



Jumping the air gap

15 years of nation-state effort

Alexis Dorais-Joncas | Senior Manager, Threat Research

Facundo Munoz | Malware Researcher



Alexis Dorais-Joncas

Senior Manager, Malware Research

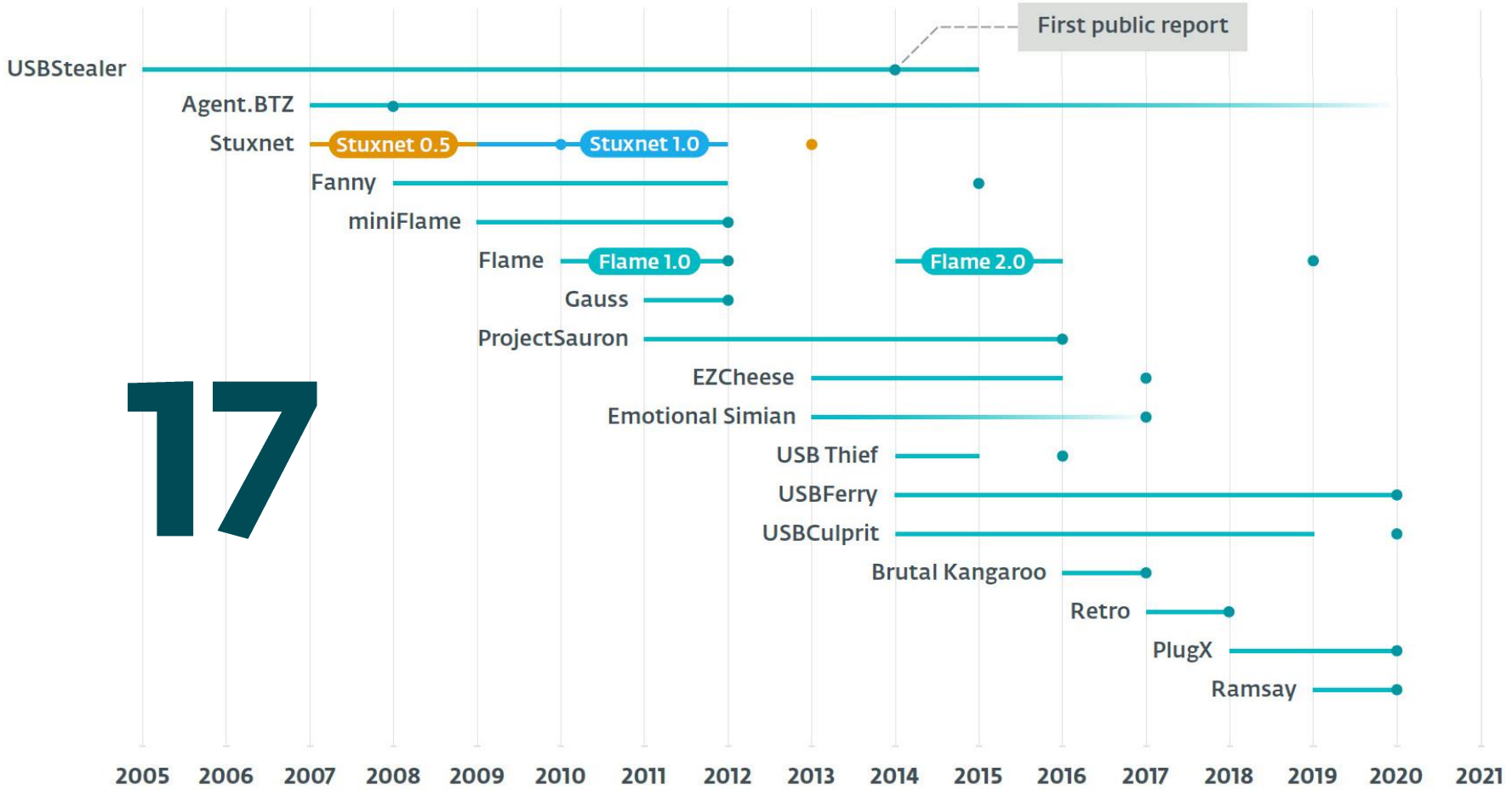


Facundo Muñoz

Malware Researcher

*Malware, or a set of malware components acting together (a framework), that implements an **offline, covert communication mechanism between an air-gapped system and the attacker***

