AMP for Endpoints ZBot

Last Updated: August 9, 2016

Cisco Systems, Inc. www.cisco.com

CHAPTER 1
INTRODUCTION

This attack scenario replicates an “in the wild” infection of ZBot. In addition to being a banking Trojan, ZBot (aka ZeuS, Gameover) has also recently been modified to incorporate a P2P botnet.

ZBot is often installed on computers via drive-by download, often from websites that have been compromised with an exploit toolkit. These toolkits attempt to exploit several browser vulnerabilities when a user visits the compromised website. In this scenario we will use AMP for Endpoints to discover the malicious activity and find all associated secondary infections.

IMPORTANT! In the following scenario the policy for the AMP for Endpoints Connector was set to audit-only mode to show the full range of actions malicious files could take and how each action is recorded and displayed by AMP for Endpoints.

CHAPTER 2
THE ATTACK

The attack starts when the victim visits a compromised website that exploits CVE-2012-4792, the Microsoft Internet Explorer Use-After-Free arbitrary code execution, a 0-day vulnerability that was exploited in the wild in December 2012. Like many attacks, the exploit sets off a chain of events including downloading and executing malware, which will show up in the AMP for Endpoints console and can be used to demonstrate how AMP for Endpoints can be used to detect and remediate such attacks.

In a typical scenario the attacker would compromise a legitimate website and use it to host the exploit or set up a server that hosts the exploit and attempt to lure users by placing a link to it in email messages or on social networking sites.

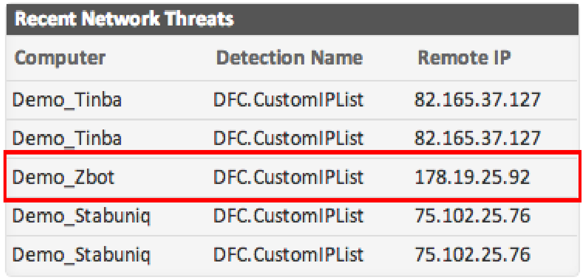
When the user visits the site, it exploits the Internet Explorer vulnerability and downloads ZBot then executes it. ZBot infects Windows Explorer as part of its P2P communication channel.

Chapter 3

Detection and Remediation

When you log in to the AMP for Endpoints Console the first page you see is the Dashboard Overview. This page shows you recent file and network detection events from your AMP for Endpoints Connectors. It's a convenient summary of the major trouble spots in your AMP for Endpoints deployment that allows you to perform triage to determine which computers are in most need of immediate attention.

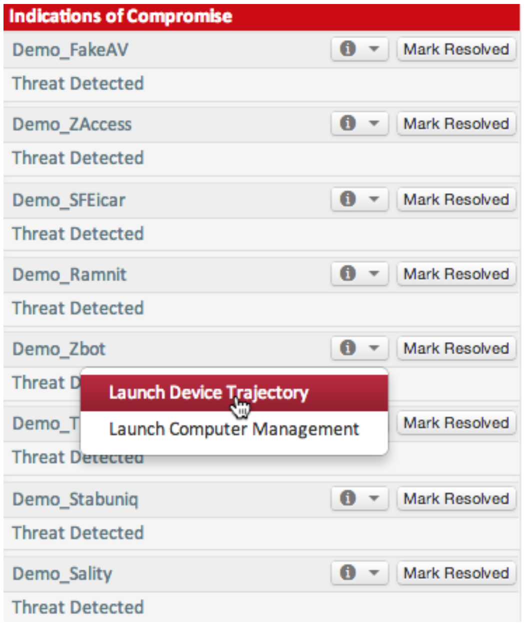
In this scenario we see under Recent Network Threats that one of the computers in our AMP for Endpoints deployment attempted a connection to a known malicious IP address. The address in question is associated with P2P communications used by ZBot.



Recent Network Threats

Computer	Detection Name	Remote IP
Demo_Tinba	DFC.CustomIPList	82.165.37.127
Demo_Tinba	DFC.CustomIPList	82.165.37.127
Demo_Zbot	DFC.CustomIPList	178.19.25.92
Demo_Stabuniq	DFC.CustomIPList	75.102.25.76
Demo_Stabuniq	DFC.CustomIPList	75.102.25.76

The same computer appears in our Indications of Compromise widget on the Dashboard. If we click the information icon next to the computer name and select Device Trajectory from the drop down menu we can get more information on what triggered this event.



