CSE 127: Computer Security

Malware

Nadia Heninger and Deian Stefan

UCSD

Fall 2019

Some material from Stefan Savage and David Wagner

Vulnerability of the week: Sudo flaw

thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html

Today

We’ve talked about ways machines can be compromised.

What happens afterward?

- Malware

Viruses, Worms, and Rootkits

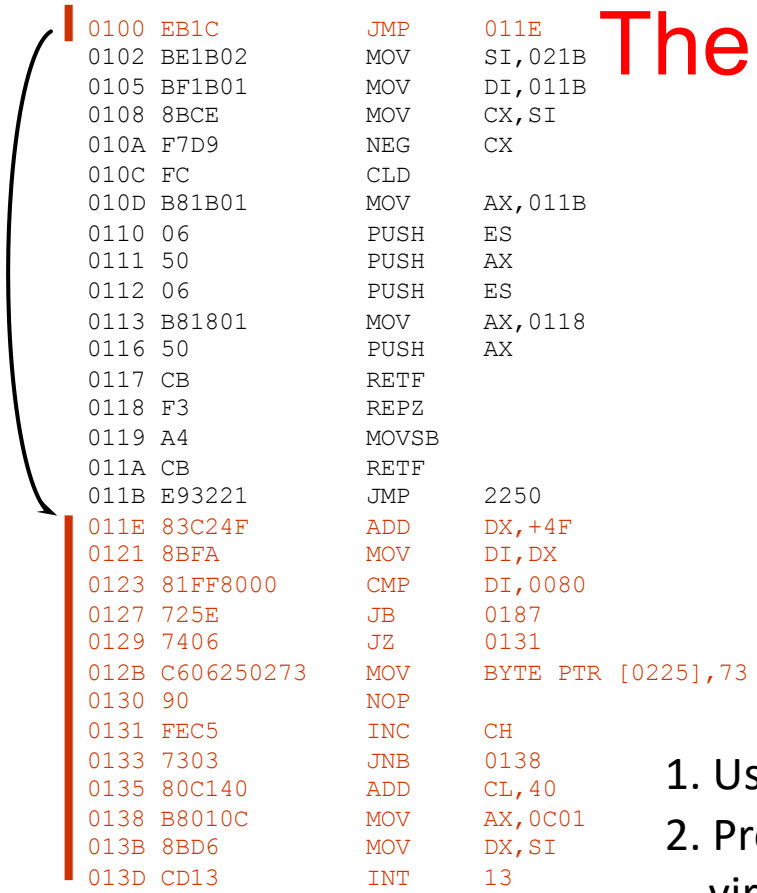
- Virus: Code propagates by arranging itself to eventually be executed.
  Biological analogue: altering stored code.

- Worm: Self-propagates by arranging itself to immediately be executed.
  Alters running code.

Not really a sharp distinction.

- Rootkit: Program designed to give access to an attacker while actively hiding its presence.

The Simple Virus



```
0100 EB1C          JMP     011E
0102 BE1B02        MOV     SI,021B
0105 BF1B01        MOV     DI,011B
0108 8BCE          MOV     CX,SI
010A F7D9          NEG     CX
010C FC            CLD
010D B81B01        MOV     AX,011B
0110 06            PUSH    ES
0111 50            PUSH    AX
0112 06            PUSH    ES
0113 B81801        MOV     AX,0118
0116 50            PUSH    AX
0117 CB            RETF
0118 F3            REPZ
0119 A4            MOVSB
011A CB            RETF
011B E93221        JMP     2250
011E 83C24F        ADD     DX,+4F
0121 8BFA          MOV     DI,DX
0123 81FF8000      CMP     DI,0080
0127 725E          JB      0187
0129 7406          JZ      0131
012B C606250273    MOV     BYTE PTR [0225],73
0130 90            NOP
0131 FEC5          INC     CH
0133 7303          JNB     0138
0135 80C140        ADD     CL,40
0138 B8010C        MOV     AX,0C01
013B 8BD6          MOV     DX,SI
013D CD13          INT     13
```

Infected Program

1. User runs an infected program.
2. Program transfers control to the virus.

The Simple Virus

```
0100 EB1C          JMP     011E
0102 BE1B02        MOV     SI,021B
0105 BF1B01        MOV     DI,011B
0108 8BCE          MOV     CX,SI
010A F7D9          NEG     CX
010C FC            CLD
010D B81B01        MOV     AX,011B
0110 06            PUSH    ES
0111 50            PUSH    AX
0112 06            PUSH    ES
0113 B81801        MOV     AX,0118
0116 50            PUSH    AX
0117 CB            RETF
0118 F3            REPZ
0119 A4            MOVSB
011A CB            RETF
011B E93221        JMP     2250
011E 83C24F        ADD     DX,+4F
0121 8BFA          MOV     DI,DX
0123 81FF8000      CMP     DI,0080
0127 725E          JB      0187
0129 7406          JZ      0131
012B C606250273    MOV     BYTE PTR [0225],73
0130 90            NOP
0131 FEC5          INC     CH
0133 7303          JNB     0138
0135 80C140        ADD     CL,40
0138 B8010C        MOV     AX,0C01
013B 8BD6          MOV     DX,SI
013D CD13          INT     13
```

Infected Program

```
0100 B435          MOV     AH,35
0102 B021          MOV     AL,21
0104 CD21          INT     21
0106 8C06A002      MOV     [02A0],ES
010A 891E9E02      MOV     [029E],BX
010E B425          MOV     AH,25
0110 B021          MOV     AL,21
0112 BA2001        MOV     DX,0120
0115 CD21          INT     21
0117 83C24F        ADD     DX,+4F
011A 8BFA          MOV     DI,DX
011C 81FF8000      CMP     DI,0080
0120 725E          JB      0187
0122 7406          JZ      0131
0124 C606250273    MOV     BYTE PTR [0225],73
0129 90            NOP
012A FEC5          INC     CH
012C 7303          JNB     0138
012E 80C140        ADD     CL,40
0132 B8010C        MOV     AX,0C01
0135 8BD6          MOV     DX,SI
0137 CD13          INT     13
```

3. Virus locates a new program.
4. Virus appends its logic to the end of the new file.

The Simple Virus

```
0100 EB1C          JMP     011E
0102 BE1B02        MOV     SI,021B
0105 BF1B01        MOV     DI,011B
0108 8BCE          MOV     CX,SI
010A F7D9          NEG     CX
010C FC            CLD
010D B81B01        MOV     AX,011B
0110 06            PUSH    ES
0111 50            PUSH    AX
0112 06            PUSH    ES
0113 B81801        MOV     AX,0118
0116 50            PUSH    AX
0117 CB            RETF
0118 F3            REPZ
0119 A4            MOVSB
011A CB            RETF
011B E93221        JMP     2250
011E 83C24F        ADD     DX,+4F
0121 8BFA          MOV     DI,DX
0123 81FF8000      CMP     DI,0080
0127 725E          JB      0187
0129 7406          JZ      0131
012B C606250273    MOV     BYTE PTR [0225],73
0130 90            NOP
0131 FEC5          INC     CH
0133 7303          JNB     0138
0135 80C140        ADD     CL,40
0138 B8010C        MOV     AX,0C01
013B 8BD6          MOV     DX,SI
013D CD13          INT     13
```

