communication protocol. |
| The botnet is used to spam others, host phishing sites and other illicit files, infect or attack others, or have adware and spyware foisted on it so the attackers can collect from various affiliate advertising programs. | Festi has been used to send email spams to promote counterfeited drugs as well as to launch DDoS attacks. |

Thus, on the basis of above similarities it can be concluded that Festi is a Botnet.

**Question 3: In this case, the attack is driven by a profit motive. Explain the ecosystem that explains how money leaves the hands of unsuspecting Americans and ends up in the accounts of the cyber criminals so they can live comfortably**.

**Answer:**

Here are the steps how the money reaches to the hands to the cyber criminals (in related to the Counterfeited Drugs Spam Industry):

1. In Counterfeit pharmaceuticals, a sponsor/owner starts a pharmaceutical afﬁliate program under which whole scheme is designed.

Here in this case study, the sponsors were **Pavel Vrublevsky and Igor Gusev. Pavel Vrublevsky is suspected to run** rogue online pharmacy **Rx-Promotion and Igor Gusev is suspected to run the affiliate program Glavmed (a.k.a. “Spamit”).**

1. The Counterfeited drugs are prepared in the countries where intellectual property rights on pharmaceutical industry products are loosely enforced.
2. Sponsoring afﬁliate programs provide drugstore storefronts, drug fulﬁlment (typically via drop shipping from India), payment processing, customer service and so on.6
3. Independent advertisers, or afﬁliates, in turn are hired to promote the program (e.g., by using botnets to send spam email or manipulating search engine results).

In this case study, **Igor Artimovich was hired by Pavel Vrublevsky to promote the program by sending spam emails using his botnet known as Festi or Topol-Mailer**.

1. Botnet owner uses the Command and control Servers to send the configuration details and the details related to the task to be performed to all the compromised zombie computers.
2. The zombie computers send the spam emails to a given list of email-addresses.
3. The spam opens links to some website (developed by the program sponsors) like “Canada Pharmacy” or “Canadian Pharmacy”.
4. The customers place the order for some drugs like Viagra and go to the payment gateway.
5. These websites are in fact Russian-based companies that have privileges to process online payments from Visa (through banks in Azerbaijan and Iceland in case of RXPromotion).
6. Thus, the money reaches to the sponsors of the affiliate program through these banks.
7. Most of the customers are found to be Americans, to whom the counterfeited medicine is delivered.
8. The affiliates (botmasters) are paid a commission on each sale that results from a click on one of their ads/mails. Commissions range from 30%–40% of gross revenue, typically paid via a quasi-anonymous online money transfer service such as WebMoney or Liberty Reserve.

In this way, the money paid by the unsuspecting Americans for the counterfeited drugs ends up into the hand of cyber-criminals.

There are different aspects of this ecosystem6:

**Affiliate Program Sponsors and Affiliates:** Both get benefited from the money which they are able to withdraw out of the hands of the customers. The loosely coupled nature of the relationship of the affiliates with afﬁliate programs allows an advertiser to switch programs at will (or even support multiple programs at once).

**Customers**:

The reasons for the customers for going online to purchase these drugs can be categorized according to the drugs category:

1. Viagra and related drugs - While they are relatively easy to obtain under prescription, seekers may prefer the online channel for reasons of embarrassment or price.
2. Addictive drugs – These drugs are not legal and people purchase them because of strong desire or need.
3. Chronic treatment – Their purchase is motivated by economics: lower direct drug costs (which can be substantial) and the absence of indirect costs (for a doctor’s visit).

**Geographical Aspect:**

Western money fuels these afﬁliate programs with the U.S., Europe, Canada and Australia constituting 97% of all orders.

