The “Mumba” Botnet Disclosed

Each year, cybercriminals generate billions of dollars by their criminal activities online. Therefore, the longer period of time a given malware remains undetected is directly correlated to a cybercriminal’s financial gain. This is why cybercriminals are investing a great deal of time and resources in protecting their systems and servers from detection.

One commonality that exists among botnets is the way in which cybercriminals are hiding their servers from being shut down by security researchers and law enforcement officials. One example of this is the “Mumba” botnet. Created by one of the most sophisticated group of cybercriminals on the internet known as the Avalanche Group, the Mumba botnet is a mass-production system for deploying phishing sites and crimeware.

A study conducted by AVG discovered one of the Avalanche Group’s servers and revealed that more than 55,000 unknowing internet user’s machines were compromised with data stealing malware inserted on their machines by the Mumba botnet. More than 60 gigabytes of data was identified on the server including credentials of social networking Web sites, banking accounts, credit card numbers, email communications and others.

Of those machines infected, 33 percent were found in the U.S., while other top infected countries included Germany, Spain, The United Kingdom, Mexico and Canada. This report will shed some light on the Mumba botnet, along with suggested ways to protect yourself from cybercriminals.

Overview

The most popular generation of malware networks (botnets) send stolen data directly back to cybercriminal servers, which makes it relatively easy for security researchers to track back and have these servers shutdown. Once cybercriminals understood how easily their unprotected servers were being shutdown, they created innovative ways to stay off-the-radar including changing security settings of servers, using application protection modules or encryptions.

Research conducted by AVG found a next generation type of protection cybercriminals are using to protect their “Holy Grail” – the command and control server malwares are communicating with as well as the server where the stolen data is dropped. Such next-generation protection involves a large network of gateways running on infected end-user PCs that shield the criminal’s server from direct access.

The “Mumba” Botnet Under Research

AVG’s team of researchers dubbed the botnet “Mumba,” due to some funky attributes they identified on the server that made it unique when comparing to other cybercrime incidents researched in the past. The findings below are based on information the team managed to collect about this botnet over the past two months.

Detected by AVG security products, the “Mumba” botnet was found to be using four different variations of the latest version of the Zeus malware to steal data from compromised machines. Zeus version 2.0.4.2 now supports the latest Microsoft operating system – Windows 7 (figure 1), and is able to steal HTTP traffic data from the Mozilla Firefox browser.

The “Mumba” botnet, which makes use of the prolific Zeus malware, has compromised more than 60GB of data from approximately 55,000 users’ PCs around the world. The data includes user credentials of social networking Web sites, banking accounts, credit card numbers, email communications and more.
By looking at Figure 1, you probably noticed OS types that do not really exist. The following PHP server side code explains why. The code converts the binary data sent by the Zeus malware about the victim’s operating system to readable information.

Figure 1 - "Mumba" botnet OS statistics
As can be seen on the code example below, Figure 2, it has logical flaws that result with wrong information on the statistics page:

```php
function osDataToString($os_data)
{
    $name = 'Unknown';
    if (strlen($os_data) >= sizeof(OSINFO) - 1)
    {
        $data = unpack('Uversion/Csp/Build/Arch', $os_data);

        // Архитектура.
        switch($data['version'])
        {
            case 2: $name = 'XP'; break;
            case 3: $name = 'Server 2003'; break;
            case 4: $name = 'Vista'; break;
            case 5: $name = 'Server 2008'; break;
            case 6: $name = 'Seven'; break;
            case 7: $name = 'Server 2000 R2'; break;
        }

        // Архитектура.
        if($data['arch'] == 0 /*PROCESSOR_ARCHITECTURE_AMD64*/)$name .= ' x64';

        // Архитектура.
        if($data['mhi'] > 0)$name .= ', 64 FP';$data['mhi'];
    }
    return $name;
}
```

Figure 2 – Code behind
Looking at the breakdown of the compromised PCs discovered, 33 percent of infected users reside within the United States, while other notable affected countries include Germany, Spain, The United Kingdom, Mexico and Canada (figure 3).  

Figure 3 - "Mumba" botnet statistics per country
Analyzing the data showed the “Mumba” botnet’s first infection campaign started at the end of April 2010. During its first week, the operators of the botnet were able to infect more than 35,000 machines (figure 4). Since then, the botnet operators conducted several smaller infection campaigns, adding 20,000 to the compromised machines in total.

