Cyber Security in a World with Professional Attackers

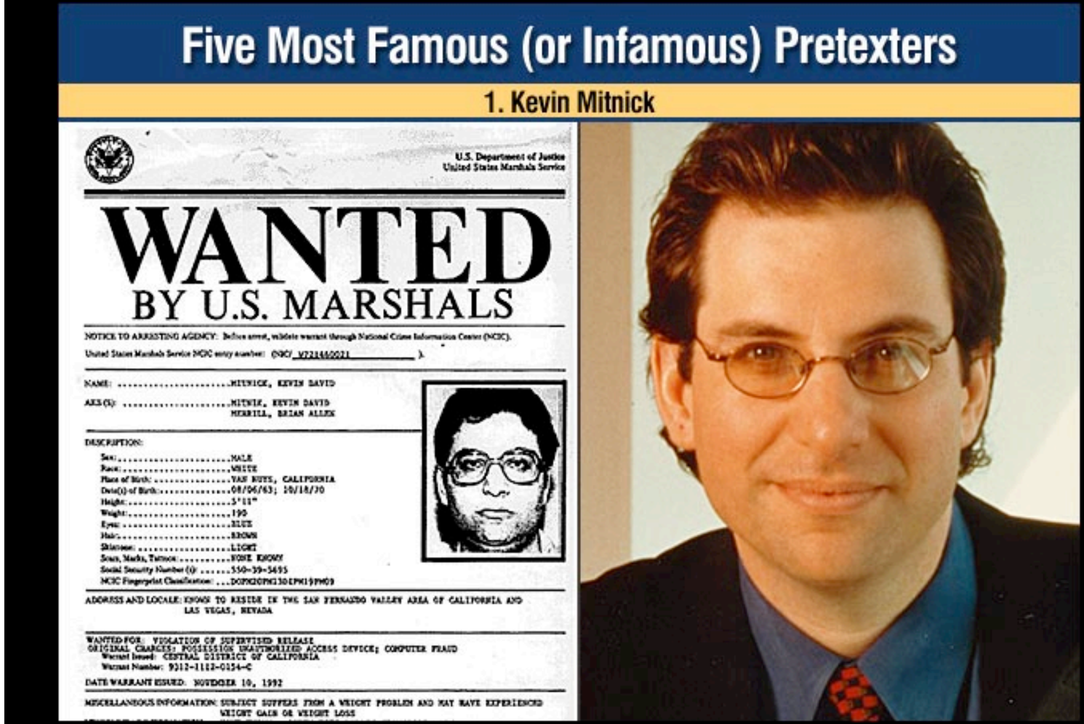
Todd Heberlein
Net Squared, Inc.
19 OCT 2012

ISSA Sacramento
http://www.issa-sac.org/meetings/index.php?View=2012101901

Overview

- Today’s emerging threat environment
- We are failing
- Glowing Embers
- Crossing the air gap
- Thoughts on “Advanced Persistent Threats”
- Google, the APT you have

Today’s Emerging Threat Environment



Five Most Famous (or Infamous) Pretexters

1. Kevin Mitnick

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM130IPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND
LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1122-0154-C

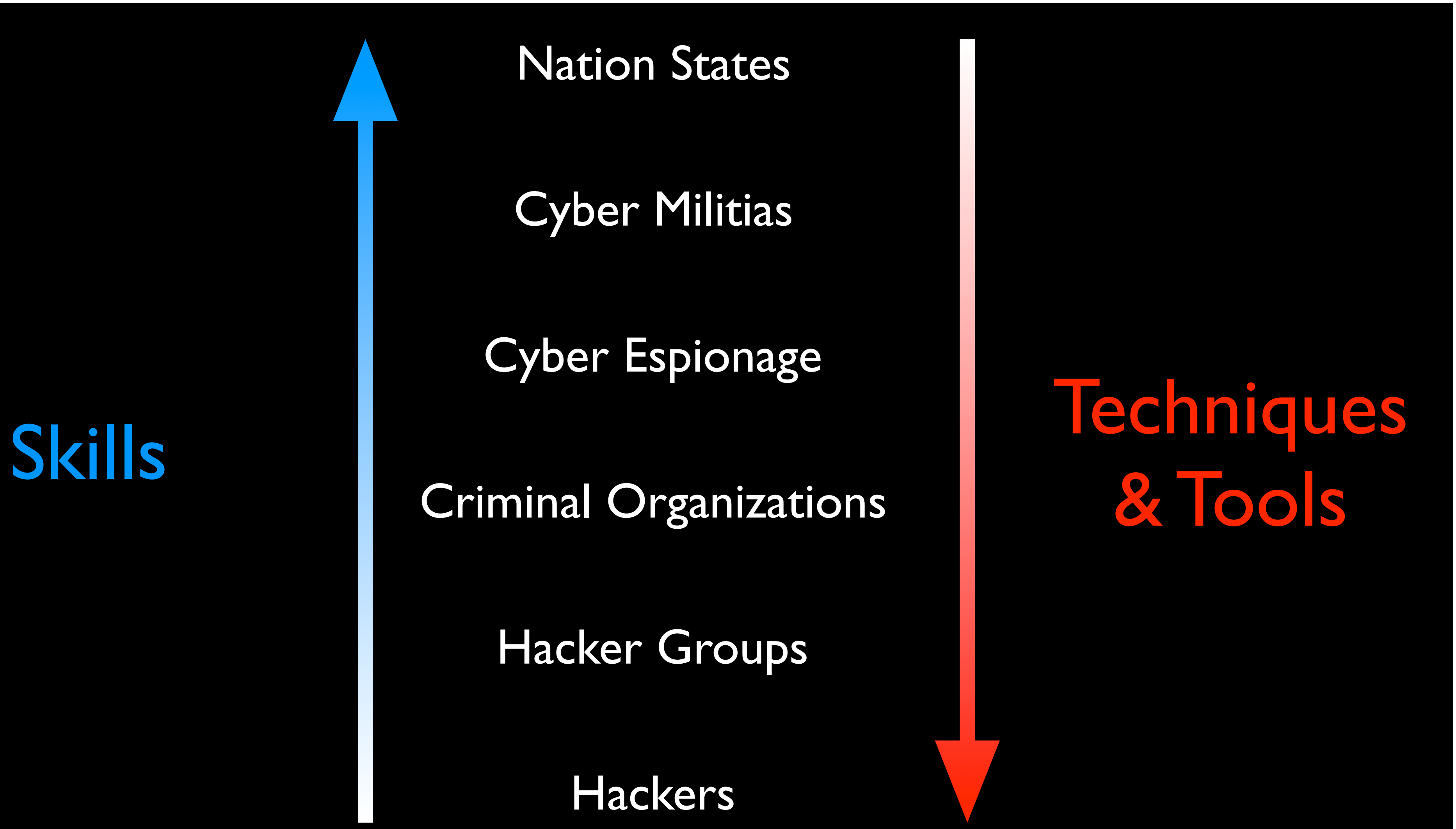
DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED
WEIGHT GAIN OR WEIGHT LOSS

UNITED STATES CYBER COMMAND
9ec4c12949a4f31474f299058ce2b22a

Yesterday's APT

Today's APT



Skills

Nation States

Cyber Militias

Cyber Espionage

Criminal Organizations

Hacker Groups

Hackers

Techniques & Tools

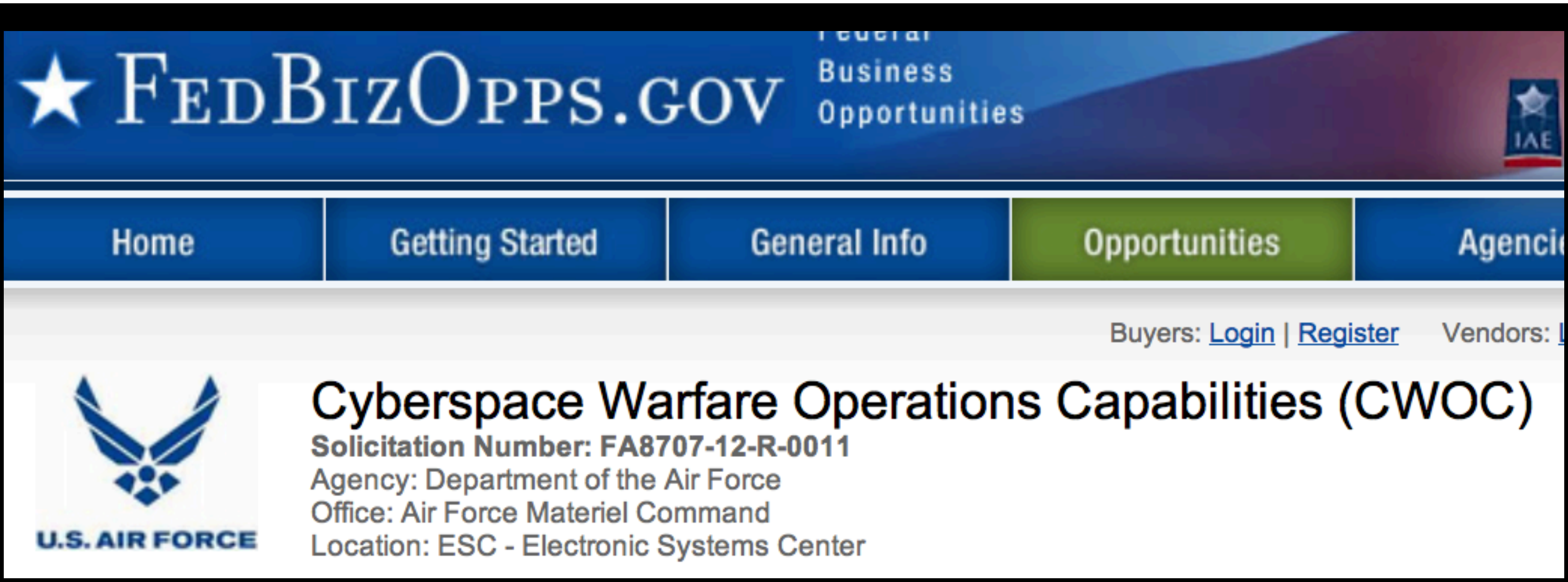
When sophisticated organizations conduct attacks, at some point the attack is captured and analyzed

Google: stuxnet analysis

flame analysis

gauss malware analysis

These analyses create blueprints and teach techniques for building future threats



Buyers: Login | Register Vendors: L

Cyberspace Warfare Operations Capabilities (CWOC)

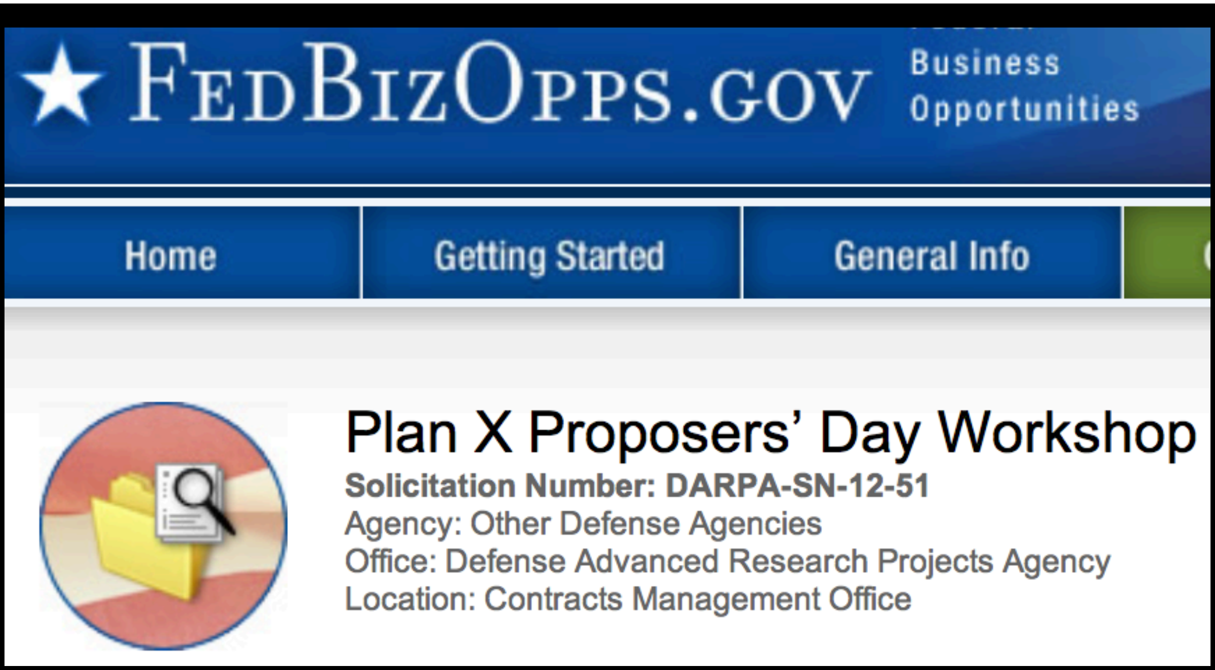
Solicitation Number: FA8707-12-R-0011

Agency: Department of the Air Force

Office: Air Force Materiel Command

Location: ESC - Electronic Systems Center

Technical Description: The ESC/HSJG Program Office is an organization focused on the development and sustainment of Cyberspace Warfare Attack capabilities that directly support Cyberspace Warfare capabilities for the operational Air Force.



Plan X Proposers' Day Workshop

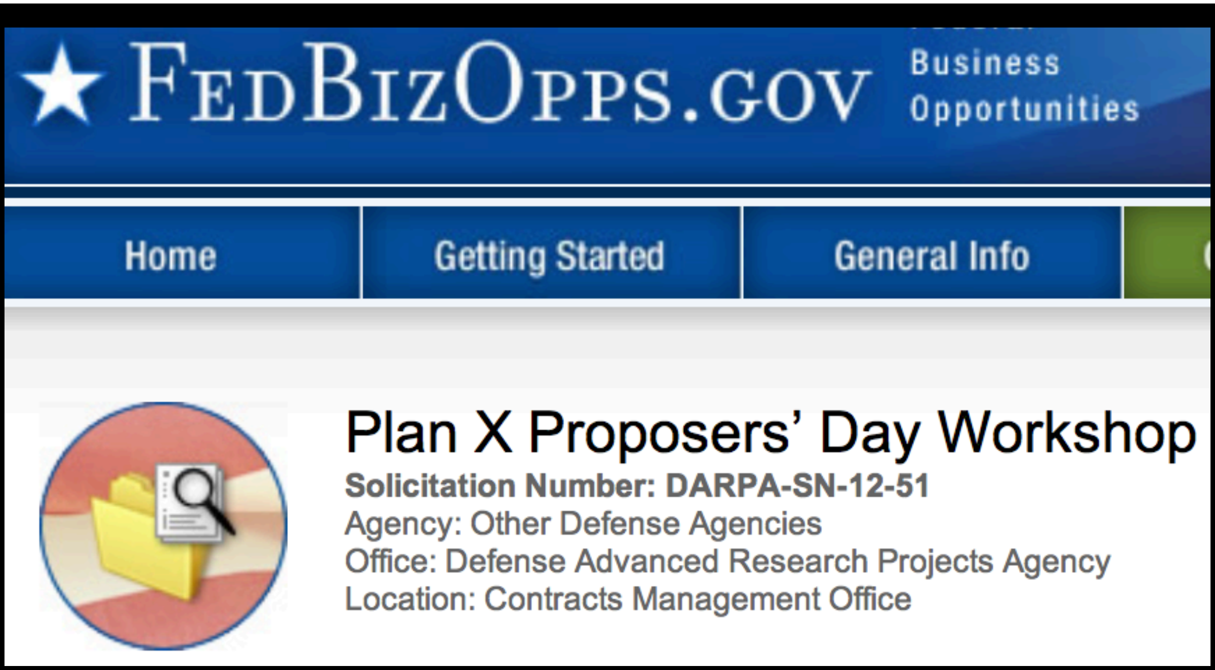
Solicitation Number: DARPA-SN-12-51

Agency: Other Defense Agencies

Office: Defense Advanced Research Projects Agency

Location: Contracts Management Office

The objective of the Plan X program is to create revolutionary technologies for understanding, planning, and managing cyberwarfare in real-time, large-scale, and dynamic network environments.



Plan X Proposers’ Day Workshop

Solicitation Number: DARPA-SN-12-51
Agency: Other Defense Agencies
Office: Defense Advanced Research Projects Agency
Location: Contracts Management Office

Please note that the Plan X Proposers' Day Workshop has been rescheduled to 15 and 16 October 2012, due to an unanticipated and overwhelming response from industry and academia.

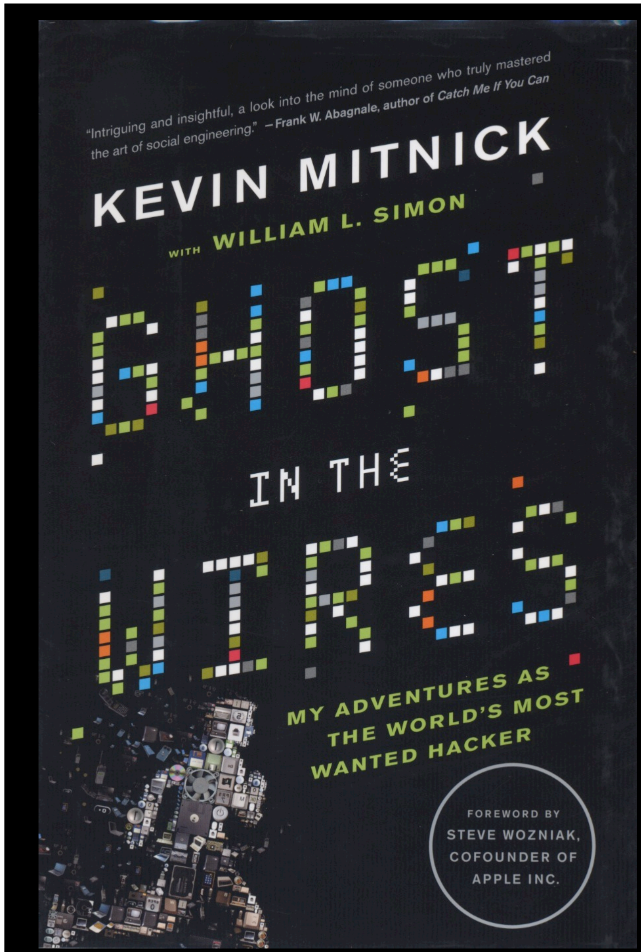
Do you think business and national adversaries aren’t doing the same thing?

This is the reality that we need to prepare ourselves for.

What the most advanced nation states are capable of today

are what you should expect to see tomorrow

Recommended readings



"Intriguing and insightful, a look into the mind of someone who truly mastered the art of social engineering." —Frank W. Abagnale, author of *Catch Me If You Can*

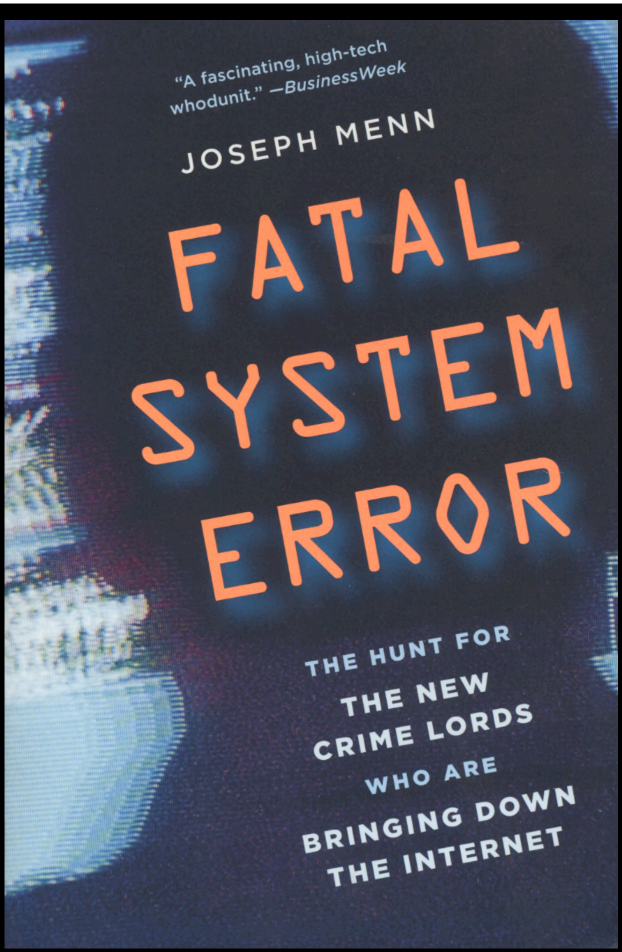
KEVIN MITNICK

WITH WILLIAM L. SIMON

GHOST IN THE WIRES

MY ADVENTURES AS THE WORLD'S MOST WANTED HACKER

FOREWORD BY STEVE WOZNIAK, COFOUNDER OF APPLE INC.

