

CSE508

# Network Security



Stony Brook University

2021-04-13

## Malware

Michalis Polychronakis

*Stony Brook University*

Stuxnet

Duqu

Flame

Gauss

...

# **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 0-day

Notified Microsoft and other researchers

Researchers started analyzing the ~0.5MB binary (huge compared to typical malware)

The team identified *four* Windows 0-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 specific software of interest is not present, the virus goes inert, remaining undetected on the system

The world eventually 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

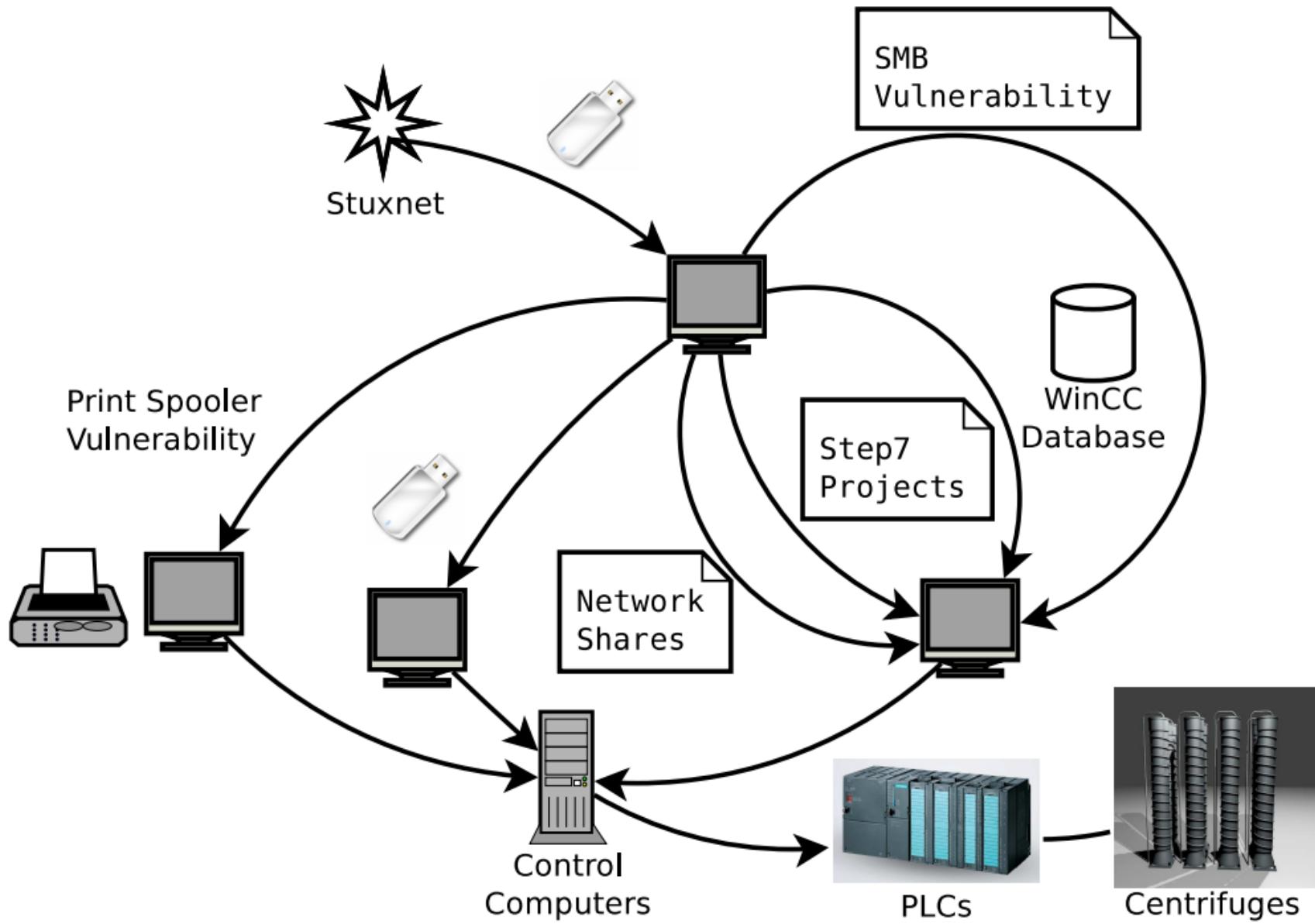
## Evolution of Stuxnet exploits

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

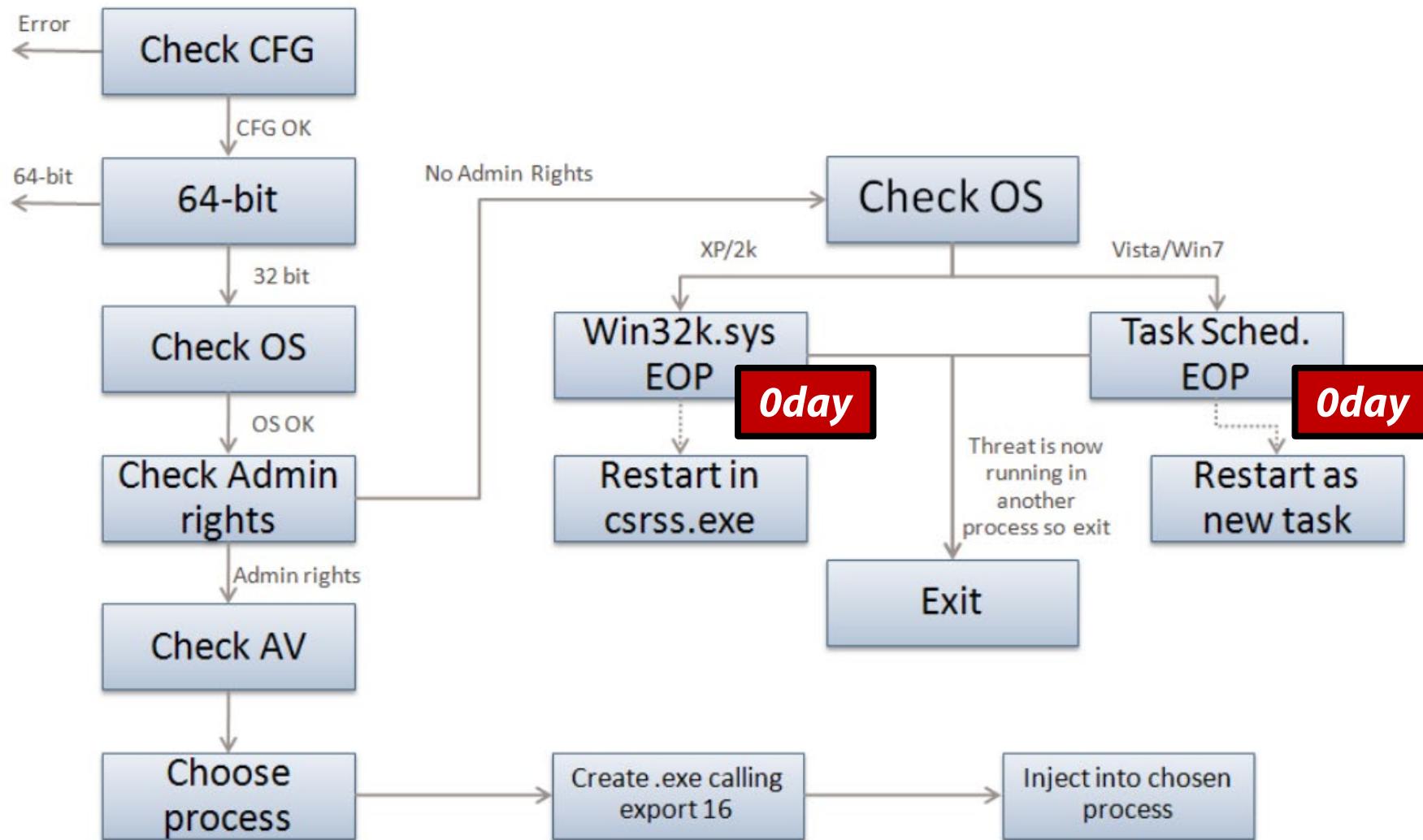
Table 3

## 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

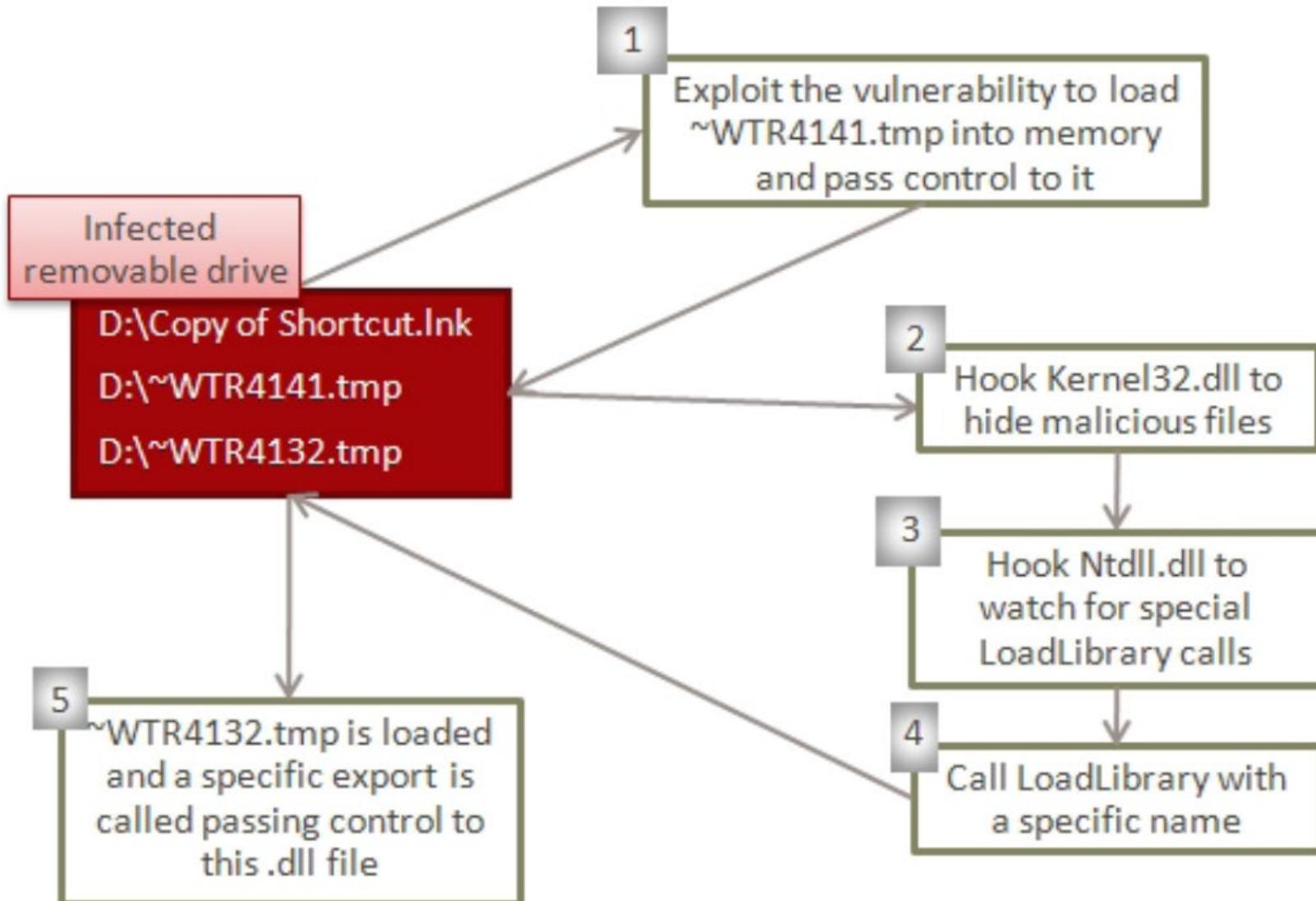
00000000:	4D5A9000	03000000	04000000	FFFF0000	MZ .....yy..
00000010:	B8000000	00000000	40000000	00000000	,.....@.....
00000020:	00000000	00000000	00000000	00000000	.....
00000030:	00000000	00000000	00000000	E0000000	.....fi...à..
00000040:	0E1FBA0E	00B409CD	21B8014C	CD215468	..ò...fi..L!Th
00000050:	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	Izw .../ .../ .../
00000090:	ACDD642F	9D1B192F	ACDD622F	9C1B192F	-Ýd .../ .../Ýb/ .../
000000A0:	8B1B182F	6D1B192F	ACDD6B2F	DA1B192F	.../m.../Ýk/Ü.../

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 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 Kernel-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

The image shows two windows side-by-side. On the left is the 'jmidebs.sys Properties' dialog, specifically the 'Digital Signatures' tab. It displays 'Digital Signature Details' with tabs for 'General' and 'Advanced'. Under 'General', there is a section titled 'Digital Signature Information' with the message 'This digital signature is OK.' This entire section is highlighted with a red rectangle. Below it, under 'Signer information', the name 'JMicron Technology Corp.' is listed, also highlighted with a red rectangle.

**Certificate**

General Details Certification Path

**Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

\* Refer to the certification authority's statement for details.

