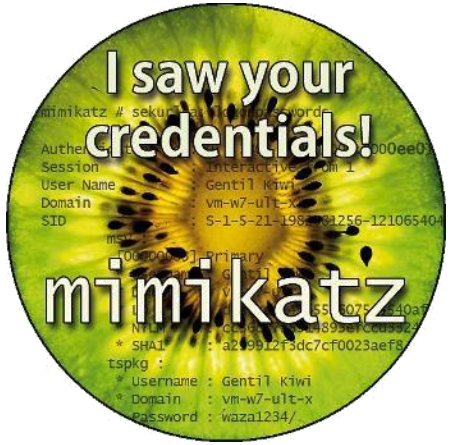
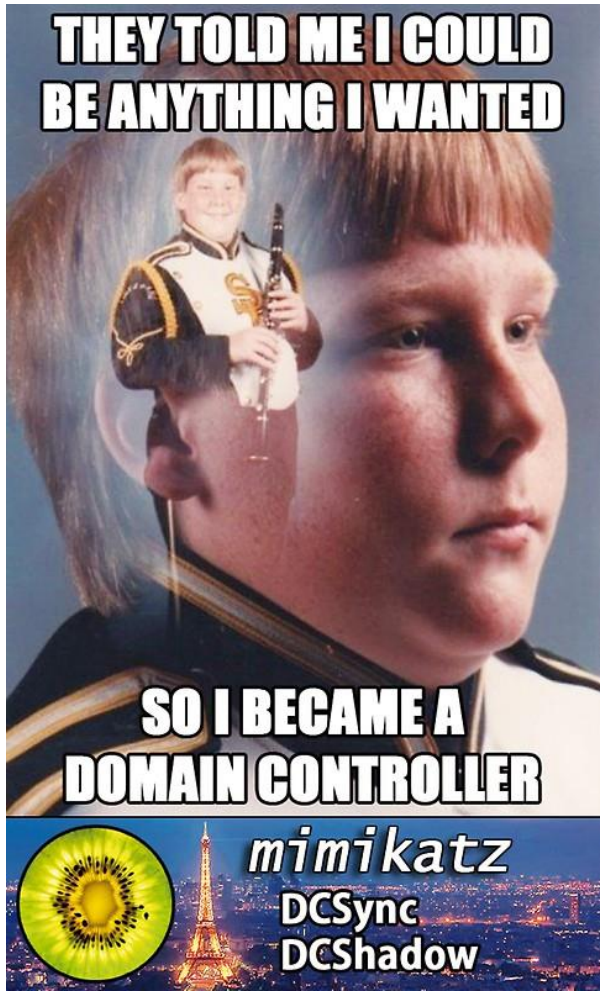
YOU « TRY » TO DETECT MIMIKATZ ;)



