IS ANTIVIRUS AN EFFICIENT TOOL FOR INDUSTRIAL NETWORK PROTECTION?

Marcelo Branquinho & Jan Seidl

CEBIT - March of 2013

TI Safe Segurança da Informação

Presentation

Marcelo Branquinho
(marcelo.branquinho@tisafe.com)

- CEO on TI Safe. Senior member of ISA and committee member of ANSI/ISA-99. Researcher in security technologies to protect critical infrastructure.

Jan Seidl
(jan.seidl@tisafe.com)

- Technical Coordinator on TI Safe. Expert in risks analysis in automation systems and researcher in the field of Malware engineering.

Follow TI Safe:

- Twitter: @tisafe
- SlideShare: www.slideshare.net/tisafe
- Facebook: www.facebook.com/tisafe
- Flickr: http://www.flickr.com/photos/tisafe

TI Safe
Segurança da Informação

You don’t have to copy...

TI Safe
Segurança da Informação

Agenda

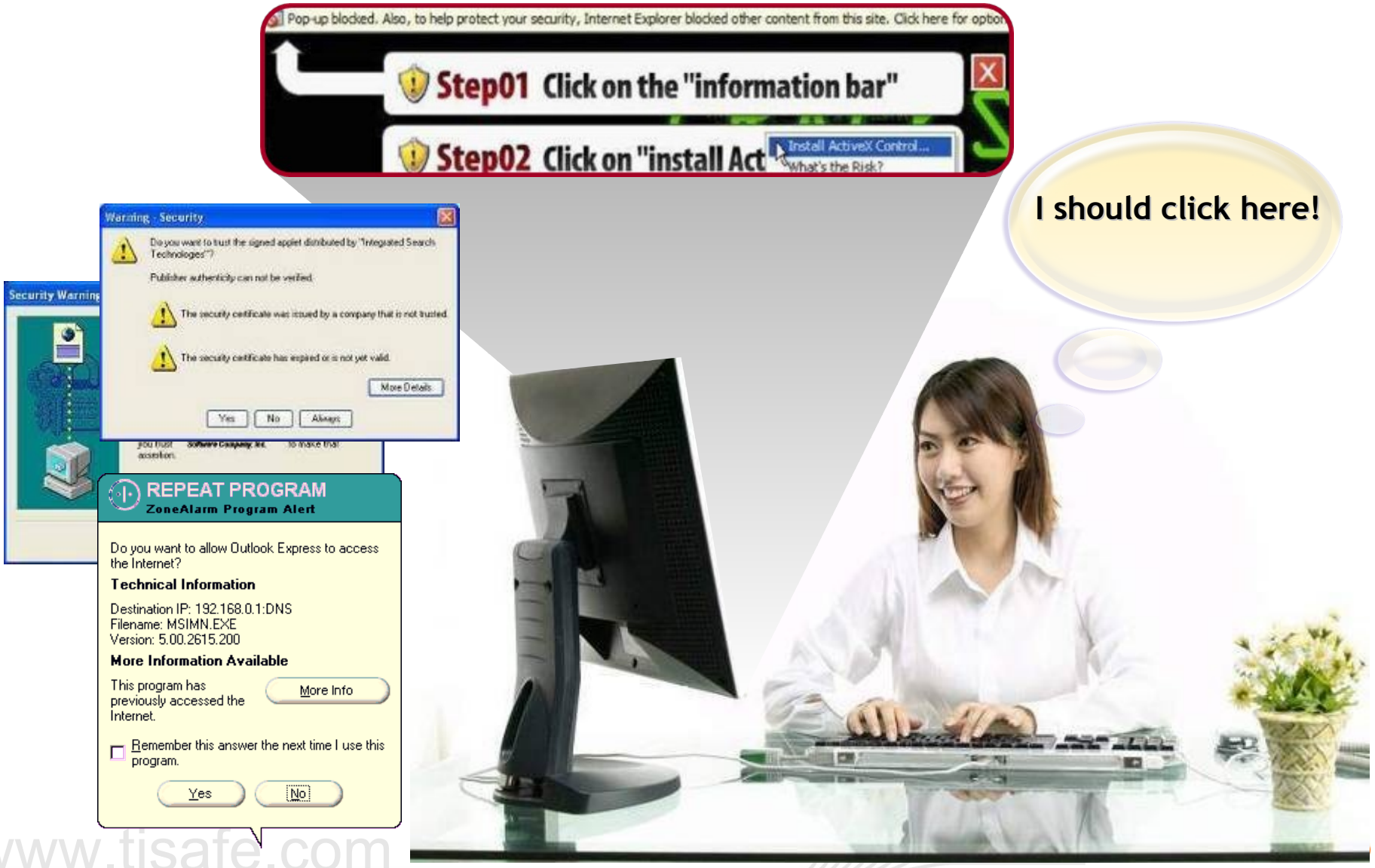
- Malware in automation networks
- The is no silver-bullet/turnkey solution
- Signature-based detection is almost useless
- Bonus: Free tools can also bypass AV
- IDPS and Whitelisting
- The defense in depth and segmentation
- Training and awareness: Educating users
- Containing an outbreak: Finding “Patient Zero” and regaining control through “Divide and Conquer”

Malware in Automation networks

Vectors of infection

- Exploits
- Removable media (Pen Drives, External HD)
- Shared Network
- External networks (connections with other companies' networks)
- 3G networks
- VPNs
- Dissatisfied employees
- Lack of user’s expertise (click on links and attachments ...)

