jamf

A loopback in device security and management

Matteo Bolognini

Product Specialist

skartek.dev

2002

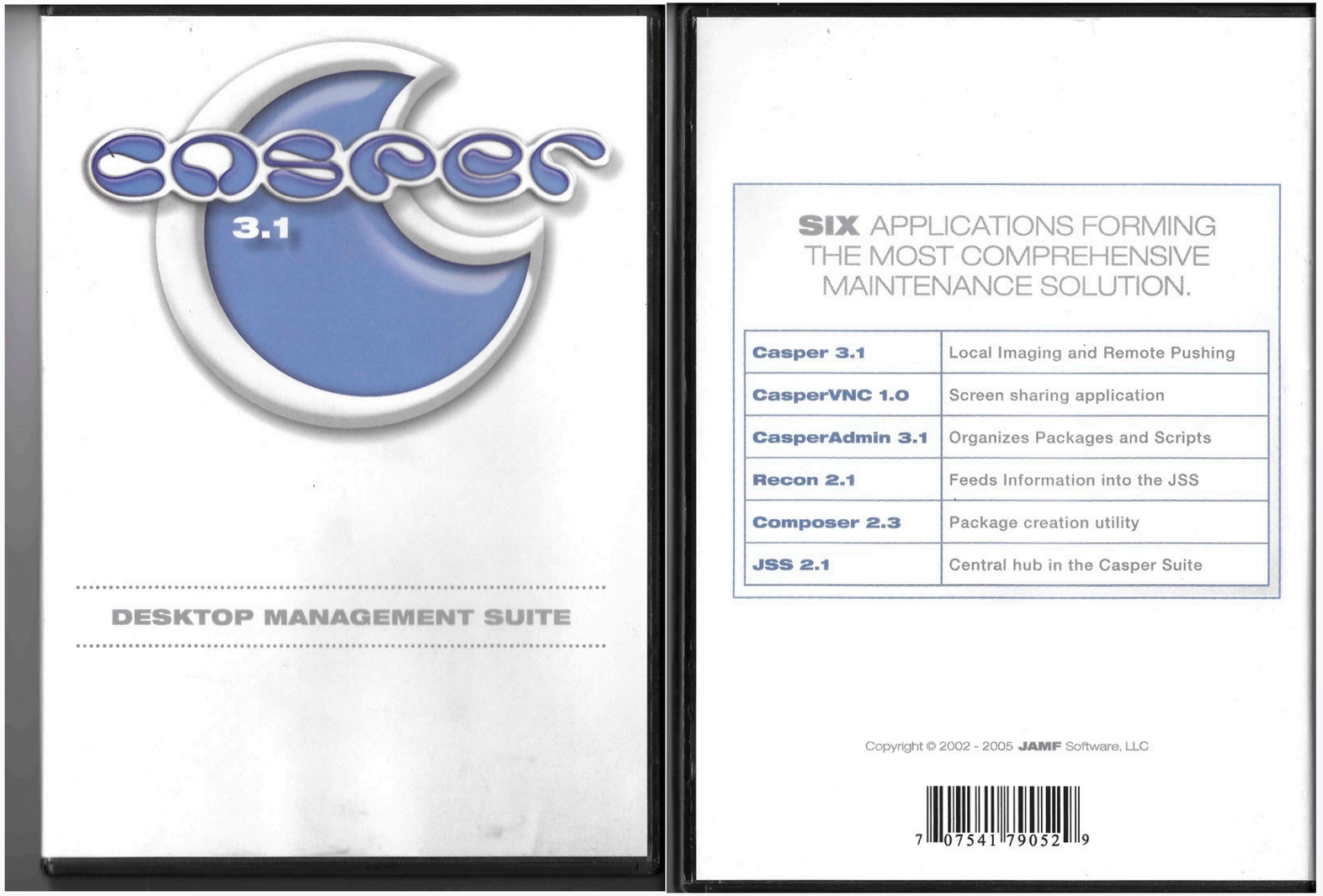
The

Beginning

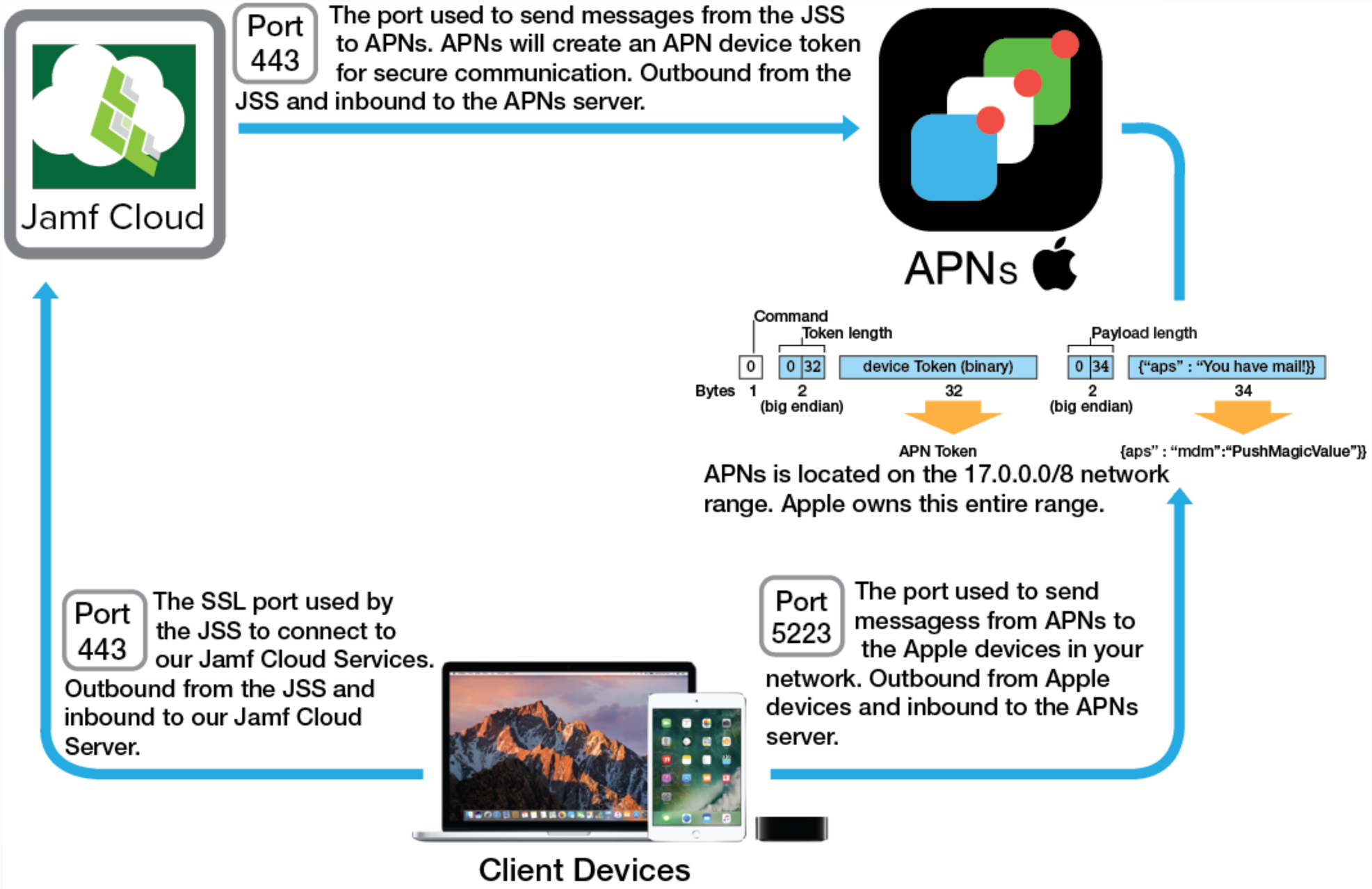
of

Device

Management

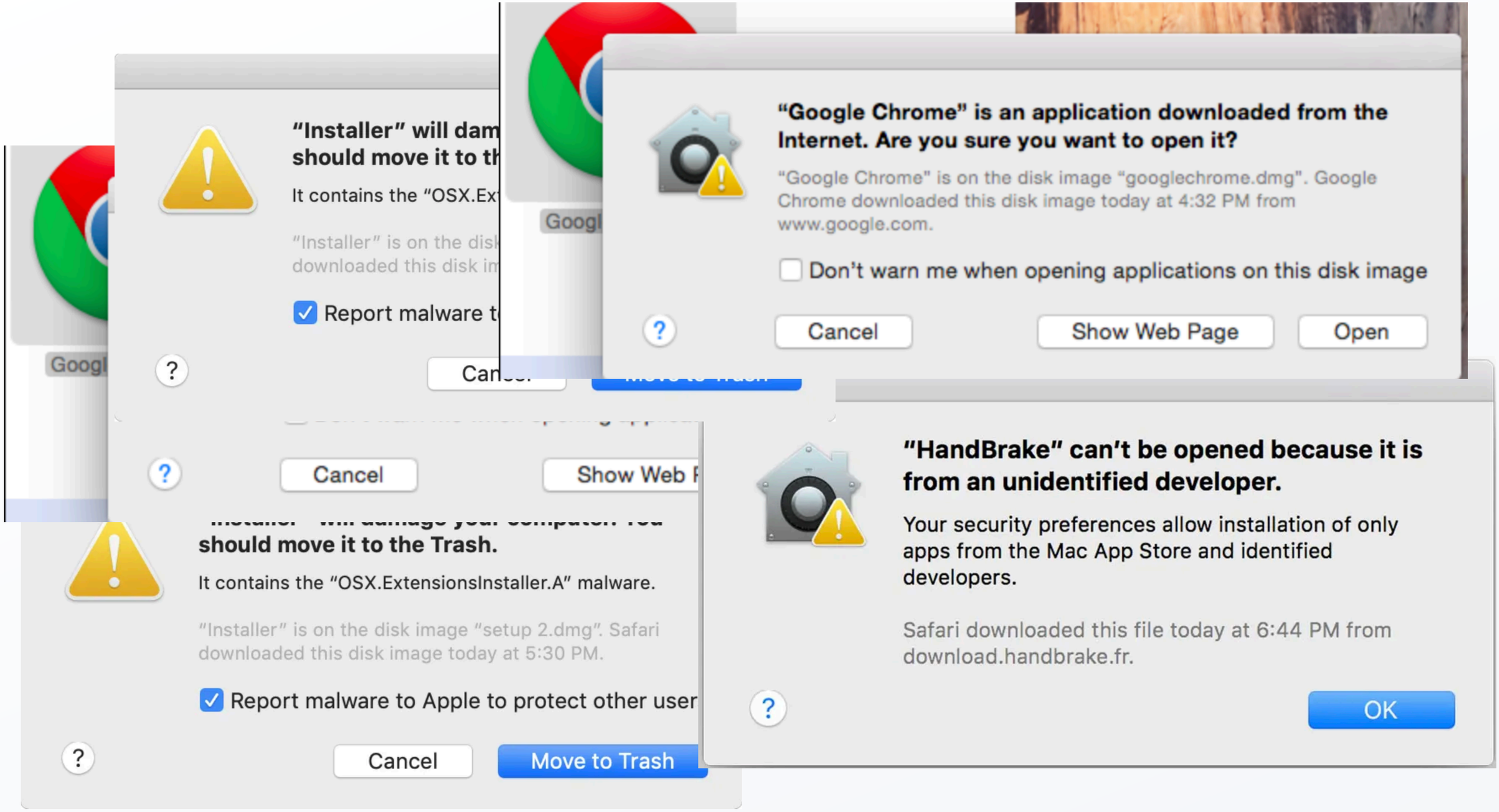


jamf

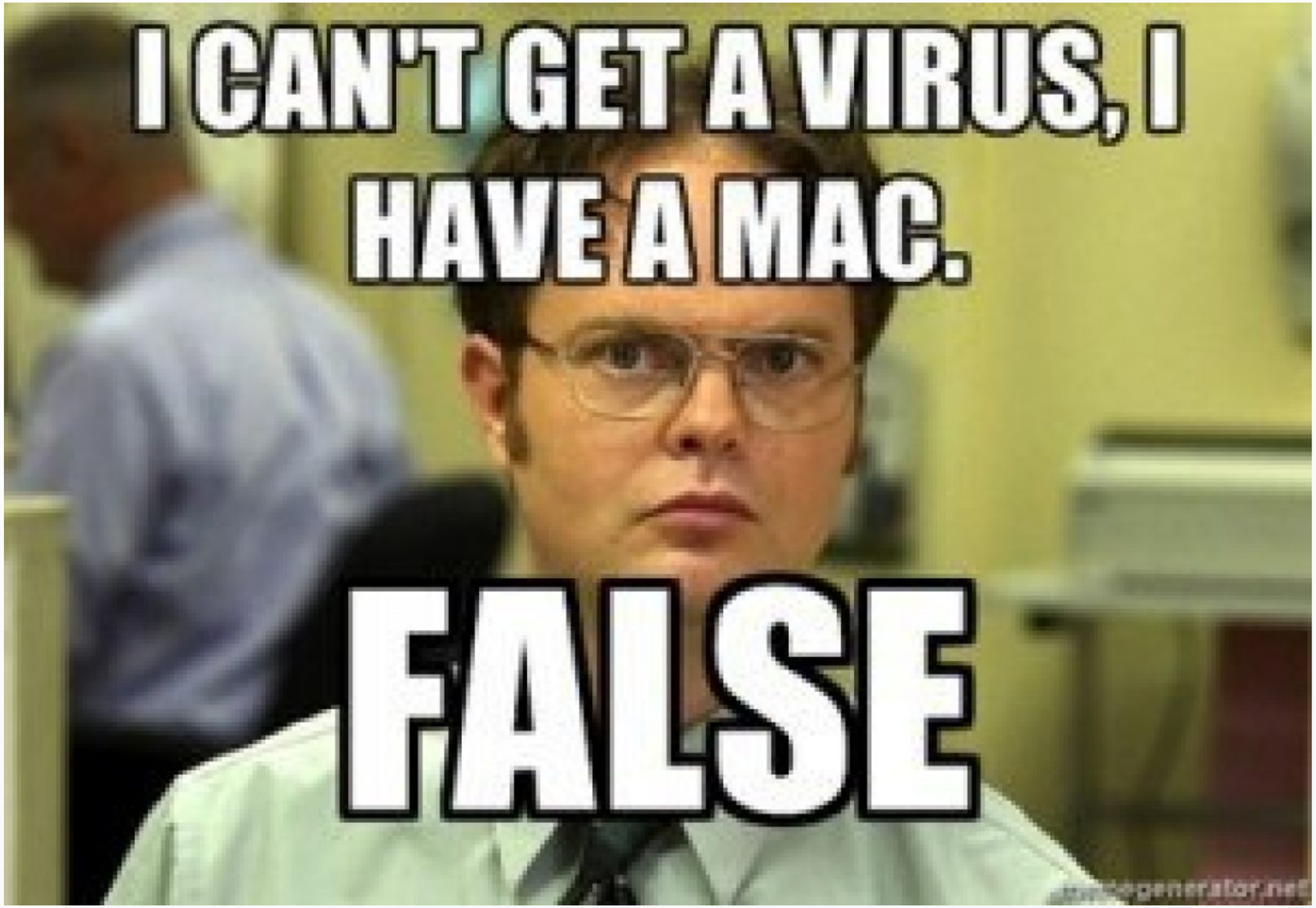

Jamf Cloud
Port 443
The port used to send messages from the JSS to APNs. APNs will create an APN device token for secure communication. Outbound from the JSS and inbound to the APNs server.
APNs
Command
Token length
Payload length
0
0 32
device Token (binary)
0 34
{"aps" : "You have mail!}}
Bytes 1
2 (big endian)
32
2 (big endian)
34
APN Token
{aps" : "mdm":"PushMagicValue"}}
APNs is located on the 17.0.0.0/8 network range. Apple owns this entire range.
Port 443
The SSL port used by the JSS to connect to our Jamf Cloud Services. Outbound from the JSS and inbound to our Jamf Cloud Server.
Port 5223
The port used to send messagess from APNs to the Apple devices in your network. Outbound from Apple devices and inbound to the APNs server.
Client Devices

