

# REDACTED

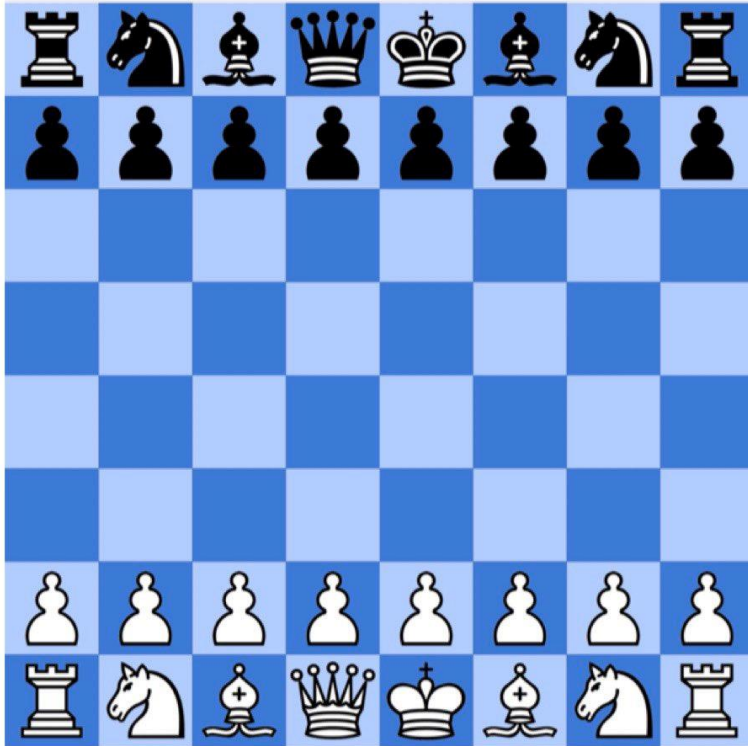
REDACTED



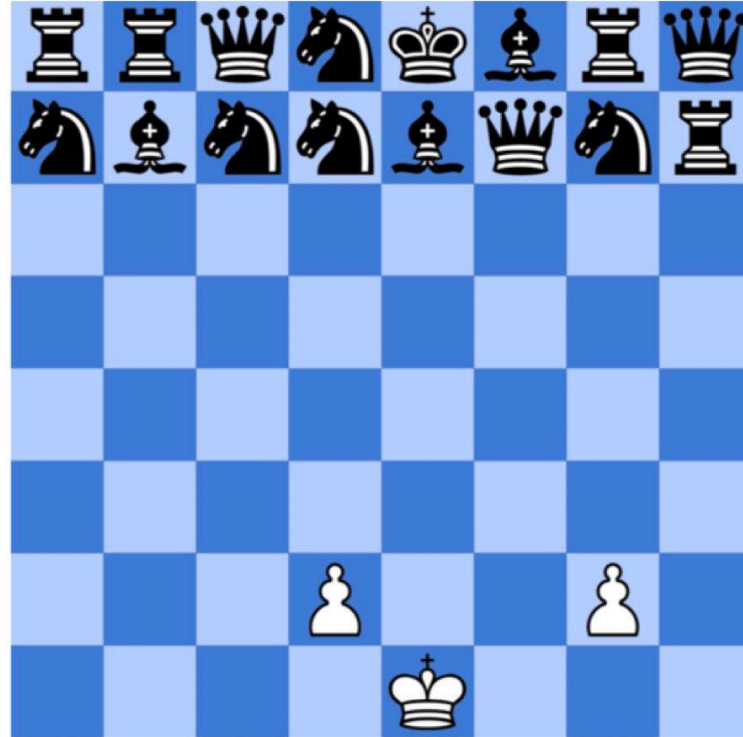
**BENJAMIN MOSSE**

2020





## Theory



## Real world

Typical comments include:

- ❖ No budget
- ❖ No management support
- ❖ Outdated technology
- ❖ Not enough technology
- ❖ Not enough people
- ❖ People not skilled enough
- ❖ Too much red tape
- ❖ Mismanagement of risks
- ❖ Cyber fraud

