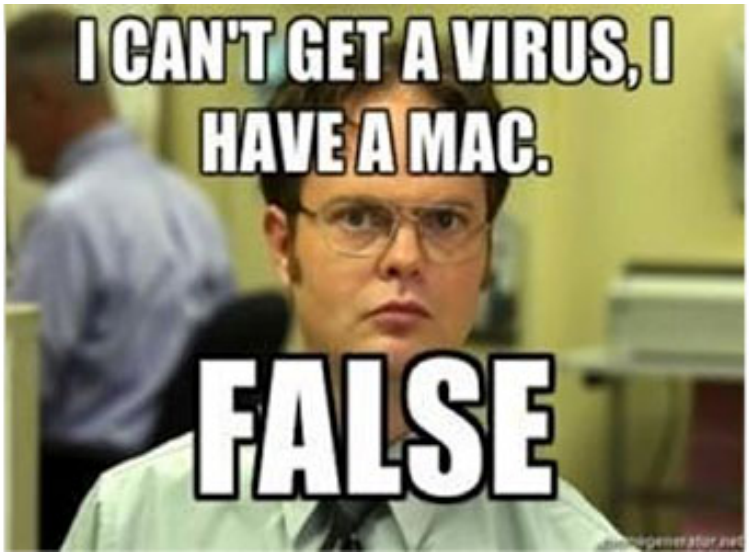
19 NOV



WireLurker: How to 'Flag It, Tag It and Bag It'

November 19, 2014 / Ryan Nolette / Advanced Threat Protection, Detection and Response, Endpoint and Server Security, Tech Toolbox

WireLurker, a recently discovered malware combination that infects OS X computers, has been all the rage in the news. WireLurker earned its name because it spreads from an infected OS X computer to an iOS device once the IOS device is connected via USB.

Recently, my colleague Berni McCoy published a blog on the basics of WireLurker and how to avoid getting infected. Since Bit9 + Carbon Black supports Windows, OS X (Mac), and Linux, we can leverage both tools to detect and protect against WireLurker.

I am going to show you how to create Carbon Black watchlists to monitor your entire enterprise for these threats. Then I will describe how to turn these watchlists into Bit9 block rules to proactively protect your organization from them.

Recon, research, repeat: gathering data for your watchlist

I am going to skip ahead here and assume you read the WireLurker report, the detector scripts, a few more blogs on the malware, and have a decent understanding of it.

From this research, you should have generated a list of known artifacts about the malware (indicators).

My list is as follows:

Known malicious files:

- Taken from detector script:

```
MALICIOUS_FILES =
[
        '/Users/Shared/run.sh',
        '/Library/LaunchDaemons/com.apple.machook_damon.plist',
        '/Library/LaunchDaemons/com.apple.globalupdate.plist',
        '/usr/bin/globalupdate/usr/local/machook/',
        '/usr/bin/WatchProc',
        '/usr/bin/itunesupdate',
        '/Library/LaunchDaemons/com.apple.watchproc.plist',
        '/Library/LaunchDaemons/com.apple.itunesupdate.plist',
        '/System/Library/LaunchDaemons/com.apple.appstore.plughelper.plist',
        '/System/Library/LaunchDaemons/com.apple.MailServiceAgentHelper.plist',
        '/System/Library/LaunchDaemons/com.apple.systemkeychain-helper.plist',
        '/System/Library/LaunchDaemons/com.apple.periodic-dd-mm-yy.plist',
        '/usr/bin/com.apple.MailServiceAgentHelper',
        '/usr/bin/com.apple.appstore.PluginHelper',
        '/usr/bin/periodicdate',
        '/usr/bin/systemkeychain-helper',
        '/usr/bin/stty5.11.pl',
]
SUSPICIOUS_FILES =
[
        '/etc/manpath.d/',
        '/usr/local/ipcc/'
]
```

