



Tools

ZmbScap: Zombie Scapper

System: Linux, Solaris, Free BSD.All Unix Variants,Windows

License: GPL v 2

Application: Anti Distributed Denial Of Service Tool

Homepage: <http://www.metaeye.org/projects/zmbscap>,
<http://zmbscap.sourceforge.net>

ZmbScap is an open source tool written in perl. It is a prevention – mechanism against distributed denial of service attacks. The tool automatically scan the target machine for specific ports and kills the agent if listening.

Quick Start: The network is full of complexities. I think we can hardly find any network which is free from attack jargon. The network is not monotonous in its context but rather segregated into complex objects. These objects get exploited in every sense. Why? Because the cold war of attacks and prevention is on the way. Attackers or Worm writers do everything to own a box. The networks always get swamped. The distributed denial of service attacks are rising. Through our study and research we found lots of networks that are under the hood of Ddos attacks. We have not found any classic and effective mechanism to stop it. ZmbScap is a solution to this. The tool is fully functional and effective in stooping the Ddos agents. You can find lots of Ddos agents like Trinoo, WinTrinoo, Shaft, Mstream, Stacheldhart Ver 1 & 2, Trinity, Entitee etc. They are considered to be the best agents to launch distributed denial of service attacks. We have designed a generic Anti Ddos tool.

Imagine you are a network administrator of a redshot technologies. You find lots of problems in the company network. The research showed that a lot of packets are coming from a specific machine. The amount of packets is great. After the analysis you find that the network is under distributed denial of service attack. The packets are coming from toggled machine. After finding the signatures of packet and command stats, scan the target. It proves that trinoo and shaft agent are running. Try to use the ZmbScap tool for killing the agent. Trigger the console and launch the ZmbScap tools as: The working usage (see Figure 1).

Choose the target IP with the free system interface. Lets say eth0 is selected with (-i)option. You wish to send two packets with (-n) option and with timeout interval with (-t) tag. Issue the required command through the console (see Figure 2).

The tool is in inadvertent running mode and sending packets to kill the agents. It scans the target for opened ports and trigger the kill commands. Finally the agent stops throwing packets. The network is working fine again.

Other useful features: The tool is based on well derived signatures with the command identifiers and aims in stopping the master agents. The signature presence makes it more modular. For more additions a user has to add only signature arguments and the code is ready to run.

The tool generates a raw ICMP and UDP packets, with signatures defined that build a payload sent to the

agent to prevent it from flooding. This is effective because the packet building take place only after the target is found in listening state. This makes the tool very subtle in its working capability.

ZmbScap posseses functionality like interface selection. This means that the user can select any interface supported by the operating system. It can be eth0, eth1 or any other. The timeout strategy has been included in the tool. It stops the zombie masters by sending a kill/stop trigger. At present the tool supports following Ddos agents:

- Stacheldhart Version 1,
- Stacheldhart Version 2,
- Wintrinoo,
- Mstream,
- Tribal Flood Network,
- Trinoo,
- Shaft,
- Trinity,
- Entitee.

Disadvantages: The tool is console based and there is no web interface yet designed. ZmbScap might be run under Linux and other operating systems of the same type. Windows XP does not support raw icmp packet building.

by Aditya K Sood, Pranay Kanwar

```
zmbscap - Zombie Scapper v0.1.
Copyright (C) Metaeye Security Group - http://zmbscap.sourceforge.net.
http://www.metaeye.org

usage: zmbscap.pl -h <target> [-i <interface>] [-n <hits>] [-t <timeout>]
<target> : ip address or hostname to scan.
<interface> : interface to use for sending packets, default eth0.
<hits> : no of times to send kill packets, default 1.
<timeout> : communication timeout in seconds, default 3 seconds.
```

