CSE509 Computer System Security

Stony Brook University

2023-04-13

Malware: Incidents

Michalis Polychronakis

Stony Brook University

Stuxnet

Duqu

Flame

Gauss

NotPetya

…

Stuxnet

The Iranian Nuclear Program

Iran started its nuclear program in the 1950s

Iran's revolution delayed the program

A few years later, the new leaders continued it

In 2002, it turned out that Iran had already developed two undeclared nuclear facilities

Iran suspended uranium enrichment in 2003 and resumed it in 2006

International Atomic Energy Agency (IAEA): *"Iran does not comply with safeguard agreements"*

17 June 2010

Belarusian security firm VirusBlokAda is contacted by an Iranian customer

- Siemens' SIMATIC WinCC server trapped in a reboot loop
- WinCC: acts as a human-machine interface for operating and modifying programmable logic controllers (PLCs)

VirusBlockAda identified an infection using a potential Windows zero-day

- Notified Microsoft and other researchers
- Researchers started analyzing the ~0.5MB binary (huge compared to typical malware)
- The team identified *four* Windows zero-days affecting Windows XP, Vista, and 7
- Heavily analyzed by other researchers in the following months

Confirmed to have existed at least one year prior and likely even before

Stuxnet

Goal: sabotage Iran's nuclear program

- Induce malfunctions in the centrifuges within Iran's nuclear enrichment facilities

Jointly built by USA and Israel

- Neither country has openly admitted responsibility

Designed to seek out and attack a single component of PLC software designed by Siemens

- If the software is not present, the virus goes inert, remaining undetected on the system

The world learned about it despite its stealthiness

- Controlled propagation gone wrong

The once-secret nuclear complex in Natanz, Iran, about 150 miles south of Tehran

Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008

Iranian President Mahmoud Ahmadinejad observes computer monitors at the Natanz plant

Extremely Specific Goal

Once the PLC is found, Stuxnet searches for the presence of two kinds of frequency converters

- Made by Fararo Paya (Iran) and Vacon (Finland)

If found, it performs two possible actions depending on the number of frequency converters found

- Set frequency to 1,064 Hz (close to 1,007 Hz at which Natanz is said to operate) ➔ reduce frequency for a short while ➔ return it back
- Increase frequency to 1,410 Hz – *"very close to the maximum speed the spinning aluminum IR-1 rotor can withstand mechanically"*

The stresses from the excessive, then slower, speeds caused the aluminum centrifugal tubes to expand

- Forcing parts of the centrifuges into sufficient contact with each other to destroy them

Siemens Simatic S7-300 PLC CPU with three I/O modules attached

Stuxnet Highlights

Four zero-day exploits

Plus MS08-067 used by the Conficker worm

Windows rootkit

Allowed Stuxnet to reintroduce itself to an infected system after the system was cleaned

Distributed C&C network

Allowed the operators to remotely control and update infected systems

Peer-to-peer updates

Updates and communication with other victims even when C&C server is not reachable

Legitimate signed digital certificates

Silent driver installation without prompting the user

Antivirus evasion techniques

Table 1

Evolution of Stuxnet versions

Version	Date	Description
0.500	November 3, 2005	C&C server registration
0.500	November 15, 2007	Submit date to a public scanning service
0.500	July 4, 2009	Infection stop date
1.001	June 22, 2009	Main binary compile timestamp
1.100	March 1, 2010	Main binary compile timestamp
1.101	April 14, 2010	Main binary compile timestamp
1.x	June 24, 2012	Infection stop date

Table 2

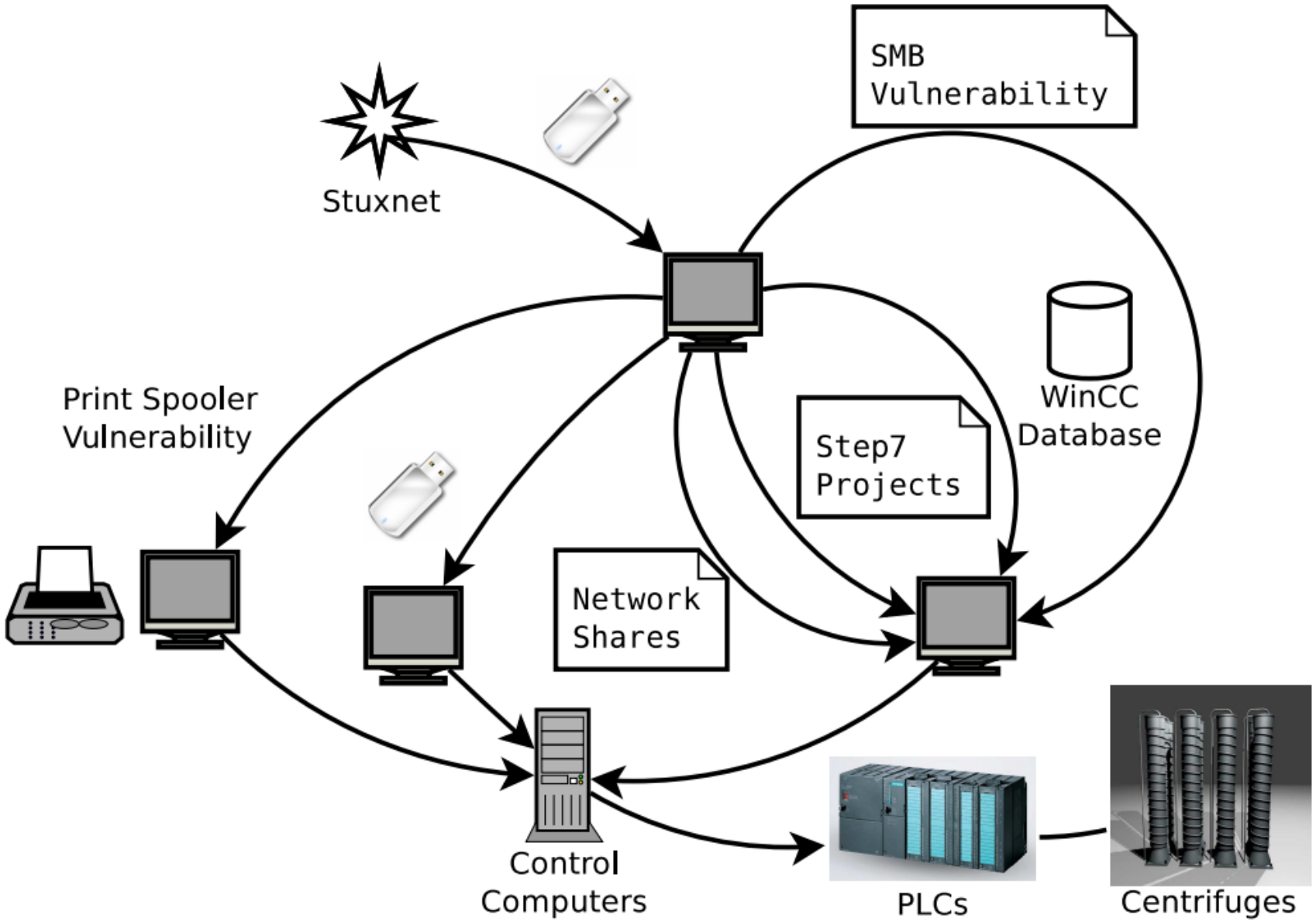
Evolution of Stuxnet exploits

Vulnerability	0.500	1.001	1.100	1.101	Description
CVE-2010-3888			X	X	Task scheduler EOP
CVE-2010-2743			X	X	LoadKeyboardLayout EOP
CVE-2010-2729		X	X	X	Print spooler RCE
CVE-2008-4250		X	X	X	Windows Server Service RPC RCE
CVE-2012-3015	X	X	X	X	Step 7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC default password
CVE-2010-2568			X	X	Shortcut .lnk RCE
MS09-025		X			NtUserRegisterClassExWow/NtUserMessageCall EOP

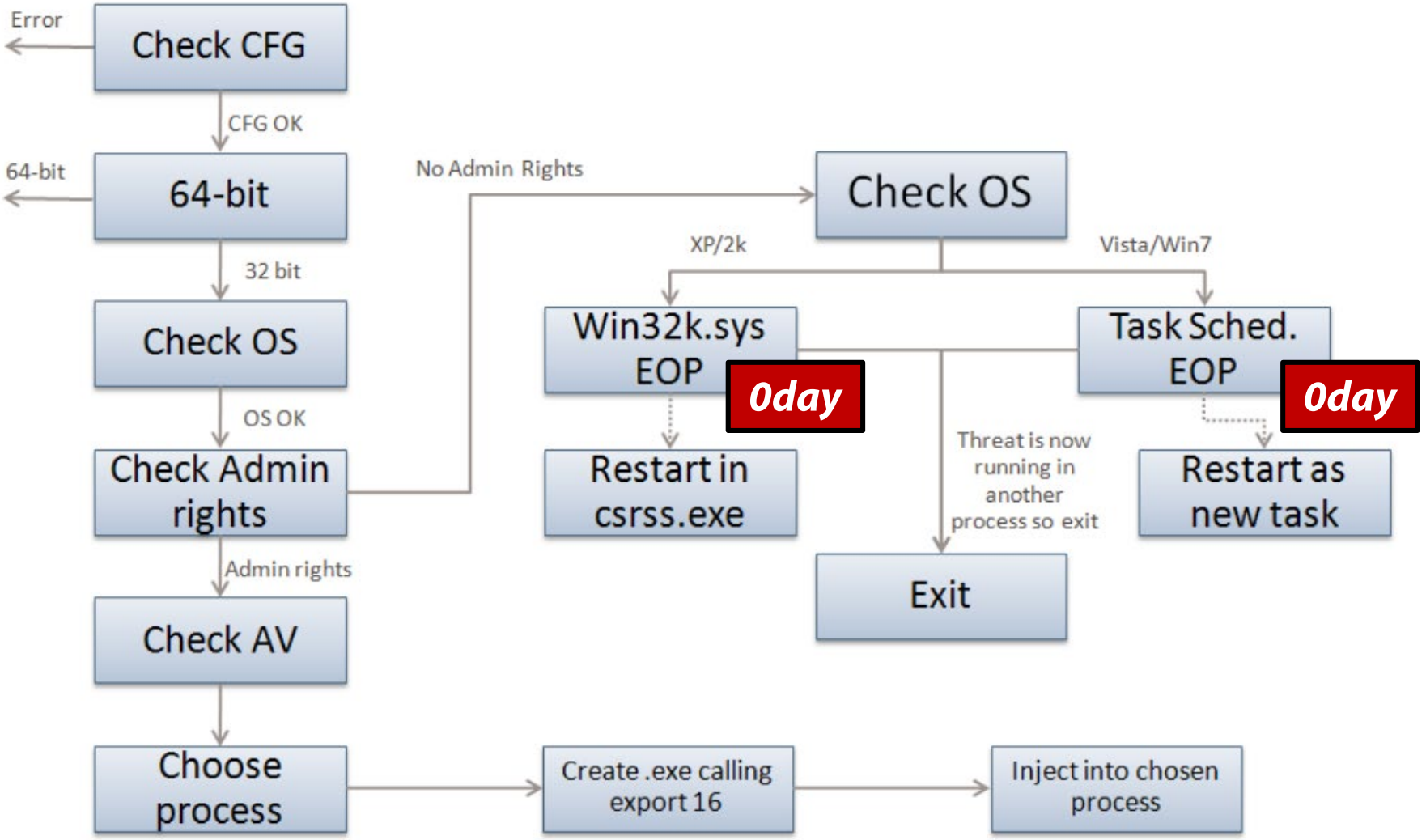
Table 3

Evolution of Stuxnet replication

Replication Technique	0.500	1.001	1.100	1.101
Step 7 project files	X	X	X	X
USB through Step 7 project files	X			
USB through Autorun		X		
USB through CVE-2010-2568			X	X
Network shares		X	X	X
Windows Server RPC		X	X	X
Printer spooler		X	X	X
WinCC servers		X	X	X
Peer-to-peer updating through mailslots	X			
Peer-to-peer updating through RPC		X	X	X