- Found through various blogs and forums:
- The first step WireLurker takes is to append an underscore to the original bundle executable name, then copy its malicious loader into the bundle to replace the original executable.
- Next, WireLurker then adds a shell script, "start.sh", and a ZIP archive, "FontMap1.cfg", to the "Contents/Resources" folder of the bundle.
  - To me, that means that we should look inside all subdirectories in /applications for start.sh and Fontmap1.cfg.
- The "hidden" flag is then set for these files. This flag is an Apple-specified file property defined at "/usr/include/sys/stat.h" as "UF_HIDDEN." With this flag set, a standard user won't see the files in the Finder, but can still view them through the Terminal.
- Look for change flag on files in /Applications.
  - This idea came from one of the scripts that the malware drops

```
#!/bin/sh
/bin/cp -rf '%@' '%@2'
/bin/cp -rf '%@_' '%@' && /usr/bin/open -a '%@'
sleep 5
/bin/cp -rf '%@2' '%@'
rm -rf '%@2'
chflags hidden '%@'
chflags hidden '%@_'
rm -f /Users/Shared/run.sh
```

- The loader first drops an embedded script file to "/Users/Shared/run.sh".
- Known network traffic
  - com\mac\update.zip
  - *\mac\getsoft.php

Now, your list may be different than mine. That's OK. The biggest perk of the watchlists, in my opinion, is their flexibility and ease of updating/adapting to incorporate new information. Basically, the more you learn, the more the feed can be refined for efficiency and effectiveness in your environment.

Breaking your findings down into watchlists

Now that we have all of this information, we need to break it down in different ways. I suggest one of two ways:

- File system artifacts, registry artifacts, memory artifacts, and network artifacts
- High confidence, medium confidence, low confidence

Both of these approaches have their pros and cons and should be chosen based on your findings and your confidence in those finding to not produce false positives.

Creating the watchlists

I chose to go with the three-tiered confidence method. I chose this approach because of my confidence in the data gathered. I think a few of these rules could produce false positive events in my environment and because of that, I have chosen the approach that allows me to separate these possible problem rules to unique watchlists. This approach will allow me to disable any noisy watchlists without turning everything off and keep my environment quiet, secure and functional.

Watchlist 1: High Confidence

- This Watchlist will contain:
  - All file paths take from the detector script
  - All registry values
  - All other static values I can find

Watchlist 2: Medium Confidence

- This Watchlist will contain:
  - Network traffic
  - Other traffic that could have potential false positive events

Watchlist 3: Low Confidence

- This Watchlist will contain:
  - Any items that will most likely produce false positives

Example Carbon Black Watchlists:

(NOTE: Not all indicators from above are used in these examples. These are simply a few examples of what you would use in Carbon Black for detecting WireLurker or a similar malware using the information you gathered online.)

Watchlist 1:

This watchlist contains all of the file artifacts I gathered. These are all indicators that if I see them, I know they are not false positives and that I should immediately take action. I have high confidence in these indicators and am treating them as such.

- filemod:Users/Shared/run.sh OR filemod:Library/LaunchDaemons/com.apple.machook_damon.plist OR filemod:Library/LaunchDaemons/com.apple.globalupdate.plist OR filemod:usr/bin/globalupdate/usr/local/machook/ OR filemod:usr/bin/WatchProc OR filemod:usr/bin/itunesupdate OR filemod:Library/LaunchDaemons/com.apple.watchproc.plist OR filemod:Library/LaunchDaemons/com.apple.itunesupdate.plist OR filemod:System/Library/LaunchDaemons/com.apple.appstore.plughelper.plist OR filemod:System/Library/LaunchDaemons/com.apple.MailServiceAgentHelper.plist OR filemod:System/Library/LaunchDaemons/com.apple.systemkeychain-helper.plist OR filemod:System/Library/LaunchDaemons/com.apple.periodic-dd-mm-yy.plist OR filemod:usr/bin/com.apple.MailServiceAgentHelper OR filemod:usr/bin/com.apple.appstore.PluginHelper OR filemod:usr/bin/periodicdate OR filemod:usr/bin/systemkeychain-helper OR filemod:usr/bin/stty5.11.pl OR filemod:etc/manpath.d/ OR filemod:usr/local/ipcc/

Watchlist 2:

This watchlist is looking for the known domain that WireLurker connects to. Currently, there is only one known domain. This is uncommon for malware these days but not unheard of. This watchlist is kept uniquely to network traffic only to cut down on editing later on. I have high confidence in this domain being malicious. However, domains change quickly, and I do not expect this watchlist to always give me a true positive result, nor do I expect it to be around for a long time.