Whoami



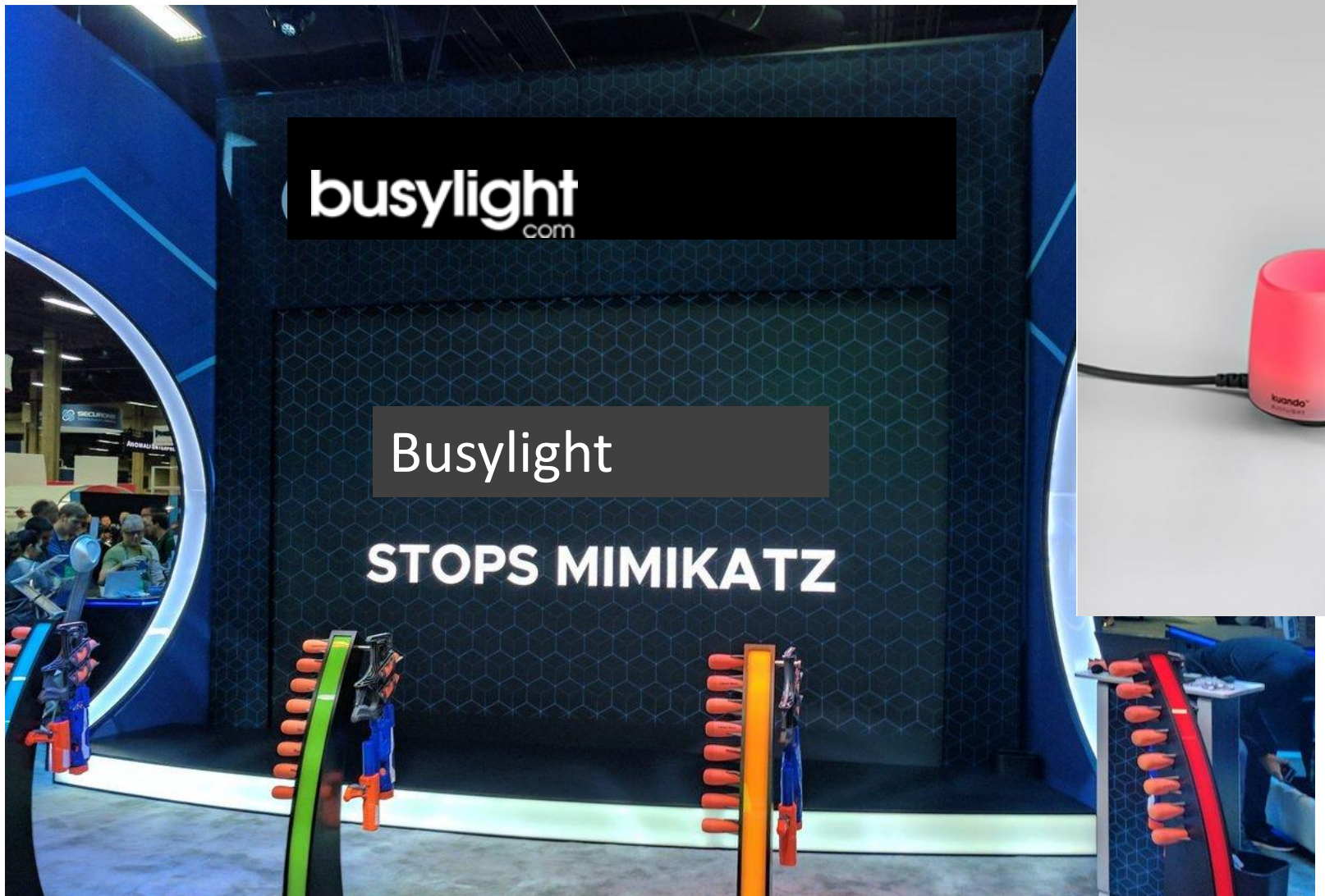
Vincent LE TOUX

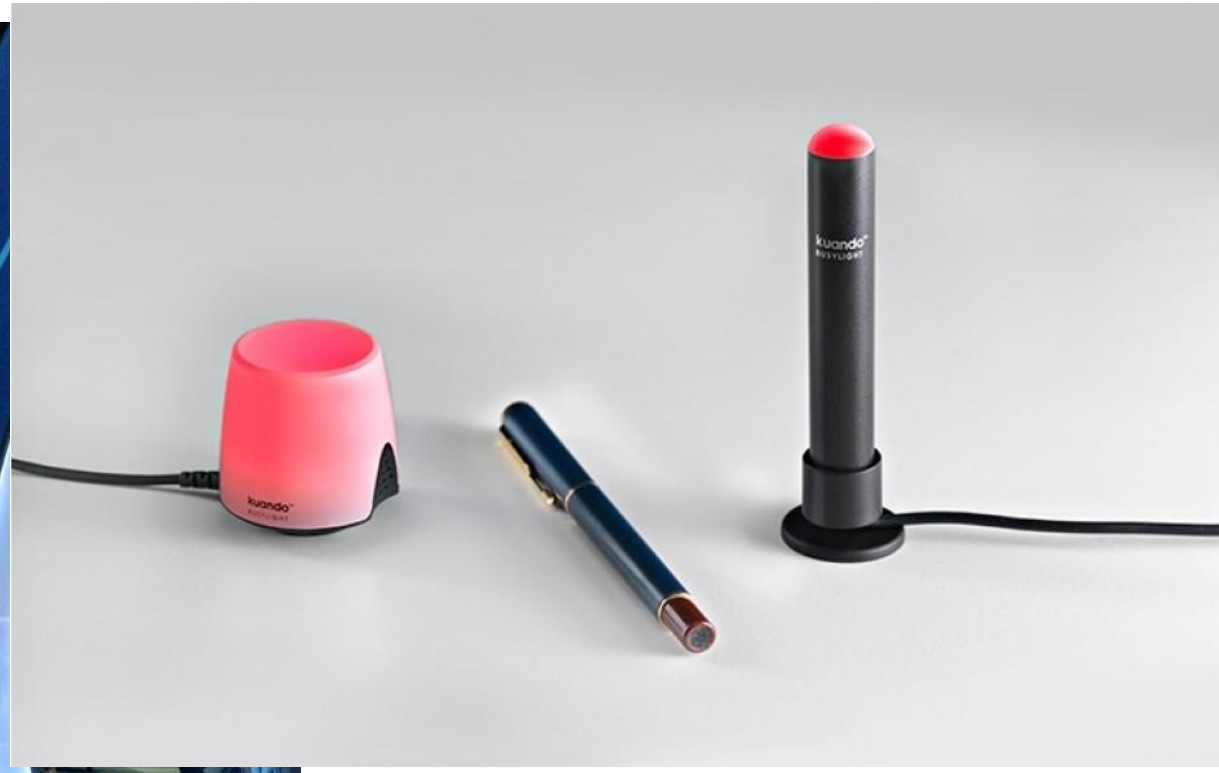
@mysmartlogon

PING CASTLE

Does this remind something to you?

Busylight stops mimikatz!

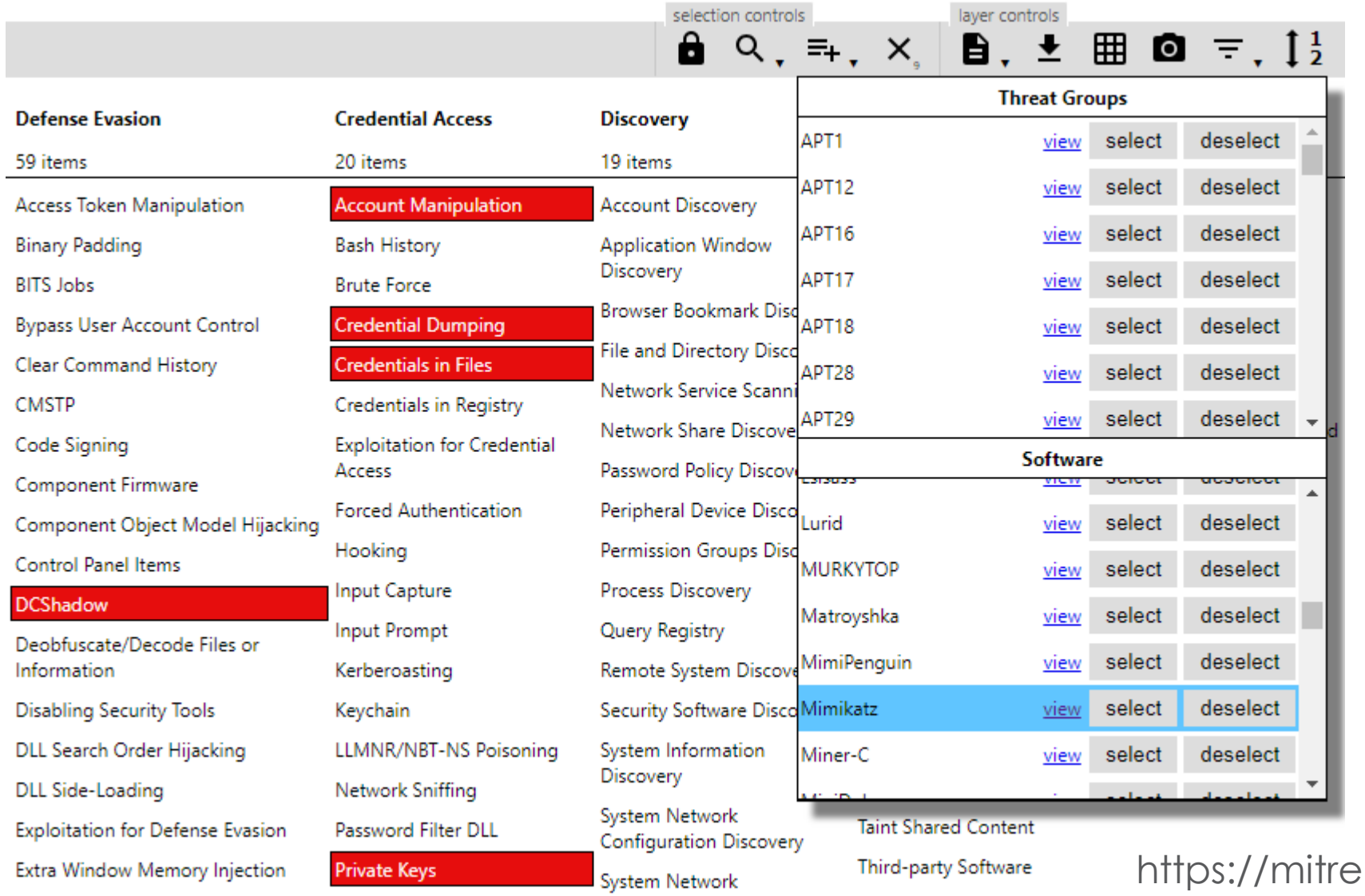




Demo

COMMON MISTAKE: MIMIKATZ IS NOT JUST ABOUT CREDENTIAL COLLECTION

No excuse: ATT&CK from Mitre



Tactic	Technique
Persistence	Security Support Provider
Privilege Escalation	SID-History Injection
Defense Evasion	DCShadow
Credential Access	Account Manipulation
Credential Access	Credential Dumping
Credential Access	Credentials in Files
Credential Access	Private Keys
Lateral Movement	Pass the Hash
Lateral Movement	Pass the Ticket

Golden ticket

https://mitre.github.io/attack-navigator/enterp

3 main areas

- Local LSASS hacking
  - **SEKURLSA::LogonPasswords**
- Remote AD hacking
  - **LSADUMP::DCSync, kerberos::golden**
- MISC
  - **CRYPTO::Certificates**

From: "Unofficial Guide to Mimikatz & Command Reference"

If you want to stop mimikatz, you have to stop every techniques!

AN EXAMPLE: UNDERSTANDING THE GOLDEN TICKET ATTACK DISCLOSURE

A reminder about the golden ticket attack

- Presented at BlackHat USA 2014

- https://www.blackhat.com/us-14/briefings.html#abusing-microsoft-kerberos-sorry-you-guys-dont-get-it

The reactions in the security community

CERT-EU

CERT-EU Security Whitepaper 2014-007

Kerberos Golden Ticket Protection

Mitigating Pass-the-Ticket on Active Directory

Miguel SORIA-MACHADO, Didzis ABOLINS, Ciprian BOLDEA, Krzysztof SOCHA
ver. 1.4
April 26, 2016

1 year later

le 22 juin 2015

BULLETIN D'ACTUALITÉ DU CERT-FR

Objet: Bulletin d'actualité CERTFR-2015-ACT-025

GESTION DU DOCUMENT

Référence	CERTFR-2015-ACT-025
Titre	Bulletin d'actualité CERTFR-2015-ACT-025
Date de la première version	22 juin 2015
Date de la dernière version	22 juin 2015
Source(s)	
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