Indications of Compromise

Demo_FakeAV | Mark Resolved
Threat Detected

Demo_ZAccess | Mark Resolved
Threat Detected

Demo_SFEicar | Mark Resolved
Threat Detected

Demo_Ramnit | Mark Resolved
Threat Detected

Demo_Zbot | Mark Resolved
Threat D

Launch Device Trajectory
Launch Computer Management

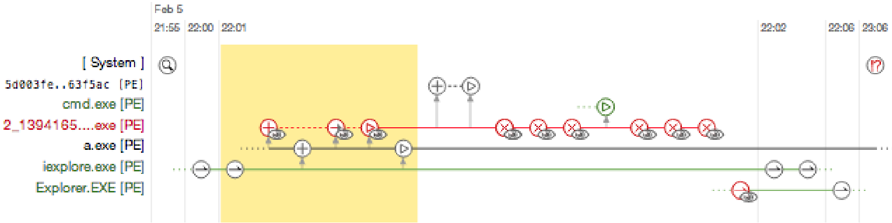
Demo_T | Mark Resolved
Threat Detected

Demo_Stabuniq | Mark Resolved
Threat Detected

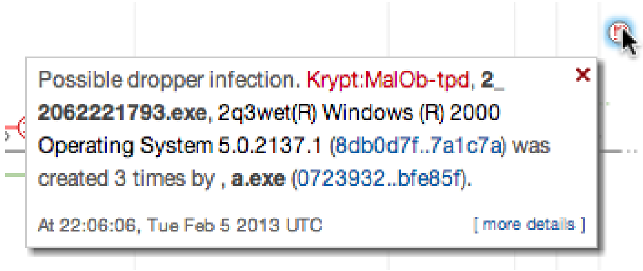
Demo_Sality | Mark Resolved
Threat Detected

Tracing Backwards

When we view the Device Trajectory for this computer can see signs that it has been compromised right away as there is one malicious file that has triggered multiple detection events as well as a highlighted area showing events that triggered an Indication of Compromise event.



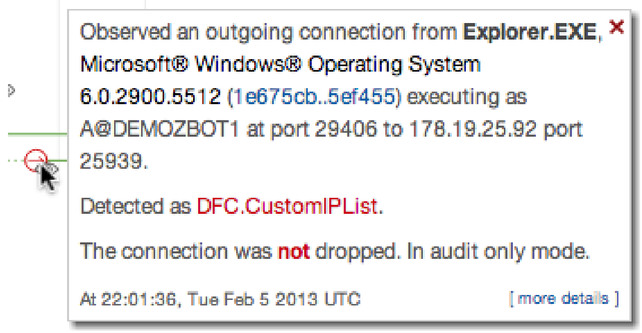
When we click on the Indication of Compromise event we can see the type of compromise that is suspected and what triggered it.



Possible dropper infection. Krypt:MalOb-tpd, **2_2062221793.exe**, 2q3wet(R) Windows (R) 2000 Operating System 5.0.2137.1 (8db0d7f..7a1c7a) was created 3 times by , **a.exe** (0723932..bfe85f).

At 22:06:06, Tue Feb 5 2013 UTC [more details]

Interestingly, we also see that explorer.exe (Windows Explorer) has made an outbound network connection to a site that we've previously blacklisted as a known command and control channel.



Observed an outgoing connection from **Explorer.EXE**, Microsoft® Windows® Operating System 6.0.2900.5512 (1e675cb..5ef455) executing as A@DEMOZBOT1 at port 29406 to 178.19.25.92 port 25939.

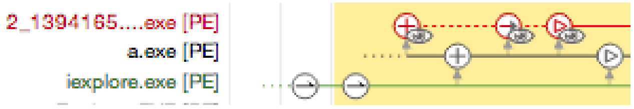
Detected as DFC.CustomIPList.

The connection was **not** dropped. In audit only mode.