Installation



Propagation: Removable Drives

Likely the initial infection vector

- Workers, outside contractors, secret agents (?), …

Versions prior to March 2010: `autorun.inf`

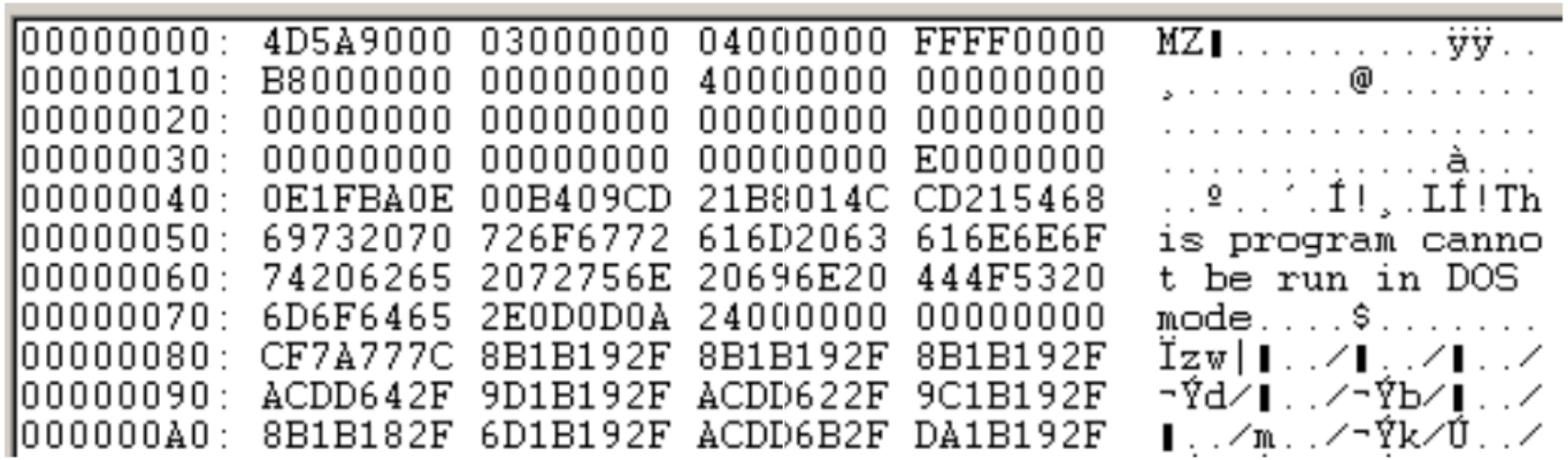
- Causes Windows to automatically run a file on removable media
- Malicious code was embedded in autorun.inf itself (!) – polyglot file that can be interpreted as both `.inf` and `.exe`
- MZ file first within the `autorun.inf` file, followed by actual AutoRun commands

Later versions: MS10-046 .LNK vulnerability **(0day)**

- *Allows local users or remote attackers to execute arbitrary code via a crafted .LNK or .PIF shortcut file, which is not properly handled during icon display in Windows Explorer*

Figure 15

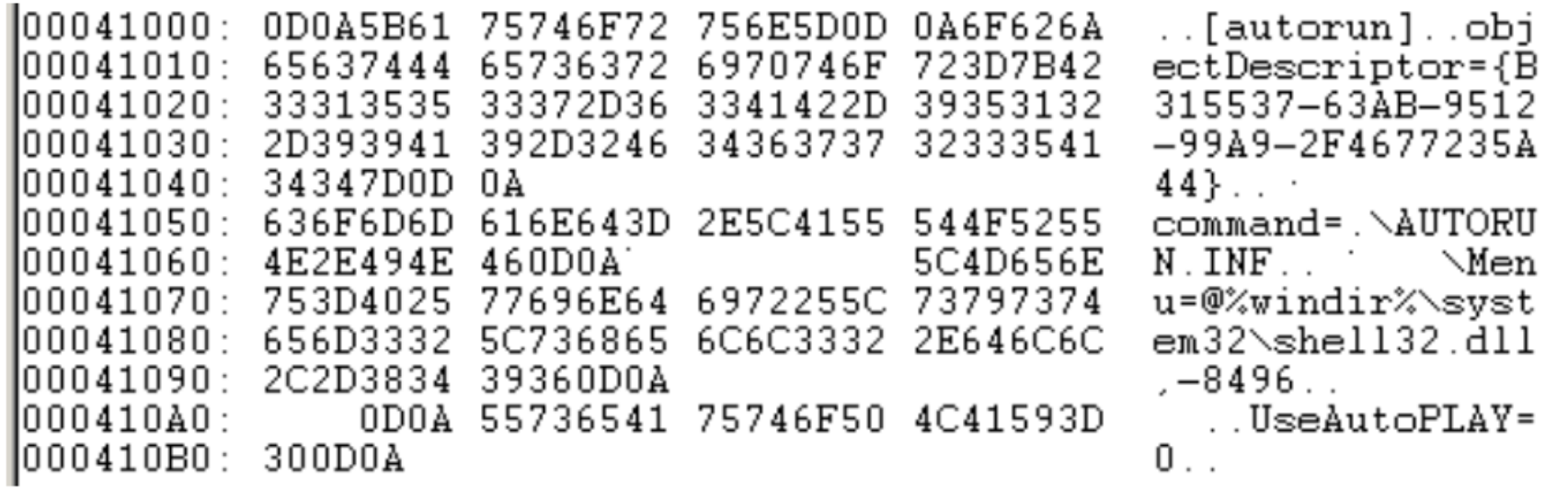
Autorun.inf header



```
00000000: 4D5A9000 03000000 04000000 FFFF0000  MZ▌.........ÿÿ..
00000010: B8000000 00000000 40000000 00000000  ¸.......@.......
00000020: 00000000 00000000 00000000 00000000  ................
00000030: 00000000 00000000 00000000 E0000000  ............à...
00000040: 0E1FBA0E 00B409CD 21B8014C CD215468  ..º..´.Í!¸.LÍ!Th
00000050: 69732070 726F6772 616D2063 616E6E6F  is program canno
00000060: 74206265 2072756E 20696E20 444F5320  t be run in DOS
00000070: 6D6F6465 2E0D0D0A 24000000 00000000  mode....$.......
00000080: CF7A777C 8B1B192F 8B1B192F 8B1B192F  Ïzw|▌../▌../▌../
00000090: ACDD642F 9D1B192F ACDD622F 9C1B192F  ¬Ýd/▌../¬Ýb/▌../
000000A0: 8B1B182F 6D1B192F ACDD6B2F DA1B192F  ▌../m../¬Ýk/Ú../
```

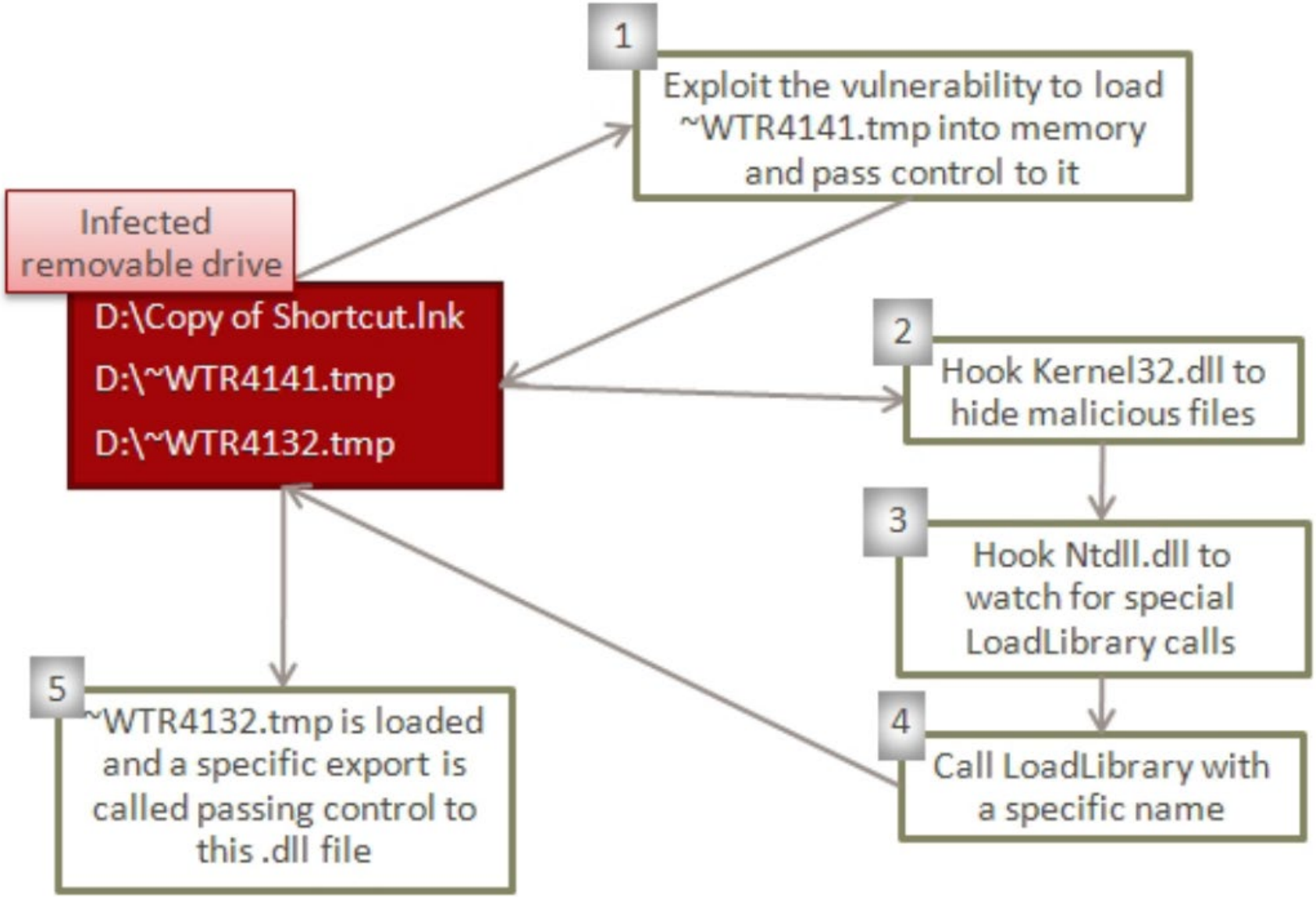
Figure 16

Autorun.inf footer



```
00041000: 0D0A5B61 75746F72 756E5D0D 0A6F626A  ..[autorun]..obj
00041010: 65637444 65736372 6970746F 723D7B42  ectDescriptor={B
00041020: 33313535 33372D36 3341422D 39353132  315537-63AB-9512
00041030: 2D393941 392D3246 34363737 32333541  -99A9-2F4677235A
00041040: 34347D0D 0A                          44}..
00041050: 636F6D6D 616E643D 2E5C4155 544F5255  command=.\AUTORU
00041060: 4E2E494E 460D0A                5C4D656E  N.INF..    \Men
00041070: 753D4025 77696E64 6972255C 73797374  u=@%windir%\syst
00041080: 656D3332 5C736865 6C6C3332 2E646C6C  em32\shell32.dll
00041090: 2C2D3834 39360D0A                    ,-8496..
000410A0:     0D0A 55736541 75746F50 4C41593D    ..UseAutoPLAY=
000410B0: 300D0A                               0..
```

