Battling the Zbot Threat

Microsoft | Security Intelligence Report: Special Edition

January through December 2010

Microsoft®

Microsoft Security Intelligence Report

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Introduction

This document provides an overview of the Win32/Zbot family of password-stealing trojans. The document examines the background of Win32/Zbot, its functionality, how it works, and provides telemetry data and analysis from calendar year 2010 about how this threat is detected and removed by Microsoft antimalware products and services.

Authors

T.J. Campana – *Microsoft Digital Crimes Unit*
Joe Faulhaber – *Microsoft Malware Protection Center*
Paul Henry – *Wadeware LLC*
Matt McCormack – *Microsoft Malware Protection Center*
Frank Simorjay – *Microsoft Trustworthy Computing*
Holly Stewart – *Microsoft Malware Protection Center*

Background

Win32/Zbot is a family of password-stealing trojans that contain backdoor functionality which allows attackers to control infected computers remotely through illicit networks called *botnets*. The Win32/Zbot family warranted a close examination because of evidence that its presence on the World Wide Web was increasing. This family of botnets first drew attention in press and media when Win32/Zbot was detected[1] in mid-2007 attacking the U.S. Department of Transportation.

The botnet world is divided between bot families that are closely controlled by independent groups of attackers and those that are created through malware kits. These kits are collections of tools, sold and shared within the malware underground, that enable aspiring botnet operators, or *bot-herders*, to assemble their own botnets by creating and spreading malware variants. For more detailed information on botnets, see the Featured Intelligence story in Volume 9 of the Microsoft Security Intelligence Report.

Win32/Zbot is a kit-based family; its variants are built using a malware kit called Zeus. Although security professionals and news accounts often make reference to “the Zeus botnet,” it’s important to realize that computers infected with Win32/Zbot do not all belong to a single large botnet, but instead many smaller independently controlled botnets that are controlled by many bot-herders.

Functionality

From its first releases in late 2006 and early 2007, Win32/Zbot included a number of functions and behaviors that often indicate professionally developed malware. These functions and behaviors include:

- Process injection, in which the malware runs within a process spawned by a legitimate program or operating system component in an effort to avoid detection.
- Encryption of stolen data using strong encryption.
- Multi-process interconnectivity, in which the malware persists across all Windows processes using a Mutex to coordinate threads.

[1] www.reuters.com/article/idUSN1638118020070717

- API hooking to intercept browser information. Rather than use a keylogging mechanism, Win32/Zbot interfaces directly with popular browsers to monitor traffic and information.
- Custom-engineered packer and obfuscation techniques to evade detection by security software.
- Easy-to-use interfaces for installing, configuring, and using the Win32/Zbot builder and server components of the Win32/Zbot kit.

Purpose and Use

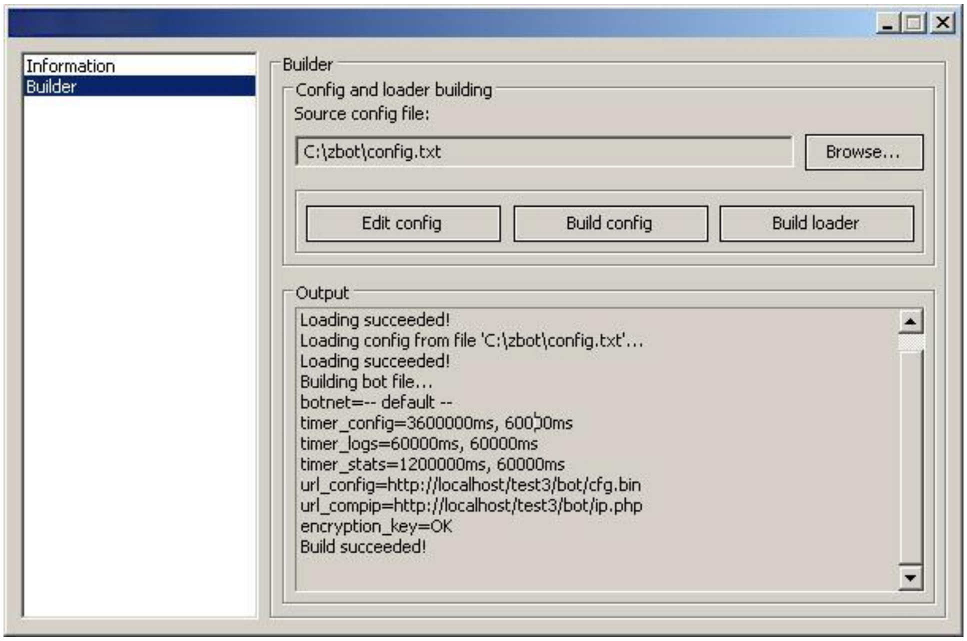
Like many botnet families, Win32/Zbot can be used for a variety of illicit purposes, including sending spam email messages, executing distributed denial-of-service (DDoS) attacks, and distributing additional malware. However, its primary purpose, and the one for which it was specifically developed, is to steal financial information from infected computers. Built-in commands allow the botnet operator to perform a number of actions that are designed to facilitate theft of financial information, including:

- Stealing login credentials for banking websites.
- Stealing website certificates for online banking.
- Deleting browser cookies, which forces users to re-enter their online data credentials so they can be stolen.
- Injecting additional HTML into banking websites and other secure pages. This technique is used to facilitate identity theft by modifying website pages to insert extra fields into web forms that prompt users to enter additional data (such as Social Security numbers).

How Win32/Zbot Works

A complete Win32/Zbot kit consists primarily of a builder component (shown in the following figure) that is used to create the Win32/Zbot malware for distribution and a web-based control panel for communication with infected computers.

Figure 1. The builder component of the Win32/Zbot malware creation kit



Source config file: C:\zbot\config.txt

```
Loading succeeded!
Loading config from file 'C:\zbot\config.txt'...
Loading succeeded!
Building bot file...
botnet=-- default --
timer_config=3600000ms, 60000ms
timer_logs=60000ms, 60000ms
timer_stats=1200000ms, 60000ms
url_config=http://localhost/test3/bot/cfg.bin
url_compip=http://localhost/test3/bot/ip.php
encryption_key=OK
Build succeeded!
```

Like most botnet families, Win32/Zbot is based on the client-server model; it requires a *command and control* (C&C) server to which the bots connect to receive instructions from the botnet operator. A kit to set up a server is sometimes bundled with the base Win32/Zbot kit, or can be obtained from other black market sellers.

The C&C server represents the weak point in a conventionally designed botnet, and takedown efforts by law enforcement and upstream networking providers typically focus on neutralizing the C&C server to render the entire botnet inoperable. Many black market sellers offer “bulletproof” hosting for C&C servers that are supposedly resistant to takedown requests.

Recent versions of Win32/Zbot malware have included a domain generation algorithm that is similar to the one used by Win32/Conficker, and is intended to make C&C servers more resistant to takedown attempts. The algorithm generates a list of pseudorandom domain names to which the bots will attempt to connect at different times. The botnet operator uses the same algorithm and seed to generate the list of domain names in advance, registers some of the domain names on the list, and points the names to the IP address of the C&C server on or before the date on which the bots are scheduled to connect to them.[2]

Attackers use a number of different methods to spread bots, including spam, social engineering, exploiting vulnerabilities in system and application software, and using other malware families to download and install bots to infected computers. The Win32/Zbot server itself is frequently packaged with exploit packs that can be used to help spread bots—for example, by automatically finding websites that are vulnerable to SQL injection and uploading exploit code that targets site visitors.[3]

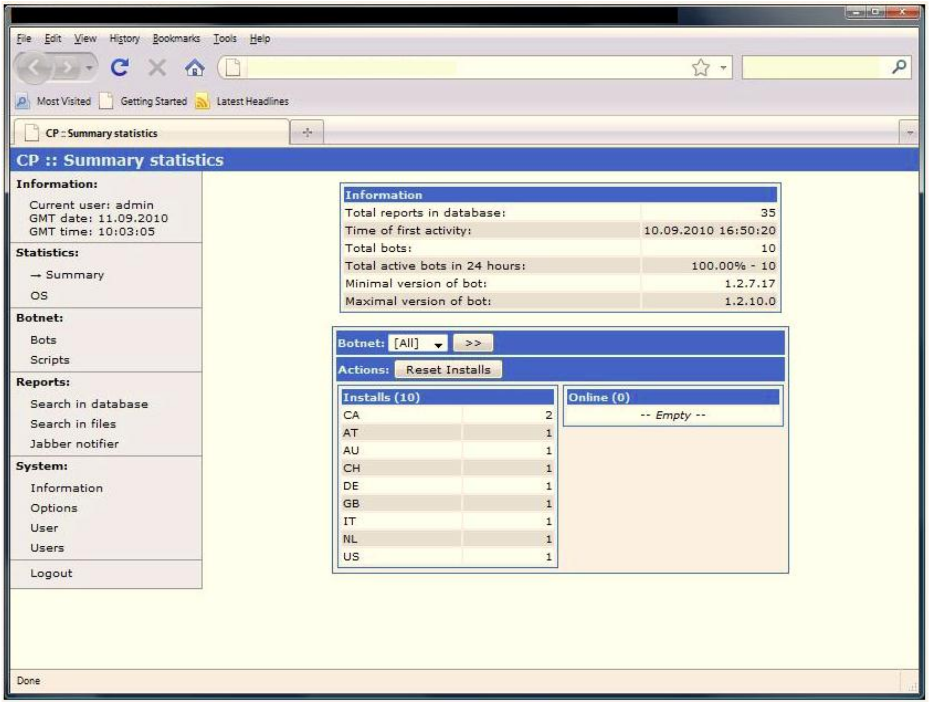
When the Win32/Zbot executable is launched on a targeted computer, it copies itself to the %system% or %appdata% directory, depending on the operating system version, the Win32/Zbot version, and the privilege level of the account that Win32/Zbot is running under. It then proceeds to inject itself into various processes in the system, typically winlogon.exe and explorer.exe, and run primarily from within those processes' contexts. At this stage, the malware initiates system-wide API hooks to obtain sensitive information, hide files, and to protect itself from removal. Win32/Zbot then contacts its C&C server to receive further instructions.