“Happy clicker” user



Vectors of spreading

- Exploits
- Removable media (Pen Drives, External HD)
- Shared Network
- External networks (connections with other companies' networks)
- 3G networks
- VPNs

Impact

- Unavailability of engineering and supervisory workstations
- Unavailability of control servers
- Unavailability of PLCs
- Disruption of control network
- Loss of data
- Intelectual property theft
- Physical damage?

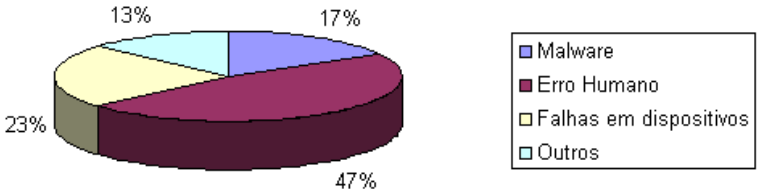
Impact

Incidents in Brazil

In most cases of contaminations observed in our customers, *there were an antivirus solution installed on the infected hosts*...

Incidents	# Cases
Malware	5
Human error	14
Device failure	7
Others	4

Incidents in Brazil



… that wasn't able to detect and prevent the spread of infection throughout the network.

Picture: Documented industrial incidents in Brazil (Source: *TI Safe Knowledge Base*)

There is no silver-bullet / turn-key solution :(

and there'll 'never' be.

Why ?

Security is a concept not a monolithic solution

Many solutions working together build up security

Don't trust “Megazord” solutions. (UTMs, applications that work in multiple areas, etc.)

Why ?

You need the best solution for each area. Each vendor has expertise in its own area and probably won't master all of them at the same time.

Security is not only on your hosts but also networks and personnel

Signature-based detection is almost useless

Why ?

Signatures are based in known patterns in files

What about unknown threats?

Polymorphism isn't something new

A wide variety of malware has its *source code available*, you can change-it, recompile-it and... VOILÁ!

Why ?

Hackers don't follow patterns

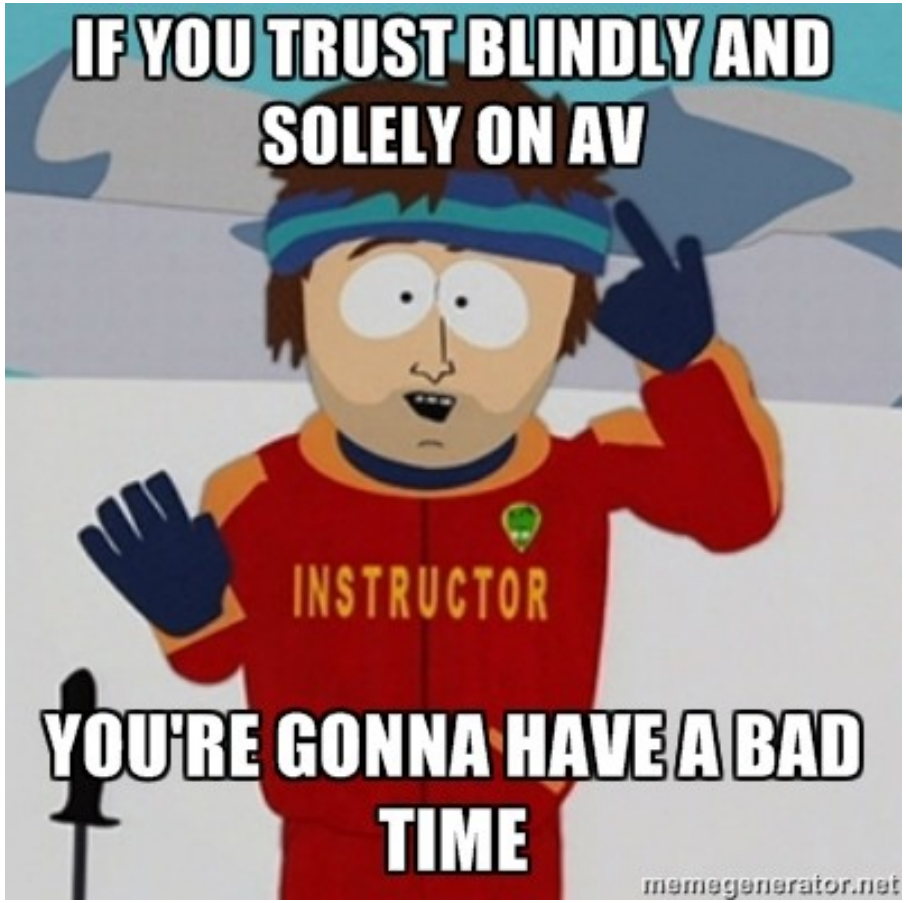
Why ?

We tested some *free* hacking tools against *popular vendors*...

Why ?

... and we got some **interesting results**.

Why ?



Tested Antivirus Solutions

- McAfee Antivirus Plus 2012
- Kaspersky Antivirus 2012
- Panda Antivirus Pro 2012
- Trend Titanium
- Norton Antivirus 2012
- F-Secure Antivirus 2012
- avast! Pro Antivirus 6
- AVG Anti-Virus FREE 2012
- Sophos Anti-Virus 7
- Microsoft Security
- Antivirus 5

All antivirus software tested (except for the free ones) were obtained from the websites of the manufacturers in their 32-bit evaluation and in English. All were installed on the 'Recommended‘ setting.