**Issued to:** Realtek Semiconductor Corp

**Issued by:** VeriSign Class 3 Code Signing 2004 CA

**Valid from:** 3/14/2007 **to:** 6/11/2010

Install Certificate... Issuer Statement OK

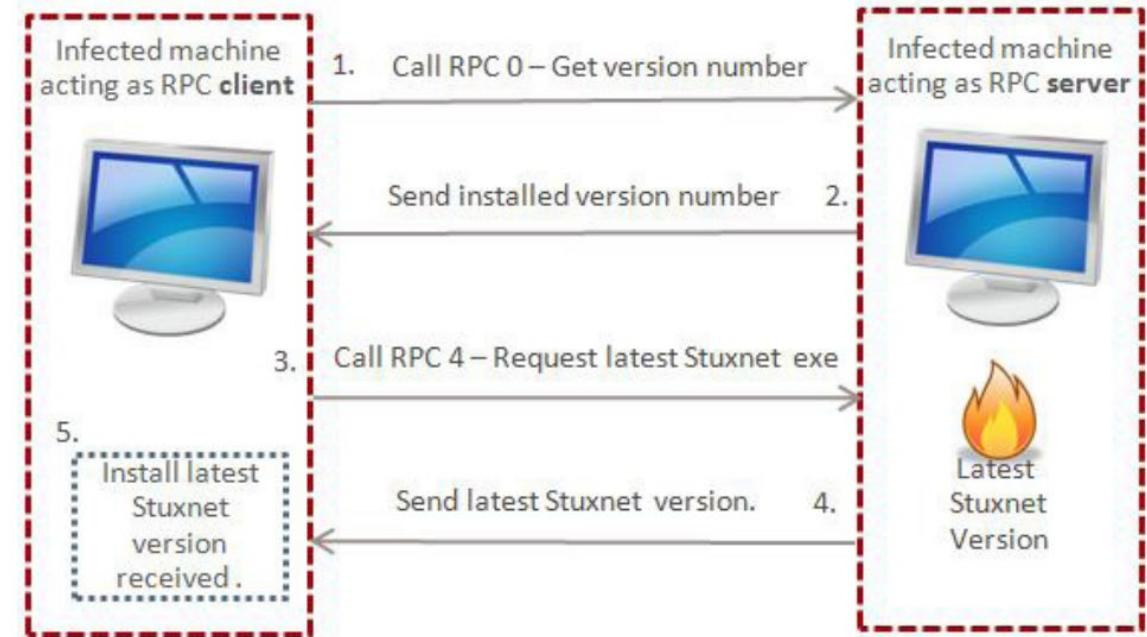
# P2P Communication

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:

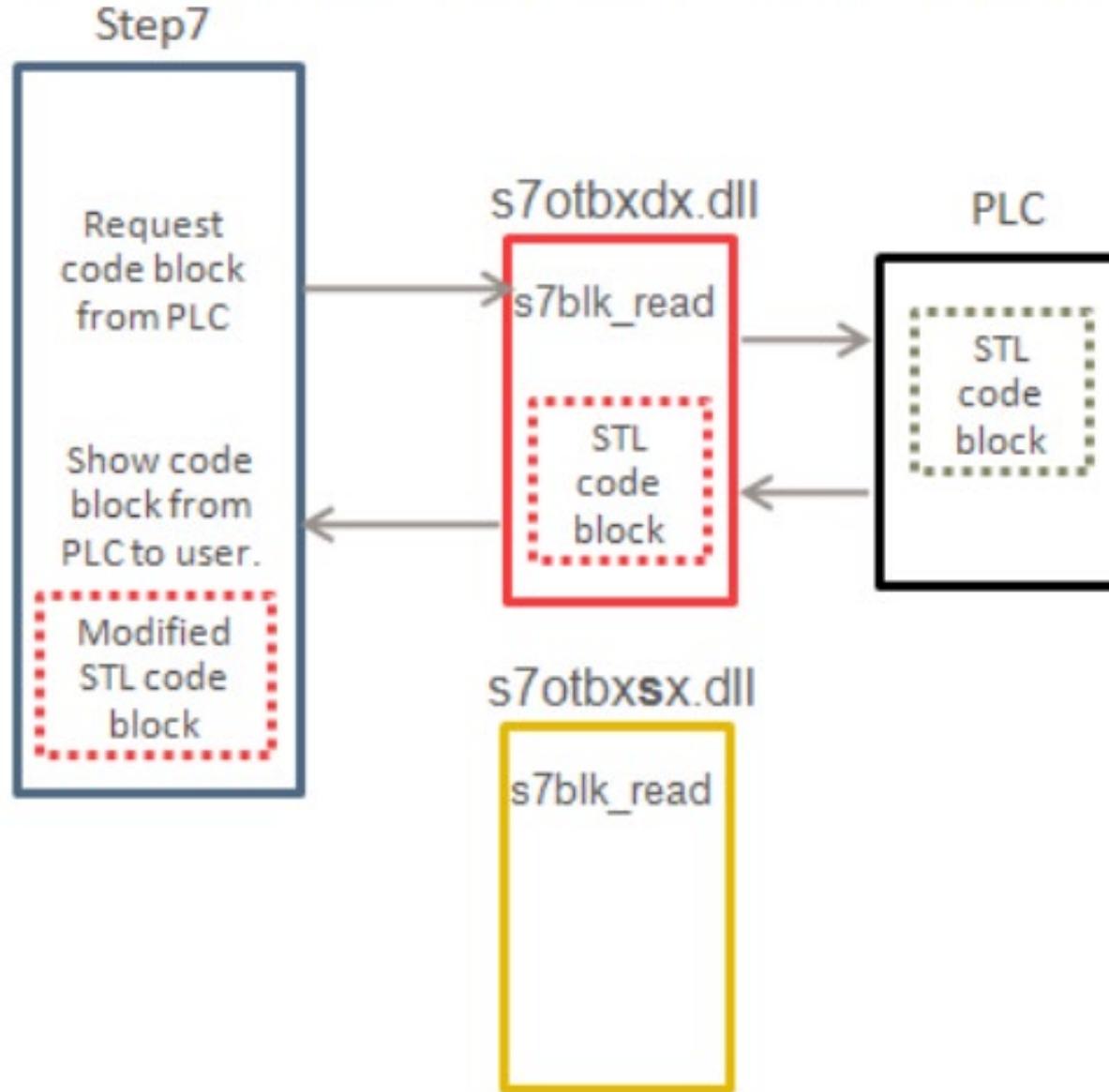
Monitor PLC blocks written to or read from the PLC

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 s7otbxidx.dll



## C&C

Upon infection, contacts two possible domains over HTTP port 80

[www\[.\]mypremierfutbol\[.\]com](http://www[.]mypremierfutbol[.]com)

[www\[.\]todaysfutbol\[.\]com](http://www[.]todaysfutbol[.]com)