Therefore, I keep it separate and can easily disable it when I deem it no longer useful.

- domain: comeinbaby.com

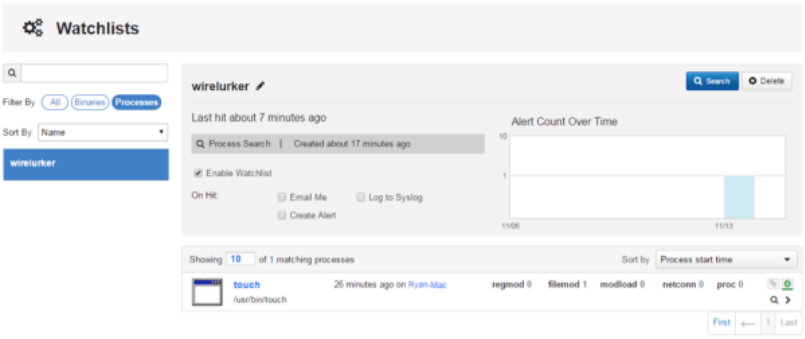
Watchlist 3:

This watchlist contains my low-confidence queries. These queries will contain false positives and I know that going into this. The reason they will fire false positives is because of how broad they are. I have high confidence that anything under "/Applications/*/start.sh" will not be legitimate but I have not tested every software ever in every environment, so I leave room for false positives.

- filemod:Applications/*/start.sh

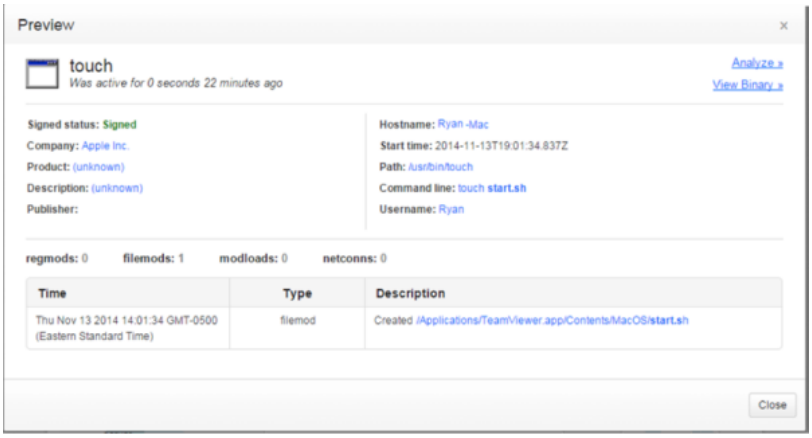
Also, the command for chflags to hidden is not an uncommon command. It is usually not used legitimately because it hides things from finder but not from command line.

- cmdline:"/usr/bin/chflags -v hidden"



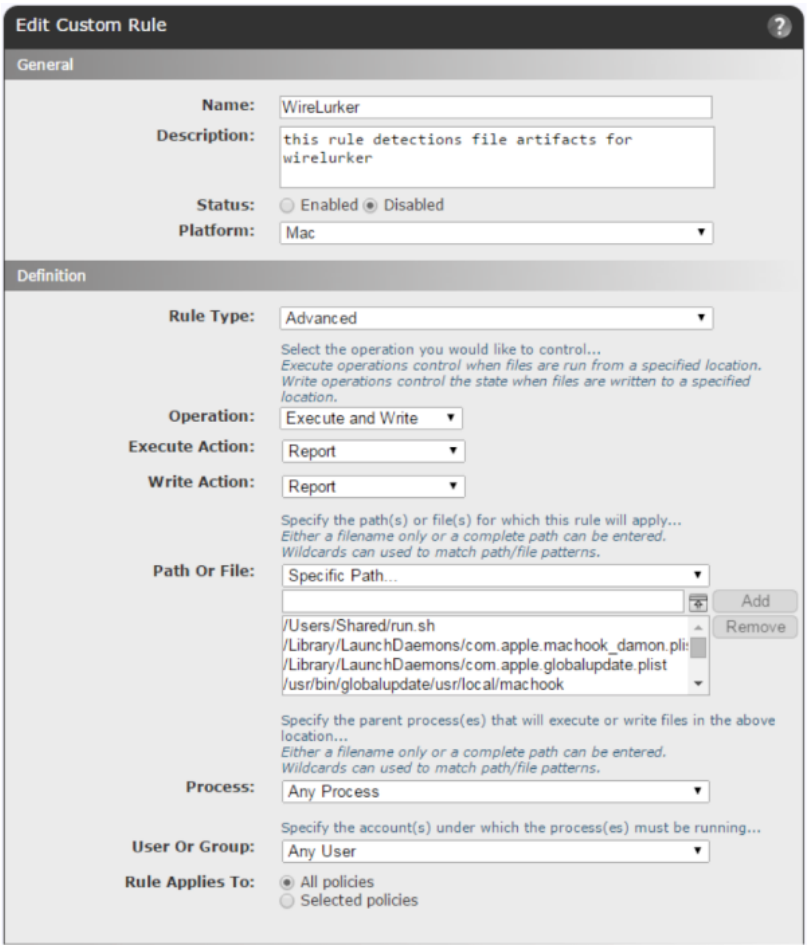
Above you can see an example of the watchlist I created for "filemod:Applications/*/start.sh." As you can see, when I set off the watchlist with the creation of start.sh in the file path of "/Applications/TeamViewer.app/Contents/MacOS/start.sh."

