# Upatre

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.

# Introduction

This attack scenario replicates an "in the wild" infection of the Upatre trojan, which has been known to drop a number of different malware variants, including Dyre that is a banking trojan variant. Upatre is typically delivered through spam campaigns which contain malicious executables that simulate PDF files that are delievered within ZIP file attachments. Once executed, Upatre downloads and opens a PDF document to attempt to re-assure the user that what they opened was in fact a PDF document, and continues to download and execute further malware.

**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 into opening a ZIP archive attachment containing a malicious executable. Once downloaded, the file uses a PDF icon with the name "Fax" to appear benign. When the malicious file is executed an outbound HTTP connection is made to a compromised Web server to download a PNG file. This PNG file is actually an encoded decoy PDF document that is decoded by Upatre and displayed to the user. These events are simple to identify within the AMP for Endpoints console as will be demonstrated.

# Detection and Remediation

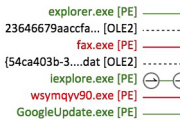
When you log in to the AMP for Endpoints Console the first page you see is the Dashboard Overview. This page shows you recent file and network detection events from your AMP for Endpoints Connectors. It's a convenient summary of the major trouble spots in your AMP for Endpoints deployment that allows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

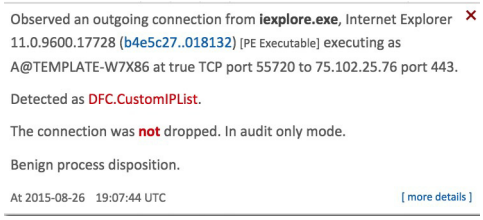
Since computers at the top of the list are considered to have more severe compromise indicators than those lower on the list, we'll start at the top. Click the information icon next to the computer name in the list and select Device Trajectory to begin the incident response process.

## Tracing Backwards

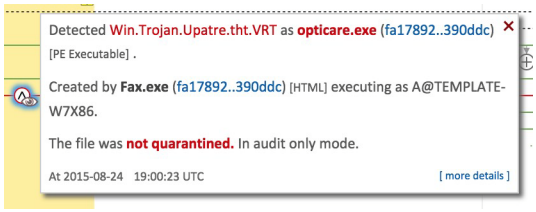
When we first look at the Device Trajectory for this computer, we immediately see obvious signs that it has been compromised since there are two red entries in the file list on the left, indicating known malware detections.




In the most recent events - those furthest to the right - we see a malicious file named wsymqyv90.exe created and executed by Internet Explorer. Prior to this we see a large number of connections being made, some of which are marked malicious by our DFC custom IP blacklist, to 75.102.25.76 on a high port 55722. This is suspicious for Internet Explorer that indicates malicious code may have been injected into the browser while running.



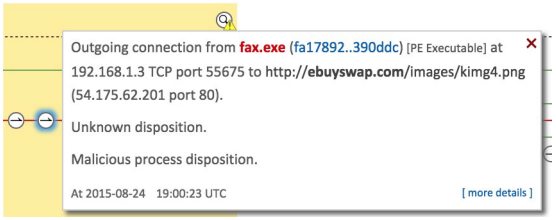

Tracing back further we see the most obvious signs that the machine has been compromised. The file fax.exe, which is detected as Win.Trojan.Upatre.tht.VRT, creates and executes a copy of itself as opticare.exe in ' C:\Users\ADMINI~1\AppData\Local\Temp\'.



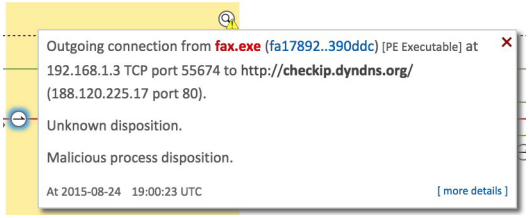
Prior to this we see 'fax.exe' executing Adobe Reader (acrord32.exe), which triggers a vulnerability detection event. This event highlights that the application 'Adobe Acrobat Reader, Version:9.3.3.177' has 54 severe vulnerabilities associated with it. This can help organizations identify vulnerable software within their enterprise that can lead to further compromises.


In this instance, the malicious executable is not executing Adobe Reader to exploit a vulnerability, rather it is using it to display a decoy document to the user.

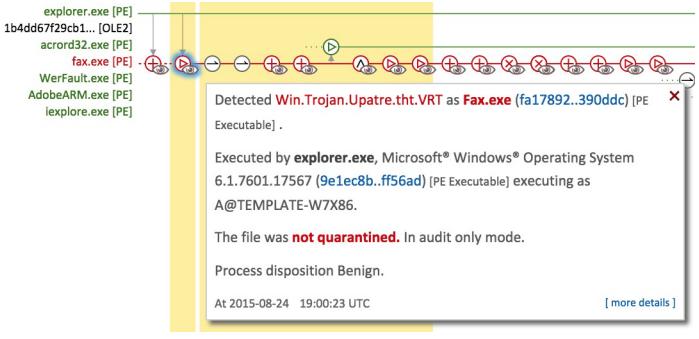
Continuing to trace back we see a connection to http://ebuyswap.com/images/kimg4.png, which turns out to be an encoded data file, that is decoded by Upatre and displayed to the user as a decoy document while they are infected.




Prior to this we see a connection to http://checkip.dyndns.org/ that is being performed to identify the external IP address of the machine being infected.




We then see the initial infection vector of the attack. First there is the creation and execution of 'fax.exe' by Explorer.exe. Explorer.exe is a common process on Windows systems that has a number of functions, one of them being the ability to decompress ZIP files. Just before the 'fax.exe' activity we see the creation of 'fax.zip' which indicates that the user saved the ZIP archive also using Explorer.exe, decompressing the malicious executable and executing it thinking that it was a legitimate Fax PDF.



What the above demonstrates is a compromise through a spear-phishing email delivering ZIP archives with a malicious executable simulating a PDF document. We then see the file make a number of command & control connections by injecting into Internet Explorer, and downloading then executing a secondary malware payload.

## Remediation

Blacklisting of remaining malicious IP address: 54.175.62.201 should suffice as the remaining files would be quarantined without auditing mode enabled.