USB Execution Flow



Propagation: MS10-061 (0day)

Printer Spooler Service Impersonation Vulnerability

Allows a local or remote user to write arbitrary files to %SYSTEM%

- An attacker can specify any file name, including directory traversal or full paths

Achieving code execution

- Write to a directory used by Windows Management Instrumentation (WMI) for application deployment: `Wbem\Mof`
- This directory is periodically scanned and any new `.mof` files are processed automatically ➔ malware activation

Propagation: MS08-067

Old SMB vulnerability used by Conficker

Can be exploited by connecting over SMB and sending a malformed path string ➔ arbitrary execution

Stuxnet verifies the following conditions before exploiting MS08-67:

- The current date must be before January 1, 2030
- Virus signature definitions for a variety of antivirus products must be dated before January 1, 2009
- The timestamps of `kernel32.dll` and `netapi32.dll` must be dated before October 12, 2008 (before patch day)

Other Propagation Vectors

Siemens WinCC

- When found, connects to its database server using a password that is hardcoded within the WinCC software
- Then sends malicious SQL code to transfer and execute Stuxnet code to infect the system

Network Shares

- Activation through either a scheduled job or using Windows Management Instrumentation (WMI)

Siemens SIMATIC Step7 Project files

- Original propagation vector of Stuxnet v0.5
- Insert Stuxnet code into Step7 project directories

Digitally Signed Kenel-mode Rootkit Drivers

Valid digital signature enables silent installation without raising suspicion

Stuxnet used two certificates across different versions

January 25, 2010: driver signed with a valid certificate belonging to Realtek Semiconductor Corps

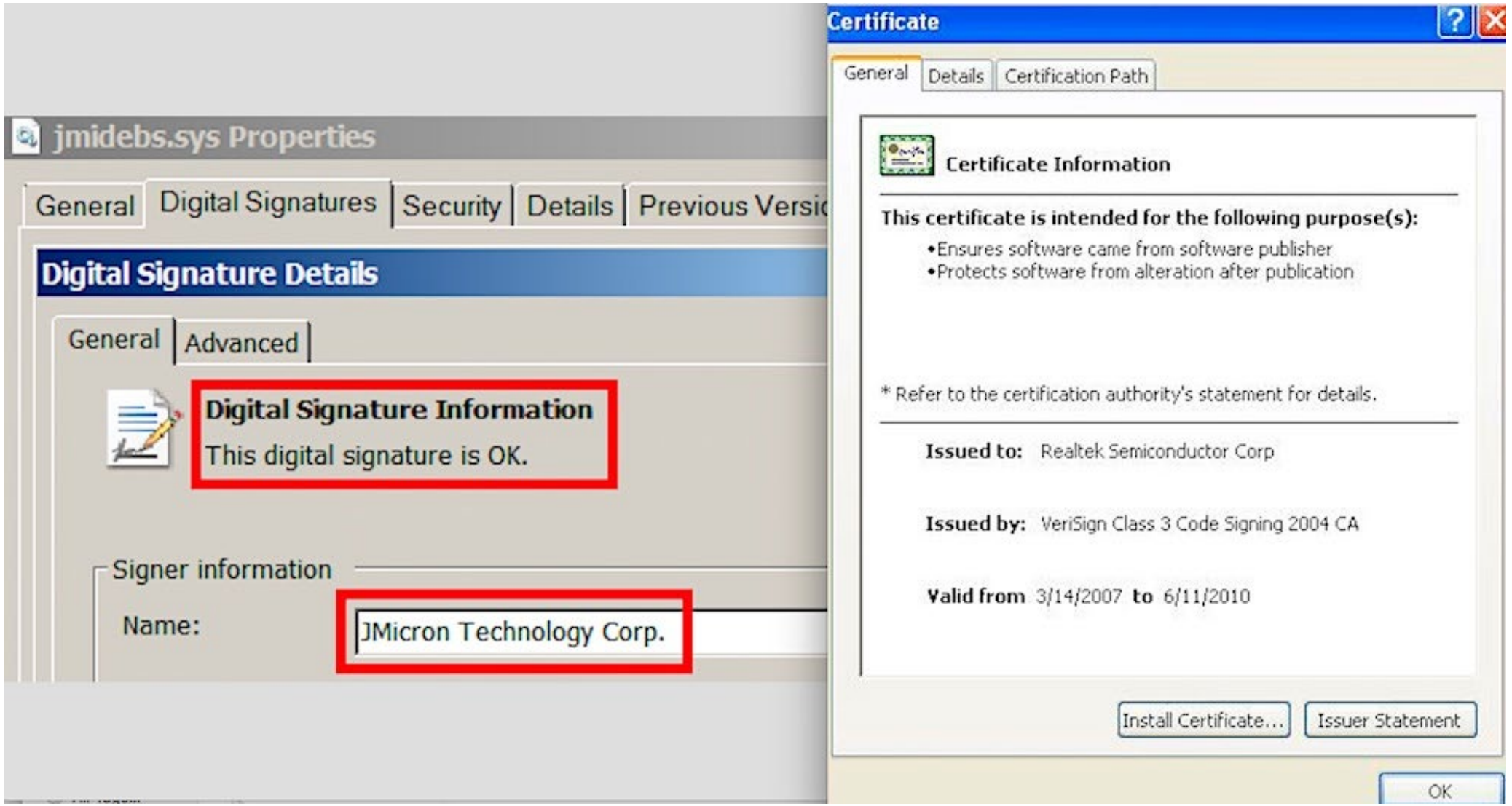
- Confirmed as compromised and revoked by Verisign on July 16, 2010

July 17, 2010: ESET identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp

- Revoked by Verisign on July 22, 2010

Both companies are located at Hsinchu Science Park in Taiwan

- The close proximity of their offices suggests the possibility that the private keys were stolen by an insider or through a physical attack



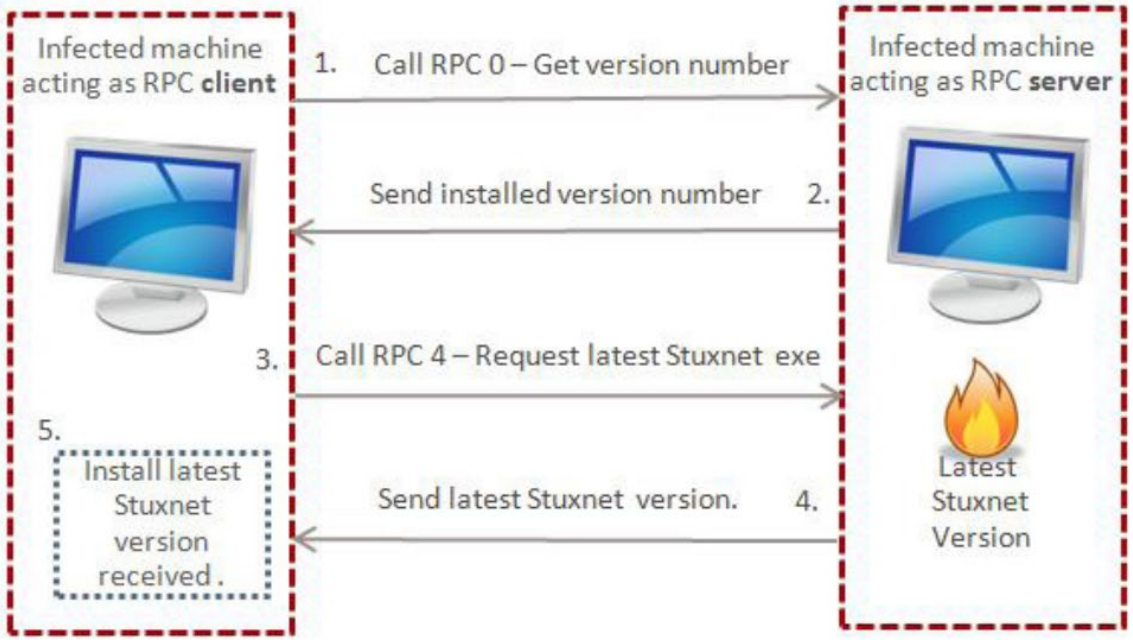
P2P Communication

Stuxnet has its own RPC server and client

Server started upon infection

Any other compromised computer can connect and ask what version of Stuxnet is installed on the remote computer

Update triggered if client (server) is older than the server (client)



Step 7 Software Infection

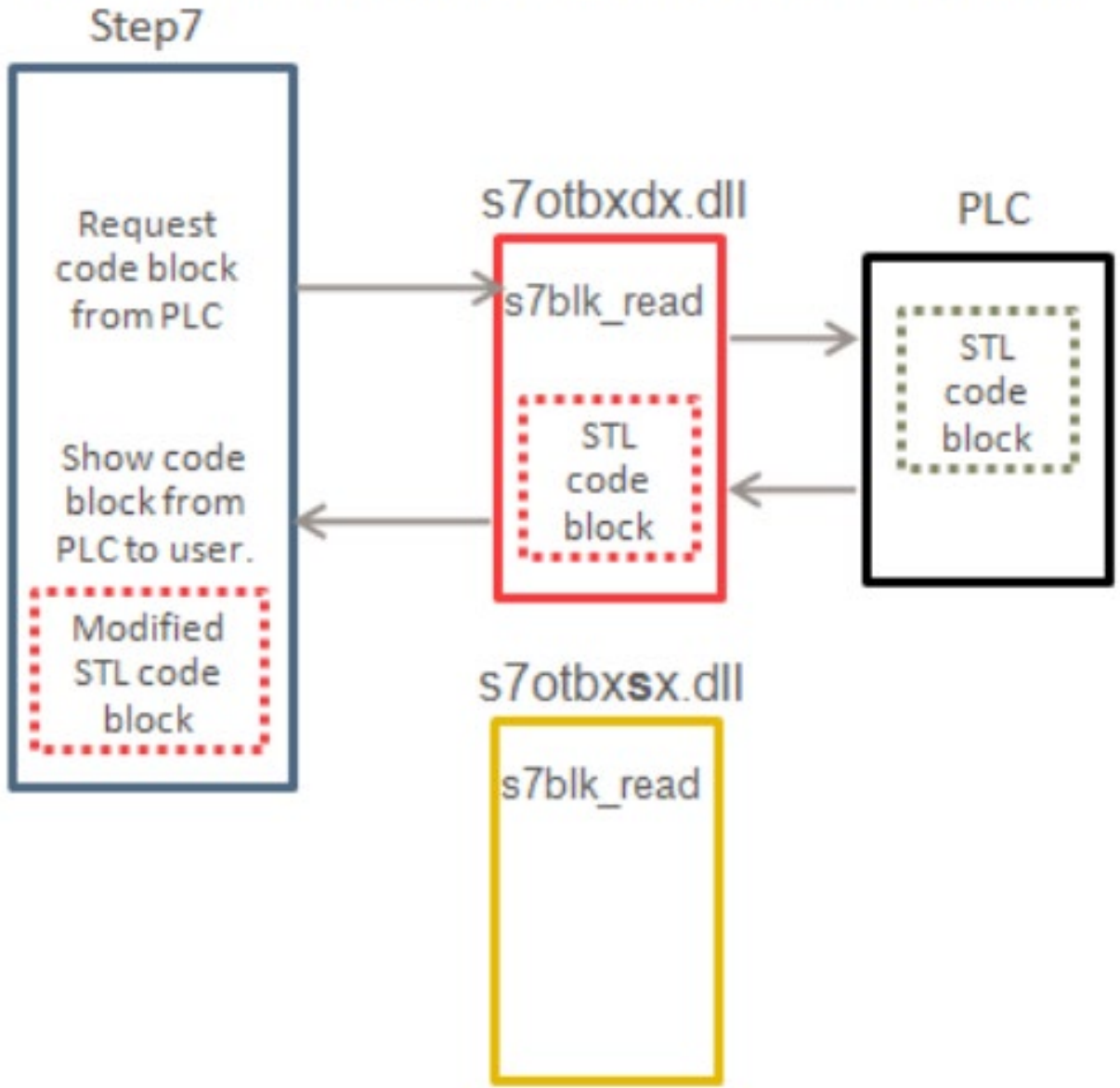
Stuxnet subverts a key communication library of WinCC (`s7otbxdx.dll`)