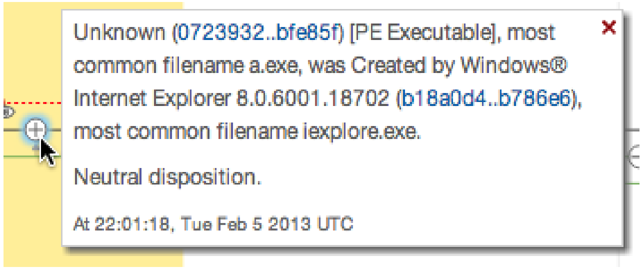
At 22:01:36, Tue Feb 5 2013 UTC [more details]

This indicates that explorer.exe has likely had another process injected into it or otherwise been subverted. Since there was only one other malicious file detected on the computer and it executed at the same time this connection was made, it is probable the two are directly related.

Looking further back in time, we can see that three executables were involved - our detected malware, iexplore.exe (Internet Explorer), and a file called a.exe with an unknown disposition.



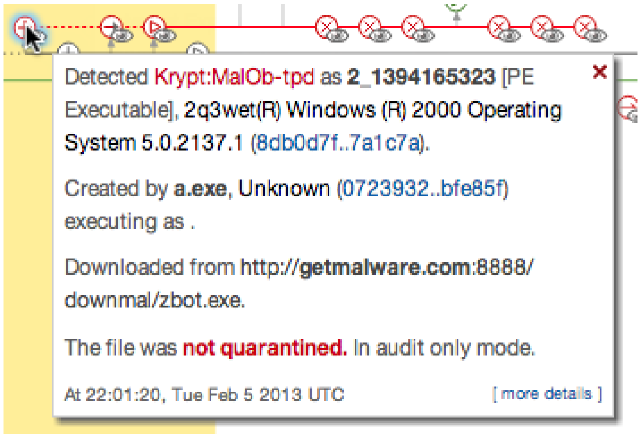
It appears that a.exe was created and executed by iexplore.exe and in turn created and executed the malware.



Unknown (0723932..bfe85f) [PE Executable], most common filename a.exe, was Created by Windows® Internet Explorer 8.0.6001.18702 (b18a0d4..b786e6), most common filename iexplore.exe.

Neutral disposition.

At 22:01:18, Tue Feb 5 2013 UTC



Detected Krypt:MalOb-tpd as **2_1394165323** [PE Executable], 2q3wet(R) Windows (R) 2000 Operating System 5.0.2137.1 (8db0d7f..7a1c7a).

Created by **a.exe**, Unknown (0723932..bfe85f) executing as .

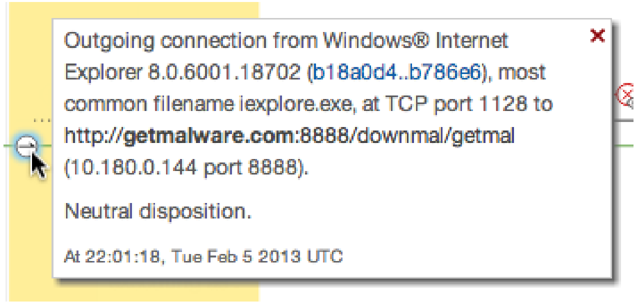
Downloaded from http://**getmalware.com**:8888/downmal/zbot.exe.

The file was **not quarantined.** In audit only mode.

At 22:01:20, Tue Feb 5 2013 UTC

This tells us that a.exe downloaded our malware sample from a remote website, behavior consistent with a pony downloader. This is an application whose sole purpose is to get onto a computer and execute so that it can download malware. These downloaders are usually not malicious themselves so that they can evade detection.

Just before a.exe was created on the computer by Internet Explorer we can see that iexplore.exe made an outbound network connection.



Outgoing connection from Windows® Internet Explorer 8.0.6001.18702 (b18a0d4..b786e6), most common filename iexplore.exe, at TCP port 1128 to http://**getmalware.com**:8888/downmal/getmal (10.180.0.144 port 8888).

Neutral disposition.