Results Matrix

		Soluções de Antivirus Testadas										
	Ataques Executados	McAfee Antivirus Plus 2012	Kaspersky Antivirus 2012	Panda Antivirus Pro 2012	Trend Titanium Maximum Security	Norton Antivirus 2012	F-Secure Antivirus 2012	avast! Pro Antivirus 6	AVG Anti-Virus FREE 2012	Sophos Anti-Virus 7	Microsoft Security Essentials	E-SET NOD32 Antivirus 5
1	EICAR	EICAR test file	EICAR-Test-File	EICAR-AV-TEST-FILE	Eicar_test_file	EICAR Test String	Trojan.Generic.6567028	EICAR Test-NOT virus!!!	EICAR_Test	EICAR-AV-Test	DOS/EICAR_Test_File	Eicar test file
2	Metasploit EXE Default Template (no encryption)	Swrort.f	Trojan.Win32.Generic	Suspicious File	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch	Win32/Heur	Mal/EncPk-ACE	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AA trojan
3	Metasploit EXE Default Template (shikata_ga_nai)	Swrort.d	Trojan.Win32.Generic	Suspicious File	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch	Win32/Heur	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
4	Metasploit EXE Notepad Template (no encryption)	Swrort.f	Trojan.Win32.Generic	Trj/Genetic.gen			Backdoor.Shell.AC	Win32:SwPatch		Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AA trojan
5	Metasploit EXE Notepad Template (shikata_ga_nai)	Swrort.d	Trojan.Win32.Generic	Trj/Genetic.gen			Backdoor.Shell.AC	Win32:SwPatch	Win32/Heur	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
6	Metasploit EXE SkypePortable Template (shikata_ga_nai)	Swrort.d	Trojan.Win32.Generic				Backdoor.Shell.AC	Win32:SwPatch		Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
7	Metasploit LOOP-VBS Default Template (no encryption)	Swrort.f	Trojan.Win32.Generic	Script Blocked	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch		Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AA trojan
8	Metasploit LOOP-VBS Default Template (shikata_ga_nai)	Swrort.f	Trojan.Win32.Generic	Script Blocked	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch		Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
9	Shellcodexec Default w/ VBS launcher	Generic.tfr!i	Trojan.Win32.Genome.vrrg	Trj/CI.A		Trojan.Gen	Trojan.Generic.6567028	Win32:Malware-gen	Trojan Generic22.KPM	Mal/Generic.L		Win32/ShellcodeRunner.A trojan
10	TI Safe Modded Shellcodeexec (w/ VBS launcher)			Script Blocked								
11	TI Safe Modded Shellcodeexec (Custom EXE w/ embedded payload)						Backdoor.Shell.AC		Trojan Generic22.SND		Trojan.Win32/Swrort.A	
12	TI Safe Custom Payload Launcher									Mal/FakeAV-FS		
13	Metasploit PDF (adobe_utilprintf)	Exploit.PDF.bk.gen	Exploit.JS.Pdfka.cil		HEUR_PDFEXP.B	Bloodhound.Exploit.213	Exploit.PDF-JS.Gen	JS:Pdfka-gen	Script/Exploit	Troj/PDFJs-B	Trojan.Win32/Swrort.A	JS/Exploit.Pdfka.NOO trojan
14	Metasploit PDF (adobe_pdf_embedded_exe)	Swrort.f	Trojan.Win32.Generic	Suspicious File	TROJ_SWRORT.SME	Bloodhound.PDF.24	Exploit.PDF-Dropper.Gen	Win32:SwPatch	Exploit.PDF	Mal/Swrort-C	Trojan.Win32/Swrort.A	PDF/Exploit.Pidief.PFW trojan
15	Metasploit PDF (adobe_pdf_embedded_exe_nojs)	Swrort.f	Trojan.Win32.Generic	Suspicious File	TROJ_PIDIEF.SMEO	Bloodhound.PDF.24	Exploit.PDF-Dropper.Gen	PDF:Launchr-C	Exploit	Mal/Swrort-C	Trojan.Win32/Swrort.A	PDF/Exploit.Pidief.PFT trojan
16	Metasploit Java Applet											

FILLED RED BLOCKS = OWNED!

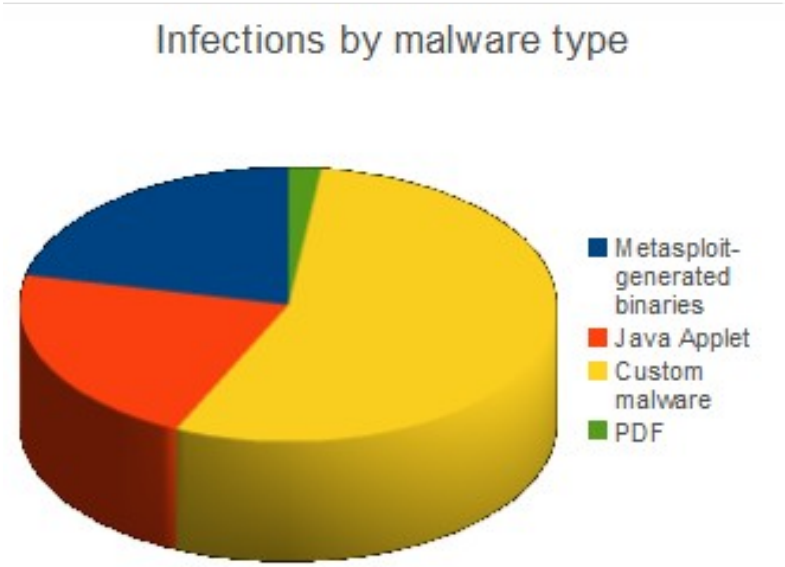
AV's can't stop targeted attacks and custom malware.