- Responsible for handling PLC block exchange between the Windows machine running the Simatic manager and the PLC
- The two are connected via a data cable

MitM attack:

- Monitor PLC blocks written to or read from the PLC
- Infect PLC by inserting its own blocks and infecting existing blocks
- Hide any evidence that the PLC is infected whenever WinCC reads an infected block

Communication with malicious version of s7otbxdx.dll



C&C

Upon infection, contacts over HTTP port 80 two possible domains

- `www[.]mypremierfutbol[.]com`
- `www[.]todaysfutbol[.]com`

Servers hosted in Malaysia and Denmark

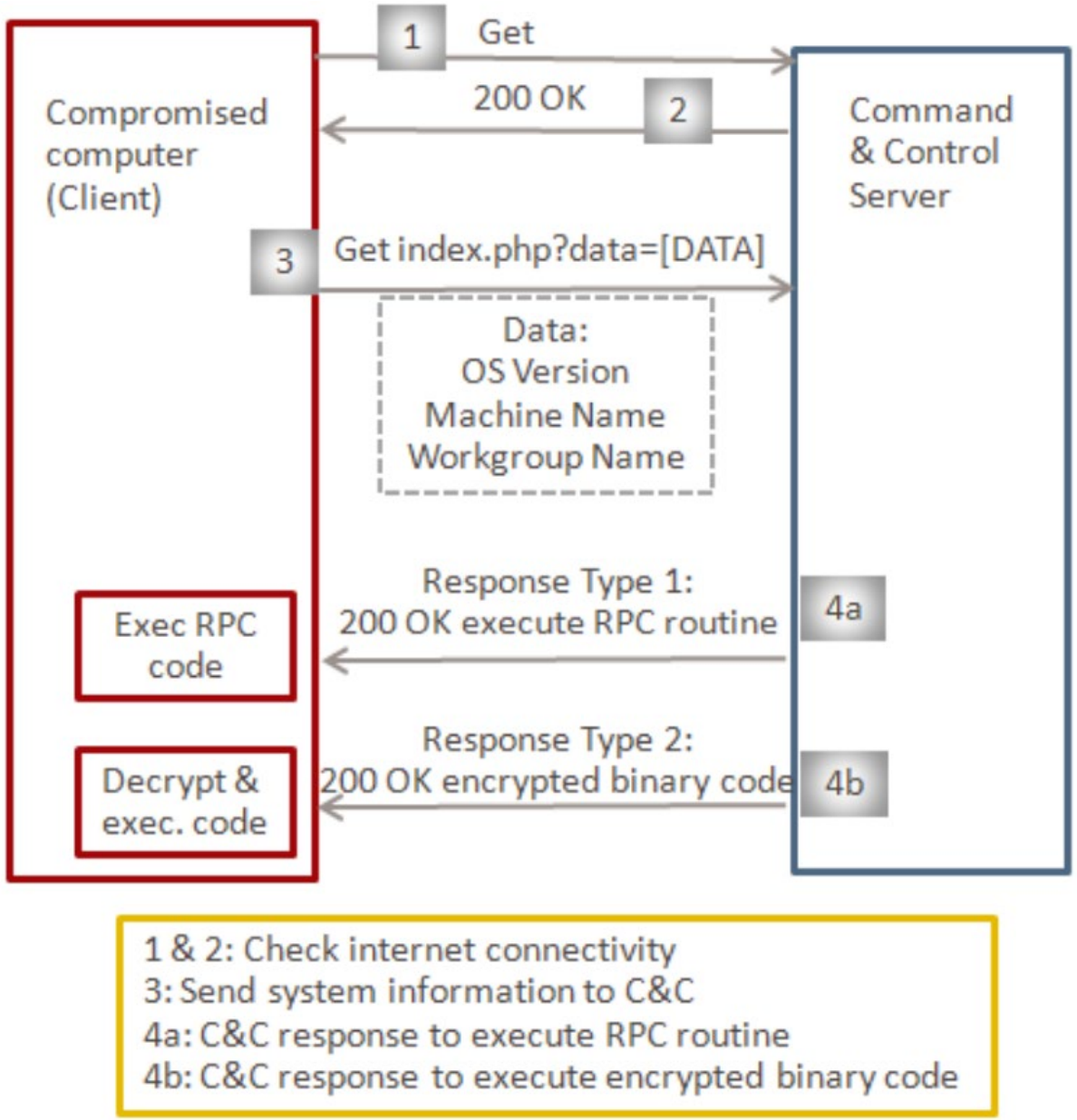
Communication “encrypted” with simple XOR

- Client to server: 0xFF
- Server to client (binary): static 31-byte long XOR key

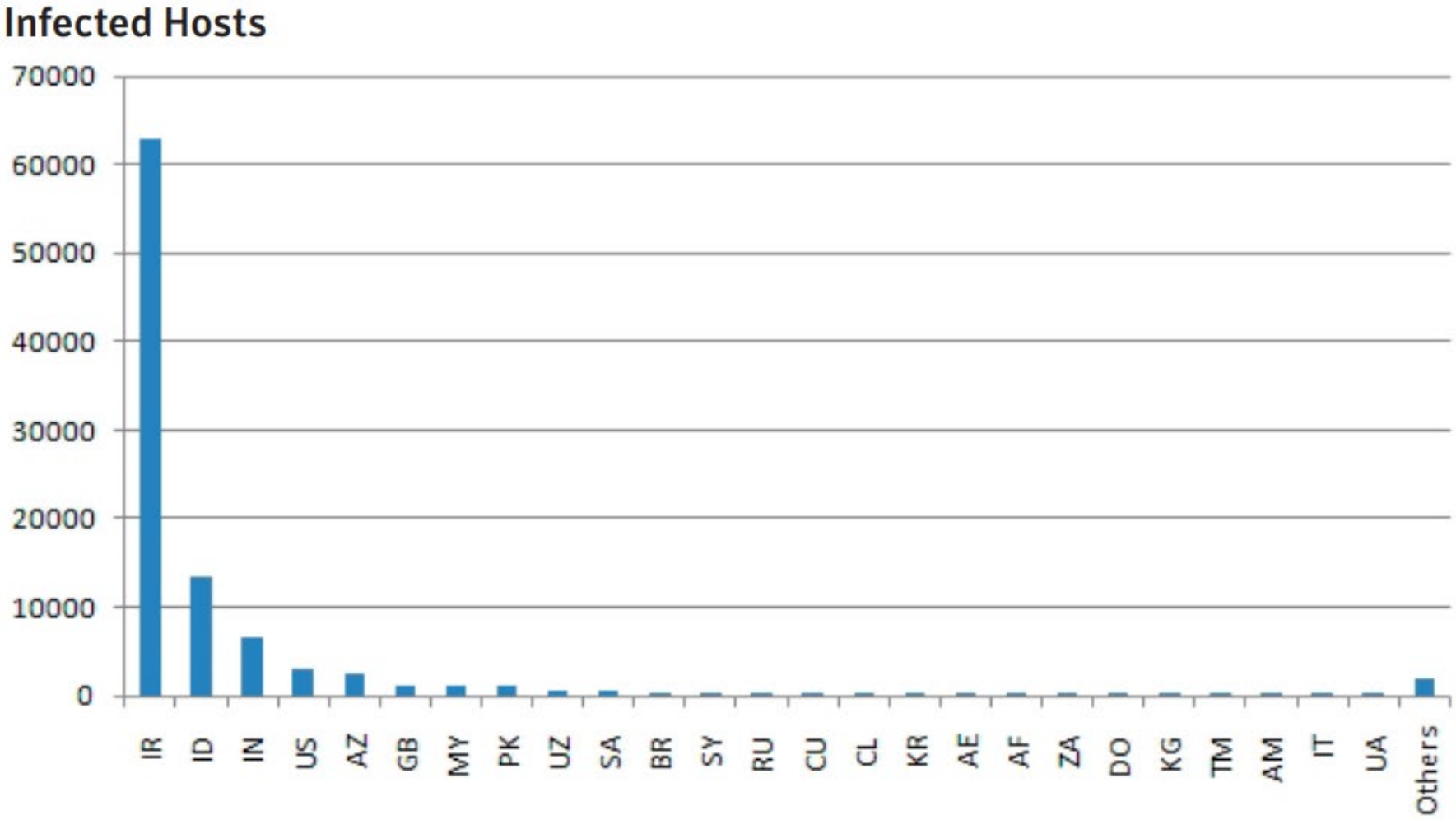
  0xF1, 0x17, 0xFA, 0x1C, 0xE2, 0x33, 0xC1, 0xD7, 0xBB, 0x77, 0x26, 0xC0, 0xE4, 0x96, 0x15, 0xC4, 0x62, 0x2E, 0x2D, 0x18, 0x95, 0xF0, 0xD8, 0xAD, 0x4B, 0x23, 0xBA, 0xDC, 0x4F, 0xD7, 0x0C

