RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: TECH-W10

Lost Boys: How Linux and mac Intersect in a Windows-Centric Security World

Josh Harriman

VP of Cyber Security Intelligence
Ziften
@IrishNewMexican

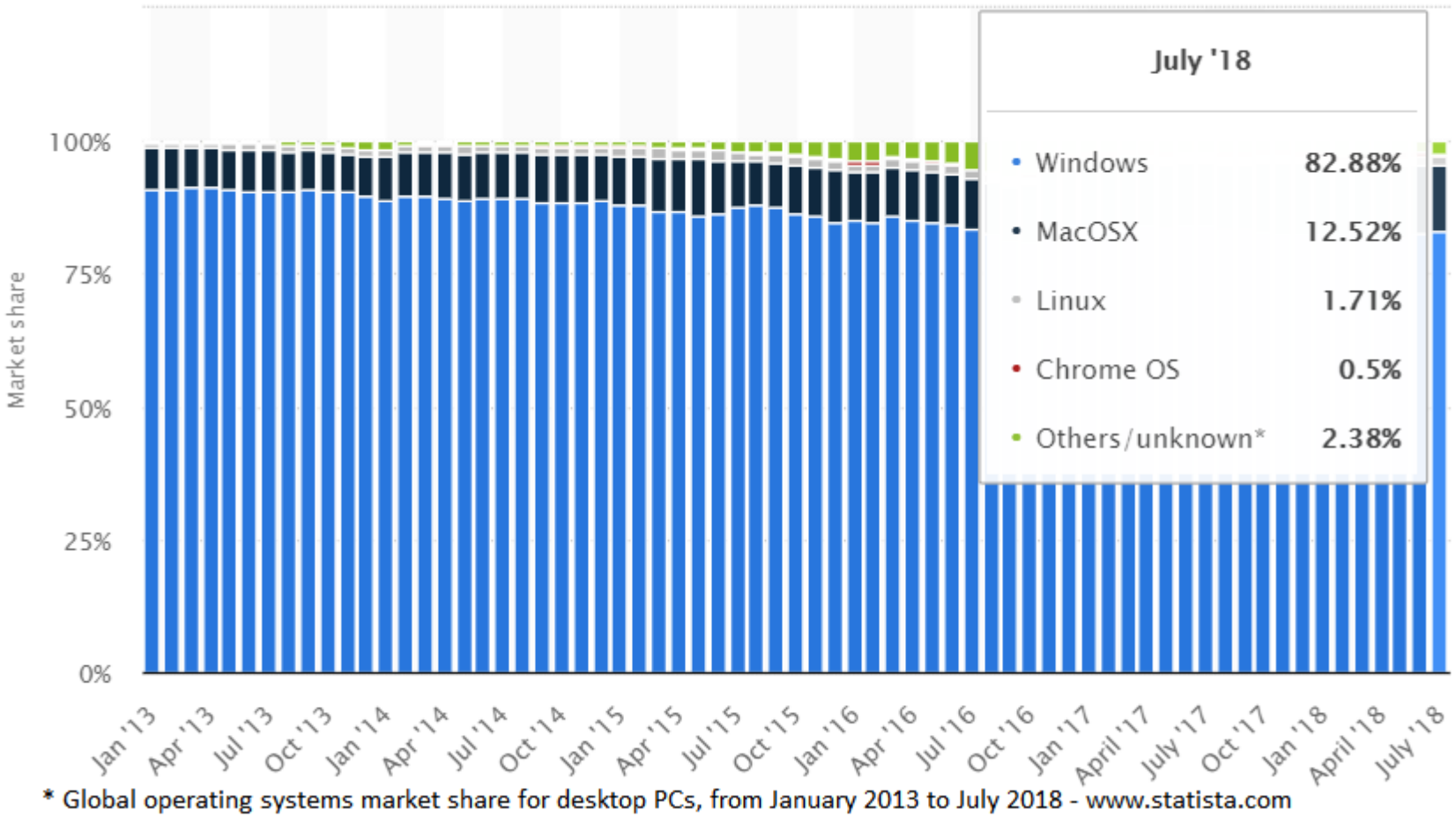
Alexander Benoit

Lead Security Analyst
sepago GmbH
@ITPirate

macOS and Linux in the workplace

- Microsoft still dominates the market share (overall)
- macOS continues to grow
- BYOD – cool, I'll bring in my killer macbook pro
- Linux – servers really, not much desktop

macOS and Linux in the workplace



* Global operating systems market share for desktop PCs, from January 2013 to July 2018 - www.statista.com

