

# The Hype Around Targeted Attacks – Are We Really Helpless?

Some Notes on  
CorpInfoSec in 2012

Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)



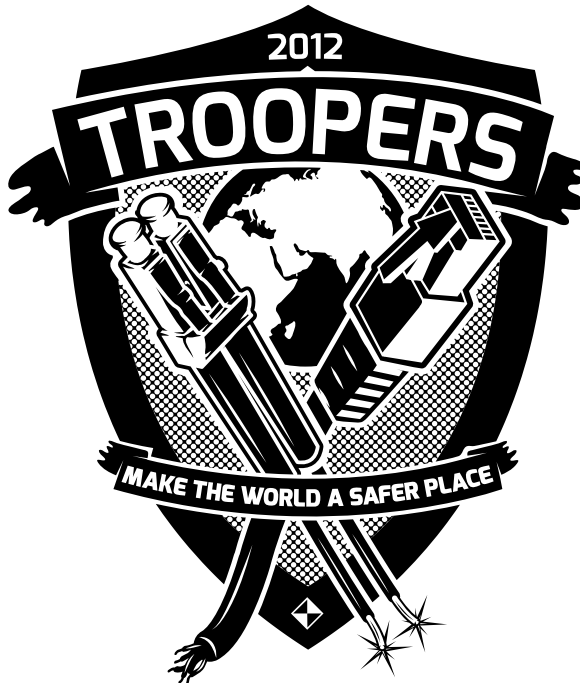
## On the Speaker

Enno Rey



- Founder (2001) and managing director of highly specialized security consulting and assessment services company ERNW (23 FTEs as of Oct 2012).
- Works as “right hand” and trusted business advisor of several CISOs of very large enterprises.
- Host of security conference *Troopers*.
- Long-time contributor to Dayton-based *Dayton Security Summit* ([www.day-con.org](http://www.day-con.org)).
- Blogs on [www.insinuator.net](http://www.insinuator.net).

## ERNW



- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- Blog: [www.insinuator.net](http://www.insinuator.net)
- Conference: [www.troopers.de](http://www.troopers.de)

## Agenda

---

- Adversaries, their Techniques and how to Defend
- Case Studies
- Conclusions





# Security

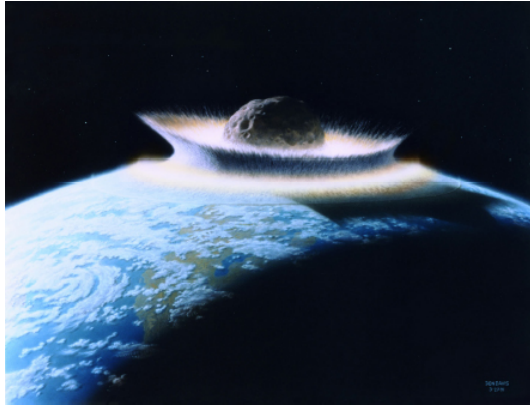


“[...] security is the absence of  
unmitigatable surprise.”

*Dan Geer*

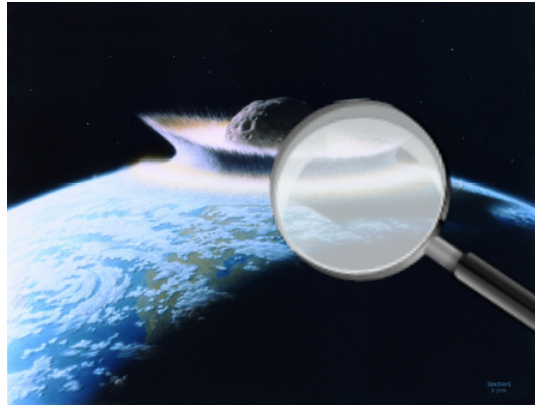
# Threat

---



- Threat: something bad that can happen
  - Regardless of relevance
    - E.g.: Meteorite hitting planet earth

## Risk



- Risk: threat “viewed by some dimensions”
  - How likely is it going to happen? [Likelihood]
  - Are we susceptible if it happens? [Vulnerability (Factor)]
  - What harm is caused in case it hits us? [Impact]
- Talking about threats does not make too much sense
  - At least not when it's about conclusions & actions...

# The Mother of all Threats: APT

This is at least what \$SOME\_SALES\_PPL tell you



## What is APT?

More than another buzzword?



### – **Advanced Persistent Threat**

→ Whether you like it or not:  
We observe that – some – attacks  
become increasingly **sophisticated**.  
= **advanced**.

## What Can be Learned from the APT Discussion?

---



- There's a “social component” in a growing number of attacks.
  - Kind-of back to the roots.
- “Social component” inherently means that attacker = human.
- In the interim, some attacks use quite advanced techniques.
  - Depends on type of attacker.

# “The Adversary” – Types of Attackers

Using a classification from Richard Bejtlich [1] we distinguish:

**Target:** Intellectual property, general intelligence and/or source code

**Examples:** Flame, Stuxnet

- ✓ Often (but not necessarily) “state-sponsored”
- ✓ Strive for *persistent* access



State-Serving  
Adversaries

Self-Serving  
Adversaries



**Target:** Seeking financial gain

**Alias:** “Criminals”

- ✓ Not necessarily interested in long-term persistent access (but in “quick money”)
- ✓ In the majority of cases do not employ “advanced” attack techniques

**Target:** Seeking attention/justice/freedom/awareness

**Alias:** „Hacktivists”

- ✓ Usually do not maintain “persistent” access
- ✓ Usually do not employ “advanced methods”



Public-Serving  
Adversaries

# Did You Notice a(nother) Main Differentiator?

## Their *Motivation*



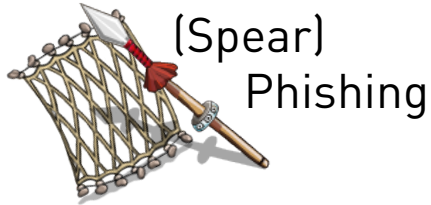
- Their motivation might vastly differ:
  - (I) Get access to IP and/or source code.
  - (II) Use your organization as stepping stone to \$OTHER\_TARGET
    - This is probably what just happened to Adobe.
  - (III) Get anything that could be of economic value
    - Might just be opportunistic to sell on black market.
  - (IV) Cause harm/bad press/embarrassment.
  
- Depending on motivation, attack techniques will be different
  - For (I) and (II) adversary probably willing to spend \$RESOURCES
    - Potentially simple math (cost/benefit calculation).
  - For (III) “standard techniques” will be used.
  - **BUT:** Even adversaries with intent (I) or (II) might use “standard techniques” first.