Infected Program

```
0100 EB1C          JMP     0117
0102 B021          MOV     AL,21
0104 CD21          INT     21
0106 8C06A002      MOV     [02A0],ES
010A 891E9E02      MOV     [029E],BX
010E B425          MOV     AH,25
0110 B021          MOV     AL,21
0112 BA2001        MOV     DX,0120
0115 CD21          INT     21
0117 83C24F        ADD     DX,+4F
011A 8BFA          MOV     DI,DX
011C 81FF8000      CMP     DI,0080
0120 725E          JB      0187
0122 7406          JZ      0131
0124 C606250273    MOV     BYTE PTR [0225],73
0129 90            NOP
012A FEC5          INC     CH
012C 7303          JNB     0138
012E 80C140        ADD     CL,40
0132 B8010C        MOV     AX,0C01
0135 8BD6          MOV     DX,SI
0137 CD13          INT     13
```

5. Virus updates the new program so the virus gets control when the program is launched.

Summary of Malicious Behavior

- Malware runs with some user privileges on machine.
  Can do anything that user can do, or escalate privileges.

- Mischief/Malice:
  - Pop up messages.
  - Trash files.
  - Damage hardware.

- Surveillance/espionage:
  - Exfiltrate information
  - Keylogging, screen capture, audio, camera

Summary of Malicious Behavior

- Economics/crime:
  - Botnet: A network of autonomous programs controlled by a remote attacker can be used at a platform for attacks.
    - Denial of service
    - Spam and clickfraud
    - Launch new exploits
  - Spam
    - Selling goods/services
    - Advanced fee fraud (419 scam)
    - Phishing/spearphishing
  - Clickfraud
    - Produce clicks on ads for revenue
    - or to deplete others' ad budgets
  - Extortion attacks
    - Ransomware: encrypt files and demand payment to decrypt
  - Steal credentials
  - Blackmail

How does malware run?

Attack a network-accessible vulnerable service.

- The Morris Worm (1988) exploited a buffer overflow in the fingerd utility, also propagated itself via rsh and cracked passwords.
  - Bogged down infected machines by uncontrolled spawning.
  - Infected 10% of internet hosts at the time.

office is, the number of their phone extension and so on. The Berkeley[3] version of the *finger* server is a really trivial program: it reads a request from the originating host, then runs the local *finger* program with the request as an argument and ships the output back. Unfortunately the *finger* server reads the remote request with *gets*(), a standard C library routine that dates from the dawn of time and which does not check for overflow of the server's 512 byte request buffer on the stack. The worm supplies the finger server with a request that is 536 bytes long; the bulk of the request is some VAX machine code that asks the system to execute the command interpreter *sh*, and the extra 24 bytes represent just enough data to write over the server's stack frame for the main routine. When the main routine of the server exits, the calling function's program counter is supposed to be restored from the stack, but the worm wrote over this program counter with one that points to the VAX code in the request buffer. The program jumps to the worm's code and runs the command interpreter, which the worm uses to enter its bootstrap.

How does malware run?

Attack a network-accessible vulnerable service.

- The Blaster Worm (2003) attacked a buffer overflow in the MS RPC interface.

Microsoft Security Bulletin MS03-026

Buffer Overrun In RPC Interface Could Allow Code Execution (823980)

Originally posted: July 16, 2003
Revised: September 10, 2003

Summary

Who should read this bulletin:
Users running Microsoft ® Windows ®

Impact of vulnerability:
Run code of attacker's choice

Maximum Severity Rating:
Critical

Recommendation:
Systems administrators should apply the patch immediately

End User Bulletin:
An end user version of this bulletin is available at:

http://www.microsoft.com/athome/security/update/bulletins/default.mspx.

The Forensics of a Virus

July 1	July 16	July 25	Aug 11
Vulnerability reported to us / Patch in progress	**Bulletin & patch available No exploit**	**Exploit code in public**	**Worm in the world**

Report

- Vulnerability in RPC/DDOM reported
- MS activated highest level emergency response process

Bulletin

- MS03-026 delivered to customers (7/16/03)
- Continued outreach to analysts, press, community, partners, government agencies

Exploit

- X-focus (Chinese group) published exploit tool
- MS heightened efforts to get information to customers

Worm

- Blaster worm discovered –; variants and other viruses hit simultaneously (i.e. “SoBig”)

Blaster shows the complex interplay between security researchers, software companies, and hackers

Source: Microsoft

computers. XFocus also developed a scanning tool that searches the Internet for computers that have the vulnerability and that have not been patched. XFocus made their source code for the exploit and the scanning tool available to the public via the Internet.

10. On or about August 11, 2003, Microsoft became aware of an Internet worm named Blaster. Blaster is based on the XFocus code and scans the Internet for targets, attacks them, and installs itself on the target computers. Each target computer then begins scanning and infecting other computers. Within three days, Blaster had infected an estimated one hundred thousand to two hundred thousand computers. By August 15, 2003, estimates were as high as more than one million infected computers. The Blaster worm included a preprogrammed payload of DDoS attack code. The attack code used a date and time based algorithm to launch a DDoS attack against Microsoft's www.windowsupdate.com domain name beginning on August 16, 2003. The Microsoft servers affected by this are located in the Western District of Washington. Despite exposure in the media and from Microsoft, hundreds of thousands, if not millions, of computers have not yet been patched.

11. On or about August 14, 2003, Microsoft became aware of several variants of the Blaster code. One particular variant was referred to by the Internet security community by a number of different names including "W32/Lovesan.worm.b" (hereinafter "Lovesan B". Microsoft engineers were able to obtain several copies of executable code for this variant. Microsoft engineers disassembled the code and were able to understand what this variant does. Lovesan B contains a variant of the Blaster worm, renamed "teekids.exe". This variant code is

How does malware run?

Attack a network-accessible vulnerable service.

- The WannaCry Ransomware (2017) used a Windows SMB exploit from the Shadow Broker archive called "Eternal Blue".

WannaCry Malware

- The "Eternal Blue" exploit used in WannaCry was developed by the NSA and not disclosed to Microsoft.
- The WannaCry ransomware repurposed this exploit after it was leaked, and it took down many companies.
- Marcus Hutchins discovered a “kill switch” sinkhole domain that stopped the spread of the malware.