Session Objectives

- Clear up misconception about macOS and Linux attacks
- Develop easy to follow strategy to cover your assets
- Give you details on how to achieve this strategy

RSAConference2019

Some history of attacks specific to macOS and Linux

macOS Management in the Enterprise Today

- most management products are built for Windows computers
- join Macs to AD & use Apple Remote Desktop to push commands
- use Mac OS X Server with Apple's Profile Manager to set policies
- 3rd party management software

macOS attacks over the years

History of Mac Malware

macOS attacks

```
# less OSX_Renepo

scriptpath=`pwd`
scriptfolder=`basename $scriptpath`
scriptname=`basename $0`

mkdir /System/Library/StartupItems/"${scriptname}"
cp "${scriptpath}"/"${scriptname}"
      /System/Library/StartupItems/"${scriptname}"/"${scriptname}"

# The lines below echo out the StartupParameters.plist file.
echo "<plist version=\"0.9\">" >>
     /System/Library/StartupItems/$scriptname/StartupParameters.plist

...
```

Renepo – 2004

macOS attacks

MacSweeper – 2008

macOS attacks

Flashback Malware – 2012

macOS attacks

Linux Management in the Enterprise Today

- "Security through obscurity"
- 100’s of Linux distributions and variations
- 1000’s of use cases (IoT, IIoT, ICS... etc.)

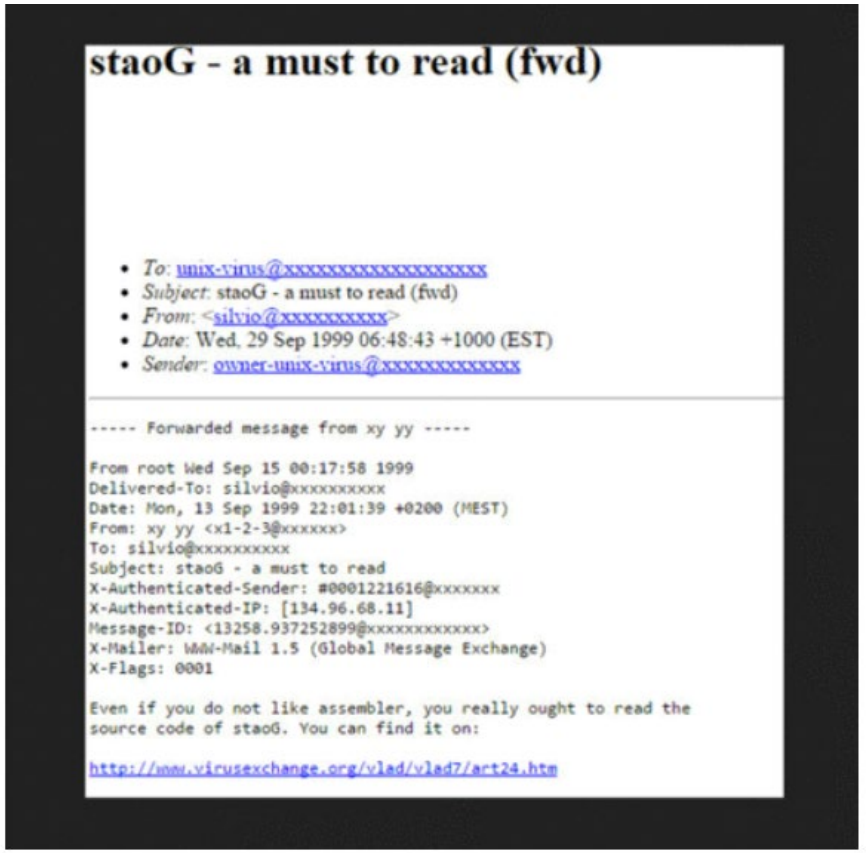
Linux attacks over the years

LINUX

A brief history of Linux malware

A look at some of the worms and viruses and Trojans that have plagued Linux throughout the years.