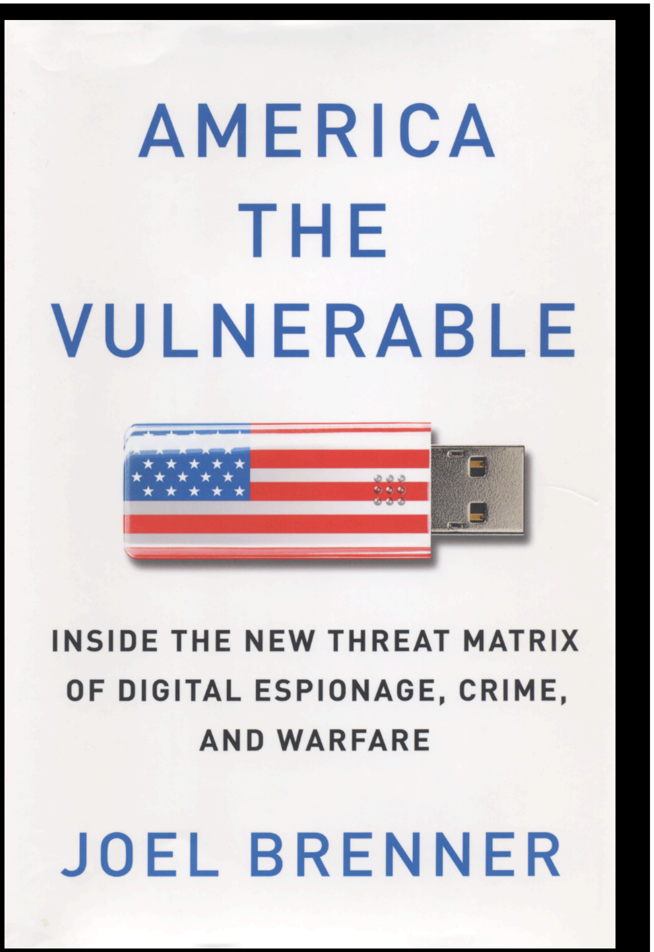


"A fascinating, high-tech whodunit." —*BusinessWeek*

JOSEPH MENN

FATAL SYSTEM ERROR

THE HUNT FOR THE NEW CRIME LORDS WHO ARE BRINGING DOWN THE INTERNET



AMERICA THE VULNERABLE

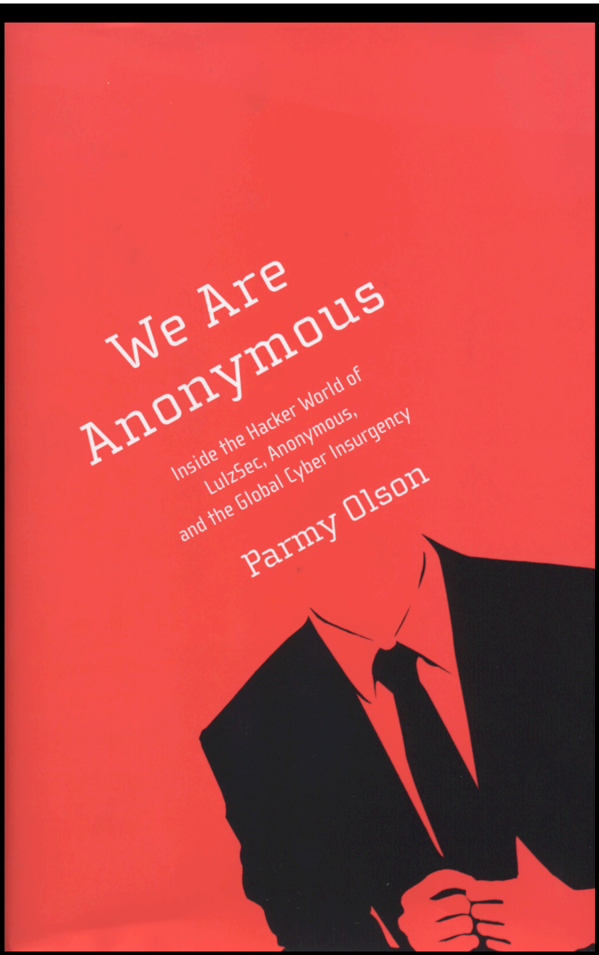
INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER

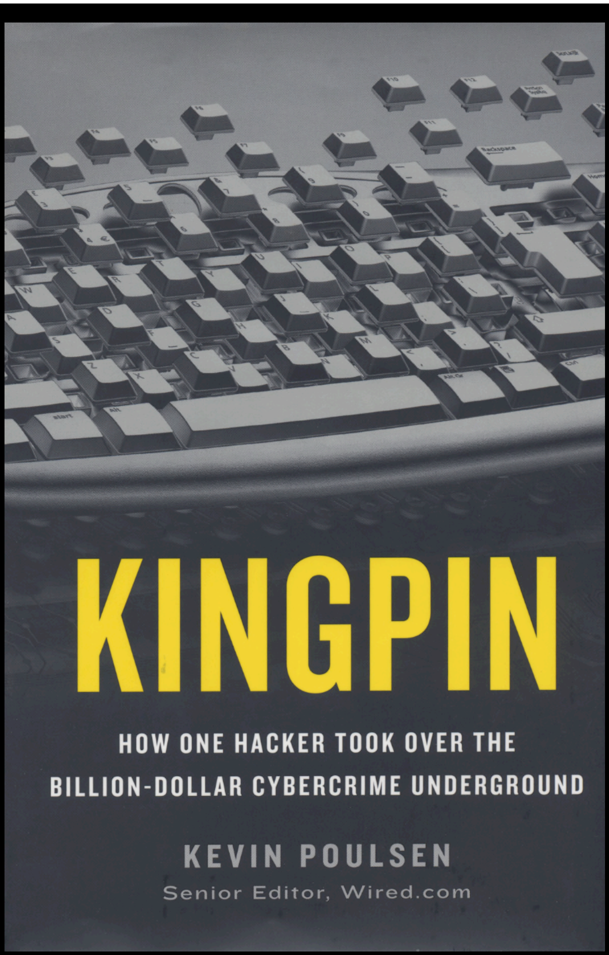
Hackers

Cyber Crime

Cyber Warfare


We Are Anonymous
Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency
Parmy Olson

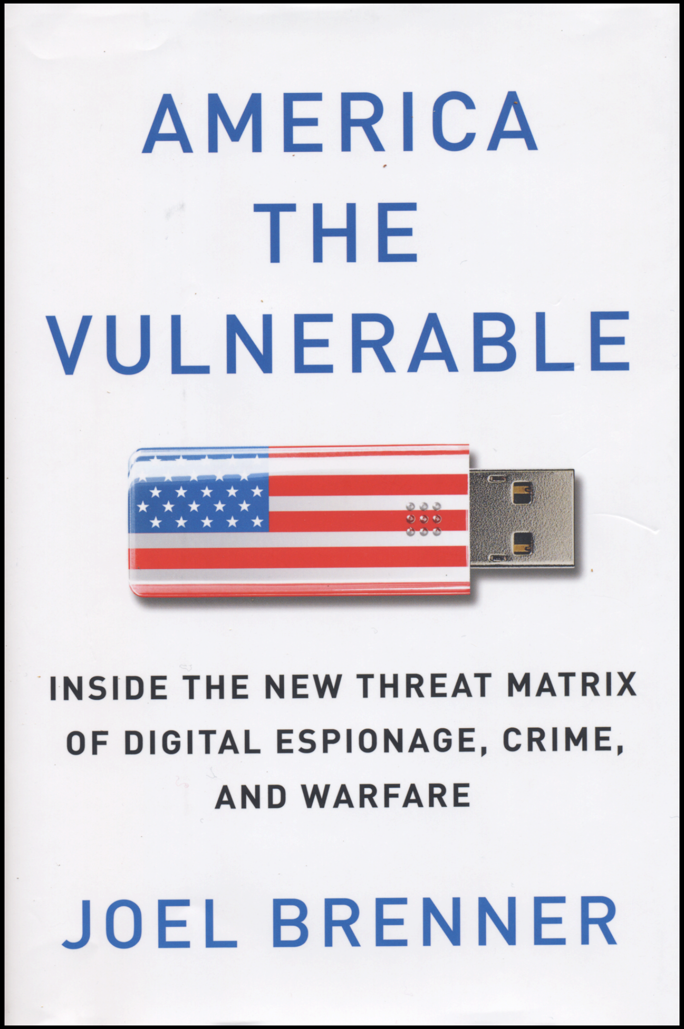
Hackers


KINGPIN
HOW ONE HACKER TOOK OVER THE BILLION-DOLLAR CYBERCRIME UNDERGROUND
KEVIN POULSEN
Senior Editor, Wired.com

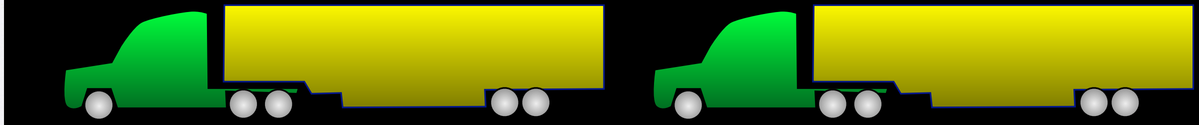
Cyber Crime

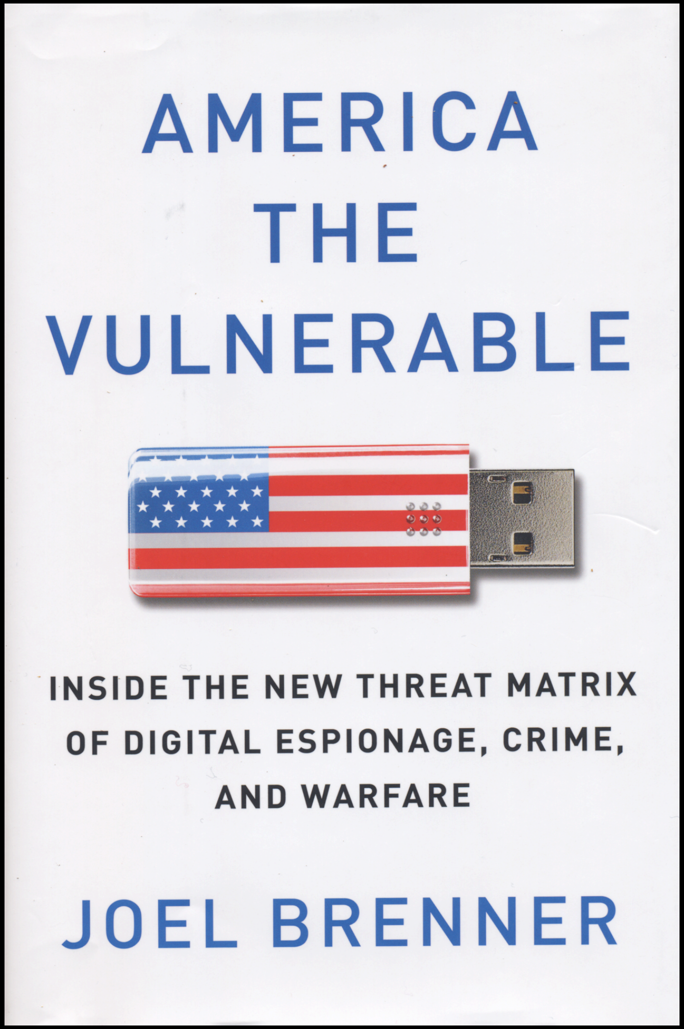
We are currently failing

> *"It's the greatest transfer of wealth in history."*
>
> – General Keith Alexander,
> Commander, U.S. Cyber Command


AMERICA THE VULNERABLE
INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE
JOEL BRENNER

In August 2006, Major General William Lord of the Air Force let the public in on the secret when he mentioned that massive heist of up to twenty terabytes.

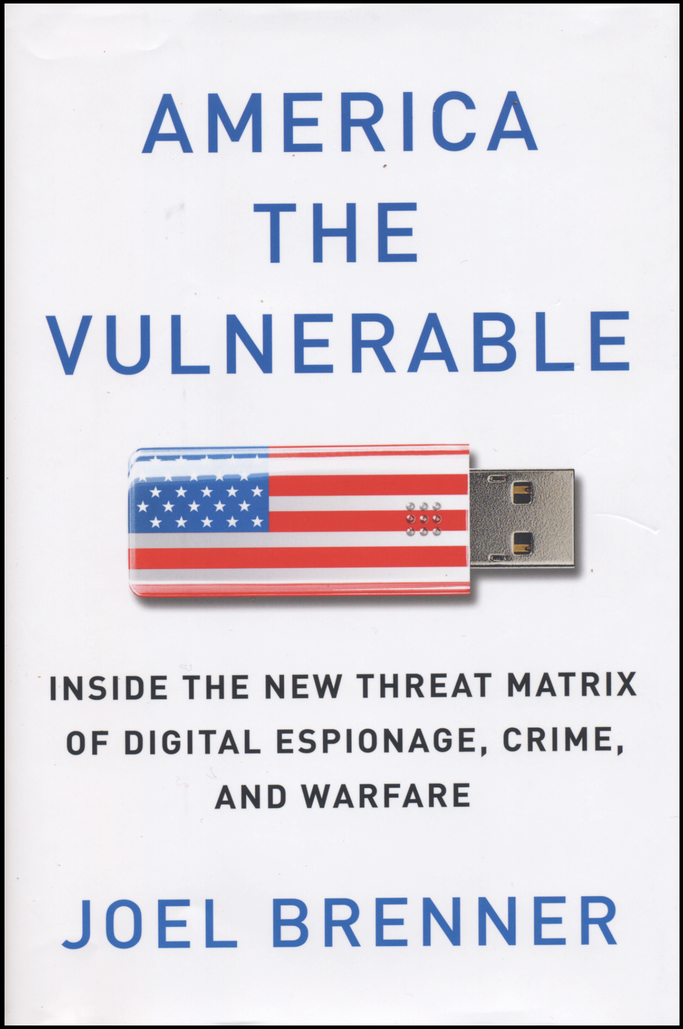




AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

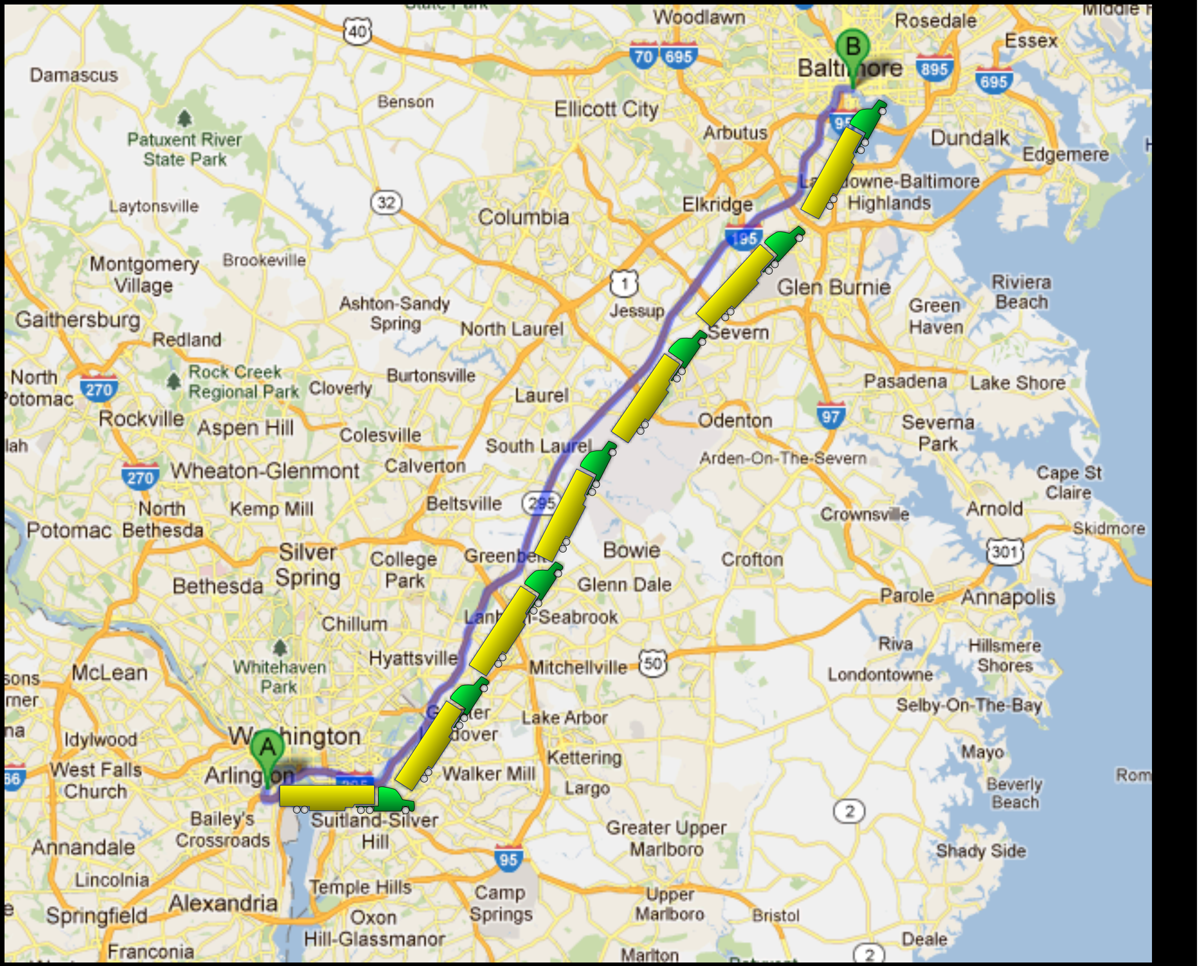
JOEL BRENNER



AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER



“It’s the greatest transfer of wealth in history.”

– General Keith Alexander,
Commander, U.S. Cyber Command

“There are two existential threats to the United States of America. One is the nuclear weapons that the Russians have. ...The other existential threat is cyber.”

– Admiral Mike Mullen, the former Chairman
of the Joint Chiefs of Staff

Market maturity:	20-25 years
Market size:	$70 Billion
Annual losses:	$200-1000 Billion

“stop spending on technology that doesn’t work. Investments in legacy security standbys (hello AV, firewalls et. al.) need to be tempered” and “Signature-based defenses don’t work anymore”

– Peter Kuper of In-Q-Tel

“Signature-based malware detection has been limping along on life support for years, yet vendors seem unwilling to aggressively invest in more-effective solutions, preferring to ‘tweak’ the existing paradigm”

– Gartner

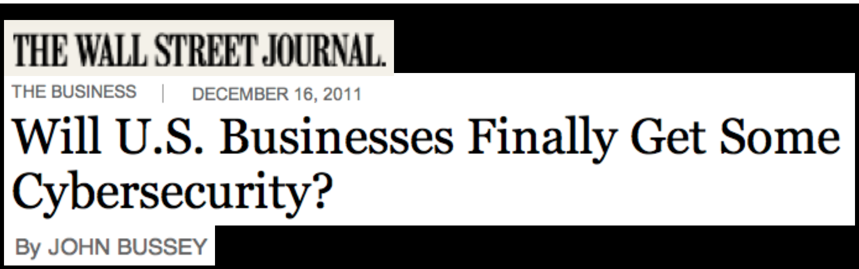
> “The security industry's going to have to think about selling solutions that actually work with this type of environment. ... Basically nothing that people have bought over the last 16 years is going to help”
>
> – Alex Stamos of Isec Partners

Why is the cyber security market in chaos?

The rise of professional attackers

Professional attackers have broken the security industry’s business model

- Subscription model
- Signatures have recurring value
- Signatures deployed before most attacks
- Detection is automated & binary



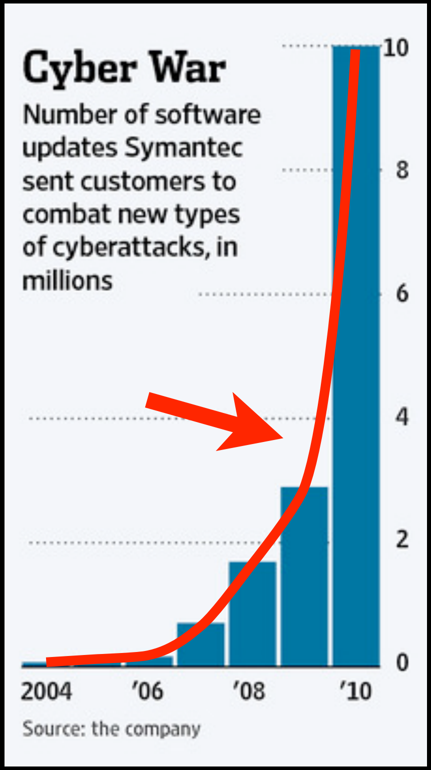
THE WALL STREET JOURNAL.

THE BUSINESS | DECEMBER 16, 2011

Will U.S. Businesses Finally Get Some Cybersecurity?

