RSA 2019

HACKING EXPOSED

CROWDSTRIKE

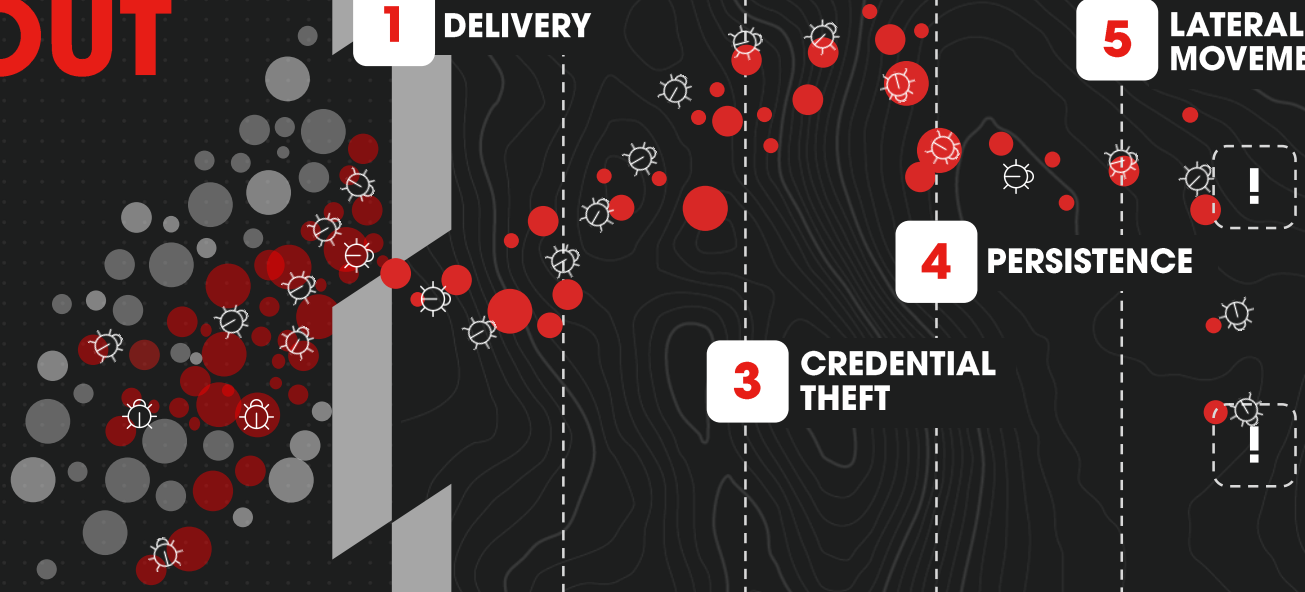
George Kurtz
CEO

Dmitri Alperovich
CTO


WHEN IT COMES TO DEFEATING ADVERSARIES
NOTHING IS MORE CRITICAL THAN SPEED
EPSON
CROWDSTRIKE
77
PETRONAS
PRIMAX
IWC
SCHAFFHAUSEN

CROWDSTRIKE

BREAKOUT TIME



RSA 2019

CROWDSTRIKE INTELLIGENCE
NAMING CONVENTIONS

CROWDSTRIKE

	ADVERSARY	CATEGORY / NATION STATE
	SPIDER	ECRIME
	CHOLLIMA	NORTH KOREA
	JACKAL	HACKTIVIST
	TIGER	INDIA
	KITTEN	IRAN

	ADVERSARY	CATEGORY / NATION STATE
	LEOPARD	PAKISTAN
	PANDA	CHINA
	BEAR	RUSSIA
	CRANE	SOUTH KOREA
	BUFFALO	VIETNAM

RSA 2019

BREAKOUT TIME BY ADVERSARY

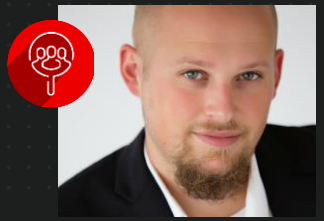
CROWDSTRIKE

SURVIVAL OF THE FASTEST:

THE 1 - 10 - 60 RULE

CROWDSTRIKE

HACKING EXPOSED HACKING MACS



Jaron Bradley
OverWatch Analyst

RSA 2019

CROWDSTRIKE

WICKED PANDA
INTRUSION

All Mac-based intrusion

- Pivoted from system to system by compromising one machine
- Some passwords stolen via spear-phishing
- 5 systems traversed within 4 hours — including a build server

CROWDSTRIKE

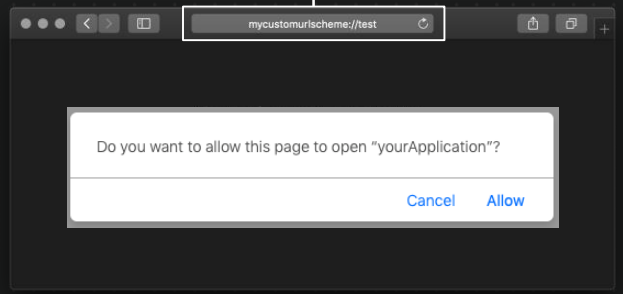
WINDY BAT
INTRUSION

- Unattributed adversary referred to industry by Windshift
- Typically targeted individuals, often with Middle East nexus
- Known for interesting Mac hacking tradecraft

DELIVERY
URL SCHEMES

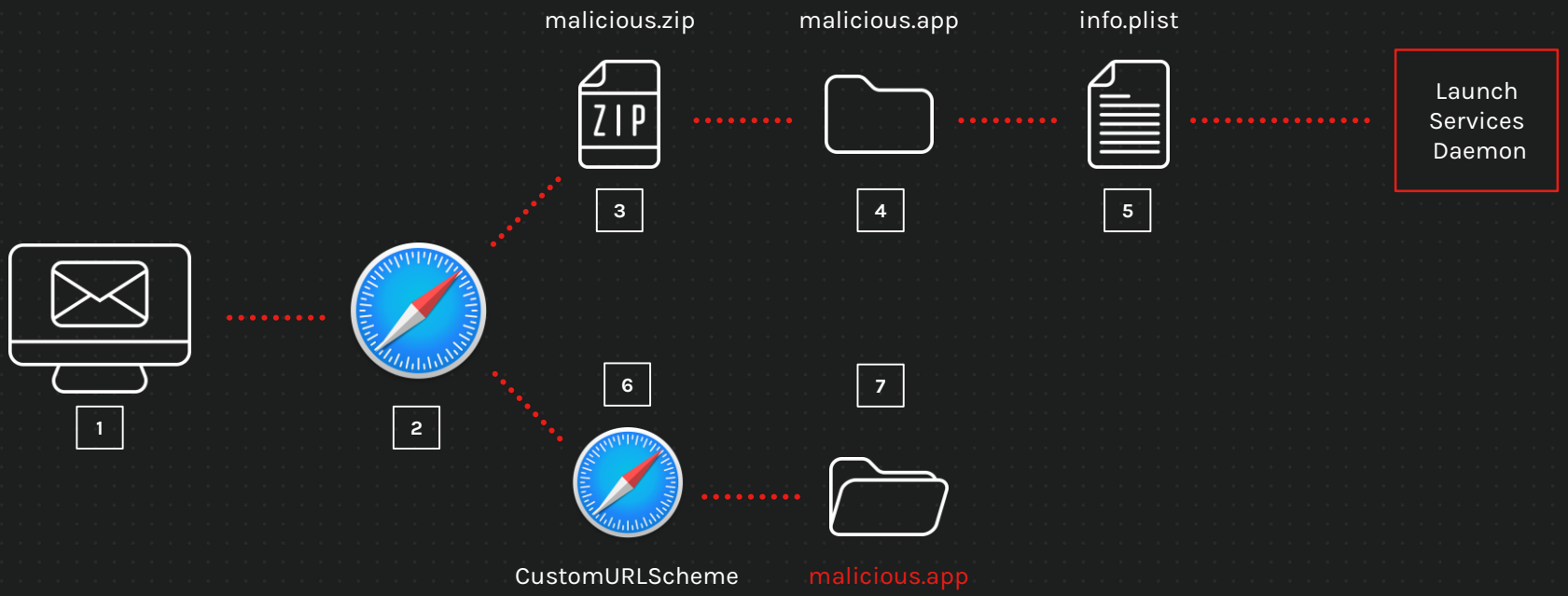
CROWDSTRIKE

mycustomurlscheme://test



Key	Type	Value
URL Types	Array	(1 Item)
Item 0	Dictionary	(2 Items)
URL Identifier	String	
URL Schemes	Array	(1 Item)
Item 0	String	myCustomURLScheme