The attacker controls the bots using a central web-based control panel, an example of which is shown in Figure 2.

[2] For more information about Win32/Conficker's use of the domain generation tactic, see “Birthday Problem and Conficker” (April 6, 2009) on the MMPC blog (http://blogs.technet.com/mmpc).

[3] For more information about this tactic, see “Automated SQL Injection Attacks” in the Reference Guide section of the Microsoft Security Intelligence Report website (www.microsoft.com/sir).

Figure 2. A Win32/Zbot control panel



CP :: Summary statistics

Information:

Current user: admin
GMT date: 11.09.2010
GMT time: 10:03:05

Statistics:

→ Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files
Jabber notifier

System:

Information
Options
User
Users

Logout

Information	
Total reports in database:	35
Time of first activity:	10.09.2010 16:50:20
Total bots:	10
Total active bots in 24 hours:	100.00% - 10
Minimal version of bot:	1.2.7.17
Maximal version of bot:	1.2.10.0

Botnet: [All] >>

Actions: Reset Installs

Installs (10)	
CA	2
AT	1
AU	1
CH	1
DE	1
GB	1
IT	1
NL	1
US	1

Online (0)
-- *Empty* --

The operator uses the control panel to issue a variety of different commands to any connected bots. Some of the functions that Win32/Zbot-infected computers can be commanded to perform include:

- Steal browser data in the following ways:
    - Take screenshots of banking sites
    - Modify webpages to extend forms to require extra information
    - Obtain HTML form data
    - Transparently redirect users to fake sites that appear to be legitimate
- Steal system information, including:
    - Protected storage credentials
    - Credentials from FTP, email, and custom applications such as WinSCP
    - Files uploaded from the system
- Modify system settings to accomplish the following:
    - Render the system unbootable to cover its tracks
    - Download and execute other binaries, which effectively means that anything could be on a system infected by Win32/Zbot

