Success stories with Cisco Amp
Context

- Sue Weier, L&S Learning Support Services (LSS)
- Amp is currently deployed on 620 machines - MacOS and Windows.
- Deployment started in March 2017 in audit mode. Audit mode is a good complement to Symantec.
- We plan to start moving administrative staff to protect mode next week.
Scenarios

- Stealthy plugin
- Macro malware
- Vulnerable software
- Absent laptop
- Adware
Stealthy plugins

- 2/24: Firewall hits escalate. Installed Amp.
- 2/28: Created a local case to have software removed.
- 3/1:
Stealthy plugins

2/15 Met with DoIT to go over the mechanics of Amp. Received account credentials and installed on test machines.

2/22 Sat in on another meeting with DoIT and a different department to hear more questions and pose some of the questions we had.

Planned on pushing out the client to some of computers the next week (2/27).
Per usual, I left my snort reports until the end of the week. When I went through them, I found some alarming data starting on 2/23.

What now?

- Whois on the destination IP
- Check Symantec logs
- Check BigFix analyses
- Logview (Qradar)
- Ask for more information from Cybersecurity
Symanetc logs

5750  2/23/2017 11:45:24 PM  Information  12130009

5751  2/23/2017 11:45:25 PM  Information  12130009

5752  2/23/2017 11:45:25 PM  Information  12130009
BigFix

- Checked Installed applications.
- Checked Services.
- Checked Programs running at startup.
- Nothing looked suspicious.
Weekend obsession

Friday - I took the machine off the network. This was not ideal for the user, but she cooperated.

Saturday - I created a firewall rule to deny outgoing traffic from that machine to the destination IP, and then put the machine back online.

Saturday night - The firewall hits escalated quickly as I watched. Daytime traffic had been about 1 ping per hour, but the traffic was much more active at night.

Deny rule: 10596

Hits on the firewall rule
At this point, I thought about Amp. So late on Sunday evening, I grabbed the installer and deployed it through BigFix.

Then I went to bed.
Amp results

No traffic marked as needing attention or malicious. Hoorah.
Device Trajectory

Start/End dates

[Graph showing device trajectory from Apr 26, 2017, 09:09 to Jun 20, 2017, 09:10]
**VirusTotal**

- **SHA256**: 5275141c08d3f1978efb150a2a966c759002f6b23a832a88eb125baddb22cd46
- **File name**: 5760ED414F35E5B4FD12522E5B2B1A1C
- **Detection ratio**: 0 / 55
- **Analysis date**: 2017-05-12 19:46:41 UTC (1 week ago)

### Antivirus Results

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>AegisLab</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>AntiLab-V3</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>Alibaba</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>ALYac</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>Arcabit</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>Avast</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>AVG</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>Avira (no cloud)</td>
<td>✔️</td>
<td>20170612</td>
</tr>
<tr>
<td>AVWare</td>
<td>✔️</td>
<td>20170612</td>
</tr>
</tbody>
</table>
Takeaways

Problem software ended up being a streaming plugin known for its malware-like behavior. It uses idle time on participating machines to process files.

Neither person knew how/when the software had been installed.

I heard back from Cybersecurity later that week, telling me that the suspicious IP number was a Zeus Tracker and that it was detected by Snort. So they didn’t have any new information, but I was able to tell them the issue was resolved.

Time savings!
Macro malware, aka fileless malware

- Macro malware started in about 1995, and it’s still around.
- Affects Windows and MacOS
- Realistic phishing emails, often from USPS or UPS.
- Staff member opens the document; macros contact server to download malware onto the computer.
- Symantec usually seems to block the outward contact, but I’d like to stop the process before then.
Macro malware, aka fileless malware

The Amp console had about a half dozen of these reports, all of which showed up at approximately the same time.
Details of file analysis include:

- Outbound HTTP GET request
- VBA Macro has action on Open
- Document File established Network Communications
- Remote IP Address Contacted
- And many more bad things.
Device Trajectory

in group A4850-LSS-Audit

[ System ]
firefox.exe [PE]
a39b492e.doc [OLE2]
winword.exe [PE]
SHA256: 90bc9b49a514874902cd4422324f1f81347ed351dd60212c3ac238f4197554
File name: USPG_Invoice_acc.virginia.doc
Detection ratio: 32 / 56
Analysis date: 2017-06-02 21:17:34 UTC (2 weeks, 3 days ago)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>VB: Trojan, Valyria, 539</td>
<td>20170602</td>
</tr>
<tr>
<td>AegeLab</td>
<td>Trojan, Script, Agantico</td>
<td>20170602</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>W97M/Downloader</td>
<td>20170602</td>
</tr>
<tr>
<td>ALYac</td>
<td>Trojan, Downloader, W97M.Gen</td>
<td>20170602</td>
</tr>
<tr>
<td>Ancabitt</td>
<td>VB: Trojan, Valyria, 539</td>
<td>20170602</td>
</tr>
<tr>
<td>Avast</td>
<td>Other: Malware-gen [Tri]</td>
<td>20170602</td>
</tr>
<tr>
<td>Avira (no cloud)</td>
<td>W97M/Dirx Agent, Iging</td>
<td>20170602</td>
</tr>
<tr>
<td>BitDefender</td>
<td>VB: Trojan, Valyria, 539</td>
<td>20170602</td>
</tr>
<tr>
<td>CAT-QuickHeal</td>
<td>W97M/Downloader, ARQ</td>
<td>20170602</td>
</tr>
<tr>
<td>Cyren</td>
<td>Downloader, XZSC</td>
<td>20170602</td>
</tr>
<tr>
<td>DrWeb</td>
<td>W97M/Hancitor, 1</td>
<td>20170602</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>VB: Trojan, Valyria, 539 (B)</td>
<td>20170602</td>
</tr>
</tbody>
</table>
Takeaways

I know what happened. :-)  
Easy cleanup.  
Time savings.
Vulnerable applications
The machine had been off for an extended period of time, causing it to become out of date.

In BigFix, I checked to see if the machine had processed the current Adobe patches. In this case, I had to apply past Adobe patches to catch the machine up with current levels.

Secunia has better scope, but Amp sends alerts.
We would never have known...
Absent laptop

Laptop was at a 192.168 IP number. We thought it was on a switch in the office where it was last inventoried.

- Laptop was actually on another continent, being used for research in the field.
- My desktop support people figured that the machine needed to check in to re-activate Windows.
- VPN was not installed on the machine.
- RA didn’t speak English and is not tech-savvy.
- No easy phone or network access.
Takeaways

At least we know where it is.

Professor ended up paying to have the machine cleaned and re-installed.

Laptop coming back after summer, and will be brought back to us.
Ad-ware

### Event Log

<table>
<thead>
<tr>
<th>Event Type</th>
<th>File Path</th>
<th>Time Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20bjk.1201</td>
<td>2017-02-02 10:59:25 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20dfz.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>W32.Adware.20wzr.1201</td>
<td>2017-02-02 10:58:29 CST</td>
</tr>
</tbody>
</table>

**Total Events:** 1031
Takeaways

At least we know the software is installed.

It’s easy to call it malware after you see how this, and it’s easy to convince users that it shouldn’t be there.

We can catch new malware installations immediately and remove them via BigFix.

In Protect mode, none of this will happen.