Servers hosted in Malaysia and Denmark

Communication “encrypted” with simple XOR

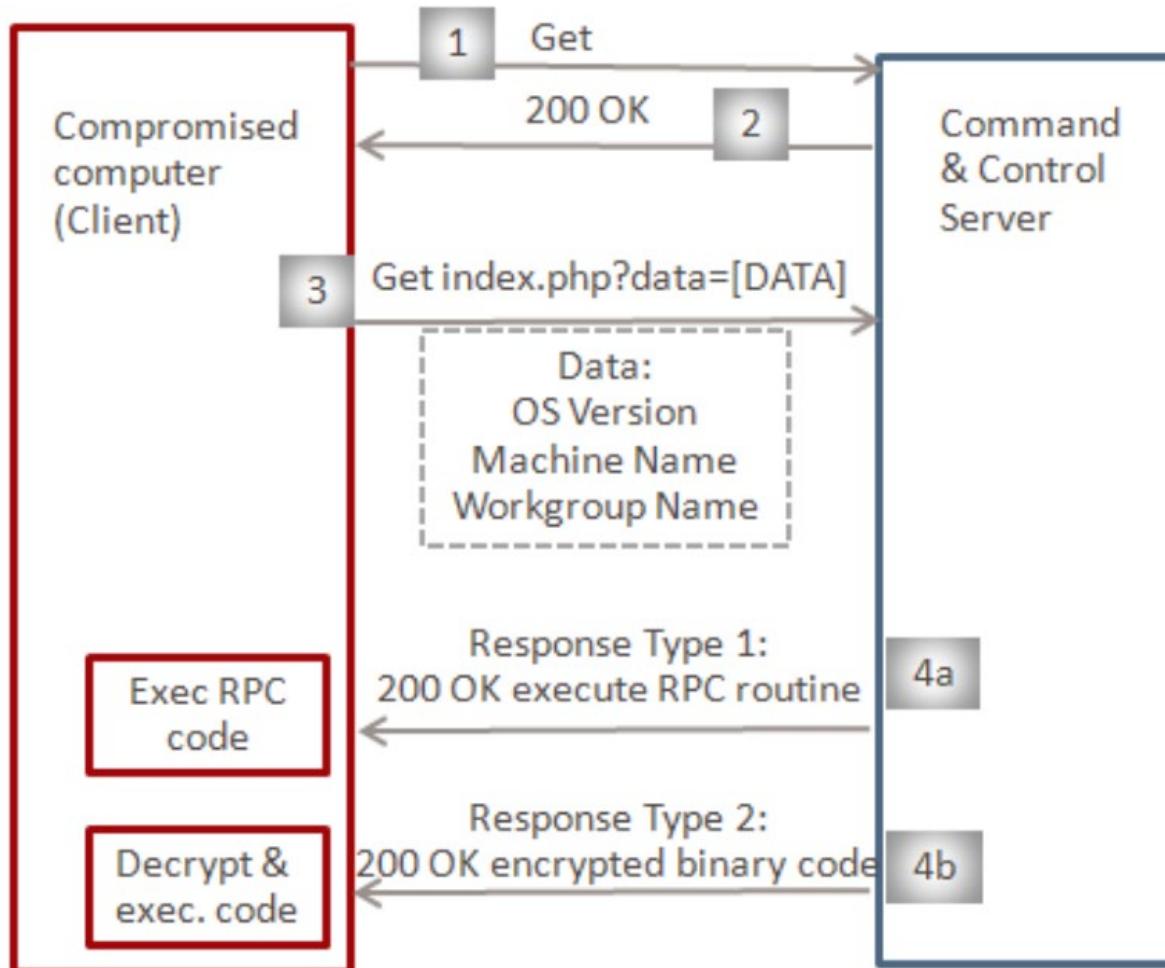
Client to server: 0xFF

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

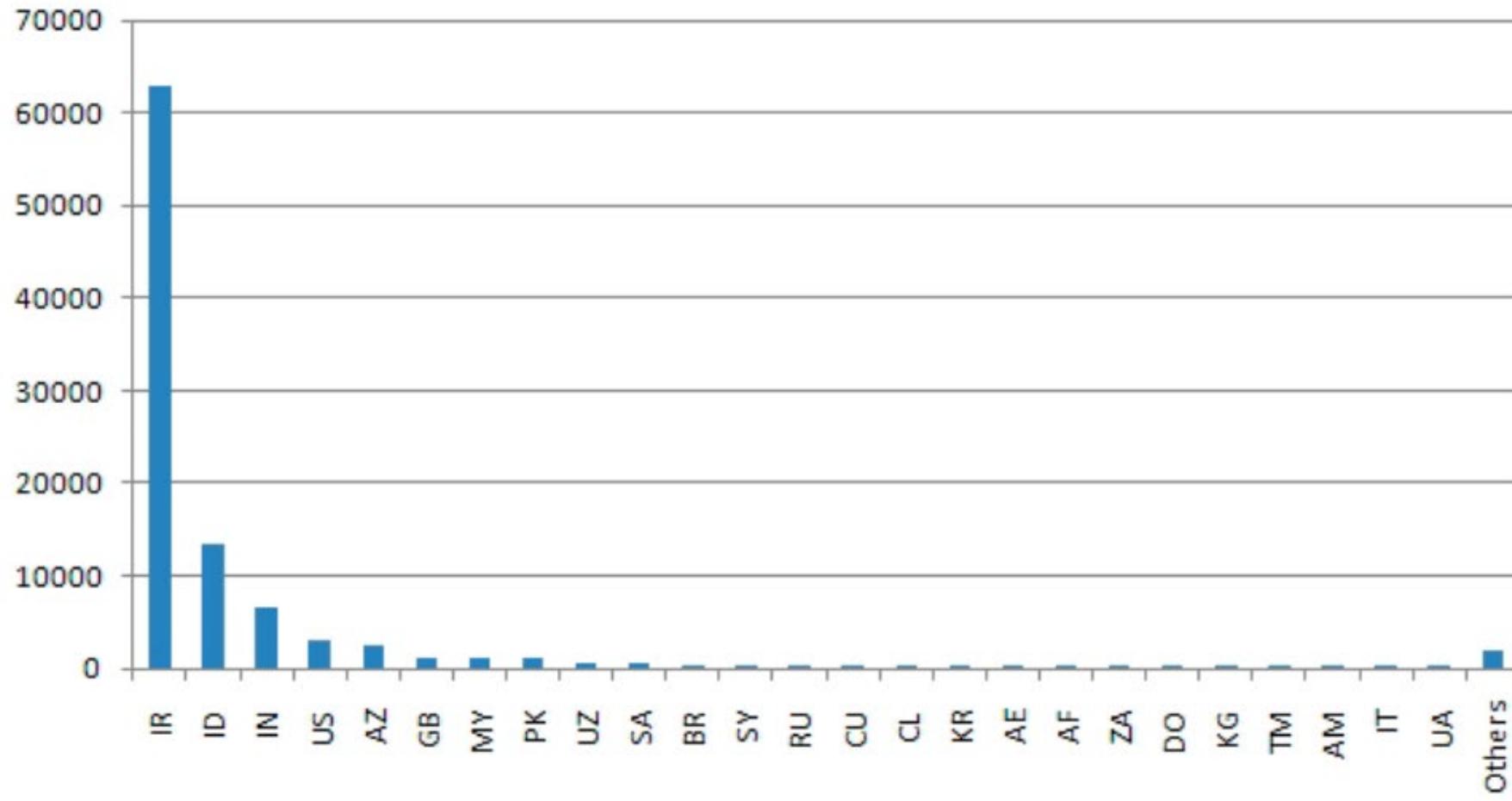
Nothing really special

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

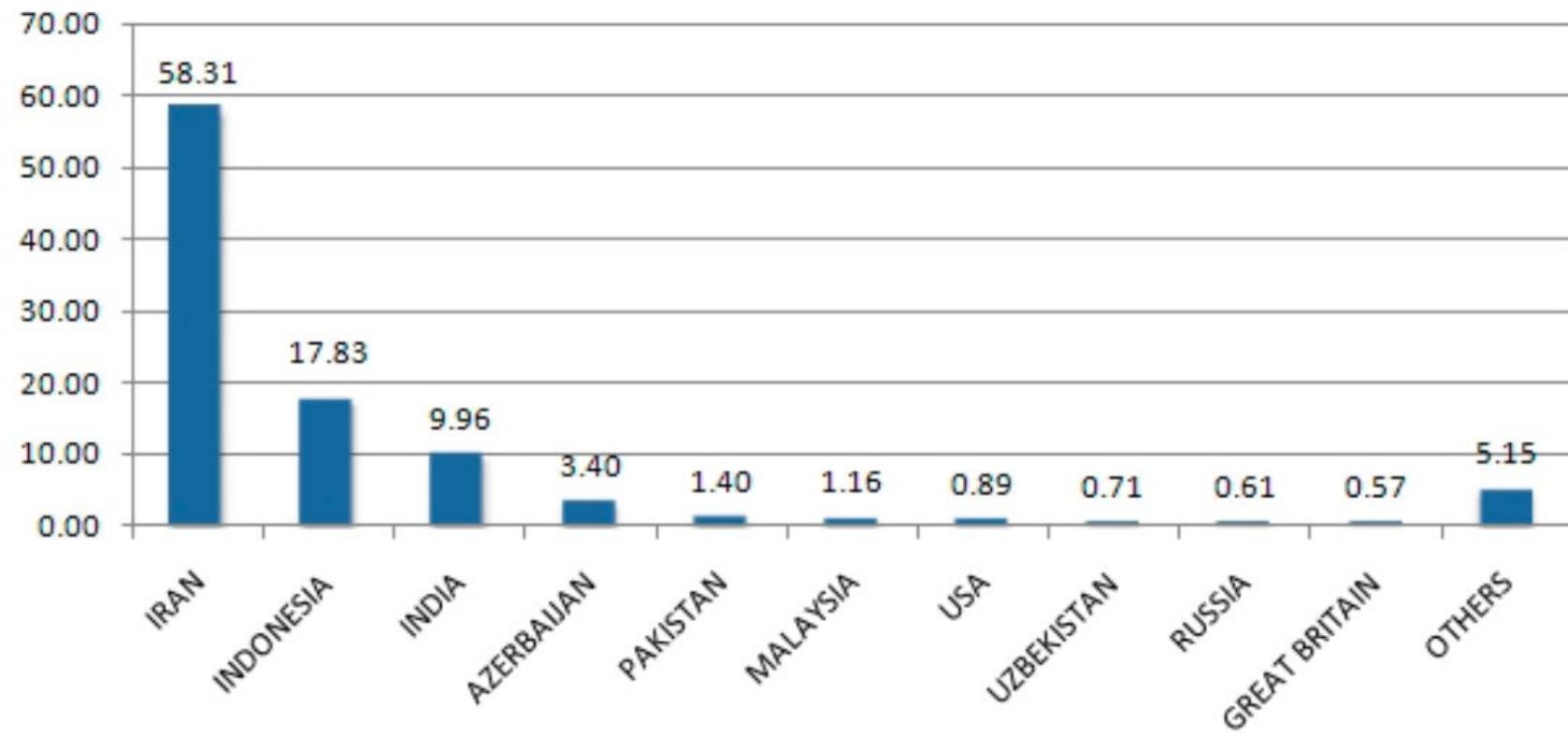
## Infected Hosts



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



### Percentage of Stuxnet infected Hosts with Siemens Software installed

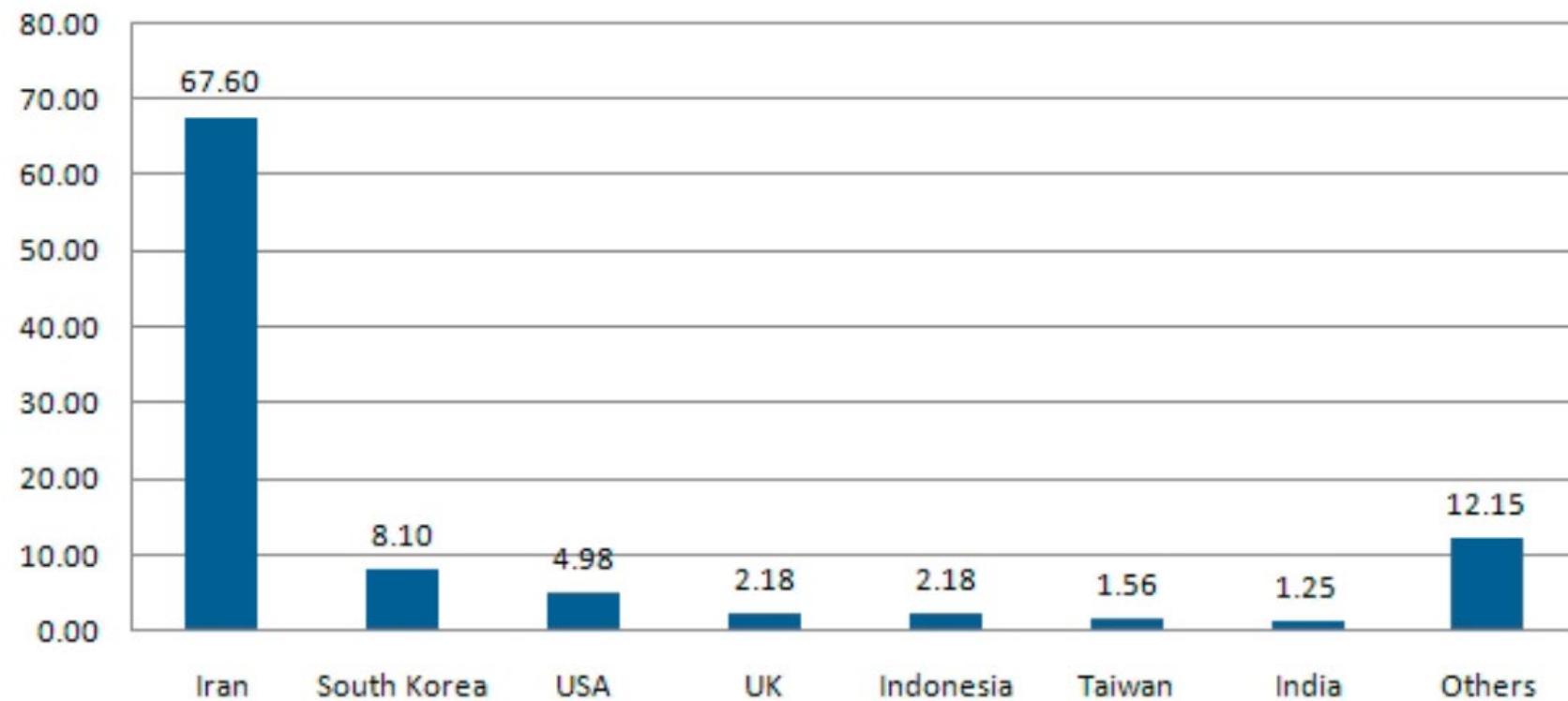


Table 2

## 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

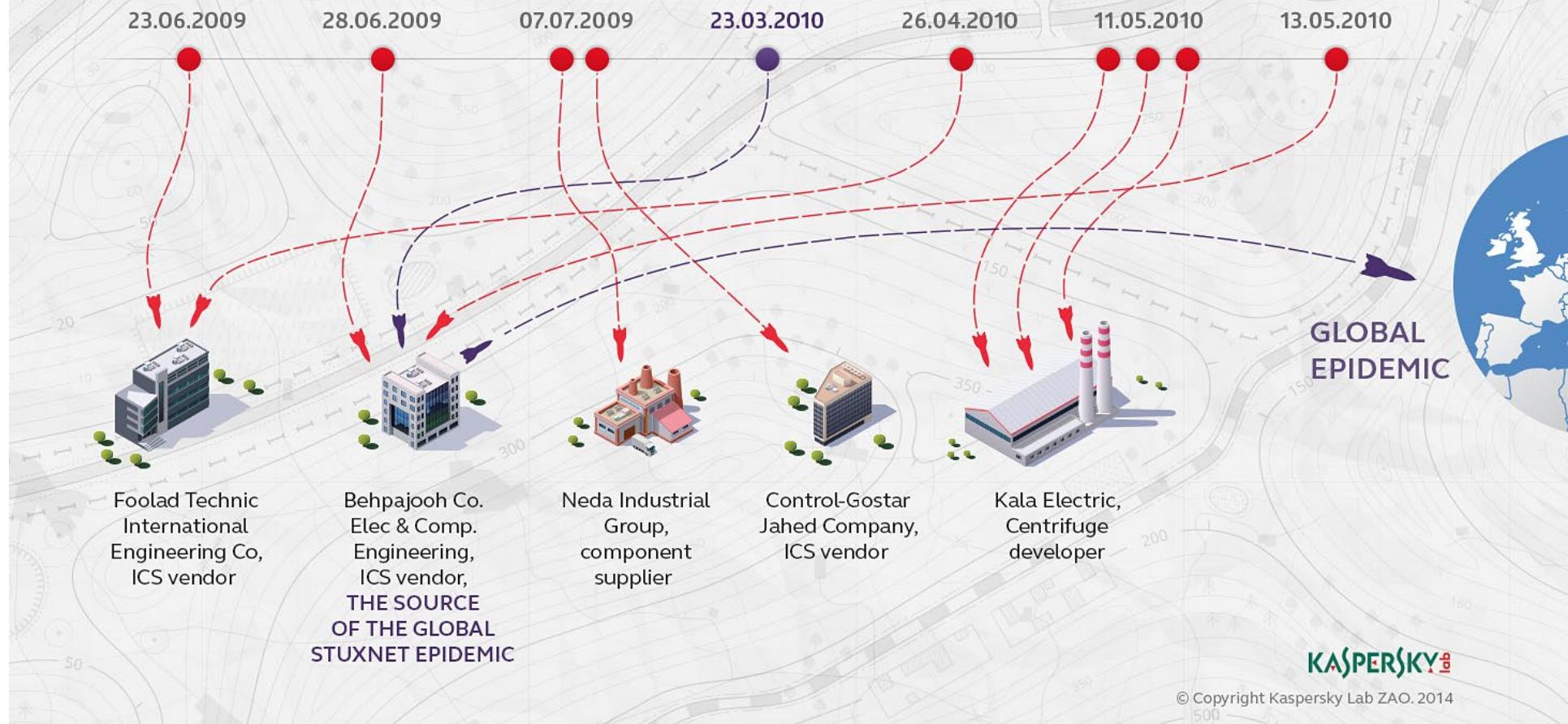
Stuxnet records a timestamp (along with other system information) each time a new infection occurs (including the initial infection)

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

## OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009.

The attack started by infecting five carefully selected organizations



## Did Stuxnet Achieve its Goal?

January 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”



# ***Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage***

The power failure was described by Iran as “nuclear terrorism” as talks were underway in Vienna to restore the 2015 nuclear deal.

By Ronen Bergman, Rick Gladstone and Farnaz Fassihi

April 11, 2021

A power failure that appeared to have been caused by a deliberately planned explosion struck [Iran](#)'s Natanz uranium enrichment site on Sunday, in what Iranian officials called an act of sabotage that they suggested had been carried out by Israel.

The blackout injected new uncertainty into diplomatic efforts that began last week to salvage the 2015 nuclear deal repudiated by the Trump administration.





# Natanz attack hit 50 meters underground, destroyed most of the facility

The attack was reportedly carried out through a remotely detonated device smuggled into the facility.

By TZVI JOFFRE, YONAH JEREMY BOB APRIL 13, 2021 16:07

The alleged Israeli attack on Iran's [Natanz nuclear facility](#) targeted an electrical substation located 40 to 50 meters underground and damaged "thousands of centrifuges," Iranian officials revealed in recent days.

Fereydoon Abbasi-Davani, former head of Iran's Atomic Energy Organization, told Iranian media on Monday that the attack hit an electrical substation located deep underground and managed to damage both the power distribution system and the cable leading to the centrifuges in order to cut power to them.

