# Beebone Botnet Takedown: Trend Micro Solutions

trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions

Written by: Dianne Lagrimas

Trend Micro, as part of a public-private collaboration with the Federal Bureau of Investigation (FBI) and other security vendors, took part in a takedown of a longstanding botnet operation named "Beebone."

On April 8th, 2015 Europol's European Crime Centre (EC3) along with numerous law enforcement agencies and private sector partners executed Operation Source. Approximately 100 command-and-control (C&C) domains were suspended in order to eliminate the threat of the malware worm AAEH, or as Trend Micro detects as VOBFUS. This threat was first found by Intel Security / McAfee Labs.

AAEH or VOBFUS is a polymorphic malware used as a means by which to pull down a variety of additional types of malware onto a victim machine.

More information about the botnet takedown can be found at the following links:

- For users in the United States - US-CERT Alert (TA15-098A)
- For users in Europe, the Middle East and Africa (EMEA) - Europol's EC3

Combatting cybercrime requires public-private collaboration like this. Security researchers can actively provide the necessary threat intelligence or information needed by law enforcement to conduct their investigations. With such information and evidence on hand, law enforcement then provides the legwork to apprehend and indict the cybercriminals responsible. The end result is a safer Internet for everyone, and those who seek to perpetuate cybercrime placed behind bars.

Trend Micro has worked closely and collaborated with law enforcement agencies to thwart cybercriminal operations and subsequently, prevent losses against users and enterprises.