By JOHN BUSSEY

Symantec estimates about 55,000 new pieces of malware are created each day

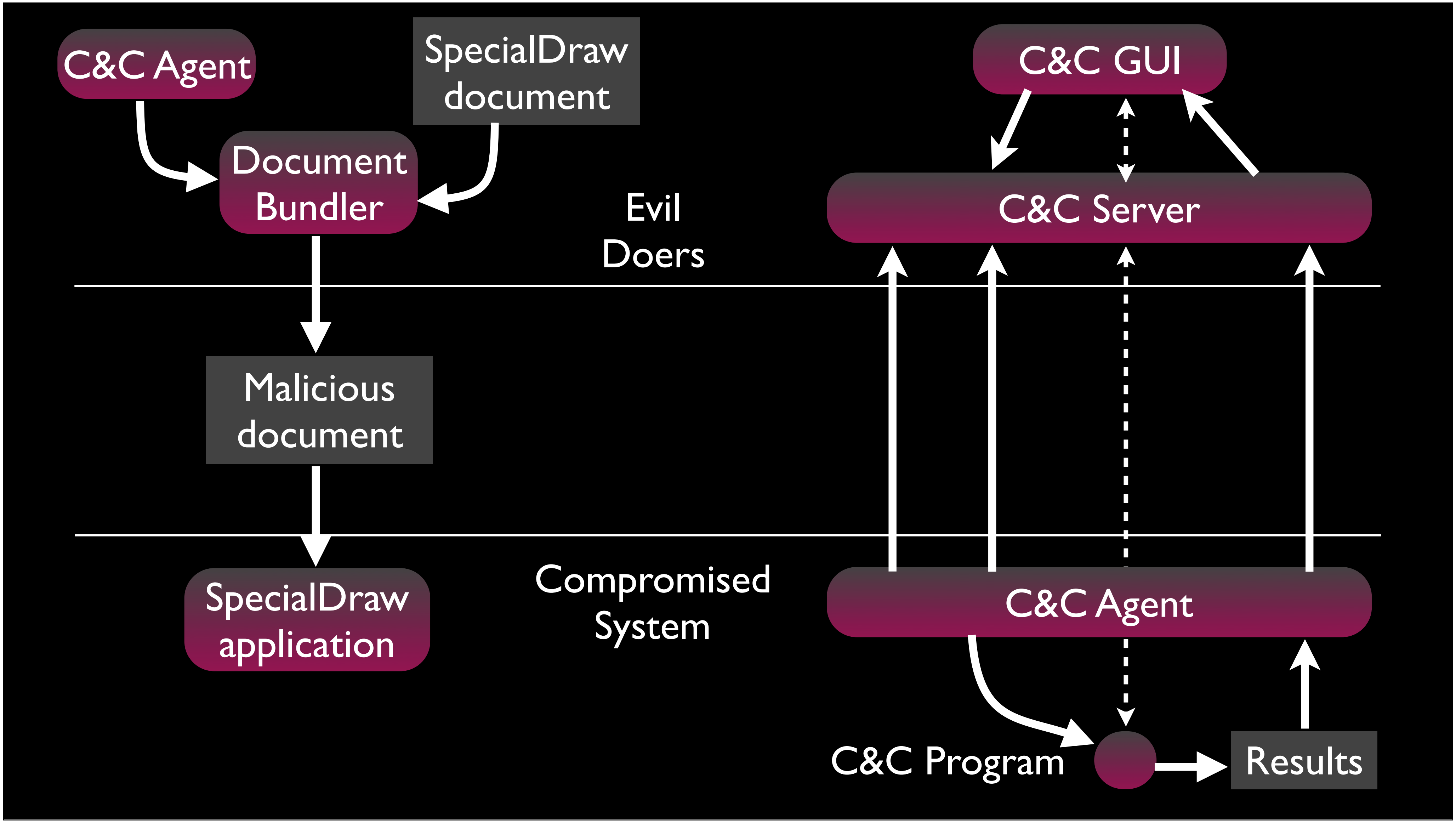


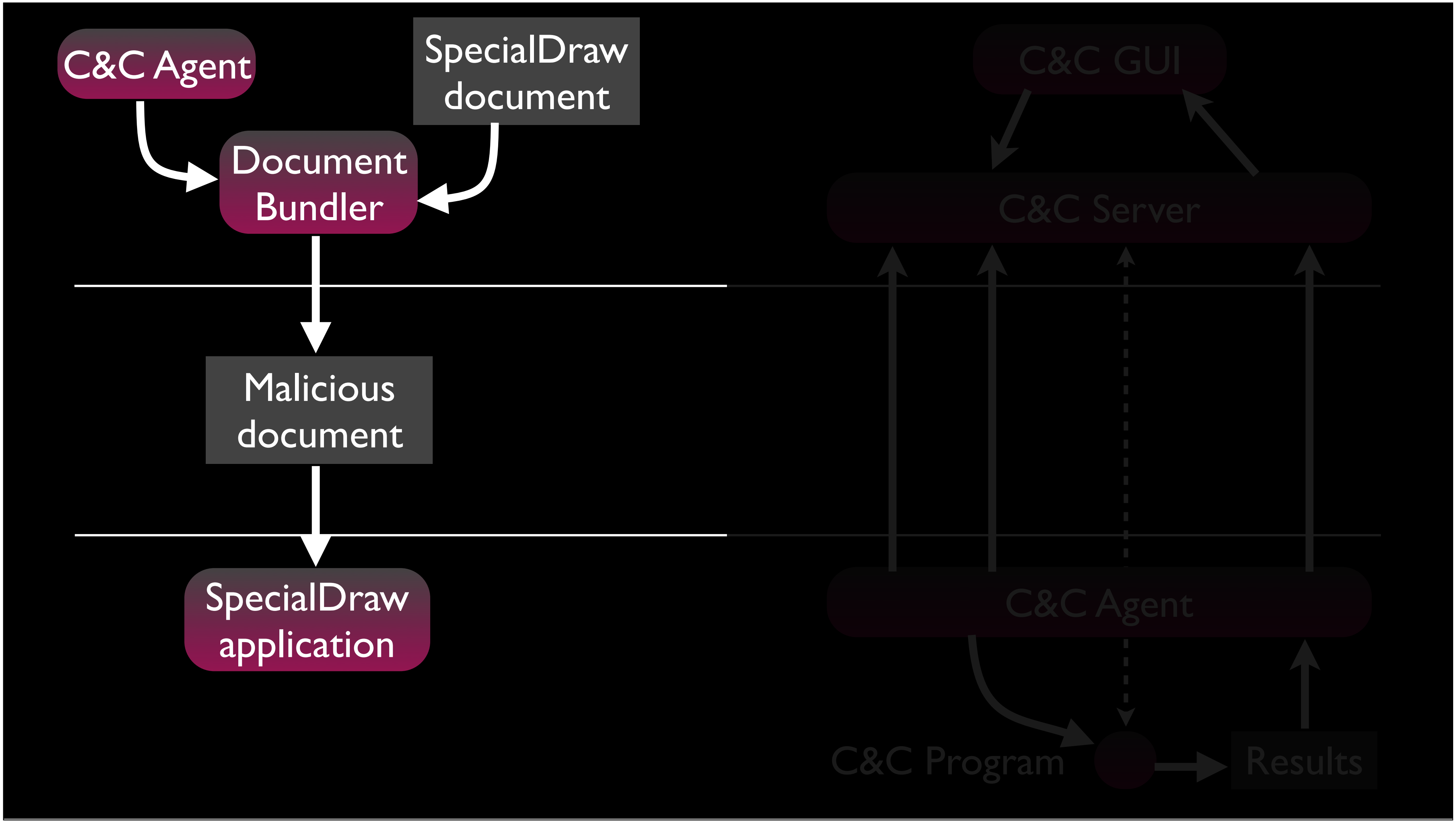
Cyber War

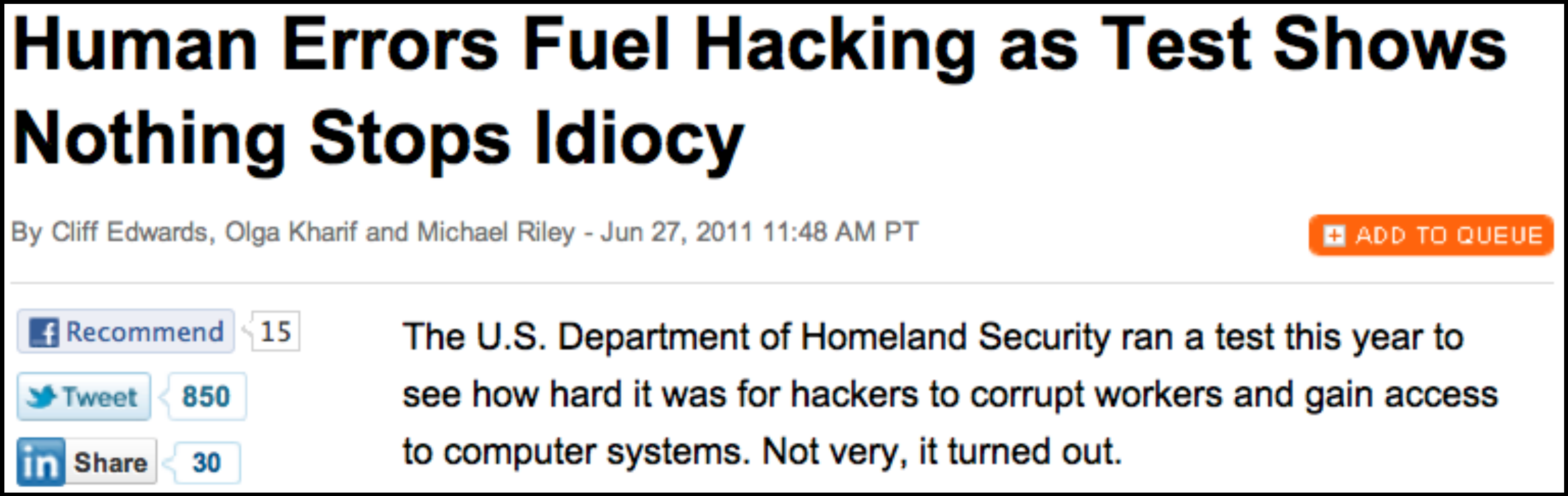
Number of software updates Symantec sent customers to combat new types of cyberattacks, in millions

Source: the company

Glowing Embers Video


C&C Agent
SpecialDraw document
Document Bundler
Evil Doers
Malicious document
SpecialDraw application
Compromised System
C&C GUI
C&C Server
C&C Agent
C&C Program
Results


C&C Agent
SpecialDraw document
Document Bundler
Malicious document
SpecialDraw application
C&C GUI
C&C Server
C&C Agent
C&C Program
Results



Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy

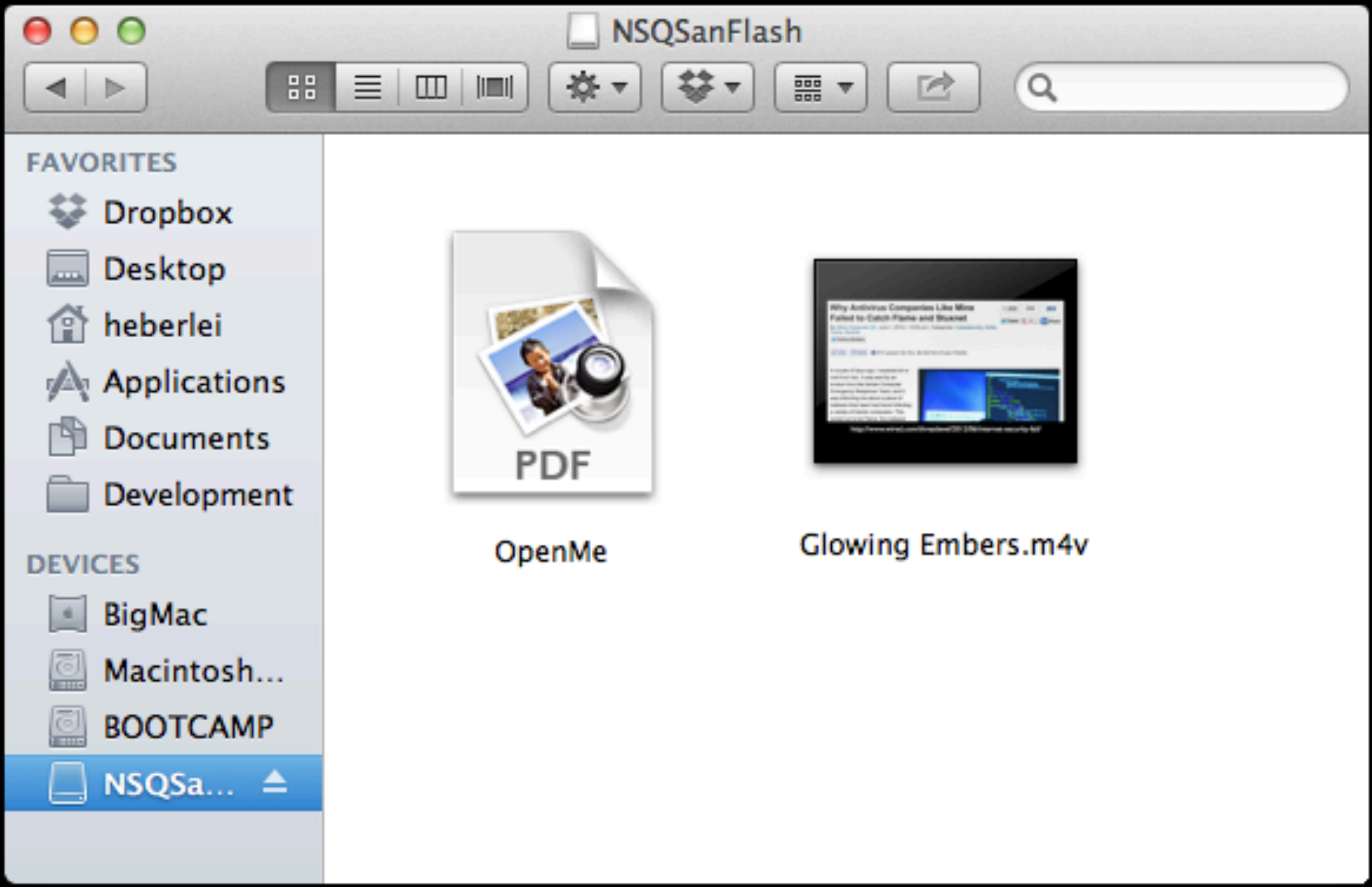
By Cliff Edwards, Olga Kharif and Michael Riley - Jun 27, 2011 11:48 AM PT

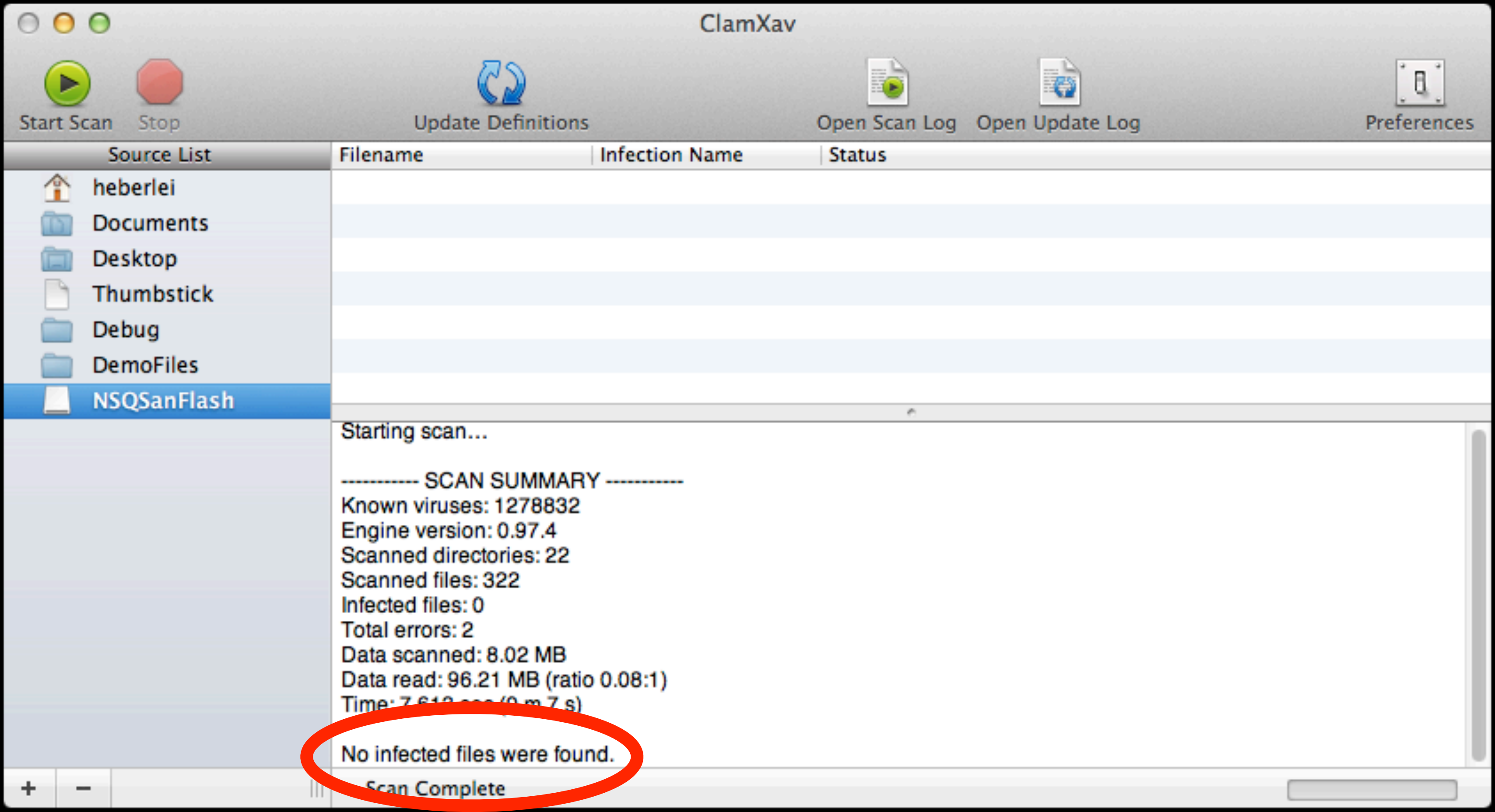
The U.S. Department of Homeland Security ran a test this year to see how hard it was for hackers to corrupt workers and gain access to computer systems. Not very, it turned out.

Staff secretly dropped computer discs and USB thumb drives in the parking lots of government buildings and private contractors. Of those who picked them up, 60 percent plugged the devices into office computers, curious to see what they contained. If the drive or CD case had an official logo, 90 percent were installed.

Demo

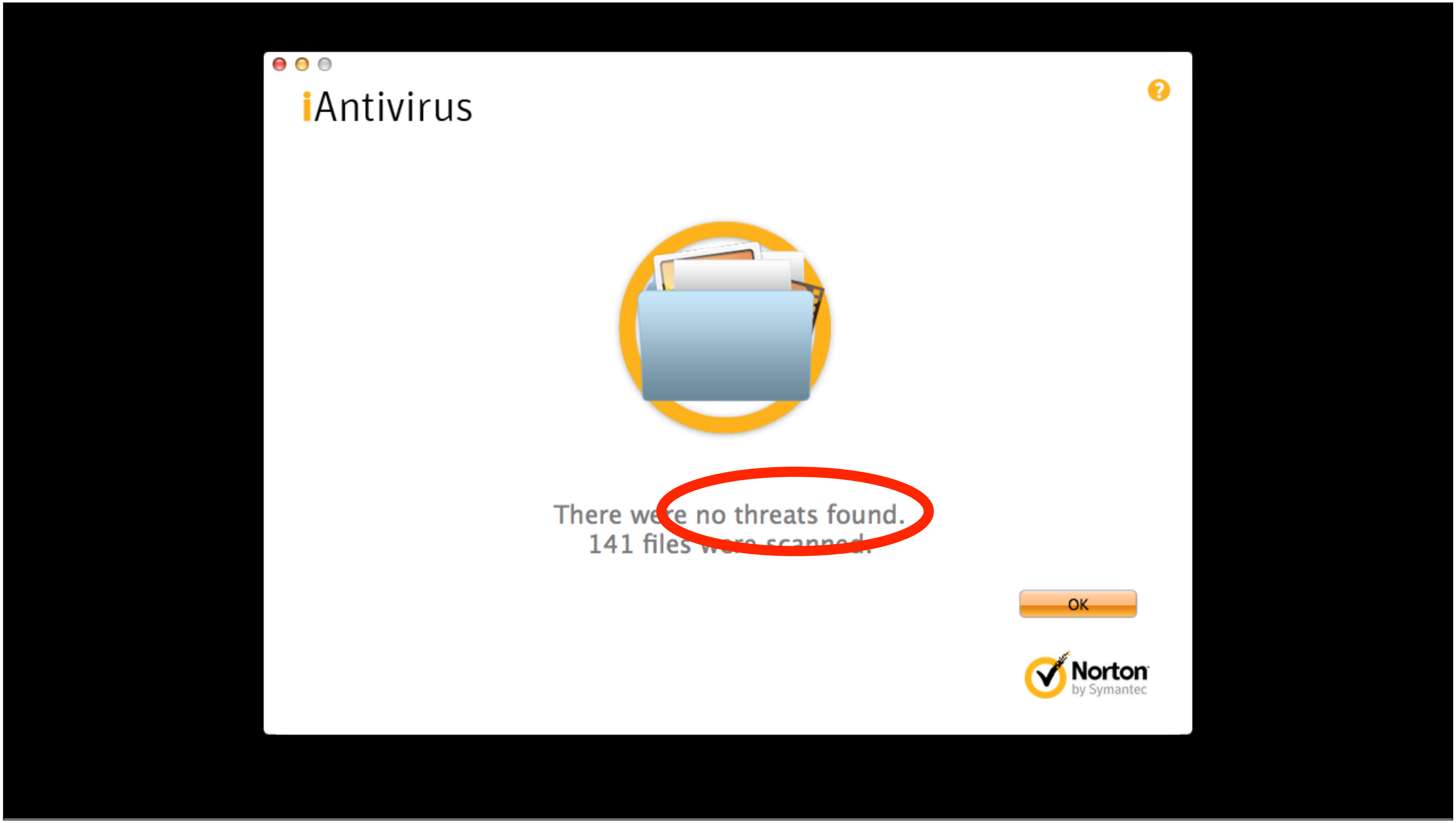
(PDF Trojan horse)


NSQSanFlash
FAVORITES
Dropbox
Desktop
heberlei
Applications
Documents
Development
DEVICES
BigMac
Macintosh…
BOOTCAMP
NSQSa…
PDF
OpenMe
Glowing Embers.m4v

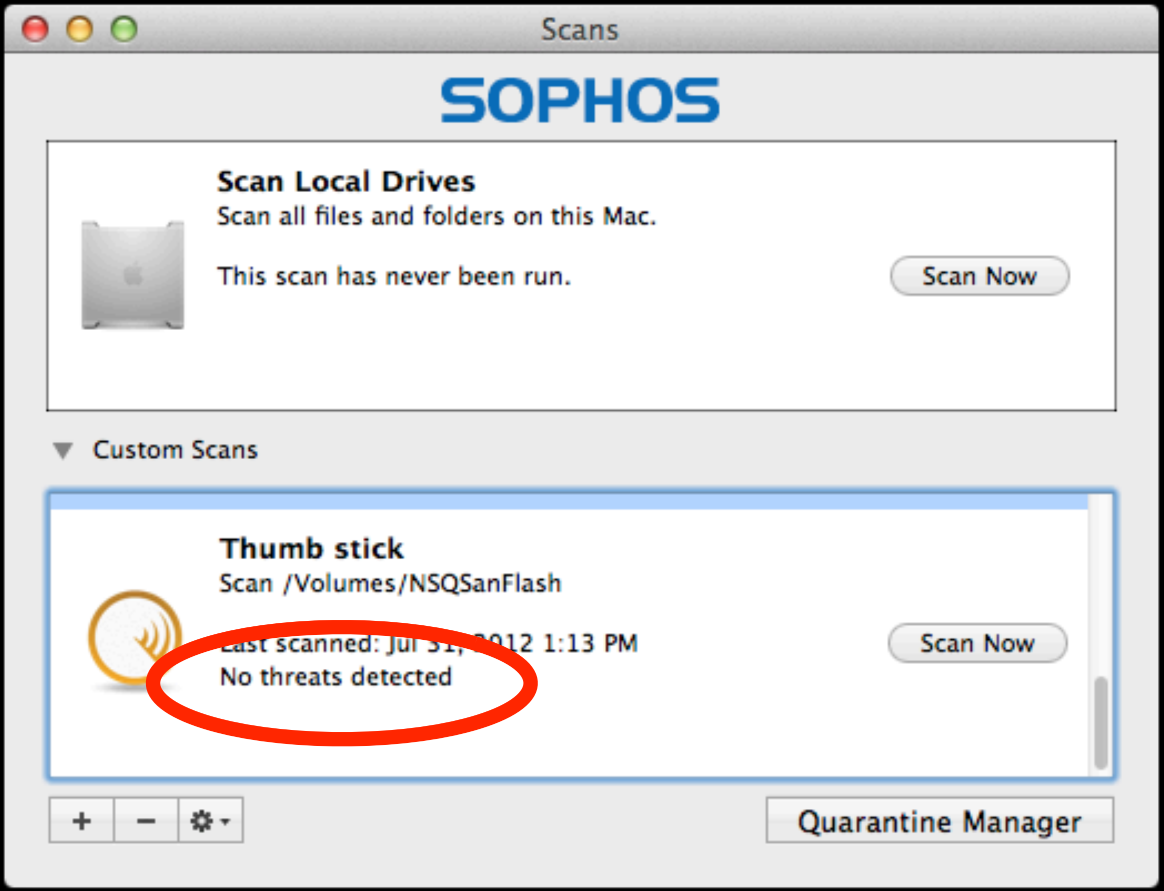


```
Starting scan...

----------- SCAN SUMMARY -----------
Known viruses: 1278832
Engine version: 0.97.4
Scanned directories: 22
Scanned files: 322
Infected files: 0
Total errors: 2
Data scanned: 8.02 MB
Data read: 96.21 MB (ratio 0.08:1)
Time: 7.612 sec (0 m 7 s)

No infected files were found.
```

Scan Complete



There were no threats found.
141 files were scanned.



Scan Local Drives

Scan all files and folders on this Mac.

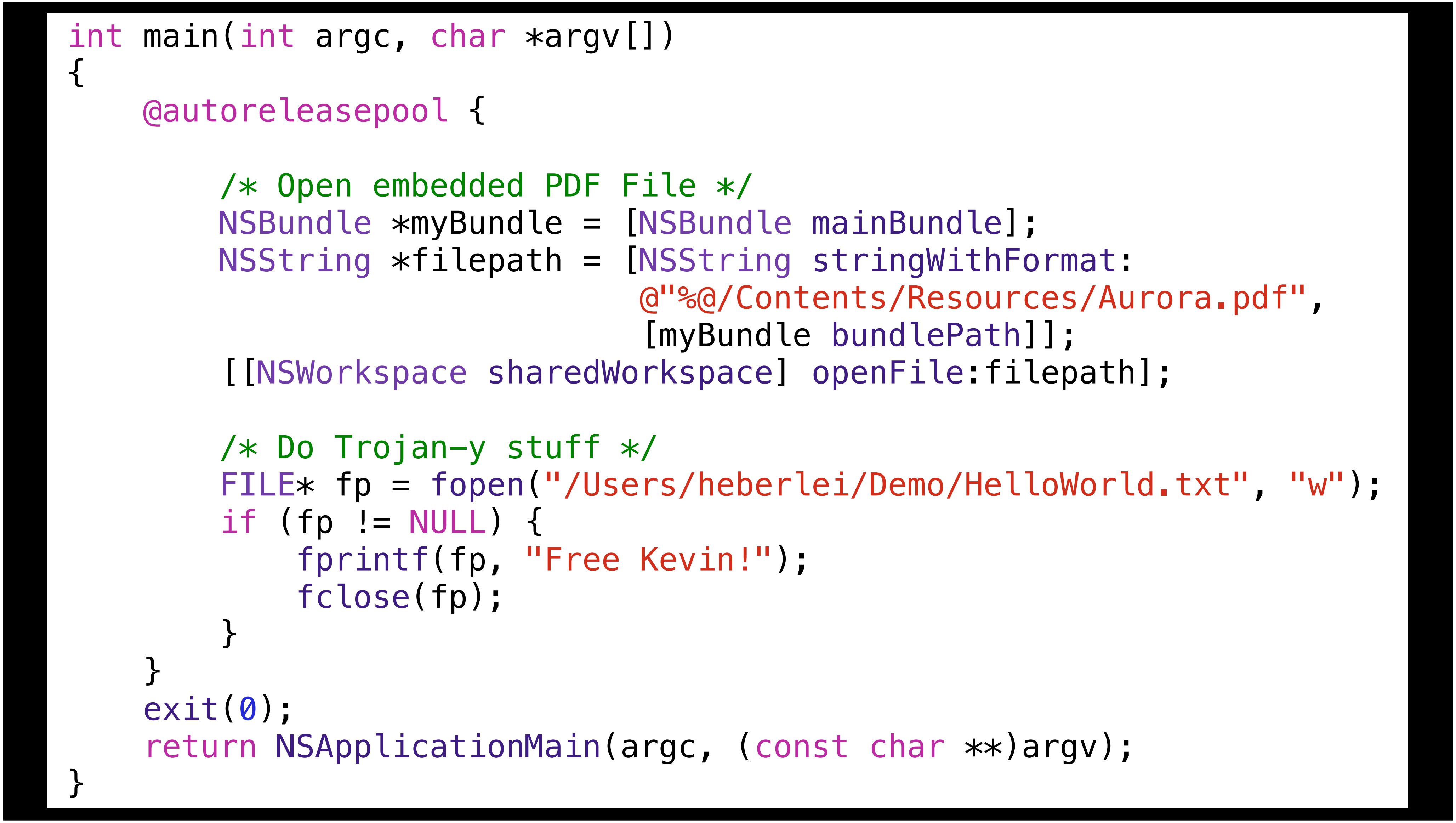
This scan has never been run.