Microsoft Security Bulletin MS17-010 – Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

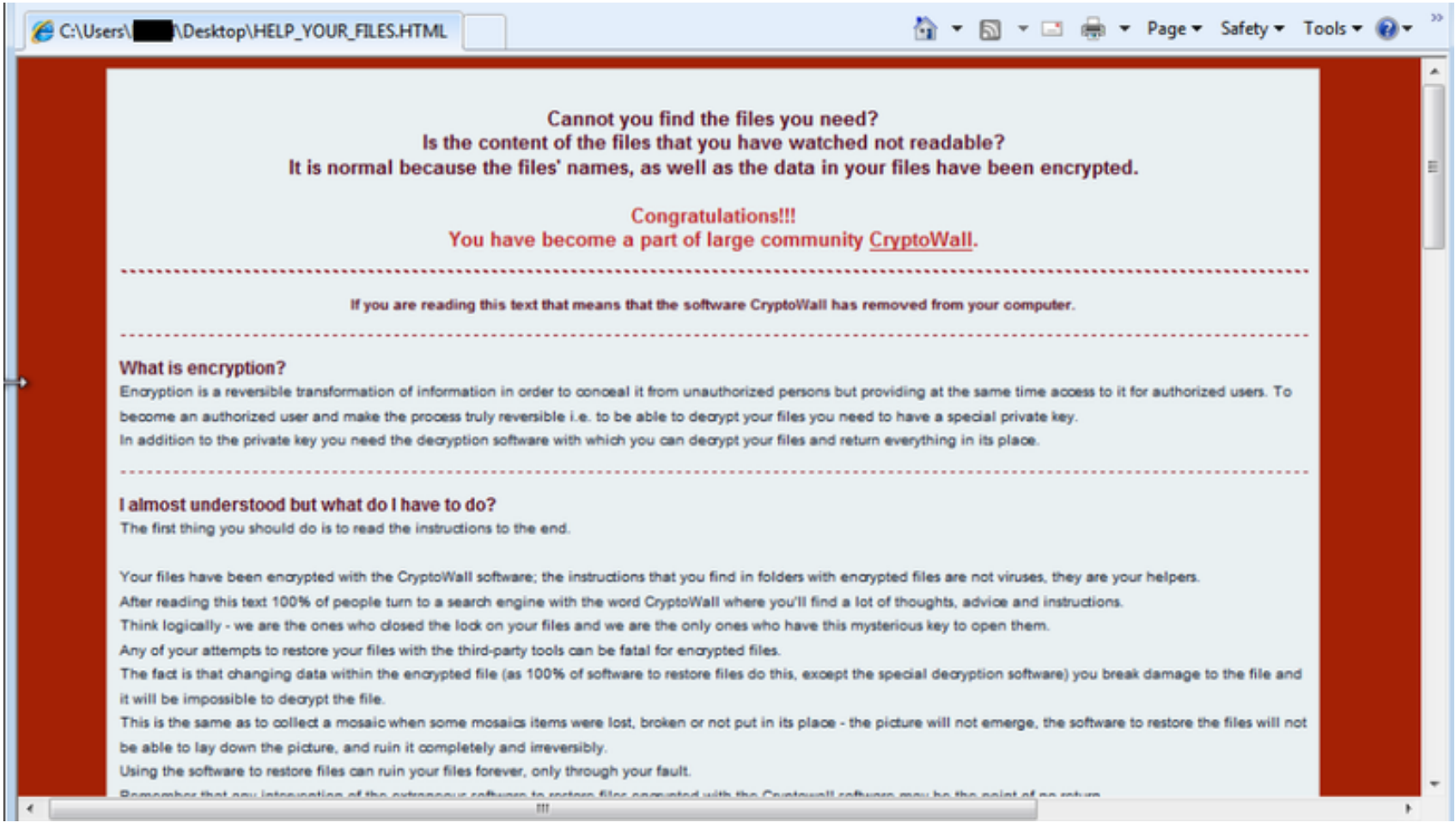
For more information about this update, see Microsoft Knowledge Base Article 4013389.

On this page

How does malware run?

Vulnerable client connects to remote system that sends over an attack “driveby”.

- Malvertising: Using web ads to deliver malicious code.
- The Cryptowall malware (2014) was a Cryptolocker clone that was delivered in malicious ads.



How does malware run?

Vulnerable client connects to remote system that sends over an attack “driveby”.

- US Government search warrants describe installing malware on a target’s computer as a “network investigative technique”.

26. In the normal course of operation, websites send content to visitors. A user’s computer downloads that content and uses it to display web pages on the user’s computer. Under the NIT authorized by this warrant, the website would augment that content with some additional computer instructions. When a computer successfully downloads those instructions from Website A, the instructions are designed to cause the “activating” computer to deliver certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the “activating” computer access to any data or functionality of that computer.

How does malware run?

Vulnerable client connects to remote system that sends over an attack “driveby”.

- US Government search warrants describe installing malware on a target’s computer as a “network investigative technique”.

ATTACHMENT B

This warrant authorizes a remote network technique in which law enforcement agents will transmit to each of the TARGET COMPUTERS described in Attachment A code and/or commands intended make the following information available to officers authorized to execute this warrant:

(1) the TARGET COMPUTER’s actual IP address, and the date and time that the IP address is determined;

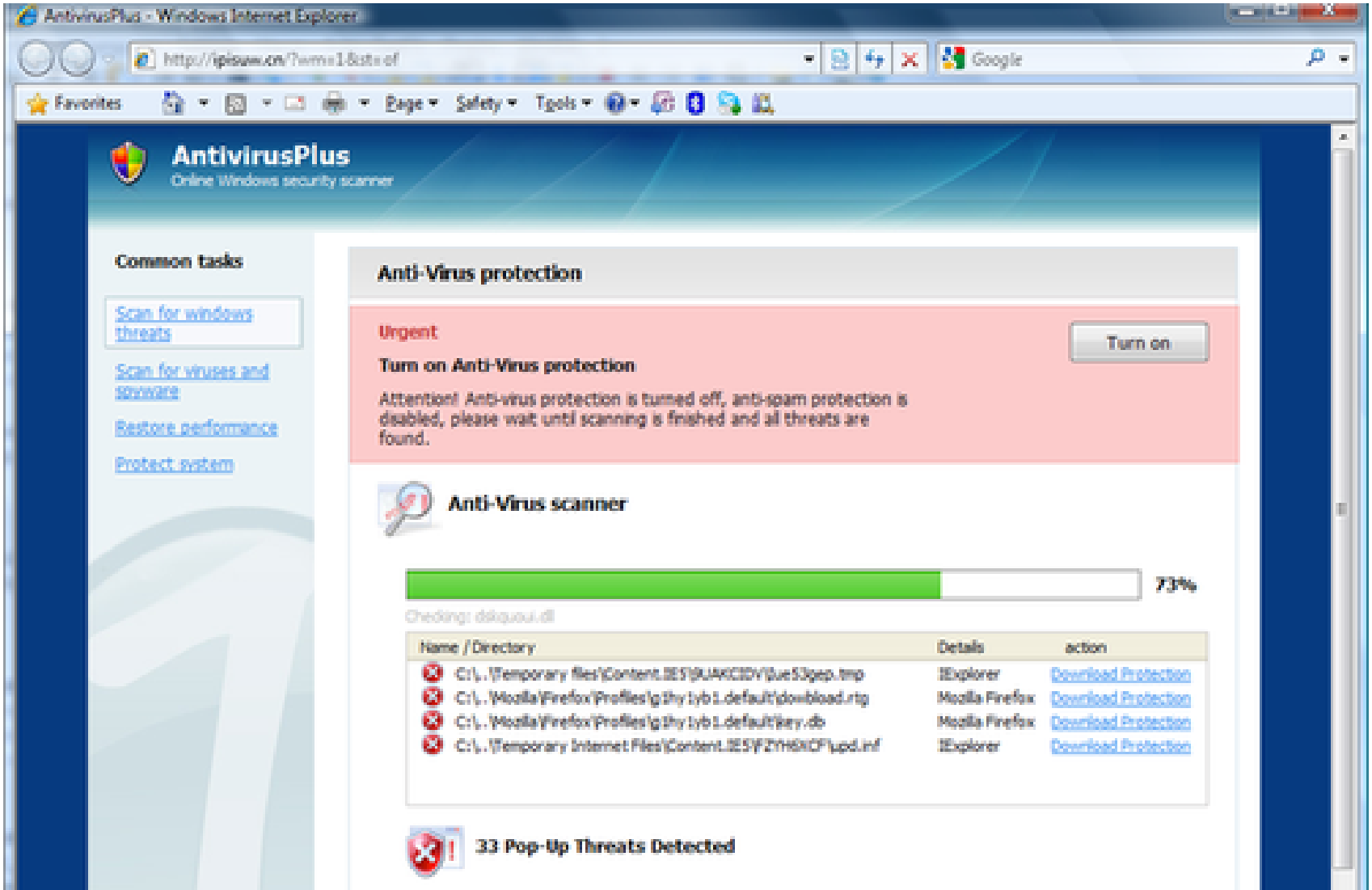
(2) The TARGET COMPUTER’S Computer Name and Media Access Control Address; and