jamf

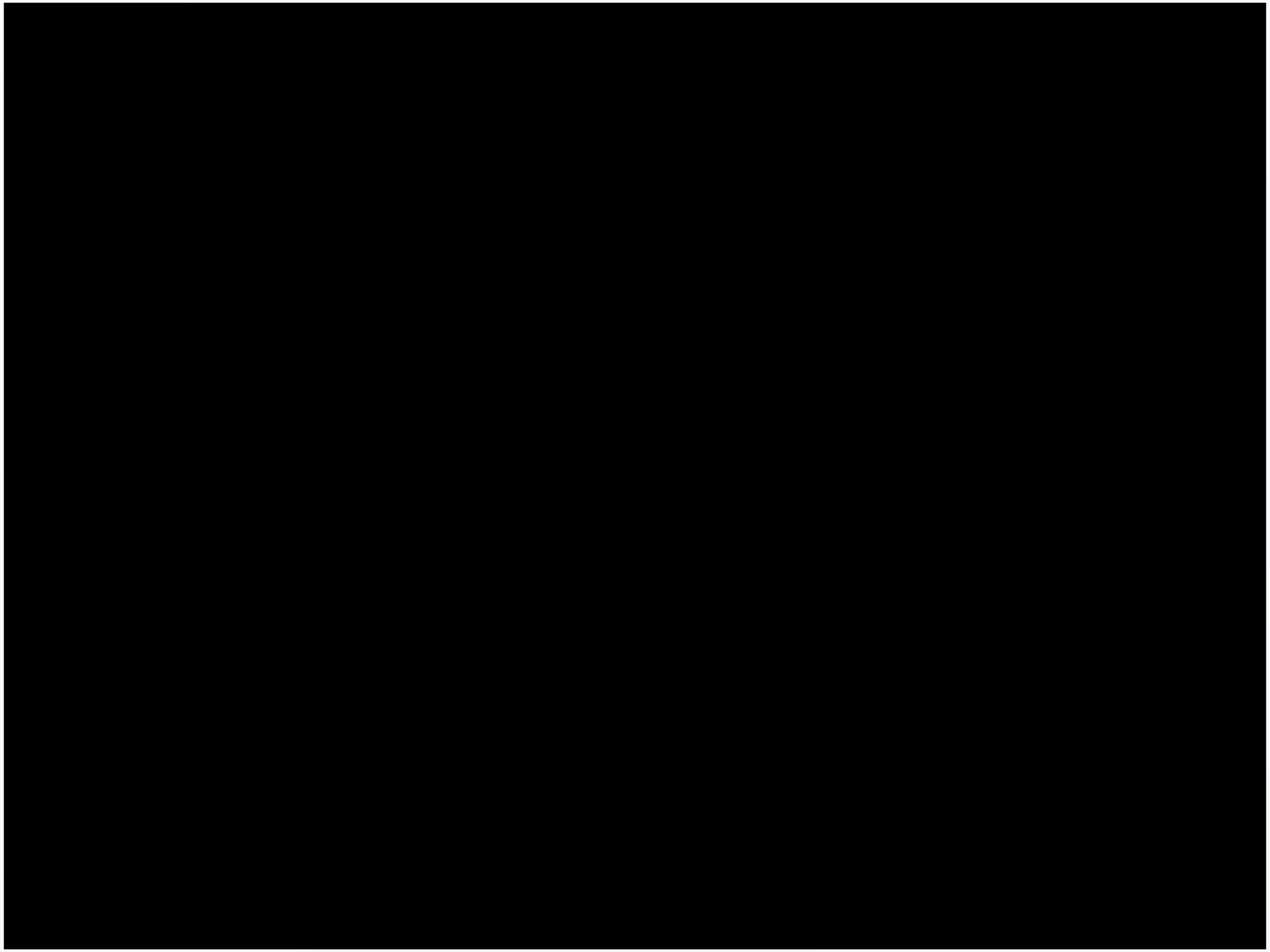
jamf


"Installer" will dam
should move it to th
It contains the "OSX.Ex
"Installer" is on the disk
downloaded this disk in
Report malware t
Cancel
Show Web P
should move it to the Trash.
It contains the "OSX.ExtensionsInstaller.A" malware.
"Installer" is on the disk image "setup 2.dmg". Safari downloaded this disk image today at 5:30 PM.
Report malware to Apple to protect other user
Cancel
Move to Trash
"Google Chrome" is an application downloaded from the Internet. Are you sure you want to open it?
"Google Chrome" is on the disk image "googlechrome.dmg". Google Chrome downloaded this disk image today at 4:32 PM from www.google.com.
Don't warn me when opening applications on this disk image
Cancel
Show Web Page
Open
"HandBrake" can't be opened because it is from an unidentified developer.
Your security preferences allow installation of only apps from the Mac App Store and identified developers.
Safari downloaded this file today at 6:44 PM from download.handbrake.fr.
OK

jamf



jamf



jamf

The first virus

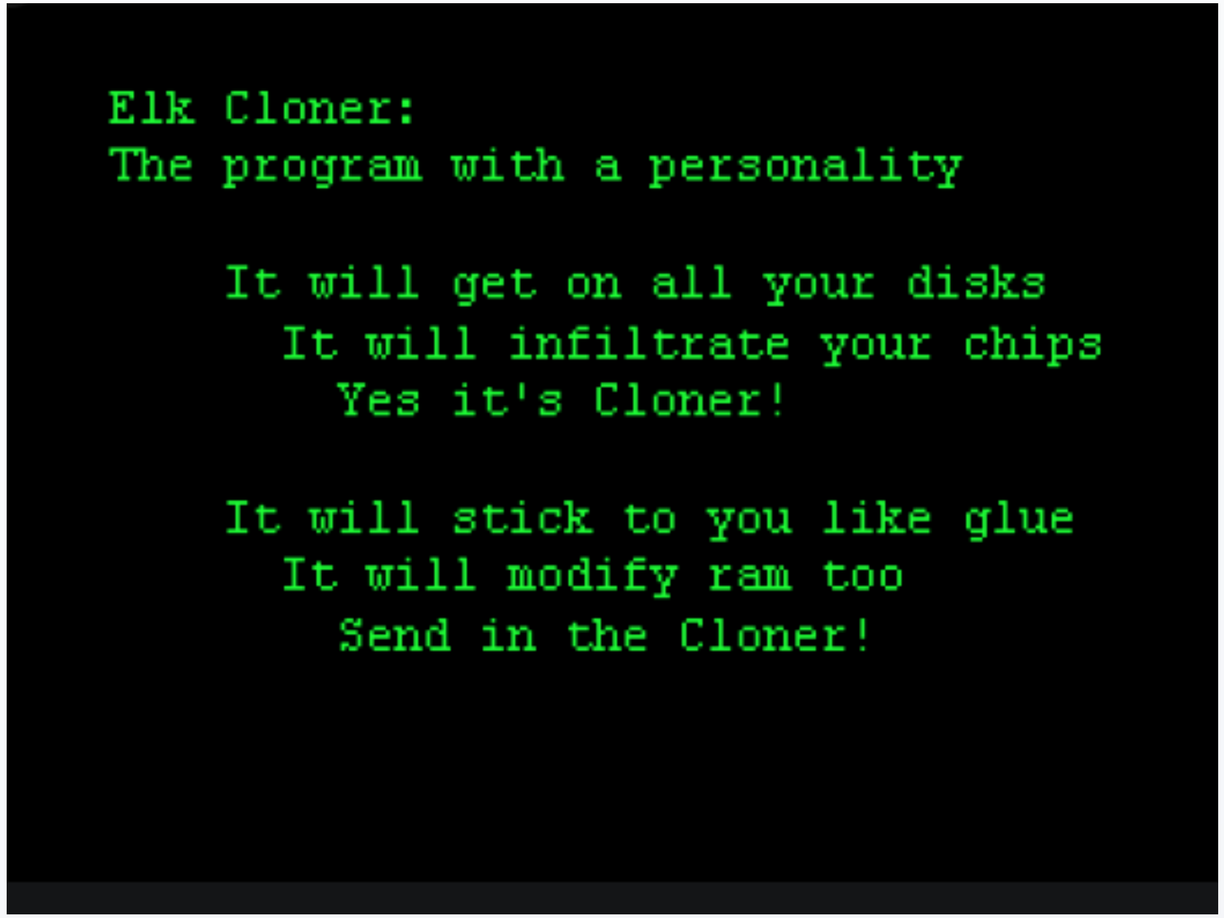
1982

Elk Cloner by Rich Skrenta

Apple DOS 3.3 - Apple II

The first appearance outside the single computer or lab where it was created.

It was a prank.



The first virus

1982

Elk Cloner by Rich Skrenta

Apple DOS 3.3 - Apple II

The first appearance outside the single computer or lab where it was created.