Thumb stick

Scan /Volumes/NSQSanFlash

Last scanned: Jul 31, 2012 1:13 PM

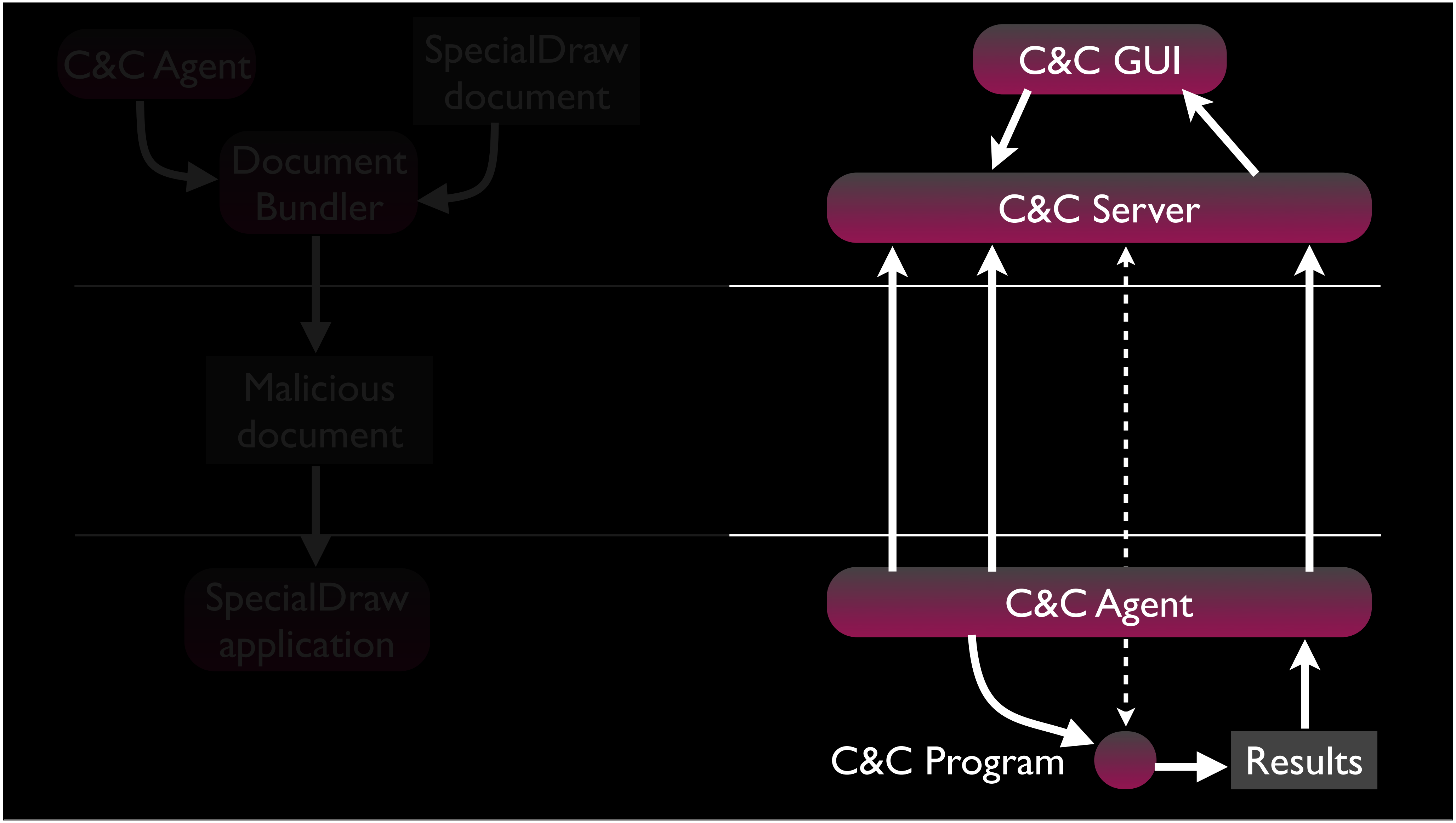
No threats detected

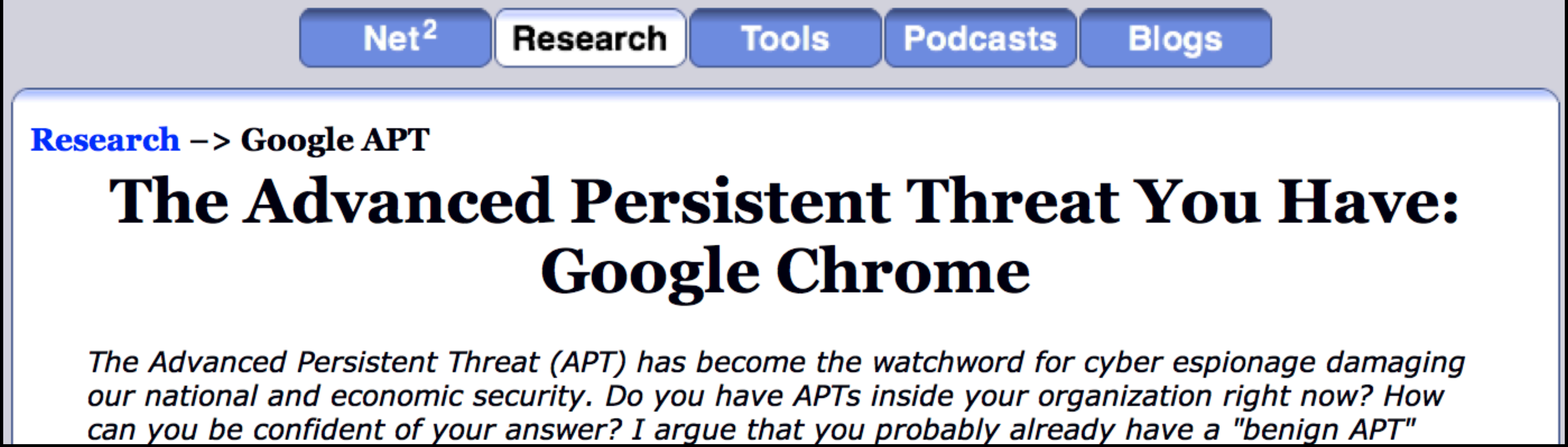


```
int main(int argc, char *argv[])
{
    @autoreleasepool {

        /* Open embedded PDF File */
        NSBundle *myBundle = [NSBundle mainBundle];
        NSString *filepath = [NSString stringWithFormat:
                              @"%@/Contents/Resources/Aurora.pdf",
                              [myBundle bundlePath]];
        [[NSWorkspace sharedWorkspace] openFile:filepath];

        /* Do Trojan-y stuff */
        FILE* fp = fopen("/Users/heberlei/Demo/HelloWorld.txt", "w");
        if (fp != NULL) {
            fprintf(fp, "Free Kevin!");
            fclose(fp);
        }
    }
    exit(0);
    return NSApplicationMain(argc, (const char **)argv);
}
```

“Advanced” Attack ??

- OS is fully patched system
- Gatekeeper is on
- My three AV systems say everything is good
- Minutes to write


C&C Agent
SpecialDraw document
Document Bundler
Malicious document
SpecialDraw application
C&C GUI
C&C Server
C&C Agent
C&C Program
Results



Research –> Google APT

The Advanced Persistent Threat You Have: Google Chrome

The Advanced Persistent Threat (APT) has become the watchword for cyber espionage damaging our national and economic security. Do you have APTs inside your organization right now? How can you be confident of your answer? I argue that you probably already have a "benign APT"

http://www.netsq.com/Documents_html/GoogleAPT/

Glowing Embers Summary

- Bypass firewalls via outbound web connections
- Bypass Network IPS with SSL connections plus payload encryption
- Bypass Anti-virus software
- Steal data, take screenshots, take pictures with the camera
- Install any new software modules
- Modify documents
- Self-destruct, secure deletes

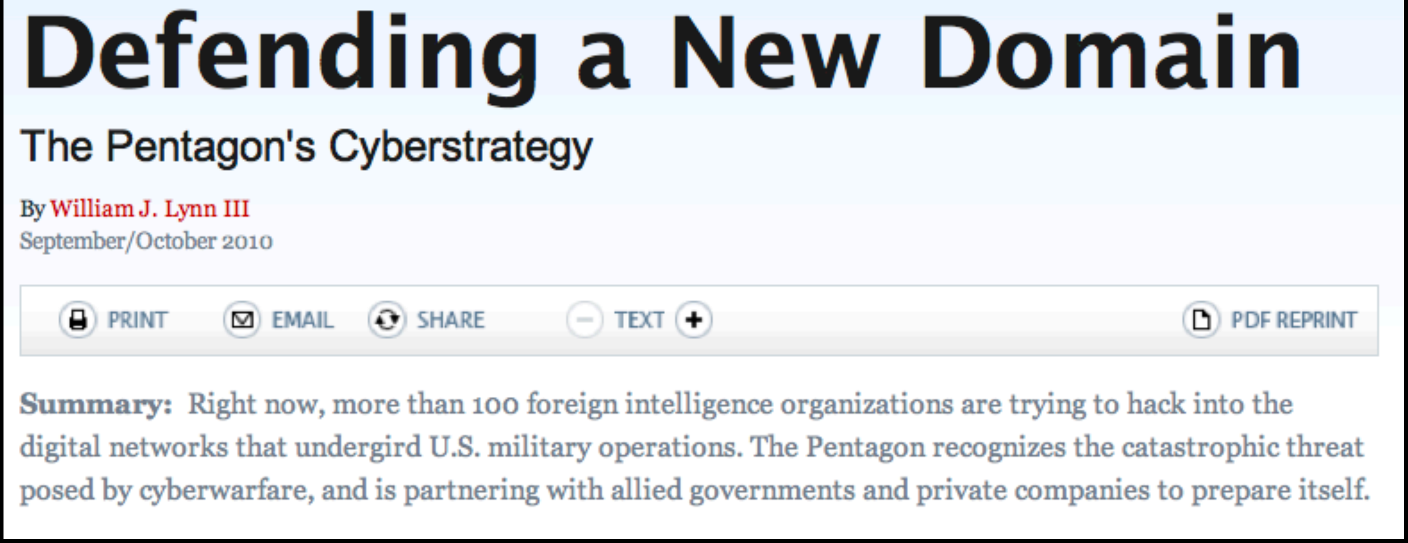
Challenge: Write your own malware (Trojan horse, C&C agent, ...) and then scan it with Antivirus software

Espionage in the 21st Century

Protecting Your Air Gap

Part I

Inspired by actual events



Defending a New Domain

The Pentagon's Cyberstrategy

By William J. Lynn III
September/October 2010

Summary: Right now, more than 100 foreign intelligence organizations are trying to hack into the digital networks that undergird U.S. military operations. The Pentagon recognizes the catastrophic threat posed by cyberwarfare, and is partnering with allied governments and private companies to prepare itself.

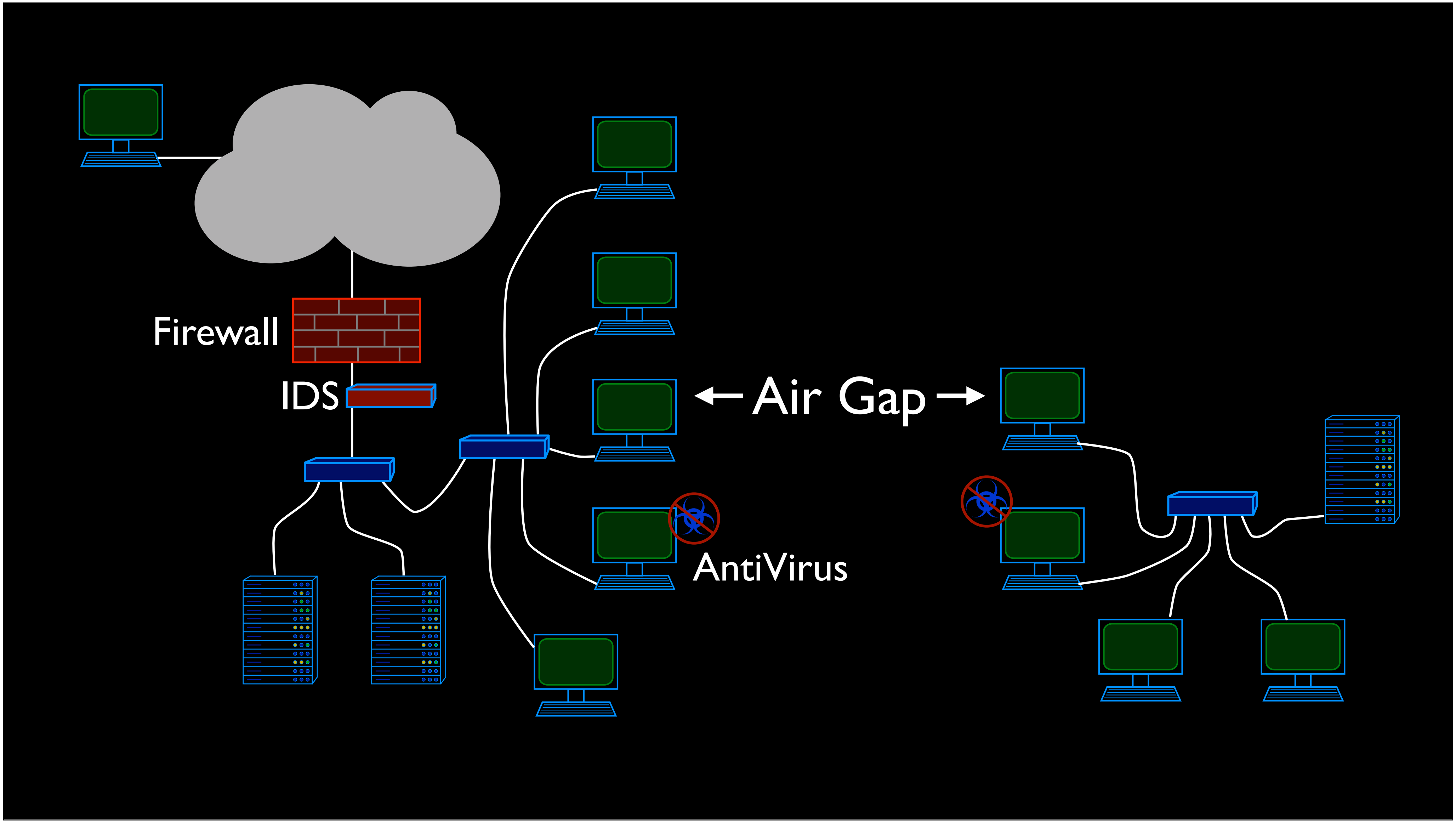
The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead

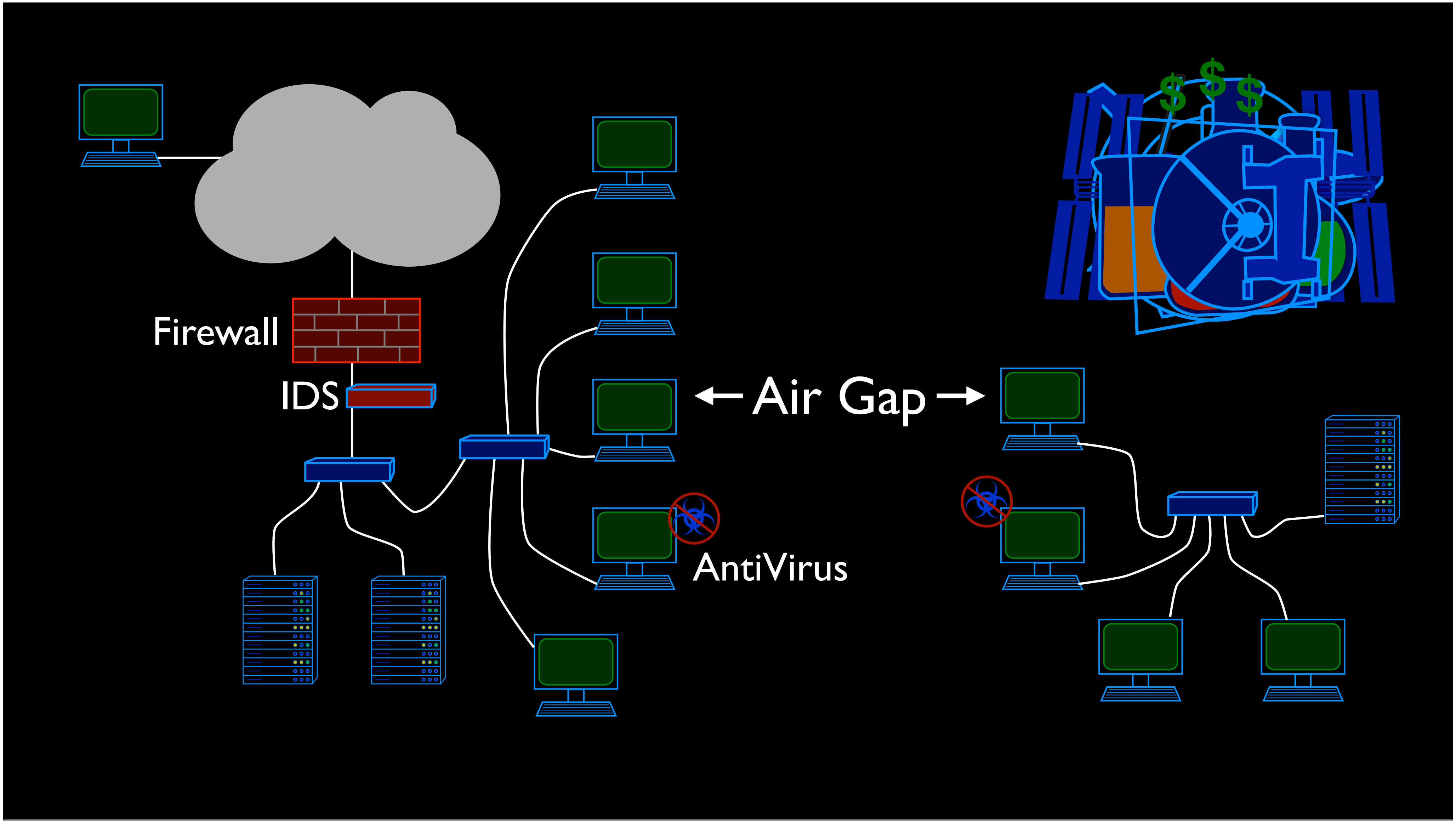
Computer virus hits US Predator and Reaper drone fleet

By Noah Shachtman, wired.com | Published 28 days ago

But they're sure that the infection has hit both classified and unclassified machines at Creech. That raises the possibility, at least, that secret data may have been captured by the keylogger, and then transmitted over the public internet to someone outside the military chain of command.

But time and time again, the so-called "air gaps" between classified and public networks have been bridged, largely through the use of discs and removable drives.

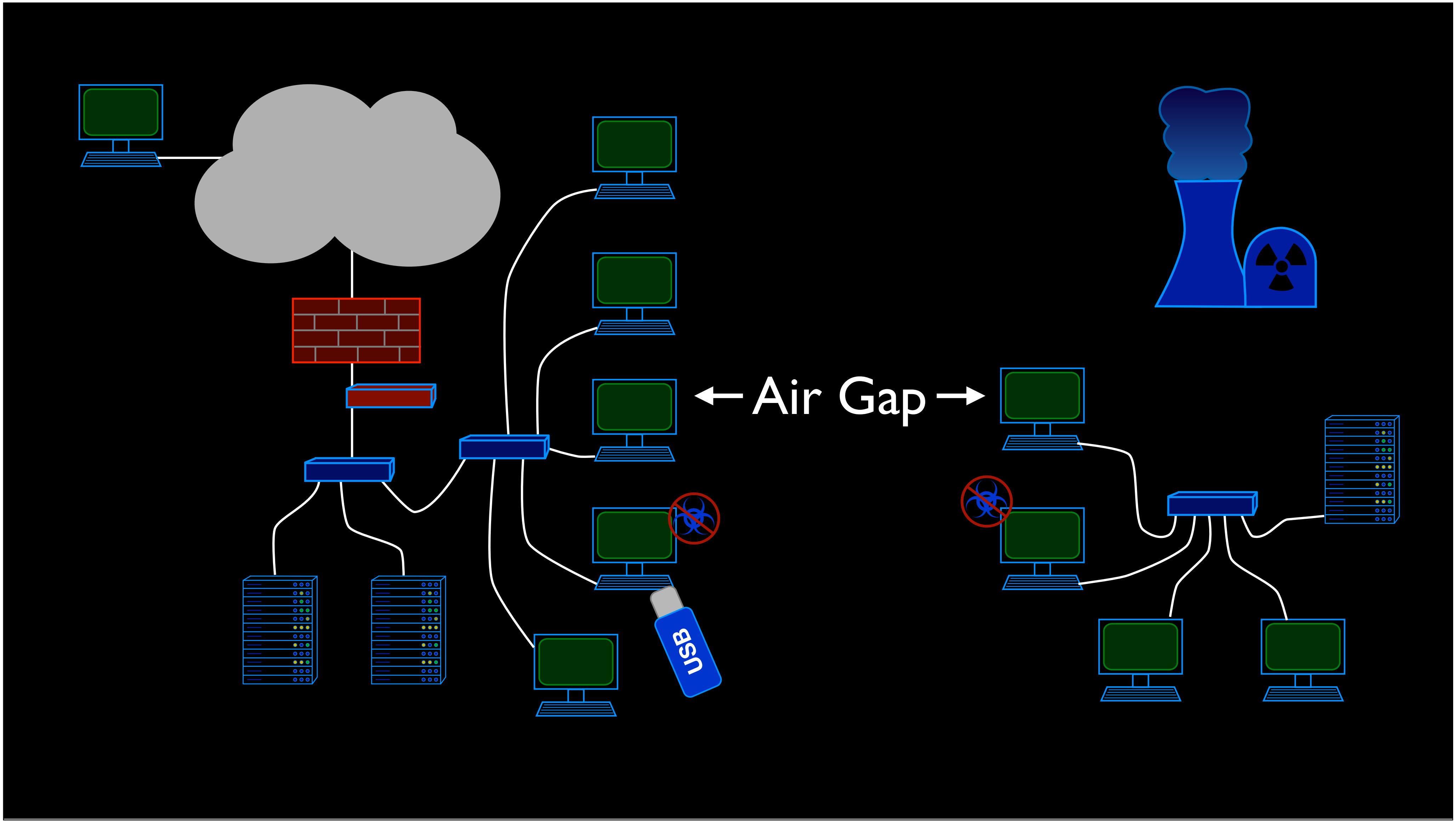

Firewall
IDS
← Air Gap →
AntiVirus


Firewall
IDS
← Air Gap →
AntiVirus
$ $ $

Are you safe?

