Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

2015: THE MOST PROLIFIC YEAR IN HISTORY FOR OS X MALWARE

After a 10-week analysis, the Bit9 + Carbon Black Threat Research team found that five times more OS X malware appeared in 2015 than during the previous five years combined.

Threat Research Briefing

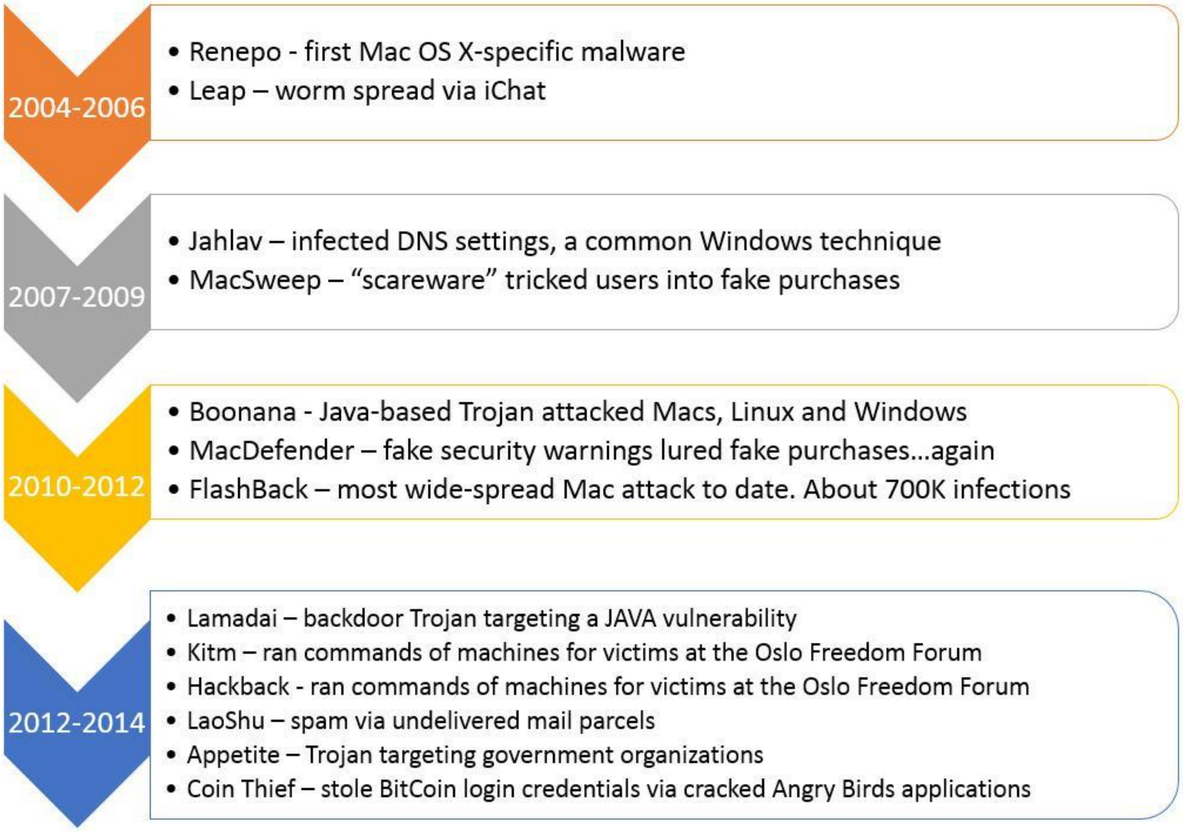
It’s been long believed that Macs have faced significantly less risk of cyber attack than PCs and, until recently, that sentiment has been largely correct. Mac users have been mostly immune from malware relative to their Windows-user counterparts. However, it appears that tide is turning.

This rise in Mac OS X malware comes after several years of rapid OS X market share gains, with 16.4 percent of the market now running OS X[1], including expanding deployment in the enterprise. This represents a growing attack surface for sensitive data, as 45 percent of companies now offer Macs as an option to their employees. [2]

In 2015 we have seen interesting OS X vulnerabilities and malware that have grabbed the security community's attention. One example is XcodeGhost, which inserts malicious components into applications made with Xcode (Apple's official tool for developing IOS and OS Apps). Additionally, it was recently revealed that OS X El Capitan, which launched in September, contains serious vulnerabilities in its Gatekeeper and Keychain features.