# BEST PRACTICES vs. BUSINESS CONSTRAINTS

## (a short list of examples)

Risk Appetite

Cost

ROSI

Ease of  
Implementation

Implementation  
Time

Knowledge &  
Skills

Strategic Fit

Labour &  
Resource Issues

Research and  
Development

Quality

Productivity

Governance



# LESSON #1

## COMMIT TO MASTERING THE "BUSINESS" SIDE OF CYBER

Ask questions and establish a dialog with key stakeholders

Negotiate

Achieve a consensus

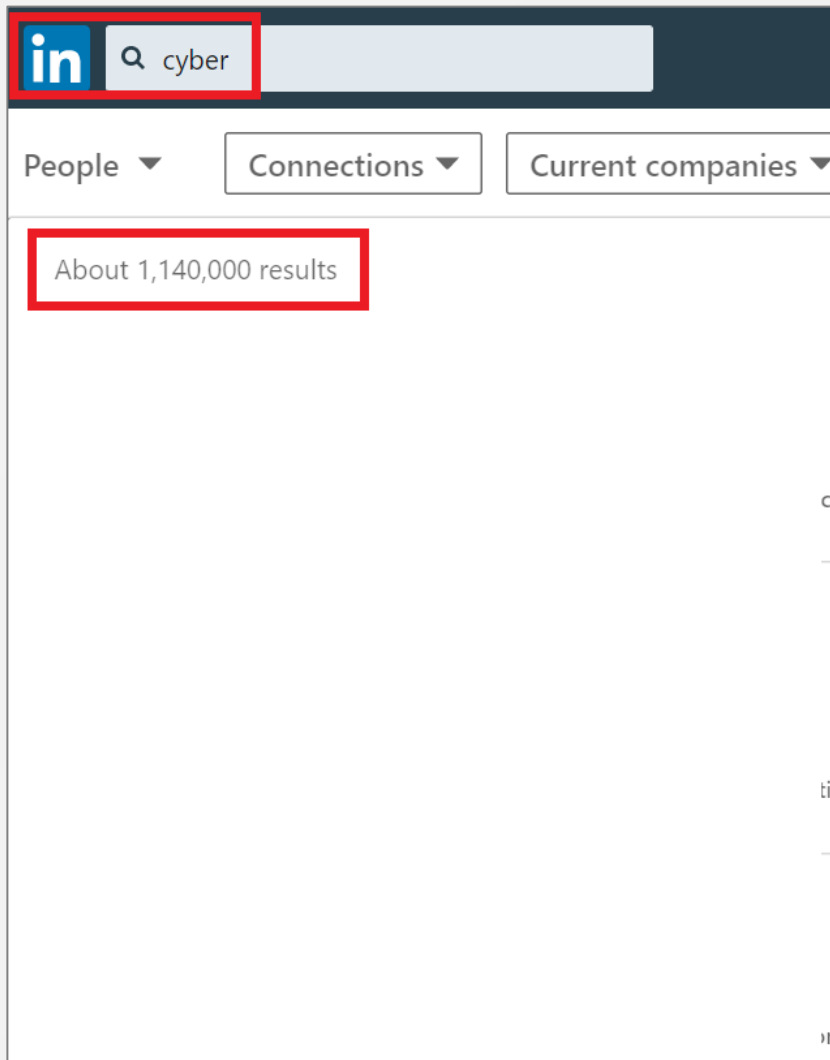
Hold yourself and them accountable

Work for the long-term



# DIFFERENT WAY OF THINKING #1

## 1,140,000 "professionals" vs. 100 malware authors



A screenshot of the LinkedIn search interface. The search bar at the top contains the word "cyber" and is highlighted with a red box. Below the search bar, there are three filter buttons: "People", "Connections", and "Current companies". Below these filters, a red box highlights the text "About 1,140,000 results".

### Only 100 cybercrime brains worldwide says Europol boss

10 October 2014



Troels Oerting (right) believes that there are a limited number of skilled malware producers

There are only "around 100" cybercriminal kingpins behind global cybercrime, according to the head of Europol's Cybercrime Centre.

Speaking to the BBC's Tech Test radio show, Troels Oerting said that law enforcers needed to target the "rather limited group of good programmers".

"We roughly know who they are. If we can take them out of the equation then the rest will fall down," he said.