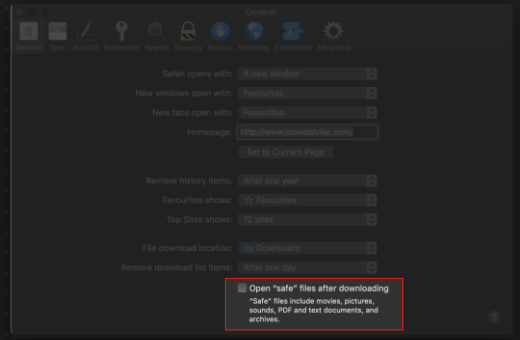
CROWDSTRIKE



DEMO

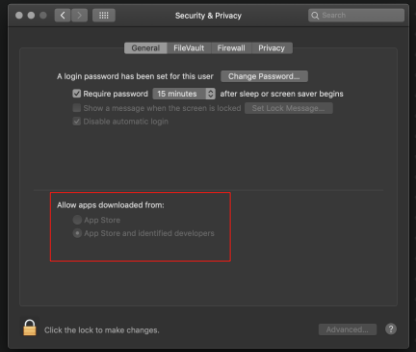
DELIVERY
COUNTERMEASURES

URL Schemes



Disable the option in Safari to "Open "safe" files after downloading"

Gatekeeper



System Preferences > Security & Privacy > Allow apps downloaded from
App Store,
App Store and identified developers