Evidence of a more malicious OS X marketplace is clearly compounding. A timeline charting Mac OS X malware prevalence in the market shows a clear upward tick:

[1] http://www.computerworld.com/article/2948474/mac-os-x/as-apple-desktop-use-grows-it-adapts.html
[2] http://appleinsider.com/articles/14/03/25/45-of-business-offers-macs-to-employees-77-find-apple-more-reliable---survey



2004-2006

- Renepo - first Mac OS X-specific malware
- Leap – worm spread via iChat

2007-2009

- Jahlav – infected DNS settings, a common Windows technique
- MacSweep – “scareware” tricked users into fake purchases

2010-2012

- Boonana - Java-based Trojan attacked Macs, Linux and Windows
- MacDefender – fake security warnings lured fake purchases…again
- FlashBack – most wide-spread Mac attack to date. About 700K infections

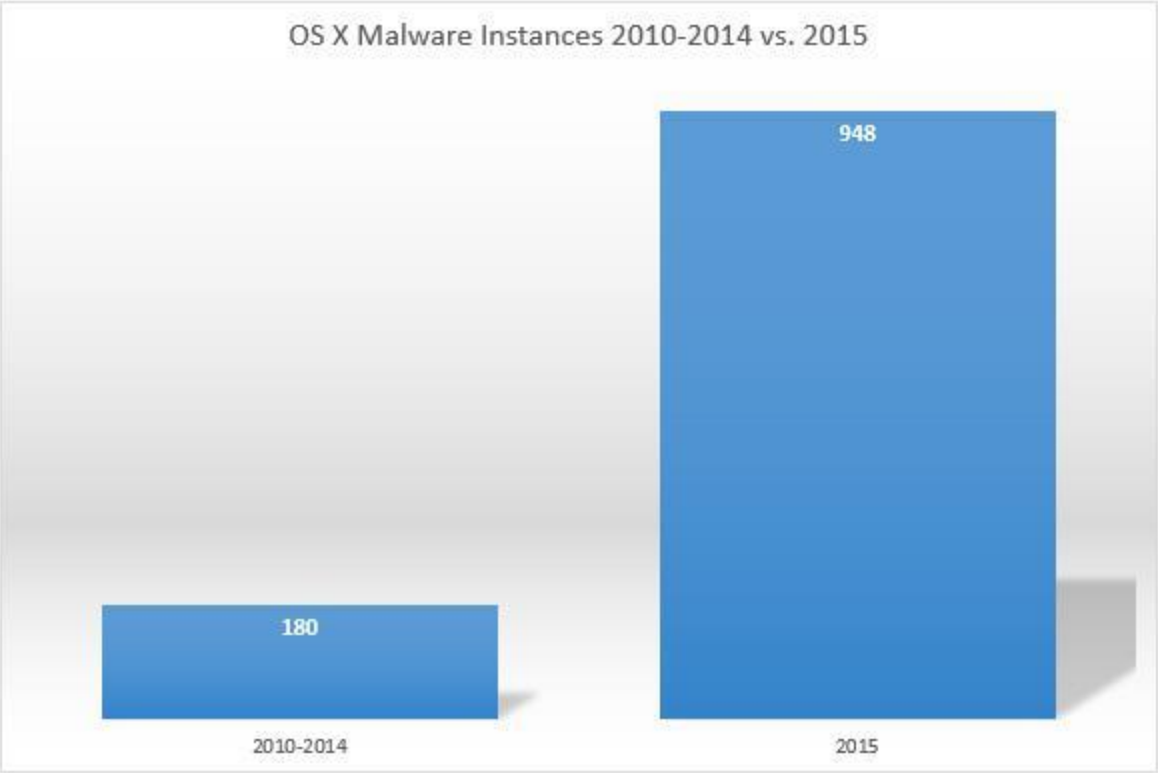
2012-2014

- Lamadai – backdoor Trojan targeting a JAVA vulnerability
- Kitm – ran commands of machines for victims at the Oslo Freedom Forum
- Hackback - ran commands of machines for victims at the Oslo Freedom Forum
- LaoShu – spam via undelivered mail parcels
- Appetite – Trojan targeting government organizations
- Coin Thief – stole BitCoin login credentials via cracked Angry Birds applications