Linux attacks



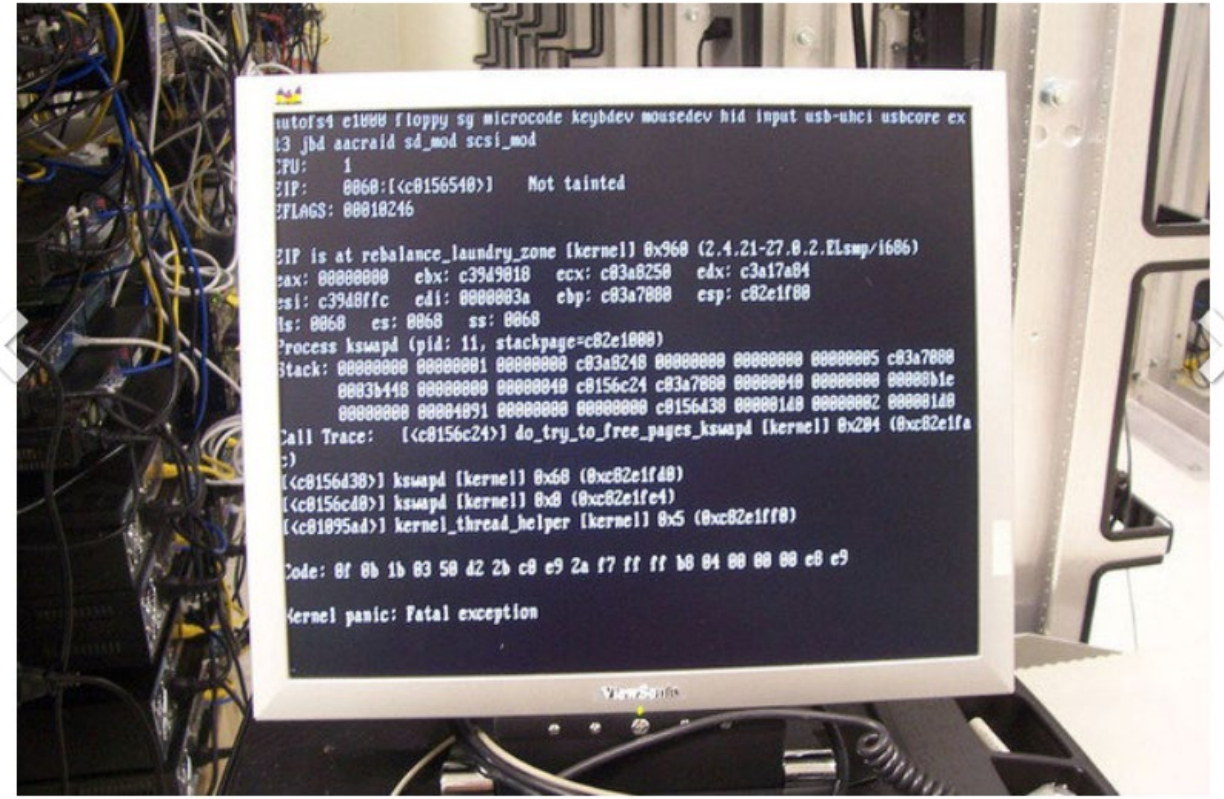
staoG - a must to read (fwd)

- *To*: unix-virus@xxxxxxxxxxxxxxxxxxx
- *Subject*: staoG - a must to read (fwd)
- *From*: <silvio@xxxxxxxxxx>
- *Date*: Wed, 29 Sep 1999 06:48:43 +1000 (EST)
- *Sender*: owner-unix-virus@xxxxxxxxxxxxx

```
----- Forwarded message from xy yy -----

From root Wed Sep 15 00:17:58 1999
Delivered-To: silvio@xxxxxxxxxx
Date: Mon, 13 Sep 1999 22:01:39 +0200 (MEST)
From: xy yy <x1-2-3@xxxxxx>
To: silvio@xxxxxxxxxx
Subject: staoG - a must to read
X-Authenticated-Sender: #0001221616@xxxxxxx
X-Authenticated-IP: [134.96.68.11]
Message-ID: <13258.937252899@xxxxxxxxxxxx>
X-Mailer: WWW-Mail 1.5 (Global Message Exchange)
X-Flags: 0001

Even if you do not like assembler, you really ought to read the
source code of staoG. You can find it on:

http://www.virusexchange.org/vlad/vlad7/art24.htm
```

Staog (1996)