- At least this is what (e.g. we as) pentesters do.
- Ok, usually they don't care of getting noticed.
- Still, would you notice “the use of standard techniques” at all?

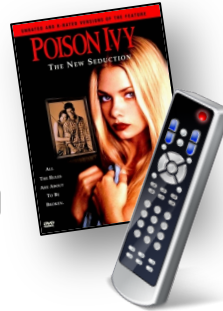


# Techniques They Use



## Remote Control of Victim's System

- E.g. Poison Ivy (RAT)







## Denial-of-Service

- Usually public-serving adversaries only



## Malicious Code

- Usually Application Level   
- 0day vs. well-known
  - This is one main differentiator between state-serving and self-serving adversaries
- Code can be signed with fake or compromised certificates 
  - State-serving adversaries only/mostly

## Data Exfiltration



## SQLi

- Usually against publicly reachable (database) systems



Just a short note on IE, Java, Flash and the like

- We're not against using those pieces.
- Business will ask for using those anyway.



And business always wins, right?

- So it's an exercise of risk management then!
  - Incl. risk acceptance & accountability!





# Trail of Blood – Adobe Flash

Version 11.x

Brief	Originally Posted	Last Update
<b>APSB12-19</b> Security updates available for Adobe Flash Player	8/21/2012	9/28/2012
<b>APSB12-18</b> Security update available for Adobe Flash Player	8/14/2012	8/14/2012
<b>APSB12-14</b> Security updates available for Adobe Flash Player	6/8/2012	6/28/2012
<b>APSB12-09</b> Security update available for Adobe Flash Player	5/4/2012	5/4/2012
<b>APSB12-07</b> Security update available for Adobe Flash Player	3/26/2012	4/1/2012
<b>APSB12-05</b> Security update available for Adobe Flash Player	3/5/2012	3/5/2012
<b>APSB12-03</b> Security update available for Adobe Flash Player	2/15/2012	2/15/2012
<b>APSB11-28</b> Security update available for Adobe Flash Player	11/10/2011	11/10/2011

**ALL of course! CRITICAL**





# A Menu of Distaste: Java SE

Brief 2012	Originally Posted	Included Fixes
Java SE Critical Patch Update – October 2012	Upcoming: October 16 2012	??
Oracle Security Alert for CVE-2012-4681	August 30 2012	4
Java SE Critical Patch Update – June 2012	June 12 2012	14
Java SE Critical Patch Update – February 2012	February 14 2012	14
Sum		32

“...exploited over a network without the need for a username and password...”

*Oracle Security Alert for CVE-2012-4681*

“12 of the 14 Java SE vulnerabilities fixed in this Critical Patch Update may be remotely exploitable without authentication.”

*Eric Mannix, Director - Oracle Software Security Assurance*

# Yet another Java flaw allows “complete” bypass of security sandbox

Flaw in last three Java versions, 8 years worth, puts a billion users at risk.

by Jon Brodtkin - Sept 26 2012, 0:20am WEDT

by **Jon Brodtkin** - Sept 26 2012, 0:20am WEDT



Java = Exposure



# Running Flash on Corp Desktops is like...



This is fast and comfortable. As business likes it.



Until something goes wrong.



– QUESTION: Who's responsible then?

# Respective Defense Techniques

- User Training & Education
- Infrastructure based (email|content) filtering
- Hardening
- Patching
- Least (admin) privilege
- Protection of credentials  
(Cached Creds, LANMAN hashes et.al.)
- Monitoring & Detection
- Incident Response
- Containment (network isolation/segmentation)

→ All this is well-known stuff!





## Let's Have a Look at Some Case Studies

---



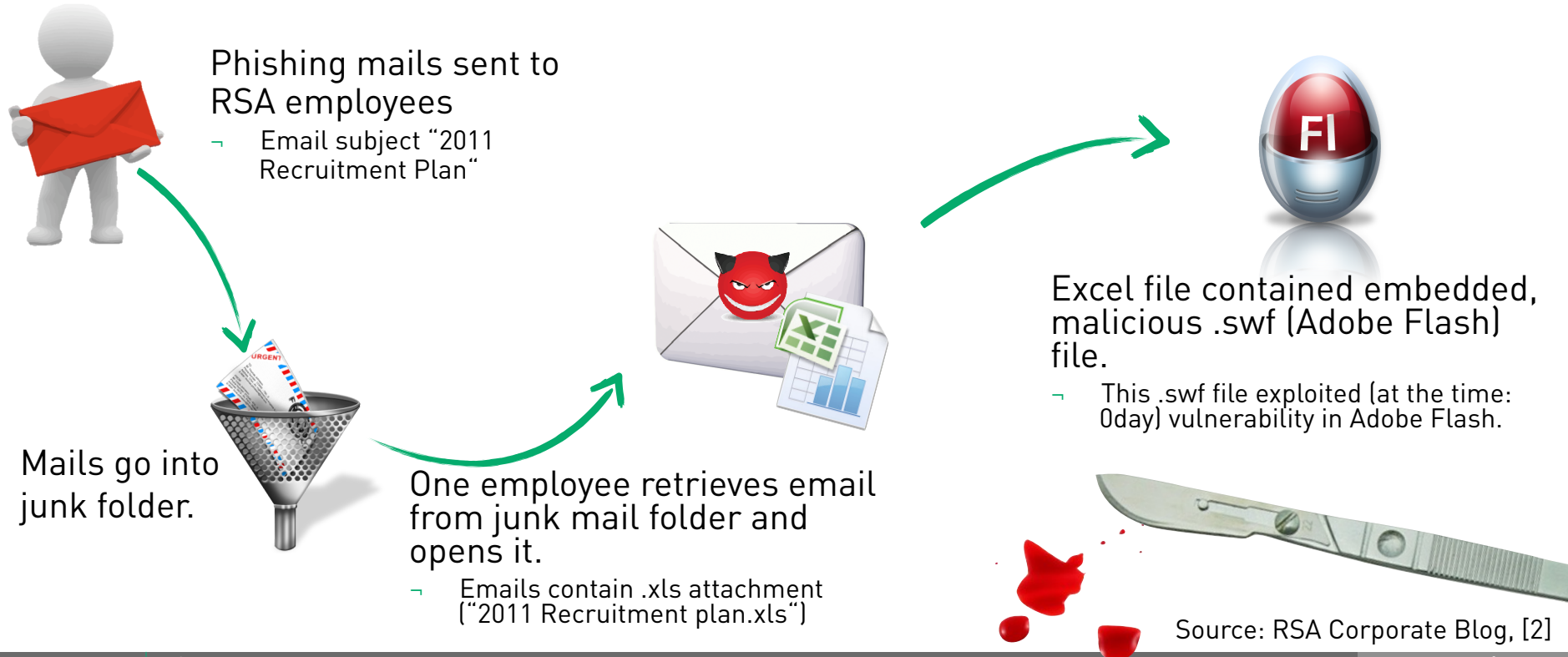
## Let's See:

---

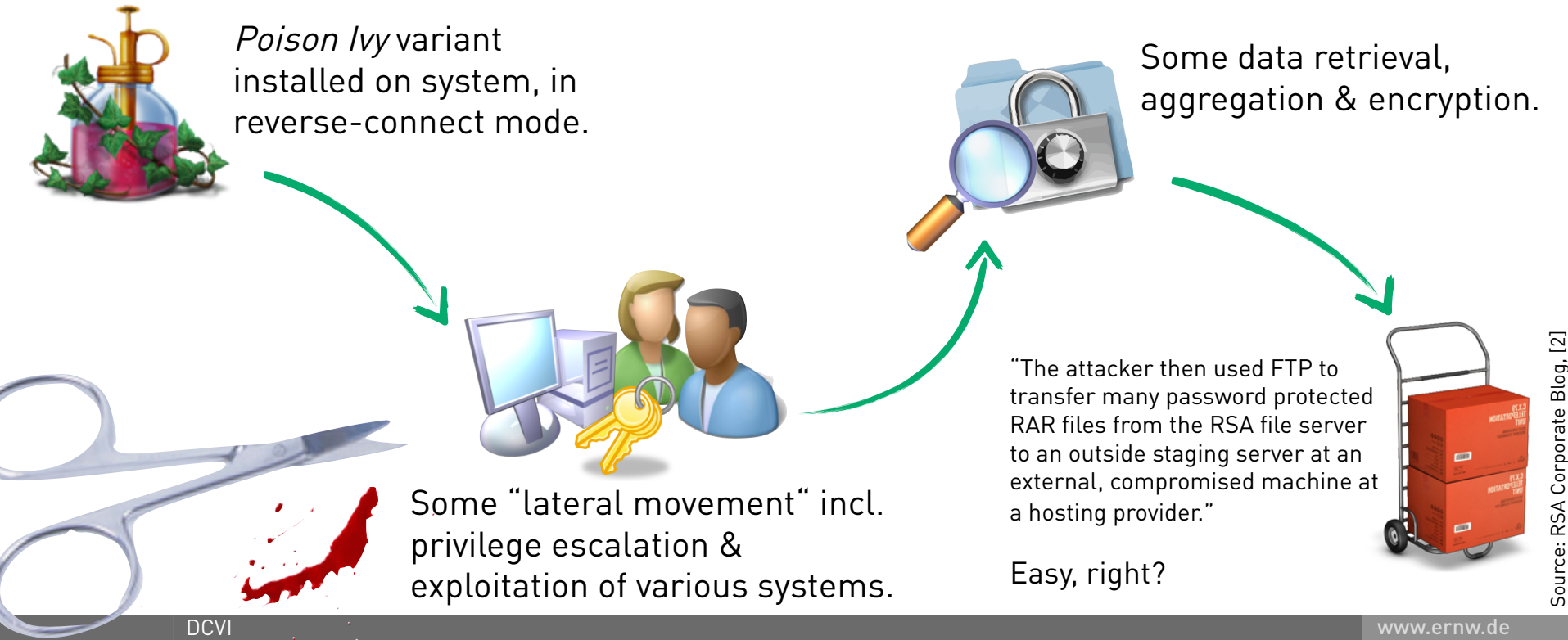


- RSA break-in (disclosed in Mar 2011)
- *Operation Shady RAT* (disclosed Aug 2011, potentially lasted 5+ years)
- *Flame* attack toolkit (disclosed May 2012, in use since at least early 2010).
- Adobe Compromised Certificate (Sep 2012)

# RSA Break-in – Anatomy of an Attack



# RSA Break-in – Anatomy of an Attack



# Operation Shady RAT –

What might have happened, some details

- Phishing emails, containing .xls files



- .xls file exploits MS Excel Featheader Vulnerability
  - CVE-2009-3129, MS09-067 (patch released 11/10/2009)



- Trojan deployed



- Trojan establishes C&C communication with some server, commands hidden in pictures in a steganographic way.



## Flame

"We've found what might be the **most sophisticated cyber weapon** yet unleashed.

[...]

It's big and **incredibly sophisticated**. It pretty much **redefines the notion of cyberwar** and cyberespionage."

*Alexander Gostev, Kaspersky Lab Expert*



### → Infection paths through:

- Two USB routines (autorun.inf / "Euphoria module")
- MS10-061 printer vulnerability
- Remote job tasks
- Domain controller rights
- SUPPORTED BY: Windows Update flaw