There are other ways in which these cyber-criminals are able to get the money,

1. **Phishing:** Acquire information such as usernames, [passwords](http://en.wikipedia.org/wiki/Password), and credit card details by masquerading as a trustworthy entity in an [electronic communication](http://en.wikipedia.org/wiki/Electronic_communication). They can sell this personal information or can use them to get the money.
2. **Fake Security Software:** Often referred to as fake antivirus, it works by convincing the user they are at risk of infection after visiting a compromised webpage that secretly installs the fake antivirus on their computer.
3. **Ransomware:** Cybercriminals can use ransomware to encrypt your documents, boot sector or other important component of your PC and hold it hostage until you pay a ransom.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Question 4: This story and other researchers who have investigated Festi talk about why law enforcement has not been able to put the guys behind it out of business. Why?**

**Answer:** There are some points that put some light on the reasons why law enforcement has not been able to put the guys behind it out of business:

1. Festi curator is Russian based and its command and control servers are situation in Russia.

The sponsors of affiliate program are also Russia based. One view is that the Russians had little incentive to invest law enforcement resources in a crime that primarily affected Americans.

1. There is a possibility that the Russian government has turned to so-called black hat hackers for political tasks, like crashing opposition websites during the presidential election, in exchange offering protection from prosecution.
2. The botnet periodically migrates to new hosting and domain names in order to decrease the rate at which it is detected using C&C URLs and corresponding IP addresses. There are only C&C domain names inside the bot’s binary with no IP addresses.
3. The suspected people were really powerful and had money with them. They tried to bribe the government officials and other people to protect them.
4. Another aspect is, whenever there was some criminal proceeding, either the wrong people were convicted or the control was transferred to some other people.
5. The counterfeited drugs were produced in India where intellectual property rights on pharmaceutical industry products are loosely enforced. So, no action could be taken from this angle of the story.

**Question 5: Attribution for cyber-attacks is challenging. What evidence has enabled Andrew Kramer, the reporter who wrote the story, to name certain individuals, who are behind the cyber-criminal activity? Explain your answer.**

**Answer:** The reporter, Andrew Kramer, was able to name certain individuals on the basis of the proceedings going on in a Russian court where evidences collected by investigating agencies were presented by the prosecutors.

But, the main reason for getting the evidences is said to be the enmity developed between owners (who were partners before) of the two long-operating pharmaceutical affiliate programs GlavMed and RX-Promotion6. The former partners were actively trying to scuttle each other’s businesses.

According to the online sources, Pavel Vrublevsky co-founded the company ChronoPay (online payment processor) along with Igor Gusev. Later, Igor Gusev left ChronoPay and started his pharmaceutical afﬁliate programs GlavMed and SpamIt. Later on, Pavel Vrublevsky started his own pharmaceutical afﬁliate program RXPromotion. Pavel Vrublevsky hired a botmaster  Igor Artimovich and his brother Dmitry Artimovich, a freelance programmer, to launch distributed denial-of-service (DDoS) attacks against one of the competitors of ChronoPay, Assist – another online processing company, which resulted in the company losing the contract with Aeroflot, an airlines company.

This incident forced the Russian agencies to look into the matter and thus, the allegations against Artimovich and Vrublevsky were supported by evidence collected by Russian computer forensics firm [Group-IB](http://group-ib.com/), which said it assisted the FSB with the investigation.

It is also said that, Artimovich - the botmaster earned thousands of dollars spamming for both Rx-Promotion and SpamIt, but he abruptly quit the SpamIt program in 2009 after accusing its administrators of under-counting his sales and commissions. Artimovich worked for Vrublevsky to promote RXPromotion program and to launch a volley of distributed denial-of-service (DDoS) attacks against SpamIt. They also targeted to break into and leak the contact and earnings data from GlavMed/SpamIt.

Thus, the two enemy groups launched DDoS attacks, hacking attempts etc. against each other which resulted in exposure of their databases, internal documents, financial dealings and organizational emails to the public and criminal investigators.

Another reason for these proceedings and evidences is the bribes paid by Gusev to some of Russia’s most powerful to secure the opening of criminal investigations against Vrublevsky and Igor Artimovich.