Linux attacks

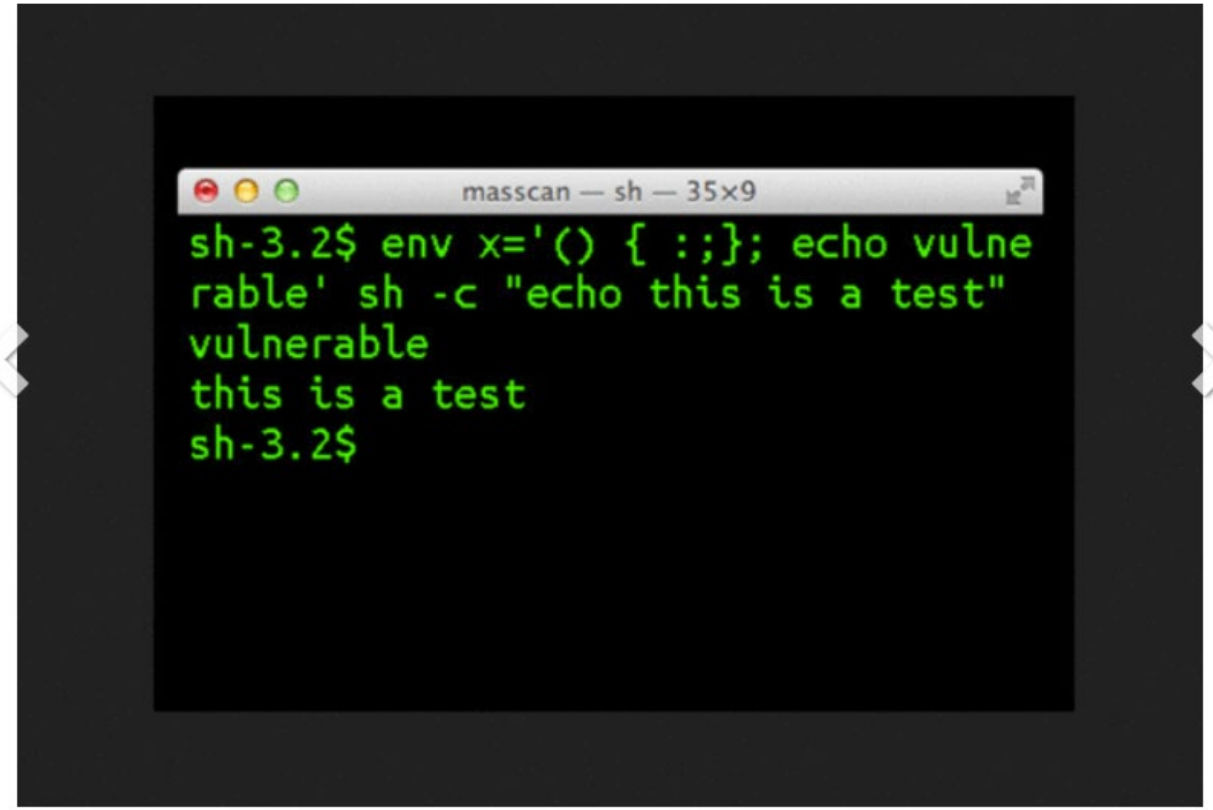


See larger image

Wikimedia CommonsCC LicenseKevin Collins

Slapper (2002)

Linux attacks



Shellshock/Mayhem (2014)

Linux attacks

DynoRoot!!!1111 (CVE-2018-1111) is a remote code execution vulnerability (as root) in Red Hat linux.

Malware not needed

- Attacks today generally don’t need sophisticated malware
  - Social engineering to gain access
  - Exploits in 3rd party software

SECURITY

In their words: Experts weigh in on Mac vs. PC security

CNET asks a host of security experts which of the major operating-system platforms is more secure for consumers. Here's what they have to say.

ziften

Using legitimate tools for nefarious actions

- Living off the land in Windows has its place in macOS and Linux
  - https://gtfobins.github.io/

GTFOBins

★ Star 872

GTFOBins is a curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks. See the full list of functions.

This was inspired by the LOLBins project for Windows.

GTFOBins is a collaborative project created by norbemi and cyrus_and where everyone can contribute with additional binaries and techniques.

RSAConference2019

Strategy to monitor macOS and Linux

You need to monitor ALL activity ALL the time

Endpoint Detection and Response (EDR) is a cybersecurity technology that addresses the need for continuous monitoring and response to advanced threats.

EDR is focused on providing the right endpoint visibility with the right insights to help security analysts discover, investigate and respond to very advanced threats and broader attack campaigns stretching across multiple endpoints.