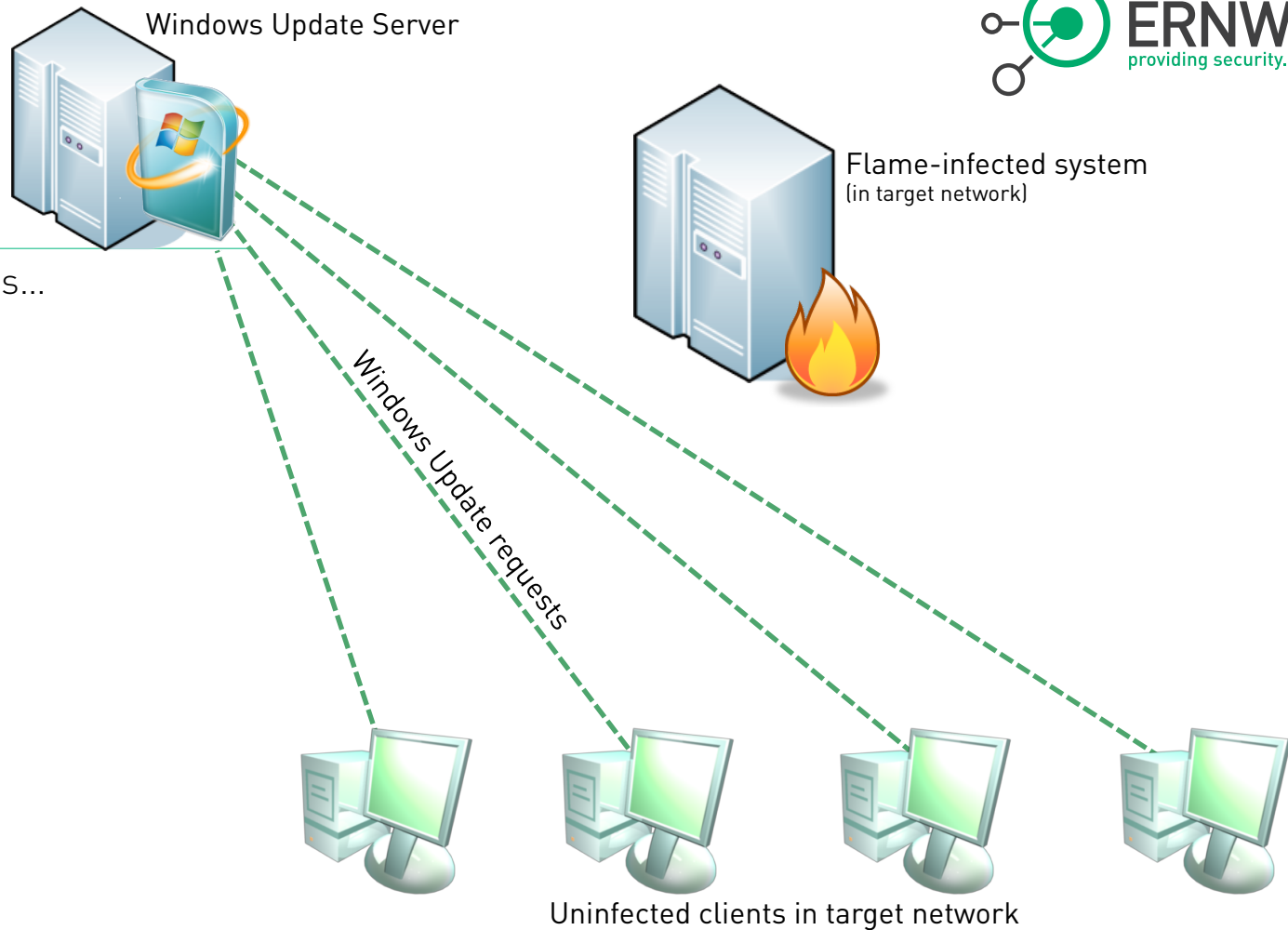
### → 20 times more code than Stuxnet

### → Up to 20 specific modules

- Eavesdropping (network|room), screenshots etc.

# Flame

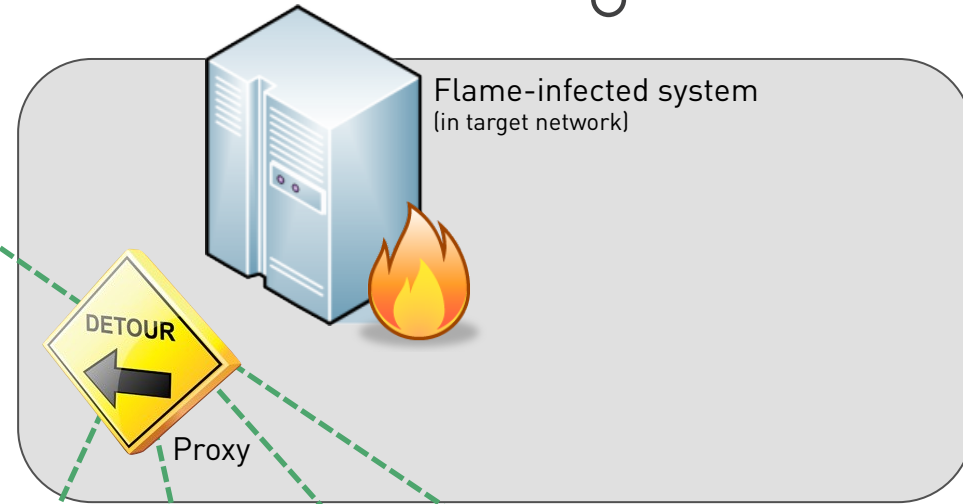
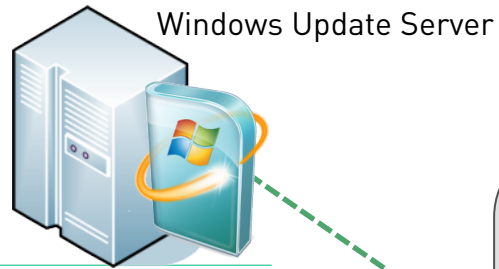
How the fire spreads...



# Flame

How the fire spreads...

- Infected system offers HTTP proxy.
  - Man-in-the-Middle for all \$Windows\_Update requests



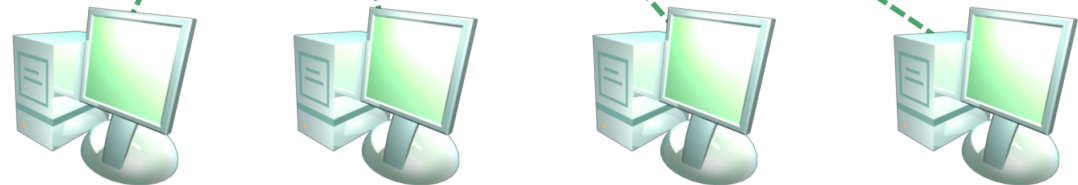
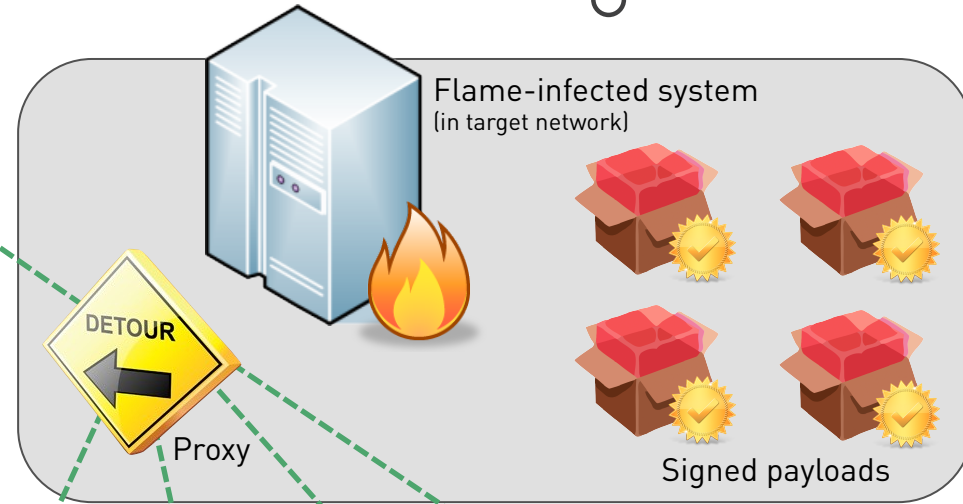
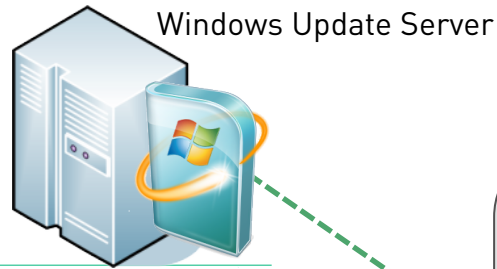
# Flame

How the fire spreads...