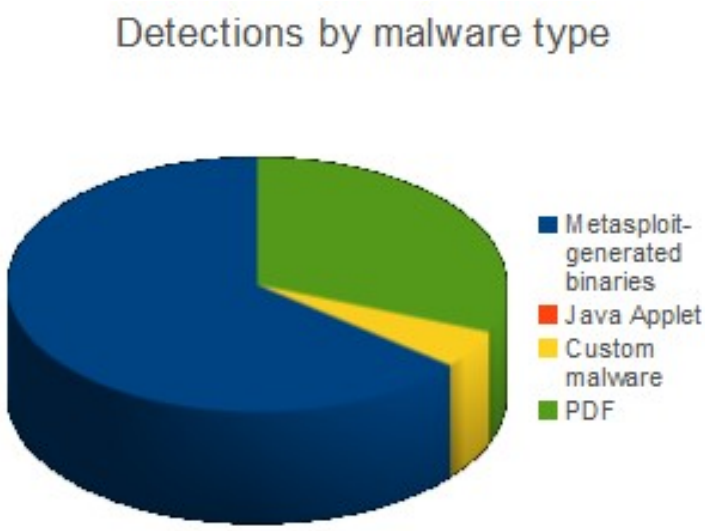
Java-based malware is even tougher to detect

Most of the antivirus solutions was unable to detect the threat in memory.

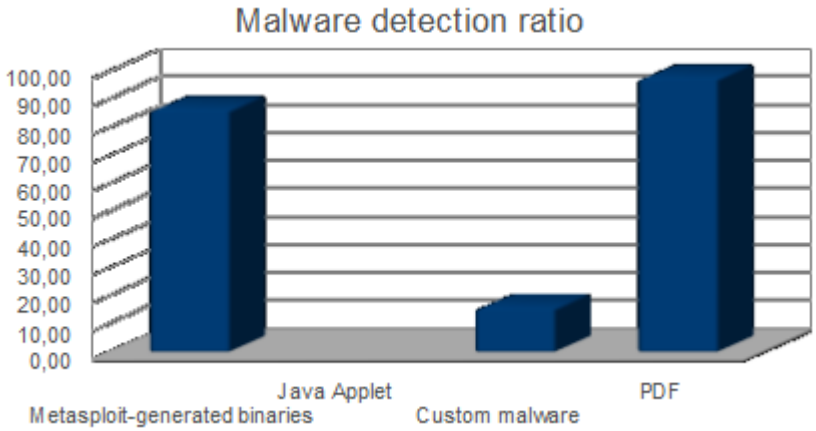
AV´s were developed for home and corporate users, not for automation plants.

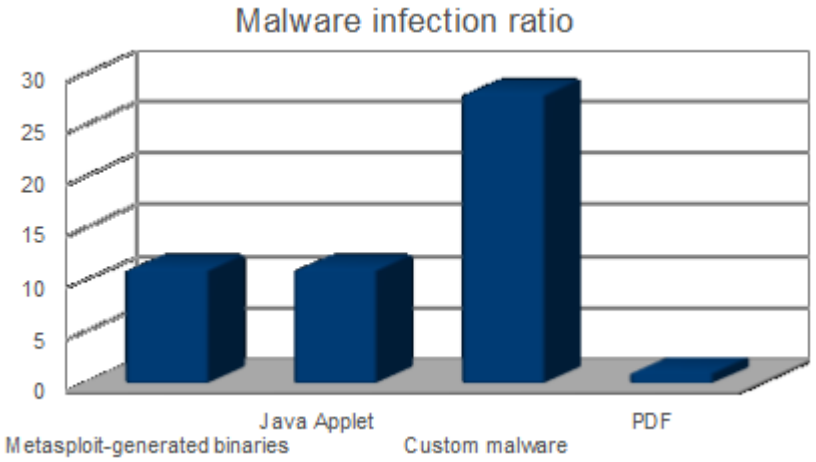
Infections and detections by malware type





Detection and infection ratios





Tested solutions ranking

#	Produto	Score
1	F-Secure 2012	13
	Sophos 7	
2	McAfee Plus 2012	12
	Kaspersky 2012	
	Avast! Pro 6	
	Microsoft Security Essentials	
	E-SET NOD32 5	
3	Panda Pro 2012	11
4	Norton 2012	9
	AVG FREE 2012	
5	Trend Titanium Maximum Security	8

Detect behaviours, not patterns

Use up-to-date network-based and host-based IDPS a lot

Yes, they also use pattern-based signatures but most of them also have behavior detection schemes

Some anti-virus products are shipped with a HIDPS to work together.

Whitelisting is better than Blacklisting

Whitelist	Greylist	Blacklist
yahoo.com	*.info	all-fioricet.com
google.com	*.biz	teen-hentai.us
msn.com	blogspot.com	weighlessrx.com