Nothing really special

- Could have been easily detected using passive DNS monitoring



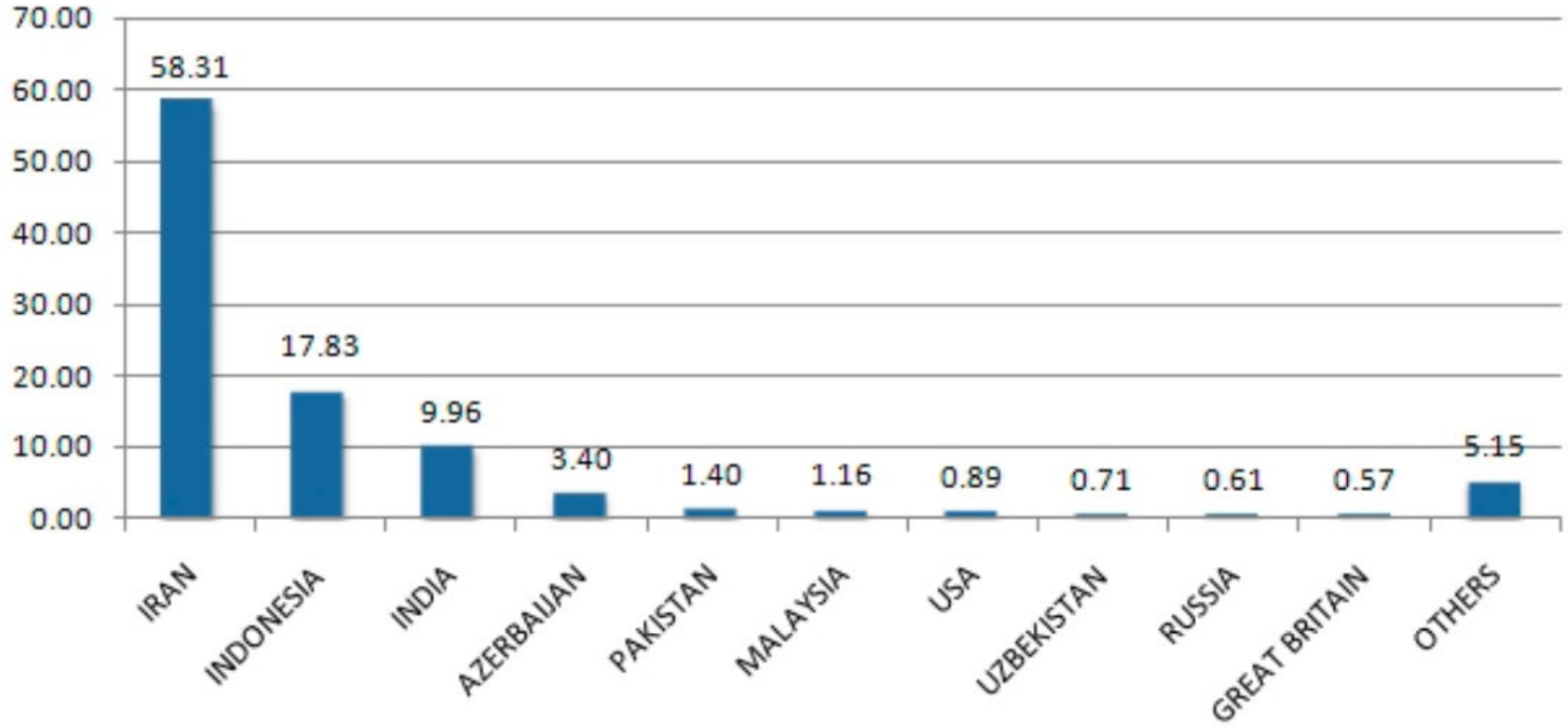
1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code



Symantec started monitoring Stuxnet's C&C traffic on July 20, 2010

As of September 29, 2010, they observed ~100,000 infected hosts (over 40,000 unique external IP addresses from over 155 countries, 60% in Iran)

Geographic Distribution of Infections



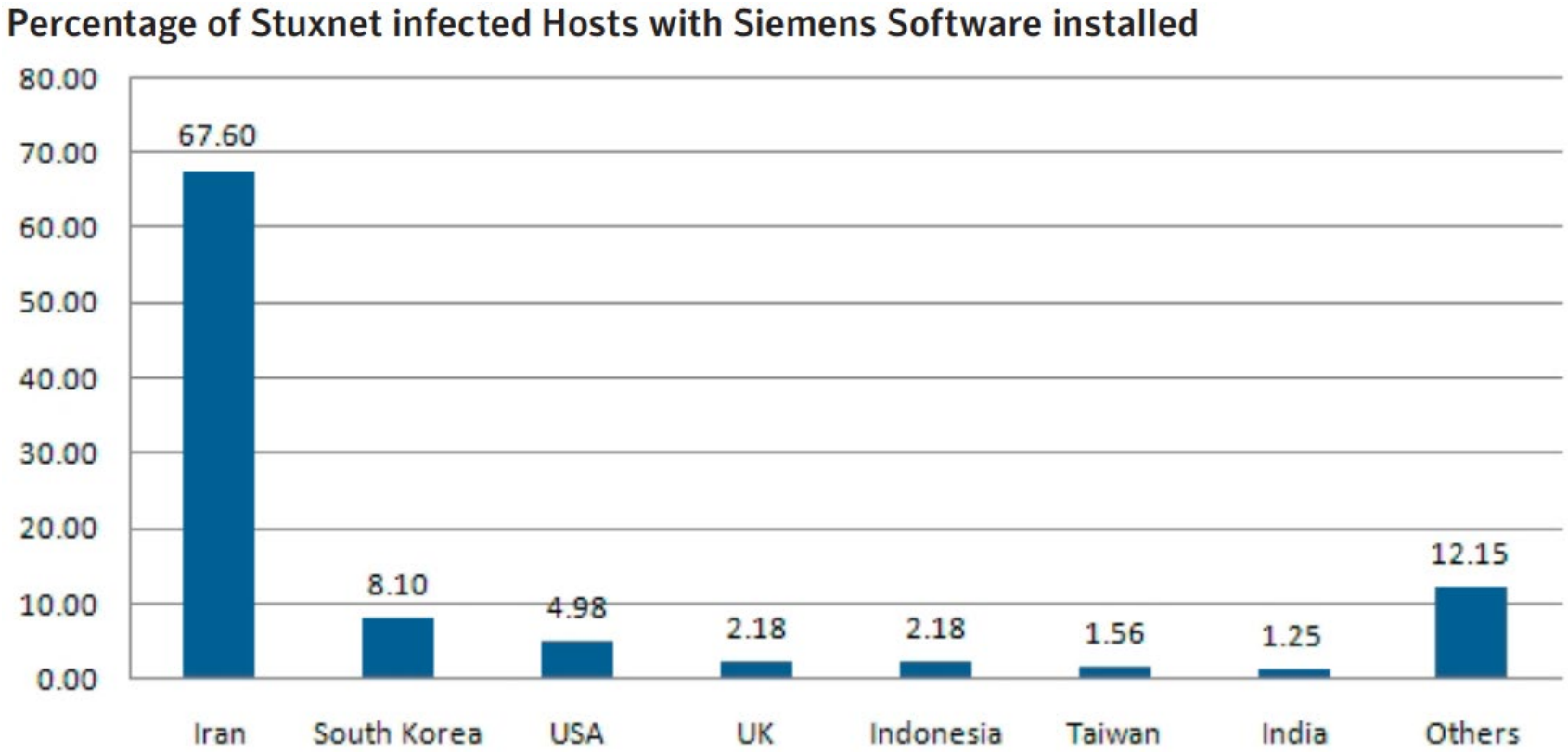


Table 2

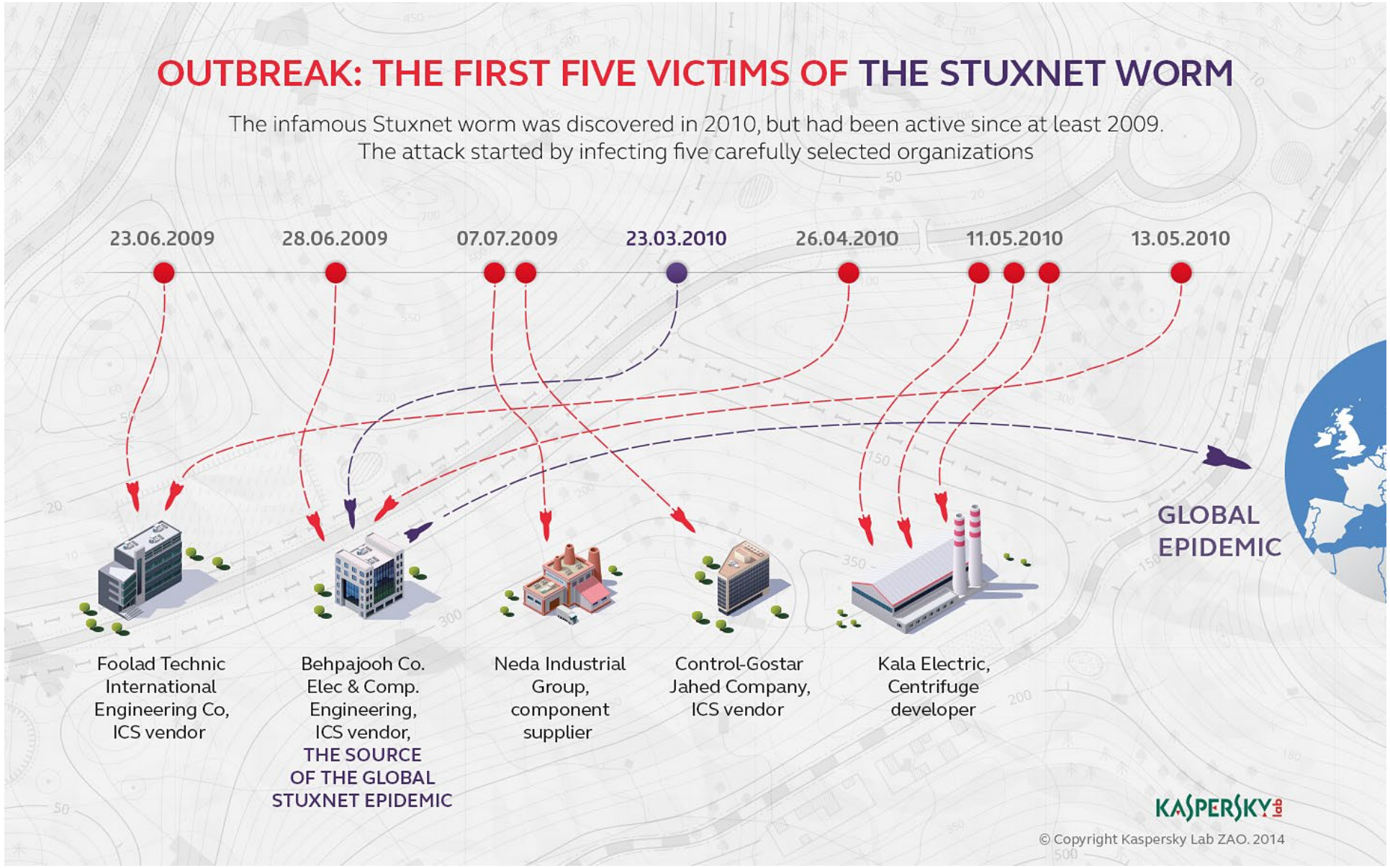
Attack Waves Against the Initial Targets

Attack Wave	Site	Compile Time	Infection Time	Time to Infect
Attack Wave 1	Domain A	June, 22 2009 16:31:47	June 23, 2009 4:40:16	0 days 12 hours
	Domain B	June, 22 2009 16:31:47	June 28, 2009 23:18:14	6 days 6 hours
	Domain C	June, 22 2009 16:31:47	July 7, 2009 5:09:28	14 days 12 hours
	Domain D	June, 22 2009 16:31:47	July 19, 2009 9:27:09	26 days 16 hours
Attack Wave 2	Domain B	March, 1 2010 5:52:35	March 23, 2010 6:06:07	22 days 0 hours
Attack Wave 3	Domain A	April, 14 2010 10:56:22	April 26, 2010 9:37:36	11 days 22 hours
	Domain E	April, 14 2010 10:56:22	May 11, 2010 6:36:32	26 days 19 hours
	Domain E	April, 14 2010 10:56:22	May 11, 2010 11:45:53	27 days 0 hours
	Domain E	April, 14 2010 10:56:22	May 11, 2010 11:46:10	27 days 0 hours
	Domain B	April, 14 2010 10:56:22	May 13, 2010 5:02:23	28 days 18 hours

Symantec gathered 3,280 unique samples (3 variants) by February 2011

Stuxnet records a timestamp (along with other system information) each time a new infection occurs (including the initial infection)

Stuxnet was a targeted attack against five different Iranian companies (12,000 infections can be traced back to these 5 organizations)



© https://arstechnica.com/information-technology/2014/11/stuxnet-worm-infected-high-profile-targets-before-hitting-iran-nukes/

Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran

Kim Zetter and Huib Modderkolk · **Contributors**
September 2, 2019

Yahoo News photo illustration; photos: AP, Getty Images. Shutterstock

For years, an enduring mystery has surrounded the Stuxnet virus attack that targeted Iran's nuclear program: How did the U.S. and Israel get their malware onto computer systems at the highly secured uranium-enrichment plant?