It was a prank.

jamf

The first virus

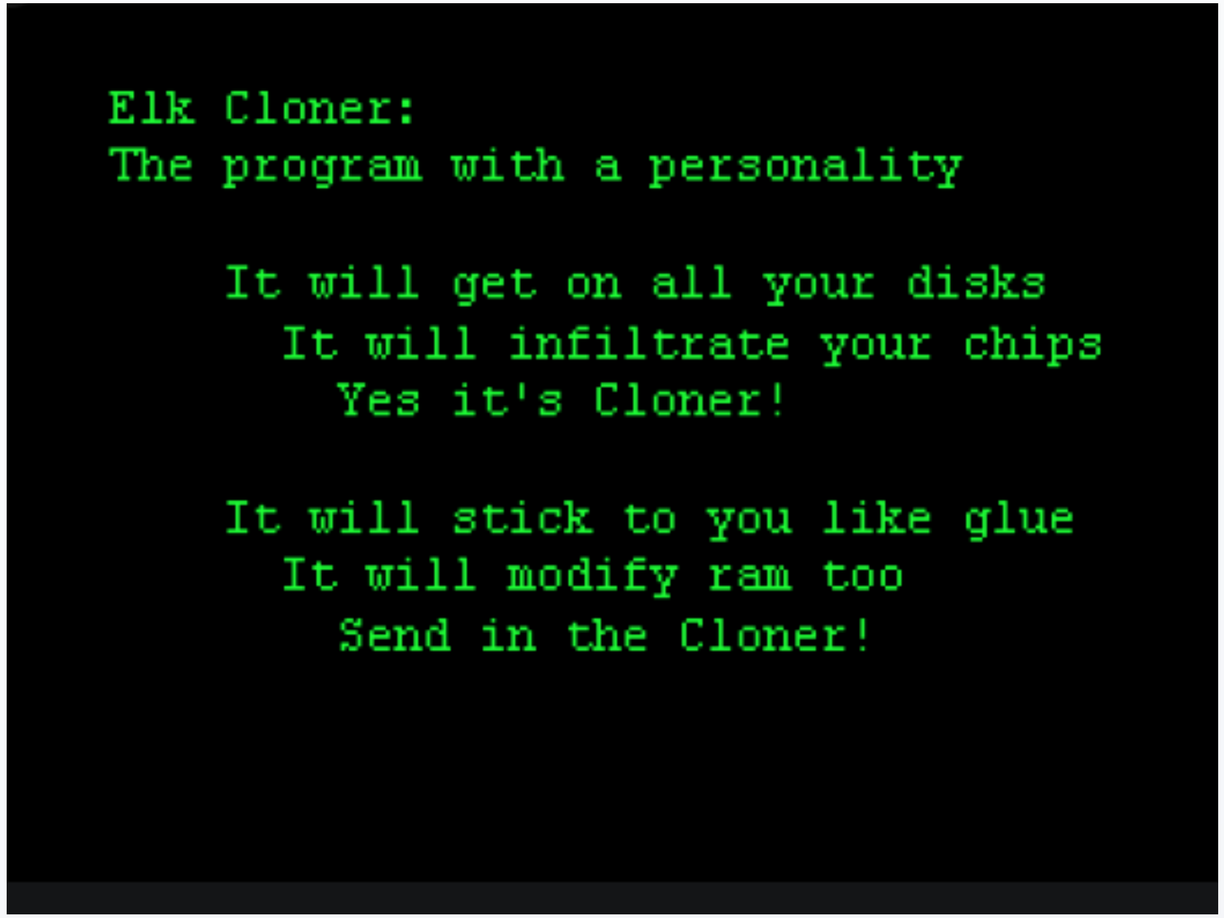
1982

Elk Cloner by Rich Skrenta

Apple DOS 3.3 - Apple II

The first appearance outside the single computer or lab where it was created.

It was a prank.



The first polymorphic & encrypted

SevenDust - 1988

Multiple mutations

SevenDust.B
added capabilities deleting all non-application files

SevenDust.C
has no payload
Polymorphic and Encrypted

```
Enclosed you will find my
custom Graphics Accelerator
that helps PPC macs speed
graphics programs up that
use 68K code. It uses a
custom blitting subroutine,
and it should work on PPC
apps as well. Please include
it in your Graphics/
Utilities directory. Thank
you very much.
```

The first backdoor

2004
Renepo

Trojan

First Mac backdoor

Extfiltrating data

```
#!/bin/bash
##############################################
##############################################
# opener 2.3.8 - a startup script to turn on
services and gather user info & hashes for Mac
OS X
##############################################
##############################################
# Originally written by DimBulb
# Additional code: JawnDoh!, Dr_Springfield,
g@pple
# Additional ideas and advice: Zo, BSDOSX
```

jamf

The first malware

2010
OpinionSpy

Essentially a tracker

7art screensavers

Believed to be
oldest Mac malware still
operating as of today!

jamf

Today

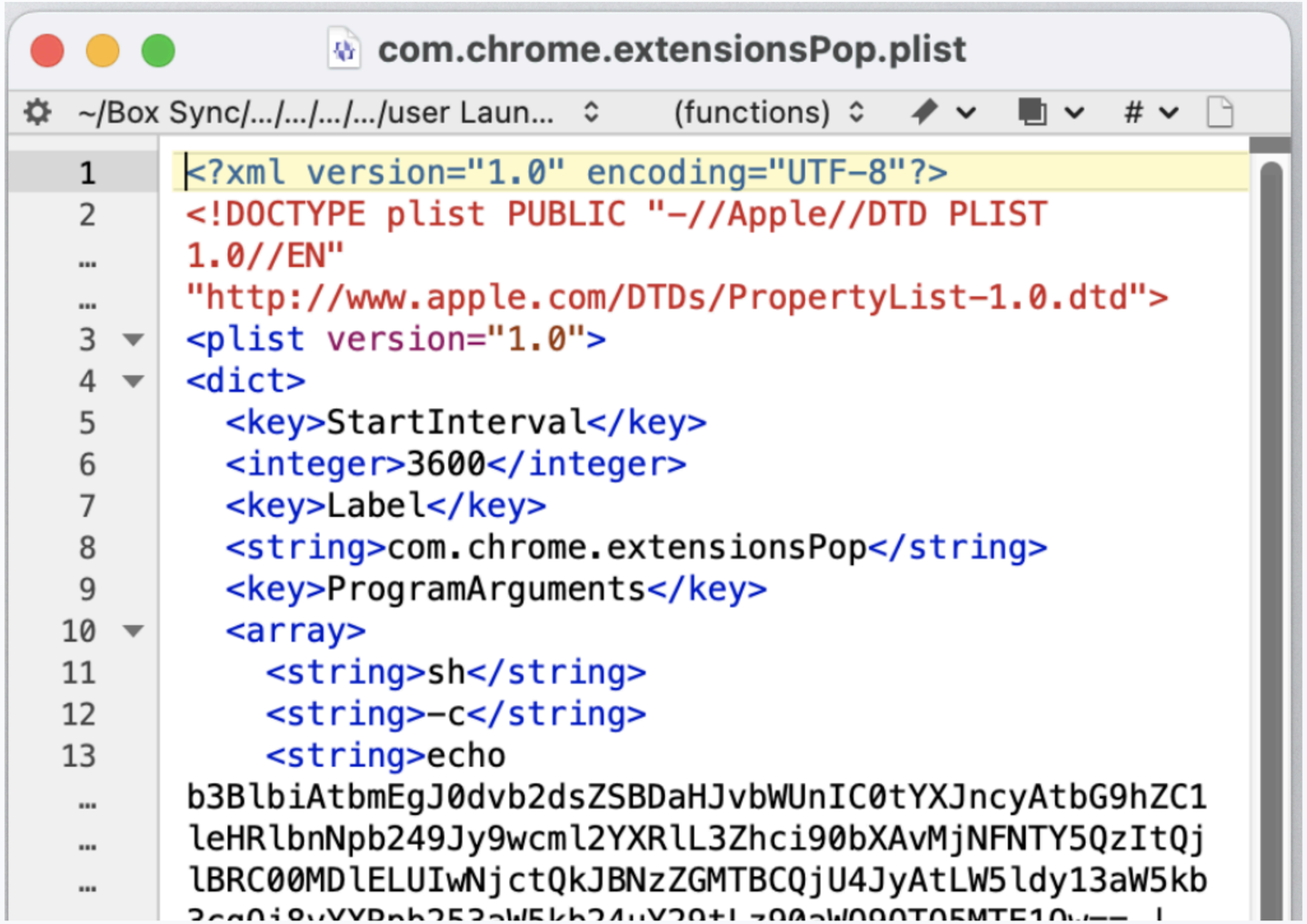
Obfuscation

Obfuscated shell scripts

Compiled AppleScript

Encryption

Payloadless



jamf

iOS

First iPhone:

