**Introduction**

This document summarizes our analysis of Zbot, and contains the following:

* Static Analysis
* Dynamic Analysis
* Summary of Functionality

This analysis was performed using the static and dynamic analysis results furnished by Any.Run and VirusTotal.

**Static Analysis**

**Synopsis of Executable**

This section contains a summary of the uploaded executable: Zbot.

*Zeus is a builder and it creates malware for hackers to build and send to their victims. The malware themselves are highly customizable and does a variety of tasks. Therefore, I used a variety of different Any.Run examples of Zbot.*

* All the file types of Zbot seem to be .exe and file size varies from 113.50 Kb to 244.00kb
* Compilation date
  + 2-Aug-19
  + 28-Jul-19
  + 7-Apr-19
  + 14-Feb-19
* Zbot usage spiked in November 2009
  + Zeus has been active since 2006, and it’s still a risk since the file can have various hashes and keeps being updated
  + Initial Rapid Release version January 07, 2010 revision 037
  + Latest Rapid Release version September 07, 2016 revision 004
  + Initial Daily Certified version January 07, 2010 revision 049
  + Latest Daily Certified version September 06, 2016 revision 020
  + Initial Weekly Certified release date January 13, 2010
* The Zeus package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command and control server.
  + vectors of infection vary widely, with popular methods including drive-by downloads and SPAM
  + The main purpose of Zeus is to steal online credentials as specified by the hacker.
* Zbot looks different to different anti-virus scanners. Various anti-virus software classify Zbot is
  + Generic Trojan
  + Backdoor
  + Win32 Trojan
  + Zbot

**Initial Behavior**

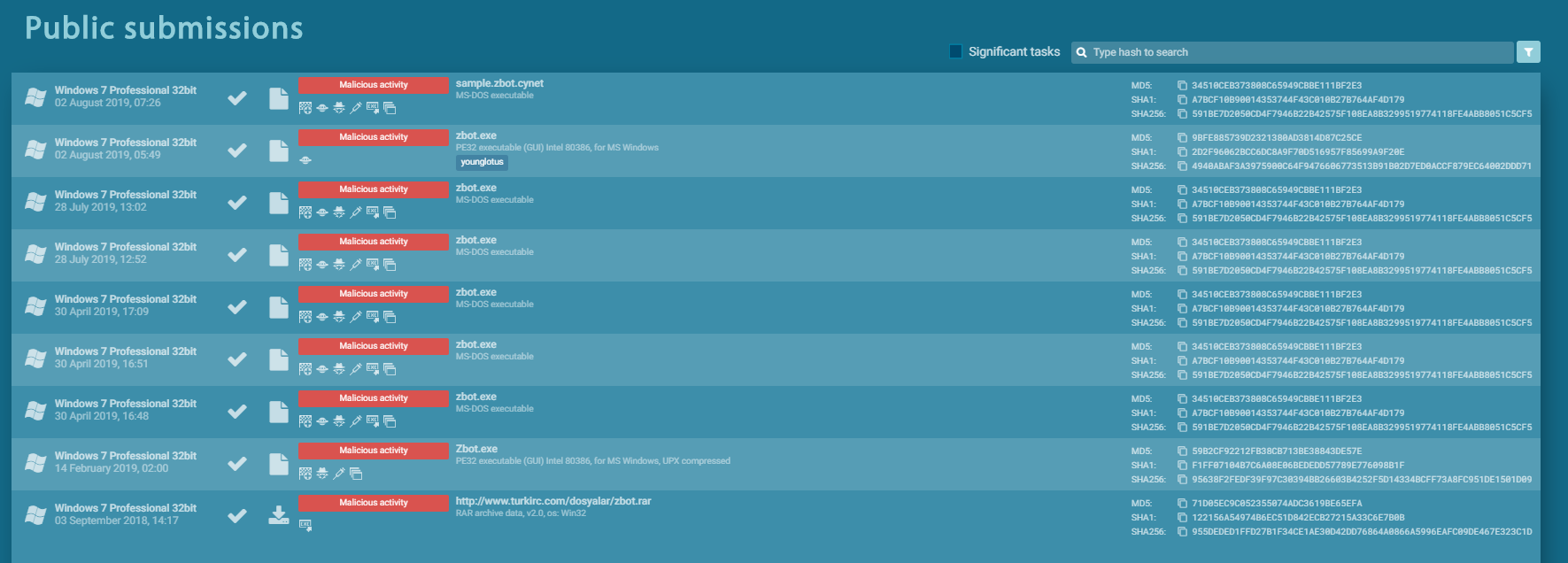
The table below summarizes the initial activity generated by the sample upon upload to Any.Run.

|  |  |
| --- | --- |
| **Activity Type** | **Count** |
| HTTP Requests | **Bot sends a GET request to the command and control server to retrieve the configuration file** |
| DNS Requests | Possible |
| Connections | Possible |
| Files Changed | **%system32%\sdra64.exe**  **Svchost.exe** |

**Dynamic Analysis**

The results below were generated by executing Zbot sample on Any.Run’s hosted platform.