17



Strong attribution

DarkHotel

Retro
2017-2019

Ramsay
2019-2020

Sednit

USBStealer
2005-2015

Tropic Trooper

USBFerry
2014-2020

Goblin Panda

USBCulprit
2014-2019

Mustang Panda

PlugX
2018-2020

Equation Group

Fanny
2008-2012

Controversial attribution

Stuxnet
2007-2012

Flame
2010-2012, 2014-2016

miniFlame
2009-2012

Gauss
2011-2012

ProjectSauron
2011-2016

Agent.BTZ
2007-201x

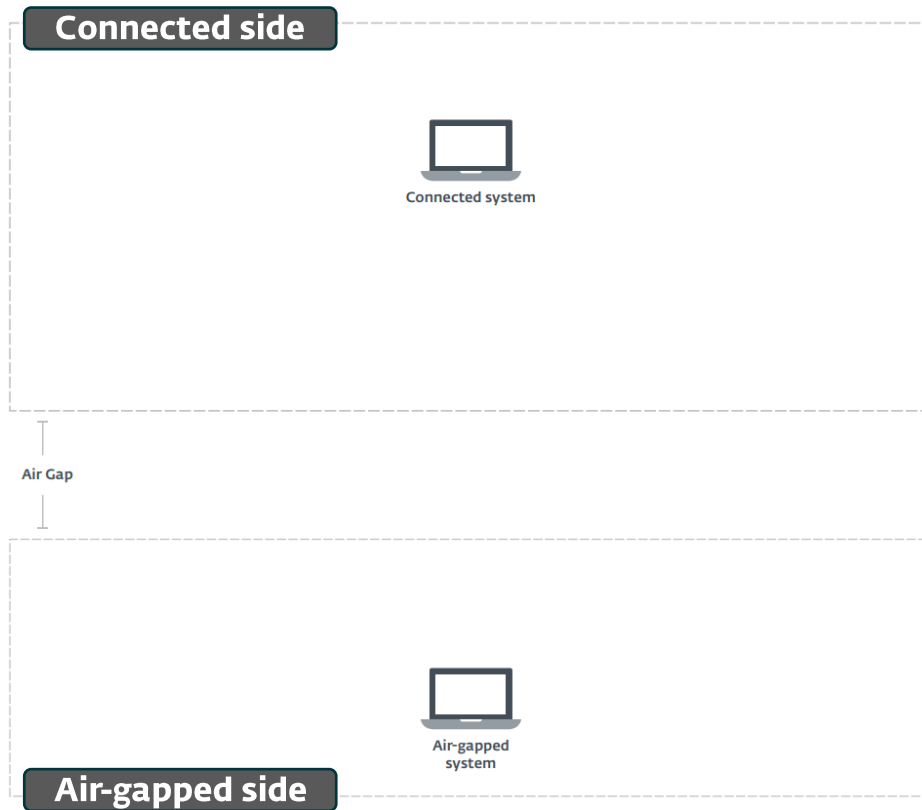
USBThief
2015

EZCheese

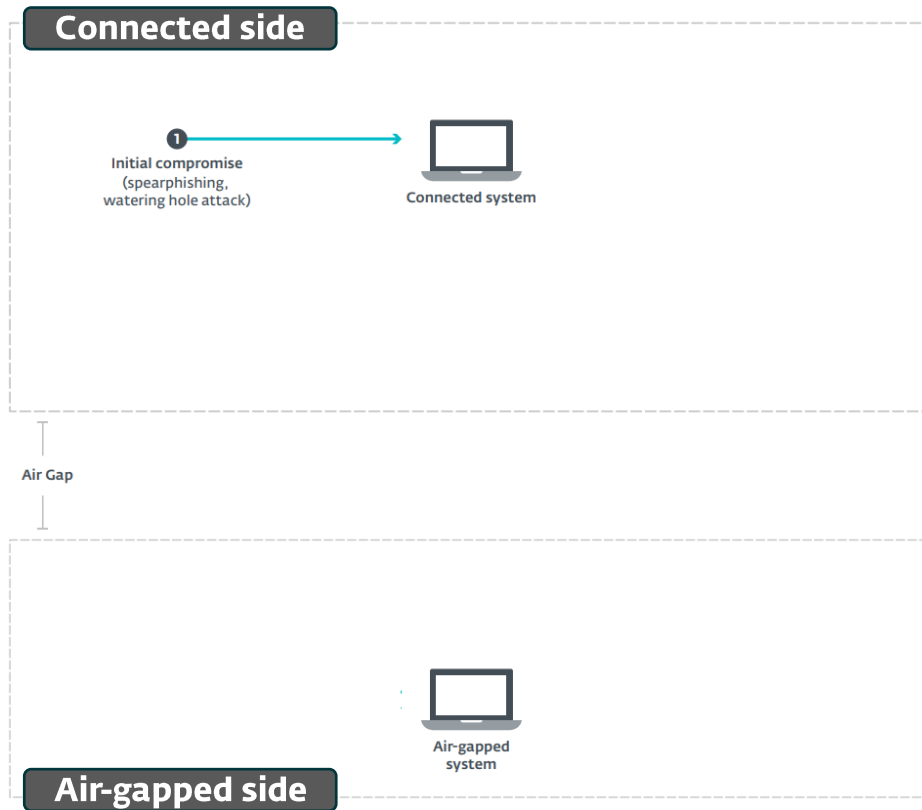
Emotional Simian

Brutal Kangaroo

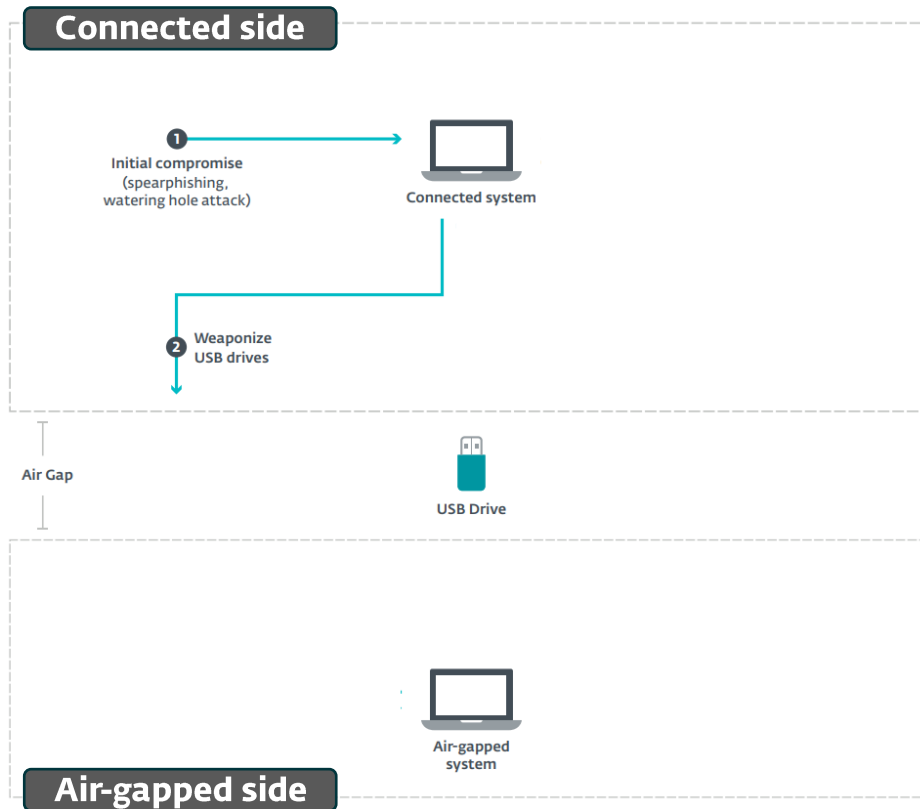
Connected frameworks



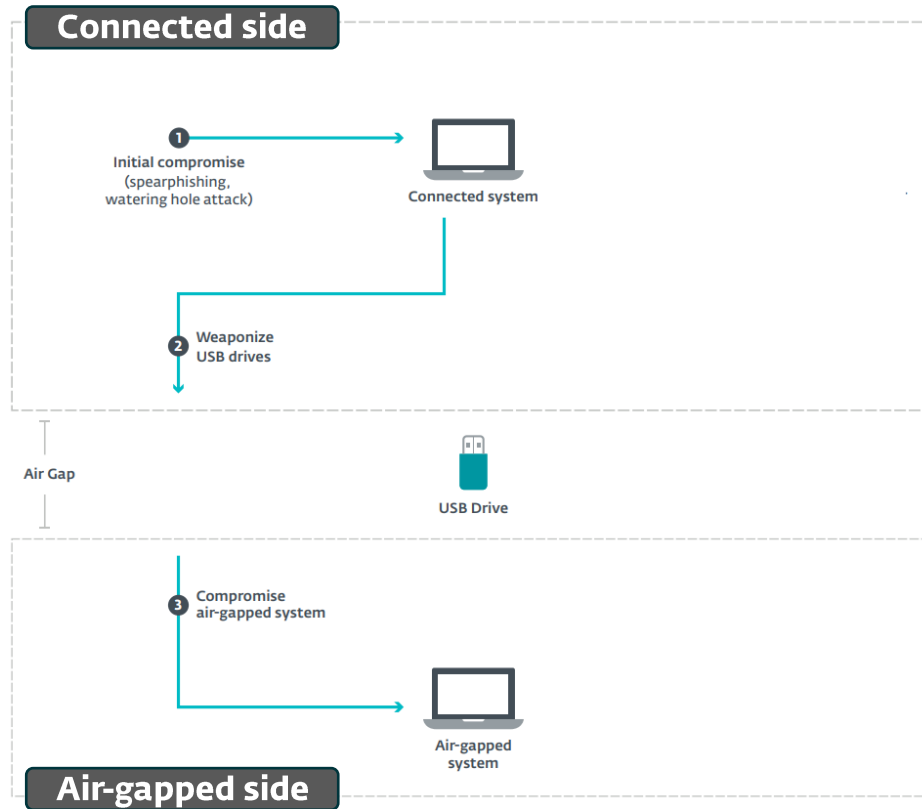