Eric Byres of Byres Security has studied Stuxnet extensively. He told the AusCERT information security conference that even with an air gap separating the protected network from the outside world, all manner of data still has to flow across that gap — including project data, software updates and patches, antivirus signatures and documentation. "Even the best attempt to completely air-gap, I believe, is just an illusion. I really don't think air gaps are viable," he said.

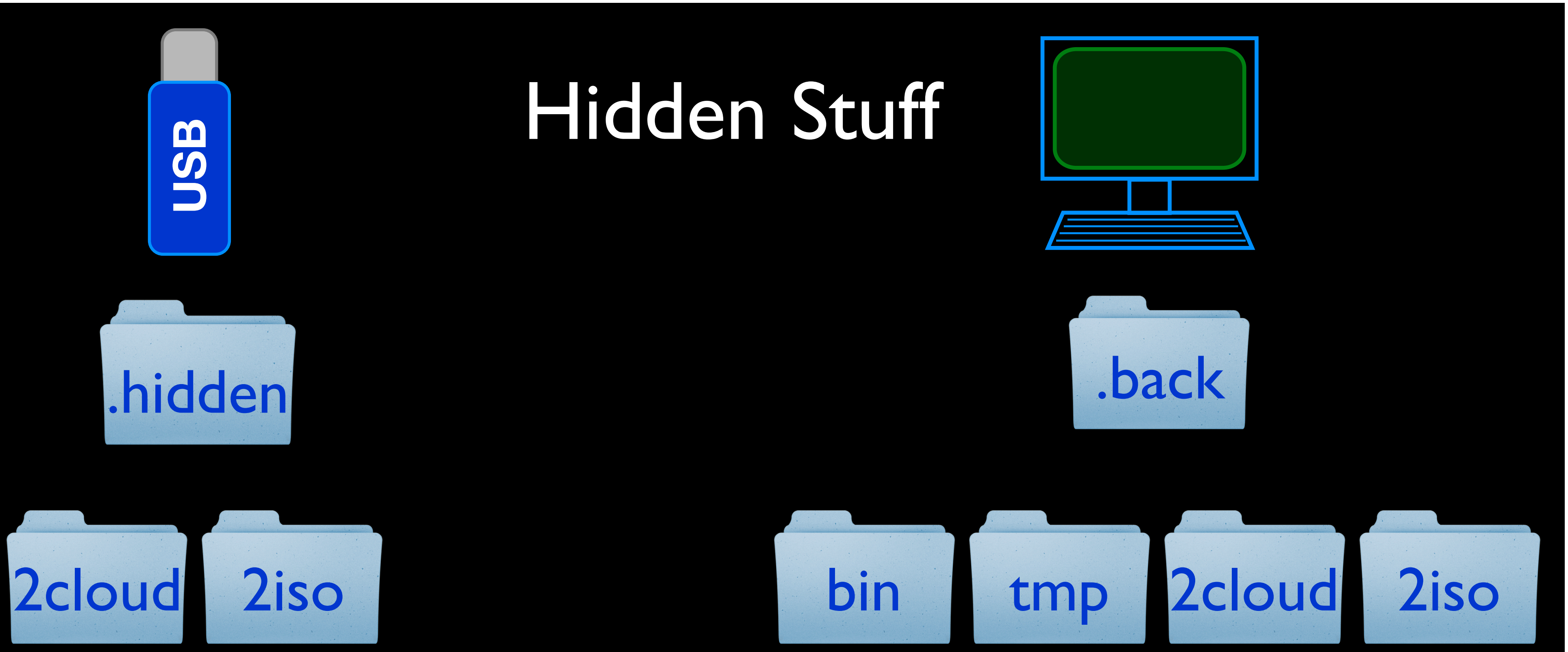
“Son of Stuxnet within a year: expert”, ZDnet


← Air Gap →
USB

Part 2

You are now infected

Hidden Stuff

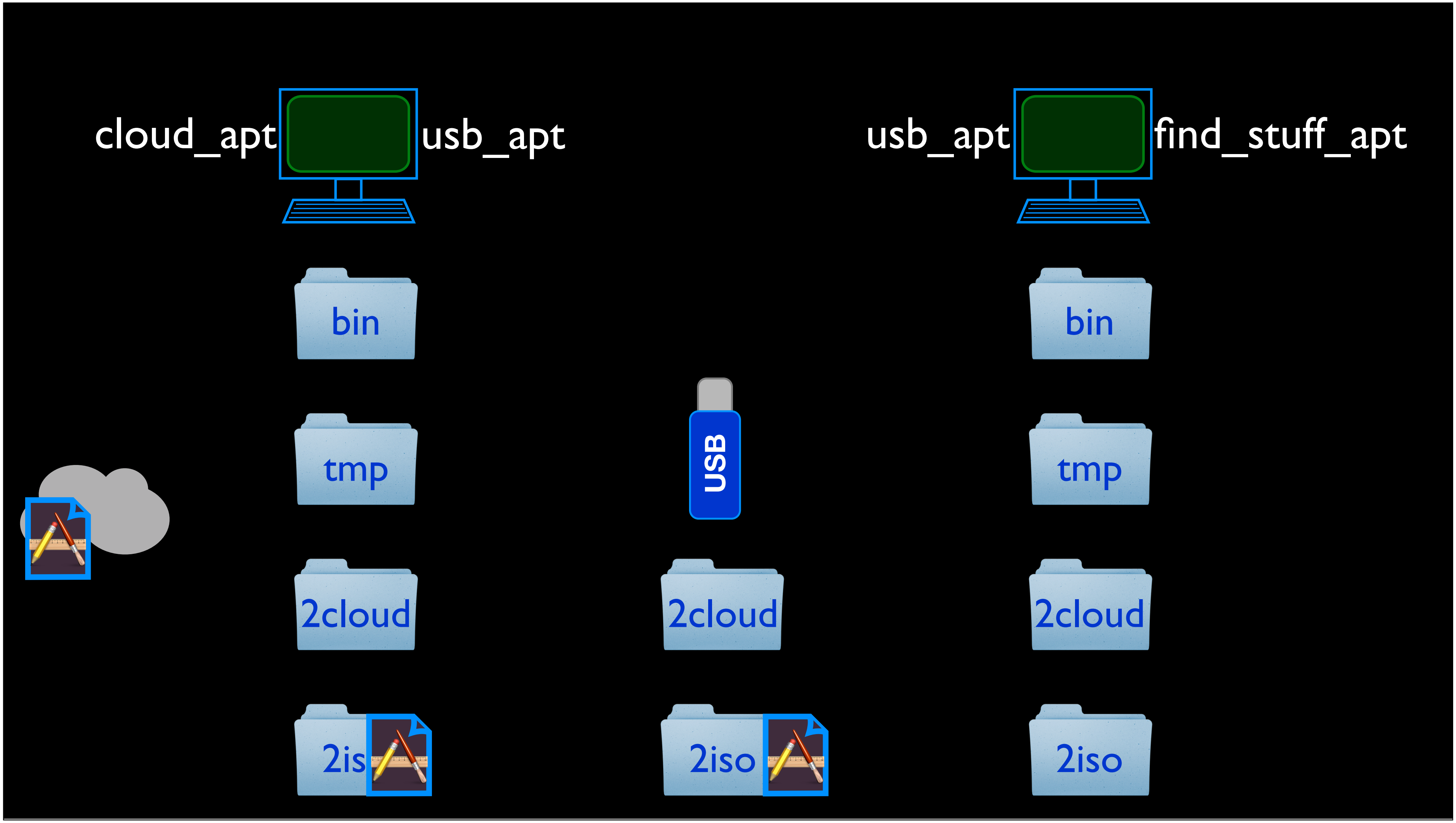


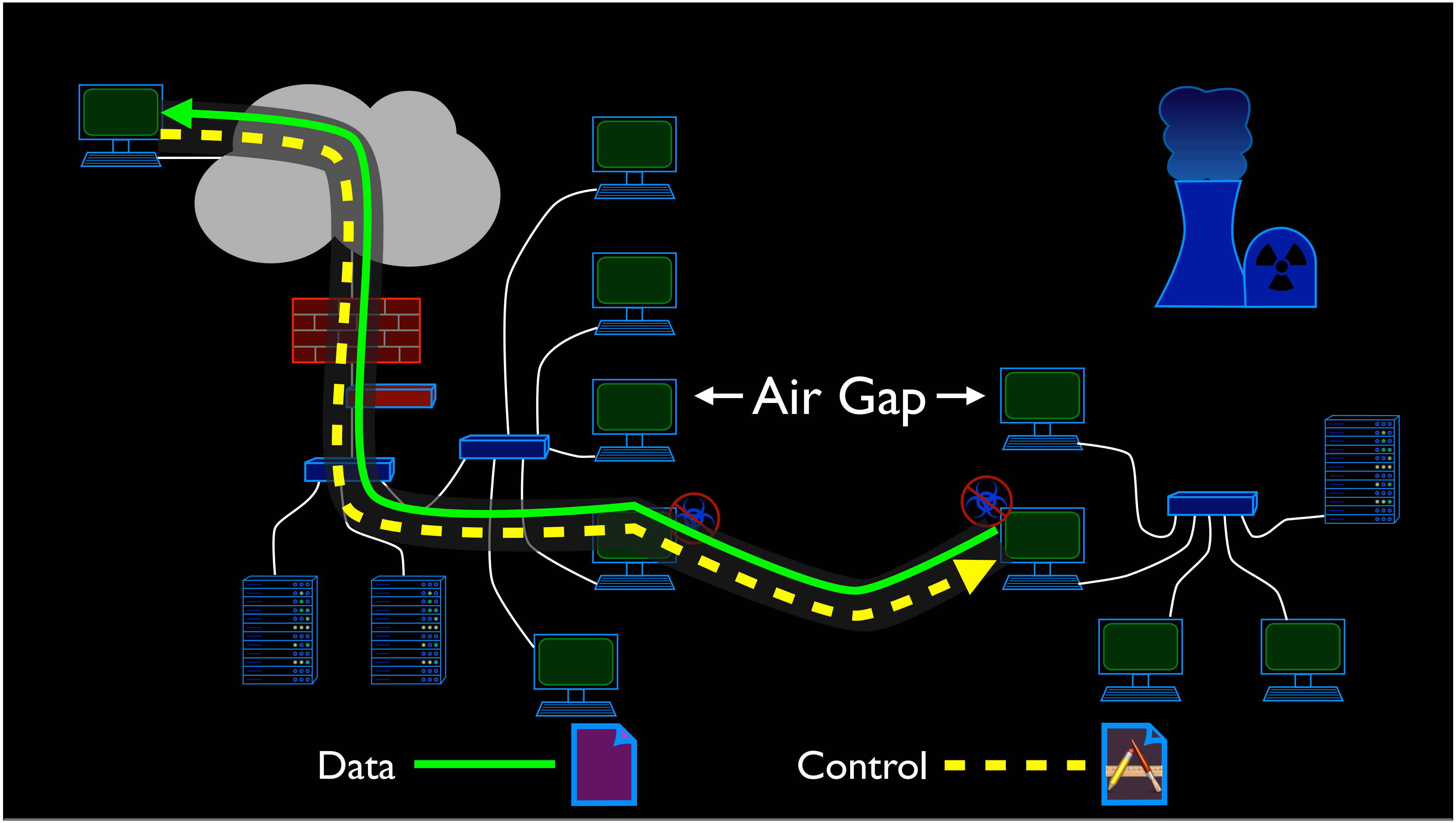
find_stuff_apt

cloud_apt

usb_apt

mds mdworker Locum fseventsd pbs diskarbitrationd quicklookd


cloud_apt
usb_apt
usb_apt
find_stuff_apt
bin
tmp
2cloud
2is
USB
2cloud
2iso
bin
tmp
2cloud
2iso

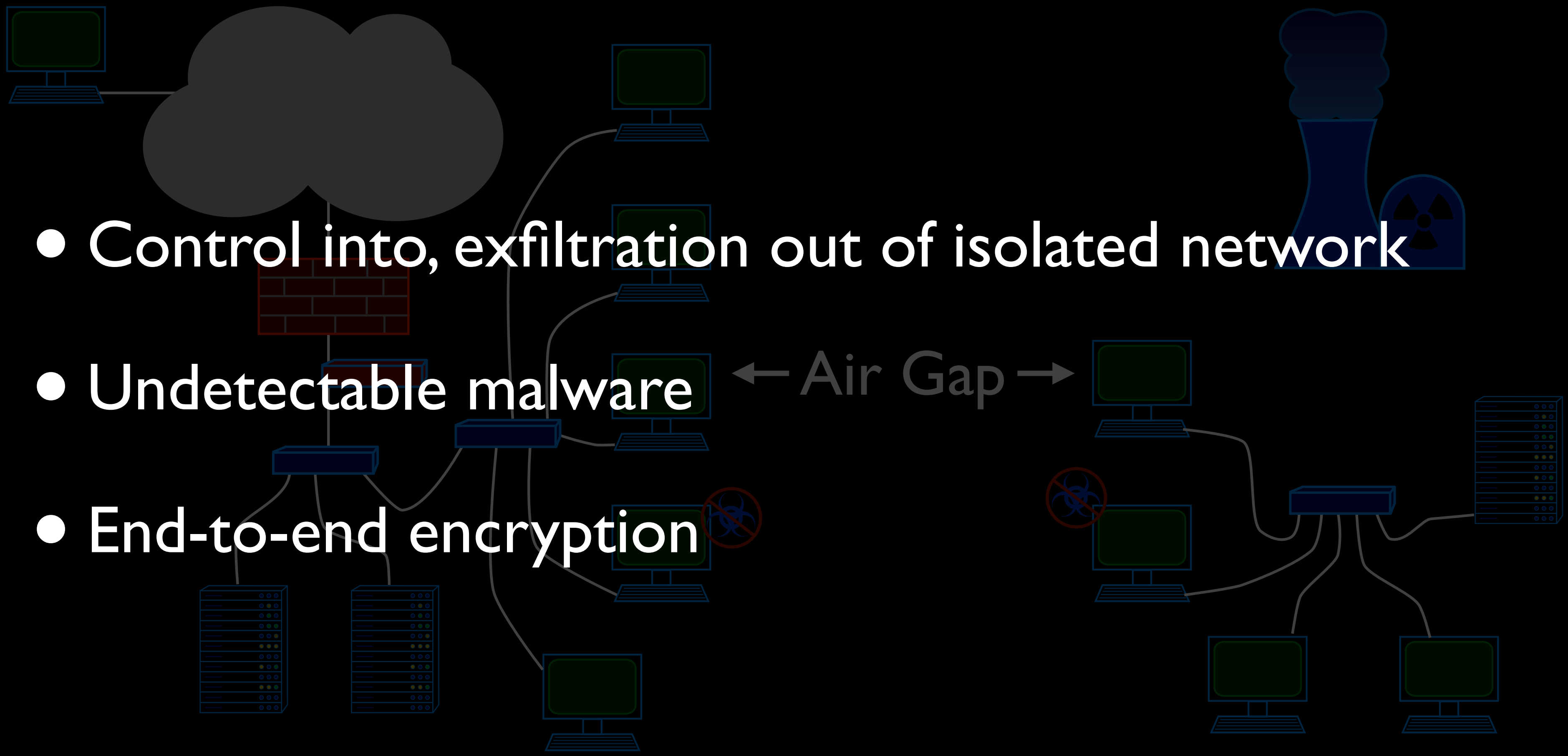


← Air Gap →

Data

Control

- Control into, exfiltration out of isolated network
- Undetectable malware
- End-to-end encryption

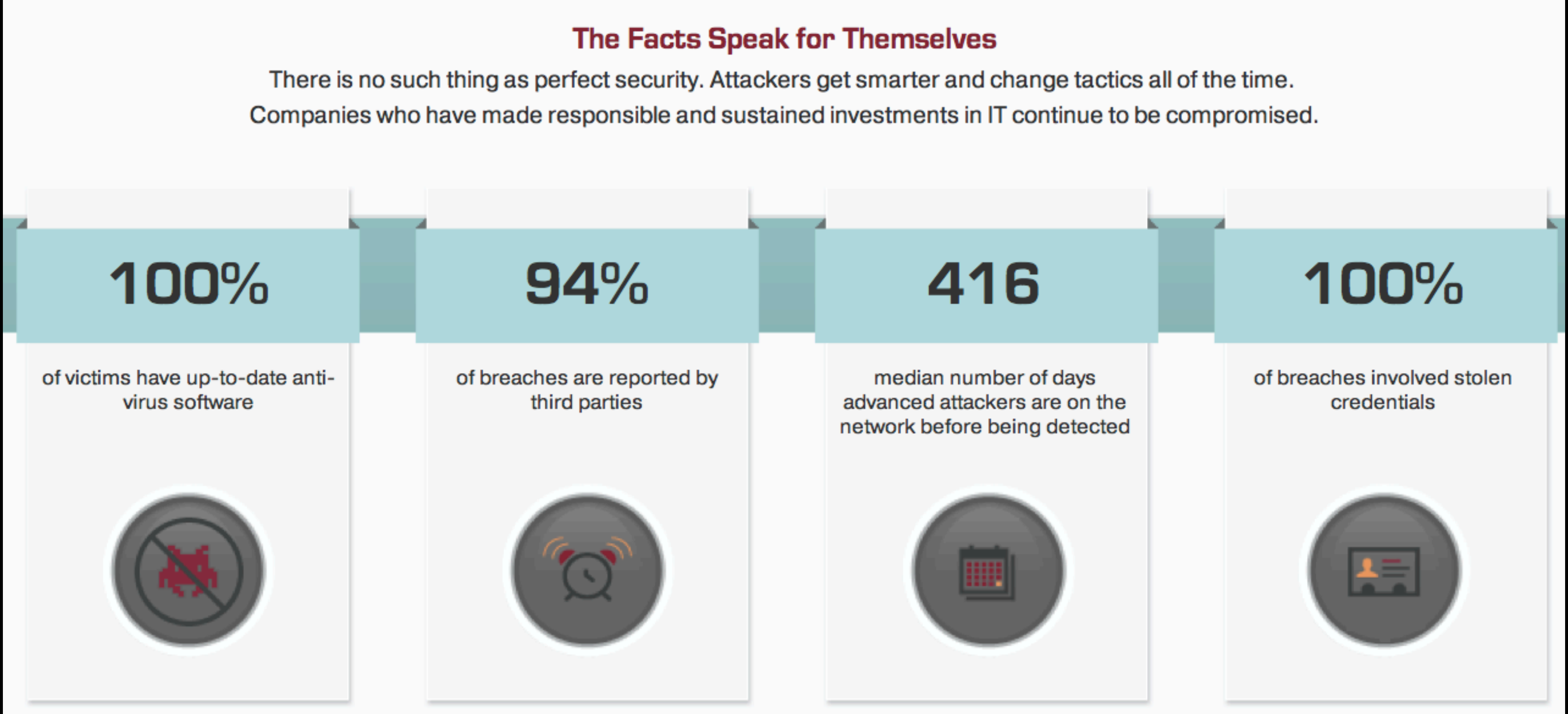


Thoughts on “Advanced Persistent Threats”

Advanced Persistent Threat

Advanced Persistent Threat

Anything that gets past automated detection / prevention



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time. Companies who have made responsible and sustained investments in IT continue to be compromised.

100%

of victims have up-to-date anti-virus software

94%

of breaches are reported by third parties

416

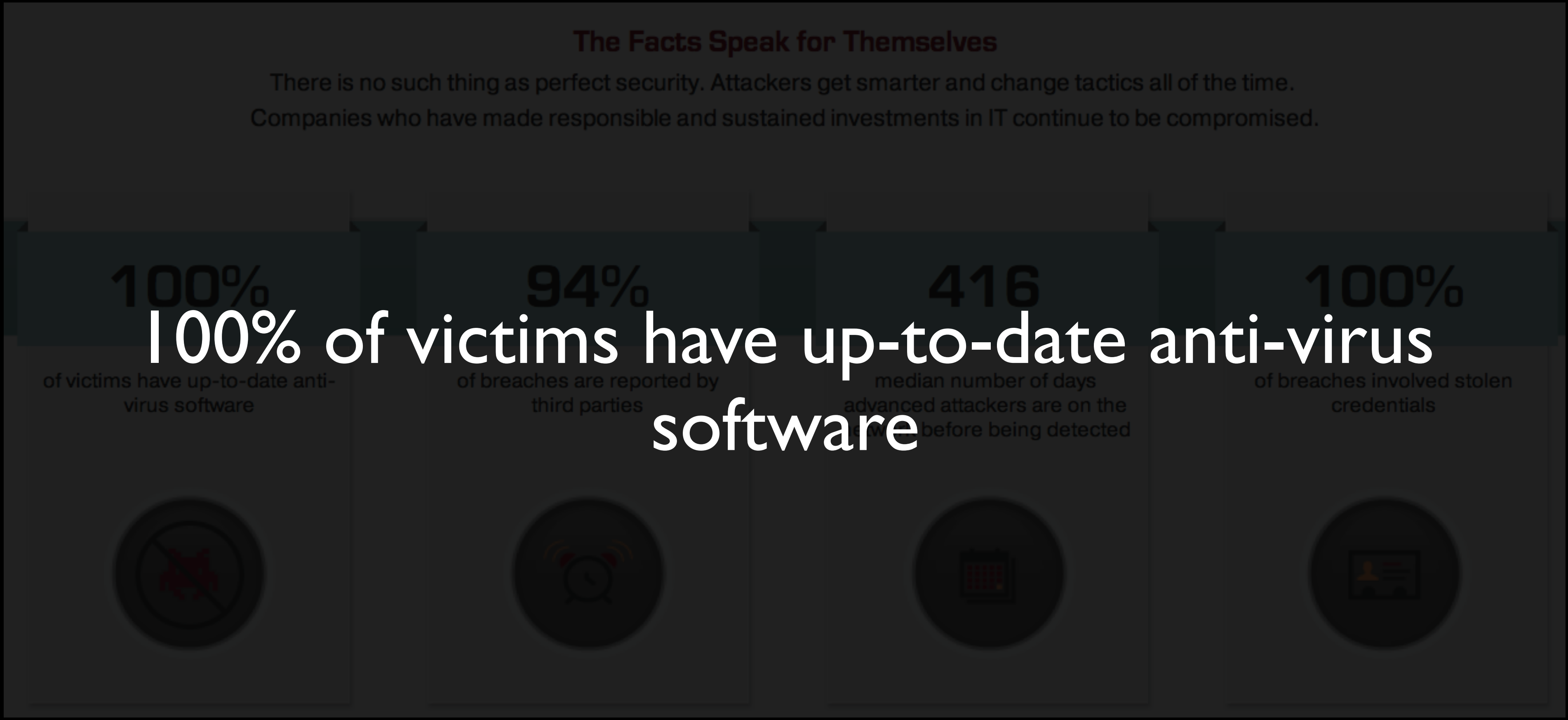
median number of days advanced attackers are on the network before being detected

100%

of breaches involved stolen credentials

http://www.mandiant.com/threat-landscape/

100% of victims have up-to-date anti-virus software



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time. Companies who have made responsible and sustained investments in IT continue to be compromised.