29 June 2007

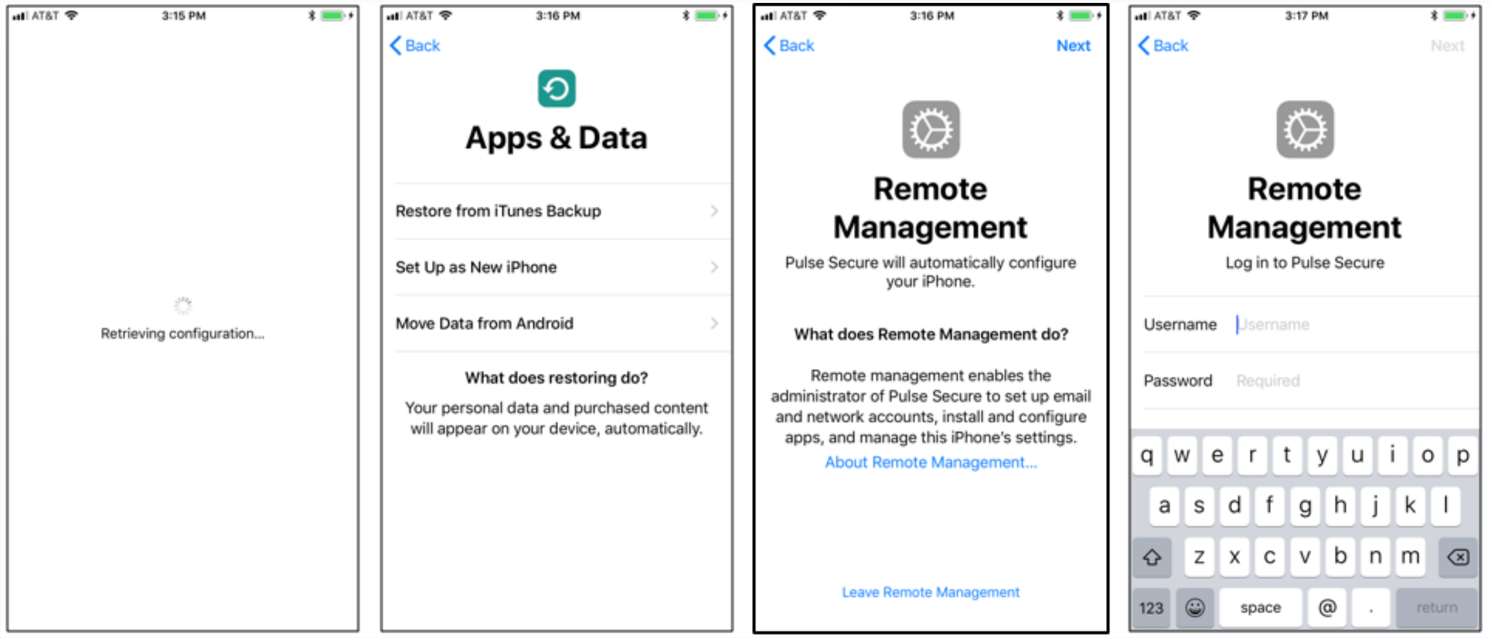
jamf

iOS

First iPhone:

29 June 2007

2010
iOS 4:
Enterprise iPhone
and iPad Administrator's
Guide



jamf

The first virus

2009
iKee

Worm

Jailbreak

jamf

The first virus

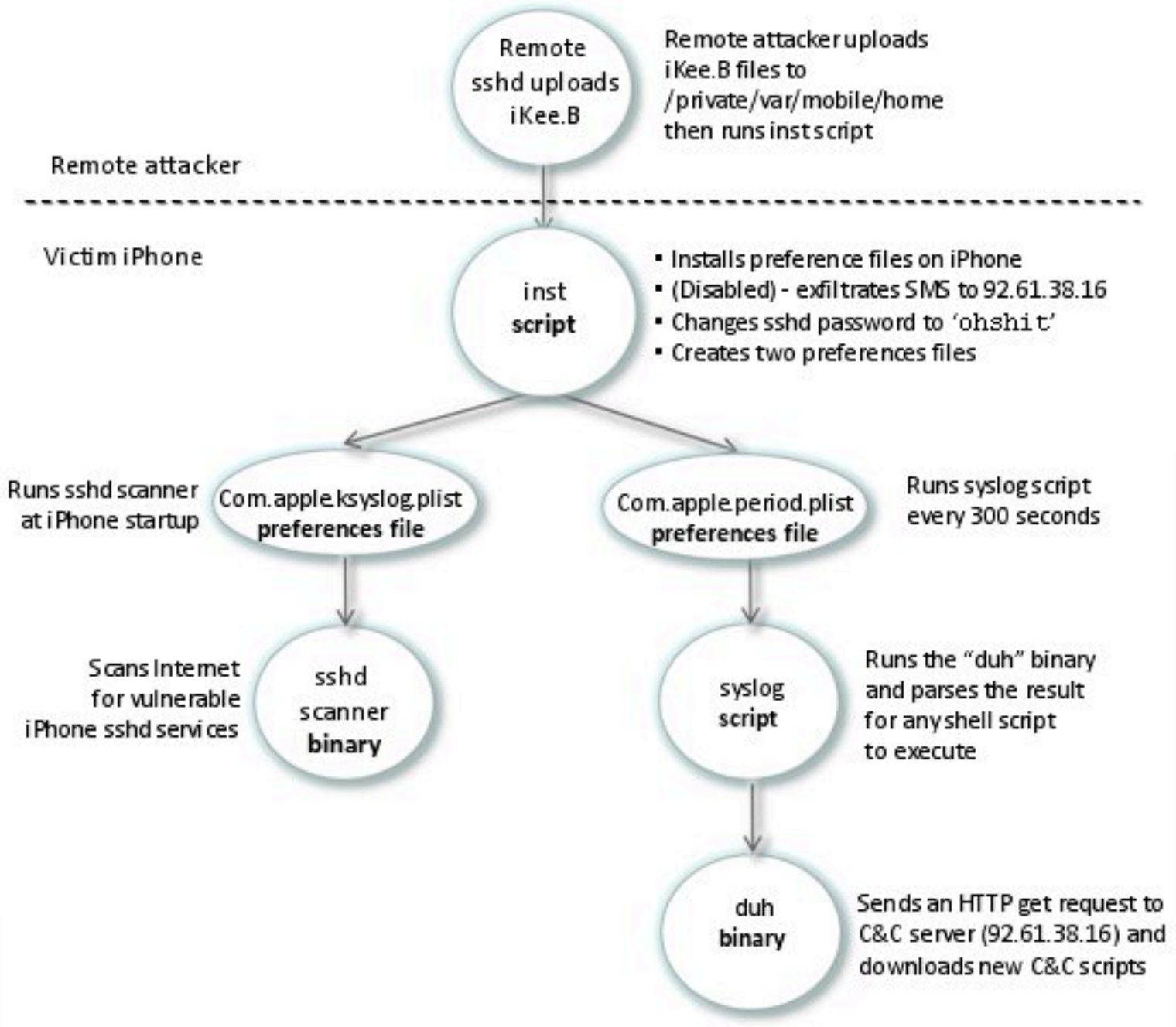
2009
iKee

Worm

Jailbreak

Change the lockscreen background to a photo of Rick Astley.

jamf


Remote sshd uploads iKee.B
Remote attacker uploads iKee.B files to /private/var/mobile/home then runs inst script
Remote attacker
Victim iPhone
inst script
▪ Installs preference files on iPhone
▪ (Disabled) - exfiltrates SMS to 92.61.38.16
▪ Changes sshd password to 'ohshit'
▪ Creates two preferences files
Runs sshd scanner at iPhone startup
Com.apple.ksyslog.plist preferences file
Com.apple.period.plist preferences file
Runs syslog script every 300 seconds
Scans Internet for vulnerable iPhone sshd services
sshd scanner binary
syslog script
Runs the "duh" binary and parses the result for any shell script to execute
duh binary
Sends an HTTP get request to C&C server (92.61.38.16) and downloads new C&C scripts