A 10-week analysis conducted by the Bit9 + Carbon Black Research Team validates the unprecedented growth in OS X malware. With an extensive global reach and a pulse on the expanding threat landscape, the Bit9 + Carbon Black team collected more than 1,400 unique OS X malware samples. Samples were aggregated from the team’s independent research efforts, open sources, experience from incident response engagements involving OS X, peer research, black lists, and contagio malware dump, among other sources.

As big-picture trends from the data began to emerge, one data point struck the team as particularly noteworthy: 2015 has been the most prolific year in history for OS X malware.

In 2015 alone, the research found, the number of OS X malware samples has been five times greater than in 2010, 2011, 2012, 2013 and 2014 combined.



The sample size in this analysis is significant enough for even the most optimistic Mac user to realize that OS X security must now be a paramount concern.

Based on the observations in the 10-week analysis, the Bit9 + Carbon Black Threat Research Team confidently expects Mac OS X malware attacks to accelerate in the coming months. As Apple continues its growth in both the consumer and enterprise markets, its platforms have become a prime target for attackers.

Security professionals, consumers and enterprise users alike should read the results of this latest analysis as a clarion call for a more comprehensive approach to enterprise security—one that encompasses the right people, processes and technology that can handle advanced threats against Mac OS X and other Apple devices.

"The Bit9 + Carbon Black Threat Research Team confidently expects Mac OS X malware attacks to accelerate in the coming months."

Observed Malware Behavior

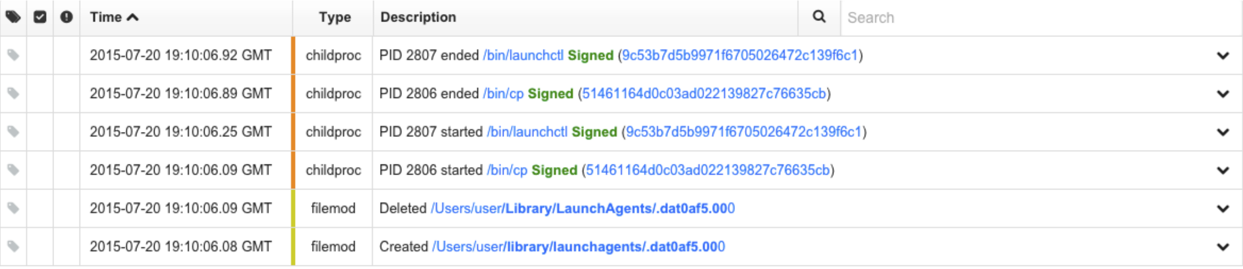
The OS X malware analyzed consisted of more than 1,400 unique samples taken from the Bit9 + Carbon Black Threat Research Team's research engagements, open sources, and from incident response engagements involving OS X, peer research, black lists, and contagio malware dump.

When looking at OS X malware, research teams cannot utilize common Windows malware analysis tools, such as process monitor. To compensate for this in their OS X research, the Bit9 + Carbon Black Threat Research Team utilized various custom and prebuilt tools, such as fs_usage, dtrace, and opensnoop to instrument machines for dynamic analysis, in addition to the custom-built Carbon Black sandbox.

By utilizing the custom-built sandbox, the research team was able to quickly identify common actions performed by malware, such as file creations and network communications. This enabled the team to look at command-and-control infrastructure as well as artifacts left as part of the malware execution.

UNIX Persistence Mechanisms Not Seen

In an interesting twist, typical UNIX persistence mechanisms were not frequently seen in the OS X malware analyzed. For example, the team's analysis found that mechanisms such as adding cron jobs and "trojaning" startup locations such as rc.common weren't typically used; instead, malware authors are choosing to use Mac OS X-specific mechanisms.