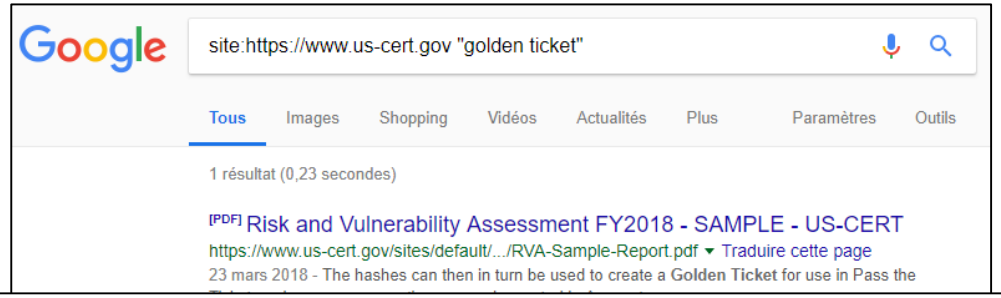
Bundesamt
für Sicherheit in der
Informationstechnik

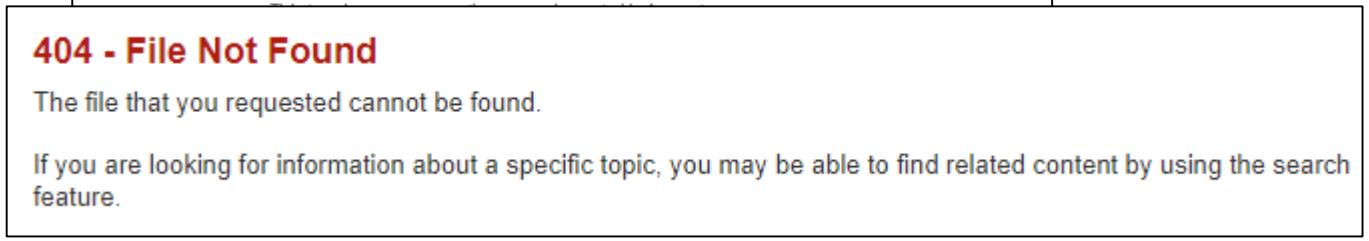
Theme

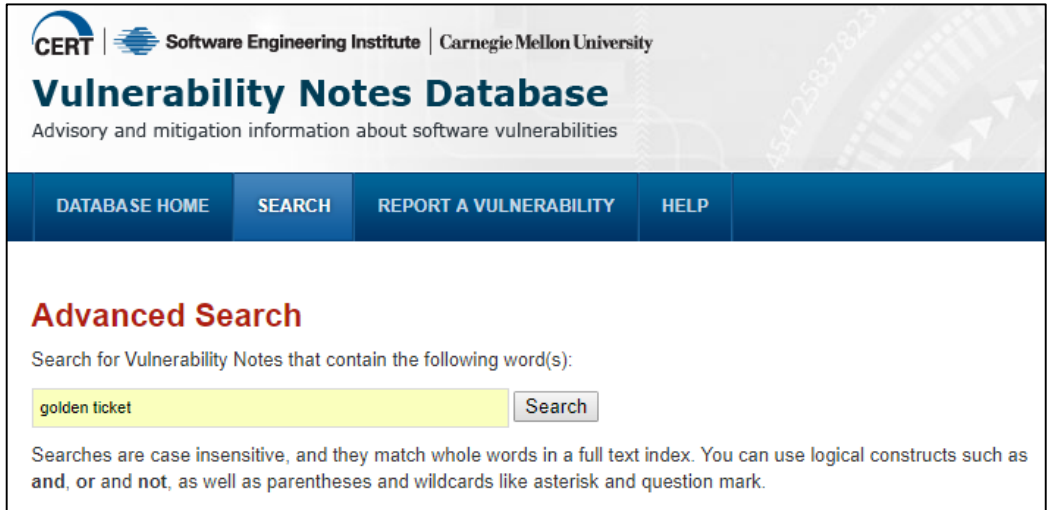
IT-Grundschutz

Umsetzungshinweise zum Baustein DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

Nothing found in US CERT databases







- Is that because the « golden tickets » attack is not a vulnerability ?
- No analysis was done ?

Thanks to wikileaks for more insight

Raytheon
Blackbird Technologies

SECRET//NOFORN

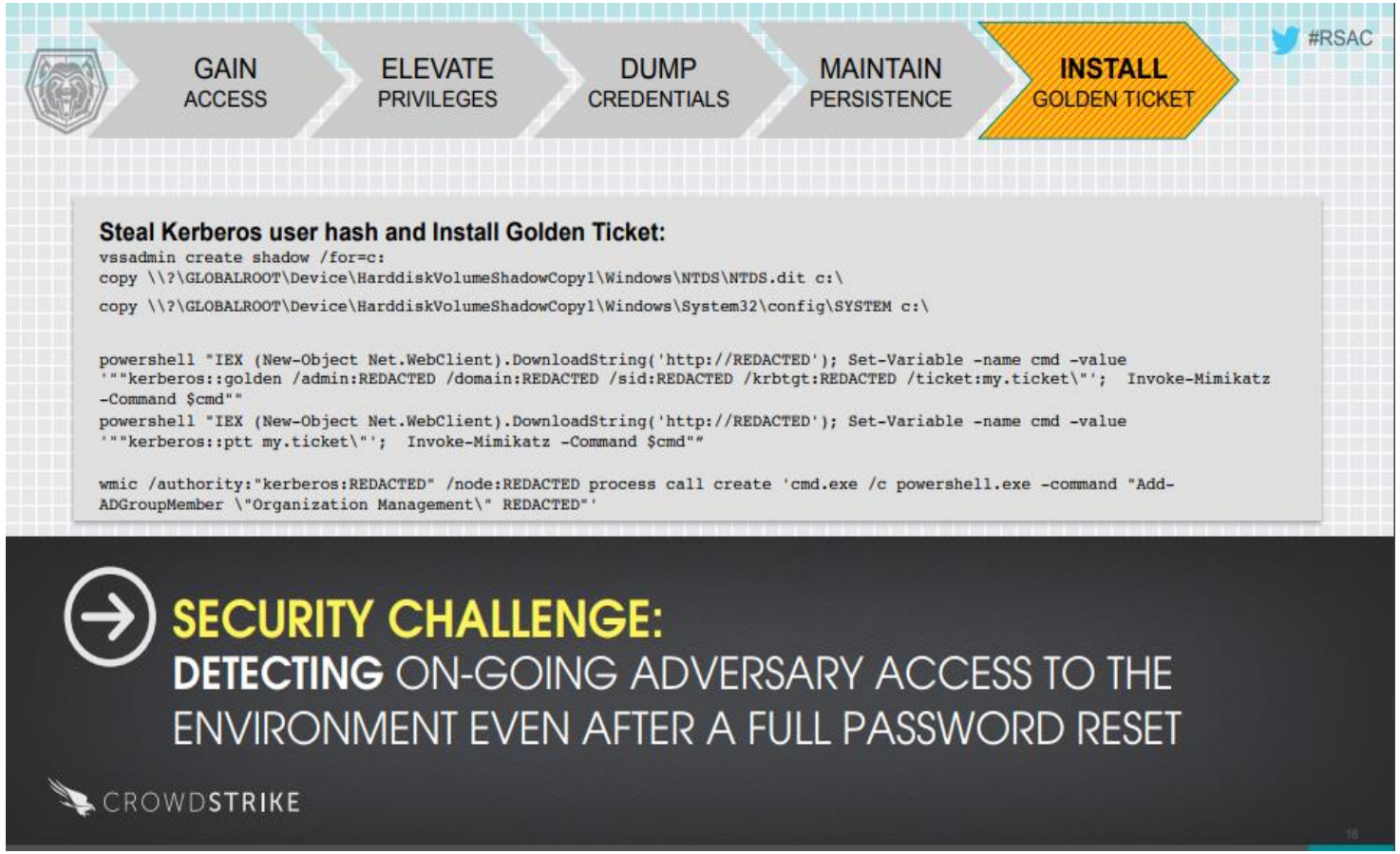
Pique Analysis Report
20150821-261-CERT-EU Kerberos Golden Ticket