Fighting Win32/Zbot

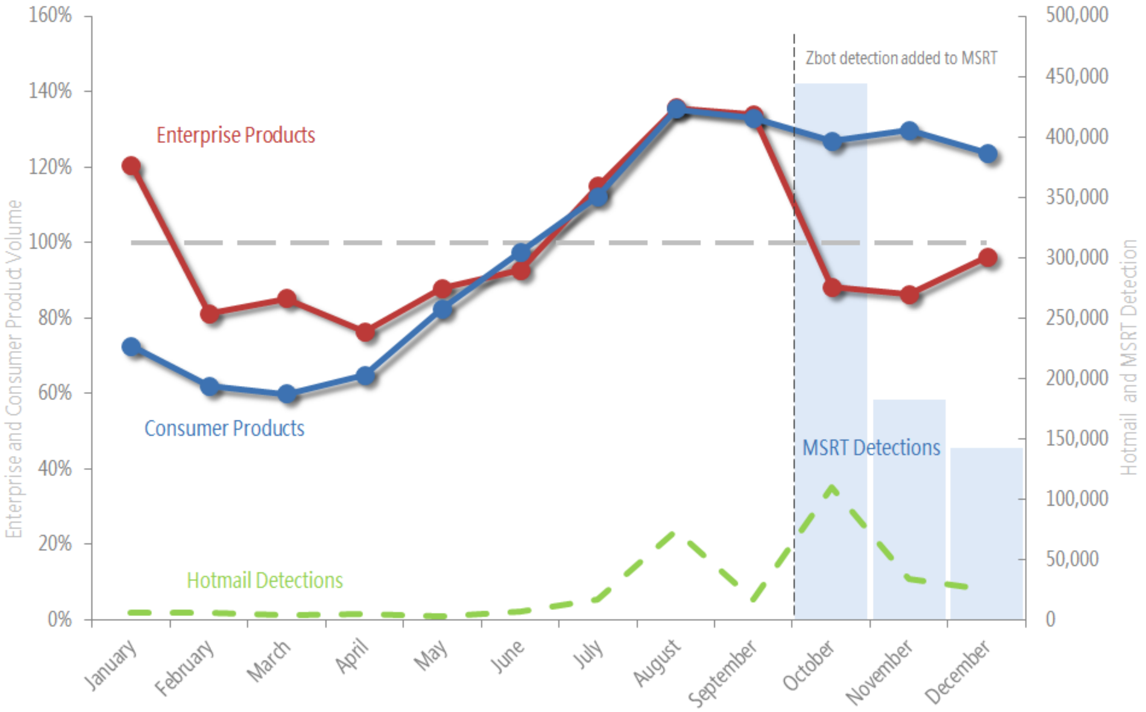
Microsoft has been actively attacking Win32/Zbot malware since 2007, when the ability to detect this threat was added to Microsoft consumer and enterprise real-time protection products. Although real-time protection was preventing Win32/Zbot infections for users of such products, the Microsoft® Malware Protection Center (MMPC) decided to broaden its attack efforts through the large installed base of Microsoft Malicious Software Removal Tool (MSRT) subscribers. In October 2010, the MMPC included detection for more than 500 different Win32/Zbot variants in the MSRT, which is offered to customers on a monthly basis through Windows® Update.

The MSRT removed Win32/Zbot infections from 444,292 computers in the first month after it was released. Although the MMPC releases new detection signatures and constantly updates old ones to keep pace with malware creators, 34 percent of the Win32/Zbot variants detected during the first month were detected using older Win32/Zbot signatures that hadn't changed since May 2010.

Because of the monthly release schedule of the MSRT, new variants that appear between updates might not be removed by the tool until the next monthly release. The Win32/Zbot family is known to have many variants and to receive regular updates, yet the high percentage of infections removed using older signatures indicates that many infected computers were not infected with recent Win32/Zbot code. (Real-time protection products, such as Microsoft Forefront® Endpoint Protection or Microsoft Security Essentials, can receive multiple definition updates daily and therefore provide the most up-to-date protection against Win32/Zbot infection.)

The addition of Win32/Zbot coverage to the MSRT appears to have had a measurable effect on the Win32/Zbot ecosystem, as shown in Figure 3.

Figure 3. Detections of Win32/Zbot by security product category in 2010, by percentage of the monthly average for enterprise and consumer products and number of detections for Hotmail and the MSRT



As Figure 3 shows, Win32/Zbot detections and removals by Microsoft enterprise security products, such as Forefront Endpoint Protection and Forefront Threat Management Gateway, increased gradually for most of the year, reaching a September high of 134 percent of the 2010 monthly average number of Win32/Zbot detections by enterprise products. In October, when the first version of the MSRT withWin32/Zbot coverage was released, the figure fell dramatically to 88 percent of the monthly average, and remained depressed the following month.

After low activity for most of the year, Win32/Zbot Hotmail detections spiked once in August and then again in October. It is unclear what prompted botnet operators to greatly increase email distribution of the Win32/Zbot malware.

Geographic Statistics

Like most malware families, Win32/Zbot does not affect all parts of the world equally. The following figures show the global distribution of Win32/Zbot infections and infection attempts for countries and regions around the world as detected by Microsoft Security Essentials in 2010.

Figure 4. The 10 locations with the highest concentration of Win32/Zbot detections in September 2010, as determined by Microsoft Security Essentials, the peak month before the release of detection in MSRT

	Country/Region	Win32/Zbot Percent of Computers With Security Essentials Reporting Detections
1	Spain	1.0%
2	United Kingdom	0.9%
3	Portugal	0.9%
4	Germany	0.4%
5	Russia	0.3%
6	Italy	0.3%
7	Turkey	0.3%
8	United States	0.2%
9	Australia	0.2%
10	Ireland	0.2%

Spain, at 1.0% (meaning, nearly one out of every 100 computers running Microsoft Security Essentials reported at least one Win32/Zbot infection attempt), had the highest percentage of detections during the period, followed by the United Kingdom (0.9%), and Portugal (0.9%).