Time ^	Type	Description
2015-07-20 19:10:06.92 GMT	childproc	PID 2807 ended /bin/launchctl **Signed** (9c53b7d5b9971f6705026472c139f6c1)
2015-07-20 19:10:06.89 GMT	childproc	PID 2806 ended /bin/cp **Signed** (51461164d0c03ad022139827c76635cb)
2015-07-20 19:10:06.25 GMT	childproc	PID 2807 started /bin/launchctl **Signed** (9c53b7d5b9971f6705026472c139f6c1)
2015-07-20 19:10:06.09 GMT	childproc	PID 2806 started /bin/cp **Signed** (51461164d0c03ad022139827c76635cb)
2015-07-20 19:10:06.09 GMT	filemod	Deleted /Users/user/**Library/LaunchAgents/.dat0af5.000**
2015-07-20 19:10:06.08 GMT	filemod	Created /Users/user/**library/launchagents/.dat0af5.000**

During analysis, the team found that most OS X malware would utilize features of the OS such as LaunchDaemons/LaunchAgents, login items and browser plugins. Malware more often resided in user-land and leveraged persistence mechanisms that supported this as opposed to attempting to reside in kernel-land by writing custom kernel extensions.

In another twist, it was the team's expectation that, given OS X's roots in FreeBSD, adapting Unix/Linux malware would be common. However, based on this 10-week analysis, there does not appear to be much, if any, Unix-style malware brought over to OS X.

Additionally, Apple introduced a new load command (LC_MAIN) to define the entry point into the Mach-O format with the release of OS X 10.8 in 2012. The previous load commands were LC_THREAD and LC_UNIXTHREAD. More than 90 percent of the OS X malware we analyzed from 2015 still uses the old load command entry point method. In analyzing samples from 2010 through 2015, the research team did not start seeing the new method being used until 2014 and, even then, it was a tiny percentage. This trend leads to a statistical indicator from the research that malware currently uses the old load command much more than the new load command. Consequently, if a Mach-O file found on a modern

Mac system uses the old load command, it's more likely to be malware than a Mach-O file using the new load command.

> "Malware authors are not updating their malware to conform to the latest specifications by Apple."

Increased Malware Prevalence, Less Sophistication

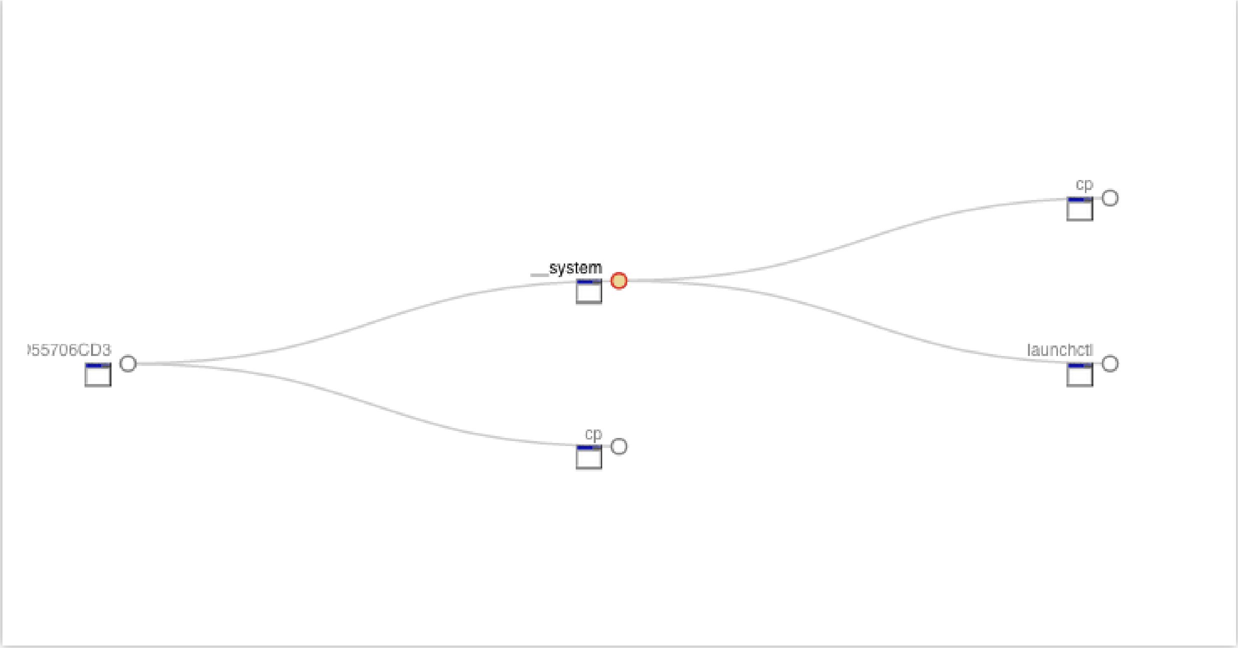
Based on Bit9 + Carbon Black's analysis, there are strong signs that suggest malware authors are seizing the opportunity to strike on the OS X platform. The result of this transition is an increased prevalence of OS X malware, even if it is not particularly sophisticated.