Compromised Machines Over Time

Figure 4 - "Mumba" botnet statistics over time
The Botnet Infrastructure

One of the interesting components of this botnet is its infrastructure. While most of the current Zeus botnets are either using bullet-proof hosting or hijacked web servers to host the data, this botnet uses a fast-flux network. Research conducted by Dancho Danchev, showed the botnet’s DNS servers are actually part of the notorious Avalanche fast-flux network.

These criminals are some of the most sophisticated on the Internet, and have perfected a mass-production system for deploying phishing sites and "crimeware". This means that mitigating the threat by going after the servers hosting the data using the “Mumba” botnet is now much harder than before.

According to a recent report by the Anti-Phishing Working Group (APWG), up until today, the Avalanche fast-flux network was mainly used for phishing attacks and hosting malware infections. The “Mumba” botnet is probably one of the first to use the Avalanche operation in order to host its stolen goods as well as the malware infection. This seems to be yet another step in the never ending arms race between the security industry and cyber criminals.

The following are some of the bots’ IP addresses resolved from the “Mumba” domain, fluxed by the Avalanche botnet:

- 41.251.70.127 (GeoIP: Morocco)
- 190.225.21.138 (GeoIP: Argentina, Buenos Aires)
- 186.9.91.96 (GeoIP: Chile, Santiago)
- 67.159.50.167 (GeoIP: United States)
- 186.58.5.234 (GeoIP: Argentina, Buenos Aires)

The DNS servers resolving these IP addresses are listed on various blacklists tracking phishing and malware activities associated with Avalanche.
The Data

AVG researchers researched the remote server despite the various layers used by the criminals to hide it. Upon accessing the server, it became relatively simple to look at the data it managed to collect from users.

The following are some screenshots of information stolen by the Trojan:

![Screenshot of stolen bank login information](image)

Figure 5 - Stolen bank login information
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot ID</td>
<td>NE3483EE109</td>
</tr>
<tr>
<td>Botnick</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>9.0.7.1</td>
</tr>
<tr>
<td>OS Version</td>
<td>XP, SP 2</td>
</tr>
<tr>
<td>CC Language</td>
<td>1504</td>
</tr>
<tr>
<td>Local time</td>
<td>22.06.2010 20:43:37</td>
</tr>
<tr>
<td>GMT</td>
<td>4211U</td>
</tr>
<tr>
<td>Session time</td>
<td>08:00:37</td>
</tr>
<tr>
<td>Report time</td>
<td>22.06.2010 19:03:27</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>IPV4</td>
<td>12</td>
</tr>
<tr>
<td>Comment for bot</td>
<td></td>
</tr>
<tr>
<td>Process name</td>
<td>C:\Program Files\Mozilla Firefox\firefox.exe</td>
</tr>
<tr>
<td>User of process</td>
<td>ME</td>
</tr>
<tr>
<td>Remote</td>
<td></td>
</tr>
<tr>
<td>User agent</td>
<td></td>
</tr>
<tr>
<td>User name</td>
<td></td>
</tr>
<tr>
<td>User ip</td>
<td></td>
</tr>
<tr>
<td>User os</td>
<td></td>
</tr>
<tr>
<td>User time</td>
<td></td>
</tr>
<tr>
<td>User country</td>
<td></td>
</tr>
<tr>
<td>User timezone</td>
<td></td>
</tr>
<tr>
<td>User id</td>
<td></td>
</tr>
</tbody>
</table>

**Data:**

```plaintext
url=_flow
close_external_flow=false
external_close_account_payment_flow=payment_flow
email_recovery=false
myAllTestSubmitID=
CONTEXT=
login_email=jonse,yahoo.de
login_password=secret
refresh_country_code=0
country=DE
term character=HTTP-1
browser name=Firefox
brower version=3.6
```  

**Figure 6 - Stolen Paypal login information**
What Should You do to Protect Yourself From These Attacks?

Cybercriminals are getting smarter and smarter at utilizing sophisticated techniques to evade detection by traditional URL filtering and database-driven security products. Protecting yourself from these attacks requires innovative Web security products that can scan the Web content you view in real-time for threats.

AVG provides this technology for FREE to anyone who wants it. By downloading AVG’s free product users are equipped with award winning anti-virus software in addition to innovative Web security product, LinkScanner.