jamf

The first trojan

2012
Find and Call

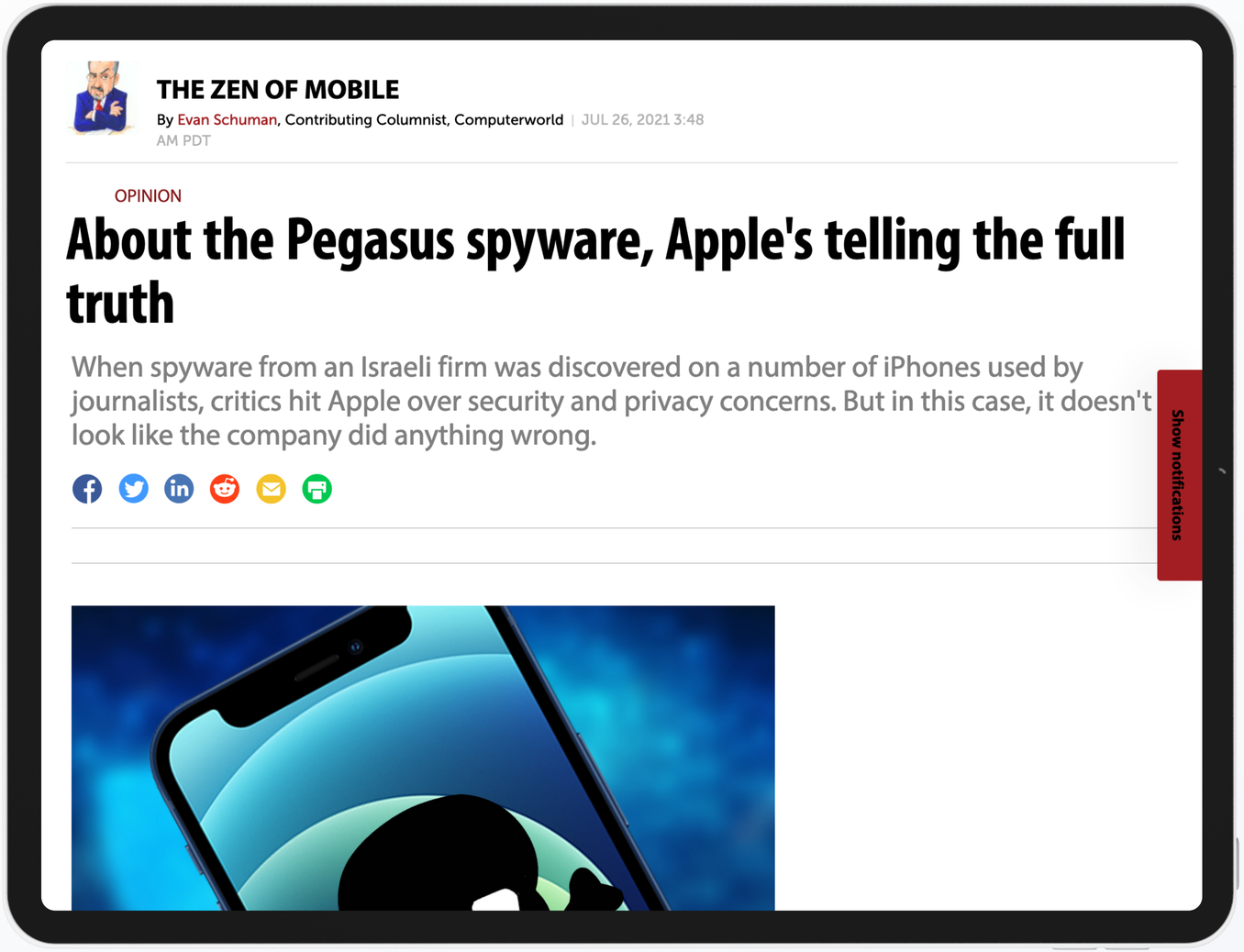
Delivered via App Store

Upload Contacts to remote server

SMS spam

jamf

Today



THE ZEN OF MOBILE

By Evan Schuman, Contributing Columnist, Computerworld | JUL 26, 2021 3:48 AM PDT

OPINION

About the Pegasus spyware, Apple's telling the full truth

When spyware from an Israeli firm was discovered on a number of iPhones used by journalists, critics hit Apple over security and privacy concerns. But in this case, it doesn't look like the company did anything wrong.