As the team noted during its analysis, OS X malware authors aren't utilizing the Unix philosophy combining "small, sharp tools" to achieve the desired results. The malware authors seem to have a more "Windows-malware" (i.e. - monolithic) approach to how the malware behaves versus a composability approach, which would take advantage of existing legitimate Unix specific OS operations as part of their design.

7 Distinct Persistence Techniques Seen

True to form, most OS X malware leverages a persistence technique in order to remain on the targeted system. While 13 documented persistence techniques have been identified, the Bit9 + Carbon Black Threat Research team identified that the vast majority of OS X malware leveraged one of just seven persistence techniques to remain active on a system.

1) **LaunchAgents –** An OS X-provided way to start programs on a per-user or system-wide basis



2) **LaunchDaemons** – An OS X-provided way to start programs on a per-user or system-wide basis, used interchangeably with LaunchAgents
3) **Cron job** – Cron is a time-based job scheduler in Unix-like computer operating systems. Cron jobs are used to run scripts/programs periodically at fixed times, dates or intervals.
4) **Login items** – The method to cause programs to run when a user logs in to an OS X account.
5) **Browser plugins** – Code that runs in the context of a Web browser. They are known for adding additional functionality to browsers.
6) **StartupItems** – Programs to run upon system startup.
7) **Binary infection** – When one executable modifies another so when the original executable is run control is passed to the malicious code prior to the original code being executed.

While the Threat Research Team identified other categories that could be leveraged to gain persistence, no malware in the wild has yet been seen or adapted to leverage them. This lack of OS X malware biodiversity currently makes finding persistent malware infections easier than on Windows systems as there are fewer places than need to be checked.

To aid those wishing to check their infection status, we have collected and outlined several detection mechanisms both enterprise security teams and individual consumers can use to gain better visibility across the expanding OS X attack surface.

Detection Mechanisms / Actions to Take for Enterprises

1 - Since OS X has until recently been largely ignored by malware and only rarely the target of advanced cyber attacks, many enterprises have failed to implement the same safeguards and controls on OS X devices as they have for Windows machines. As OS X malware and targeted attacks have increased, this security gap has left many organizations exposed and unable to identify or stop infections. This reality has been compounded by the lack of OS X support from many endpoint security vendors and is a strategic vulnerability for organizations with large OS X deployments.

If your organization is currently running OS X, it may mean that attackers are actively exploiting and targeting your systems. Most infections our sensors see are of the adware variety, however, we have noticed an increase in more sophisticated malware. This risk can be managed and monitored by deploying an enterprise-class, scalable endpoint threat detection and response solution, such as Carbon Black.