The first-of-its-kind virus, designed to sabotage Iran's nuclear program, effectively launched the era of digital warfare and was unleashed some time in 2007, after Iran began installing its first batch of centrifuges at a controversial enrichment plant near the village of Natanz.

The courier behind that intrusion, whose existence and role has not been previously reported, was an inside mole recruited by Dutch intelligence agents at the behest of the CIA and the Israeli intelligence agency, the Mossad, according to sources who spoke with Yahoo News.

Did Stuxnet Achieve its Goal?

Januray 2010: IAEA investigators observed that centrifuges were being replaced at "an incredible rate"

- More than double the normal rate

May 2010: IAEA stated that the Natanz facility contained 3,900 operational centrifuges

- 20% reduction in working centrifuges compared to one year before
- In addition, thousands of installed centrifuges were simply idle

November 2010: the Iranian government acknowledged that its nuclear program suffered an electronic attack

- Understandably downplayed the impact of the attack
- President Mahmoud Ahmadinejad admitted that the attack *"creat[ed] problems for a limited number of our centrifuges"*

Duqu

Duqu

Discovered in September 2011 by CrySyS Lab

- Budapest University of Technology and Economics

Goal: information gathering

- Information related to industrial control systems
- Stealing digital certificates (and corresponding private keys)
- Remote access trojan (RAT) functionality

Striking similarity to Stuxnet

- Overall design, internal structure, modules, implementation, …
- Digitally signed driver (different cert)

Just ~20 known victims, including some in Europe

- Many involved in the manufacturing of industrial control systems

Duqu Infection Strategy

Phishing email to the intended target

- Microsoft Word document attachment

Targeted attack: *no self-replication capability*

- Removes itself automatically after 30 days

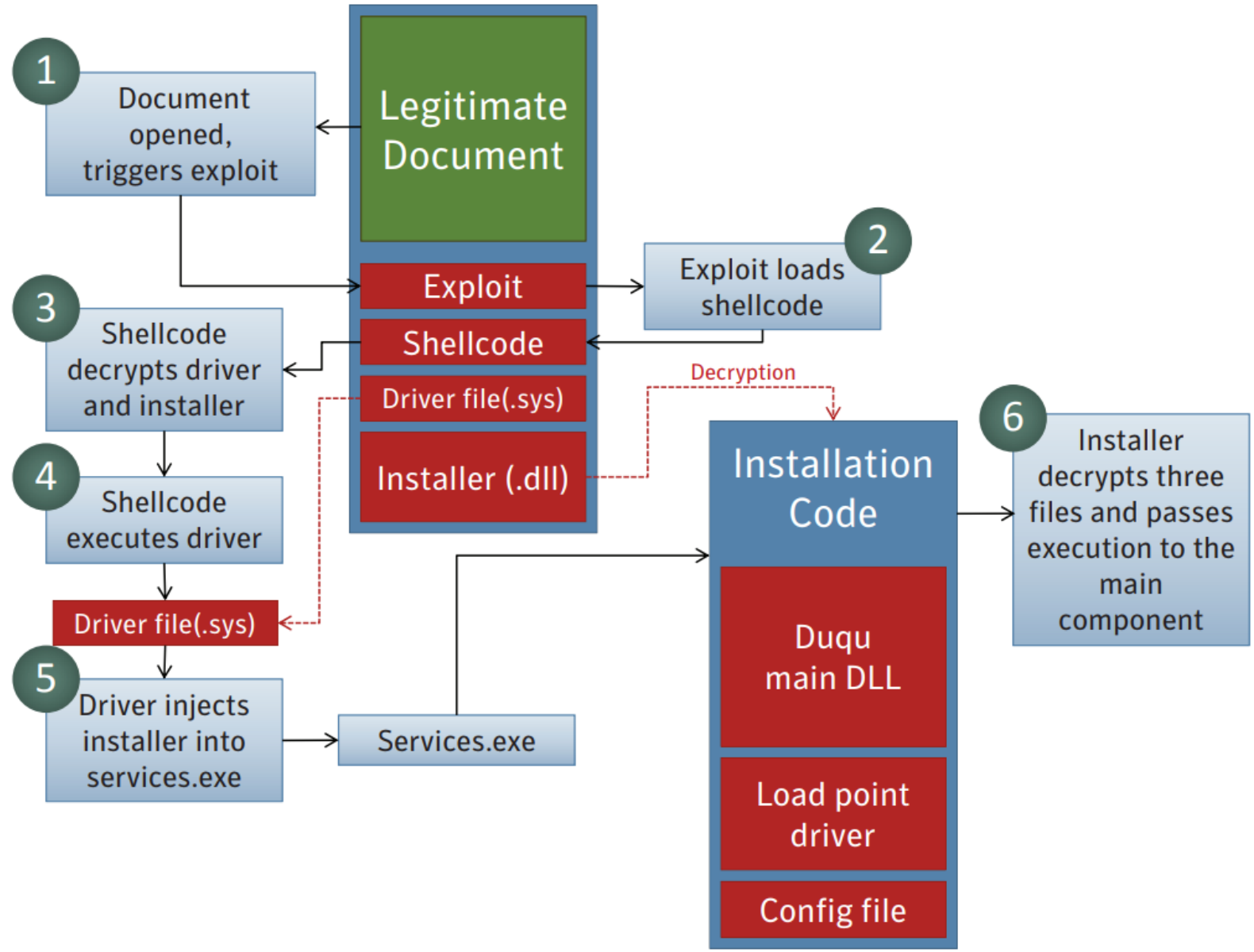
Single zero-day exploit

- MS11-087: Vulnerability in Windows Kernel-Mode Drivers
- Kernel exploit that allows remote code execution (Win32k TrueType font parsing engine)
- First patch in December 2011, further patches in May 2012

Driver signed with valid digital certificate

- C-Media Electronic Inc., headquartered in Taipei, Taiwan
- Revoked on October 14, 2011

W32.Duqu installation process



Duqu C&C

C&C servers configured to simply forward all port 80 and 443 traffic to other servers (potentially other proxies)

Custom C&C protocol

- HTTP and HTTPS communication
- Downloading/uploading dummy `.jpg` files for covert communication
- Additional encrypted data appended to the `.jpg` file

Each attack used one or more C&C servers

- India, Belgium, Vietnam, Germany, China, …

Distribution of additional components

- Infostealer for network enumeration, recording keystrokes, and gathering system info

Flame

Flame

Another information stealer modular malware

“A complete attack toolkit designed for general cyber-espionage purposes”

Discovered in May 2012 by MAHER Center of Iranian National CERT, Kaspersky, and CrySyS

“Most complex malware ever found” ~6MB main component, ~20MB in total

“Twenty times" more complicated than Stuxnet

In operation since at least February 2010 (Kaspersky)

Linked to an attack in April 2012 that caused Iranian officials to disconnect their oil terminals from the Internet

Thousands of victims in Iran and Middle East, but also Europe

Flame Technical Characteristics

Payloads:

- Record audio/video (incl. Skype), screenshots, keystrokes, network traffic, …
- Turn computers into Bluetooth beacons that attempt to download contact information from nearby devices

Several C&C servers around the world

- The program then awaits further instructions from these servers

Extensive use of evasion techniques

- Stealthy process injection and hooking
- Checks for more than 300 AV products
- Uses 5 different encryption algorithms for code obfuscation and hiding its data in files

Flame Propagation

No dropper was ever found (initial infection unknown)

Standard propagation strategies: LAN, USB sticks, Spooler+LNK exploits (same as Stuxnet)

Unique propagation strategy: **Windows Update MitM**

- Turns infected machines into proxies for Windows Update
- Infected machine is announced as a proxy for the domain via the Web Proxy Auto-Discovery Protocol (WPAD)
- When a victim updates, the query is intercepted and an infected update is pushed

Key challenge: (infected) updates must be *signed by Microsoft* to be successfully installed

Flame MD5 Hash Collision Attack

The attackers used the Microsoft Terminal Services Licensing infrastructure to obtain their fake certificate

- Allows licensing servers to automatically obtain certificates from activation servers
- The customer's licensing server generates a key pair and sends the public key to Microsoft's activation server (in a certificate request message)
- The activation server then issues the certificate for the public key and sends it back to the licensing server
- The certificate does not contain any extensions for restricting key usage ➔ *can be used for code signing*

Caveat: the provided certificate contains "MS Hydra extensions," which are rejected by Windows Vista and on

- The certificate can be used as is for code signing only on Windows XP and earlier systems

Flame MD5 Hash Collision Attack

The signature on the certificate is generated on the MD5 hash of the certificate's content