Figure 1. Usage Prompt Of ZmbScap

```
$ perl zmbscap.pl -h 172.31.1.3 -i eth0 -n 2 -t 3
zmbscap - Zombie Scapper v0.1.
Copyright (C) Metaeye Security Group - http://zmbscap.sourceforge.net.
http://www.metaeye.org

[+] Pinging host 172.31.1.3.
[+] Host is up.

[+] Scanning host 172.31.1.3 using interface eth0.

[+] Detected possible infection: Trinoo.
[+] Trying to kill Trinoo.
[+] Kill packet sent 2 time(s).

[+] Detected possible infection: Shaft.
[+] Trying to kill Shaft.
[+] Kill packet sent 2 time(s).
```

Figure 2. Working Mode Of ZmbScap

TrueSword 4

System: Windows 98/2000/Me/XP/Vista

License: Commercial

Application: Anti-malware software

Homepage: <http://www.securitystronghold.com>

True Sword is developed to protect user's computer against malicious programs, doing harm to their computer and breaking their privacy. This programs include trojans, spyware, adware, trackware, dialers, keyloggers, and even some special kinds of viruses.

Quick start: Suppose your computer or a host on your network hasn't been running at its optimal performance level. After ruling out hardware issues, you suspect that the system has been bogged down by unwanted malware and you want to scan the system to review and remove any unwanted malicious software. You can do this easily with True Sword 4 by Security Stronghold.

By choosing to scan either an entire computer, a specific drive, or simply by choosing a specific directory, you can see what software may be consuming system resources and causing unwanted activity on your host.

The first thing you will want to do when running True Sword 4 is to update the software with the latest information. To do this, simply click update and then select your update source. Once your software has been updated, you can begin your scan by selecting start! As the scan runs, you will see its progress in the main window. Alerts regarding suspicious software will pop up and ask for your input. Here, you may choose whether or not you would like True Sword to solve the problem, ignore it or seek more information regarding the threat. By checking the box stating, *Don't ask and do it always*, you can teach the software to ignore or solve the problem on its own upon each scan. Once your selection is made, the scan will continue. If you have taken action on something and decide that action was taken by mistake, simply click the Undo button and the change will be reversed.

Other useful features: True Sword scans your hard disks, registry and processes and removes all malicious software found. It also removes malicious BHOs and tracking cookies. It can find and eliminate over 180 000 types of spyware, addware and trojans. What sets True Sword 4 apart from its competitors is its ability to run scans based on a number of different criteria. By selecting Options, you can elect which parts of the system you would like to scan, whether you would like to scan cookies and registry items only, or if you would like to scan entities such as host files, startup items or registry entries. You can even customize how you would like True Sword to respond when it finds a virus or spyware. In this options section, you can even restore changes made previously by True Sword by viewing the list of changes True Sword made to your system and selecting undo. By adding the option to scan the system upon startup, you can be sure your system is being checked on a regular basis even with little action on your part.

Disadvantages: An inexperienced user, who seeks more information about a specific threat, may find the information provided to be too technical and literal to be of use. Users will have to review these alerts carefully to determine whether or not they are truly detecting unwanted software.

by Jennifer Allen



Figure 1. TrueSword Database update

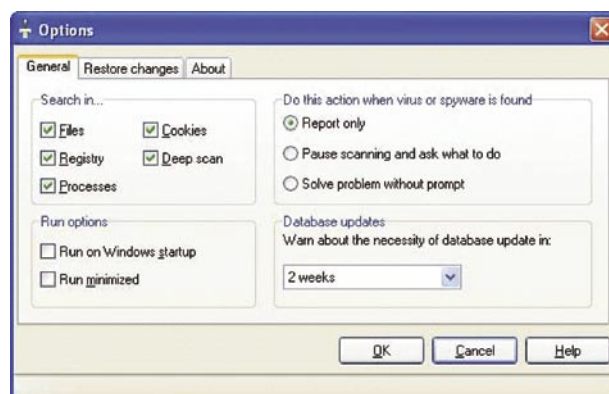


Figure 2. TrueSword options