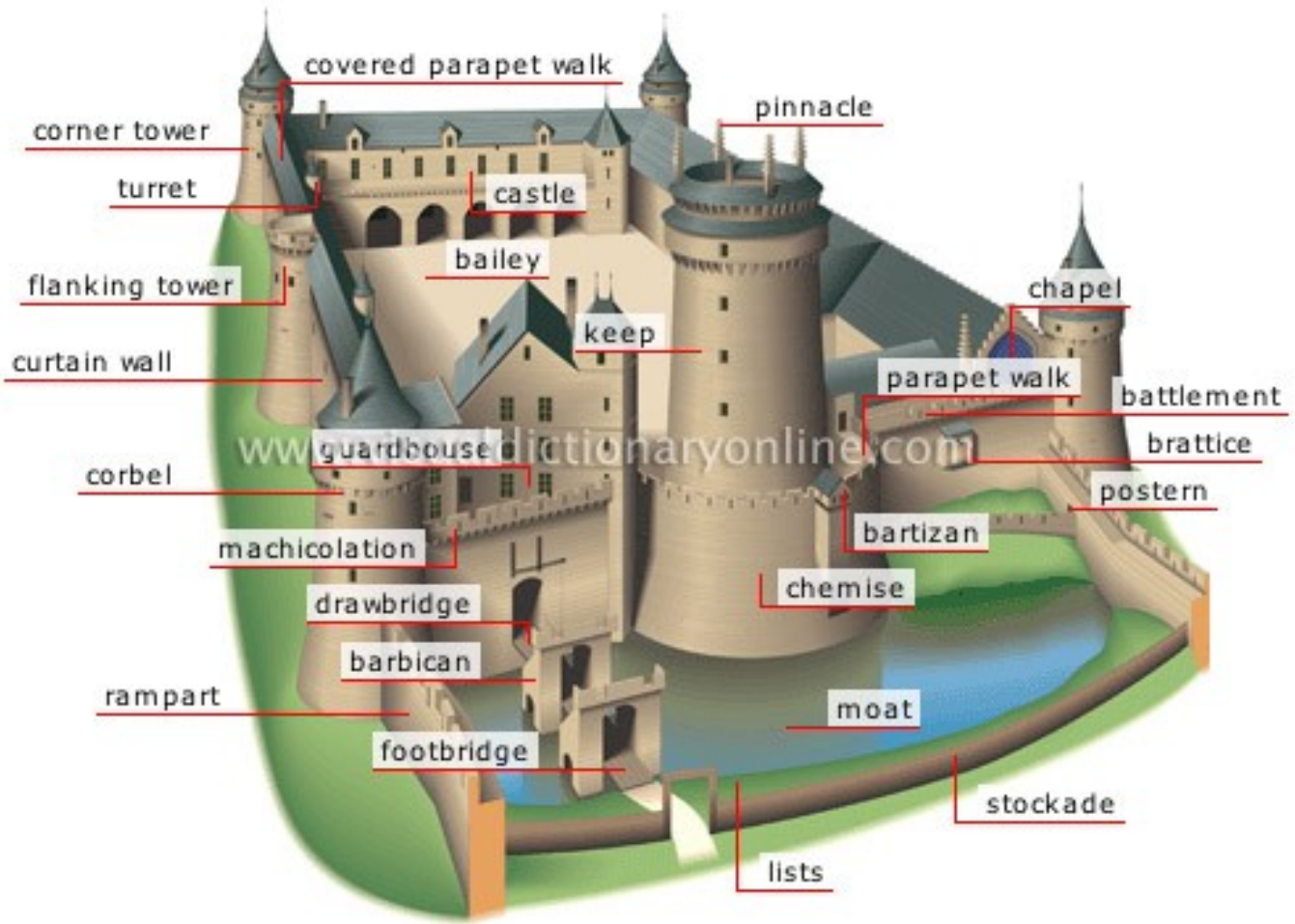
Photo credit: Codinghorror

Whitelisting is better than Blacklisting

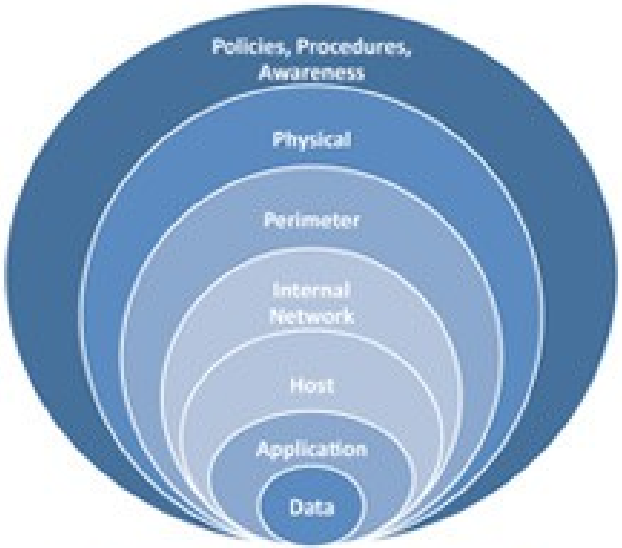
Because you **can't** relate ALL malicious URLs and/or keywords.

Stop your internal dialog!
You CAN'T! Get over it :)