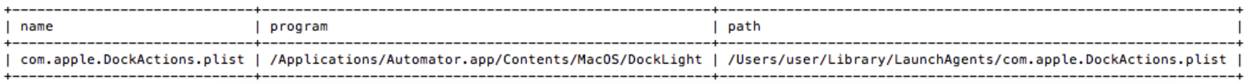
On OS X devices, the Carbon Black agent continually records all process executions, file and system modifications, and attempted and established network connections. It analyzes this data against the latest threat intelligence and behavioral indicators to detect malicious activity. This information is centrally recorded and stored to provide enterprises with a single view from which current and historical infection status, number of devices infected, and impact can be investigated and confirmed within seconds. High-risk organizations or systems can gain additional protection by using an application control solution, such as the Bit9 Security Platform, which will control the execution of untrusted or arbitrary code to dramatically reduce the risk of malware infection and halt the malware’s ability to execute in the first place.

2 - osquery is a more comprehensive and enterprise-grade opensource tool maintained by Facebook (https://osquery.io/). Using osquery you can conduct some monitoring and analysis based upon the following queries.

For looking at LaunchDaemon, LaunchAgent, startup items, and login malware you can utilize the following queries:

- select name,program,path FROM launchd;
- select name,program,path FROM launchd where username = ‘root’;
- select name,linked_against,path from kernel_extensions;
- select name,path,type,source from from startup_items;
- select * from preferences where domain = ‘loginwindow’;
- select * from preferences where domain = ‘loginitems’;
- select * from crontab

The picture below is an example of a system infected with the Olyx backdoor that can be seen in the osquery of “select name,program,path FROM launchd”



```
+-----------------------------+------------------------------------------------------+--------------------------------------------------------------+
| name                        | program                                              | path                                                         |
+-----------------------------+------------------------------------------------------+--------------------------------------------------------------+
| com.apple.DockActions.plist | /Applications/Automator.app/Contents/MacOS/DockLight | /Users/user/Library/LaunchAgents/com.apple.DockActions.plist |
+-----------------------------+------------------------------------------------------+--------------------------------------------------------------+
```

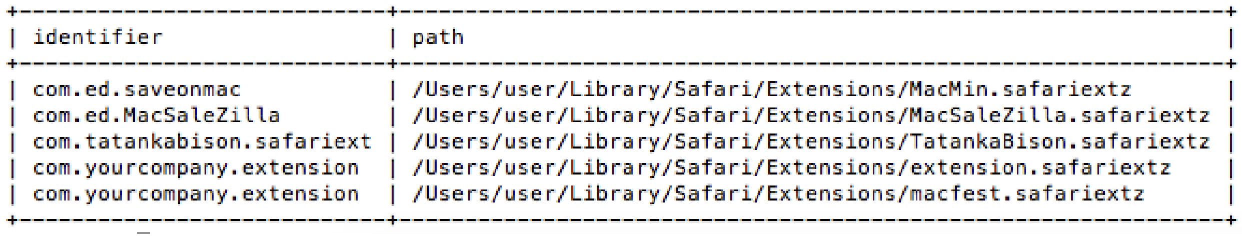
A fair amount of OS X malware also interfaces with the launchd, and to do that they execute the launchctl command to load/unload daemons and agents. Watching for this type of activity is useful as well. To do this with osquery the queries would be:

- select * from shell_history where command = “launchctl”;
- select * from shell_history where command = “/bin/launchctl”;

A majority of the adware would install its own browser extensions. To look at browser extensions you can utilize the following osqueries:

- select identifier,path from safari_extensions; (mostly adware malware)
- select identifier,path from chrome_extensions; (mostly adware malware)