Goal: *obtain a signed certificate without Hydra*

- Usable for code signing even on Windows Vista and Windows 7

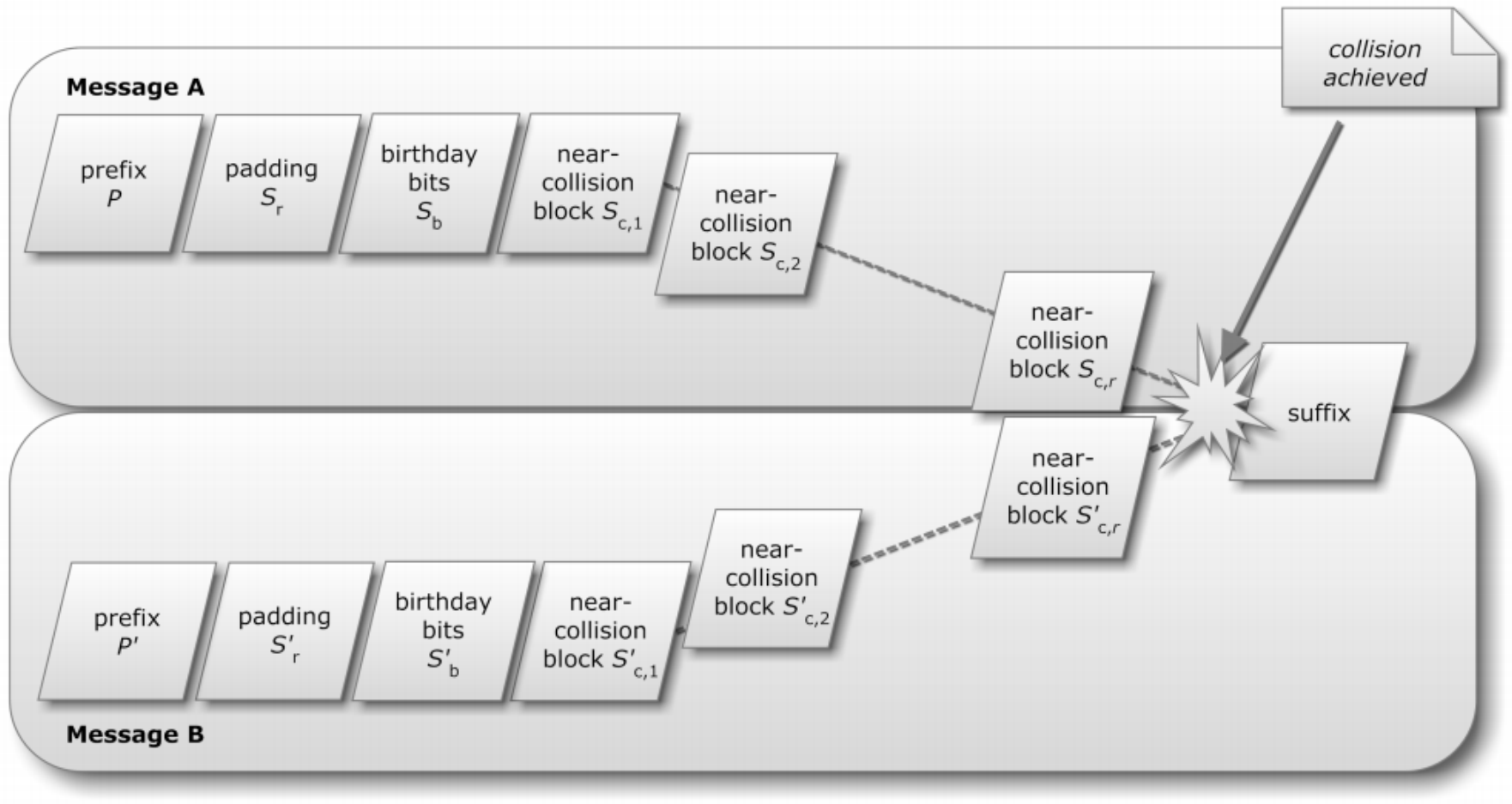
Chosen-prefix hash collision attack

- Start with two chosen (different) inputs, and append "near collision" blocks to both until they yield the same hash value

Outcome: valid *forged* certificate

- *Does not contain the Hydra extension*
- *Matches the hash of a legitimate certificate signed by the CA*

Chosen-prefix Collision



Flame C&C over USB (!)

Infection and data exfiltration from air-gapped networks

- Relies on humans to carry data between air-gapped and internet-connected systems

Flame's operation in restricted environments continues normally

- Documents, audio recordings, etc. are collected and stored by Flame locally

When a USB stick is inserted, Flame reads a hidden database file on it

- If it doesn't exist, it is created with default values
- `EventLog` stores messages from (multiple) infected machines that used this DB before
- `EventLogParams` contains details for all above messages (IP, host name, media ID, …)

Flame does not store leaked documents on the stick unless it had been plugged into a system that successfully contacted the C&C servers

- Easy to determine based on the information contained in EventLogParams

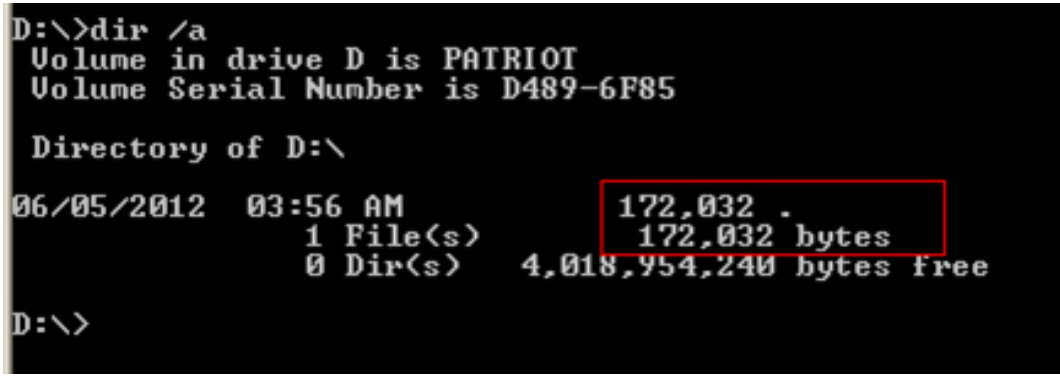
Flame C&C over USB (!)

The file created on the memory stick is named "`.`" (dot)

- The short file name associated with this file entry is `HUB001.DAT`
- The Windows API does not allow the creation of a file named "`.`"
- To achieve this, Flame is performing a RAW write on the FAT directory entry

The dot filename remains invisible

- Ignored by Windows Explorer because it is interpreted as the current directory
- Only the used space in the file system is visible to Windows



`dir /a` reveals the "`.`" file entry, but it still cannot be accessed until the FAT directory entry is manually modified

Gauss

Gauss

Discovered in June 2012 by Kaspersky

- Infostealer similar to Flame and Duqu

Two main distinguishing features:

1) Steals credentials for bank/social networks/email/IM accounts through man-in-the-browser

- In addition to previous infostealer capabilities

2) Gödel module: encrypted with RC4, but the decryption key is *not* embedded in the malware

- Key derived from the MD5 hash performed 10000 times on the combination of the %PATH% and %PROGRAMFILES% environment variables on the victim's machine
- The content of these sections remains unknown…

Supply Chain Attacks

Masquerading as the Windows Update service (Flame) is the ultimate malware spreading mechanism

If we cannot trust the security update mechanism, then what is left?

Supply Chain Attacks

Infected packages/modules distributed through legitimate channels

- Signed with the creator's signature ➔ bypass allowlisting mechanisms

Many infection points

- Insiders at vendor/factory or intermediaries
- Interception of legitimate shipments of equipment (NSA)
- Break into development infrastructure of software vendors (e.g., compromise employee's computer through spear-phishing)
- Compromise the Internet-accessible web servers that a vendor uses to distribute software updates or new releases
- MitM (esp. when TLS is not used during update/delivery)
- Change of ownership (e.g., acquire popular Chrome extension and turn it malicious)
- Third-party code/libraries that developers use in their projects (e.g., Android ad libraries)

CCleaner Attack (2017)

An infected installer was put on the company's official servers

The rogue package was distributed "legitimately" for almost a month

- Vendor's official servers, as well as third-party download sites

"Two-stage backdoor" was added to the application's initialization code

- Download and execute additional malicious code
- Domain name generation algorithm (DGA) to find its C&C servers

Estimated 1.65 million victims

- *But the attackers actually targeted a very specific subset of them:* ***only 40 users (!)***

Photos of an NSA "upgrade" fact

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

Incognito

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS SUBSCRIBE SIGN IN

AT LEAST THEY PICK UP THE EXTRA SHIPPING —

Photos of an NSA "upgrade" factory show Cisco router getting implant

Servers, routers get "beacons" implanted at secret locations by NSA's TAO team.

SEAN GALLAGHER - 5/14/2014, 3:30 PM

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

NSA techs perform an unauthorized field upgrade to Cisco hardware in these 2010 photos from an NSA document.

259

A document included in the trove of National Security Agency files released with Glenn Greenwald's book *No Place to Hide* details how the agency's Tailored Access Operations (TAO) unit and other NSA employees intercept servers, routers, and other network gear being shipped to

FURTHER READING
NSA hacker in residence dishes on how to "hunt" system admins

The Petya Plague Exposes the Th

https://www.wired.com/story/petya-plague-automatic-software-updates/

Incognito

WIRED

The Petya Plague Exposes the Threat of Evil Software Updates

SIGN IN | SUBSCRIBE

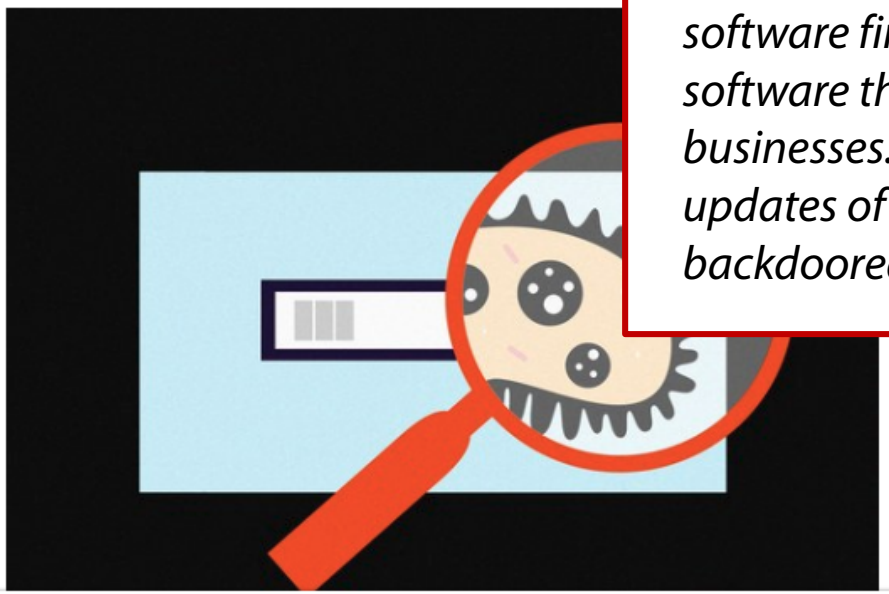
BUSINESS | CULTURE | GEAR | IDEAS | SCIENCE | SECURITY | TRANSPORTATION

SHARE

242

ANDY GREENBERG SECURITY 07.07.17 10:00 AM

THE PETYA PLAGUE EXPOSES THE THREAT OF EVIL SOFTWARE UPDATES



"…hackers penetrated the network of the small Ukrainian software firm MeDoc, which sells a piece of accounting software that's used by roughly 80-percent of Ukrainian businesses. By injecting a tweaked version of a file into updates of the software, they were able to start spreading backdoored versions of MeDoc software"

