SIMDA: A Botnet Takedown | Security Intelligence Blog

By Trend Micro

Archived: 2026-04-05 21:04:41 UTC

The collaboration between Trend Micro, INTERPOL, Microsoft, Kaspersky Lab, and the Cyber Defense Institute resulted in a triumph for the security industry earlier this week: the takedown of the SIMDA botnet. Trend Micro provided information such as the IP addresses of the affiliated servers and statistical information about the malware used, which led to the disruption of the botnet activities.

SIMDA, the Malware Behind the Botnet

The botnet relies on the backdoor SIMDA for its operations. One notable feature of the malware is that it modifies HOSTS files, which redirects users to malicious sites whenever they try to access legitimate sites. Our research shows that the malware targeted popular sites including Facebook, Bing, Yahoo, and Google Analytics, as well as their regional counterparts: e.g., Yahoo Singapore, Bing Germany, etc. This shows that the botnet creator wanted to affect as many users as it can, on a global scale. Here's a sample screenshot of a modified HOSTS file.

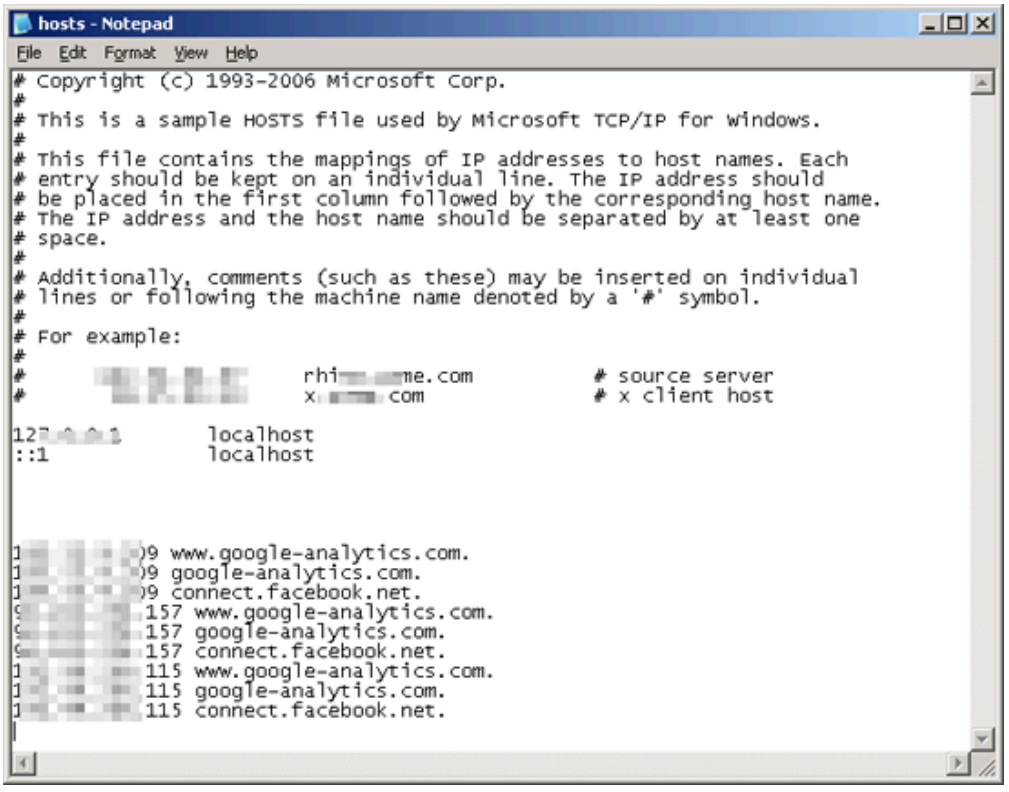

Figure 1. Modified HOSTS file

Analysis also reveals that the malware collects information about the affected system. It also checks for the presence of certain processes, including those used for malware analysis. The latter could be seen as a detection precaution.

Further research shows that the botnet activity spanned the globe. We found that the redirection servers were located in 14 countries, among which include the Netherlands, Canada, Germany, Russia, and the United States. Botnet victims were also scattered. Feedback from the Trend Micro™ Smart Protection Network™ lists at least 62 affected countries, including the United States, Australia, Japan, Germany, Italy, among others. Below is a visualization of the redirection servers located in several countries:

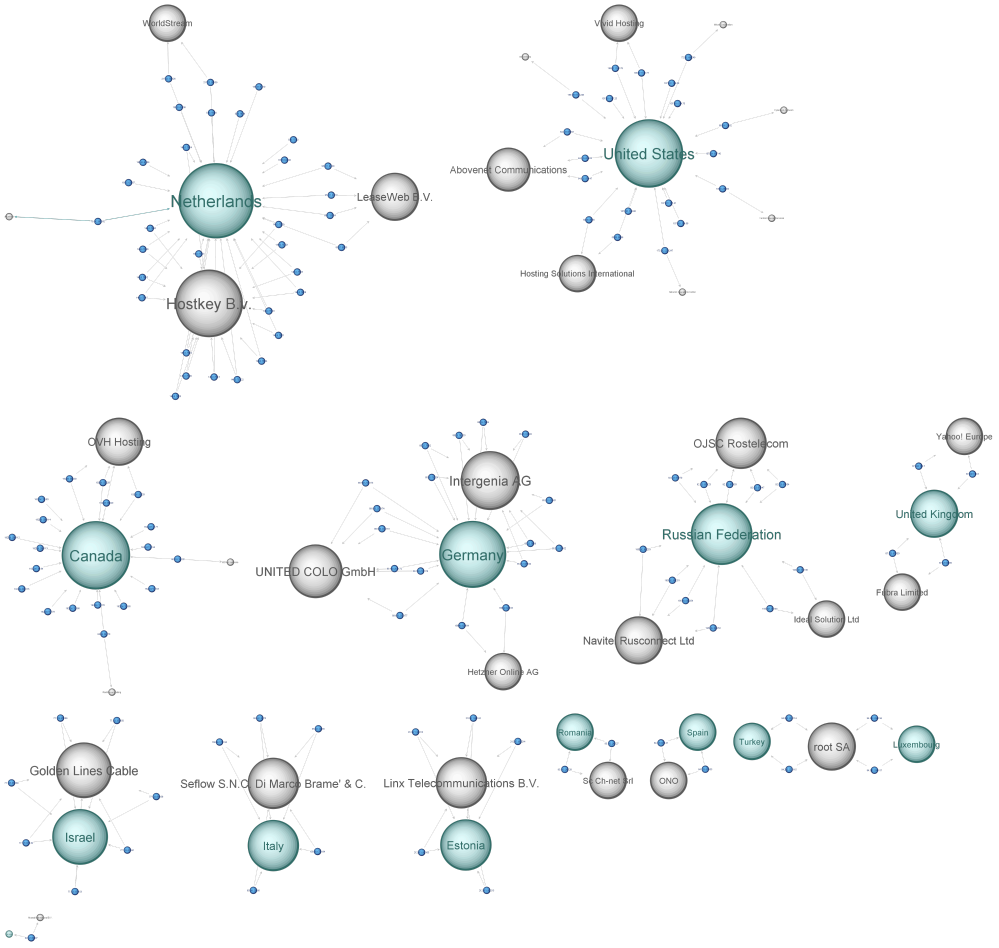

Figure 2. Redirection IPs

(Click to enlarge)

Botnets in the Threat Landscape

Botnets have deep ties throughout the threat landscape. For most cybercriminals, creating a botnet is the precursor for other malicious activities. Botnets can be used to send spam, perform distributed denial-of-service (DDoS) attacks, perform click fraud, or attack targeted domains.

For cybercriminals to launch these attacks, they need to be in constant communication with all their infected computers, whose numbers can reach the thousands and above. This is where command-and-control (C&C)

servers come in. A C&C infrastructure allows cybercriminals to have a dedicated connection between themselves and their victim's network. Our Global Botnet Map shows the connection between bots and C&C servers, highlighting the location of the C&C servers and the victimized computers they control.

Botnets are harmful to users in two ways: they push threats to users and they force victims to be unwitting accomplices to malicious activities. Being part of a botnet means a user is no longer in control of his computer; the bot master can dictate what the infected computers can and will do.

Addressing Botnets

Cybercriminals employ different tricks to add more victims to their botnets. For example, they often take advantage of peer-to-peer (P2P) networks to distribute disguised malware. Spammed messages are another go-to method for adding more computers to their botnets.

We advise users to be cautious when opening emails. Avoid opening emails and attachments from senders who are unknown or who cannot be verified. P2P networks aren't inherently malicious but users should be aware that dealing with these sites can increase their chances of encountering malware. Users should also invest in a security solution that goes beyond simple malware detection; features such as spam detection and URL blocking can go a long way in protecting users from threats.

We mentioned that SIMDA modifies HOSTS files as part of its redirection routines. There might be instances where the modified HOSTS files may remain even after detecting and removing SIMDA from the affected computer. The presence of these modified files might lead to further infections. We advise users to manually check HOSTS files and to remove any suspicious record in these files.

Trend Micro protects users from the SIMDA botnet by detecting malware variants as BKDR_SIMDA.SMEP and BKDR_SIMDA.SMEP2, and other BKDR_SIMDA variants. TROJ_HOSIMDA.SM is the Trend Micro detection name for the modified HOSTS files. All associated URLs have been blocked as well. Non-Trend Micro customers may use *Trend Micro Housecall* for scanning.

This entry was posted on Sunday, April 12th, 2015 at 11:03 pm and is filed under Botnets . You can leave a response, or trackback from your own site.