At 22:01:18, Tue Feb 5 2013 UTC

While connecting to remote sites is expected behavior for Internet Explorer, it is the last connection made before a.exe was downloaded and executed. This makes the site listed the most likely candidate for the point of origin of our attack.

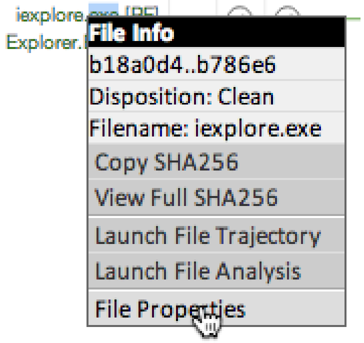
Remediation

Now that the origin of the compromise has been identified we can begin the process of remediation and blocking future compromise by this threat. Using Outbreak Control lists we can stop vulnerable applications from executing, detect and quarantine unknown files, and black list associated IP addresses.

Application Blocking

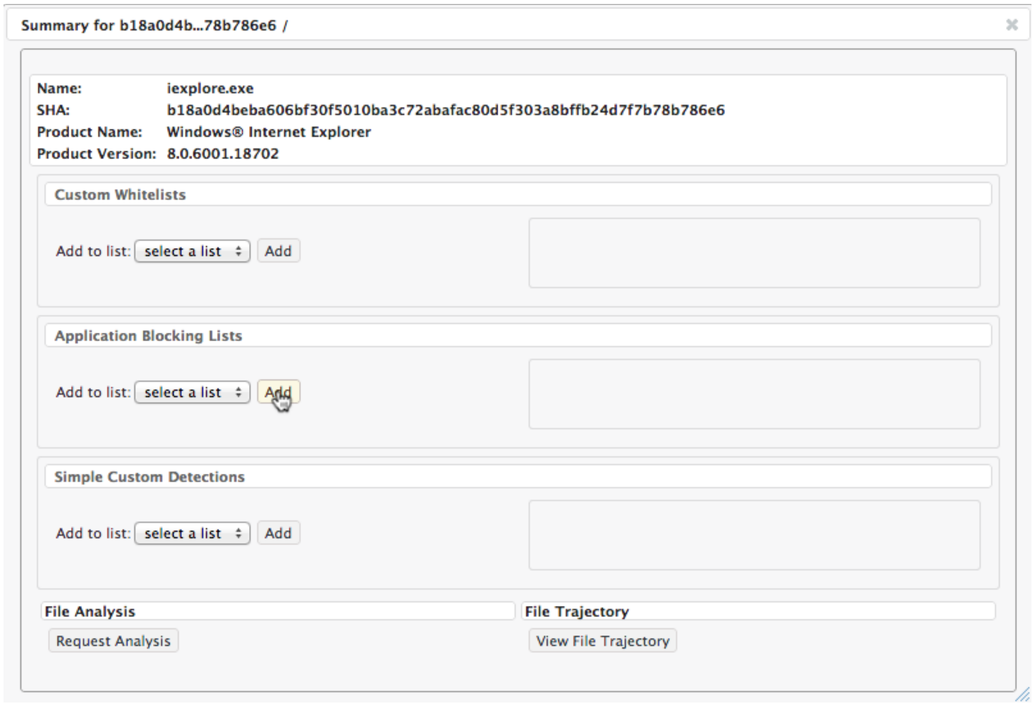
First, we can close off the original entry point of the infection by upgrading Internet Explorer to a version that is not vulnerable to the exploit used. We can also prevent the vulnerable version from running by adding it to an Application Blocking List. This is convenient if you don't want users running the vulnerable application before the upgrade is deployed or in cases where there is no patch or fix available yet.

To add iexplore.exe to an Application Blocking list, right click on its SHA-256 anywhere from Device Trajectory or File Trajectory and select File Properties from the context menu.



File Info
b18a0d4..b786e6
Disposition: Clean
Filename: iexplore.exe

From the File Properties dialog, select the name of a list from the Application Blocking Lists section and click Add.