(3) a unique identifier (e.g., a series of numbers, letters, and/or special characters) for the TARGET COMPUTER.

How does malware run?

Social engineering: Trick user into running or installing.

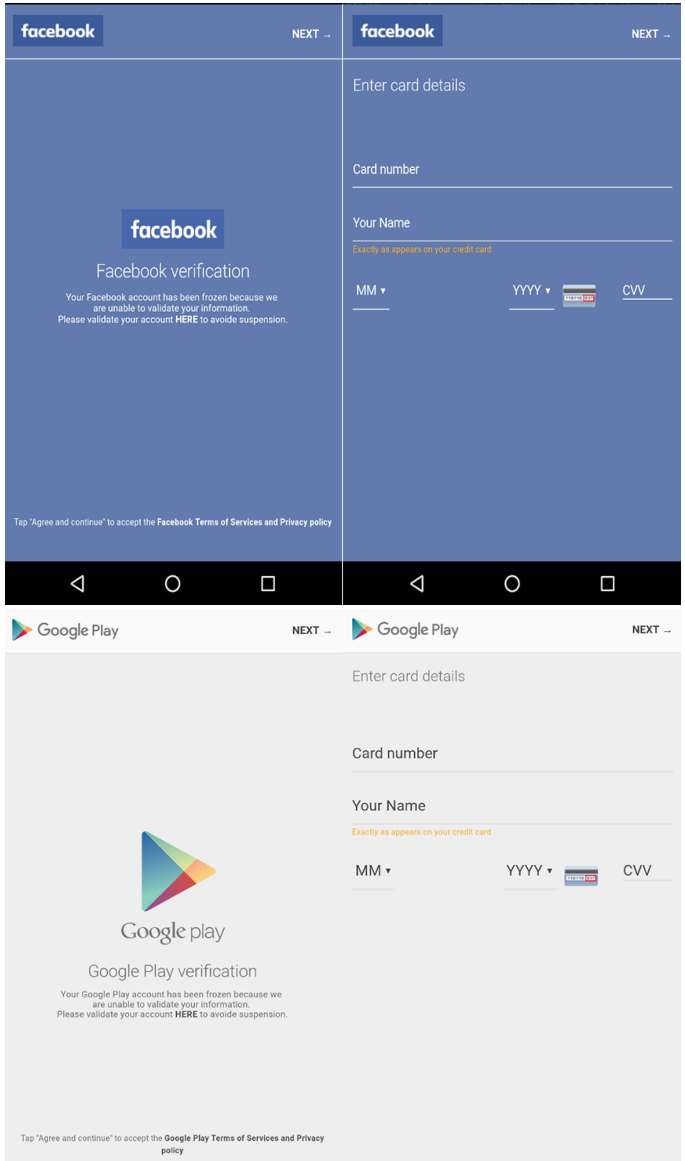
- Fake antivirus: Pops up warning that machine is infected and offers to clean for a fee.



How does malware run?

Social engineering: Trick user into running or installing.

- Flashlight trojan horse apps that steal credentials.



How does malware run?

Social engineering: Trick user into running or installing.

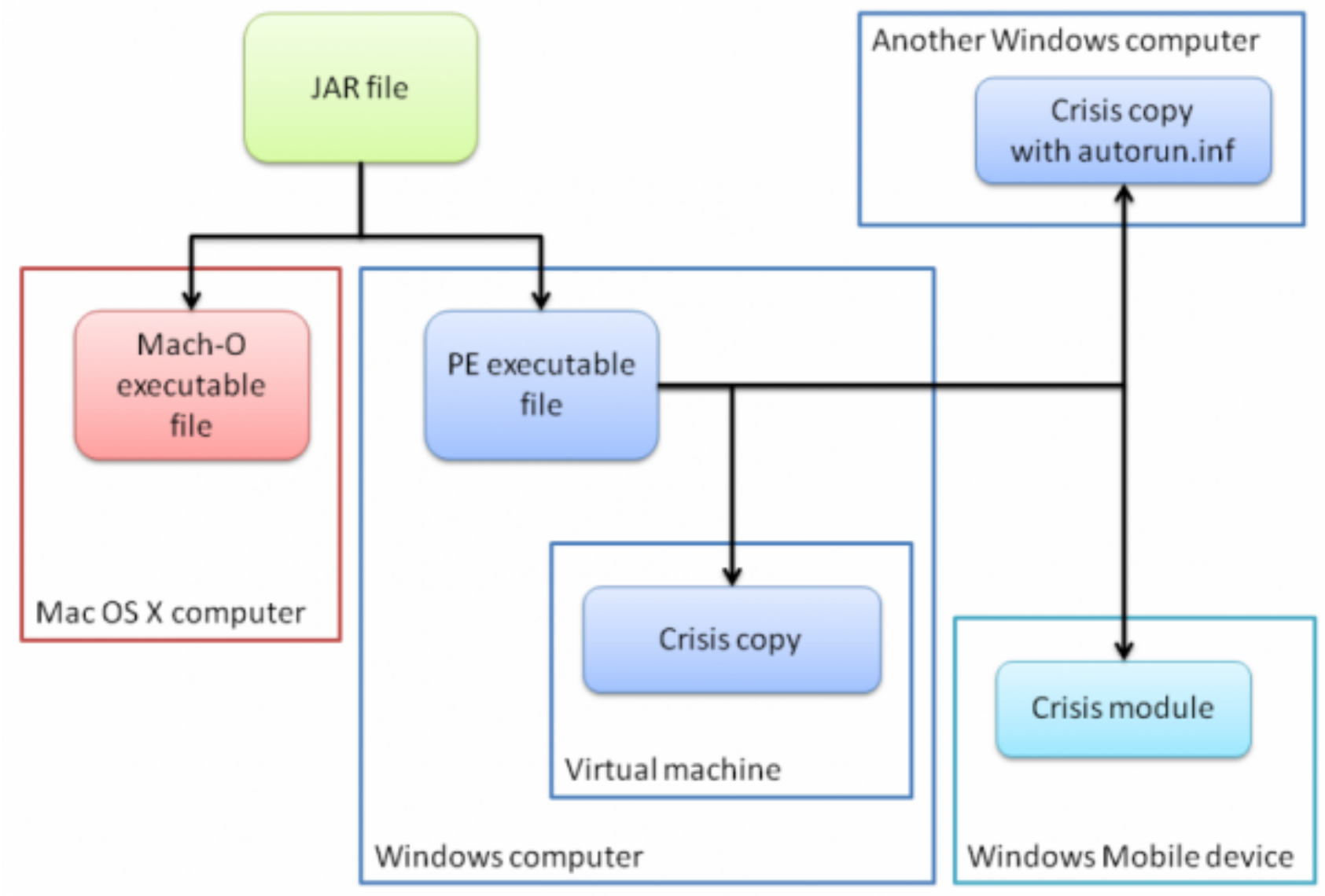
- Hacking Team: State-sponsored malware (2012)