MOST POPULAR

CULTURE

Exclusive: What to Expect From Sony's Next-Gen PlayStation

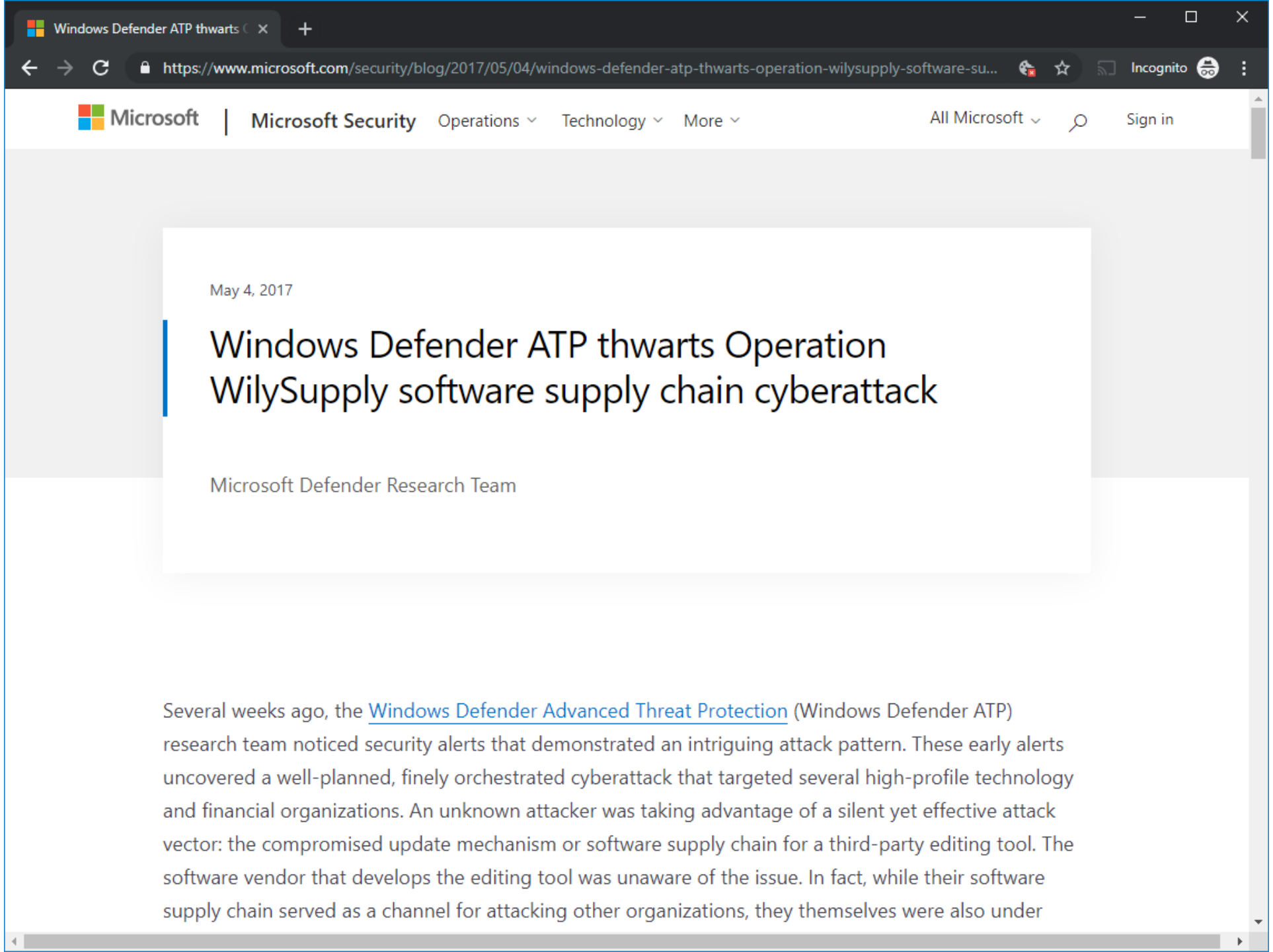
MORE STORIES

3 FREE ARTICLES LEFT THIS MONTH

Ad-free browsing + unlimited access. Subscribe

Sign In or Register if you're already a subscriber.

CLOSE


Windows Defender ATP thwarts
https://www.microsoft.com/security/blog/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-su...
Incognito
Microsoft | Microsoft Security
Operations
Technology
More
All Microsoft
Sign in
May 4, 2017
Windows Defender ATP thwarts Operation WilySupply software supply chain cyberattack
Microsoft Defender Research Team
Several weeks ago, the Windows Defender Advanced Threat Protection (Windows Defender ATP) research team noticed security alerts that demonstrated an intriguing attack pattern. These early alerts uncovered a well-planned, finely orchestrated cyberattack that targeted several high-profile technology and financial organizations. An unknown attacker was taking advantage of a silent yet effective attack vector: the compromised update mechanism or software supply chain for a third-party editing tool. The software vendor that develops the editing tool was unaware of the issue. In fact, while their software supply chain served as a channel for attacking other organizations, they themselves were also under

ShadowPad in corporate network

AO Kaspersky Lab [RU] | https://securelist.com/shadowpad-in-corporate-networks/81432/

Incognito

APT REPORTS

ShadowPad in corporate networks

Popular server management software hit in supply chain attack

By GReAT on August 15, 2017. 6:00 pm

ShadowPad, part 2: Technical Details (PDF)

In July 2017, during an investigation, suspicious DNS requests were identified in a partner's network. The partner, which is a financial institution, discovered the requests originating on systems involved in the processing of financial transactions.

Further investigation showed that the source of the suspicious DNS queries was a software package produced by NetSarang. Founded in 1997, NetSarang Computer, Inc. develops, markets and supports secure connectivity solutions and specializes in the development of server management tools for large corporate networks. The company maintains headquarters in the United States and South Korea.

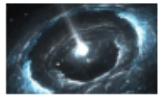
IN THE SAME CATEGORY


Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities


GreyEnergy's overlap with Zebrocy


A Zebrocy Go Downloader


APT review of the year


DarkPulsar FAQ

Gaming industry still in the scope

https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

Incognito

Gaming industry still in the scope of attackers in Asia

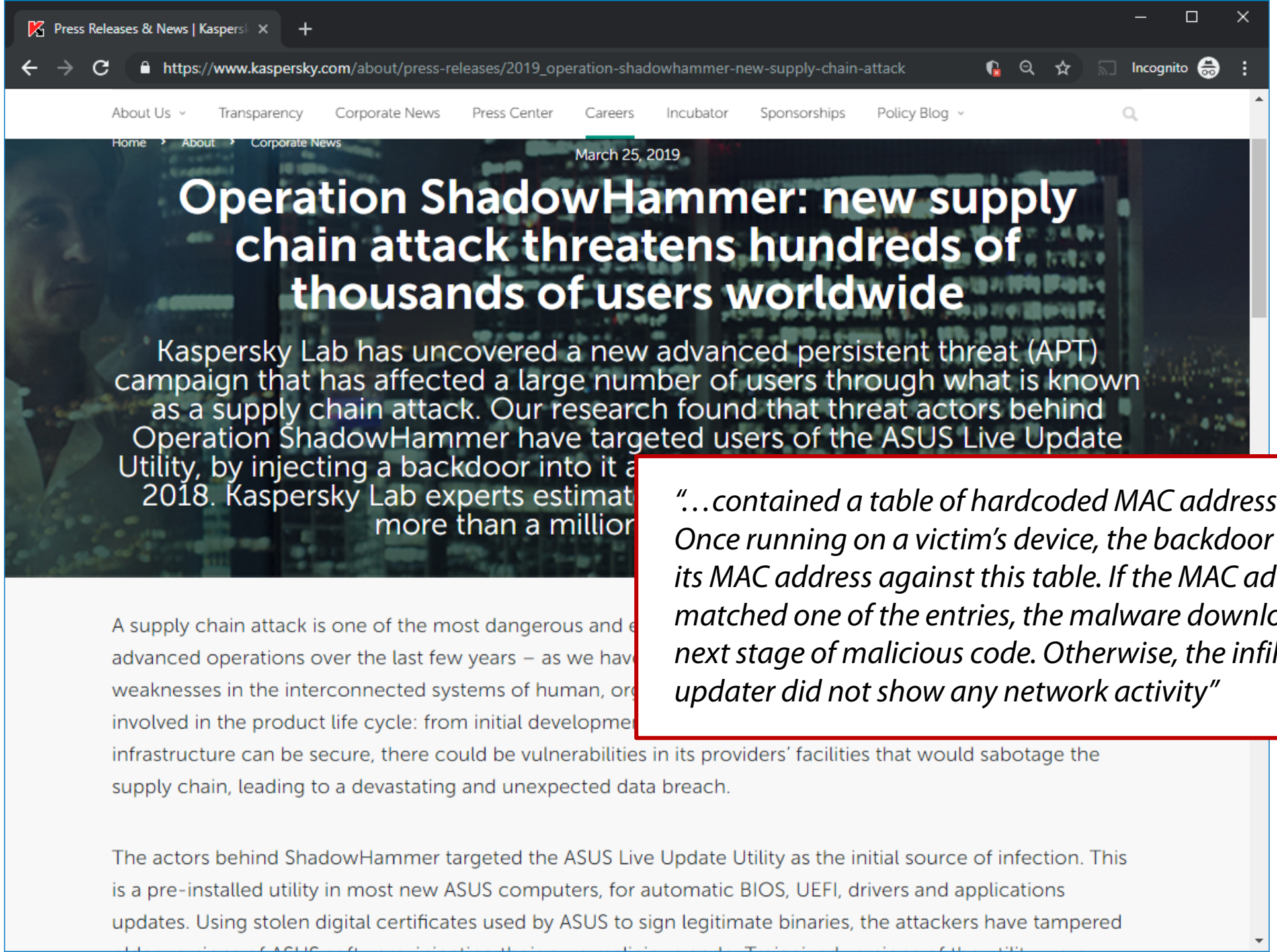
Asian game developers again targeted in supply-chain attacks distributing malware in legitimately signed software

Marc-Etienne M.Léveillé 11 Mar 2019 - 11:27AM

Share

This is not the first time the gaming industry has been targeted by attackers who compromise game developers, insert backdoors into a game's build environment, and then have their malware distributed as legitimate software. In April 2013, Kaspersky Lab reported that a popular game was altered to include a backdoor in 2011. That attack was attributed to perpetrators Kaspersky called the Winnti Group.

Yet again, new supply-chain attacks recently caught the attention of ESET Researchers. This time, two games and one gaming platform application were compromised to include a backdoor. Given that these attacks were mostly targeted against Asia and the gaming industry, it shouldn't be surprising they are the work of the group described in Kaspersky's "Winnti – More than just a game".



"…contained a table of hardcoded MAC addresses […] Once running on a victim's device, the backdoor verified its MAC address against this table. If the MAC address matched one of the entries, the malware downloaded the next stage of malicious code. Otherwise, the infiltrated updater did not show any network activity"

Marc-Etienne M.Léveillé
@marc_etienne_

Here's something interesting: the backdoor in ASUS Update Setup.exe is _again_ located in the CRT, just like the CCleaner case and recent games with a backdoor. This time in _crtExitProcess. #ShadowHammer

```
; void __cdecl __noreturn __crtExitProcess(UINT uExitCode)
___crtExitProcess proc near             ; CODE XREF: _fast_error_exit+20↑p
                                        ; _malloc+2A↑p ...

uExitCode       = dword ptr  8

                mov     edi, edi
                push    ebp
                mov     ebp, esp
                push    [ebp+uExitCode]
                call    decrypt_and_launch_payload
                pop     ecx
                push    [ebp+uExitCode] ; uExitCode
                call    ds:ExitProcess
___crtExitProcess endp
```

11:31 AM · Mar 25, 2019 · Twitter Web Client

Mining for malicious Ruby gems

blog.reversinglabs.com/blog/mining-for-malicious-ruby-gems

Incognito

April 16, 2020

Mining for malicious Ruby gems

Typosquatting barrage on RubyGems software repository users

BLOG AUTHOR
Tomislav Maljic, Threat An

These days, organizations are acknowledgin
their systems. They are putting in effort to ac
eliminating blindspots in the attack chain
incident happening. This makes it harder for threat actors to achieve their malicious intentions, as attacking such organizations directly is less likely to yield results.

To bypass such measures, threat actors are always on the lookout for new attack

"One typosquatted gem, 'atlas-client' […] had 2,100 downloads, close to 30% of the total downloads that the legitimate gem 'atlas_client' had"

"The script then checks if the clipboard data matches the format of a cryptocurrency wallet address. If it does, it replaces the address with an attacker-controlled one"