1.0 (U) Analysis Summary

(S//NF) This report covers two reports on an attack known as "passing the golden ticket", a Kerberos TGT ticket. One report was provided by CERT-EU titled, "Protection from Kerberos Golden Ticket", and the other report a slide deck from the 2015 RSA Conference titled, "Hacking Exposed: Beyond Malware." The RSA Conference slide deck touches on passing the golden ticket. The CERT-EU report focuses, as the title suggests, on detecting and mitigating a passing the golden ticket attack and there are essentially no technical details on how to perform the attack. The RSA Conference slides provides some redacted PowerShell script commands that invoke mimikatz to build a golden ticket, but little technical discussion on implanting an attack from beginning to end. The report describes what access and artifacts are required to build a golden ticket, but it does not provide any technical details in achieving the required level of access or pivoting to collect the necessary artifacts.

https://wikileaks.org/vault7/document/2015-09-20150821-261-CERT-EU-Kerberos_Golden_Ticket/2015-09-20150821-261-CERT-EU-Kerberos_Golden_Ticket.pdf

Don’t mix BlackHat with RSA !



Root cause:
Wrong information flow in the infosec community

TRYING TO DETECT MIMIKATZ

Buy an Antivirus (or not) 1/2 ?

1) Mimikatz is not a « virus »

49 engines detected this file

49 / 57

SHA-256	b985bca0eaf044c321f1d4274ec1cf9660e5d90553c557b3769f0bce744fa3ae
File name	mimikatz.exe
File size	394 KB
Last analysis	2017-01-13 17:45:50 UTC

2017

Detection | Details | Relations | Behavior | Community 1

Ad-Aware	Gen:Variant.Zusy.157789	AegisLab	HackTool.W32.Mimikatz.i!c
AhnLab-V3	HackTool/Win32.Mimikatz.R185194	ALYac	Gen:Variant.Zusy.157789
Antiy-AVL	HackTool/Win32.Mimikatz	Arcabit	Trojan.Zusy.D2685D
Avast	Win32:PUP-gen [PUP]	AVG	HackTool.AEHJ
Avira	SPR/Mimikatz.i.3	AVware	Trojan.Win32.Generic!BT
BitDefender	Gen:Variant.Zusy.157789	CAT-QuickHeal	Trojan.ZAgent
ClamAV	Win.Tool.Mimikatz-5	CMC	HackTool.Win32.Mimikatz!O
Comodo	UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_62% (D)
Cyren	W32/Mimikatz.A.gen!Eldorado	DrWeb	Trojan.StartPage.54019
Emsisoft	Gen:Variant.Zusy.157789 (B)	eScan	Gen:Variant.Zusy.157789
ESET-NOD32	a variant of Win32/RiskWare.Mimikatz.G	F-Prot	W32/Mimikatz.A.gen!Eldorado

+13 AV
Only +4 detection ?

53 engines detected this file

53 / 70

SHA-256	b985bca0eaf044c321f1d4274ec1cf9660e5d90553c557b3769f0bce744fa3ae
File name	mimikatz
File size	394 KB
Last analysis	2019-03-06 12:52:55 UTC

2019

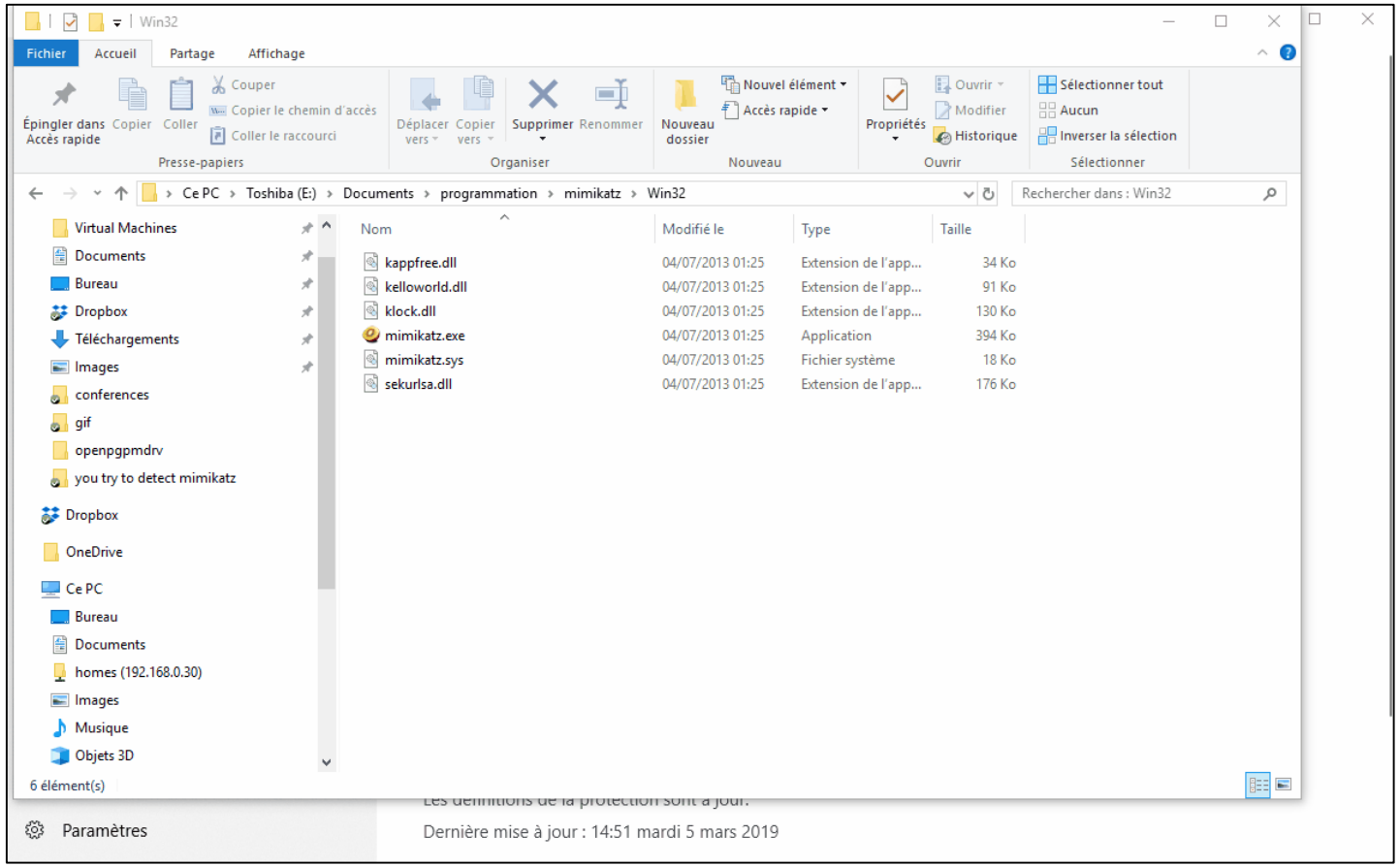
Detection | Details | Relations | Behavior | Community 1

Ad-Aware	Gen:HackTool.WinCred.2	ALYac	Gen:HackTool.WinCred.2
Antiy-AVL	HackTool/Win32.Mimikatz	Arcabit	Gen:HackTool.WinCred.2
Avast	Win32:PUP-gen [PUP]	AVG	Win32:PUP-gen [PUP]
BitDefender	Gen:HackTool.WinCred.2	CAT-QuickHeal	Trojan.ZAgent
ClamAV	Win.Tool.Mimikatz-5	CMC	HackTool.Win32.Mimikatz!O
Comodo	Malware@#28a1xy4zc9bjk	CrowdStrike Falcon	win/malicious_confidence_100% (W)
Cybereason	malicious.1990cc	Cylance	Unsafe
Cyren	W32/Mimikatz.A.gen!Eldorado	DrWeb	Trojan.StartPage.54019
eGambit	Trojan.Generic	Emsisoft	Gen:HackTool.WinCred.2 (B)
Endgame	malicious (high confidence)	eScan	Gen:HackTool.WinCred.2
ESET-NOD32	a variant of Win32/RiskWare.Mimikatz.G	F-Prot	W32/Mimikatz.A.gen!Eldorado
Fortinet	Riskware/Mimikatz	GData	Win64.Riskware.Mimikatz.B
Ikarus	HackTool.Mimikatz	Jiangmin	HackTool.Mimikatz.d

https://www.virustotal.com/#/file/b985bca0eaf044c321f1d4274ec1cf9660e5d90553c557b3769f0bce744fa3ae/detection

Buy an Antivirus (or not) 2/2 ?