100%
of victims have up-to-date anti-virus software

94%
of breaches are reported by third parties

416
median number of days advanced attackers are on the network before being detected

100%
of breaches involved stolen credentials

http://www.mandiant.com/threat-landscape/

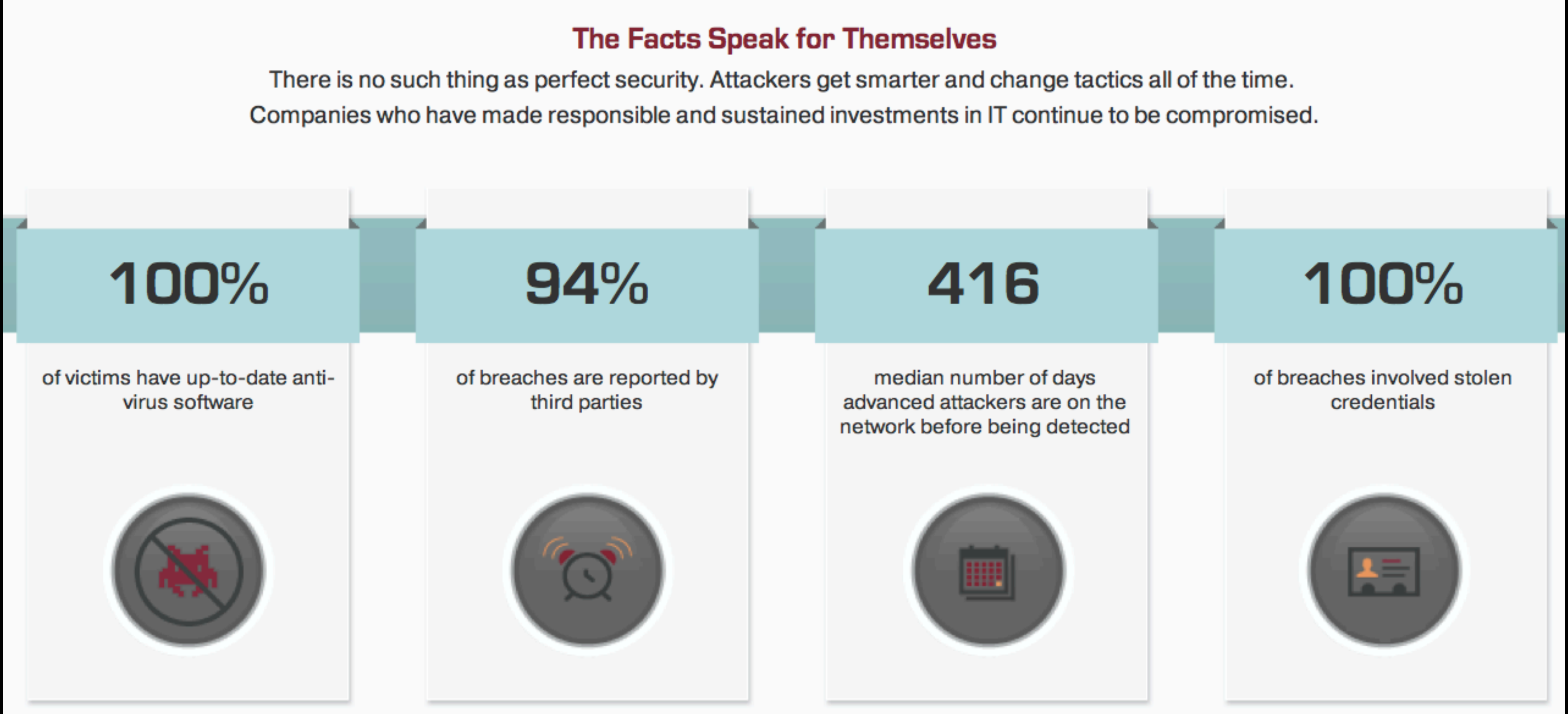
Advanced Persistent Threat

1: Relentless until successful

Not a crime of opportunity

2: Long-lived

No longer a smash and grab



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time. Companies who have made responsible and sustained investments in IT continue to be compromised.

100%
of victims have up-to-date anti-virus software

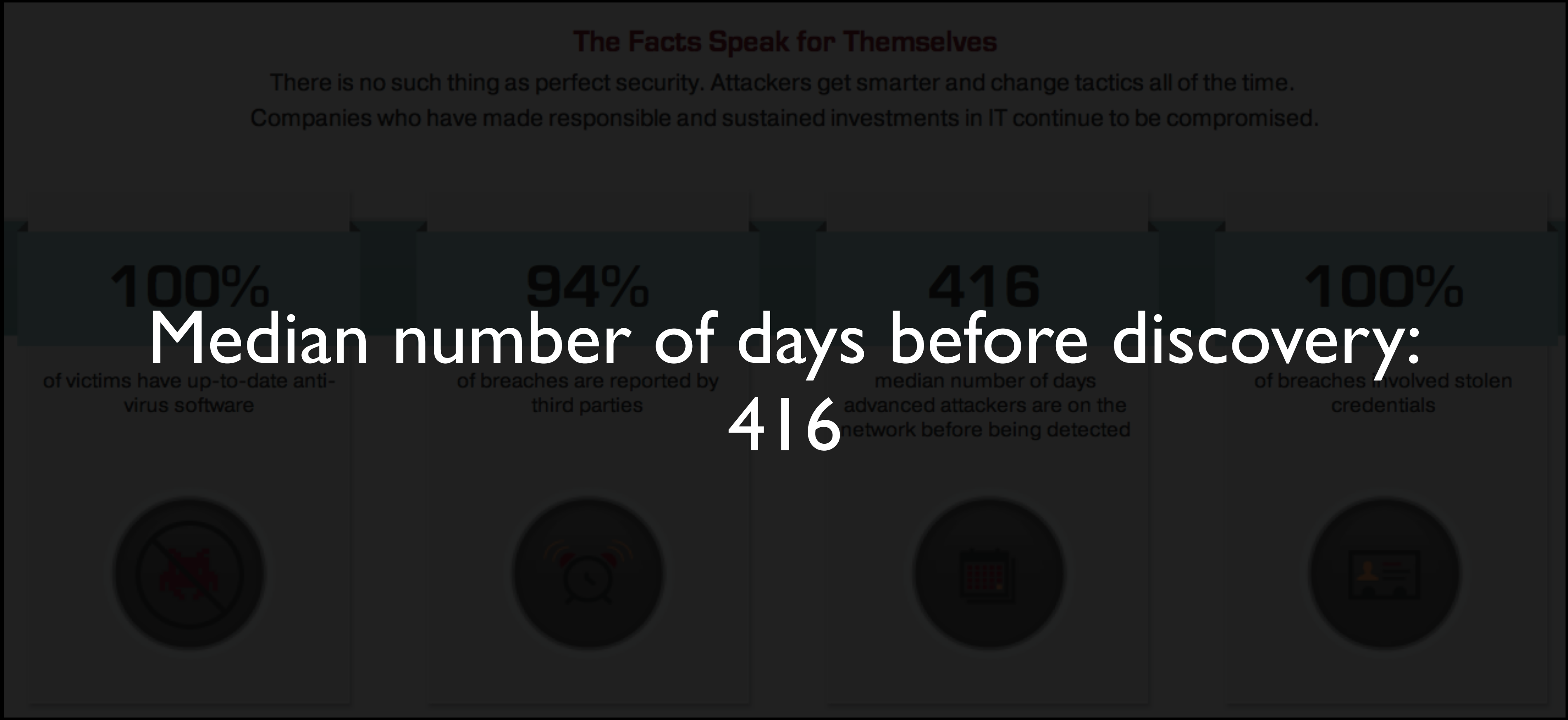
94%
of breaches are reported by third parties

416
median number of days advanced attackers are on the network before being detected

100%
of breaches involved stolen credentials

http://www.mandiant.com/threat-landscape/

Median number of days before discovery: 416



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time. Companies who have made responsible and sustained investments in IT continue to be compromised.

100%
of victims have up-to-date anti-virus software

94%
of breaches are reported by third parties

416
median number of days advanced attackers are on the network before being detected

100%
of breaches involved stolen credentials

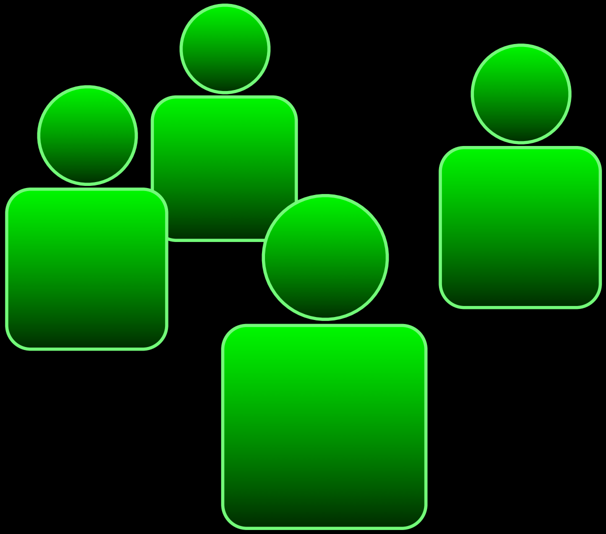
http://www.mandiant.com/threat-landscape/

Advanced Persistent Threat

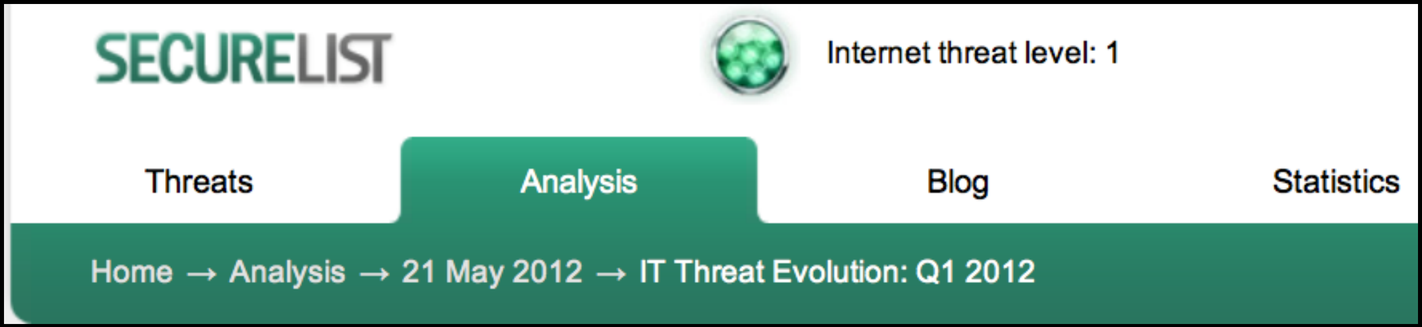
A Threat is like Soylent Green

Advanced Persistent Threat

It’s made of people



Advanced Persistent Threat



SECURELIST

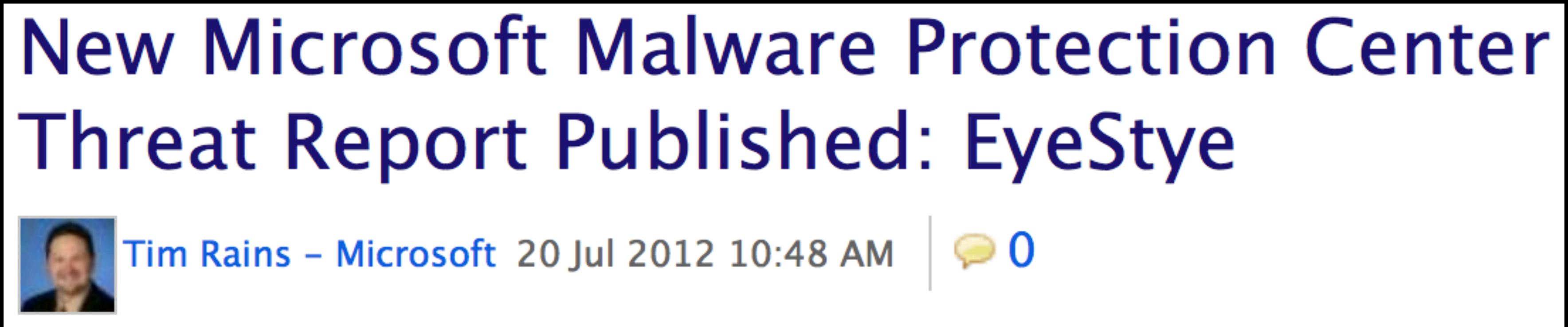
Internet threat level: 1

Home → Analysis → 21 May 2012 → IT Threat Evolution: Q1 2012

"Although patching is effective against this ['fileless' bot] and similar threats, ..."

http://www.securelist.com/en/analysis/204792231/IT_Threat_Evolution_Q1_2012

Advanced Persistent Threat

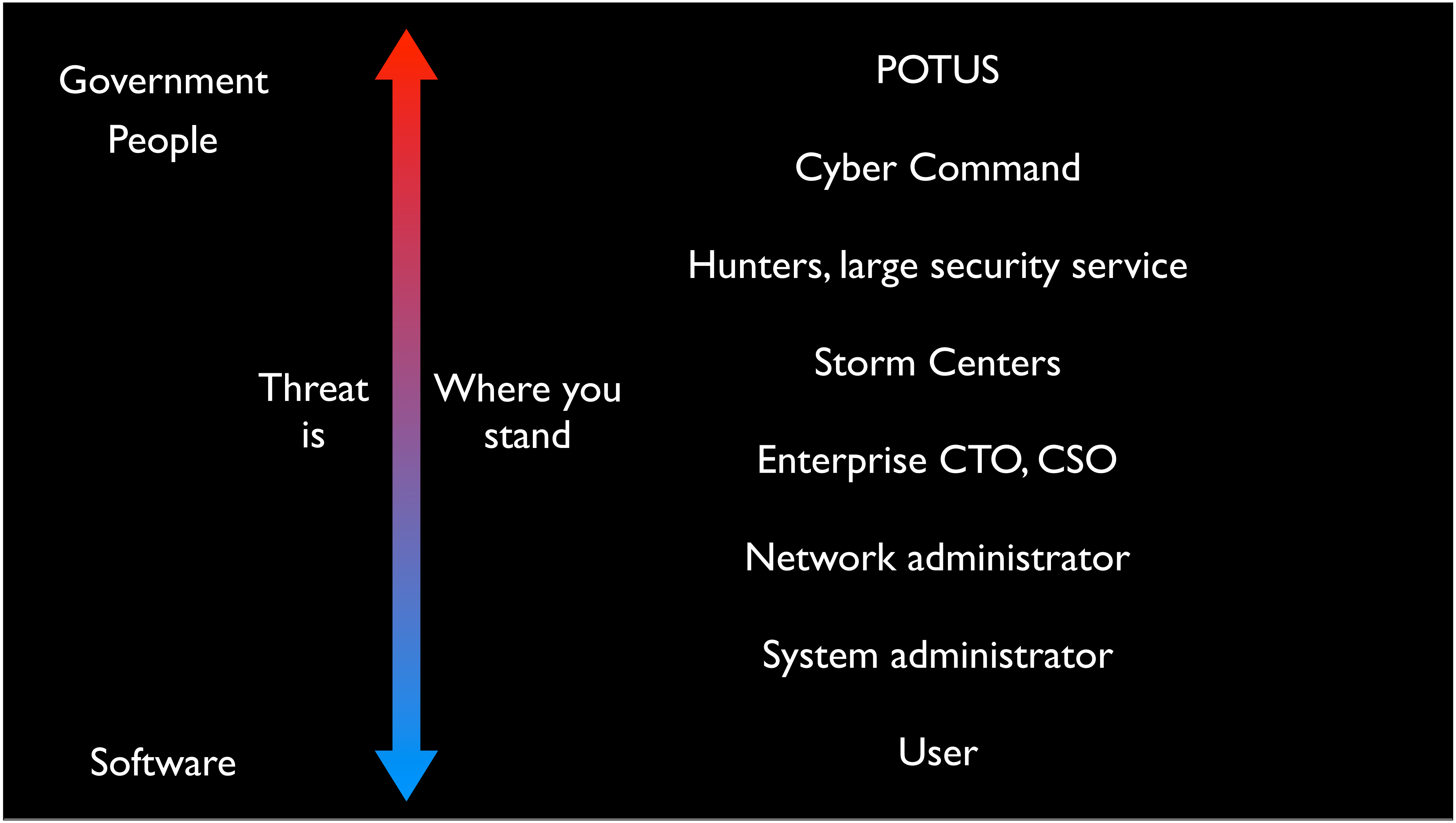


New Microsoft Malware Protection Center Threat Report Published: EyeStye

Tim Rains - Microsoft 20 Jul 2012 10:48 AM 0

"Four specific families of threats contributed to the steep rise in the malware infection rates ..."

http://blogs.technet.com/b/security/archive/2012/07/20/new-microsoft-malware-protection-center-threat-report-published-eyestye.aspx



Government

People

Threat is

Where you stand

Software

POTUS

Cyber Command

Hunters, large security service

Storm Centers

Enterprise CTO, CSO

Network administrator

System administrator

User

Google, the APT, from the audit trail perspective

Audit Explorer Tutorial Videos

http://www.netsq.com/Tools/AuditExplorer/Videos/

The Advanced Persistent Threat You Have: Google Chrome

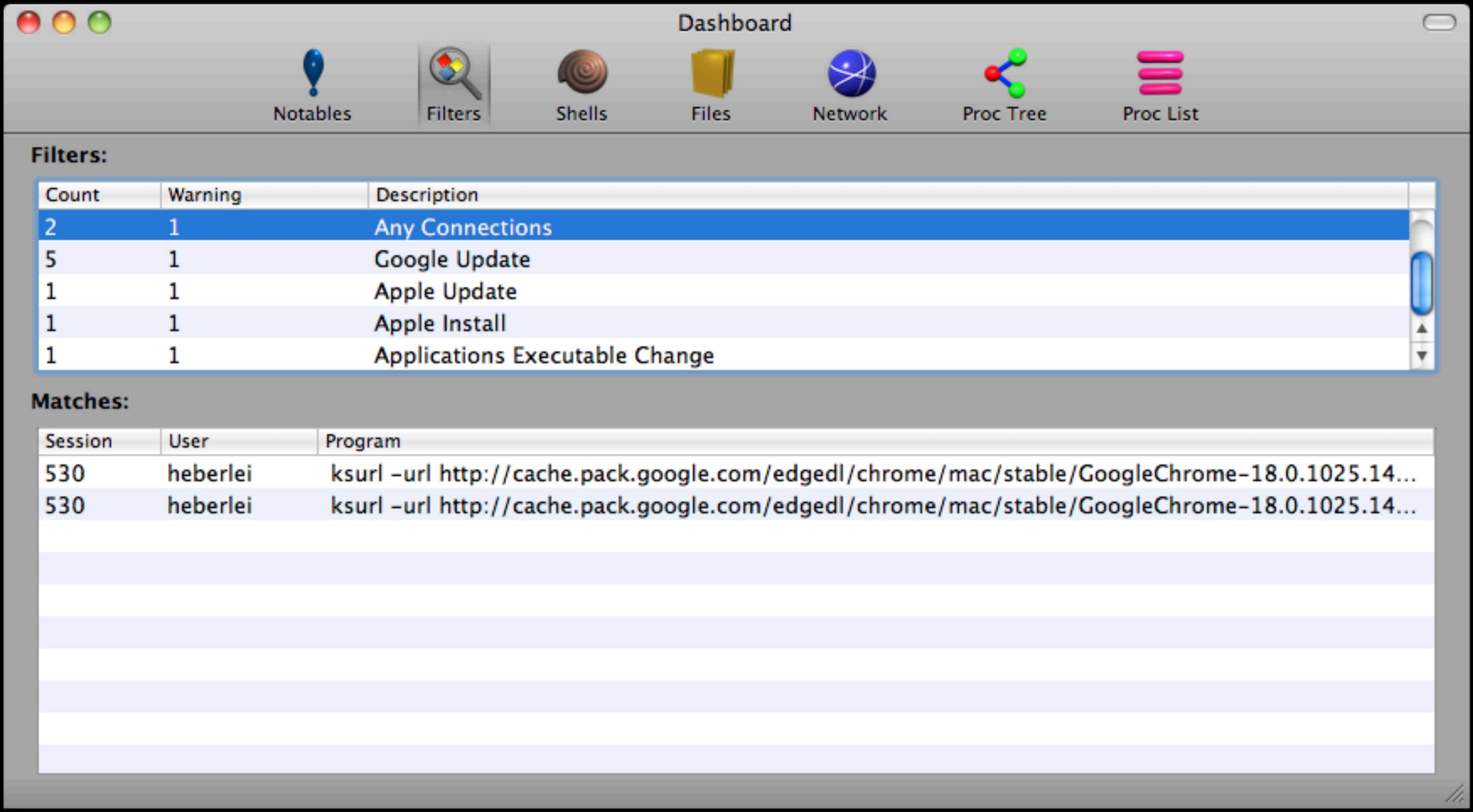
http://www.netsq.com/Research/Single.php?stuff=papers&num=23

The Making of "The Advanced Persistent Threat You Have: Google Chrome"

http://www.netsq.com/Research/Single.php?stuff=papers&num=24

Why Google Update

- C&C agent that wakes up periodically and checks for new commands
- Blends in with normal traffic
- Downloads commands and executes them
- Modifies security-critical software on your system
- Gets rid of the evidence
- If you can’t analyze this, can you analyze real APTs?