Uploaded to contact form on July 13, 2012:

Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d embrouilles. . .
http://freeme.eu5.org/scandale%20(2).doc

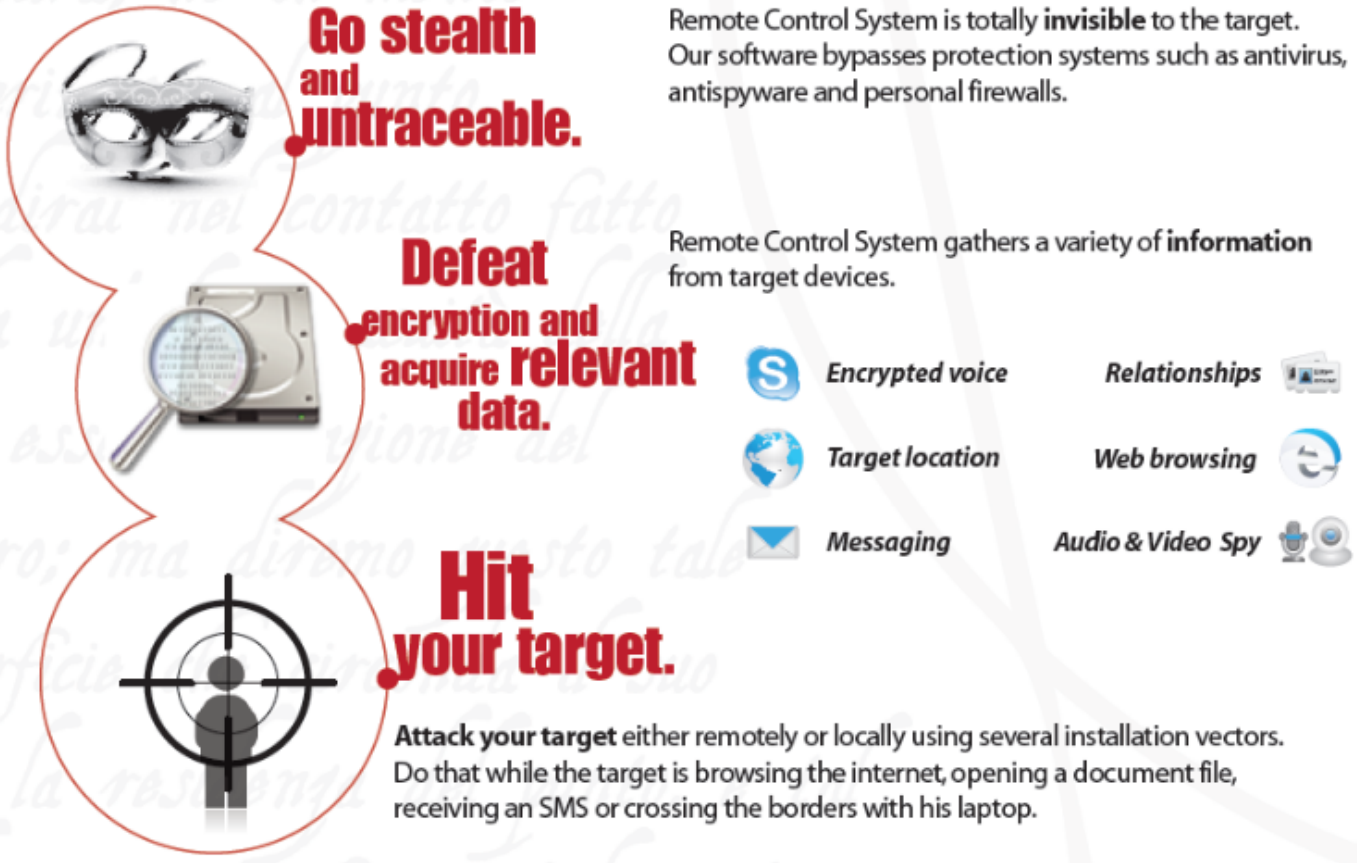
https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