- Infected system offers HTTP proxy.
  - Man-in-the-Middle for all \$Windows\_Update requests

Here comes the interesting part:

- Terminal Server Licensing Service allowed to sign code as if it came from Microsoft
  - No access to Microsoft's internal PKI infrastructure needed
  - Originally intended to authorize Remote Desktop services



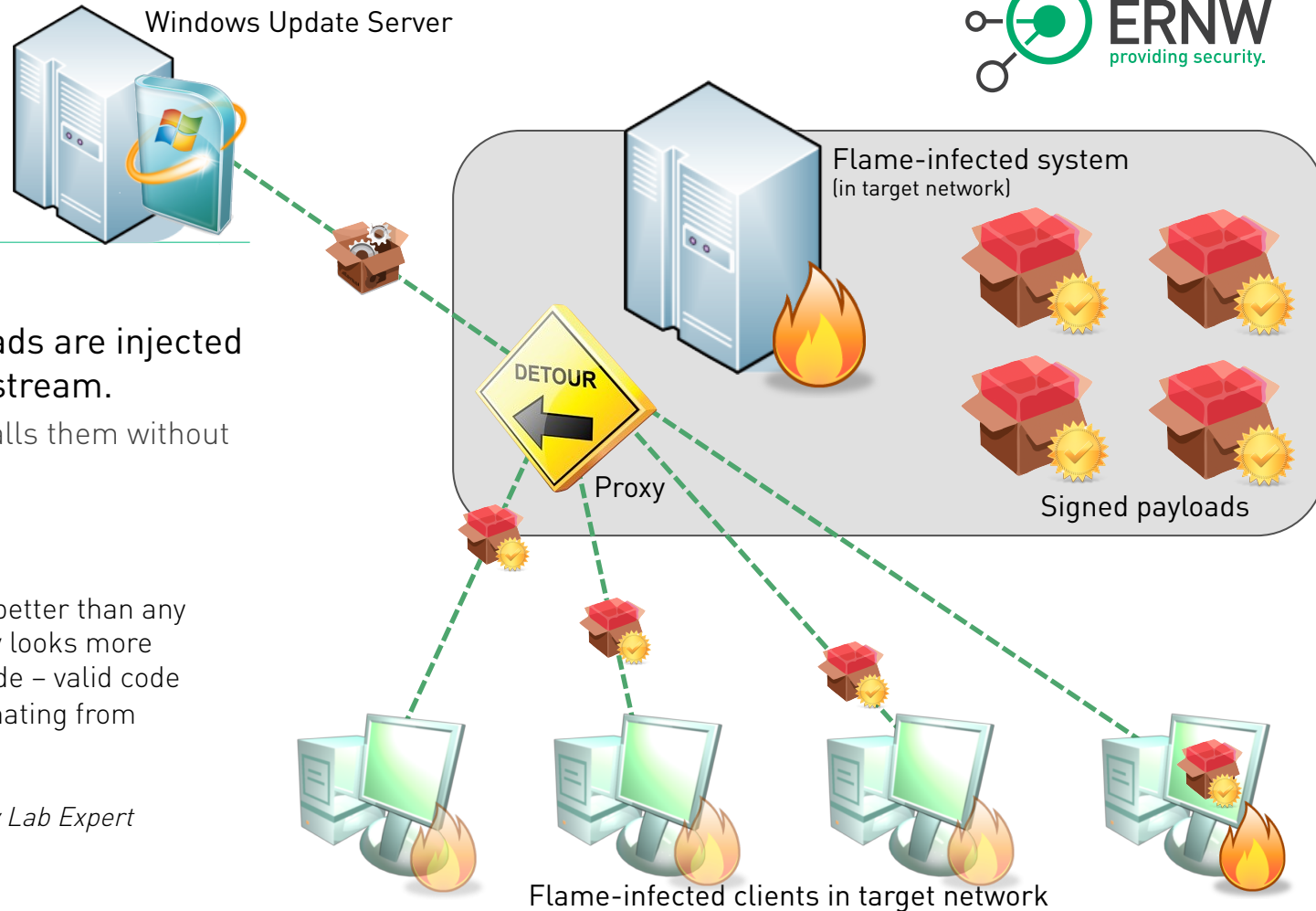


# Flame

- Malicious payloads are injected into the update stream.
  - Windows installs them without any warnings!

“What we’ve found now is better than any zero-day exploit. It actually looks more like a ‘god mode’ cheat code – valid code signed by a keychain originating from Microsoft.”