2) If it worked 100% of time, we won't have this discussion ;-)



Example with Windows Defender on my computer:

- The first official version of mimikatz (the one shown in the previous slide) compiled in 2013

- Analysis performed March, 6th 2019

Root cause: Signature instead of « Behavior » detection

Time to Do It Yourself ?

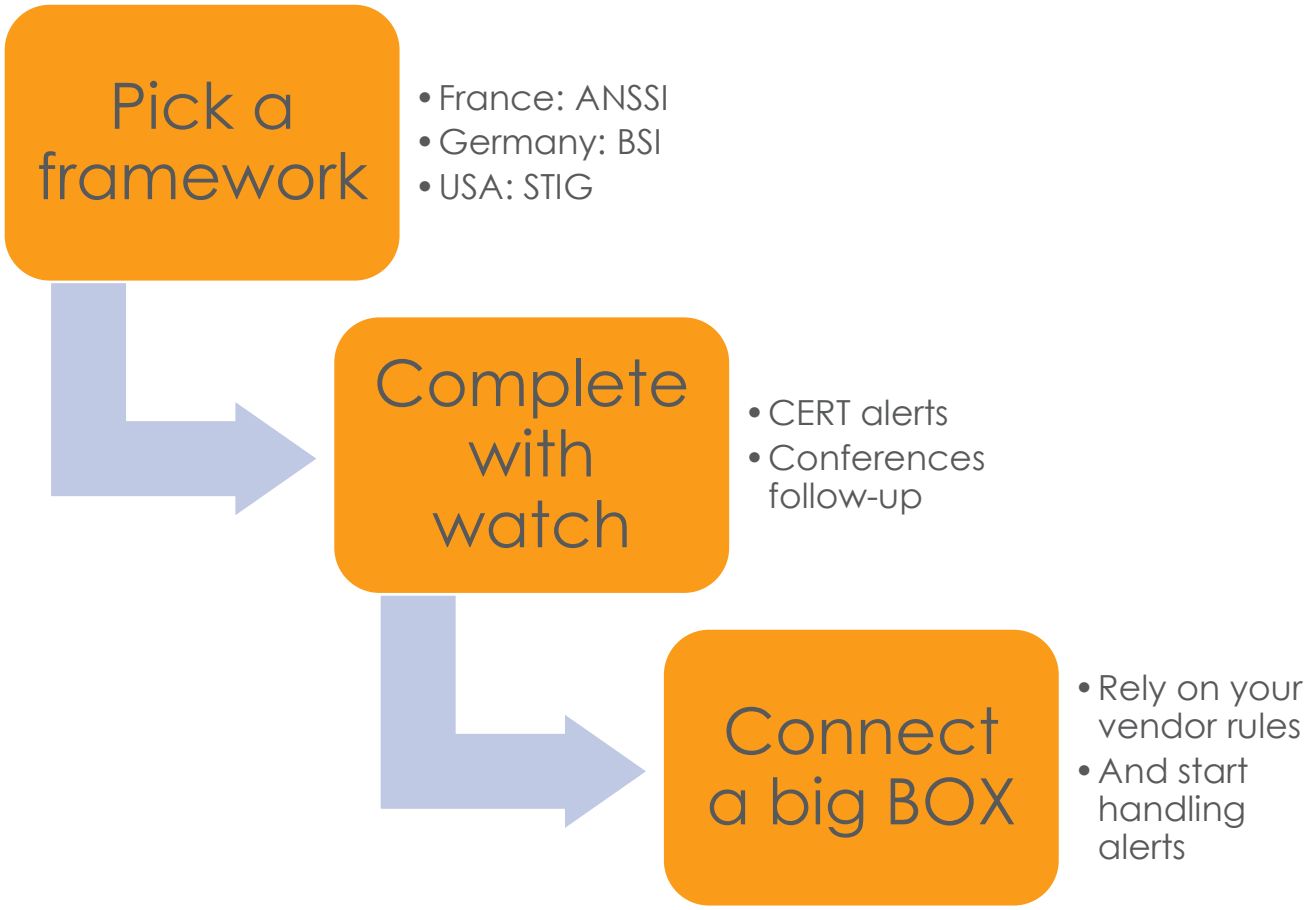
Let's start with the basics and progress

- Idea: you cannot win the « tour de France » if you do not know how to ride a bike

- Same with mimikatz

DETECT: THE CISO WAY

Let's try the CISO way



Example of frameworks

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz

B 5.16 Active Directory

DAT-NT-17/ANSSI/SDE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 10 septembre 2014

N° DAT-NT-17/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 49

NOTE TECHNIQUE

RECOMMANDATIONS DE SÉCURITÉ RELATIVES
À ACTIVE DIRECTORY.

Public visé:	
Développeur	
Administrateur	✓
RSSI	✓
DSI	
Utilisateur	

NIST

NATIONAL VULNERABILITY DATABASE

NVD

NCP

Active Directory Domain STIG Ver 2, Rel 10 Checklist Details

What about the watch?

- Follow your national CERT (CERT-FR, CERT-Bund, US-CERT, …)
- If you have to follow only one person on twitter:
  - @PyroTek3 – Sean Metcalf is the author of www.adsecurity.org and retweet any AD focused topics
- So many interesting AD leaders:
  - @gentilkiwi – Mimikatz's author for new features ;-)
  - Specter ops team: @harmj0y, @tifkin_, @_wald0, @cptjesus, @enigma0x3, ..
  - @DirectoryRanger – linked with ERNW (Troopers)
  - List of persons to follow: https://adsecurity.org/?page_id=4031
- Don't follow @NerdPyle since he doesn't talk AD anymore ;-)

A BOX ? What about a SIEM ?

A Siem « process » ALL events you are sending to it

And you « detect » mimikatz !

Wait …

Frameworks & Watch vs Reality

- Good point: frameworks are explicit (no unlimited list of problems to fix)
- Twitter is the best source of data
- But:
  - Based on the assumption you have no history (few domains, …)
  - Not all attacks are covered by CERT alerts
  - Heterogeneous coverage between framework
  - Basic security problem not covered

Staled Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			Temporary admins
			Weak password

