



CozyDuke

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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](http://www.cisco.com/go/offices).



# Introduction

This attack scenario replicates an "in the wild" infection of the CozyDuke (aka CozyBear, CozyCar or "Office Monkeys") Trojan. This Trojan has been known to target high-profile organizations via spear-phishing campaigns. It delivers its payloads via compromised web servers. These initial payloads provide anti-detection routines and a vector to download the second stage that provides typical trojan functionality such as command execution interfaces, screen captures, file transfers, system information exfiltration, etc. 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.



# The Attack

The attack is an email phishing campaign that entices the user to click a link to download a ZIP archive containing a malicious executable file. Once downloaded, the file uses an Adobe Flash icon to appear benign. When the user opens the file it plays a flash movie while their machine is infected with the CozyDuke Trojan. In order to appear legitimate CozyDuke drops a signed AMD executable, which it then uses to load its own malicious DLL files on execution using [DLL search path abuse](#). These events are simple to identify within the console as will be demonstrated.

In a typical scenario these download links point to web servers that have been previously compromised by attackers that are then used as a delivery vector for their malicious files and communications.



# Detection and Remediation

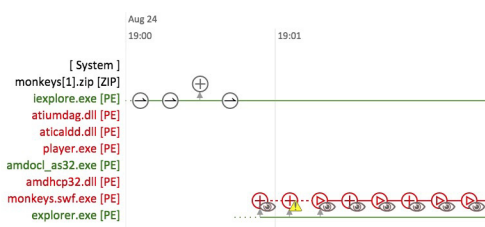
When you log in to the AMP for Endpoints Console the first page you see is the Dashboard Overview. This page shows you recent file and network detection events from your Connectors. It's a convenient summary of the major trouble spots in your AMP for Endpoints deployment that allows you to perform triage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

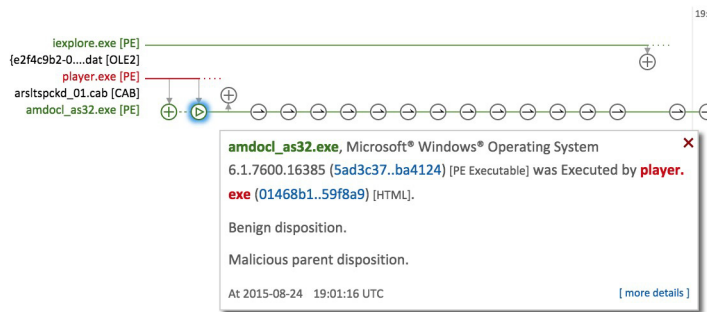
Since computers at the top of the list are considered to have more severe compromise indicators than those lower on the list, we'll start at the top. Click the information icon next to the computer name in the list and select Device Trajectory to begin the incident response process.

## 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 are five red entries in the file list on the left, indicating known malware detections.



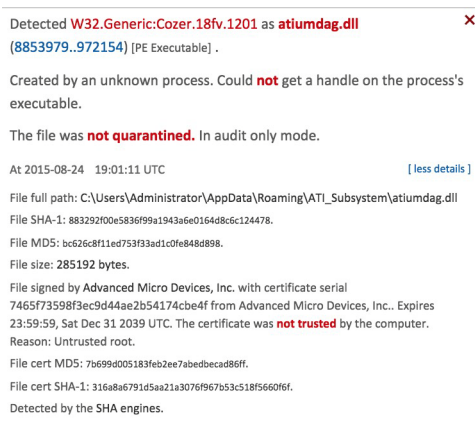
In the most recent events - those furthest to the right - we see a large number of network connections being made by a seemingly benign executable 'amdocl\_as32.exe'. Although the executable itself appears to be marked 'clean' (highlighted in green) the file is being launched by a malicious executable called 'player.exe' being detected as 'W32.Generic:CozyDukeB.18fx.1201'.



If we continue to trace back further we see three other malicious files called 'aticaldd.dll' (detected as W32.0DC7438BE5-100.SBX.VIOC.), 'amdhcp32.dll' (detected as W32.Generic.KCX.18fv.1201.), and 'atiumdag.dll' (detected as W32.Generic.Cozer.18fv.1201.) being created by 'player.exe'.

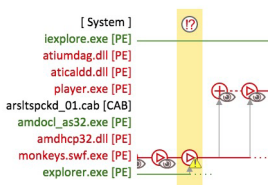


The files are suspicious in and of themselves as they are detected, however, DLLs being dropped show another malware technique. If we look at the paths of the DLL files and the dropped clean file we see they all reside within the **c:\users\administrator\appdata\roaming\ati\_subsystem\** directory.

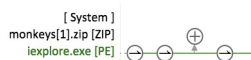


This indicates the clean file being dropped is being used by the malware authors to launch malicious DLL files. This is commonly known as "DLL search path abuse" in which the original author of the clean (typically signed) software does not check the authenticity of the shared libraries it is loading within its search path and in turn can be used to load anything (including malicious files).


If we continue to trace back further we see the initial creation and execution of our 'player.exe' file. It was created and executed by another malicious file that is called 'monkeys.swf.exe' being detected as 'W32.GenericKD:CozyDukeB.18f0.1201.'.



We also see that this file was created by 'explorer.exe' - another common and clean Windows executable. 'Explorer.exe' on Windows serves a number of purposes, including having the ability to decompress archived files. If we look further in the past we see the creation of the file 'monkeys[1].zip' by Internet Explorer. This is indicative that the file was downloaded from the Internet.



Prior to this, Internet Explorer made a connection to 'http://sanjosemaristas.com/monkeys.zip' which confirms this suspicion.

```
Outgoing connection from ieexplorer.exe [common filename], Internet   
Explorer 11.0.9600.17728 (b4e5c27..018132) [PE Executable] at 192.168.1.3  
TCP port 54141 to http://sanjosemaristas.com/monkeys.zip  
(188.120.225.17 port 80).  
  
Unknown disposition.  
  
Benign process disposition.  
  
At 2015-08-24 19:00:00 UTC \[ more details \]
```

What the above demonstrates is the attack scenario that involves a user clicking and downloading an executable within a zip file from a clicked link (in this case a spear-phishing email link), decompressing the file using 'explorer.exe', and the execution of the archived file. The further connections made by 'amdocl\_as32.exe' are also being made to the same compromised server, this is indicative of command and control communications.

## Remediation

In order to prevent any further CnC communications, a remediation step would include the blacklisting of IP address 188.120.225.17. The next step would include identifying any further infections of CozyDuke within your enterprise. In order to do this you can upload the [CozyDukePersistDetected.ioc](#) Endpoint IOC and perform a scheduled, or on-demand Endpoint IOC Flash Scan. The Endpoint IOC provided checks for Windows registry run keys that are known to be used by the CozyFuke trojan, namely 'Microsoft\Windows\CurrentVersion\Run\atibtmon\_Plugin' which contains a reference to the 'amdocl\_as32.exe' executable providing the aforementioned malicious DLL as a parameter 'atiumdag.dll'. It also verifies the presence of the 'aitumdag.dll' file on the filesystem within the 'ATI\_Subsystem' directory.