*Alexander Gostev, Kaspersky Lab Expert*



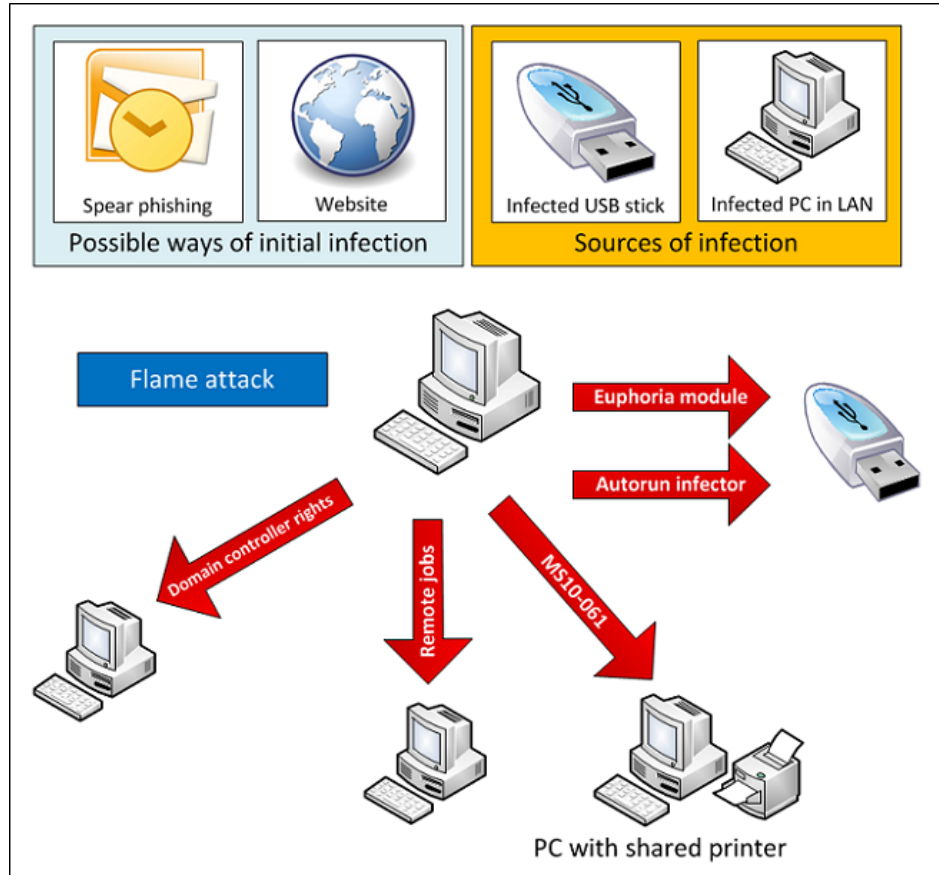
## Flame

---

- Not fully understood yet:

“Consider this: it took us several months to analyze the 500K code of Stuxnet. It will probably take year to fully understand the 20MB of code of Flame.”

[https://www.securelist.com/en/blog/208193522/The\\_Flame\\_Questions\\_and\\_Answers](https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers)



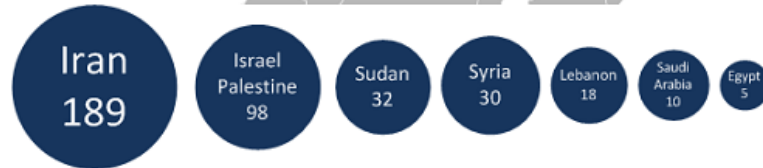
[https://www.securelist.com/en/blog/208193522/The\\_Flame\\_Questions\\_and\\_Aswers](https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Aswers)

## Flame

Target region: Middle East

Question: would the impact have been the same in other parts of the world?

[Hint: “overall security posture” might play a role here]



# Adobe Certificate Compromise



- “We have identified a compromised build server that required access to the code signing service as part of the build process.”
  - “Although the details of the machine’s configuration were not to Adobe corporate standards for a build server, this was not caught during the normal provisioning process.”
    - Question: When was the last audit of that machine?
- “All entities authorized to request digital signatures were provisioned according to an established procedure that verified the identity of the entity and verified that the release engineering environment met the relevant assurance criteria.”
  - Question: Who had (which kind of) access to the build server? Presumably mostly developers, right?
  - Question: Where did the signed binaries get stored? How to exfiltrate them?

Source: Adobe Security (ASSET) Blog, [4]



**Mikko Hypponen**

@mikko

 Follow










Our sample repository has 5127 files that have been signed with the compromised Adobe certificate.

[pic.twitter.com/too9MoYA](https://pic.twitter.com/too9MoYA)

 Reply  Retweet  Favorite

First seen: ☐ Last 24h ☐ Last 2 weeks ☐ Last month ☒ Any Order by:  search [advanced](#)

Found 5127 results.

Add detection ▾ Analyze ▾ Categorize ▾ Email ▾ Exclusions ▾ Export ▾ Tag ▾ Ticket ▾											
<input type="checkbox"/>	System	Filename	Detection	Last scanned	Threat	Weight	Gemini	File type	File size	First seen	Last seen
<input type="checkbox"/>	[FATS]	 default Tantor file...	CLEAN	2 months ago	Clean	0	0	PE32_GUI	670.7 KB	2 months ago	2 months ago
<input type="checkbox"/>	[FATS]	 install_flashplayer1...	CLEAN	1 weeks ago	Clean	0	0	PE32_GUI	757.9 KB	10 months ago	1 weeks ago
<input type="checkbox"/>	[FATS]	 37249e0db6b61f2609c9...	CLEAN	6 months ago	Clean	0	0	PE32_GUI	3.0 MB	16 months ago	16 months ago
<input type="checkbox"/>	[FATS]	 1.tmp	CLEAN	13 months ago	Clean	0	0	PE32_DLL	304.2 KB	22 months ago	13 months ago
<input type="checkbox"/>	[FATS]	 1.tmp	CLEAN	1 days ago	Clean	0	0	PE32_DLL	304.2 KB	19 months ago	1 days ago
<input type="checkbox"/>	[FATS]	 flashplayer10-3_b1_a...	CLEAN	2 months ago	Clean	0	0	PE32_GUI	3.0 MB	20 months ago	19 months ago
<input type="checkbox"/>	[FATS]	 a6dc98198bd8a10bac1d...	CLEAN	1 days ago	Clean	0	0	PE32_GUI	4.5 MB	21 months ago	8 months ago
<input type="checkbox"/>	[FATS]	 setup.exe	CLEAN	20 months ago	Clean	0	0	PE32 executable for	9.0 MB	21 months ago	6 months ago
<input type="checkbox"/>	[FATS]	 bcee42dbad920b837ac1...	CLEAN	16 months ago	Clean	0	0	PE32_GUI	3.2 MB	16 months ago	16 months ago

## Adobe Cert Compromise

## Root Cause Vulnerabilities

---

→ These include:

– Human behavior



– COTS software with debatable security quality



– Failures in operational processes



– Still insufficient patching landscape



– Insufficient handling of external media



# Conclusions – Ask yourself

- Do state-serving adversaries constitute a *relevant risk* for us?
  - If not: what other relevant risks are there [for us]?
- If yes, are we willing to accept this risk?
- If not, are we willing to spend significant effort on mitigation?
  - If not, go back to point 2 (“are we willing to accept?”)
- If so, what **are** the mitigation options?
  - Containment (network isolation/segmentation)
  - Sophisticated monitoring & detection capabilities





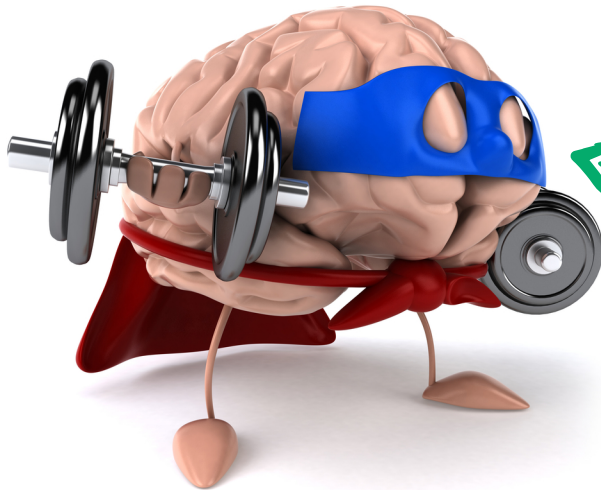
# AAA – Anti APT Appliance

– Do we need this?