Legend:

the framework has at least one rule covering this item

this item is not covered by any framework rule

SIEM vs Reality

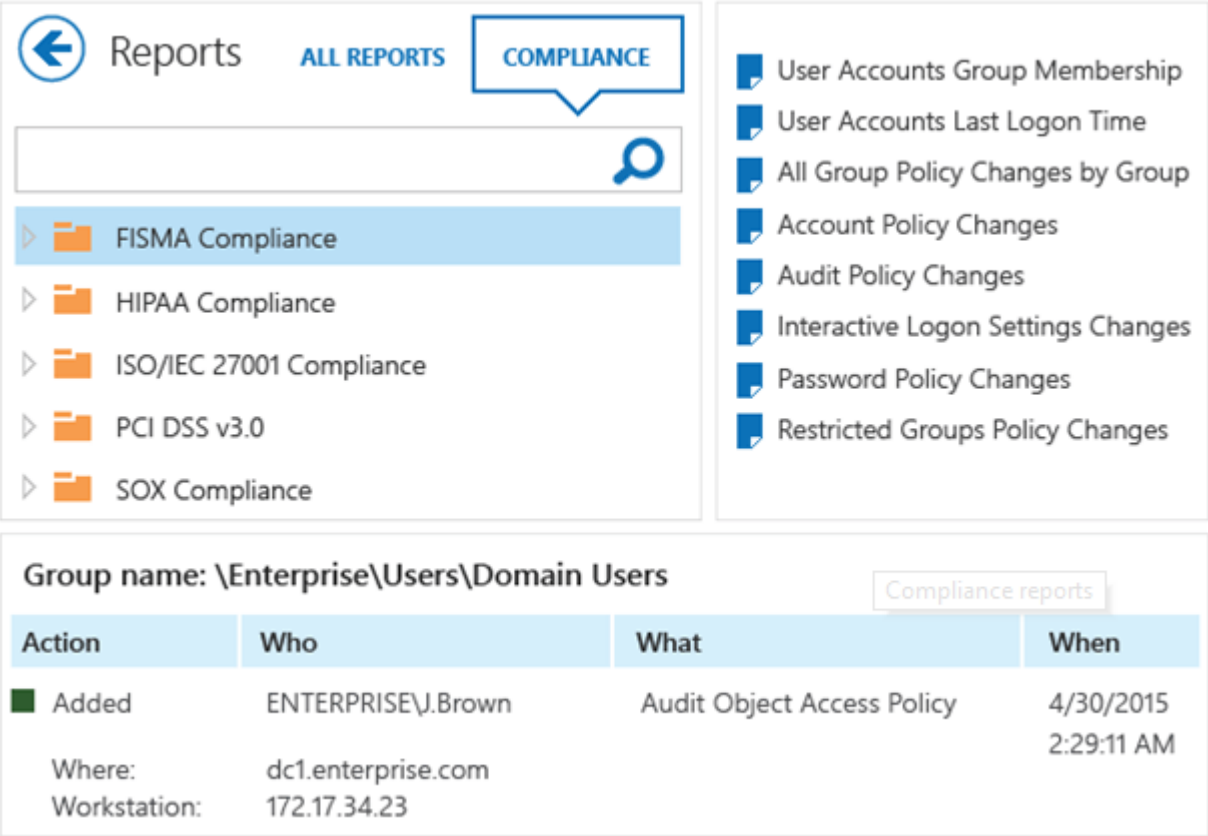
- What you think:
  « new attacks automatically covered »

- What you have:
  - An increase of 30% of your EPS
  - Brute force attack detected
  - Logs collected (which logs?)

- What you don't have:
  - DCSync, Golden ticket, … Detection

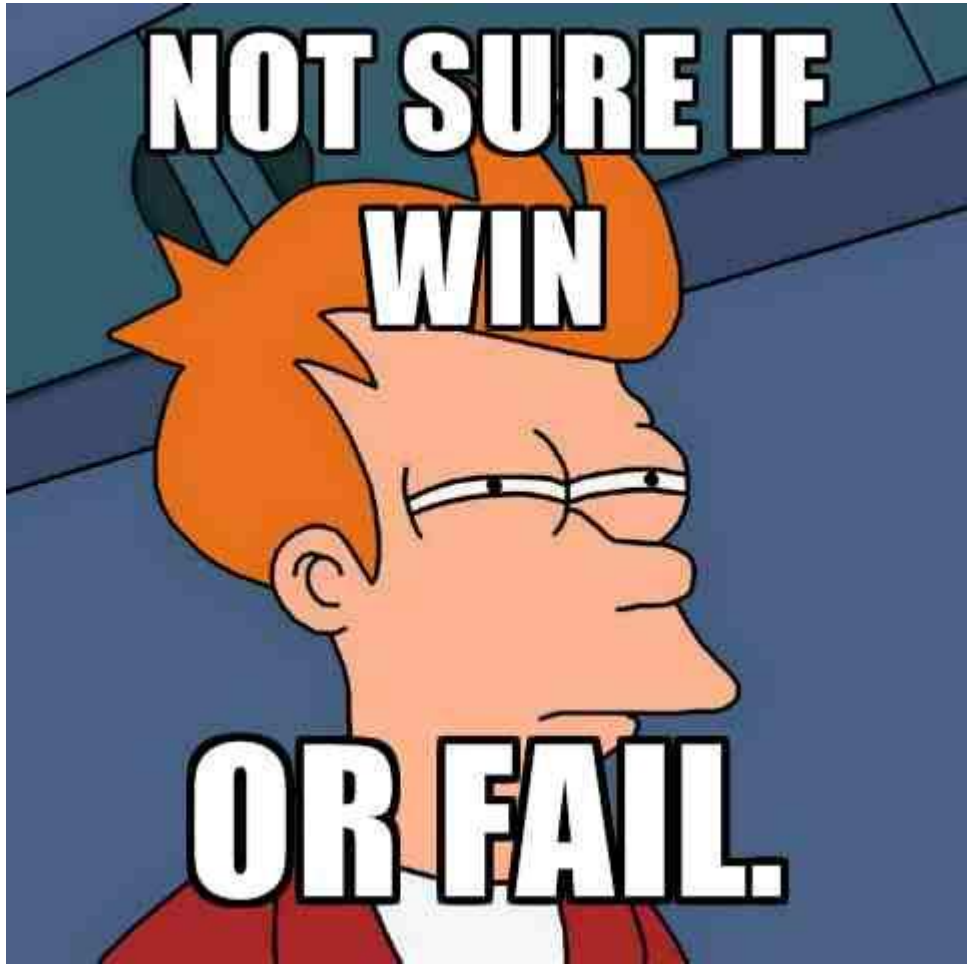
In short no mimikatz detection

And compliance?



Compliance reports from a AD security vendor:
It does not detect mimikatz…

In summary



- Frameworks are structed
  but do not cover all attacks
- Watch covers advanced topics
  but not the basic one
- SIEM process logs
  but are they the right logs and
  what about the rules?

LETS GET TECHNICAL: ZOOMING ON CREDENTIAL THEFT

Evolution of LSASS security posture

LSASS.exe

Windows 7:
Mimikatz is a post compromission tool
This is not a vulnerability

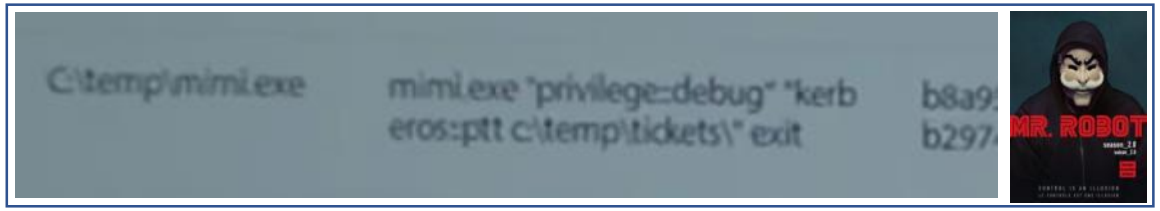
LSASS.exe

Windows 8.1:
Prohibit storage of sensitive passwords ("Restricted Admin mode for Remote Desktop Connection", "LSA Protection", "Protected Users security group")