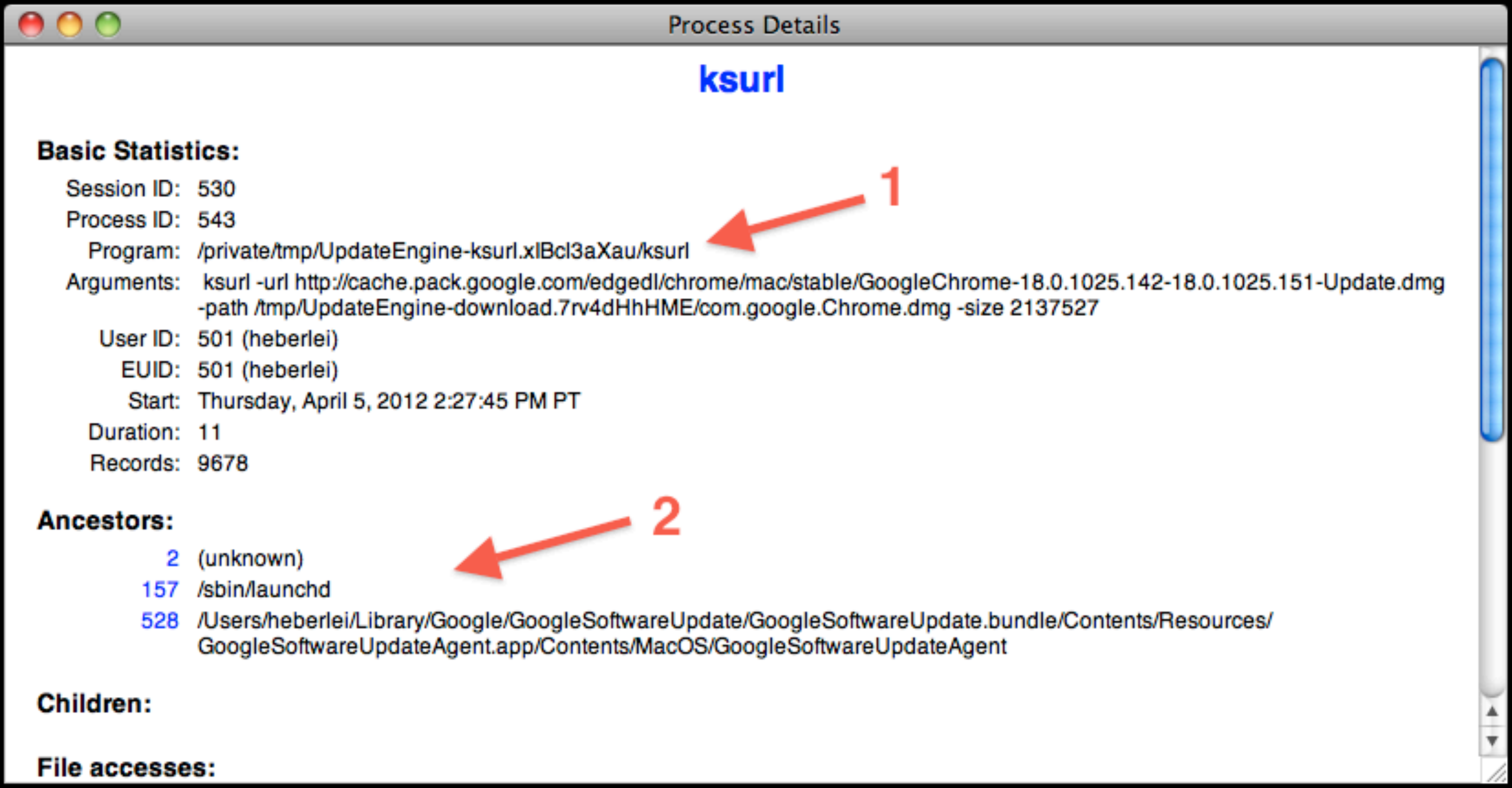


Filters:

Count	Warning	Description
2	1	Any Connections
5	1	Google Update
1	1	Apple Update
1	1	Apple Install
1	1	Applications Executable Change

Matches:

Session	User	Program
530	heberlei	ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.14...
530	heberlei	ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.14...



ksurl

Basic Statistics:

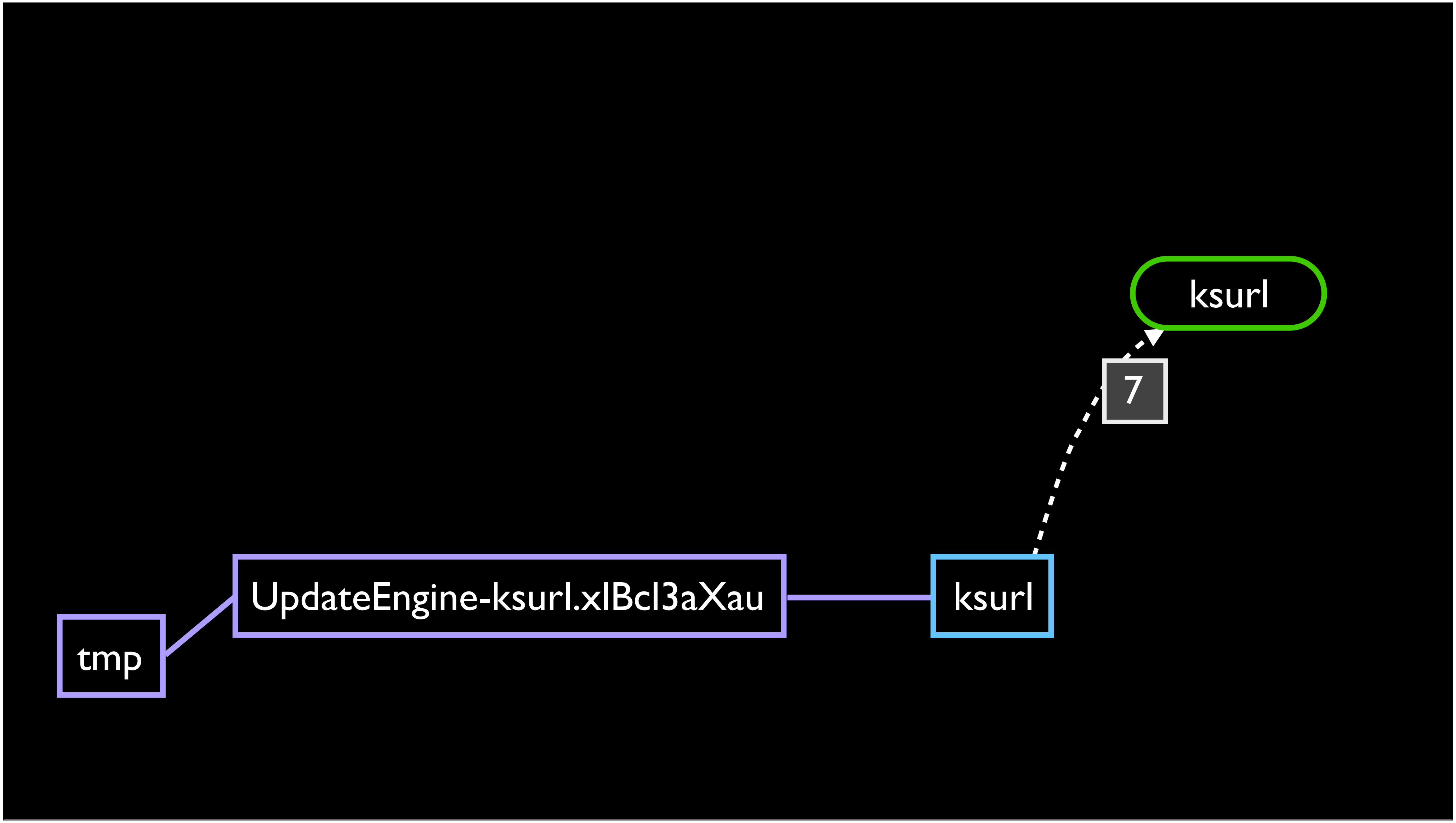
Session ID: 530
Process ID: 543
Program: /private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
Arguments: ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.142-18.0.1025.151-Update.dmg -path /tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg -size 2137527
User ID: 501 (heberlei)
EUID: 501 (heberlei)
Start: Thursday, April 5, 2012 2:27:45 PM PT
Duration: 11
Records: 9678

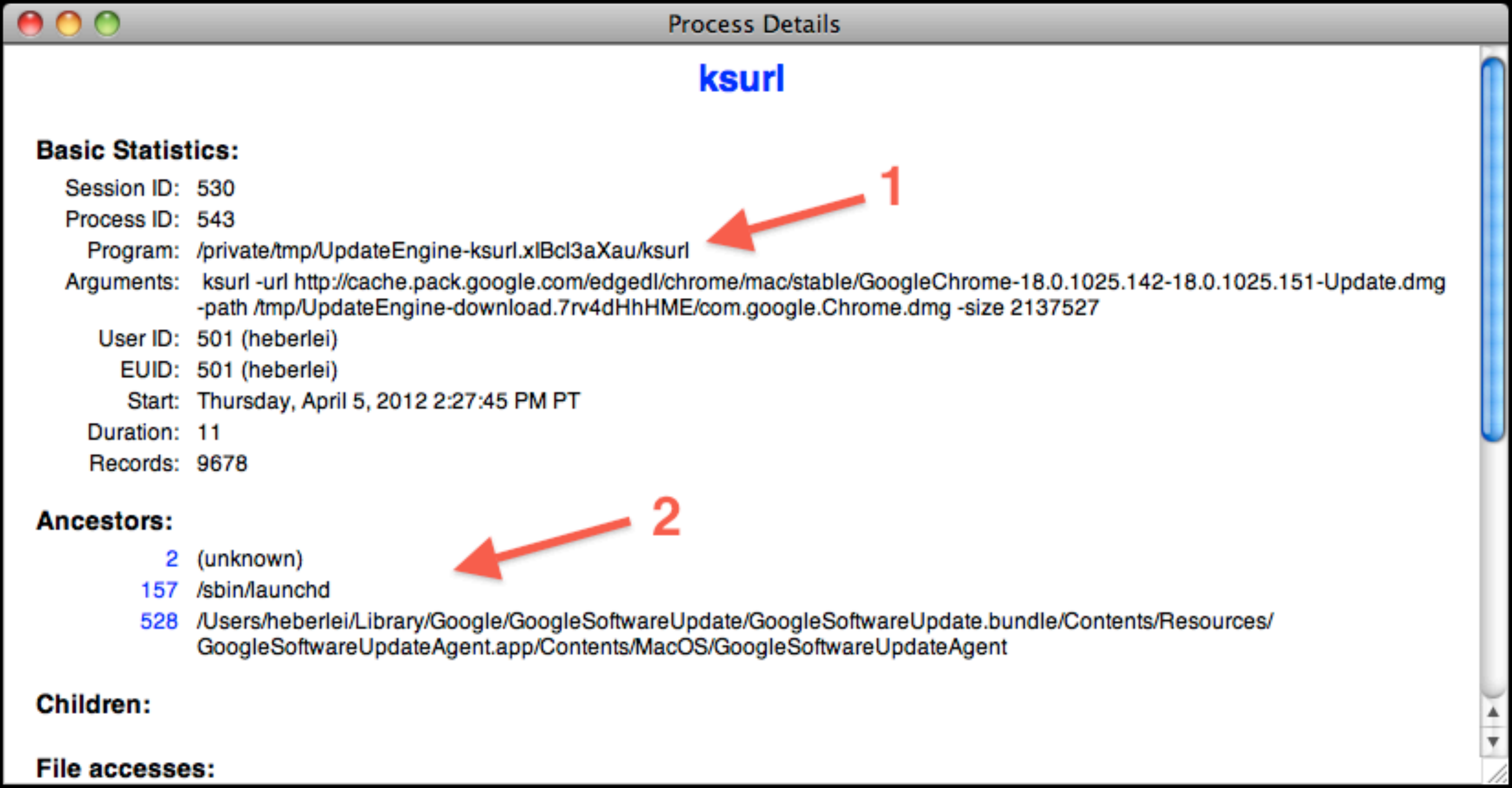
Ancestors:

2 (unknown)
157 /sbin/launchd
528 /Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareUpdateAgent.app/Contents/MacOS/GoogleSoftwareUpdateAgent

Children:

File accesses:


ksurl
7
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl



ksurl

Basic Statistics:

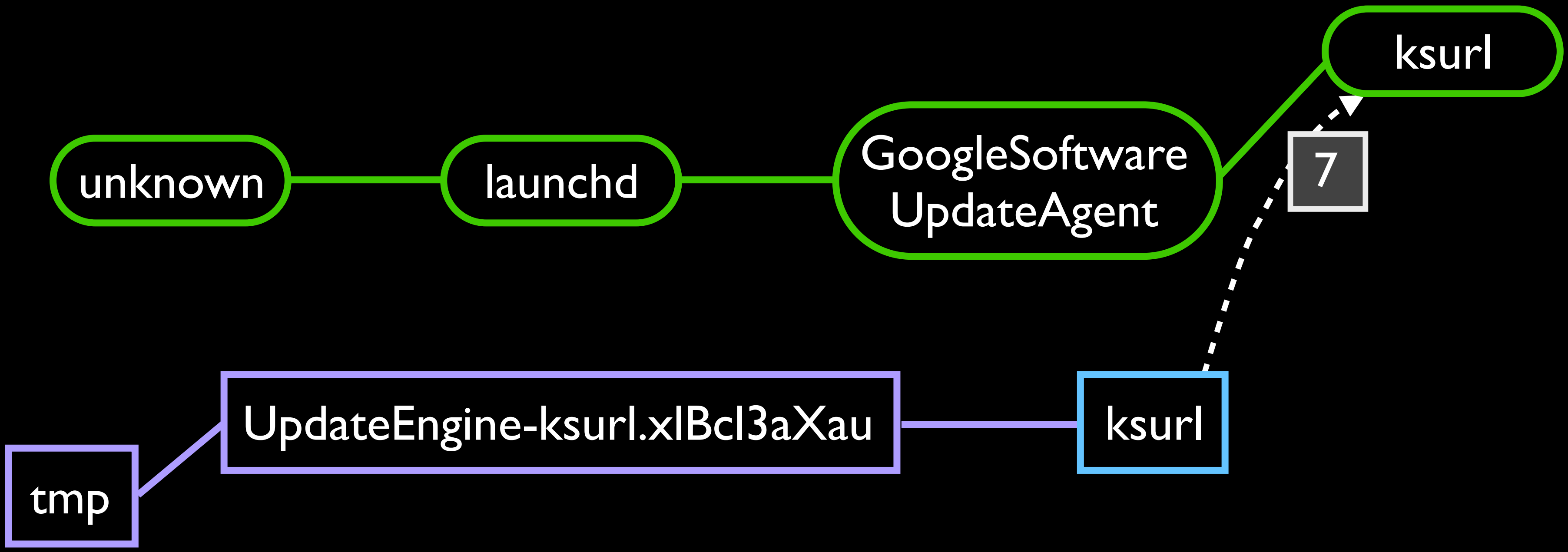
Session ID: 530
Process ID: 543
Program: /private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
Arguments: ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.142-18.0.1025.151-Update.dmg -path /tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg -size 2137527
User ID: 501 (heberlei)
EUID: 501 (heberlei)
Start: Thursday, April 5, 2012 2:27:45 PM PT
Duration: 11
Records: 9678

Ancestors:

2 (unknown)
157 /sbin/launchd
528 /Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareUpdateAgent.app/Contents/MacOS/GoogleSoftwareUpdateAgent

Children:

File accesses:



unknown

launchd

GoogleSoftware UpdateAgent

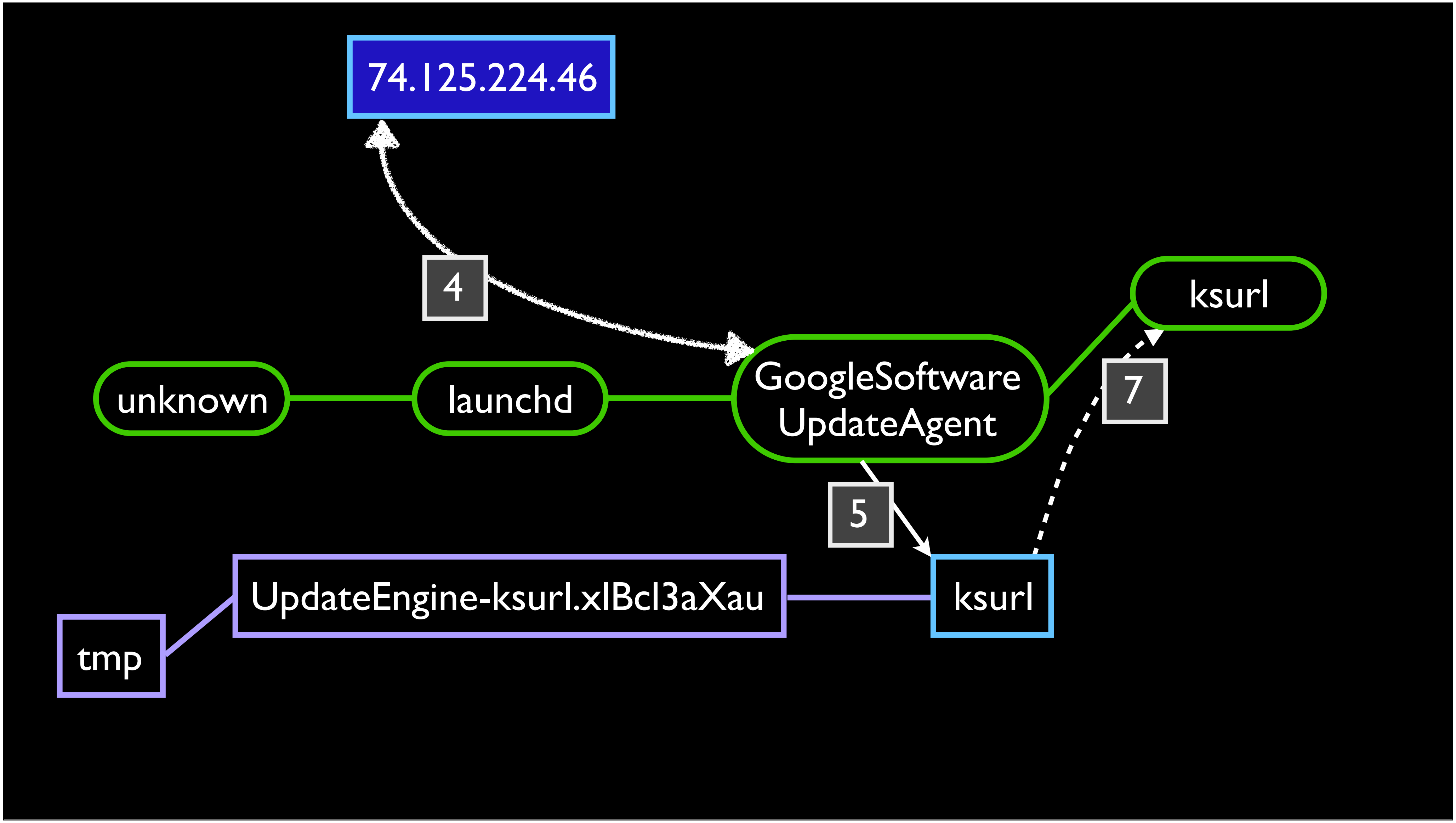
ksurl

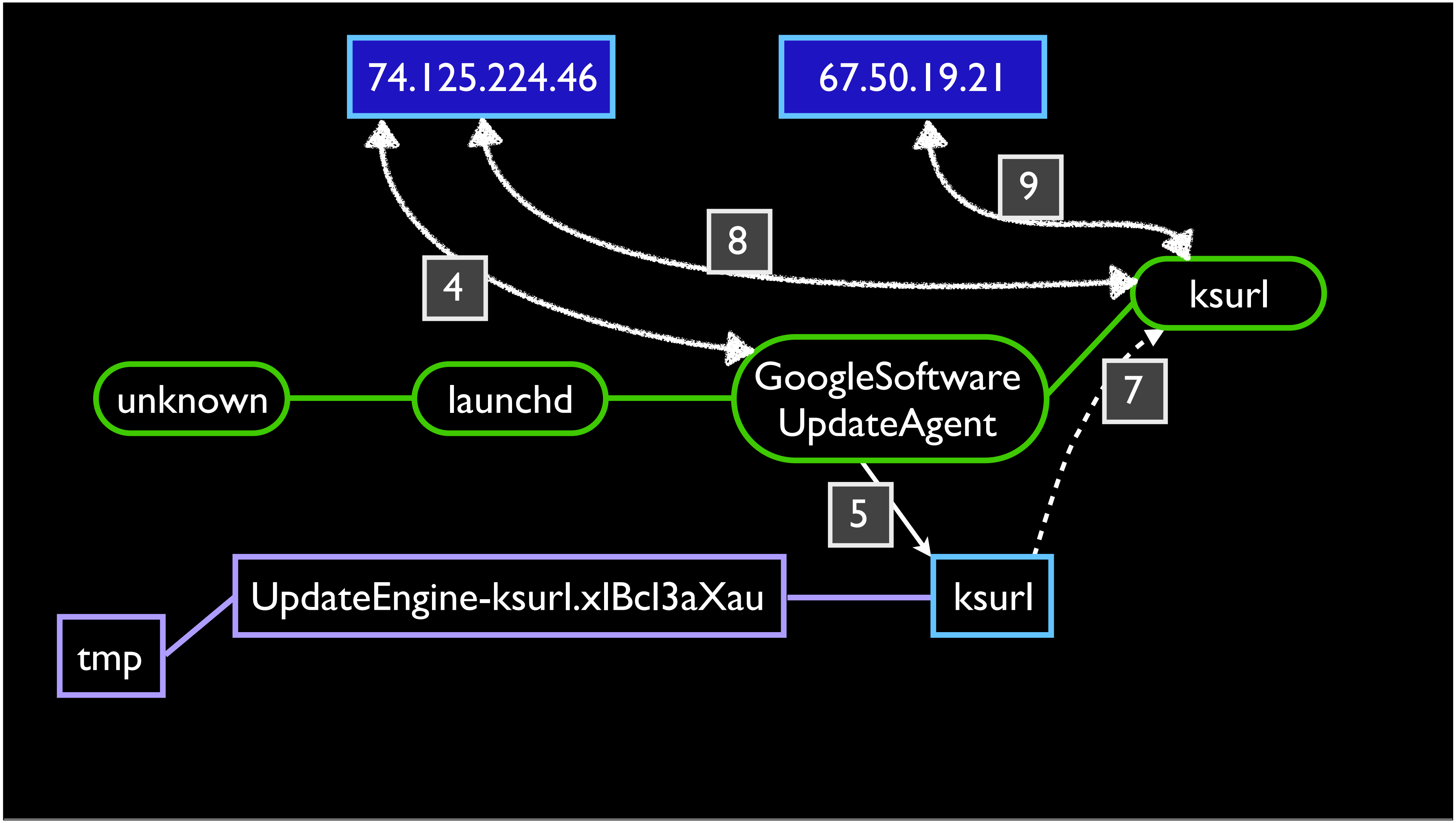
7

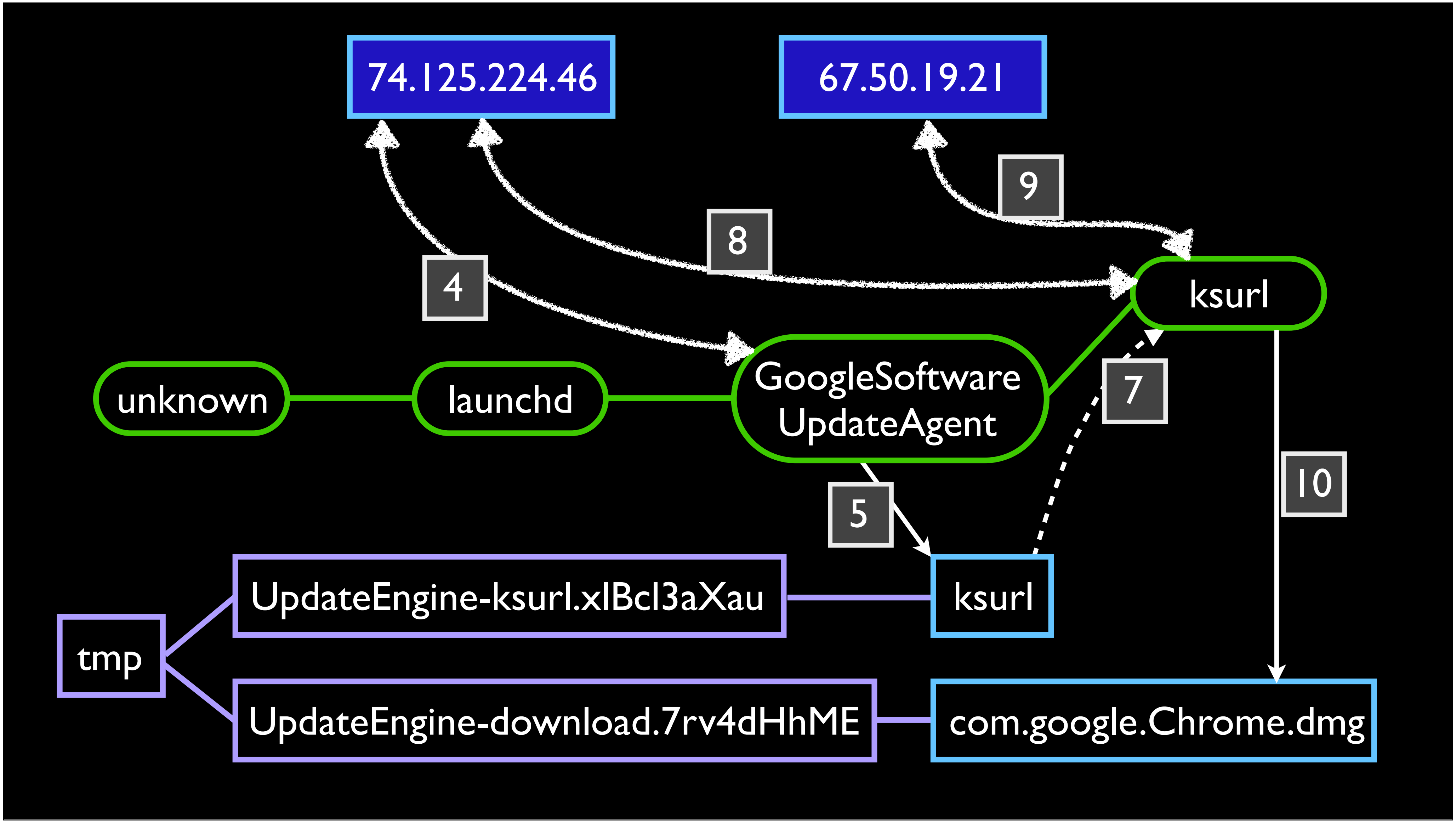
tmp

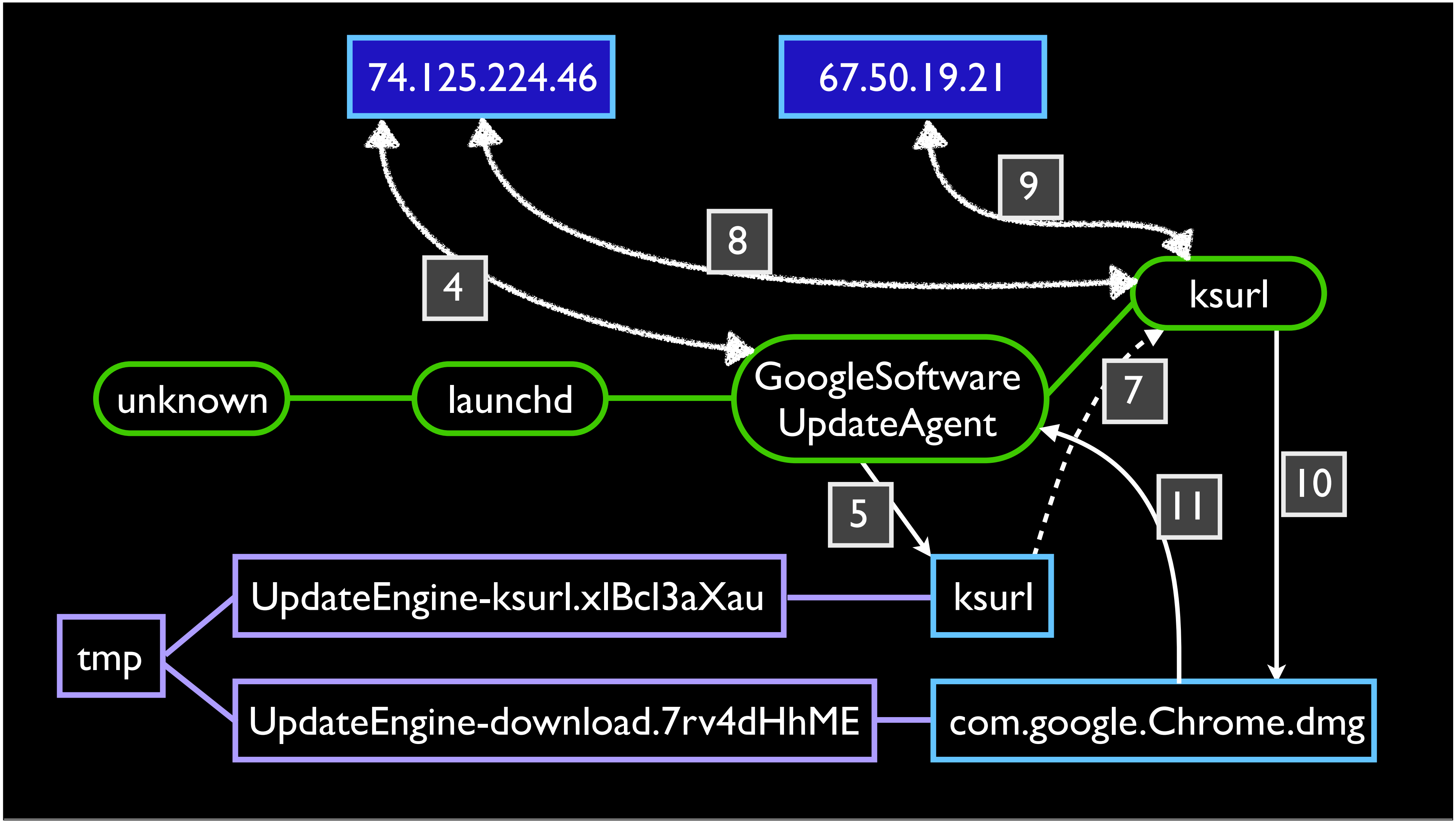
UpdateEngine-ksurl.xlBcl3aXau

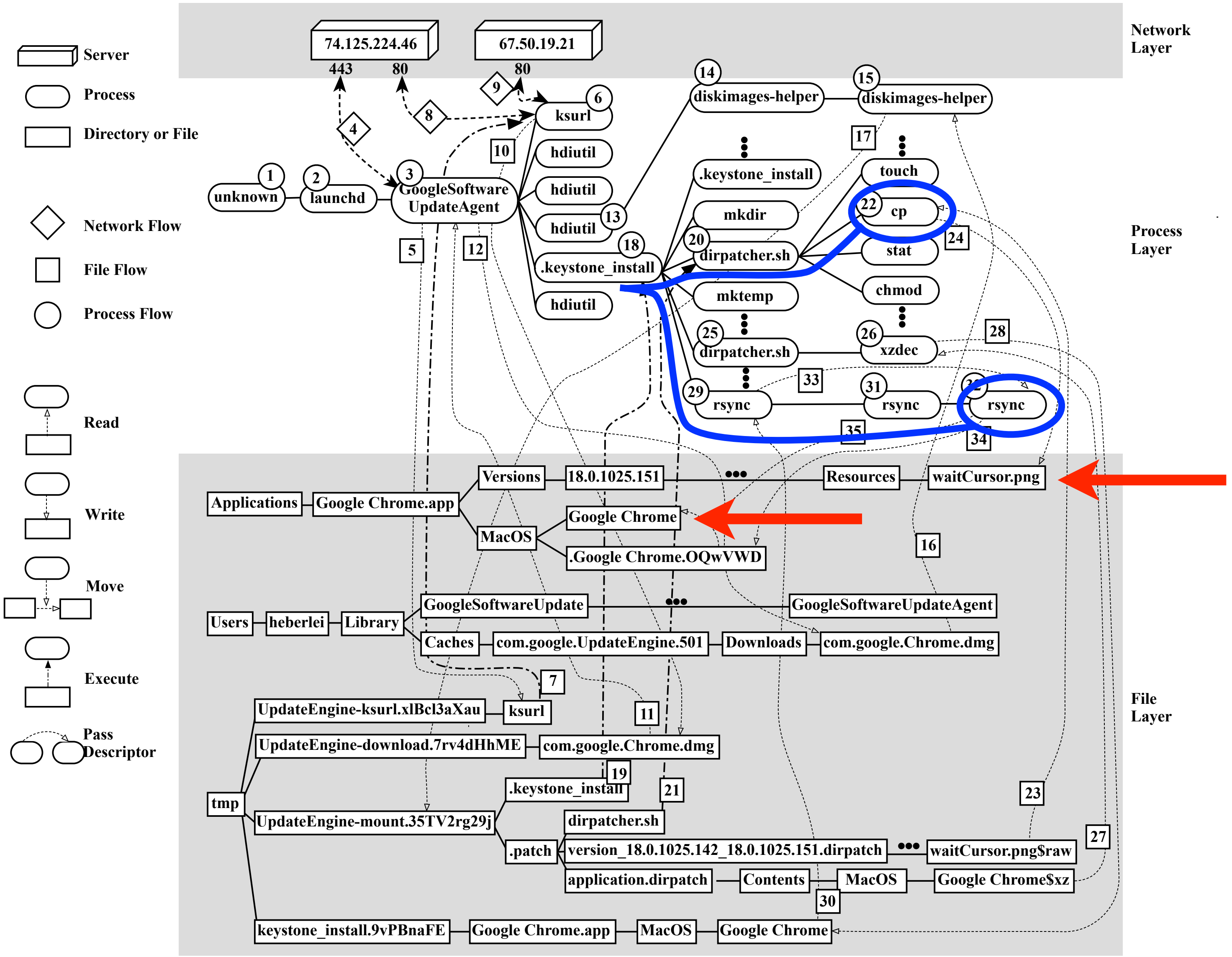
ksurl


74.125.224.46
4
ksurl
unknown
launchd
GoogleSoftware UpdateAgent
7
5
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp

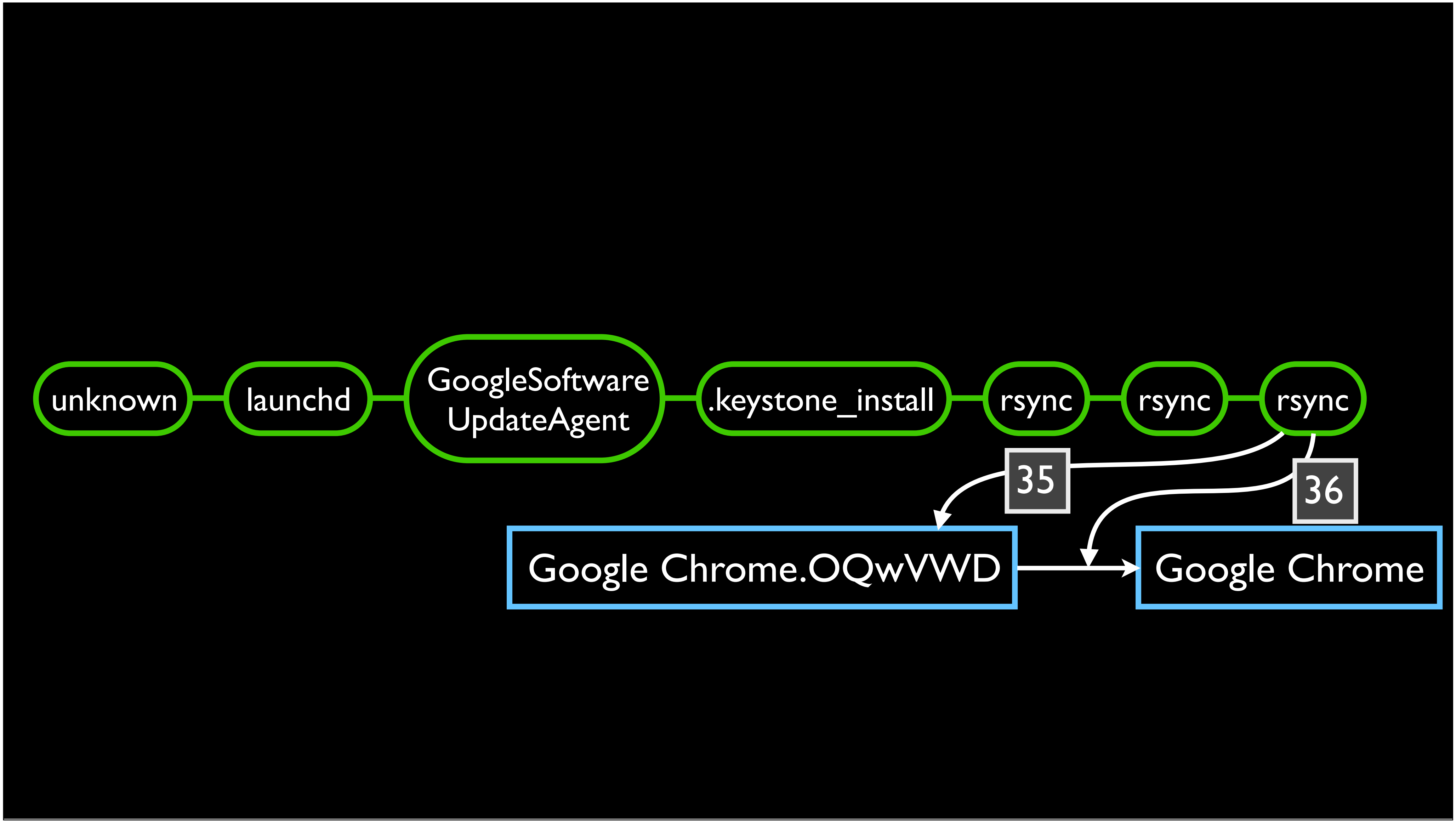

74.125.224.46
67.50.19.21
9
8
4
ksurl
unknown
launchd
GoogleSoftware UpdateAgent
7
5
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp

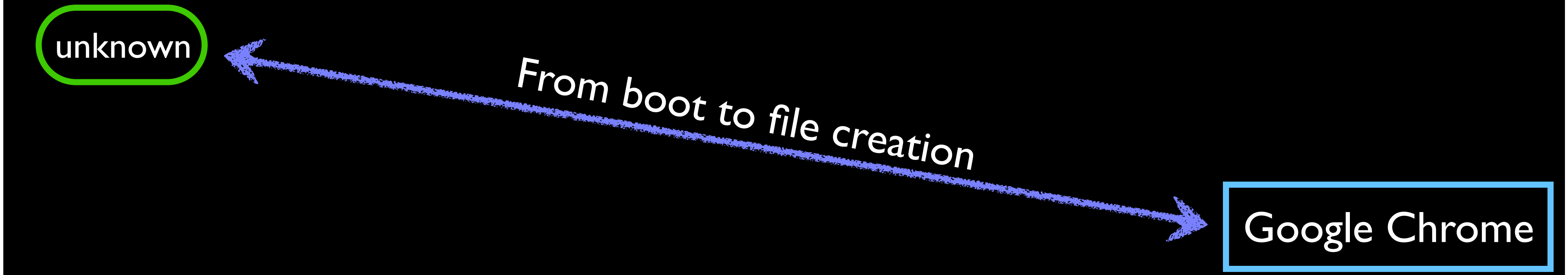

74.125.224.46
67.50.19.21
9
8
4
ksurl
unknown
launchd
GoogleSoftware UpdateAgent
7
10
5
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg


74.125.224.46
67.50.19.21
9
8
4
ksurl
7
GoogleSoftware UpdateAgent
unknown
launchd
5
11
10
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg



Server
Process
Directory or File
Network Flow
File Flow
Process Flow
Read
Write
Move
Execute
Pass Descriptor
Network Layer
Process Layer
File Layer
74.125.224.46
443
80
67.50.19.21
80
unknown
launchd
GoogleSoftware UpdateAgent
ksurl
hdiutil
hdiutil
hdiutil
.keystone_install
hdiutil
diskimages-helper
diskimages-helper
.keystone_install
mkdir
dirpatcher.sh
mktemp
dirpatcher.sh
rsync
touch
cp
stat
chmod
xzdec
rsync
rsync
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
33
34
35
Applications
Google Chrome.app
Versions
18.0.1025.151
Resources
waitCursor.png
MacOS
Google Chrome
.Google Chrome.OQwVWD
Users
heberlei
Library
GoogleSoftwareUpdate
GoogleSoftwareUpdateAgent
Caches
com.google.UpdateEngine.501
Downloads
com.google.Chrome.dmg
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg
.keystone_install
UpdateEngine-mount.35TV2rg29j
dirpatcher.sh
.patch
version_18.0.1025.142_18.0.1025.151.dirpatch
waitCursor.png$raw
application.dirpatch
Contents
MacOS
Google Chrome$xz
keystone_install.9vPBnaFE
Google Chrome.app
MacOS
Google Chrome

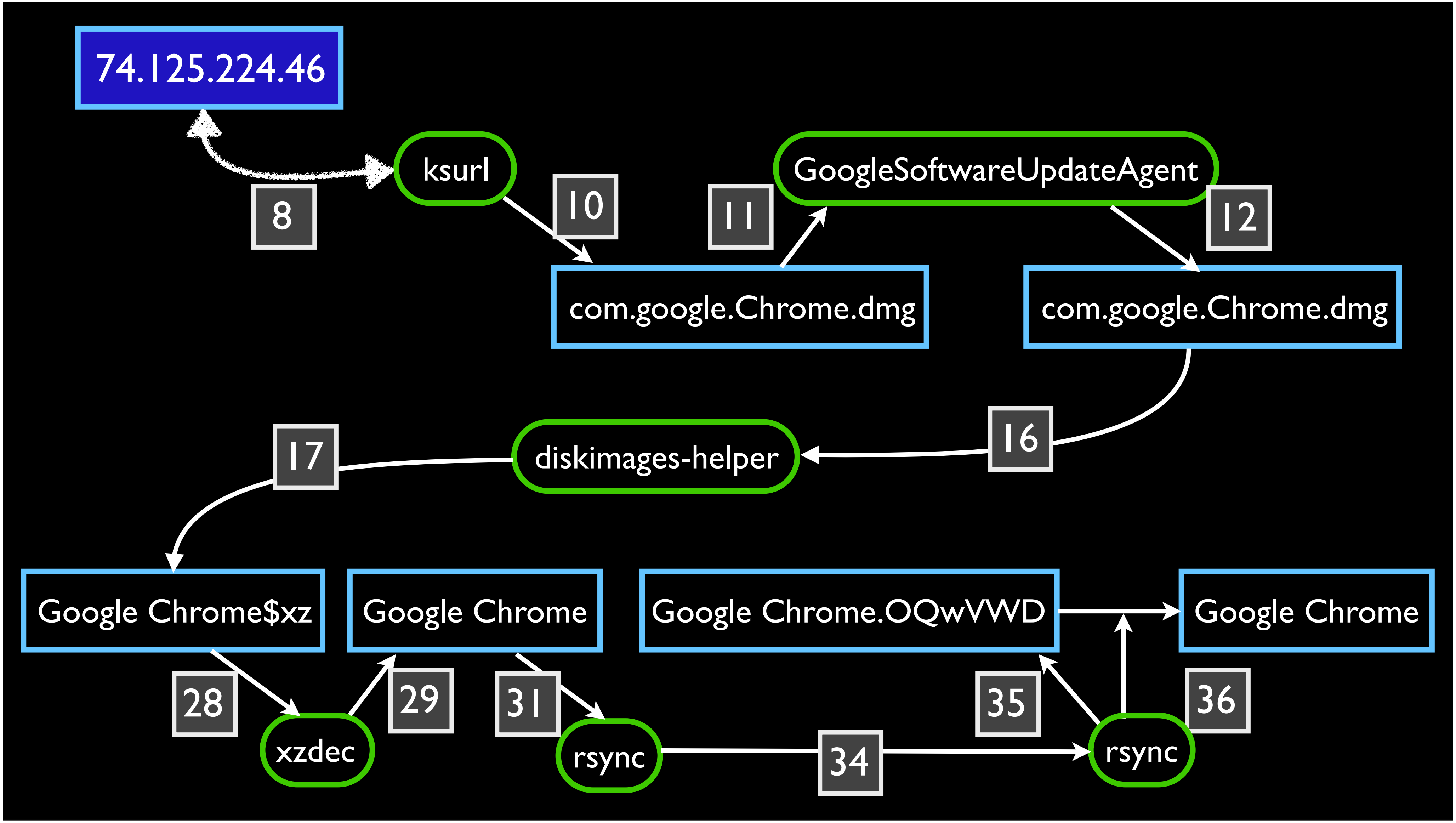

unknown
launchd
GoogleSoftware UpdateAgent
.keystone_install
rsync
rsync
rsync
35
36
Google Chrome.OQwVWD
Google Chrome

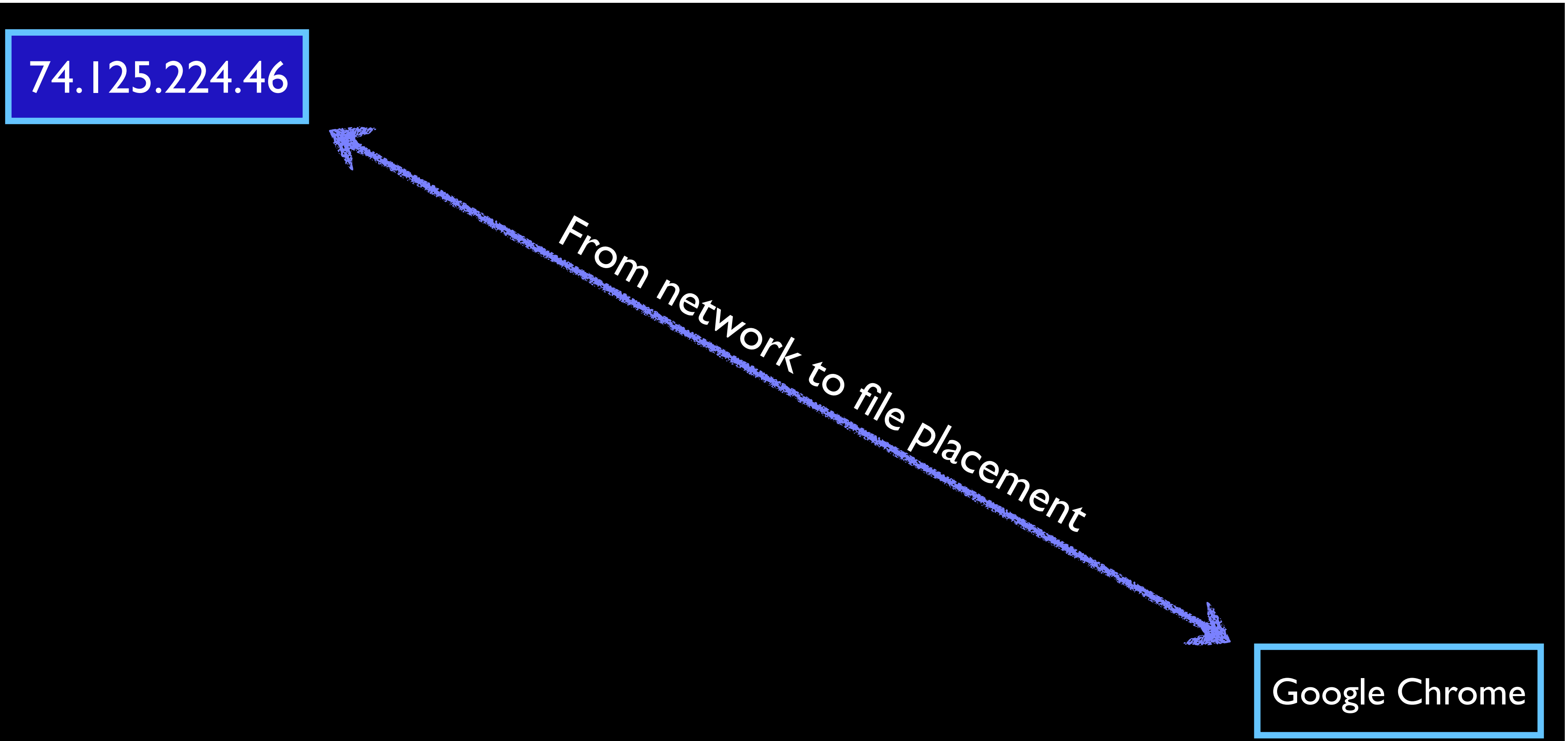


unknown

From boot to file creation

Google Chrome


74.125.224.46
8
ksurl
10
com.google.Chrome.dmg
11
GoogleSoftwareUpdateAgent
12
com.google.Chrome.dmg
16
diskimages-helper
17
Google Chrome$xz
28
xzdec
29
Google Chrome
31
rsync
34
rsync
35
Google Chrome.OQwVWD
36
Google Chrome



74.125.224.46

From network to file placement

Google Chrome

Conclusions

- Today’s emerging threat environment includes professional attackers
- We are failing because our tools, data source, and concepts of operations don’t match the threat of professional attackers
- “Glowing Embers” shows a way to establish a C&C agent
- “Crossing the air gap” shows nothing is safe
- “Advanced Persistent Threats” captures the key concepts
- “Google, the APT you have” lets you practice for real APTs

Contact me: Todd Heberlein

web: www.NetSQ.com

email: LTH@NetSQ.com

email: todd_heberlein@mac.com