Connected frameworks



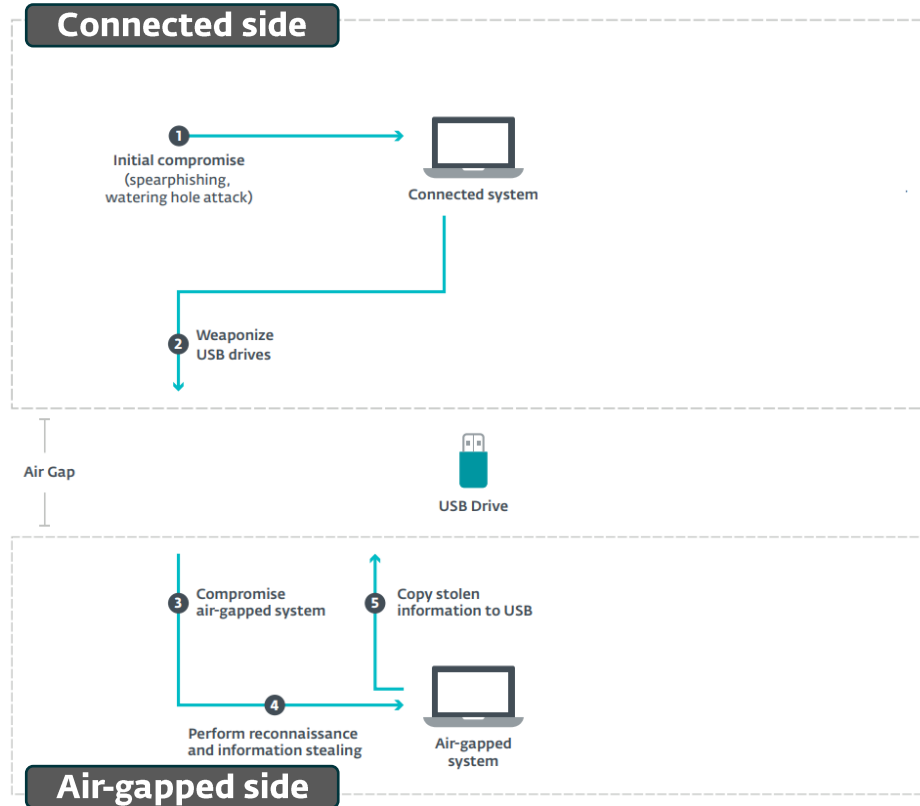
Connected frameworks



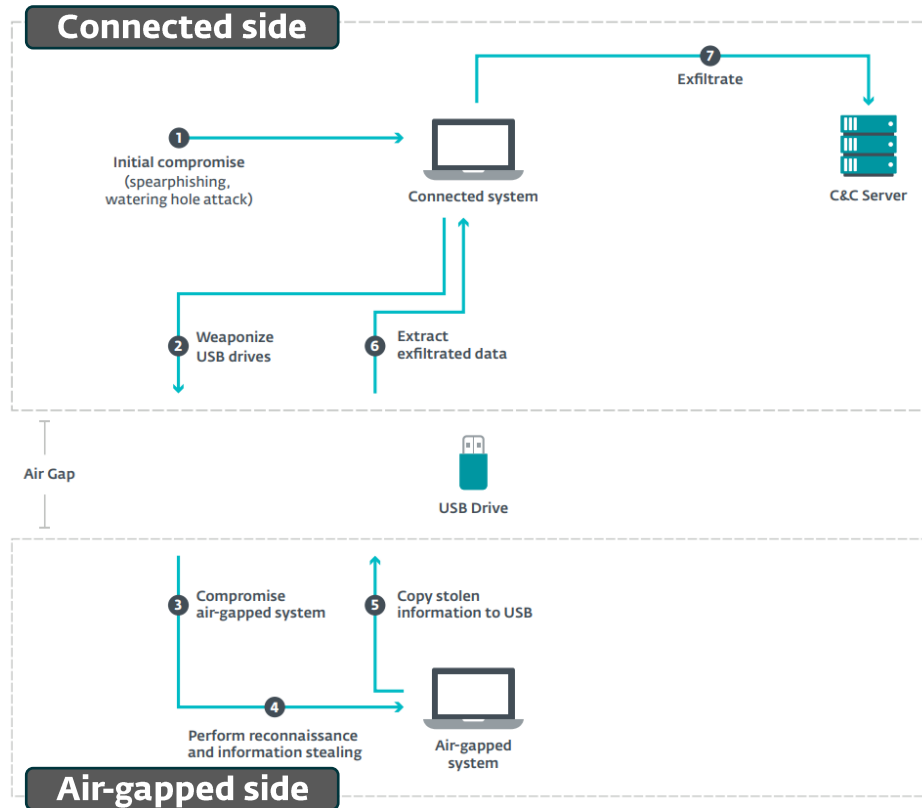
Connected frameworks



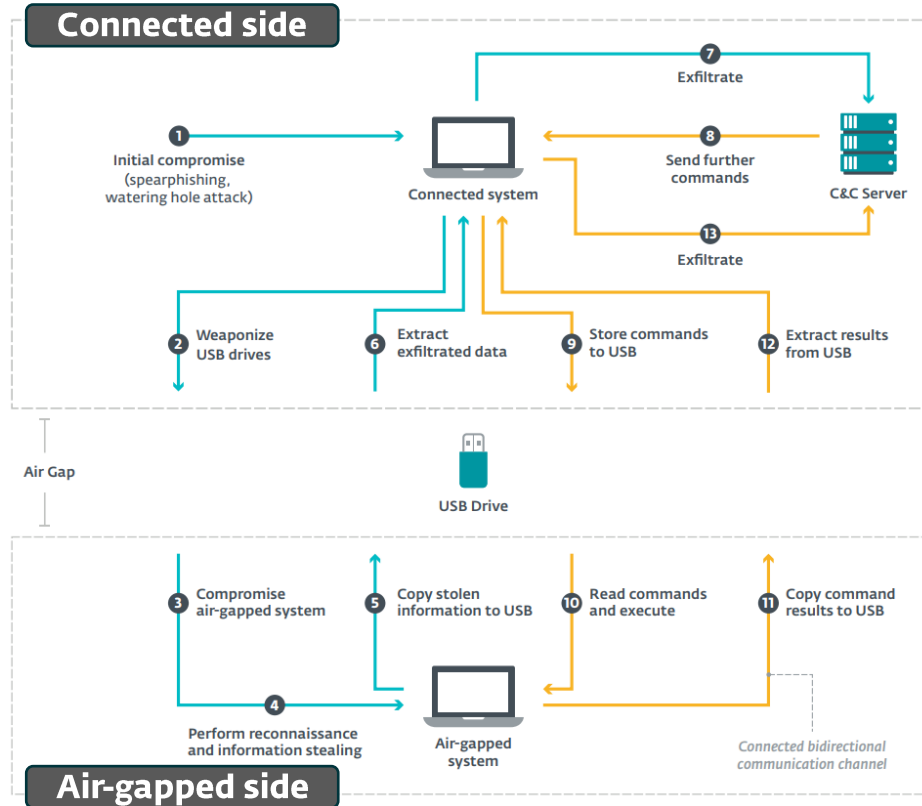
Connected frameworks



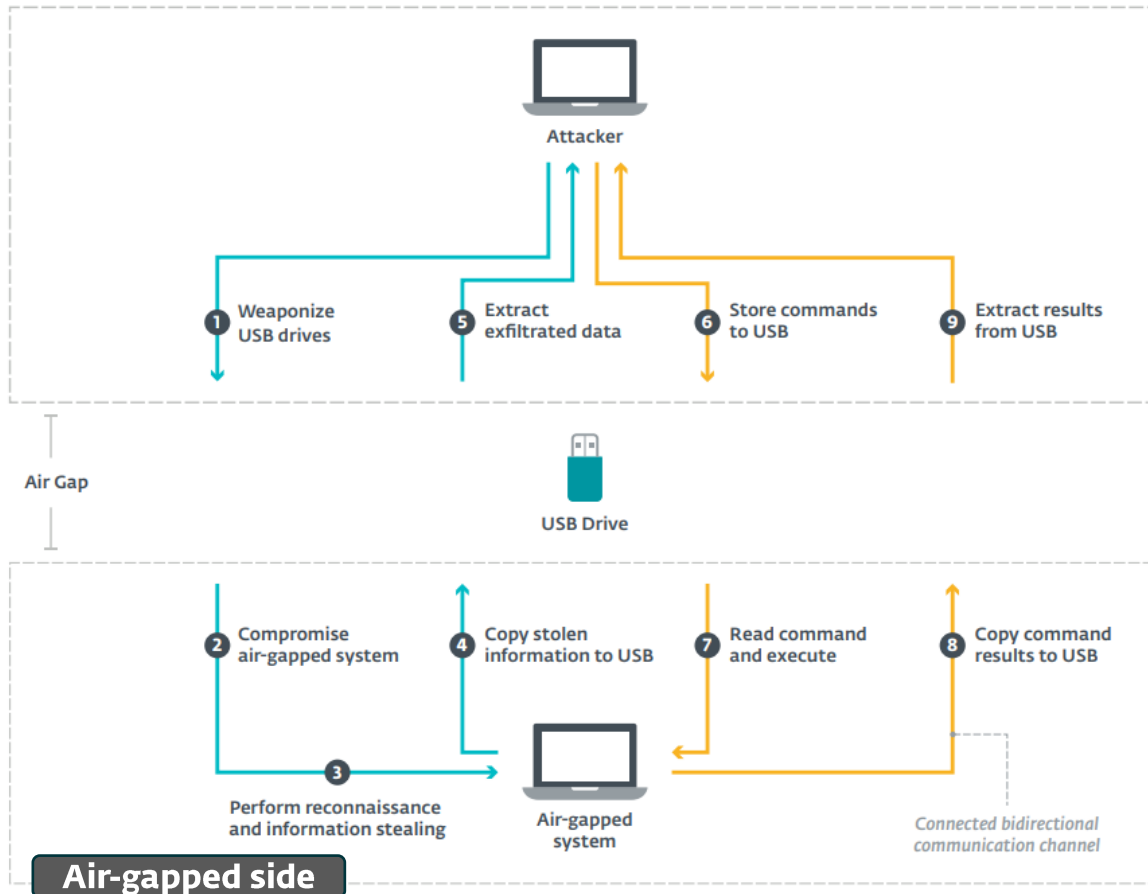
Connected frameworks



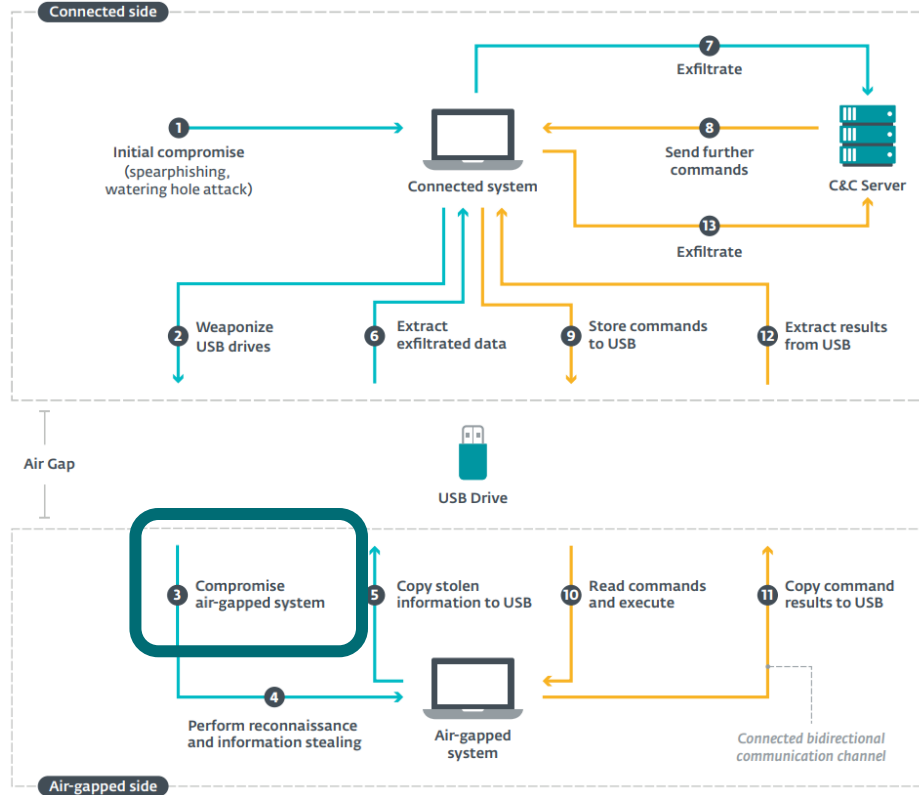
Connected frameworks



Offline frameworks



Air-gapped side: Initial execution vectors



Automated execution

Advisory date	CVE	Vulnerability name	Exploited in the wild
2010-08-02	CVE-2010-2568	Shortcut Icon Loading Vulnerability (remote code execution)	Fanny, Stuxnet, Flame, Gauss, miniFlame

Advisory date	CVE	Vulnerability name	Exploited in the wild
2010-08-02	CVE-2010-2568	Shortcut Icon Loading Vulnerability (remote code execution)	Fanny, Stuxnet, Flame, Gauss, miniFlame

2019-08-13	CVE-2019-1188	LNK Remote Code Execution Vulnerability	
2019-09-10	CVE-2019-1280	LNK Remote Code Execution Vulnerability	
2020-03-10	CVE-2020-0684	LNK Remote Code Execution Vulnerability	
2020-02-11	CVE-2020-0729	LNK Remote Code Execution Vulnerability	
2020-06-09	CVE-2020-1299	LNK Remote Code Execution Vulnerability	
2020-07-14	CVE-2020-1421	LNK Remote Code Execution Vulnerability	

Automated Execution

What's so Fanny?