LSASS.exe

Then:
More and more protection such as virtualisation

New ways to prevent mimikatz

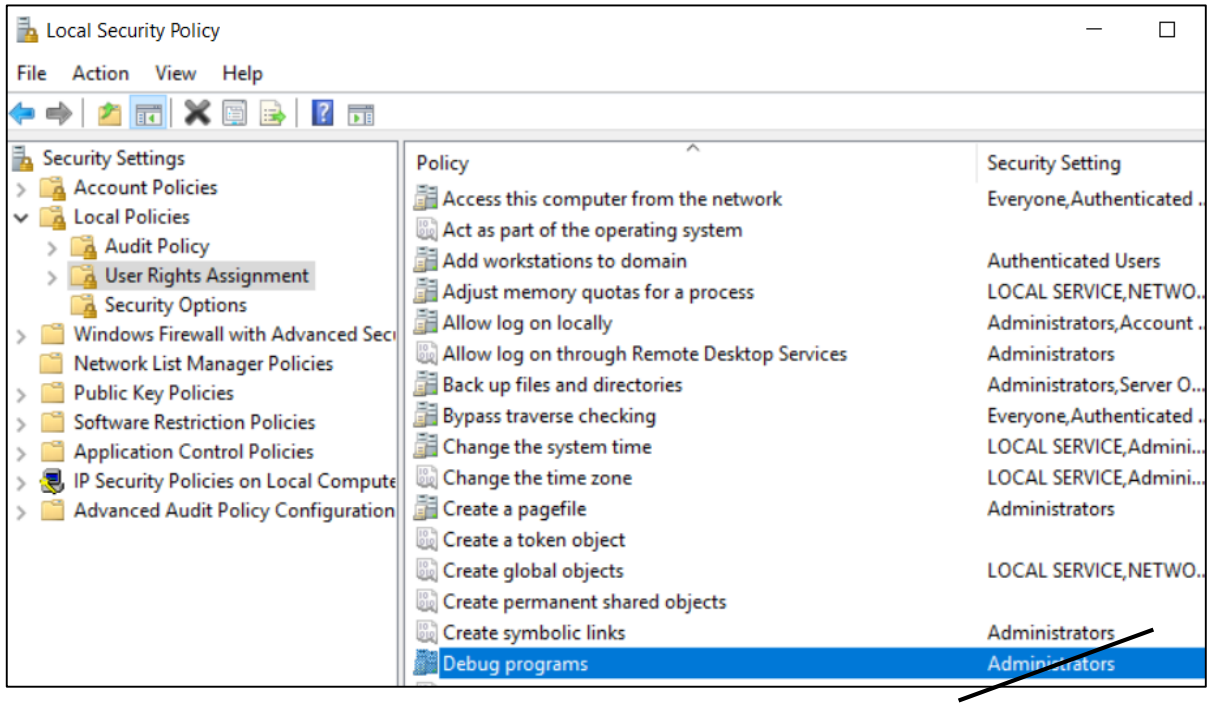


mimikatz 2.1.1 x64 (oe.eo)

```
  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz #
```



Mimikatz requires the « debug privilege » - Just remove it!

psst: run mimikatz as system ;-)

Status of LSA protection

	Applicable Windows version, edition	Protection mechanism	Requirement	Bypassed by
Restricted Admin mode for Remote Desktop Connection	Windows 7 patched	Prevent credentials to be sent on a remote server	None	Allow authentication by « pass-the-hash » & « pass-the-ticket » via CredSSP
Protected Users security group	Windows 7 patched	Force Kerberos only SSP	None	Kerberos ticket stolen
LSA Protection Mode	Windows 7 patched	Restrict access to LSA process on the OS	Requires LSA signature of ALL third party components using EV certificate	!processprotect /process:lsass.exe /remove
Credential Guard	Windows 10 Enterprise only	Isolate secrets from OS on Hypervisor	Secure boot (TPM) & HyperV (Not VMWare)	Capture credentials before being stored

The most effective protection is difficult to implement when dealing with legacy

But there is no place such as LSASS.exe

Methods to read LSASS.exe memory

Genuine Debug access

- Dll injection
- Memory copy

Requires Debug Privilege ✓

Genuine access to passwords

- Security Package
- Authentication package
- Password filters (« ProjectSauron »)

✗

Genuine memory access

- Smart Cards driver (« Calais database »)
- Sub Package (*)

✗

Lessons learned: removing « debug privilege » is not enough

(*) https://docs.microsoft.com/en-us/windows/desktop/secauthn/subauthentication-packages

Demo 2 - mimilib

In fact, LSASS is only a « gold mine »