**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)

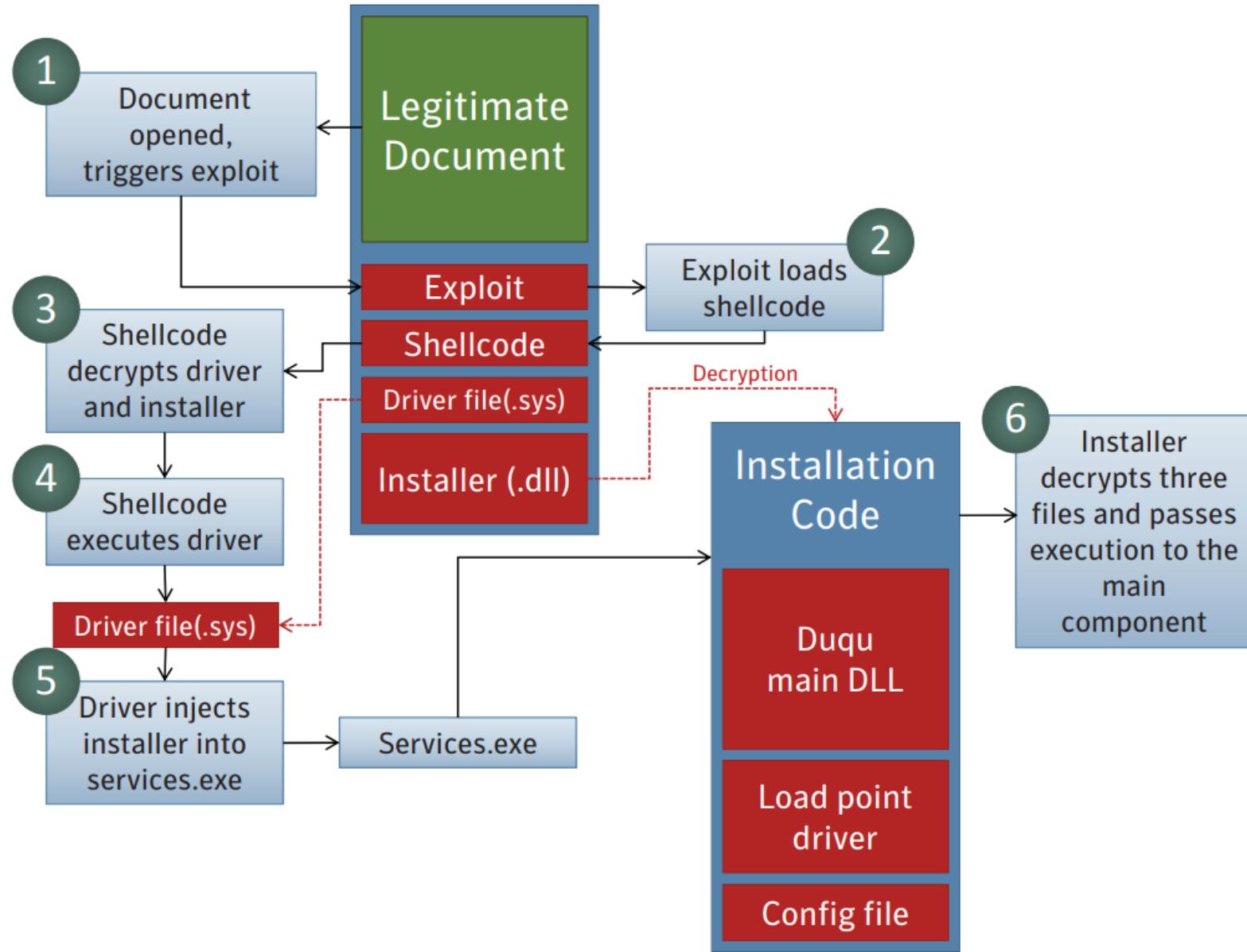
First patch in December 2011, further patches in May 2012

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 a “Microsoft Hydra extension,” which is rejected by Windows Vista and on

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

# 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**

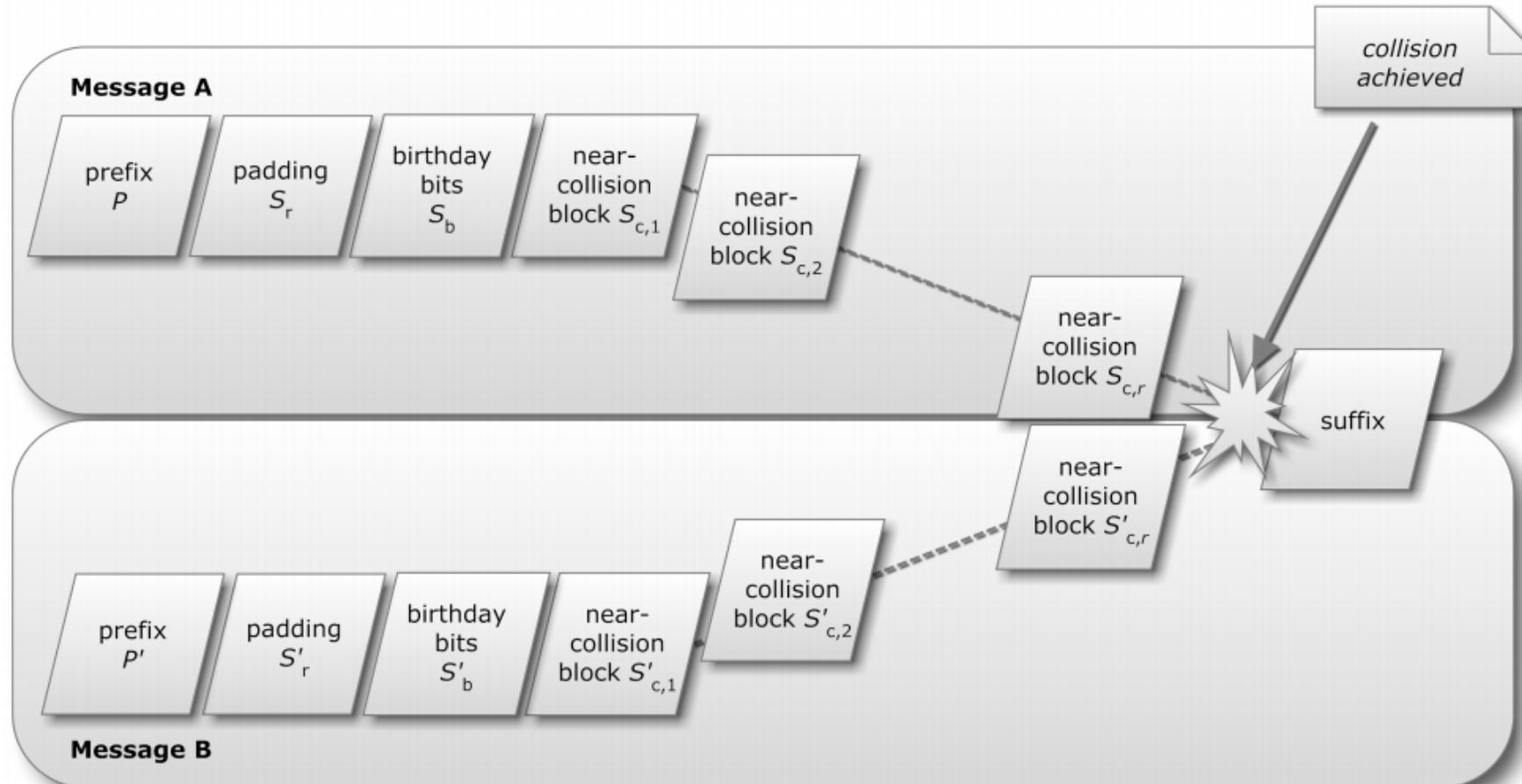
Start with two chosen (different) inputs, and append “near collision” blocks to both until they yield the same hash value