- Historical data is important as well

Step by step

1. Do you know your assets in your network?
2. Are they managed by IT?
3. What can you find out about them without managing them?
4. Once managed, what do you need to monitor?

***What*, where and when**

- Find a tool that can *find* unmanaged assets
  - There are enterprise solutions available to do this
    - Go to the Vendor hall and have some conversations

- Using arp scan or arp cache (on managed systems) can give results of other systems in your network that you need to be aware of

Unmanaged Assets

Hostname	Ip Address	Mac Address	Manufacturer	Isgateway	Isdhcp	Isdns	First Seen	Last Seen	Reporting system
NY- FH...	10.200.139.106	8c:85:90:30:84...		False	False	False	2019-02-13	2019-02-13	RL
10.	10.160.133.7	f8:38:80:45:12:...		False	False	False	2019-02-12	2019-02-12	CH .EK
NY- 2.gl...	10.200.76.148	e4:b9:7a:c5:d4...		False	False	False	2019-02-12	2019-02-12	FF
10. 0	10.200.140.50	8c:45:00:8c:d1...		False	False	False	2019-02-11	2019-02-12	NY !
GUI	10.160.132.92	24:a2:e1:f3:cb:...	Apple	False	False	False	2019-02-13	2019-02-13	JE 270
NY- 3G...	10.200.67.213	04:69:f8:ed:53:...	Apple	False	False	False	2019-02-11	2019-02-11	US OXX1
US- I71...	10.160.132.59	c4:b3:01:a7:f3:...	Apple	False	False	False	2019-02-11	2019-02-11	JE 270
CHI 2	10.200.138.186	48:d7:05:d5:63...	Apple	False	False	False	2019-02-11	2019-02-11	SN 70
LAF 8L...	10.161.50.15	44:1c:a8:f0:99:...	HonHaiPr	False	False	False	2019-02-13	2019-02-13	ID 211
NY- .gl...	10.200.137.80	00:23:15:e6:a4...	IntelCor	False	False	False	2019-02-11	2019-02-11	NY !
10. 19	10.200.138.219	9c:b6:d0:8e:09...	RivetNet	False	False	False	2019-02-11	2019-02-11	SN 70
MA R-D...	10.160.133.135	38:f9:d3:4e:d1:...		False	False	False	2019-02-13	2019-02-13	CH 5
NY- .gl...	10.200.139.6	64:5d:86:63:92...		False	False	False	2019-02-13	2019-02-13	RL)
10. 5	10.161.50.245	f0:98:9d:59:e8:...		False	False	False	2019-02-13	2019-02-13	ID 211
NY- 5H...	10.200.138.255	8c:85:90:30:92...		False	False	False	2019-02-13	2019-02-13	RL)
10. 0	10.160.132.60	18:81:0e:85:d9...		False	False	False	2019-02-13	2019-02-13	JE 270

What, *where* and when

- Everywhere in your network
  - Corporate
  - VPN access
  - Every system you can touch
  - Cloud environments

- Match against your systems management tool report
  - Is the system compliant and protected?
  - Filevault (macOS), SELinux (if applicable)

Filevault status monitoring

Checks to see if FileVault (Full Disk Encryption) is enabled on Mac OS systems.

Group: All **Date:** Custom Refresh Report

Between: 2018-07-03 **and** 2019-02-21

Search thes

System	Filevault Status	Status Date
Andreas-MacBook-Air.local	True	2018-09-10
C02PWN6FG8WN.local	False	2018-09-10
Chriss-MacBook-Pro-2.local	True	2018-09-10
Chriss-MBP-2	True	2018-09-10
Gregs-MacBook-Pro-2.local	False	2018-09-09
Gregs-MacBook-Pro-2.local	False	2018-09-10
Gregs-MBP-2	False	2018-07-14
Gregs-MBP-2	False	2018-09-07
gregs-mbp-2.ziften.local	False	2018-07-30
Kims-MacBook-Air.local	True	2018-09-10
Logans-MacBook-Pro-2.local	True	2018-08-25
Logans-MacBook-Pro-2.local	False	2018-10-22

Jamf

Need advanced options for your Apple deployment?

Jamf Pro has what you are looking for.

Self Service

Empower users with your own app store. Let them install apps, update software and maintain their own device without a help desk ticket.

Patch Management

Automatically combat security vulnerabilities and ensure you users always get the latest and greatest software.

Integrations

Jamf Pro integrates with Apple School Manager, directory services / Active Directory, SAML single sign-on and API integrations.