The picture below is an example of a system infected by various pieces of adware



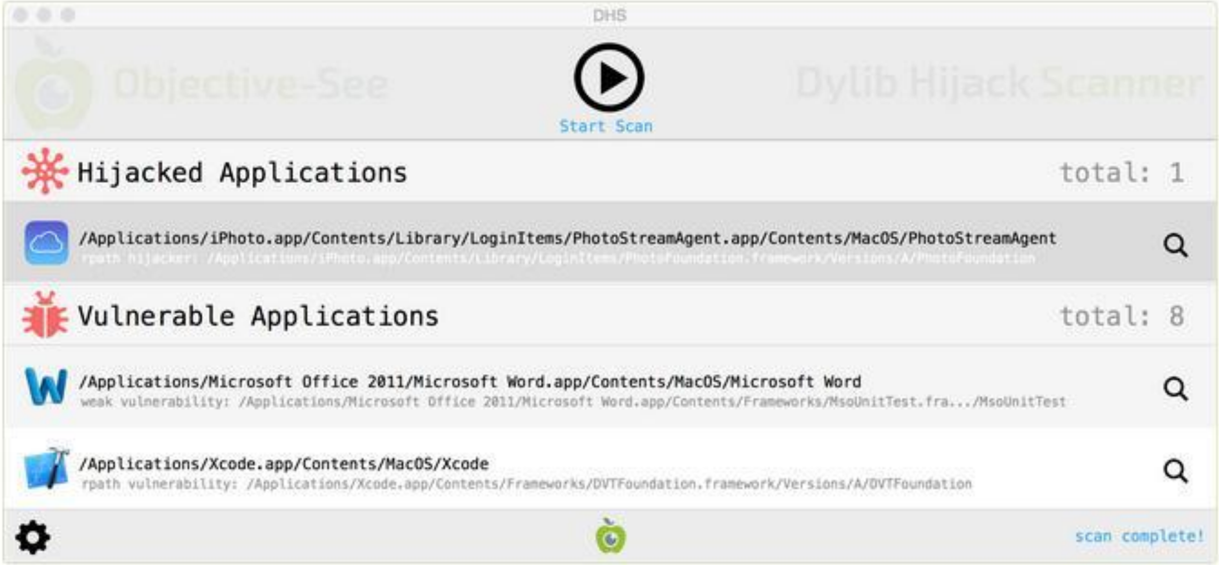
```
+----------------------------+---------------------------------------------------------------+
| identifier                 | path                                                          |
+----------------------------+---------------------------------------------------------------+
| com.ed.saveonmac           | /Users/user/Library/Safari/Extensions/MacMin.safariextz       |
| com.ed.MacSaleZilla        | /Users/user/Library/Safari/Extensions/MacSaleZilla.safariextz |
| com.tatankabison.safariext | /Users/user/Library/Safari/Extensions/TatankaBison.safariextz |
| com.yourcompany.extension  | /Users/user/Library/Safari/Extensions/extension.safariextz    |
| com.yourcompany.extension  | /Users/user/Library/Safari/Extensions/macfest.safariextz      |
+----------------------------+---------------------------------------------------------------+
```

Detection Mechanisms for Consumers

Consumers should ensure they have an antivirus software program installed and that it is running with the latest update. While many OS X antivirus products are only moderately effective, for consumers, this will provide a base-level of protection. There are numerous free options available from companies such as Avast, MalwareBytes and Sophos.

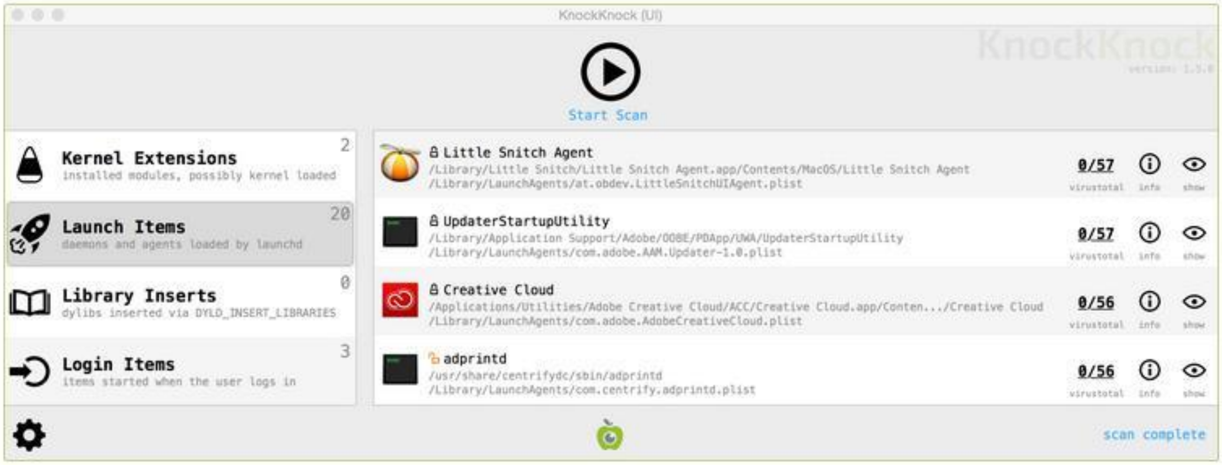
For consumers wishing to see if they have already been compromised, the following utilities are available:

Dynamic Hijack Scanner - a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked. (More here: https://objective-see.com/products/dhs.html)



```
Hijacked Applications                                                          total: 1
/Applications/iPhoto.app/Contents/Library/LoginItems/PhotoStreamAgent.app/Contents/MacOS/PhotoStreamAgent
rpath hijacker: /Applications/iPhoto.app/Contents/Library/LoginItems/PhotoFoundation.framework/Versions/A/PhotoFoundation
Vulnerable Applications                                                        total: 8
/Applications/Microsoft Office 2011/Microsoft Word.app/Contents/MacOS/Microsoft Word
weak vulnerability: /Applications/Microsoft Office 2011/Microsoft Word.app/Contents/Frameworks/MsoUnitTest.fra.../MsoUnitTest
/Applications/Xcode.app/Contents/MacOS/Xcode
rpath vulnerability: /Applications/Xcode.app/Contents/Frameworks/DVTFoundation.framework/Versions/A/DVTFoundation
```

KnockKnock - uncovers persistently installed software in order to generically reveal such malware. (More here: https://objective-see.com/products/knockknock.html)



Kernel Extensions 2
installed modules, possibly kernel loaded

Launch Items 20
daemons and agents loaded by launchd

Library Inserts 0
dylibs inserted via DYLD_INSERT_LIBRARIES

Login Items 3
items started when the user logs in

```
Little Snitch Agent                                                                  0/57
/Library/Little Snitch/Little Snitch Agent.app/Contents/MacOS/Little Snitch Agent
/Library/LaunchAgents/at.obdev.LittleSnitchUIAgent.plist

UpdaterStartupUtility                                                                0/57
/Library/Application Support/Adobe/OOBE/PDApp/UWA/UpdaterStartupUtility
/Library/LaunchAgents/com.adobe.AAM.Updater-1.0.plist

Creative Cloud                                                                       0/56
/Applications/Utilities/Adobe Creative Cloud/ACC/Creative Cloud.app/Conten.../Creative Cloud
/Library/LaunchAgents/com.adobe.AdobeCreativeCloud.plist

adprintd                                                                             0/56
/usr/share/centrifydc/sbin/adprintd
/Library/LaunchAgents/com.centrify.adprintd.plist
```

Research Methodology

For 10 weeks the Bit9 + Carbon Black Threat Research Team collected more than 1,400 unique OS X malware samples aggregated from its independent research efforts, open sources, experience from incident response engagements involving OS X, peer research, black lists, and contagio malware dumps, among other sources. The samples were then analyzed both statically and dynamically in a custom-built sandbox. This analysis focused on how OS X malware persists and what file system utilizations it has seen. From that research, the team noticed a significant increase in the prevalence of OS X malware, which was the impetus for this report.

About Bit9 + Carbon Black

Bit9 + Carbon Black is the market leader in Next-Generation Endpoint Security. We have sold more licenses, have more experience, and more customers than any other NGES company because our solution is the most effective way to prevent, detect and respond to advanced threats that target users, servers, and fixed-function devices. That's why more than 60 MSSP and IR leaders, including Dell SecureWorks, EY, Optiv and Solutionary, have chosen our technology as a key component of their security offerings, and 25 of the Fortune 100 rely on us as a critical element of their advanced threat defense and compliance strategies. By the end of 2015, we expect to achieve $70M+ in annual revenue, 70 percent growth, 7 million+ software licenses sold, and almost 2,000 customers worldwide. We were voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2014 Awards, and a 2015 SANS survey found that 68 percent of IR professionals are using or evaluating Carbon Black.