The defense in depth



The defense in depth



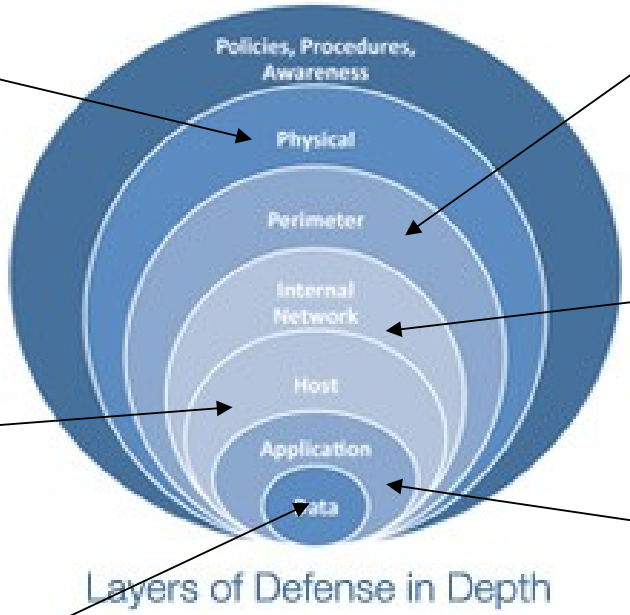
Layers of Defense in Depth

Photo credit: Sentrillion

The defense in depth

Locks, cameras etc

Firewalls, IDPS, Data diodes



Layers of Defense in Depth

Photo credit: Sentrillion

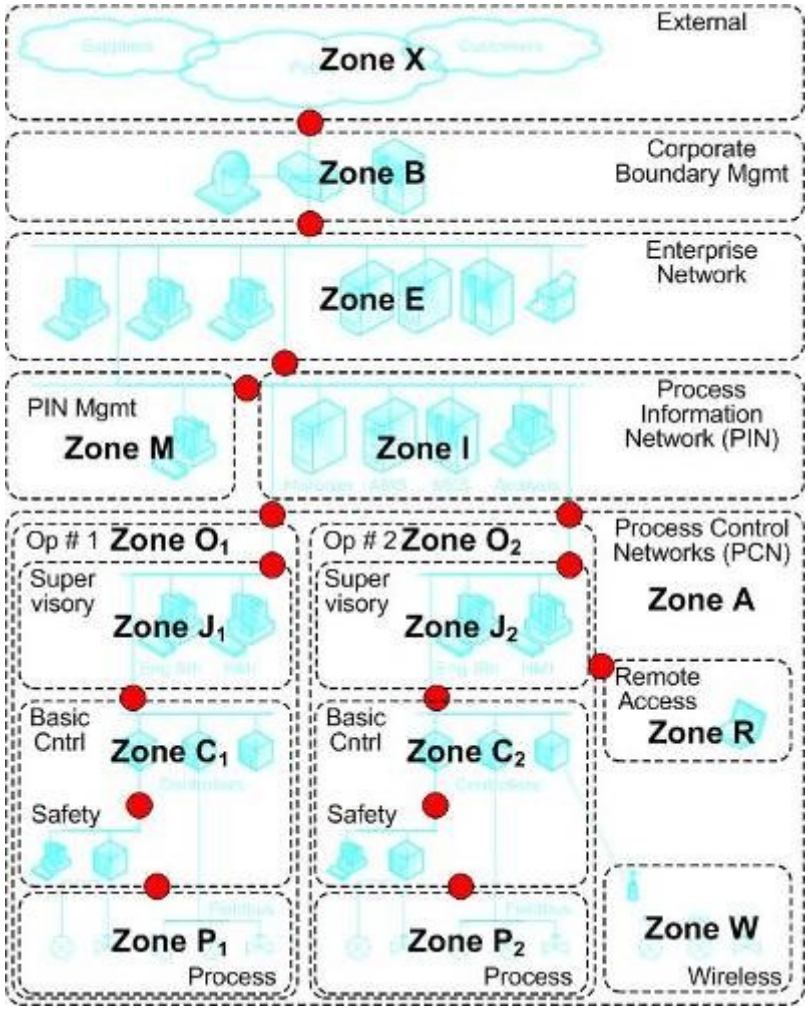
Segmentation, VLANs, port-mirrored IDS

Whitelisting software, HIDPS, central logging

WAFs, strong architechture

Encryption and access control

Network Segmentation



The zones and conduits model as proposed by ANSI ISA-99

Educating Users

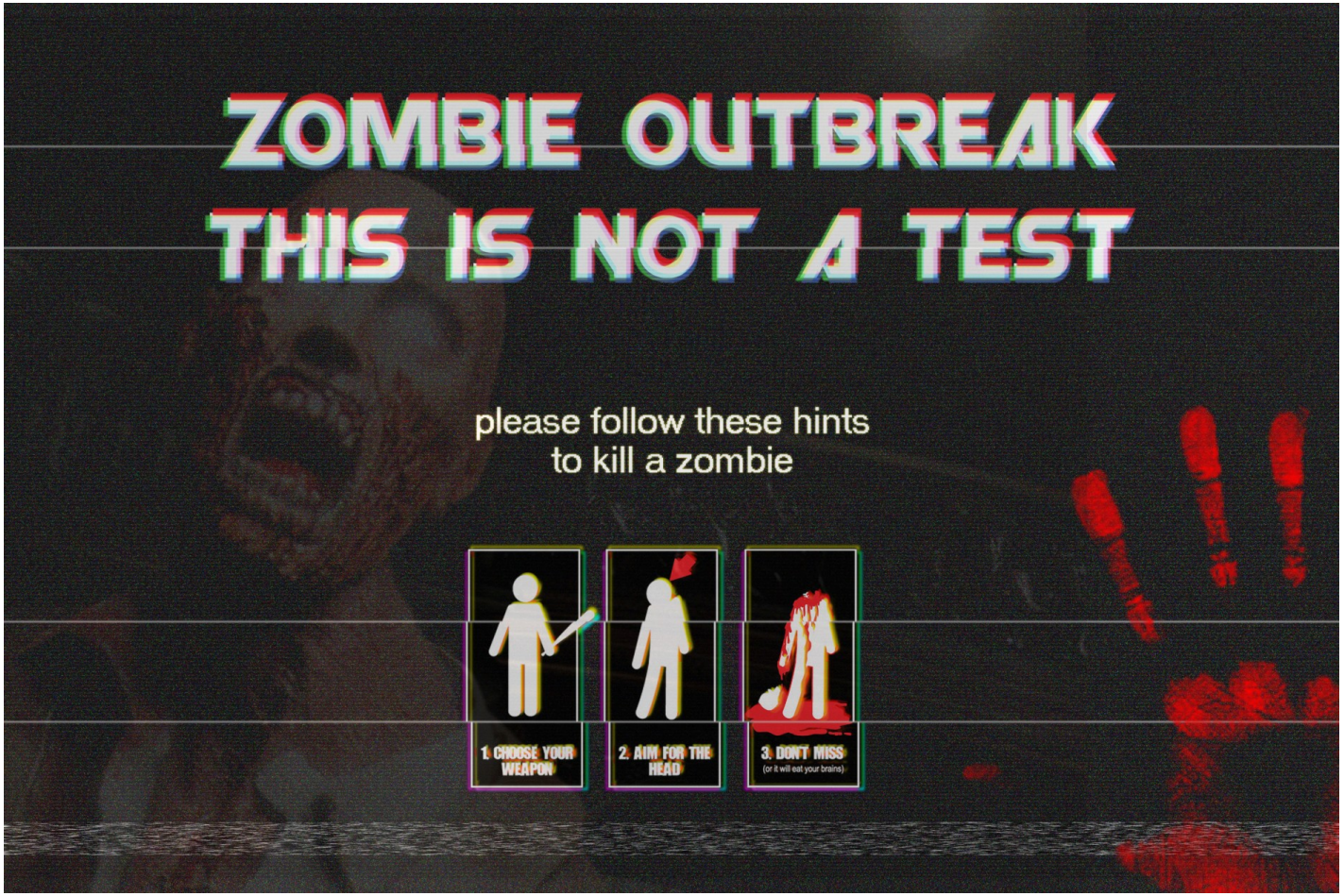
Promote workshops and “security day” to promote **awareness**