This PrivLib-boosted Worm, which spreads using the Stuxnet LNK exploit and the filename "fanny.bmp" was compiled on Mon Jul 28 11:11:35 2008, if we are to trust the compilation timestamp. It arrived in our December 2008 collection from the wild, so the compilation might very well be correct.

```
000: 4C 00 00 00 01 14 02 00 00 00 00 00 00 00 00 00  L  @  Å
010: 00 00 00 46 81 00 00 00 00 00 00 00 00 00 00  F
020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
050: 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30  ▼PàOÐ ê:i>φ +0
060: 30 9D 14 00 2E 00 20 20 EC 21 EA 3A 69 10 A2 DD 0 . ilê:i>φY
070: 08 00 2B 30 30 9D 14 04 00 00 00 00 00 00 0E 00  +00
080: 00 00 69 3A 5C 66 61 6E 6E 79 2E 62 6D 70 00 00  i:\fanny.bmp
090: 4D 79 20 4E 61 6D 65 00 00 00 00 00 00 00 00 00  My Name
0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Source: Securelist - Kaspersky

Non-automated execution: Unknowingly triggered

Main techniques:

- Abuse of Windows AutoRun/AutoPlay feature, via malicious autorun.inf files
- Planting decoy files to lure potential victims
- Rig existing files with malicious code or exploits

Non-automated execution: Unknowingly triggered

Stuxnet's autorun.inf

```
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..
```

Source: Symantec

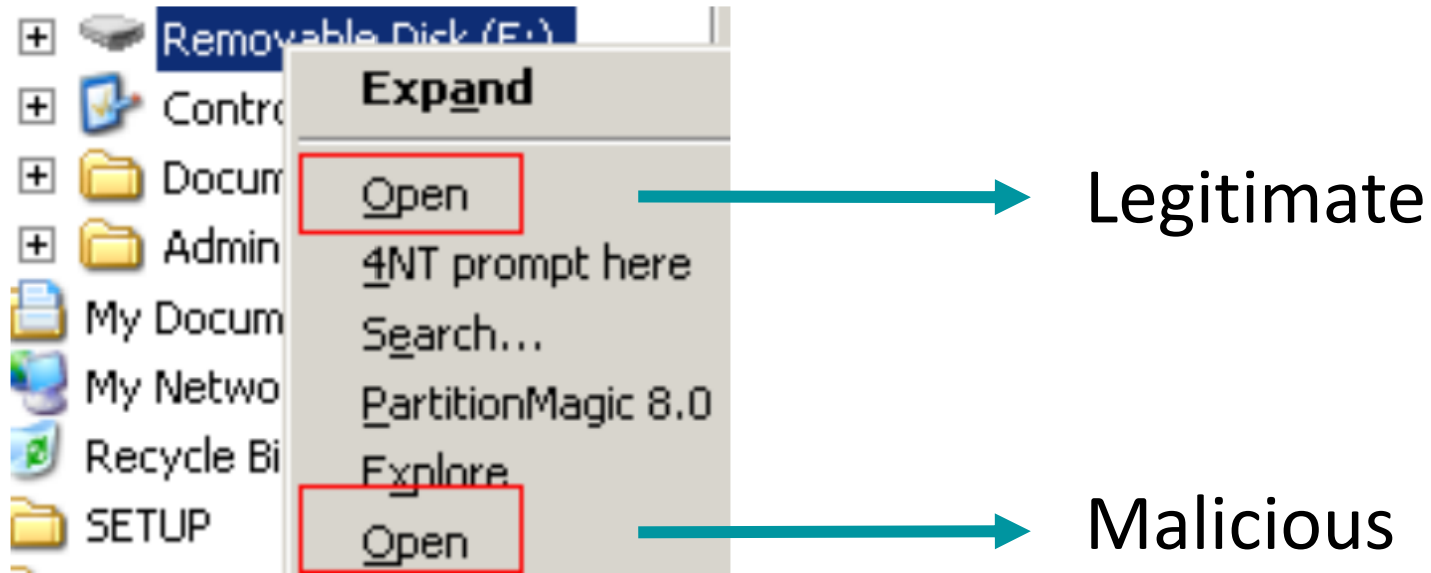
Non-automated execution: Unknowingly triggered

Stuxnet's autorun.inf instructions:

```
Hidden autorun commands
.?AVZdhrnpldcahnGvqzdhRnpldcahn@gfjjefwq@sr@@@
[autorun]
objectDescriptor={B315537-63AB-9512-99A9-2F4677235A44}
Menu\command=.\AUTORUN.INF
Menu=@%windir%\system32\shell32.dll,-8496
UseAutoPLAY=0
```

Source: Symantec

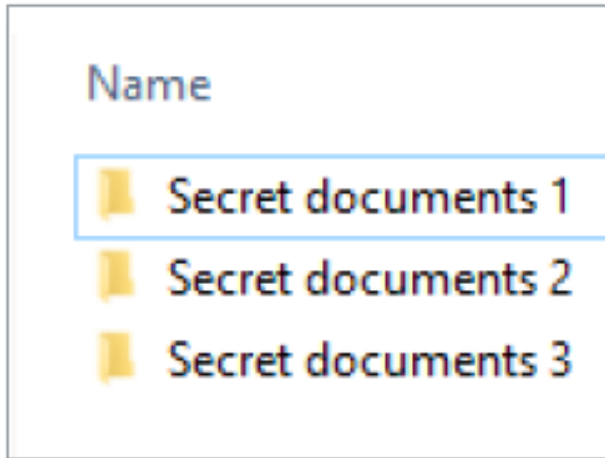
Non-automated execution: Unknowingly triggered



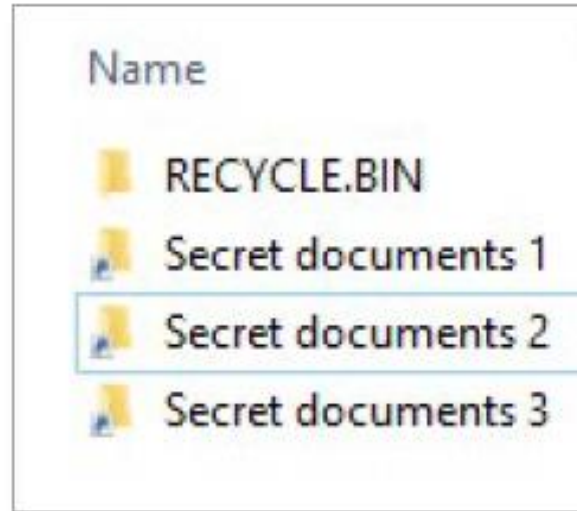
Source: Symantec

Non-automated execution: Unknowingly triggered

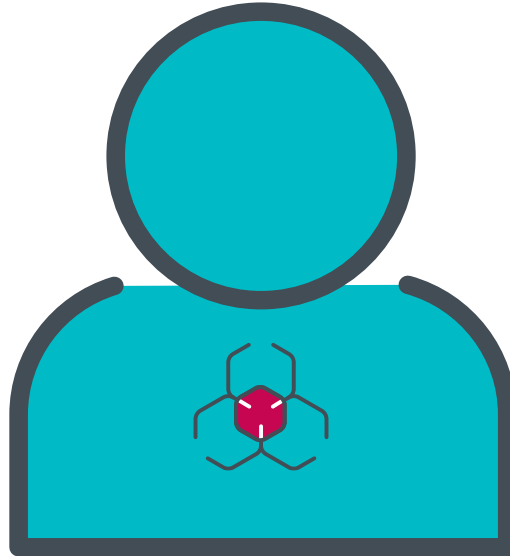
Clean



Weaponized



Non-automated execution: deliberately triggered



Non-automated execution: deliberately triggered

Cycldek: Bridging the (air) gap

APT REPORTS

03 JUN 2020

⌚ 16 minute read



Source: Securelist - Kaspersky

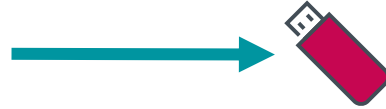
Non-automated execution: deliberately triggered

Connected side



RedCore victim

Infects it, if contains marker.



Air-gapped side

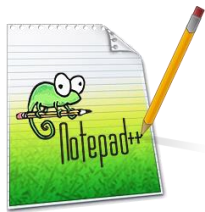


Executes the malware on the target.

Non-automated execution: deliberately triggered



Non-automated execution: deliberately triggered



NppPlugin.dll



HealthCheck.exe



RichEd20.dll

Communication Protocols and Exfiltration

A Fanny Equation: “I am your father, Stuxnet”

APT REPORTS

17 FEB 2015

🕒 12 minute read



Source: Securelist - Kaspersky

Communication Protocols and Exfiltration

FAT Specification. Directory structure:

Descriptive name of field	Offset (byte)	Size (bytes)	Description
DIR_Name	0	11	"Short" file name limited to 11 characters (8.3 format).
DIR_Attr	11	1	Legal file attribute types are as defined below: ATTR_READ_ONLY 0x01 ATTR_HIDDEN 0x02 ATTR_SYSTEM 0x04 ATTR_VOLUME_ID 0x08 ATTR_DIRECTORY 0x10 ATTR_ARCHIVE 0x20

Communication Protocols and Exfiltration

Invalid directory entry