More Options

From advanced configurations to custom scripts, Jamf Pro gives you the options to check every box.

What, where and *when*

- All the time visibility
  - Look at system and user behavior

- Historical lookback is very important
  - What was the system doing 6 months ago?
  - Use this information to update your security procedures

Historical timeline

Timeline of processes executed on this system

Date: Custom ▾ Refresh Report

Between: 2019-02-07 **and** 2019-02-08

Search these 54 r

mainn...	PID	Processimagepath	Timestamp	Commandline
	2268	/System/Library/Frameworks/Sec...	2019-02-07 19:06:21	/System/Library/Frameworks/Se...
	2269	/System/Library/PrivateFramewor...	2019-02-07 19:06:22	/System/Library/PrivateFramewo...
	2271	/usr/bin/sudo	2019-02-07 19:07:16	sudo spctl –status
	2276	/System/Library/Frameworks/Add...	2019-02-07 19:17:59	/System/Library/Frameworks/Ad...
	2277	/Applications/System Preferences....	2019-02-07 19:19:08	/Applications/System Preference...
	2278	/usr/libexec/diskmanagementd	2019-02-07 19:19:08	/usr/libexec/diskmanagementd
	2283	/System/Library/CoreServices/Ma...	2019-02-07 19:19:08	/System/Library/CoreServices/M...
	2284	/System/Library/PreferencePanes...	2019-02-07 19:19:12	/System/Library/PreferencePane...
	2285	/System/Library/PrivateFramewor...	2019-02-07 19:19:15	/System/Library/PrivateFramewo...
	2286	/System/Library/Frameworks/Sec...	2019-02-07 19:19:19	/System/Library/Frameworks/Se...
	2291	/Applications/System Preferences....	2019-02-07 19:19:53	/Applications/System Preference...
	2298	/System/Library/PrivateFramewor...	2019-02-07 19:19:59	/System/Library/PrivateFramewo...
	2299	/System/Library/Frameworks/Sec...	2019-02-07 19:20:04	/System/Library/Frameworks/Se...
	2300	/usr/bin/sudo	2019-02-07 19:20:34	sudo spctl –master-enable
	2322	/usr/sbin/ocspd	2019-02-07 21:31:38	/usr/sbin/ocspd

RSAConference2019

Some tools and techniques

Turn on some logging…and then look at that data

Auditing OSX

- openBSM project created by McAfee Research
- The Basic Security Module (BSM) interface to audit records and audit event stream format were defined by Sun Microsystems
- openBSM provides an auditing system available as part of the core OS X
  - **Advantages**: openBSM adds support for security event auditing. Event auditing supports reliable, fine-grained, and configurable logging of a variety of security-relevant system events, including logins, configuration changes, and file and network access. These log records can be invaluable for live system monitoring, intrusion detection, and post mortem analysis.

Auditing Linux

Linux System Monitoring and More with Auditd

Auditd

- Audit is actively developed by Red Hat and is available for most, if not all, major distributions. If it is not already installed on your system, you can find it by searching in your system's repositories. In Debian-based systems, the package is simply called *audit*, while in RPM-based systems, it shows up as *auditd*. In most Red Hat-related systems, such as Fedora and CentOS, auditd is usually installed by default.
  - https://www.linux.com/learn/linux-system-monitoring-and-more-auditd
  - https://www.linux.com/learn/customized-file-monitoring-auditd

RSAConference2019

What do you do now

Apply what we discussed today, tomorrow and always

- After the conference next week, find your missing assets
  - Do you have unmanaged macOS and Linux systems
  - Do you know you have those systems, but are ignoring them?
- By the middle of Q2 this year, you should have at least tested a solution either from a vendor (PoC) or home grown
  - Talk with at least 3 vendors this week
- By the end of 2019, you should never have a blind spot with your macOS and Linux population
  - Either purchase a solution from a vendor, or apply some tactics we discussed today

References

- https://github.com/darkoperator/Posh-SecMod/blob/master/Discovery/Discovery.psm1
- https://www.scip.ch/en/?labs.20150108
- https://gtfobins.github.io/
- https://www.fortinet.com/blog/threat-research/microsoft-word-file-spreads-malware-targeting-both-apple-mac-os-x-and-microsoft-windows.html_
- https://opensource.apple.com/source/OpenBSM/
- https://www.linux.com/learn/linux-system-monitoring-and-more-auditd