# AAA – Anti APT Appliance

- No! We need this: **Common Sense!**  
**Risk mgmt & good**  
**infosec practice.**



## Conclusions (II)



- Next question: Who are you able to defend against?

This is a crucial one. Quite some organizations can't properly defend against self-serving adversaries. How can they think about defending against state-serving adversaries then?



- Run faster than bear or run faster than guy next to you?

Next question: Are self-/public-serving adversaries a relevant risk for us?

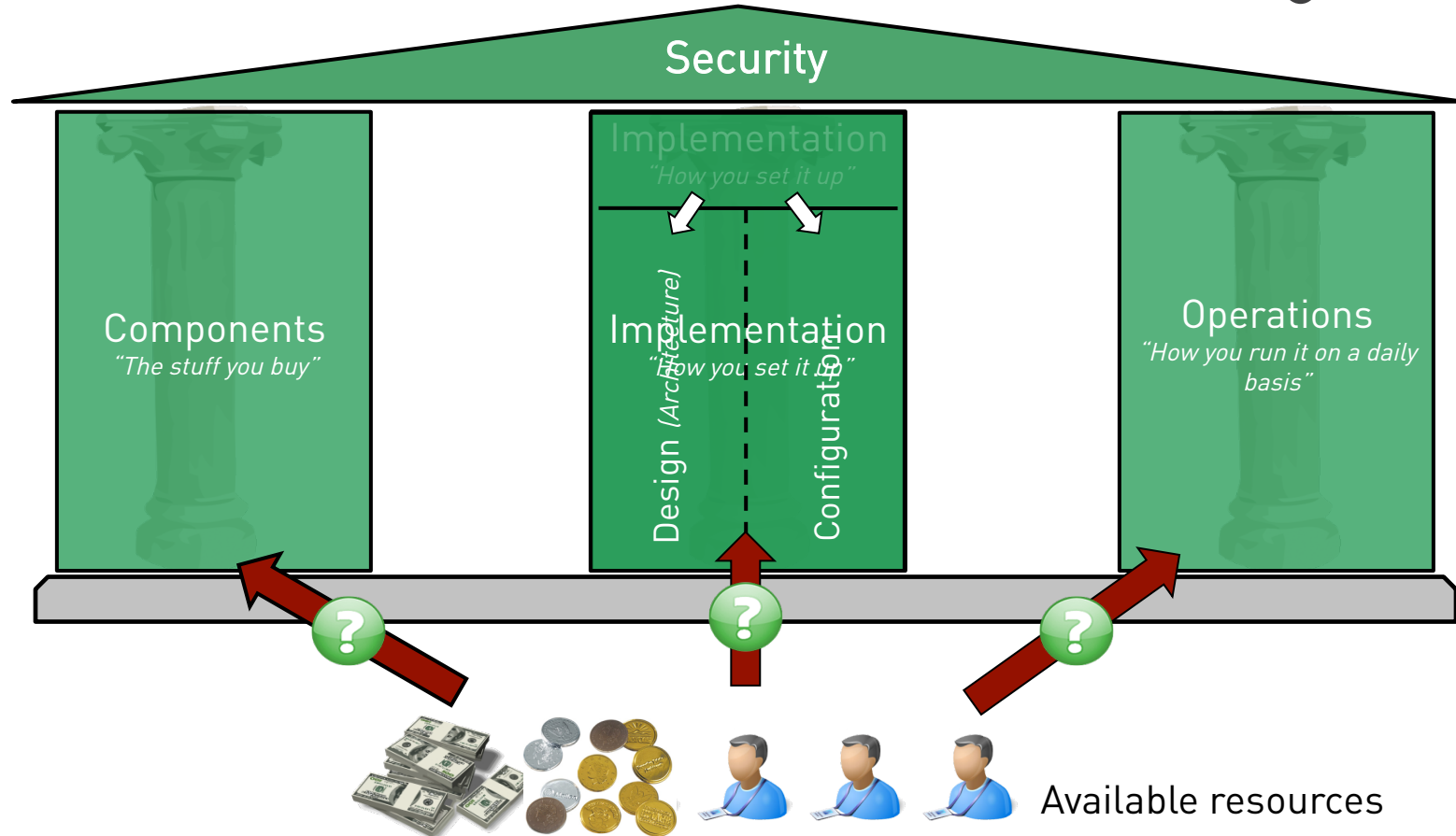


- If yes,  
DO YOUR  
HOMEWORK.





- I've mentioned pretty much all the basic technology & practices stuff already, in this talk.

# Operations is key, aka *The House of Security*



# What other areas of concern do we see?

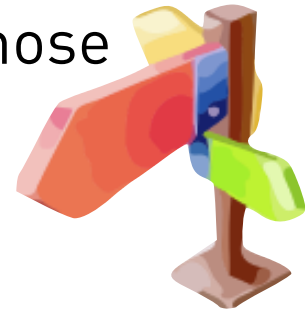
- We think that, for many of you, there's two more important areas of concerns:
  - Business partner connections 
  - Mobile Security 
- Do you see the potential link of those two and \$DETERMINED\_ADVERSARIES?