Show notifications

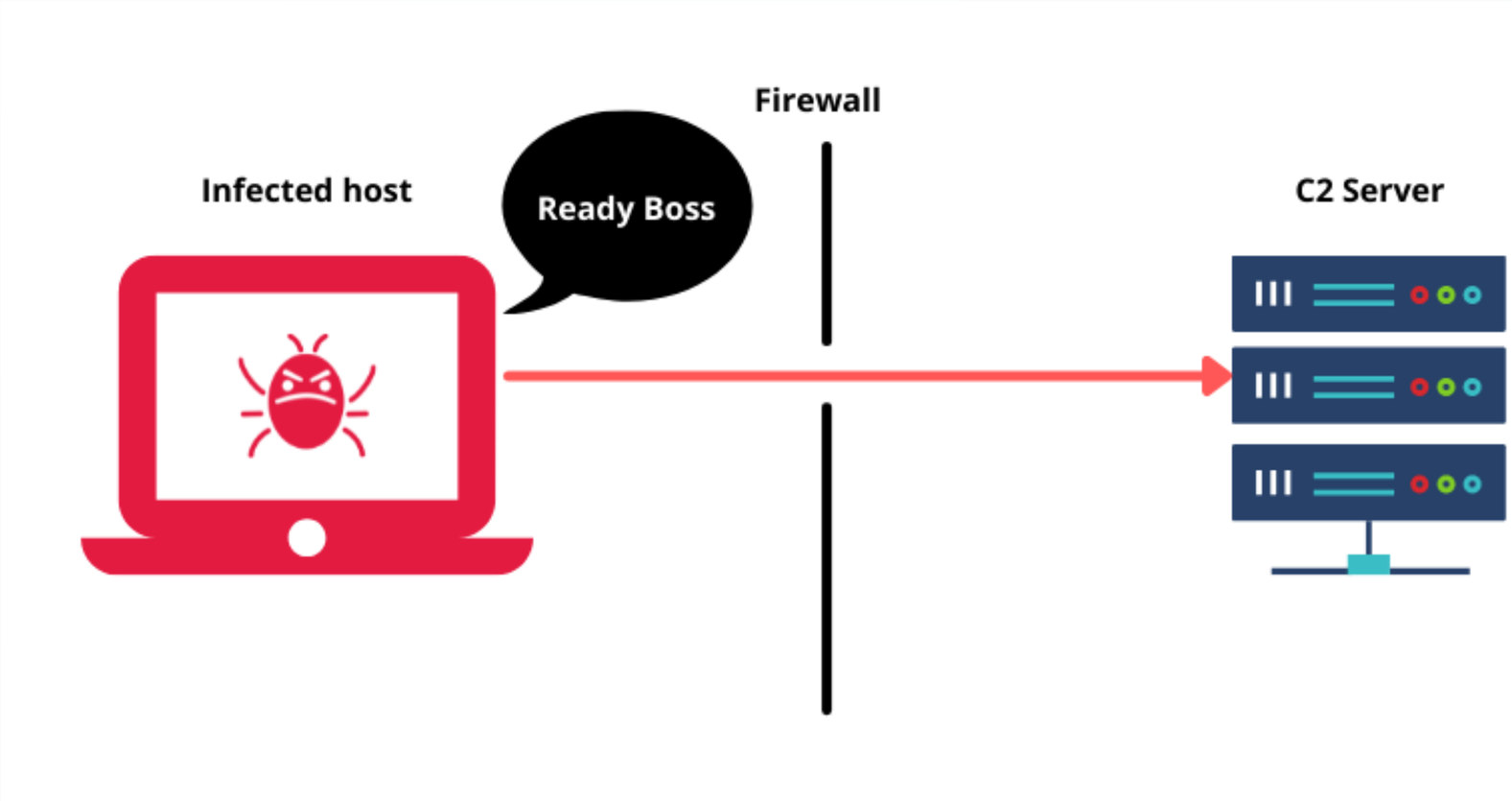
jamf

Back to Mac

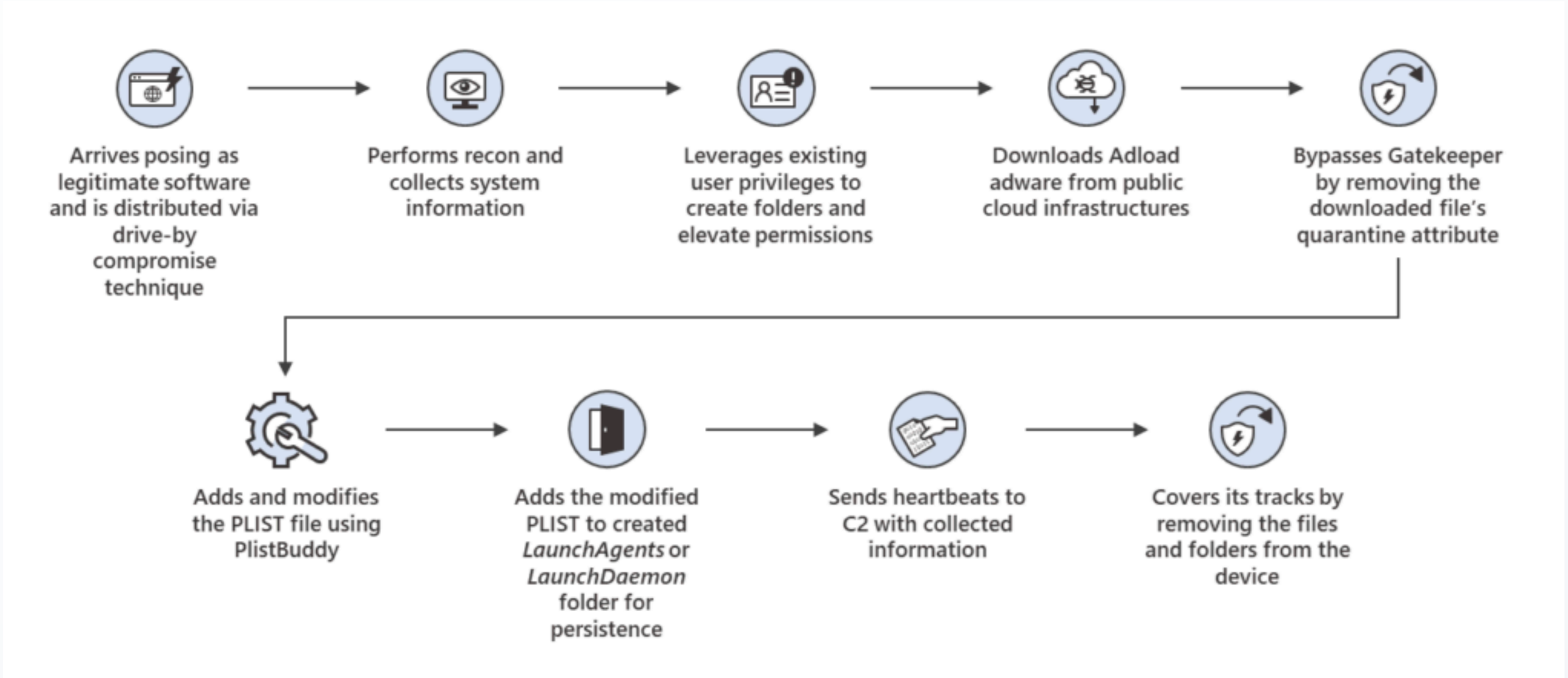
Jamf Protect on-device

Malware is becoming payload less

C2 servers

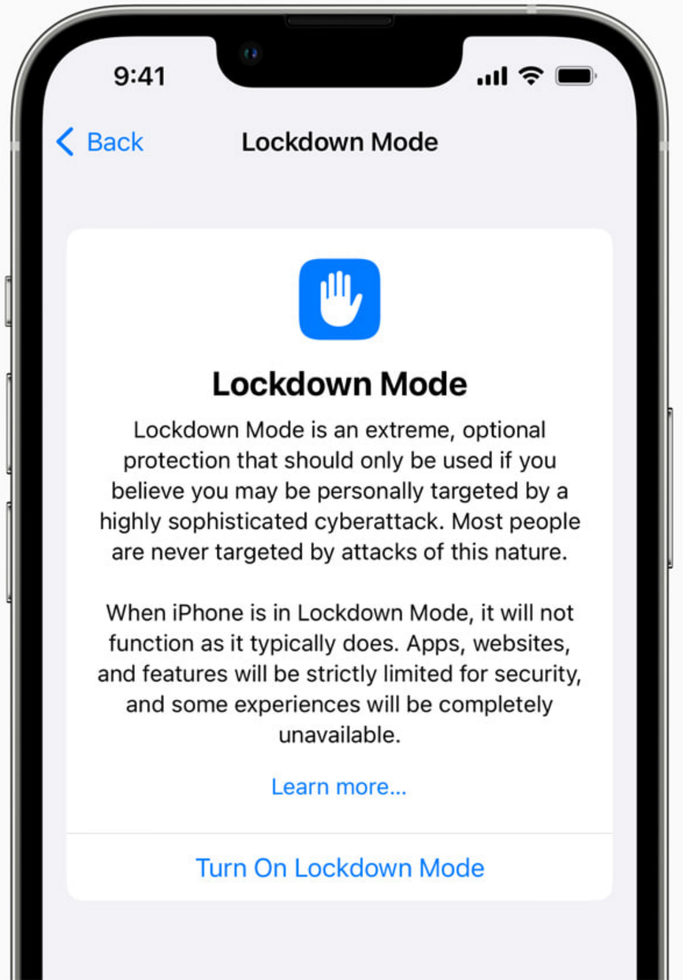


UserAgent



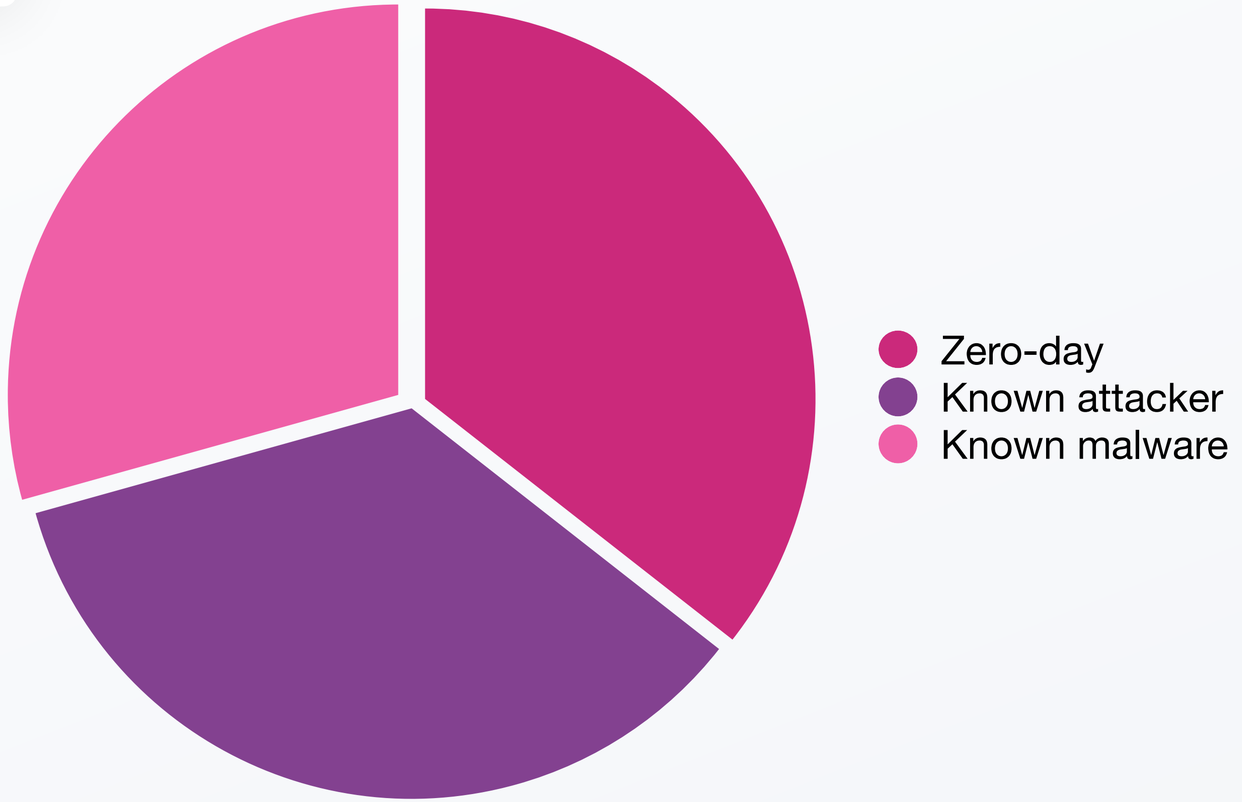
jamf

Empower users



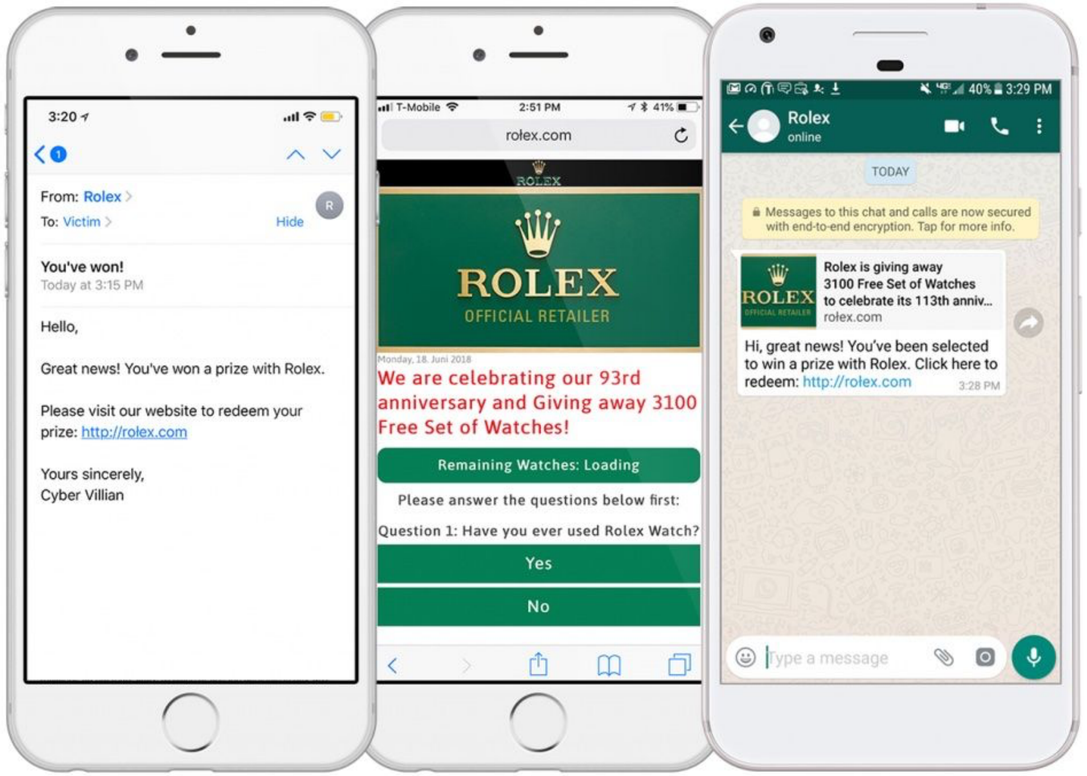
jamf

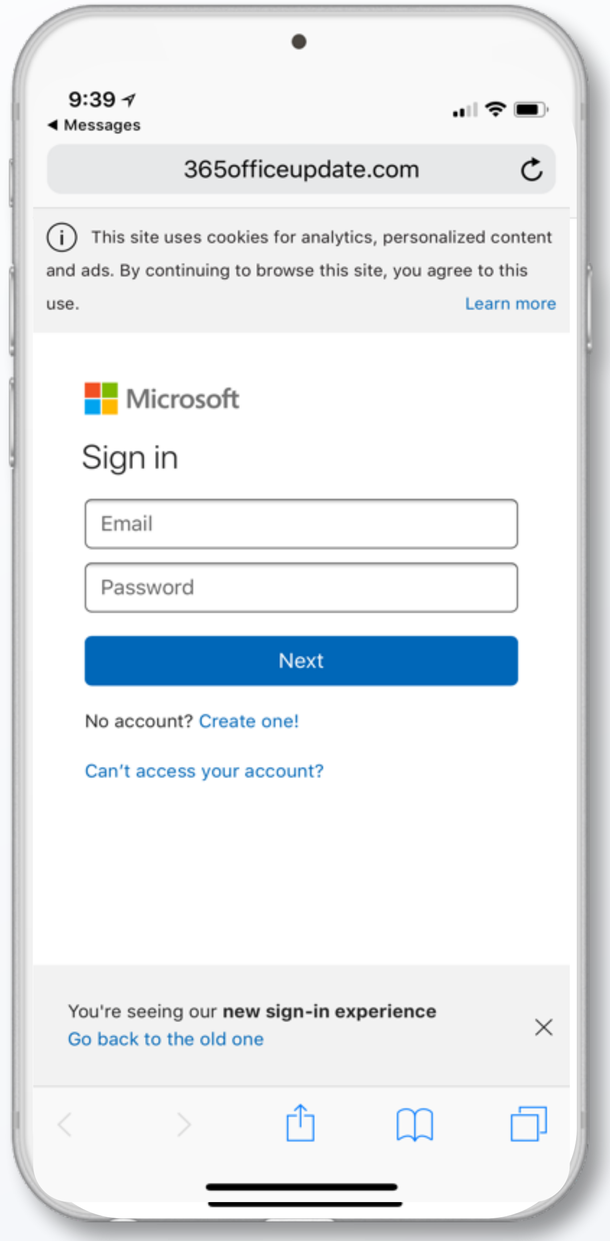
Only one-third of malware samples extracted from customer environments were previously-known