```
51 50 40 98 2D B4 CE 06 00 00 00 18 00 9C 1E 00 | QP@|- 'to ...o .| .  
02 00 02 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

Hidden storage space



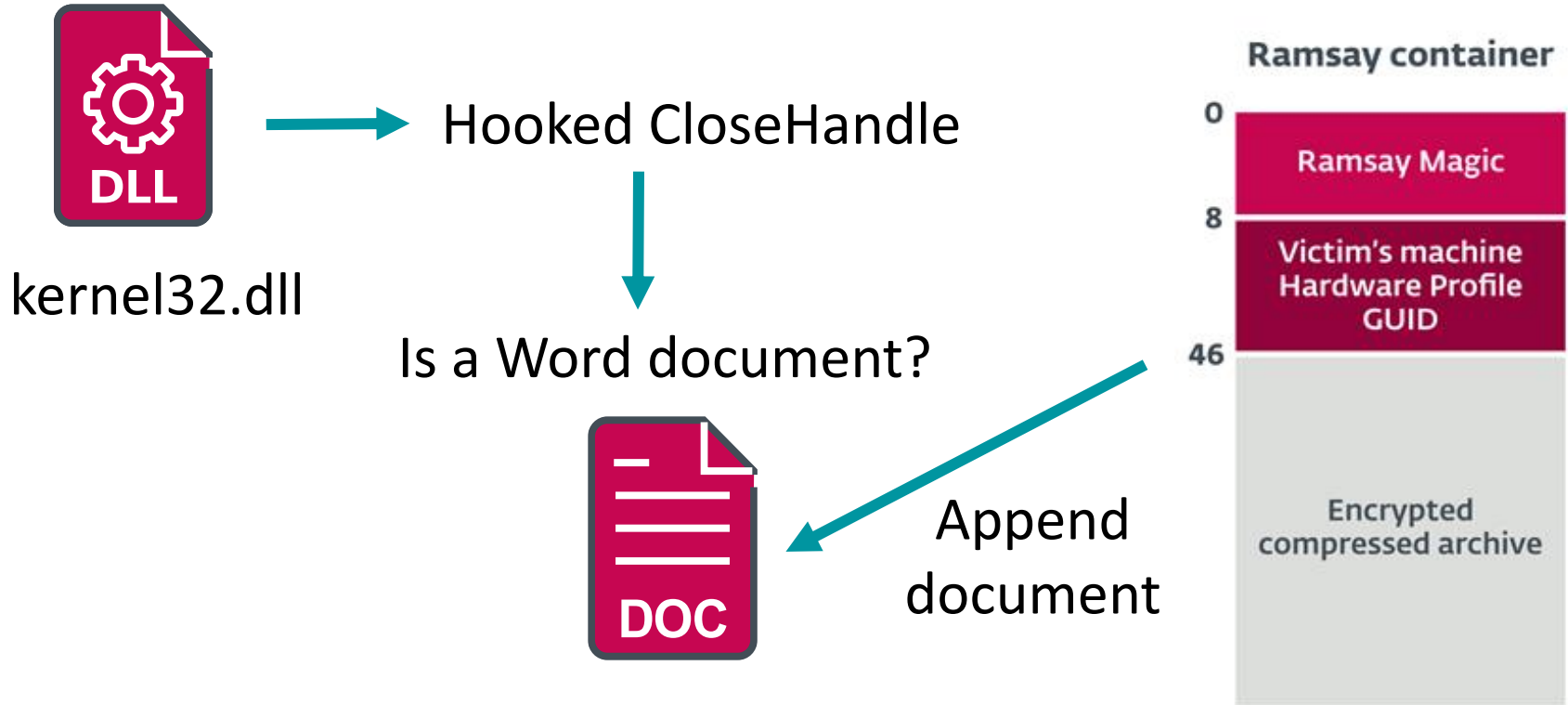
Modules Commands Stolen data

Communication Protocols and Exfiltration

welivesecurity™ BY eset®

Ramsay: A cyber-espionage toolkit tailored for air-gapped networks

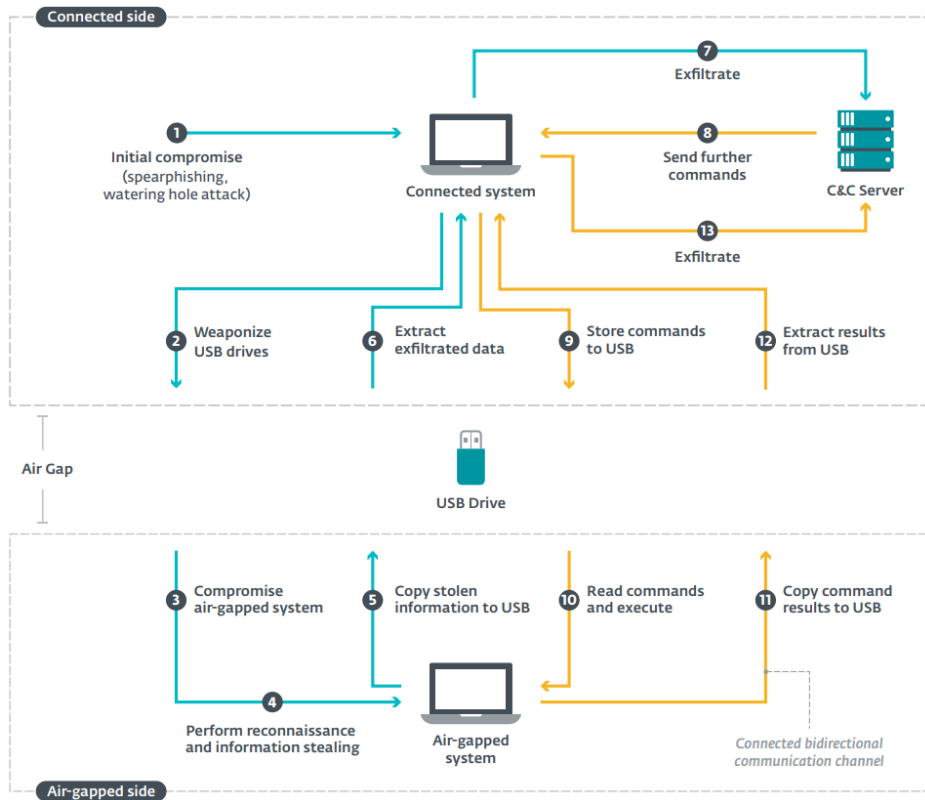
Communication Protocols and Exfiltration