Your users don't really know the impact of using a 3G modem to check their personal email or Facebook wall

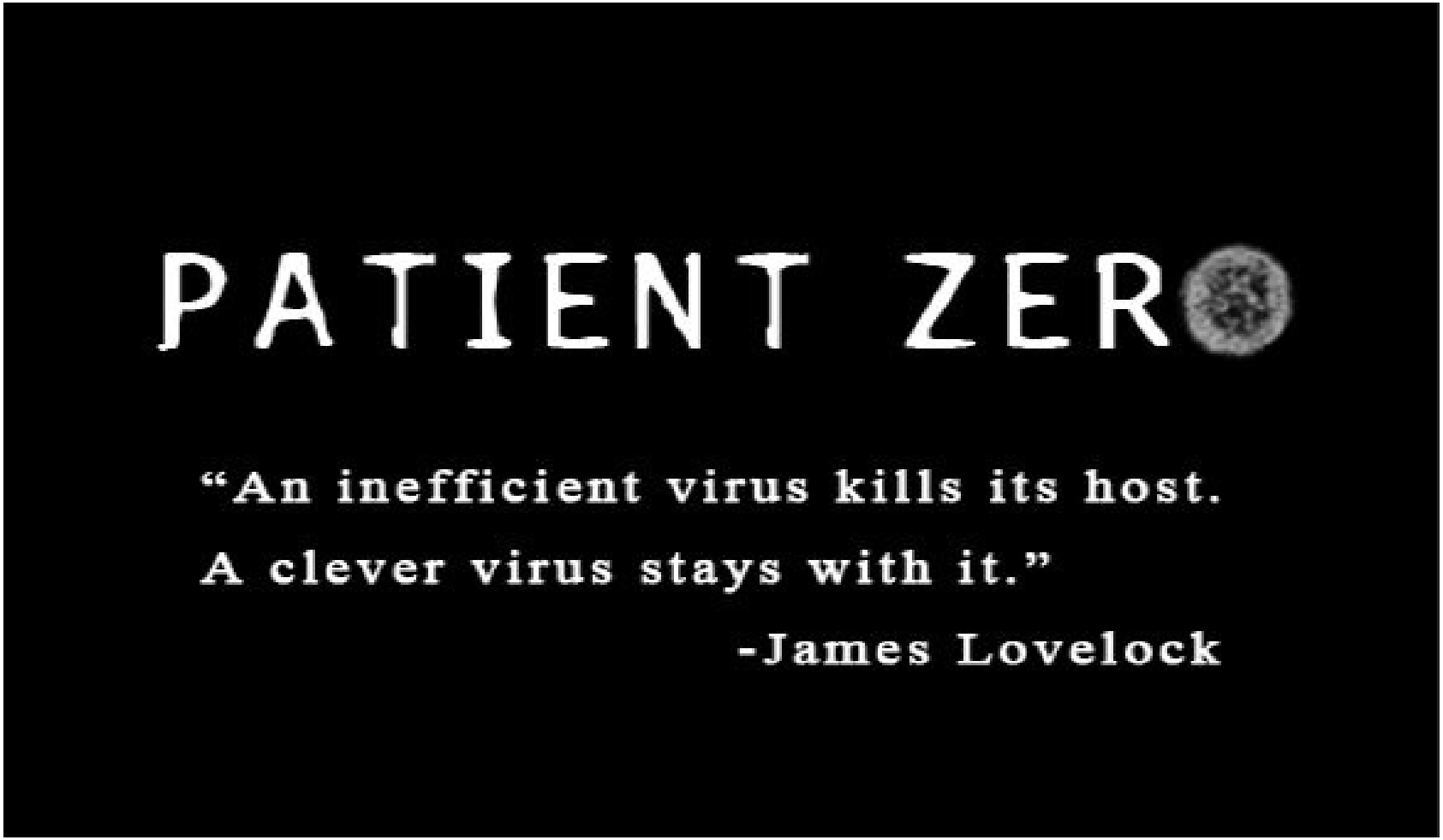
Even less that they can ruin plant's processes by clicking on a link sent by that hot girl he's chatting for weeks