Hacking Team Installation Pathways

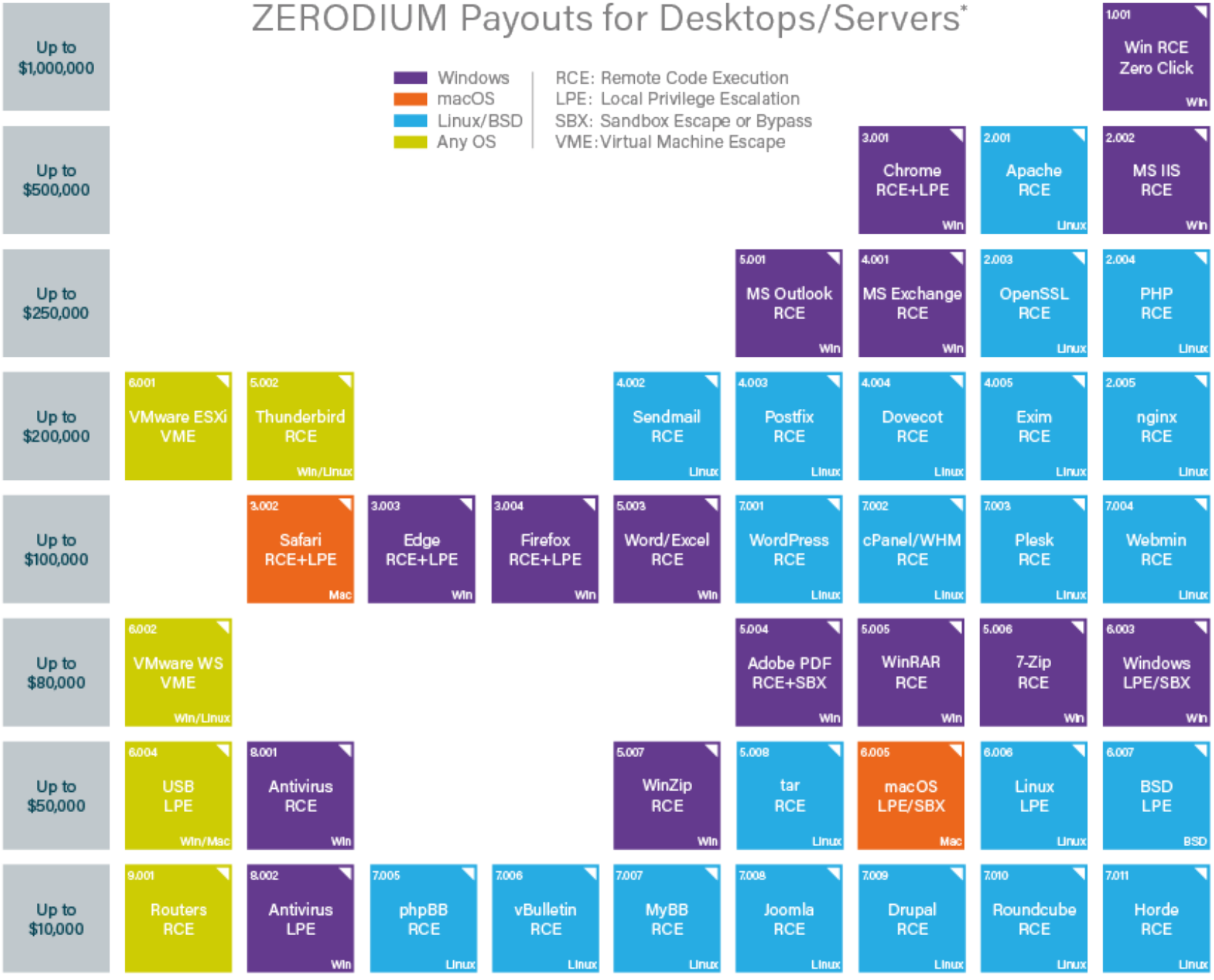


Symantec

Hacking Team Marketing Materials



Lucrative legal market for exploits



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS

Up to $2,500,000										1.001 Android FCP Zero Click (Android)
Up to $2,000,000										1.002 iOS FCP Zero Click (iOS)
Up to $1,500,000									2.001 WhatsApp RCE+LPE Zero Click (iOS/Android)	2.002 iMessage RCE+LPE Zero Click (iOS)
Up to $1,000,000									2.003 WhatsApp RCE+LPE (iOS/Android)	2.004 SMS/MMS RCE+LPE (iOS/Android)
Up to $500,000	3.001 Persistence (iOS)	2.005 WeChat RCE+LPE (iOS/Android)	2.006 iMessage RCE+LPE (iOS)	2.007 FB Messenger RCE+LPE (iOS/Android)	2.008 Signal RCE+LPE (iOS/Android)	2.009 Telegram RCE+LPE (iOS/Android)	2.010 Email App RCE+LPE (iOS/Android)	4.001 Chrome RCE+LPE (Android)		4.002 Safari RCE+LPE (iOS)
Up to $200,000	5.001 Baseband RCE+LPE (iOS/Android)		6.001 LPE to Kernel/Root (iOS/Android)	2.011 Media Files RCE+LPE (iOS/Android)	2.012 Documents RCE+LPE (iOS/Android)	4.003 SBX for Chrome (Android)	4.004 Chrome RCE w/o SBX (Android)	4.005 SBX for Safari (iOS)		4.006 Safari RCE w/o SBX (iOS)
Up to $100,000	7.001 Code Signing Bypass (iOS/Android)	5.002 WiFi RCE (iOS/Android)	5.003 RCE via MitM (iOS/Android)	6.002 LPE to System (Android)	8.001 Information Disclosure (iOS/Android)	8.002 [k]ASLR Bypass (iOS/Android)	9.001 PIN Bypass (Android)	9.002 Passcode Bypass (iOS)		9.003 Touch ID Bypass (iOS)

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

How does malware run?

Social engineering: Trick user into running or installing.

- Exploit USB autorun functionality.

Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric[‡†] Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Bursztein[◇] Michael Bailey[†]

[†] University of Illinois, Urbana Champaign [‡] University of Michigan [◇] Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

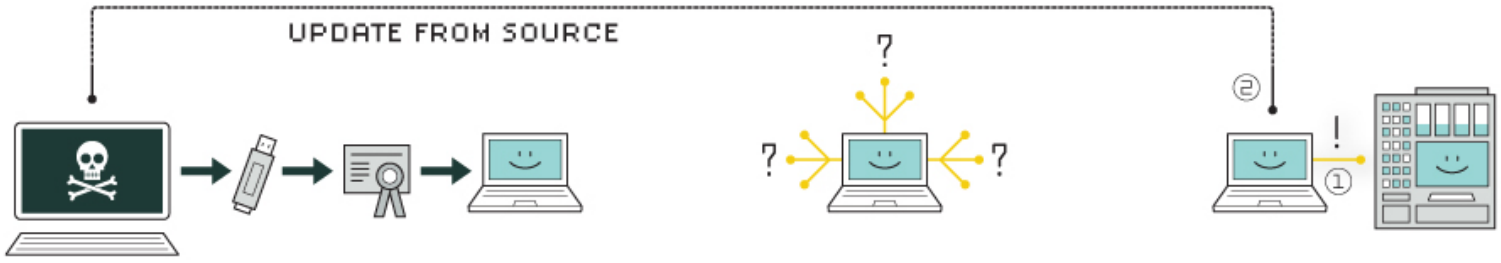
Fig. 1: **Drive Appearances**—We dropped five different types of drives. We chose two appearances (keys and return label) to motivate altruism and two appearances (confidential and exam solutions) to motivate self-interest, as well as an unlabeled control.

How does malware run?

Social engineering: Trick user into running or installing.

- Stuxnet (2010) exploited USB autorun functionality to target centrifuge controllers on airgapped network.
  - First public example of state-sponsored malware targeting Iranian uranium enrichment program.
  - Once inside network also spread via Windows RPC vulnerability.
  - Used four different 0day exploits, had rootkit, stolen code-signing certificates.

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

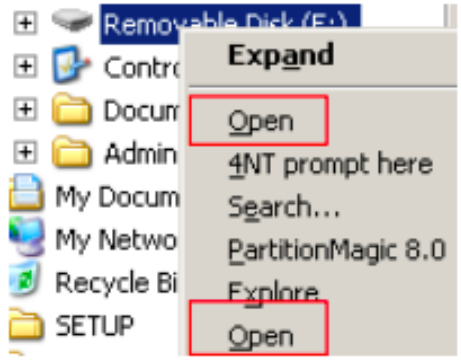
Stuxnet social engineering exploits

In addition to this, Stuxnet also uses another trick to enhance the chances that it will be executed. The autorun commands turn off autoplay and then add a new command to the context menu. The command that is added is found in %Windir%\System32\shell32.dll,-8496. This is actually the "Open" string. Now when viewing the context menu for the removable device the user will actually see two "Open" commands.

One of these Open commands is the legitimate one and one is the command added by Stuxnet. If a user chooses to open the drive via this menu, Stuxnet will execute first. Stuxnet then opens the drive to hide that anything suspicious has occurred.