**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

```
D:\>dir /a
Volume in drive D is PATRIOT
Volume Serial Number is D489-6F85

Directory of D:\

06/05/2012  03:56 AM           172,032 .
                           1 File(s)   172,032 bytes
                           0 Dir(s)   4,018,954,240 bytes free

D:\>
```

*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 whitelisting mechanisms

Many infection points

Insiders at vendor/factory or intermediaries

Interception of legitimate shipments of equipment (NSA)

Break into development infrastructure/pipeline 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 commonly used by developers (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 (!)***



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



## SHARE

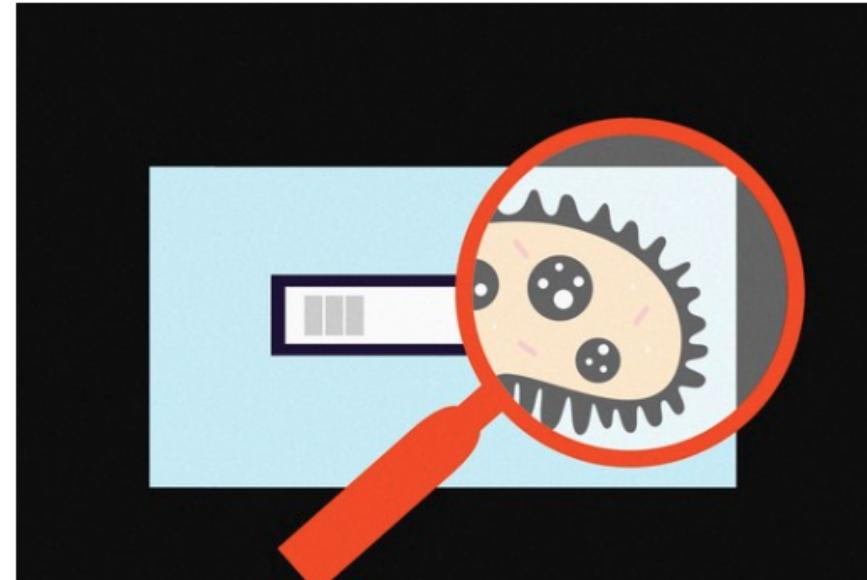


242



ANDY GREENBERG SECURITY 07.07.17 10:00 AM

# THE PETYA PLAGUE EXPOSES THE THREAT OF EVIL SOFTWARE UPDATES



3

FREE ARTICLES LEFT THIS MONTH

Ad-free browsing + unlimited access. [Subscribe](#)

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

CLOSE X

## MOST POPULAR



CULTURE

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

PETER RUBIN

*“...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”*



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

## 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.

The screenshot shows the NetSarang website with the XManager Enterprise 5 product page. The top navigation bar includes links for Online Store, Reseller Login, and Korean. The main content features the XManager Enterprise 5 logo and a brief description of the Secure UNIX/Linux Connectivity Solution. Below this, there are links for Product Detail and Download. At the bottom, there are links for Evaluate Software, Ask questions, and Purchase Software.

## IN THE SAME CATEGORY



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



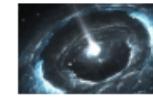
GreyEnergy's overlap with Zebrocy



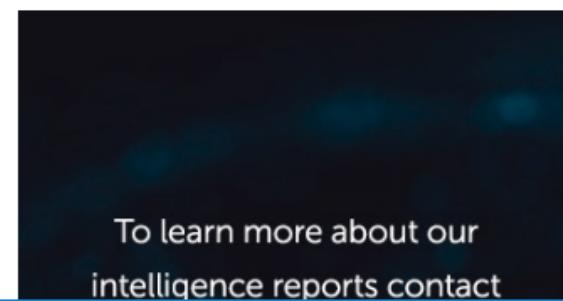
A Zebrocy Go Downloader



APT review of the year



DarkPulsar FAQ



# Gaming industry still in the scope of attackers in Asia

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



Marc-Etienne M. Léveillé | 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".



March 25, 2019

# Operation ShadowHammer: new supply chain attack threatens hundreds of thousands of users worldwide

Kaspersky Lab has uncovered a new advanced persistent threat (APT) campaign that has affected a large number of users through what is known as a supply chain attack. Our research found that threat actors behind Operation ShadowHammer have targeted users of the ASUS Live Update Utility, by injecting a backdoor into it at least between 2017 and 2018. Kaspersky Lab experts estimate that the attack affected more than a million users worldwide.

A supply chain attack is one of the most dangerous and effective infection vectors used by threat actors to conduct advanced operations over the last few years – as we have seen with ShadowHammer. Supply chain attacks exploit weaknesses in the interconnected systems of human, organizational, material, financial, and technological components involved in the product life cycle: from initial development stage through to the final consumer. Even if the infrastructure can be secure, there could be vulnerabilities in its providers' facilities that would sabotage the supply chain, leading to a devastating and unexpected data breach.

*“...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”*

The actors behind ShadowHammer targeted the ASUS Live Update Utility as the initial source of infection. This is a pre-installed utility in most new ASUS computers, for automatic BIOS, UEFI, drivers and applications updates. Using stolen digital certificates used by ASUS to sign legitimate binaries, the attackers have tampered

Emergency Assistance Package for COVID-19 Impacted Industries

[Read more](#)

Search

[CONTACT US](#)

Blog

[Solutions](#) ▾[Products & Technology](#) ▾[Partners](#) ▾[Resources](#) ▾[Company](#) ▾[GET STARTED](#)

April 16, 2020

# Mining for malicious Ruby gems

## Typosquatting barrage on RubyGems software repository users



BLOG AUTHOR

Tomislav Maljic, Threat Analyst at ReversingLabs



These days, organizations are acknowledging the importance of security in their systems. They are putting in effort to adopt security measures to

eliminating blindspots in the attack chain that would increase the risk of a security 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.

*"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"*



# Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

## FIREEYE | EVASION | SUPPLY CHAIN

## Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
  - FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
  - The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
  - The campaign is widespread, affecting public and private organizations around the world.
  - FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public [GitHub page](#). FireEye products and services can help customers detect and block this attack.

## Summary

FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software.

## Recent Posts

26 Jan 2021

## Phishing Campaign Leverages WOFF Obfuscation and Telegram Channels for Communication >

21 Jan 2021

## Training Transformers for Cyber Security Tasks: A Case Study on Malicious URL Prediction >

20 Jan 2021

Emulation of Kernel Mode  
Rootkits With Speakeasy >

RSS FEED: STAY CONNECTED