Never forget what your users means to your security

Containing an outbreak



Finding patient zero



Finding patient zero

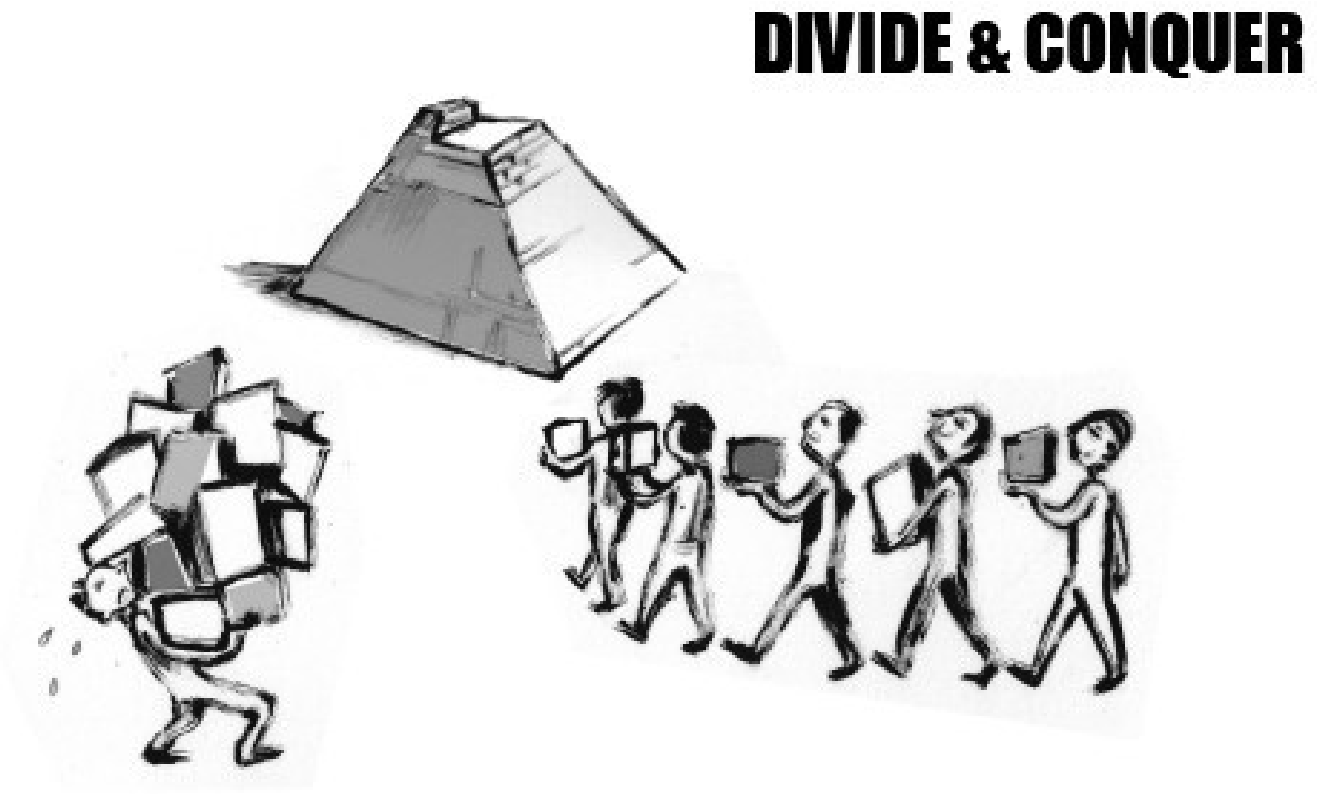
You better have monitoring!

Find hosts that are communicating on ports and hosts that it shouldn't, performing unusual network noise etc

Perform forensic analysis on suspected hosts to confirm infection date

Find the first infection point. Try to determinate how it happened. Close the hole.

Cleaning by dividing & conquering



Cleaning by dividing & conquering

Isolate clean networks from infected ones.

Create a *clean copy* of the infected network structure.

Reinstall infected hosts from known-good backups and place them in the clean network to avoid reinfection

Destroy and set fire to infected network.

(fire actually not needed)

Conclusion

Conclusion

Sophisticated Malware or unknown vulnerabilities (zero-day) laughs at the face of most antivirus solutions

We can say that no market anti-virus solution is able to provide complete protection for automation networks and lead companies to have a "**false sense of security**".

It is necessary to use complementary controls.

Conclusion

We recommend the following security practices:

Segment your network according to what recommends *ANSI/ISA-99 standard in its zones and conduits model*.

Periodic rule reviews of firewalls and IPS that protect automation network, driven by the best practices.

Conclusion

We recommend the following security practices:

Enforce control over any device that is connected to the SCADA network (third party laptops, removable media, modems, etc.) and deep inspection of new software before they are installed can increase a lot the security level and prevent infections.

Do not allow the use of e-mail and web access from inside the automation network **by any means** and, where possible, update critical computer security patches.

Conclusion

Our experience shows that the *disinfection of a contaminated automation network is quite time and resource costly, complex and depends on the cooperation of manufacturers for success*, making the process quite slow.

We encourage the international community to **create a best practices guide on automation plant disinfection** that can serve as a baseline to guide companies that are experiencing this problem to regain control over their control systems and supervision of a planned and preferably fast way.

Conclusion

Companies should be prepared for the worst and

have a contingency plan.

It is essential to have automated backup tools installed on servers as well as redundant critical automation network.

Questions?

Marcelo.branquinho@tisafe.com

Jan.seidl@tisafe.com

+55 (21) 2173-1159 / +55 (11) 3040-8656

Twitter: @tisafe

Skype: ti-safe