Figure 18

Two "Open" commands

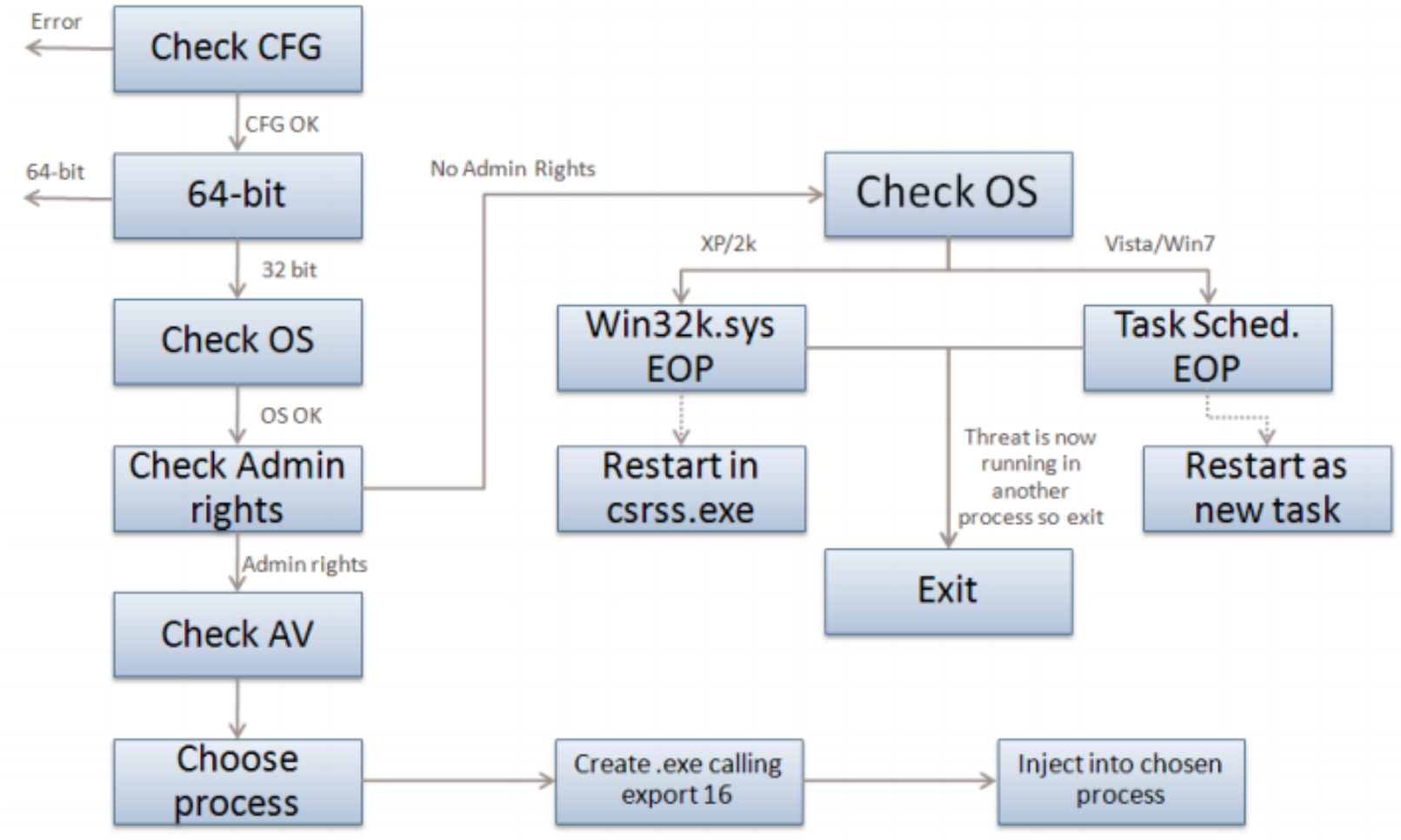


http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxr

Stuxnet exploit flow

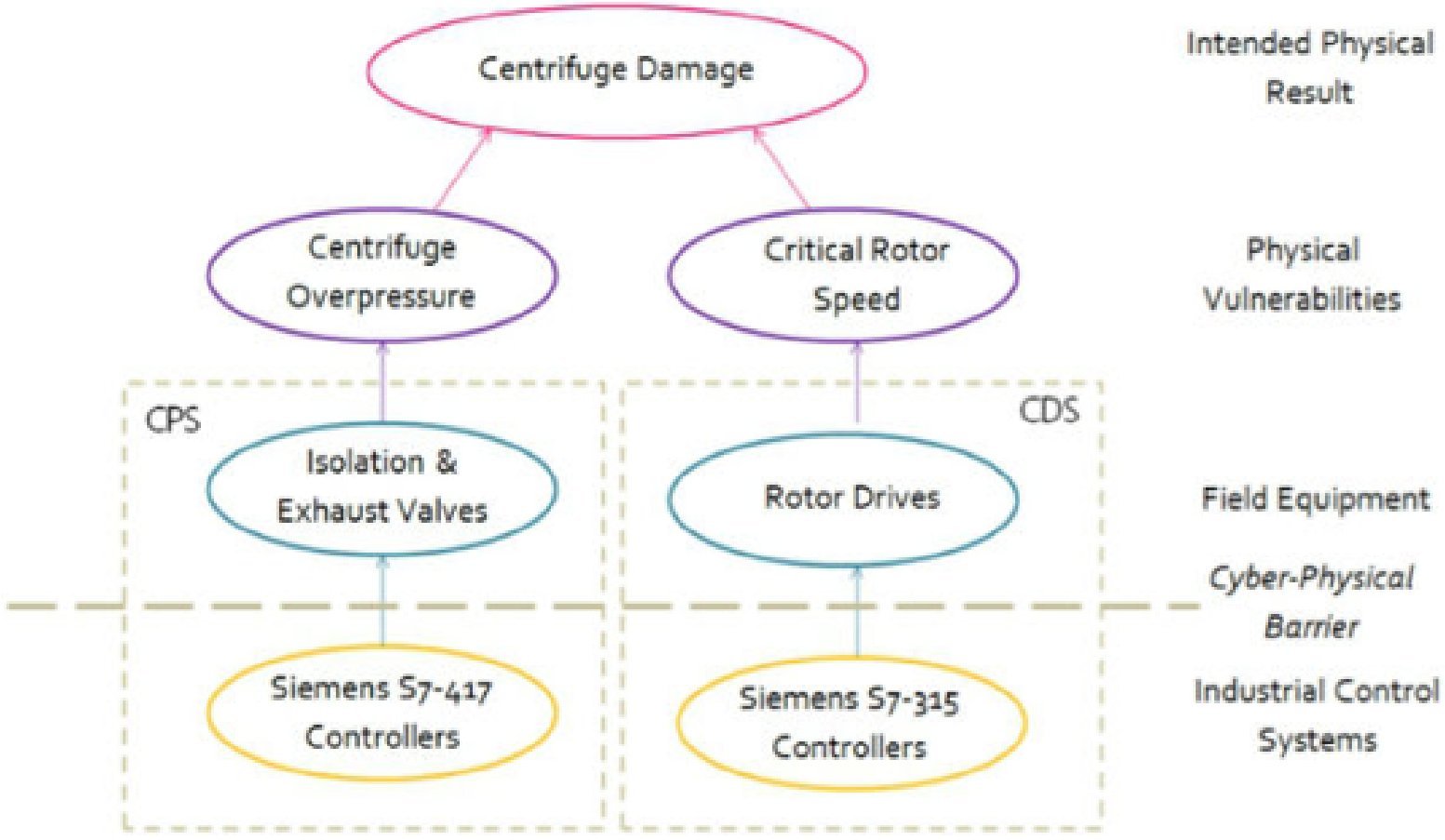
Figure 10

Control flow for export 15



http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxr

Stuxnet targeted Industrial Control Systems



http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack

http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Enlarge This Image

Hasan Sarbakhshian/Associated Press

Iran's nuclear enrichment facility at Natanz.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

