PlugX

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Introduction

This attack scenario replicates an "in the wild" infection of PlugX, also known as Korplug, which is a Remote Access Tool (RAT). PlugX has been detected in targeted attacks not only against military, government, and political organizations but also against regular companies. PlugX delivers three file components and exploits DLL search/load ordering. The three files are a legitimate (usually digitally signed) file, a malicious DLL that is loaded by the legitimate file, and a binary file that contains the malicious code loaded by the DLL. PlugX's capabilities include copying, creating, modifying, and opening files, logging keystrokes and active windows, logging off the current user, restarting/rebooting the affected system, creating, modifying and/or deleting registry values, capturing video or screenshots of user activity, setting connections, and terminating processes.

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.

The Attack

The attack starts when the victim visits a website exploiting a vulnerability in Internet Explorer. The exploit payload downloads and executes a PlugX variant, which uses a digitally signed McAfee executable to load and launch a malicious DLL file.

Detection and Remediation

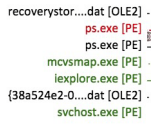
When you log in to the AMP for Endpoints Console the first page you see is the Dashboard Overview. This page shows you recent file and network detection events from your AMP for Endpoints Connectors. It's a convenient summary of the major trouble spots in your AMP for Endpoints deployment that allows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

The Indications of Compromise on the Dashboard Overview helps with triage by listing computers with multiple events or separate events that correlate with certain types of infections. In our scenario we see that the top computers with indications of compromise have experienced file detections.

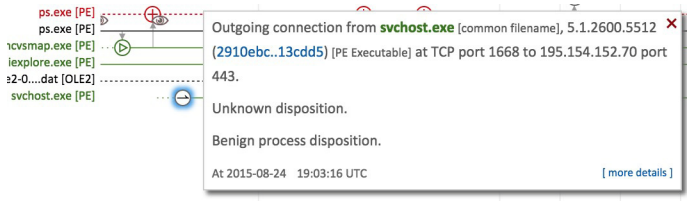
Since computers at the top of the list are considered to have more severe compromise indicators than those lower on the list, we'll start at the top. Click the information icon next to the computer name in the list and select Device Trajectory to begin the incident response process.

Tracing Backwards

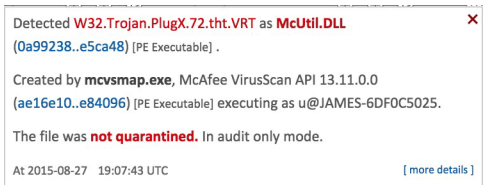
When we first look at the Device Trajectory for this computer, we immediately see obvious signs that it has been compromised since there is a red entry in the file list on the left, indicating known malware detections.



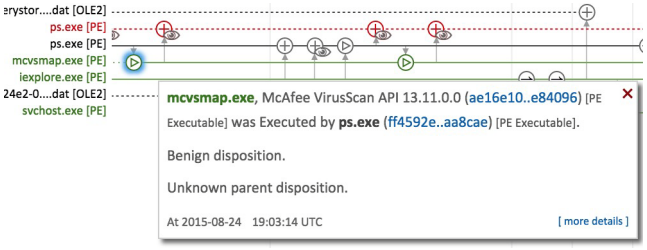
In the most recent events - those furthest to the right - we see connections being made by svchost.exe to 195.154.152.70 on port 443. This is suspicious as it is abnormal for svchost.exe to be making these kind of connections.



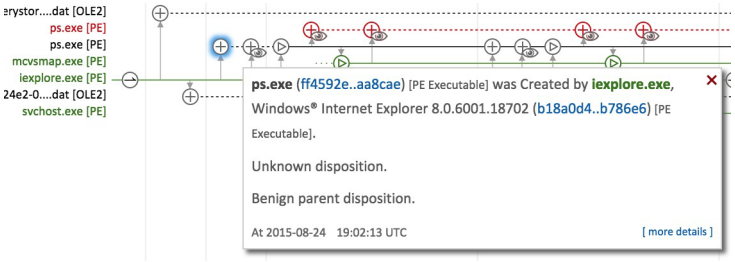
Tracing back further we see a creation event for the malicious 'McUtil.DLL' DLL file being detected as 'W32.Trojan.PlugX.72.tht.VRT' created by the clean (highlighted in green) 'mcvsmap.exe' file in the 'C:\Documents and Settings\All Users\VirusMap\' directory.



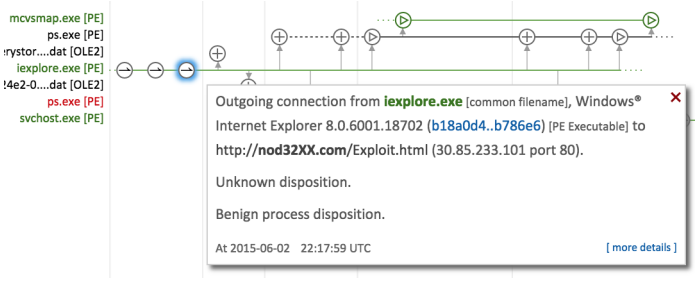
Continuing to trace back we see the execution of 'mcvsmap.exe' by an executable called 'ps.exe' that is being detected as 'W32.Trojan.PlugX.72.tht.VRT'. This is common practice for malware authors to identify and utilize legitimate signed executables that do not perform authenticity checks on DLL files being loaded, which they exploit to load their own malicious DLL files (in this instance the malicious DLL file has been identified as McUtil.DLL).



Prior to this we see that 'ps.exe' was created and executed by iexplore.exe, which is indicative that the browser was compromised providing the attacker with code execution that they used to download and execute the malicious PlugX payload.



If we continue to trace back we can find the initial point of compromise which was a visit to 'http://www.nod32XX.com/Exploit.html' using Internet Explorer.



The above demonstrates a PlugX infection via browser exploitation, in which PlugX drops a legitimate McAfee binary and a malicious DLL for it to load. Once loaded PlugX injects into svchost.exe and proceeds to contact its command and control server at '195.154.152.70'.

Remediation

In order to prevent any further malicious command and control communications, a remediation step would include the blacklisting of IP address 195.154.152.70. In order to identify any further infections of PlugX within your enterprise you can also upload the PlugXRunMethodDetected.ioc Endpoint IOC and perform a scheduled, or on-demand Endpoint IOC Flash Scan. The Endpoint IOC provided checks for the presence of a service called 'VIRUSMAP'. This is done by checking the Windows registry path 'SYSTEM\CONTROLSET001\SERVICES\VIRUSMAP' for the 'ImagePath' key. What this key specifies is the path for the service executable to be executed on start up. In the case of PlugX this is the legitimate 'VirusMap\mcvsmap.exe' executable being abused to load the malicious PlugX DLL 'McUtil.DLL'. This IOC also checks for the presence of the 'msiexec.exe' process, which is not necessarily malicious in and of itself, but this is the final process PlugX injects into upon infection.