Below, you can see the drill down of the command the script used to create this file (it used the touch command).



Example Bit9 block rules:

We all want to proactively blog threats like. Below is a screen shot of the creation of a block rule in Bit9 that will not allow these files to run if they are found. The alternative to this is to keep your endpoints in high enforcement and you will not have to create custom block rules because this malware will not be allowed to run on a Bit9 protected host.



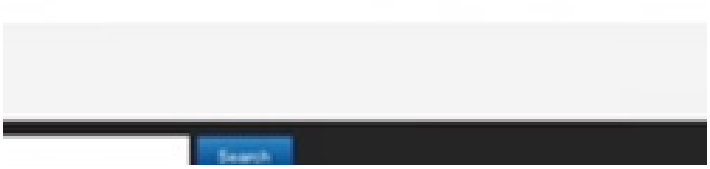
Conclusion

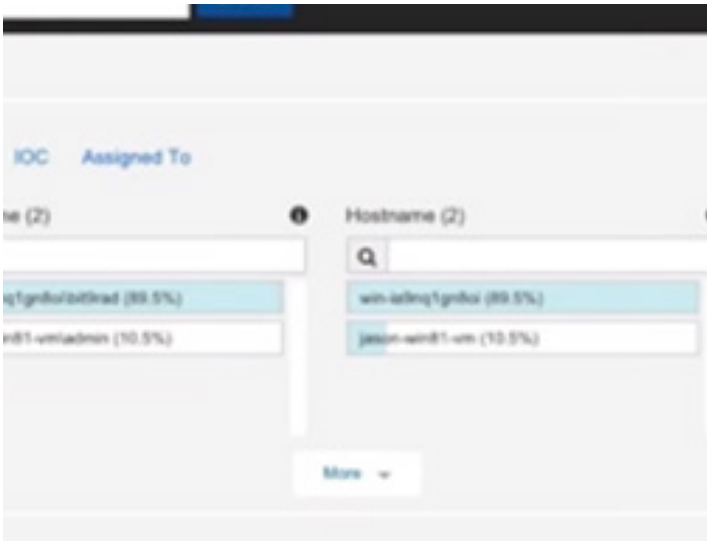
Using these types of techniques, you can find enough information online about pretty much any common threat/malware and create a watchlist for detection and a block rule for protection. In this post I used WireLurker as an example, but it could have easily been replaced with Zeus, CryptoLocker, or whatever is currently threatening your environment.

Until next time, remember my motto. Flag it, Tag it, and Bag it.