Summary for b18a0d4b...78b786e6 /

Name: iexplore.exe
SHA: b18a0d4beba606bf30f5010ba3c72abafac80d5f303a8bffb24d7f7b78b786e6
Product Name: Windows® Internet Explorer
Product Version: 8.0.6001.18702

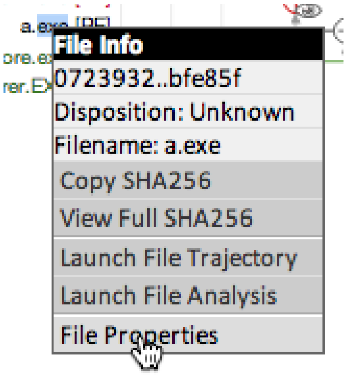
Custom Whitelists
Add to list: select a list Add
Application Blocking Lists
Add to list: select a list Add
Simple Custom Detections
Add to list: select a list Add
File Analysis
Request Analysis
File Trajectory
View File Trajectory

Make sure that the Application Blocking List you have selected is applied to any applicable policies. You can repeat this step to add iexplore.exe to other Application Blocking Lists as well. An Application Blocking List does not quarantine applications you add to it, but instead prevents them from running.

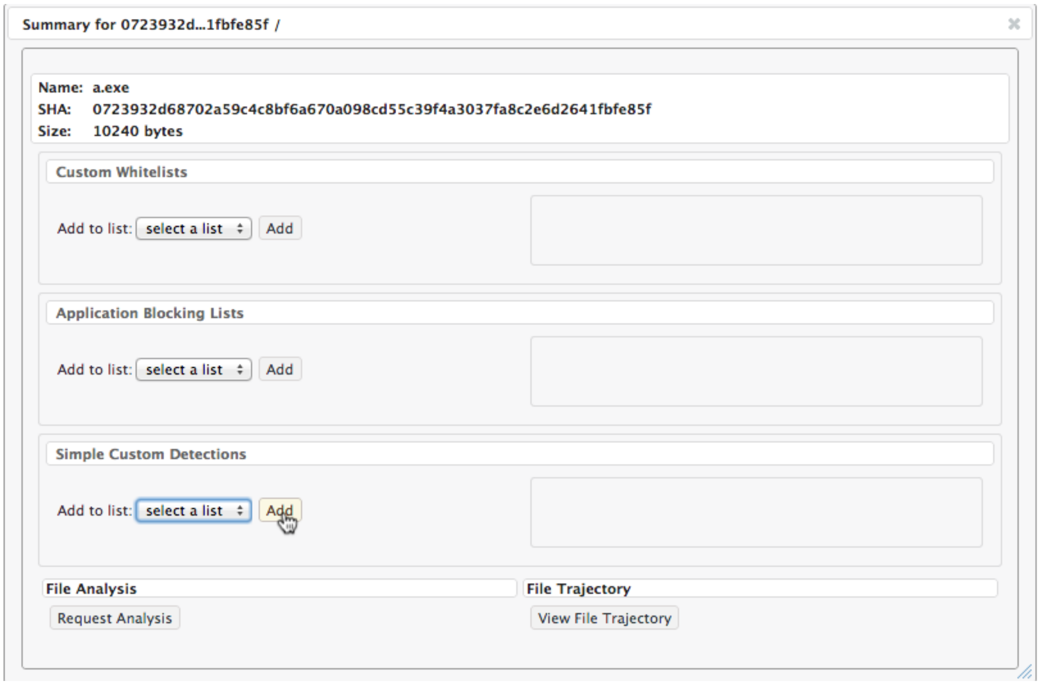
Simple Custom Detections

Next we'll add a.exe to a Simple Custom Detection list. This will not only detect and quarantine any new instances of the file, but any existing ones as well the next time they are created, moved, or executed. We can do this the same way we added Internet Explorer to the

Application Blocking List. In Device Trajectory, right click on a.exe in the left column and select File Properties from the context menu.


File Info
0723932..bfe85f
Disposition: Unknown
Filename: a.exe

From the File Properties dialog, select the name of a Simple Custom Detection list and click Add.