Figure 5. Average monthly Win32/Zbot detections per capita by Microsoft Security Essentials, 2010

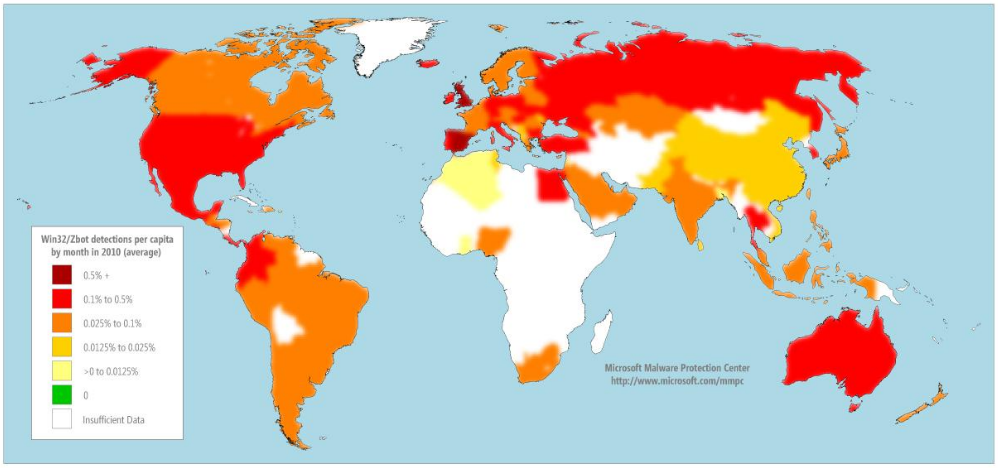
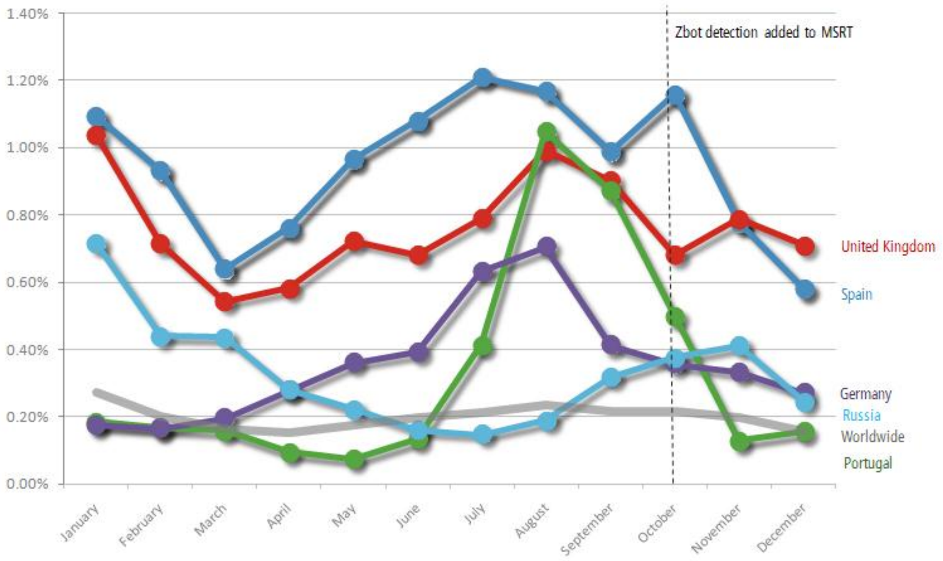

Win32/Zbot detections per capita by month in 2010 (average)
0.5% +
0.1% to 0.5%
0.025% to 0.1%
0.0125% to 0.025%
>0 to 0.0125%
0
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Figure 6. Percent of computers running Security Essentials reporting at least one Win32/Zbot detection by month in 2010, top five country/regions and worldwide average



One interesting trend about the top country/region list for Win32/Zbot detections shown in Figure 4 is that seven of the top 10 most-infected locations are in the top quintile of economies ranked by per-capita GDP,[4] compared to three of the top 10 most-infected locations overall.

[4] As determined by the International Monetary Fund for 2009.

Guidance: Defending Against Malicious and Potentially Unwanted Software

Effectively protecting users from malware requires an active effort by both organizations and individuals. It’s important to maintain up-to-date anti-malware defenses and to stay informed about the latest developments in malware propagation techniques, including social engineering.

For in-depth guidance, see the following resources in the “Mitigating Risk” section of the Microsoft Security Intelligence Report website:

- Promoting Safe Browsing
- Protecting Your People

Microsoft®
One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security