Tags: advanced threat protection | All Posts | Detection and Response | endpoint and server security

More Posts





October 8, 2015 / *by Editorial Staff*

Extending Infoblox DNS Threat Intelligence for Endpoint Remediation

(Editor's Note: This post originally appeared on infoblox.com.) Today, I am delighted to have a chance to speak about a topic that's really interesting to me – how Infoblox plays into a security ecosystem. Traditionally, Infoblox is thought of as a DNS, DHCP and IP Address Management, It's also been thought of as a DDI…

February 10, 2016 / *by Ryan Murphy*

February 10, 2016 – Morning Cyber Coffee Headlines – Bob Dylan

Good morning! Sit with Carbon Black this morning over a cup of coffee (or tea) and browse a few industry headlines to get the day started. We've got just enough information below to get you through that first cup…enjoy! February 10, 2016 – Headlines What's the real cost of a security breach? – Help Net…

March 25, 2016 / *by Ryan Murphy*

March 25, 2016 – Morning Cyber Coffee Headlines – Easter Edition

Good morning! Sit with Carbon Black this morning over a cup of coffee (or tea) and browse a few industry headlines to get the day started. We've got just enough information below to get you through that first cup…enjoy! March 25, 2016 – Headlines Carbon Black in the News: FBI iPhone backdoor case on hold as…

June 3, 2015 / *by Editorial Staff*

Decoupling Network from Endpoint Security

(Editor's note: This blog appears as part of the eBook, "Should You Buy Endpoint Security from a Network Security Vendor?" available here.) By Richard Stiennon, Chief Research Analyst, IT-Harvest Decoupling, an engineering term used to describe breaking a problem into its component parts, is a useful concept for IT security. In mechanical engineering it means…

Subscribe

ENTER YOUR EMAIL ADDRESS

PREFERENCES

- Blog Posts
- Morning Coffee
- Community Perspectives
- Tech Toolbox

SUBSCRIBE

Categories

Advanced Threat Protection (184)

Community Perspectives (125)

Compliance (15)

Detection and Response (161)

Endpoint and Server Security (160)

Featured (1)

Mobile Security (4)

Morning Coffee (113)

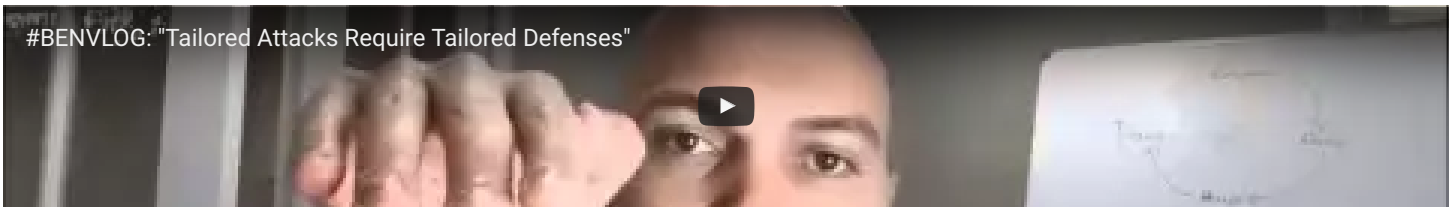
Prevention (91)

Response (115)

Tech Toolbox (82)

Uncategorized (2)

BenVlog: Tailored Attacks Require Tailored Defenses



Authors

Adam Koblentz | Alex Baker | Ben Johnson | Ben Tedesco | Berni McCoy | Threat Intel Team | Editorial Staff | Brent Midwood | Bruce Van Dyke | Chris Berninger | Chris Lord | Christopher Strand | Dave Brown | David Dorsey | Eric O' Neill

Tags

Ben Johnson | bit9 | Carbon Black | detection | endpoint security | incident response | malware | morning coffee | security | security headlines

Carbon Black on Twitter

Lunchtime Listen: @chicagoben on @FedNewsRadio discussing threat intelligence and securing endpoints https://t.co/NStTgTLAxL #infosec #DFIR
2 hours ago

Had a blast at the @splunk event in Seoul yesterday! #cybersecurity https://t.co/DeRg2BYuYR
2 hours ago

We're hiring a versatile #UX #Designer! Apply here: https://t.co/dz42tR14nB https://t.co/GbnKjI7VjH
2 hours ago

Join fellow #security pros in #London on July 6th! Learn how to transform your #SOC https://t.co/tW1wxOWH2i https://t.co/xT0U8IsiBY
2 hours ago

Happy Tues., morning coffee readers! Here are today's Carbon Black #infosec headlines - https://t.co/LPWCLDlZdF
3 hours ago

Archives

2016

2015

2014

2013