Summary for 0723932d...1fbfe85f /

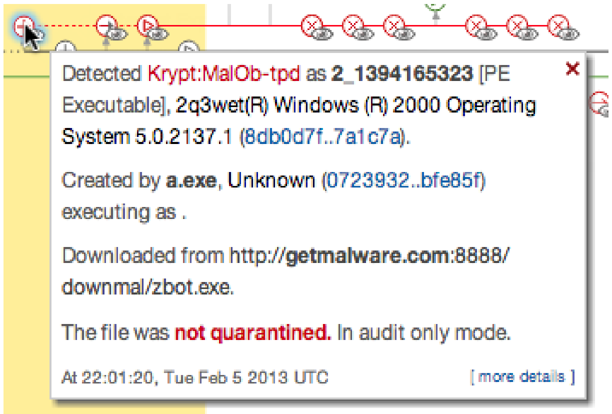
Name: a.exe
SHA: 0723932d68702a59c4c8bf6a670a098cd55c39f4a3037fa8c2e6d2641fbfe85f
Size: 10240 bytes

You can do this multiple times for each Simple Custom Detection list you want to add the file to.

IP Black Lists

The new Device Flow Control (DFC) feature of AMP for Endpoints Connector version 3.1.0 and later allows you to monitor and block network connections. You can create custom IP White and Black lists and assign them to policies wherever they're needed. In this example we have multiple threats downloading files from remote hosts. The remote access Trojan component of our demo threat could also send and receive information through a network channel in a real world scenario. DFC allows you to block both upstream and downstream connections associated with a threat.

In our scenario we can go through the Device Trajectory looking for network traffic.



Detected Krypt:MalOb-tpd as 2_1394165323 [PE Executable], 2q3wet(R) Windows (R) 2000 Operating System 5.0.2137.1 (8db0d7f..7a1c7a).

Created by a.exe, Unknown (0723932..bfe85f) executing as .

Downloaded from http://getmalware.com:8888/downmal/zbot.exe.

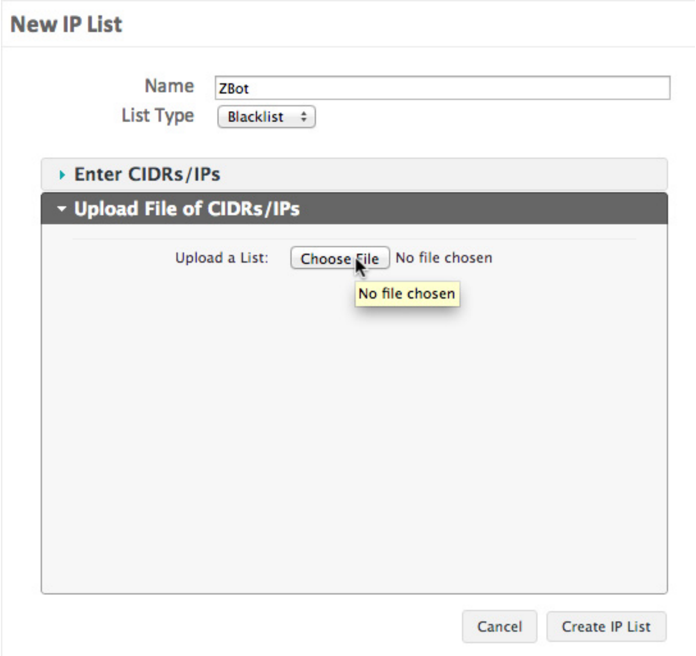
The file was not quarantined. In audit only mode.

At 22:01:20, Tue Feb 5 2013 UTC [more details]

Copy the relevant IP addresses and paste them into a text file. You can also add specific ports where necessary (eg. x.x.x.x:yy). You can also add entire CIDR blocks to your IP lists if you choose.

WARNING! Exercise caution when adding IP addresses or CIDR blocks to a black list. Malware may often be hosted on addresses also hosting legitimate websites and services.

Once you have added all the IP addresses you want to your list, go to Outbreak Control > IP Black/White Lists in the AMP for Endpoints Console. Click on Create IP List then give the list a name, select Blacklist for the List Type, and choose the Upload File of CIDRs/IPs. Click Choose File and select your text file from the dialog.



New IP List

Name: ZBot

List Type: Blacklist

Upload a List: Choose File No file chosen

Once your list has been uploaded, click Create IP List. Next, go to any policies you want to add your list to and edit them.