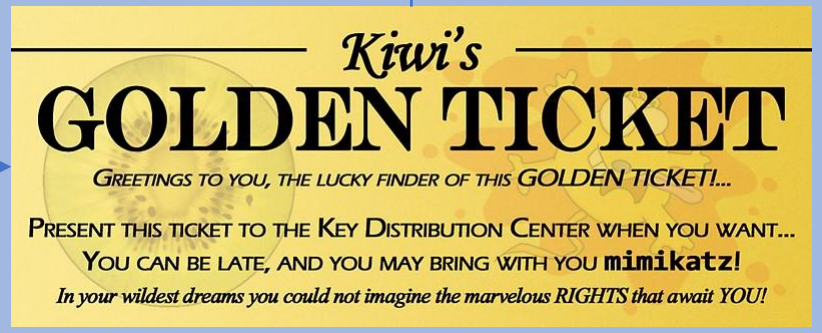
LSASS.exe

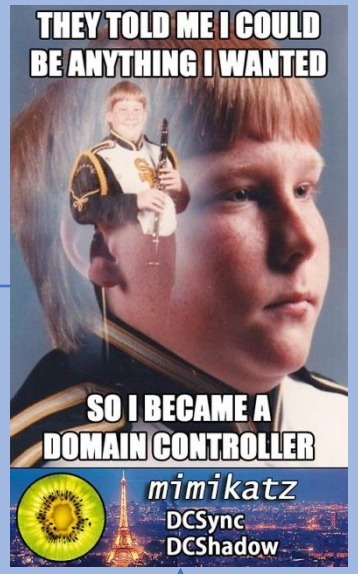
Golden flakes still in the river

Demo 3 – driver + SSPI

ZOOMING ON ACTIVE DIRECTORY

How it works: 1/2

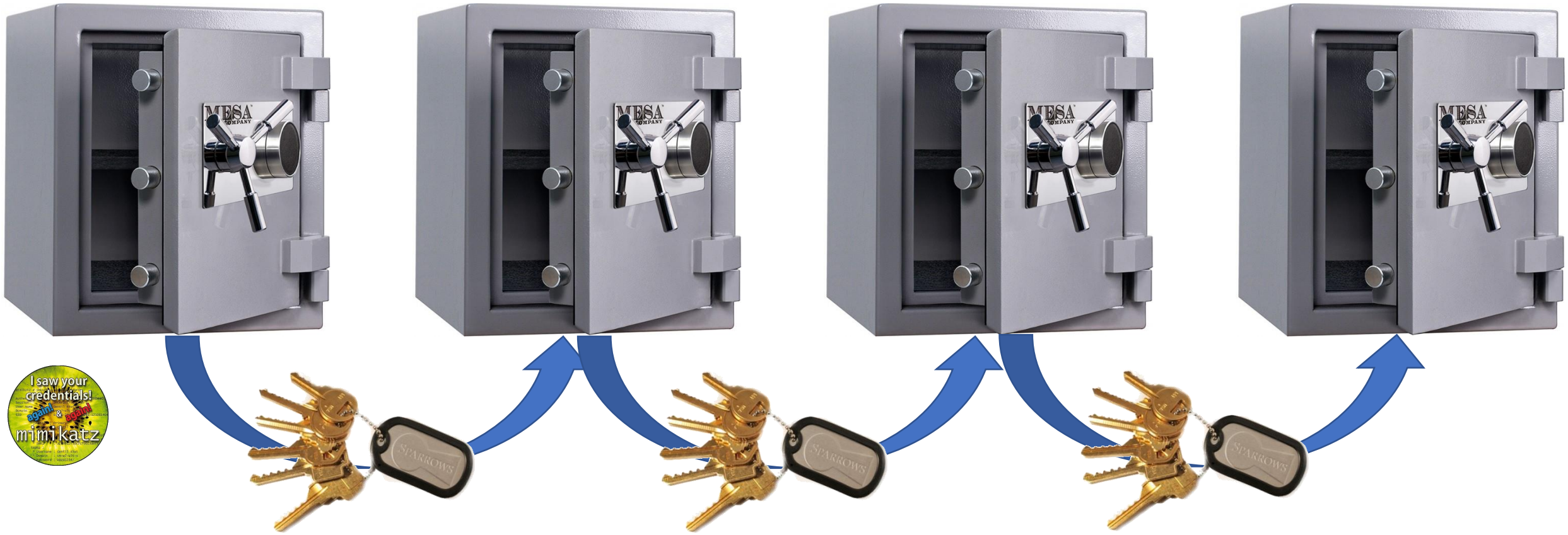




In short: the golden ticket factory

Previous chapter

How it works: 2/2

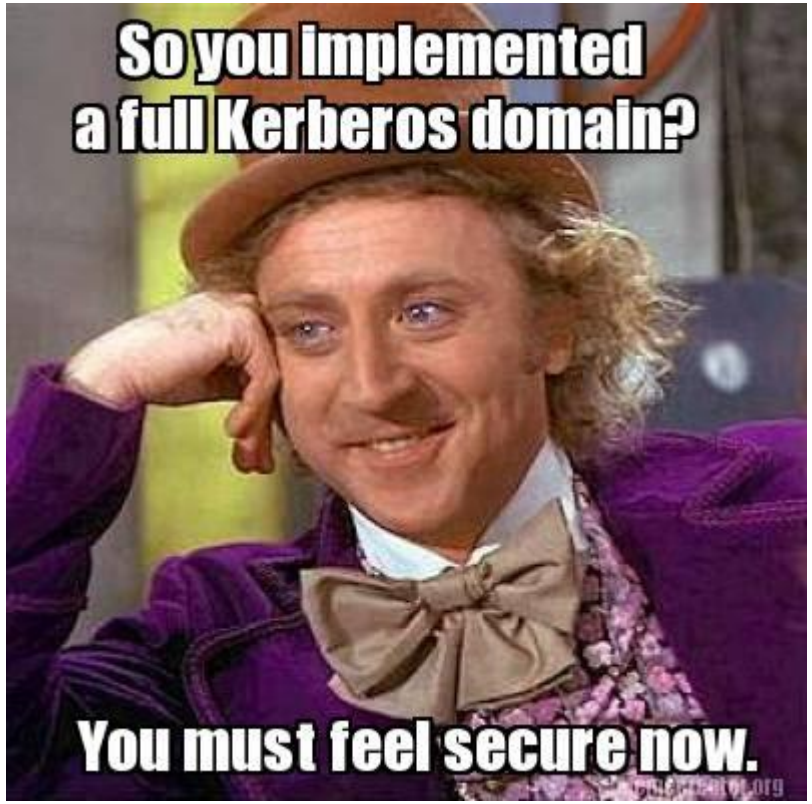


1) Retrieve the credentials to open the first « safe »
2) Then abuse it to get other credentials to open other safes

Quickest way to propagate to other domains

The root causes

- It is not about credential / authentication but about AD **secret managment**
- It is about **network seggregation**
- It is about having **unknown trust relationship** with other domains



Is a technical project the solution?

Demo 4: And … trust are not a strict border

HOW TO « DETECT » MIMIKATZ ?

Rule #1: accept you can't

You don't need mimikatz to be mimikatzed

Attacks implemented in other tools. Example:

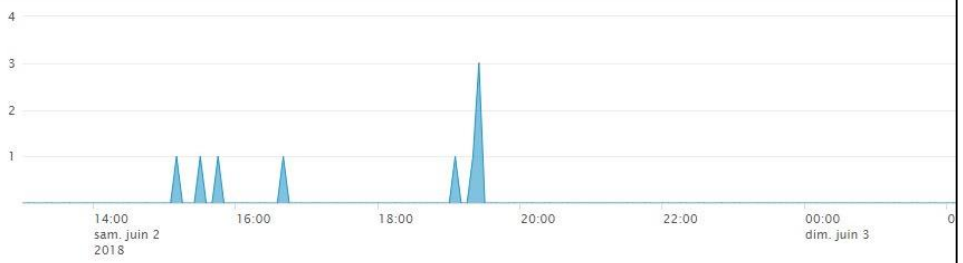
- Credential dump: Quarks PwDump
- DCSync: secretsdump.py from Impacket
- Kerberos, DPAPI: GhostPack
- DCSync, Golden ticket: MakeMeEnterpriseAdmin

- New mimikatz: kekeo !

Rule #2: apply the author recommendations

```
/*      Benjamin DELPY `gentilkiwi`
        http://blog.gentilkiwi.com
        benjamin@gentilkiwi.com
        Licence : https://creativecommons.org/licenses/by/4.0/
*/
rule mimikatz
{
        meta:
                description              = "mimikatz"
                author                   = "Benjamin DELPY (gentilkiwi)"
                tool_author              = "Benjamin DELPY (gentilkiwi)"
```

DSTime	Computer	DSUserSid	DSDomainName	DSUserName	DSObjectType	DSObjectName	DSS
06/02/2018 19:28:53	dc.lab.local	NONE_MAPPED	LAB	SilverTicketUser	domainDNS	DC=lab,DC=local	succ
06/02/2018 19:26:21	dc.lab.local	NONE_MAPPED	LAB	GoldenTicketUser	domainDNS	DC=lab,DC=local	succ
06/02/2018 19:25:06	dc.lab.local	NONE_MAPPED	LAB	GoldenTicketUser	domainDNS	DC=lab,DC=local	succ
06/02/2018 19:22:26	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	succ
06/02/2018 19:09:12	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	succ
06/02/2018 16:40:28	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	succ
06/02/2018 15:45:26	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	succ
06/02/2018 15:33:50	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	succ
06/02/2018 15:10:13	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	succ



Do you know @gentilkiwi published yara rules ?

Same for DCSync Detection ?

Check out (and adapt)
https://gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2

Rule #3: Know your scope !

I'm still surprised to see companies that :

- Do not know how much AD they have
- Cannot list open shares (with passwords) or local admins
- Have still some MS17-010 unpatched

My gift to the community:
https://www.pingcastle.com

PING CASTLE

CONCLUSION

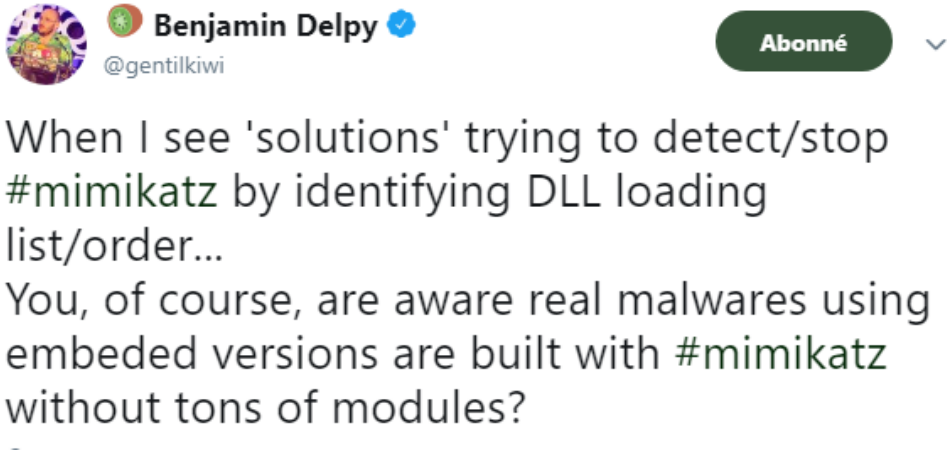
Mimikatz is a brand

You cannot fight an image

http://github.com/gentilkiwi/mimikatz
http://github.com/vletoux/pingcastle
@mysmartlogon

And for techies

- You can (sometimes) detect mimikatz as a whole application



- But maybe you should understand the attack behind rather than looking for a tool…