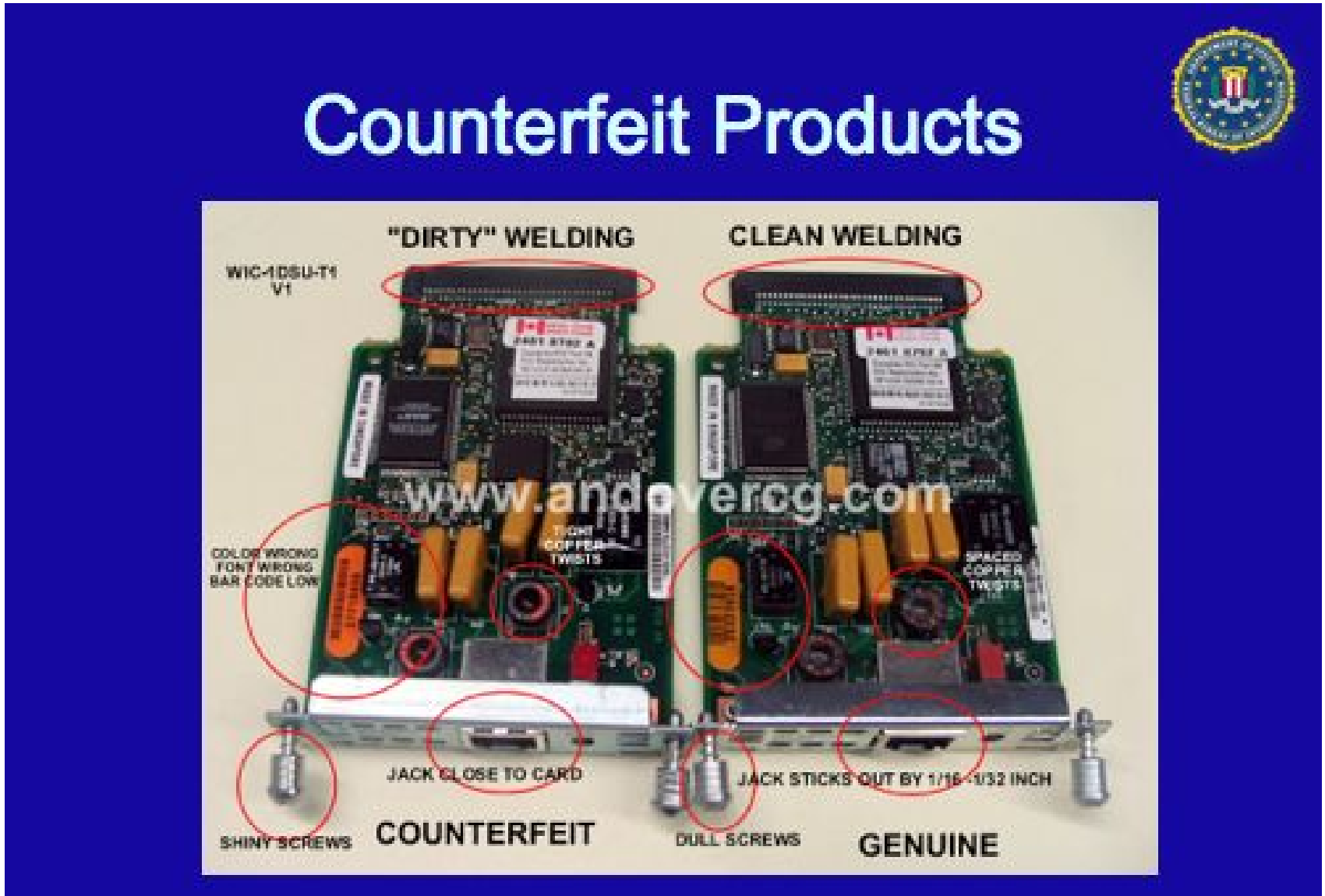
At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

Multimedia

How does malware run?

Insert into system component at manufacture.

- Fake Cisco equipment sold in China contained malware (2008).



How does malware run?

Insert into system component in supply chain.

- NSA supply chain interdiction to insert backdoors into Cisco products (2014).

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

How does malware run?

Compromise software provider.

- Juniper code base compromised in 2012 and 2014, discovered in 2015.

2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)

▼ [JSA10713] Show Article Properties

PRODUCT AFFECTED:

Please see below for details.

PROBLEM:

During an internal code review, two security issues were identified.

Administrative Access (CVE-2015-7755) allows unauthorized remote administrative access to the device. Exploitation of this vulnerability can lead to complete compromise of the affected device.

This issue only affects ScreenOS 6.3.0r17 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

Upon exploitation of this vulnerability, the log file would contain an entry that '**system**' had logged on followed by password authentication for a username.

Example:

Normal login by user **username1**:

```
2015-12-17 09:00:00 system warn 00515 Admin user username1 has logged on via SSH from …..
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username1' at host …
```

Compromised login by user **username2**:

```
2015-12-17 09:00:00 system warn 00515 Admin user system has logged on via SSH from …..
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username2' at host …
```

Note that a skilled attacker would likely remove these entries from the local log file, thus effectively eliminating any reliable signature that the device had been compromised.

How does malware run?

Attacker with local access downloads/runs directly.

- Example: Phone spyware for stalking/domestic abuse.

http://gizmodo.com/how-the-hell-are-these-popular-spying-apps-not-illegal-1682660414

How does malware run?

Attacker with local access downloads/runs directly.

- Mirai Botnet (2016) exploited hard-coded default usernames/passwords for IoT devices.
  - Continuously scans for devices, logs in, and infects itself.
  - Used for DDoS attacks.

Countermeasures

- Signature-based detection
  - Look for bytes corresponding to virus code.
  - Antivirus software is a multibillion dollar industry.

- AV arms race:
  - Virus writers change viruses to evade detection.
  - One idea: Virus encrypts its code. Static code detection works less well; decryption code is small, generic.

- Cleanup:
  - Best way: rebuild from original media/backups
  - Some malware contains rootkits
    Kernel patches to hide its continuous presence

- Analysis:
  - Run in VM/sandboxed environment
  - Modern malware tries to detect if it runs in VM/fresh install and acts less maliciously