Mobile is **not risk-free**

Mobile users face more threats as the enterprise perimeter falls

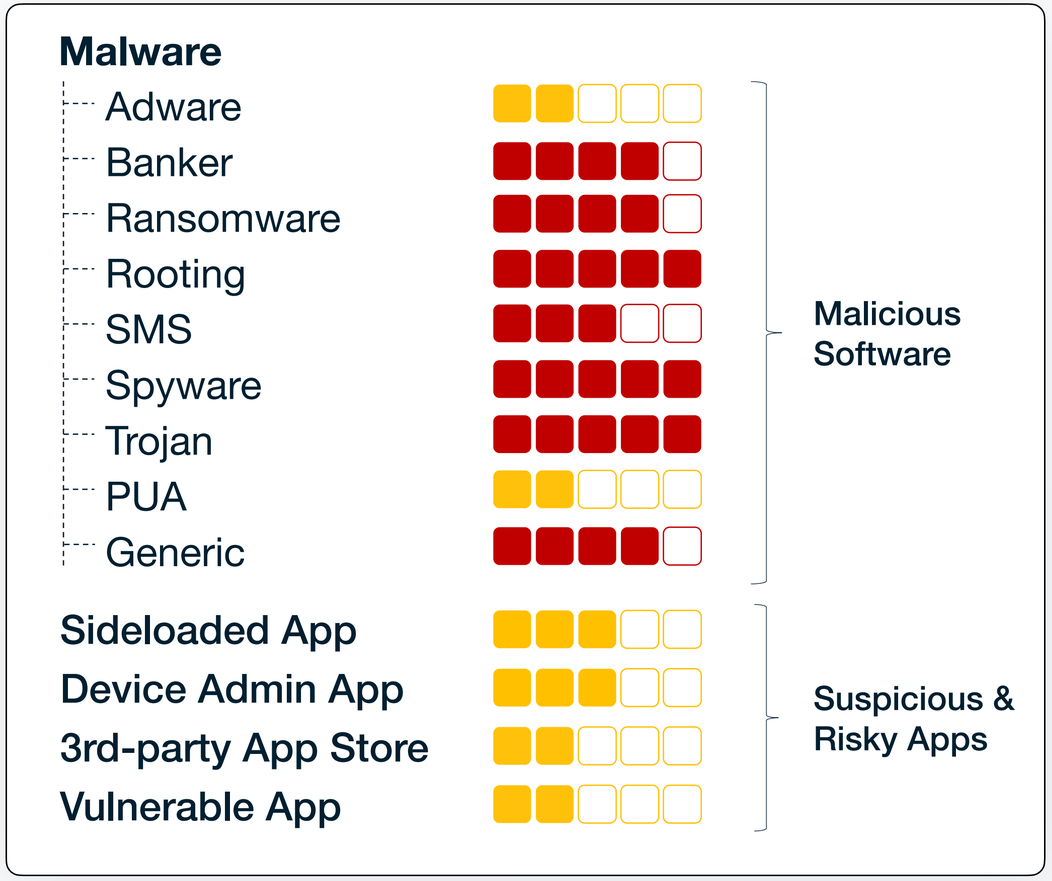


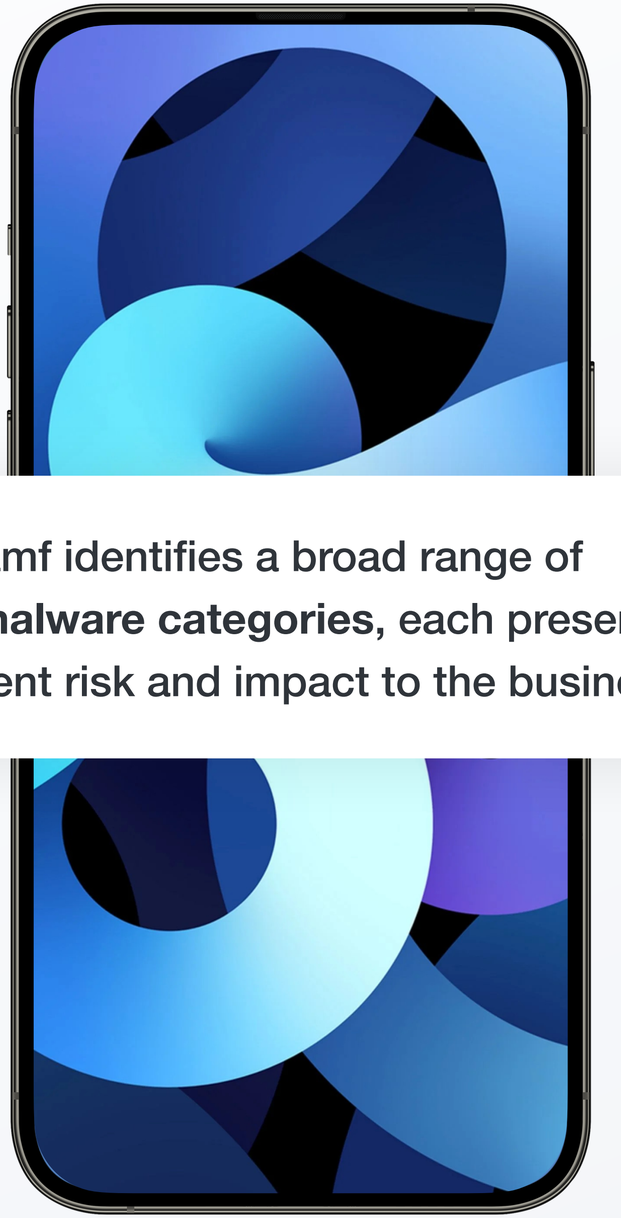


jamf

Mobile is **not risk-free**

Mobile users face more threats as the enterprise perimeter falls





Jamf identifies a broad range of **mobile malware categories**, each presenting a different risk and impact to the business

jamf


That's all Folks!