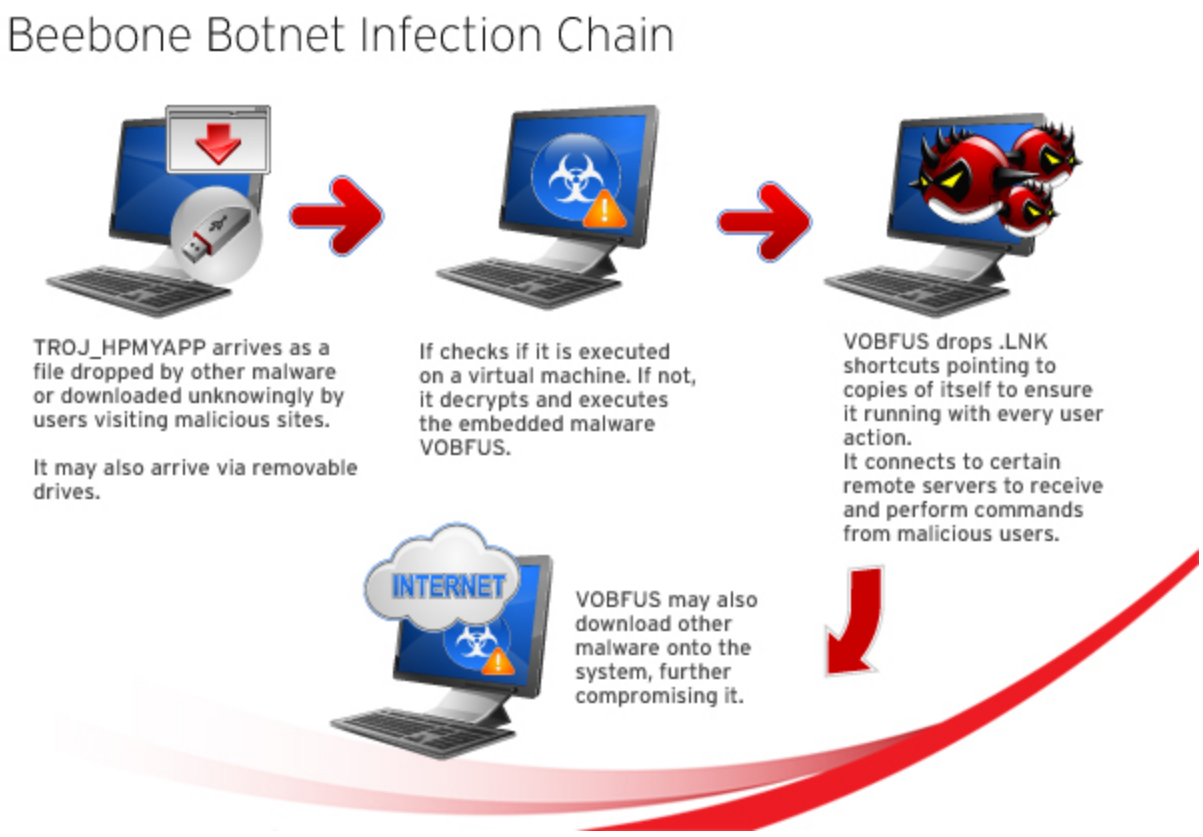
**Botnet Takedowns**

Trend Micro is an active partner with global law enforcement and government task forces in the takedowns of botnets in order end their operations. Internet safety of both our customers as well as the Internet at large is paramount to Trend Micro, and we see supporting these activities as a proactive means to protect our customers before they are affected by them.

In 2011, Trend Micro researchers along with the FBI and Estonian police joined forces to take down a botnet composed of 4,000,000 bots in an operation called as "Operation Ghost Click," which took a C&C with more than 100 servers and two data centers offline. Our collaboration also resulted in the arrests of several members of Rove Digital, the Estonia-based cybercriminal gang behind this operation.

Most recently, Trend Micro also aided law enforcement in the disruption of the activities related to Gameover ZeuS. This specific variant of the notorious online banking Trojan came with an added peer-to-peer (P2P) functionality to its C&C server, making it resilient to takedowns.

**Technical Data**



This section describes some of the technical data uncovered that supports Operation Source's involvement in cybercrime.

### *TROJ_HPMYAPP*

The malware detected as TROJ_HPMYAPP.SM is the Trend Micro detection for malware that use a custom packer (or a "hacker" packer).

Packers have long been used for legitimate purposes, but may also be used for malicious intent, such as evading antivirus detection and concealing vital malware components. Custom packers do not have a specific arrival method since they are dependent on the malware it carries; in this case, the AAEH or VOBFUS malware, which will be tackled in depth later on.

The custom packer first checks if the file *myapp.exe* exists on the system, and if it does, the packer terminates itself. This function was possibly written by malware authors to prevent the malware authors from infecting their own computers.

Once the custom packer completes the system check, it will decrypt and execute the embedded malware, VOBFUS.

After the custom packer checks for certain virtual machine modules, it then then decrypts VOBFUS in memory and executes it.

One thing that our engineers noted is that that the packer used here is similar to the packer used the recent TorrentLocker series of attacks that hit the ANZ region in early January 2015.While this does not necessarily mean both attacks are related, it does point to the packer method being used more commonly by cybercriminals.

### *VOBFUS*

After AAEH or VOBFUS is executed in memory, it carries out its routines which include checking for strings on the system to see if it is running on a virtual machine. This is a typical tactic to evade security vendors' efforts in analyzing the malware, meaning that those behind the attack are anticipating security counter-efforts. If the malware detects that it is running on a virtual machine, it does not execute its malicious routines.

If not, it then proceeds to dropping .LNK or shortcut files in removable drives that point to a copy of itself. The malware tricks users into clicking the shortcut files that use file names like *Love You.exe*, *Nude.exe*, etc.

Additionally, the malware uses the names of existing folders and file names with common extension. This routine enables a copy of VOBFUS to execute first before opening or running the real folder or file.

VOBFUS also attempts to connect to certain remote DNS servers. After it does this, it will receive commands from remote malicious users.

It is important to note that AAEH or VOBFUS may be used to download other malware. This means that cleanup for AAEH or VOBFUS will not necessarily clean secondary infections that may have occurred because of it.

***Network Fingerprints***

The following network fingerprints have also been validated. Listed below is the network traffic:

*timechk[1-9]{1,2}.[com|net|org]*

**Trend Micro Solutions**

Trend Micro endpoint users are protected from this threat via Trend Micro™ Internet Security, while businesses are also protected via Trend Micro™ OfficeScan and Trend Micro™ Worry-Free Business Security.

Trend Micro™ Deep Discovery detects network traffic or C&C communications related to the Beebone botnet.

Non-Trend Micro users can also be protected against this threat by using our free online virus scanner HouseCall, which is able to clean and detect threats related to the Beebone botnet.

**This page will be updated with further developments with regard to Operation Source.*