# Given this is a 45 Min Talk...

here's the 1-slide advice on Business Partner Connections

- You should have a flexible way of handling those
  - One size („implement 2-staged firewall for each connection to \$UNTRUSTED Partner“ or “put them all in one *Business Partner DMZ*”) does not fit all.
- Develop mature risk management process for them
  - Incl. risk acceptance & follow-up



## Business Partner Connections

B	C
More specifically: does \$COMPANY hold shares of \$BUSINESS_PARTNER?	Don't know.
Who currently manages the IT infrastructure of \$BUSINESS_PARTNER?	\$BUSINESS_PARTNER's own IT department.
Does \$BUSINESS_PARTNER dispose of security relevant (e.g. ISO 27001) certifications or are they willing to provide SAS 70/ISAE 3402/SSAE 16 ("Type 2") reports?	Yes, relevant reports (SAS 70 etc., "Type 2") provided (pls attach).
What is – from your perspective – \$BUSINESS_PARTNER's maturity level as for information security management, processes and overall posture?	Overall lower than \$COMPANY standards (pls explain/provide examples).
<b>Connection Details</b>	
How long will the connection be needed?	Limited period of time (pls specify).
Which \$COMPANY resources does \$BUSINESS_PARTNER need to access?	Broad access to resources/network needed.
Does a risk assessment for the mentioned (\$COMPANY) resources exist?	No.
What is the highest (data) classification level that \$BUSINESS_PARTNER needs access to?	Confidential
What is the highest (data) classification of data stored on systems that \$BUSINESS_PARTNER accesses by some means (even if this data is not part of the planned access)?	Confidential
Will data be accessed/processed that is covered by regulatory frameworks [e.g. Data Protection, PCI, ICOFR]?	Don't know.
What would – from your perspective – be the impact for \$COMPANY in case the data in question was disclosed to unauthorized 3rd parties?	Financial loss / loss or revenue < 250.000 EUR (pls provide estimates).
What would – from your perspective – be the impact for \$COMPANY in case the data in question was irreversibly destroyed?	Regulatory exposure/violation of laws or contracts (pls specify).
What would – from your perspective – be the impact for \$COMPANY in case the service(s) in question was/were rendered unavailable for a certain time?	Reputational loss / loss of customer confidence (pls specify).
Can you specify <i>where</i> (e.g. country) the resources to-be-accessed/data processed are located?	Luxembourg only
Are resources to-be-accessed/data processed stored in Luxembourg?	
Can you specify <i>in which part(s) of the \$COMPANY network</i> the resources to-be-accessed are located?	One or more DMZ(s) only
Does the connection terminate solely (with)in a DMZ or are the potential connection endpoints located in other parts of the \$COMPANY network (e.g. CN or SSA)?	In other parts of the network (e.g. CN or SSA) as well
Can you specify how (e.g. web-related method like HTTP[S], [Windows] network share[s] etc.) the \$COMPANY resources will be accessed?	Other (pls specify).
Who – from your knowledge – initiates the individual network connections/requests?	Only outbound connections (leaving from \$COMPANY network) are needed.
Can you specify the level of privileges \$BUSINESS_PARTNER will need/dispose of as for the	



# Business Partner Connections

						Contractual Controls	Number & Type of Sec GWs	IDS/IPS	Encryption	Logging & Analysis	Security Testing (PenTest/Audit) of controls	(Need for) Connection and Controls Review	Risk Acceptance must be signed by
	trust	exposure	protection need	Samples/ Comments									
Type 1	high	high	high	scenario might occur after M & A ("we now own [& hence trust] them; they need access to our databases, ERP & AD; but they still have their own, legacy [= 'exposed'] IT") or in joint ventures.		strong needed	single layer recommended "for compliance reasons"	recommended if doable with reasonable op_effort	mandatory	recommended	recommended every 36 months	mandatory every 12 months	OE VP level
Type 2	high	high	low	might not occur very often in real life.		needed	depends / tbd	-	mandatory	-	recommended every 60 months	recommended every 36 months	depends / tbd
Type 3	high	low	high	probably default case of TBP ("they wouldn't be a 'trusted business partner' if we assumed they were heavily exposed").		strong needed	single layer recommended "for compliance reasons"	recommended if doable with reasonable effort	mandatory	recommended, for compliance reasons	recommended every 36 months	recommended every 36 months	director level
Type 4	high	low	low	mostly BusApp ("we trust Bloomberg, but we don't let them heavily into our network and the stuff is not highly sensitive anyway"), maybe some other cases		recommended	-	-	strongly recommended	-	-	recommended every 60 months	senior mgr
Type 5	low	high	high	EBP, with strong controls - or, in reality, risk acceptance - needed then. Might occur after M & A ("now somebody else owns them and runs [= 'exposure'] their network; but they still need to access our databases, ERP & AD").		needed, plus RA	one layer mandatory + one additional control, final word by ISO	recommended	mandatory	mandatory	mandatory every 24 months	mandatory every 12 months	OE VP level
Type 6	low	high	low	common EBP case (don't trust them, expect the worst as for their exposure, do not let them access sensitive stuff).		needed	one layer mandatory + one additional control recommended	recommended if doable with reasonable op_effort	mandatory	strongly recommended	recommended every 36 months	mandatory every 24 months	director level
				EBP with limited access (thus limited...			one layer mandatory + one additional control recommended	recommended if doable with reasonable op_effort	mandatory	recommended	recommended every 36 months		

See also: <http://www.insinuator.net/2012/02/a-structured-approach-to-handling-external-connections-part-1/>

And this is the 1-slide advice for Mobile Security  
(going to be discussed extensively at this event anyway)

- Do not store sensitive data on those devices.
  - They are – still – not secure enough.
  - Remember what I said about “the social component”.
- In case you do (and I know, most of you do ;-)), perform risk management.
- Always think about the “social component”.
  - If you think that going with \$SOME\_CONTAINER\_APP helps, do you think your (VIP) users are going to use that one, in a proper way? ;-)



# Anything Else? – Yes! 3 Days ago: *Patch Tuesday*...

## Microsoft Security Bulletin Advance Notification for October 2012

Published: Thursday, October 04, 2012

Bulletin ID	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Affected Software
Bulletin 1	Critical Remote Code Execution	May require restart	Microsoft Office, Microsoft Server Software
Bulletin 2	Important Remote Code Execution	May require restart	Microsoft Office
Bulletin 3	Important Elevation of Privilege	May require restart	Microsoft Office, Microsoft Server Software, Microsoft Lync
Bulletin 4	Important Remote Code Execution	May require restart	Microsoft Office, Microsoft Server Software
Bulletin 5	Important Elevation of Privilege	Requires restart	Microsoft Windows
Bulletin 6	Important Denial of Service	Requires restart	Microsoft Windows
Bulletin 7	Important Elevation of Privilege	May require restart	Microsoft SQL Server



There's never enough time...

**THANK YOU...**



**...for yours!**

# Q&A

Feel free to ask now, or later: [erey@ernw.de](mailto:erey@ernw.de)



# Sources

- [1] <https://blog.mandiant.com/archives/3055>
- [2] <http://blogs.rsa.com/rivner/anatomy-of-an-attack/>
- [3] [http://www.securelist.com/en/blog/208193566/Flame\\_Replication\\_via\\_Windows\\_Update\\_MITM\\_proxy\\_server](http://www.securelist.com/en/blog/208193566/Flame_Replication_via_Windows_Update_MITM_proxy_server)
- [4] <http://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html>