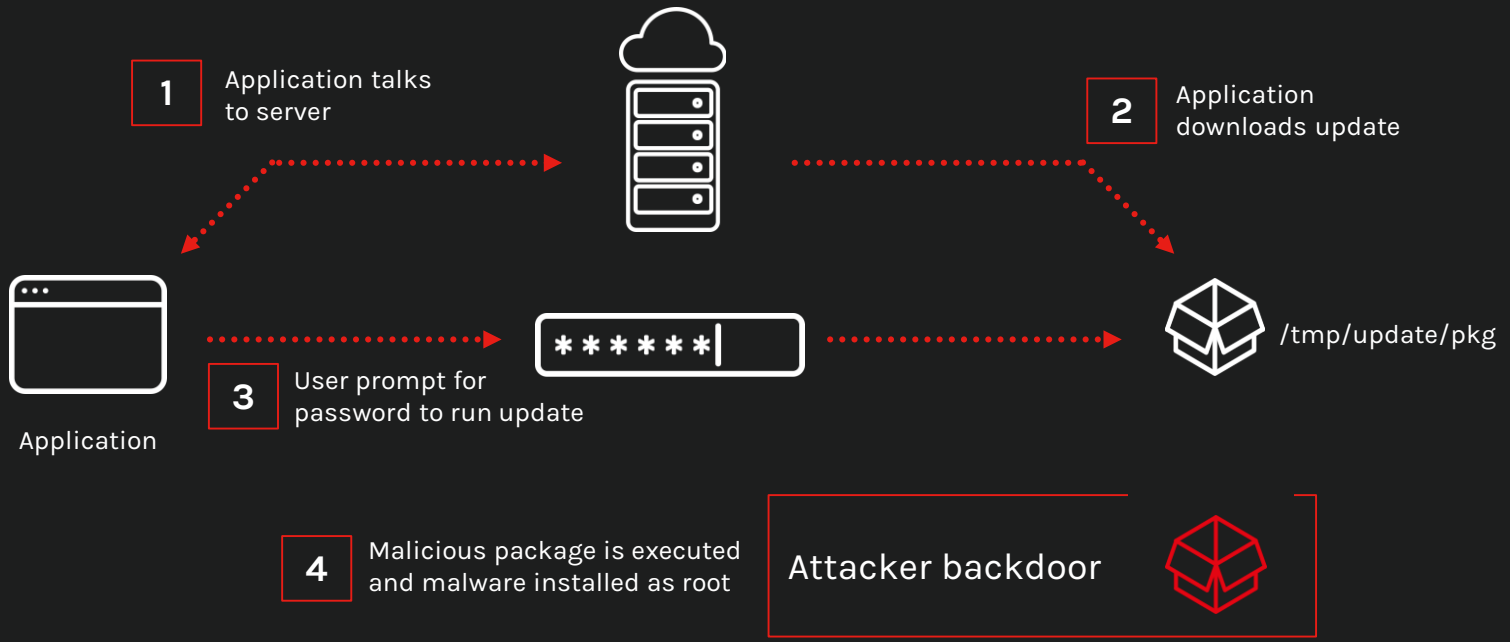
Office Macros

User Awareness Training

Office Product > Preferences > Security & Privacy > Disable Macros without notification

CROWDSTRIKE

PRIVILEGE ESCALATION
POOR UPDATE PRACTICE

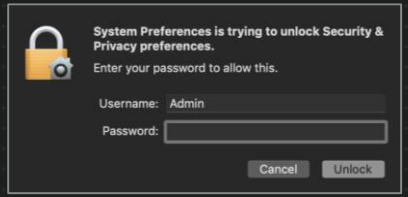


DEMO

PRIVILEGE ESCALATION
COUNTERMEASURES

CROWDSTRIKE

Download on the App Store



Installer Takeovers

Install applications from the Apple Store when possible to ensure Sandbox is applied

Keep system up to date to patch privilege escalation 0-days that are discovered for macOS

User awareness on password popup prompts

CROWDSTRIKE

CREDENTIAL THEFT
HASHDUMP

Using System Integrity Protection, Apple has restricted direct access to the files inside /var/db/dslocal/nodes/Default/users/, rendering a handful of hash dumping tools and techniques outdated

defaults read /var/db/dslocal/nodes/Default/users/$USER.plist ShadowHashData was probably the command most frequently referenced that no longer works

The dscl command can still be used to access ShadowHashData
dscl . read /Users/$USER dsAttrTypeNative:ShadowHashData

DEMO

CROWDSTRIKE

CREDENTIAL THEFT
COUNTERMEASURES

Hashdump

Use a good password

Use products that notify or monitor for access to credential files

Keychain Theft

Change your keychain password to be something different than your login password

security set-keychain-password ~/Library/Keychains/login.keychain-db

SSH

Always use a password associated with private keys

Don’t use plaintext passwords at the command line level

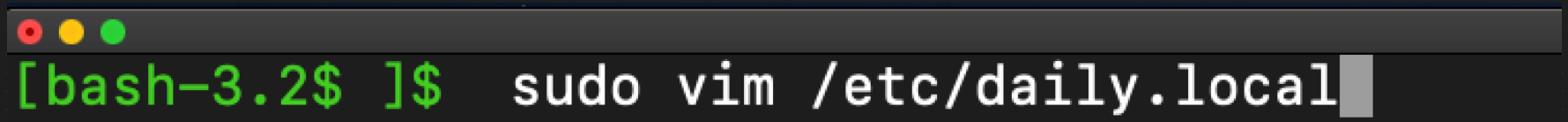
Run cleanup scripts to remove ssh artifacts

CROWDSTRIKE

PERSISTENCE

Standard ASEPS	SIP Protected ASEPS	Lesser-Used ASEPS
/Library/LaunchAgents (root) /Library/LaunchDaemons (root) ~/Library/LaunchAgents (user) ~/Library/LaunchDaemons (user)	/System/Library/LaunchAgents /System/Library/LaunchDaemons	/private/etc/daily.local /private/etc/weekly.local /private/etc/monthly.local