**Process Environment**



* *https://app.any.run/tasks/8997c8a3-3a1f-43c7-b8fb-a3e6e72b8894/*
* *https://app.any.run/tasks/cbbba64e-2453-4aca-814b-2fd55f8e3e91/*
* *https://app.any.run/tasks/07644b1f-5493-44a1-ac09-ef6bfa5801d1/*
* *https://app.any.run/tasks/c15db619-356d-4e18-8930-da2d422429c5/*

*I used various Zbot samples to compile a list of various Environments they are all within a Windows 7.*

* The user the process runs as
  + Usually explorer.exe
* Version information of Explorer
  + 6.1.7600.16385 (win7\_rtm.090713-1255)
* Indicators of suspicious activity
  + Runs injected code in another process
  + Changes the autorun value in the registry
  + Changes the login/logoff helper path in the registry
  + Creates files in the user directory
  + Starts CMD.EXE for commands execution
  + Executable content was dropped or overwritten
  + Starts itself from another location
  + Actions looks like stealing of personal data
  + Application was injected by another process
  + Changes internet zones settings
  + Modifies the Internet Explorer registry keys for privacy or tracking
  + Connects to CnC Server

**Network Activity `**

* If Zbot makes HTTP requests, they are to get the updated compile file from the Command and Control
* If Zbot makes DNS requests they are to change the IP address of the target to whatever the hacker intends

The following table describes the servers that the sample communicated with.

|  |  |  |  |
| --- | --- | --- | --- |
| **Request Type** | **Target Domain** | **Target IP Address** | **Reputation** |
| TCP Protocol | lu1164224557.oicp.net | 174.128.255.232 | Malicious |

**In the above example it was used to get the updated compile file from the Command and Control Server**

**Filesystem Modifications**

The Zbot changes the registry files including winlogon.exe, increases its privileges, injects its code and a string table into this process, and creates a thread to execute this code

* If Any.Run reports suspicious file modifications, list and summarize them here
* HKEY \_ LOCAL \_ MACHINE\Software\Microsoft\Windows NT\winlogon\Userinit
* Creates: \lowsec with local.ds and user.ds
  + To keep track of user and local data and send to the Command and Control
* Web Page Injection
  + Add input file that look like they are apart of the page for the user to input sensitive information

**Summary**

* At a high-level Zbot is a generic malware that hackers can create for a certain target
* What were the most prominent signs of malicious behavior?
  + Changes values in the registry
    - To allow complete access to all information of user
  + Stealing of personal data
    - To Send to the attacker
  + Injects website input fields
    - for the user to input more personal data for the attacker
  + Changes internet zones settings
    - If the attacker wants the user to go to their domain for a bank login rather than the actual webpage
  + Connects to CnC Server

**Containment Strategy**

This document contains counsel as to the scope and severity of infections by Zbot, as well as steps to fix infected computers and prevent future attacks.

**Scope**

*Windows devices are targeted specifically windows 7 to gain access to a wide variety of users. Targets of this could be data monitoring of a large group of individuals looking for trends or a database of information. Or cause destruction for a large group of users.*

**Severity**

*Based on this information, the recommend a timeline for patching is as soon as possible*. *Look for information on:*

* How much damage Zbot does to the infected computer?
  + the computer would show little signs of infection since the point of the Zbot is to spy on the user. Slightly slower internet speeds would be the only signal
  + Very little damage
* How hard is it to remove without replacing the computer.
  + Since the bot can look like a various of different files it would be slightly difficult for the antivirus find all of it within the computer.
  + Medium
* How much data it can get access to it exposes all personal information on the user and gets the user to send even more than just what’s provided.
  + It sends all the data to the attacker

Based on the above, we conclude that this sample is of **Zeus/Zbot** severity, and should be considered **Medium\High**

**Solution**

*Zbot relies heavily on social engineering in order to infect computers so users have to be wary of spam emails that trick them into clicking links.*

As of February 24, 2010, Trojan.Zbot has been seen using the following vulnerabilities:

* AOL Radio AmpX ActiveX Control 'ConvertFile()' Buffer Overflow Vulnerability (BID 35028)
* Microsoft Active Template Library Header Data Remote Code Execution Vulnerability (BID 35558)
* Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness (BID 10514)
* Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download Vulnerability (BID 30114)
* Adobe Reader 'util.printf()' JavaScript Function Stack Buffer Overflow Vulnerability (BID 30035)
* Adobe Acrobat and Reader Collab 'getIcon()' JavaScript Method Remote Code Execution Vulnerability (BID 34169)
* Adobe Reader and Acrobat (CVE-2009-2994) U3D 'CLODMeshDeclaration' Buffer Overflow Vulnerability (BID 36689)
* Adobe Acrobat and Reader Multiple Arbitrary Code Execution and Security Vulnerabilities (BID 27641)

The Zeus threat is actually comprised of three parts: a toolkit, the actual Trojan, and the command & control (C&C) server. The toolkit is used to create the threat, the Trojan modifies the compromised computer, and the C&C server is used to monitor and control the Trojan.

Keeping the most updated antivirus is effective since the malware has a recognizable template however there are many varieties that keep being created, therefore staying up to date is important