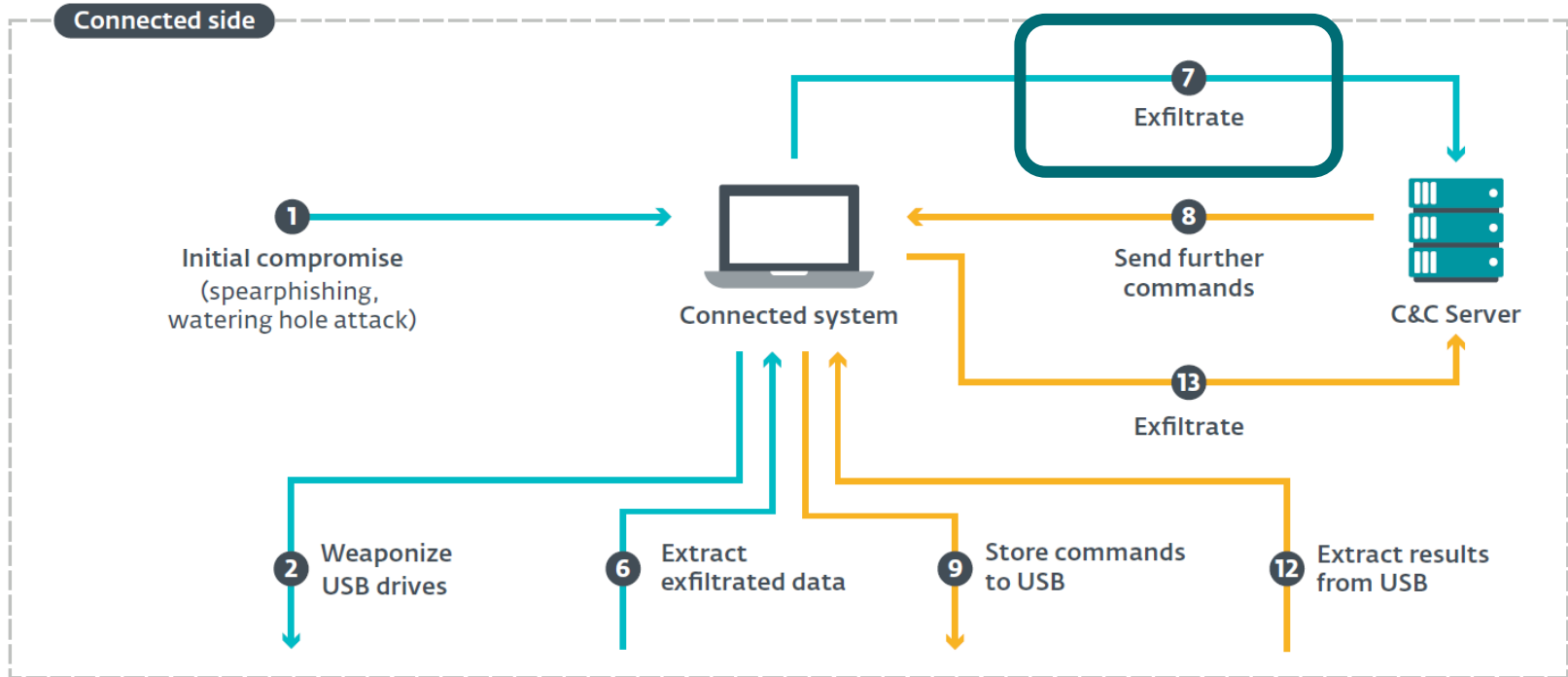
How to defend



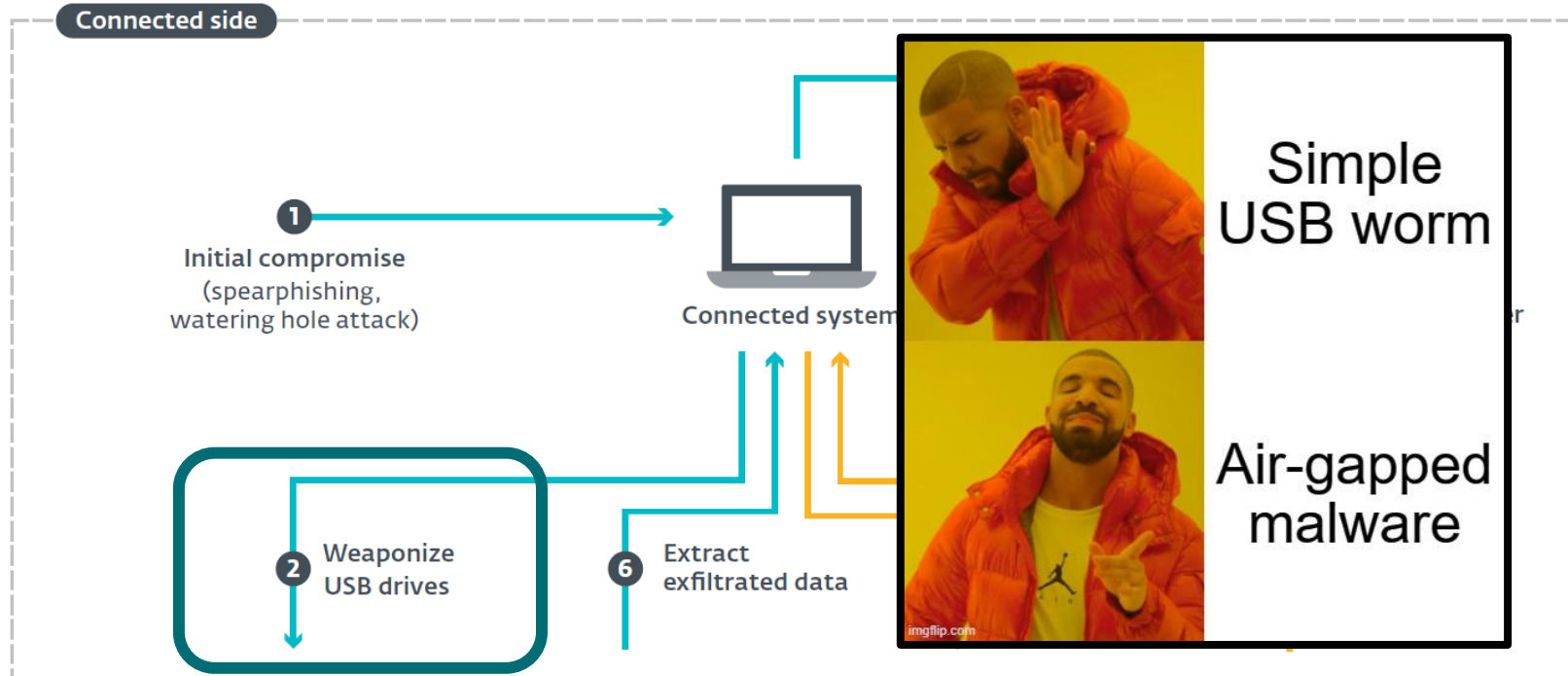
Identifying air-gapped malware



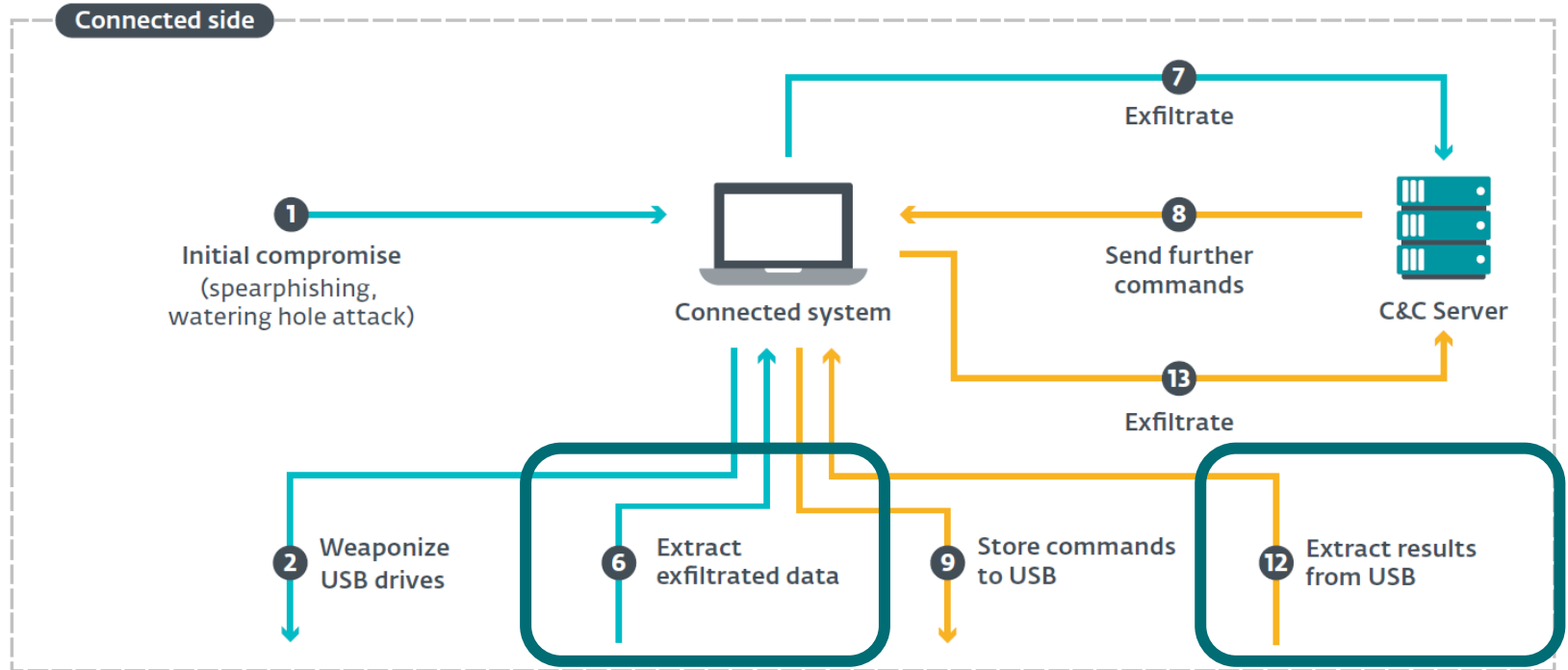
Identifying the connected-side component



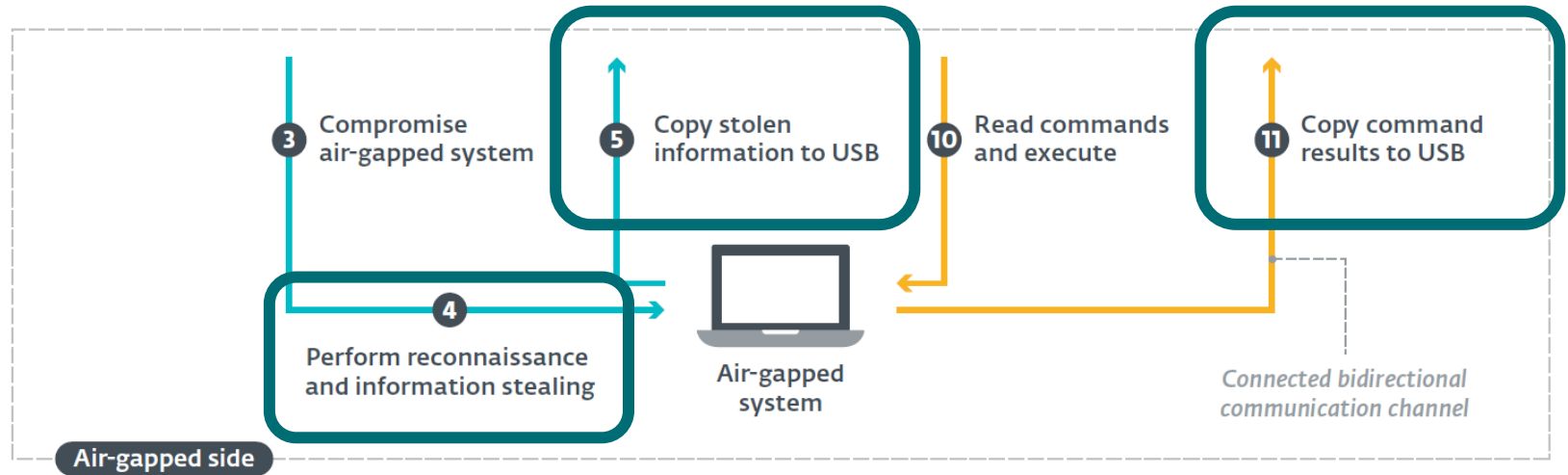
Identifying the connected-side component



Identifying the connected-side component



Identifying the air-gapped side component



Challenges



Ramsay

Todo

- prepare YARAs for VTI
 - all known components
 - try to find the missing component that can communicate with Ramsay over the file-based protocol
 - update YARA with last sample and run a retrohunt



Alexis Dorais-Joncas

Senior Manager, Malware Research

dorais@eset.com

[@adorais](https://twitter.com/adorais)



Facundo Muñoz

Malware Researcher

facundo.munoz@eset.com

[@0xfrmz](https://twitter.com/0xfrmz)