ASEP Piggybacking
/var/root/Library/preferences/com.apple.loginwindow.plist


[bash-3.2$]$ sudo vim /etc/daily.local

PERSISTENCE
COUNTERMEASURES

Monitor ASEPS being created in your environment

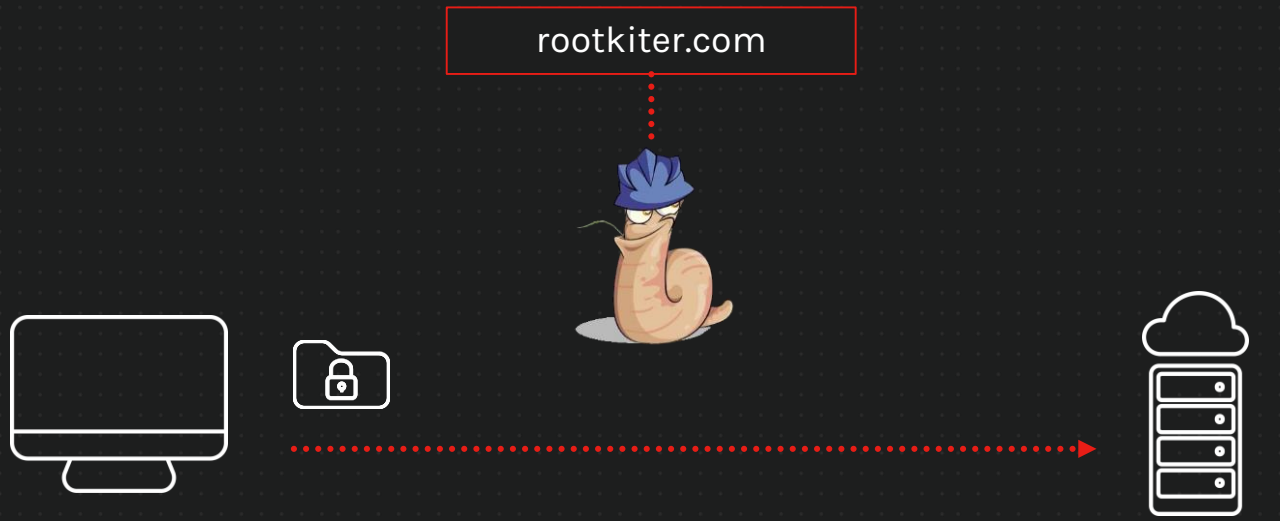
Free Tool:

Block Block
by Objective-See

objective-see.com

CROWDSTRIKE

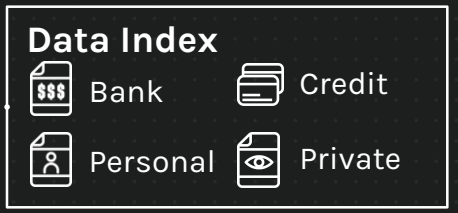
EXFIL
EARTHWORM

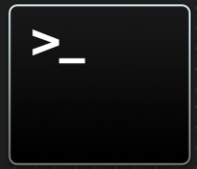


EXFIL
mdfind

mdfind provides macOS Spotlight functionality at the command line level.

Spotlight is constantly running in the background, indexing data by keywords



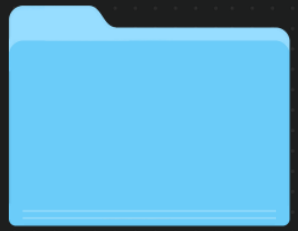



```
mdfind confidential -onlyin
~/Documents/ -0 | xargs -0
tar -rvf /tmp/exfil.tar
```

DEMO

CROWDSTRIKE

EXFIL
COUNTERMEASURES



Confidential.noindex
75 items

Force no indexing using folder name <folder>.noindex

Look for outbound SSH and SOCKS Tunnels

CROWDSTRIKE

INTRODUCING
AutoMacTC

RSA 2019

INTRODUCING AutoMacTC

CROWDSTRIKE

What it is: A Python framework for forensic triage collection on macOS

Purpose: Quickly gather forensic data from systems of interest for incident response

Key Features:

- Easy to use
- Runs natively on all Macs
- Captures and parses critical artifacts **out-of-the-box**
- Customizable data collection
- Produces simple, consistent, accessible output

Blog: blog.crowdstrike.com

RSA 2019

CROWDSTRIKE

THIS YEAR'S "CUFFIES" RECIPIENTS ALL LEVERAGED SPEED

MAC ACTOR CUFFIE

WICKED PANDA

FASTEST ACTOR CUFFIE

COZY BEAR

CROWDSTRIKE

RSA 2019

OODA

OBSERVE – ORIENT – DECIDE – ACT

LIFETIME
ACHIEVEMENT
AWARD

JOHN BOYD

REMEMBER 1-10-60

IT'S ALL ABOUT SPEED

THANK YOU

CROWDSTRIKE

www.crowdstrike.com