The main evidences were:

1. In court proceedings, Pavel Vrublevsky, Maksim Permakov(an employee of Pavel), and Artimovich brothers were named in Assist-DDoS attacks case.
2. Permakov, conceded his role in using Festi which provides strength and solid base to the whole story.
3. According to some source7, Artimovich confessed that he launched DDoS attacks against Assist after receiving instructions and payment from Vrublevsky. This also supports the complete story.
4. Group-IB presented detailed information on [the malware](http://www.threatexpert.com/report.aspx?md5=20bb760b428bae36378e0d3d1622c272) and control servers, and shared with investigators screen shots of the botnet control panel allegedly used to coordinate the DDoS attack against Assist. 8
5. Group-IB’s evidence suggested Artimovich had used a botnet called **Topol-Mailer/Festi** to launch the attacks. 8
6. Group-IB said Artimovich’s botnet was repeatedly used to attack several rogue pharmacy programs that were competing with Rx-Promotion. 8
7. Artimovich allegedly used the nickname **Engel** on **Spamdot.biz**, an online forum owned by the co-founders of **SpamIt** and **GlavMed**. Engel was found to be communicating with Spamdot member and SpamIt affiliate “Docent”. 9
8. Engel’s profile on Spamdot.biz lists his email address as “support@id-search.org”. That domain is no longer online, but [archive.org reveals](http://web.archive.org/web/20090104083329/http:/id-search.org/bot.html) that Engel used it as the home base for a bot whose sole purpose was to harvest email addresses from billions of Web pages. 9
9. The data leaked from Glavmed/Spamit includes a list of contact information, earnings and bank account data for hundreds of spammers and hackers who were paid to promote the program’s online pharmacies. Those records suggest that for most of 2007, Artimovich was earning thousands of dollars a month sending spam to promote Spamit pharmacy sites. 8
10. The [document](http://i.imgur.com/eU7wO.jpg) with FSB states that Engel was paid for the DDoS services with funds deposited into a WebMoney account “Z578908302415″. According to the leaked Spamit affiliate records, that same WebMoney account belonged to a Spamit affiliate who registered with the program using the email address “support@id-search.org.” [Historic WHOIS records](http://krebsonsecurity.com/wp-content/uploads/2011/06/idsearchWHOIShistorical.txt) maintained by DomainTools.com reveal that for a two-month period in 2008 those registration records were exposed; during that brief window, records listed the registrant as Igor Artimovich from Kingisepp, Russia, a town 68 miles west of St. Petersburg. 8
11. The emails and documents leaked from the hacking intrusion into ChronoPay last year show that Artimovich and Vrublevsky exchanged numerous emails about payment for unspecified services. Among them is an email receipt from WebMoney showing a transfer of more than $9,000 from an account Vrublevsky controlled to Artimovich’s Z578908302415 purse on July 6, 2010, just days before the DDoS attacks began. 8
12. Hundreds of chat conversations apparently between Gusev and his right-hand man, Dmitry Stupin, were leaked online. They indicate that Gusev may have caused [Vrublevsky’s arrest](http://krebsonsecurity.com/2011/06/chronopay-co-founder-arrested/) by paying Russian law enforcement investigators to go after Artimovich. 10
13. A leaked chat allegedly between Gusev and Stupin, dated Sept. 26, 2010 also provides some evidence. The two men had already decided [to close SpamIt](http://krebsonsecurity.com/2010/09/spam-affialite-program-spamit-com-to-close/), and were considering whether to do the same with GlavMed. They also discussed about the bribes paid for the investigations against Vrublevsky and Artimovich. 10

The above mentioned evidences provide a strong base for the whole story and throw some light on the characters involved. This whole investigation and exposed evidences resulted in the identification of the criminals involved.

**REFERENCES:**

1. <http://www.welivesecurity.com/wp-content/media_files/king-of-spam-festi-botnet-analysis.pdf>
2. <http://krebsonsecurity.com/2011/06/pay-per-install-a-major-source-of-badness/>
3. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/pay_per_install.pdf>
4. <http://www.nytimes.com/2013/09/03/business/global/online-attack-leads-to-peek-into-spam-den.html?pagewanted=all&_r=0>
5. <http://www.korelogic.com/Resources/Presentations/botnets_issa.pdf>
6. <http://cseweb.ucsd.edu/~apitsill/papers/UsenixSec12.pdf>
7. <http://www.xakep.ru/post/56038/default.asp>
8. <http://krebsonsecurity.com/2011/06/financial-mogul-linked-to-ddos-attacks/>
9. <http://krebsonsecurity.com/2012/06/who-is-the-festi-botmaster/>
10. <http://krebsonsecurity.com/tag/igor-artimovich/>