# LESSON #2

## CHALLENGE THE STATUS QUO

Challenge what you've been taught

Challenge the industry's authority figures

Challenge the industry best practices

Evolve fast and develop new ways of operating

# DIFFERENT WAY OF THINKING #2: Millions of Dollars vs. \$0

<b>ANTI FRAUD &amp; IDENTITY MANAGEMENT</b> 				<b>MOBILE SECURITY</b> 	
<b>PREDICTIVE INTELLIGENCE</b> 		<b>BEHAVIORAL ANALYTICS / ANOMALY DETECTION</b>  		<b>AUTOMATED SECURITY</b> 	
<b>APP SECURITY</b> 		<b>IOT SECURITY</b> 		<b>DECEPTION SECURITY</b> 	



```
Empire: PowerShell post-exploitation agent | [Version]: 1.0.0
[Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub

EMPIRE

90 modules currently loaded
0 listeners currently active
0 agents currently active
```

```
95 auxilliary/encode/encode -u http://10.10.10.10:8080/ -p 'POST' -e 'base64' -t 'http://10.10.10.10:8080/'
295 exploit/multi/http/wordpress_rce -u http://10.10.10.10:8080/ -p 'POST' -e 'base64' -t 'http://10.10.10.10:8080/'
35 payload/wordmap/wordmap -u http://10.10.10.10:8080/ -p 'POST' -e 'base64' -t 'http://10.10.10.10:8080/'
```

```
PS C:\mimikatz\mimikatz_trunk\64\ - .\mimikatz.exe
##### mimikatz 2.1 (x64) built on Mar  5 2017 22:41:35
## A ## "A la Vie, a L'Amour"
## \ ## /s = "
## \ ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz (oe,oe)
##### with 20 modules * * *

mimikatz # privilege:debug
Privilege '20' OK

mimikatz # sekurlsa:pth /user:jeff /domain:jefflab.com /ntlm:d4dad8b9f8ccb87f6d6d02d7388157ea
user : jeff
domain : jefflab.com
program : cmd.exe
listeners : no
NTLM : d4dad8b9f8ccb87f6d6d02d7388157ea
PID 4240
TID 5608
LSA Process is now R/W
LUID 0 - 12683024 (00000000:00c138f0)
msv1_0 - data copy @ 0000020830f9880 : OK !
kerberos - data copy @ 00000208316b778
aes128_hmac -> null
rc4_hmac_nt - OK
rc4_hmac_old -> null
rc4_md4 - OK
rc4_hmac_nt_exp - OK
rc4_hmac_old_exp - OK

mimikatz # _
```

# MimiKatz

We know of organisations that spend 100M per year on cyber security and that can't stop a penetration tester with Metasploit



# LESSON #3

## KEEP IT SIMPLE

Use what's already available onsite

Don't rely on major network upgrades

Use simple, small tools that can easily be approved



# EXAMPLES

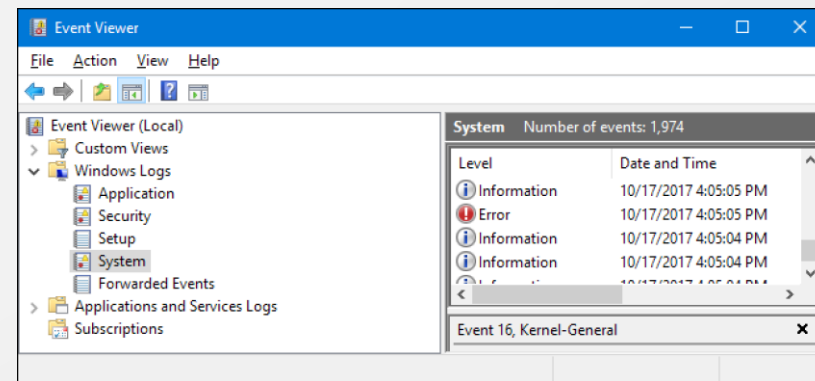


```

C:\Users\jorj> get-command -name service

CommandType Name             Version Source
-----
Cmdlet       Get-Service             1.1.0 Microsoft.PowerShell.Management
Cmdlet       New-Service              1.1.0 Microsoft.PowerShell.Management
Cmdlet       Remove-Service           1.1.0 Microsoft.PowerShell.Management
Cmdlet       Set-Service              1.1.0 Microsoft.PowerShell.Management
Cmdlet       Stop-Service             1.1.0 Microsoft.PowerShell.Management
Cmdlet       Suspend-Service          1.1.0 Microsoft.PowerShell.Management
  
```

**Windows Powershell**



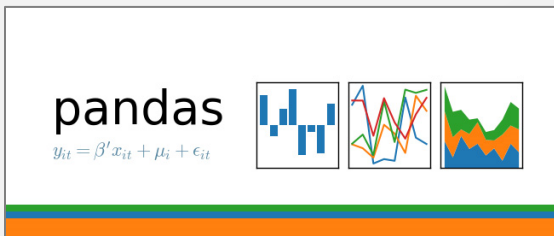
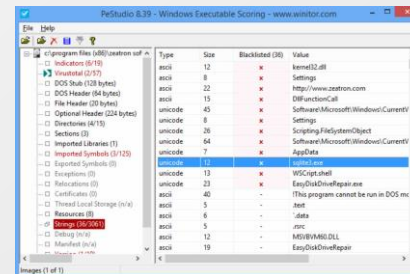
```

C:\WINDOWS\system32\cmd.exe - DumpIt.exe -h
04/12/2006 17:53 105 264 pspasswd.exe
27/04/2010 11:04 169 848 PsService.exe
04/12/2006 17:53 207 664 psshutdown.exe
04/12/2006 17:53 187 184 psuspend.exe
10/02/2007 09:46 64 126 Pstools.chm
06/11/2007 09:17 39 psversion.txt
18/07/2011 13:29 17 fichier(s) 3 222 169 octets
 2 Rép(s) 2 563 469 312 octets libres

C:\remotetools>DumpIt.exe -h
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size: 536870912 bytes < 512 Mb>
Free space size: 2563469312 bytes < 2444 Mb>

* Destination = \\?\C:\remotetools\OZ-C06A6A6F2D3C-20121022-172945.raw
-> Are you sure you want to continue? [y/n] y
+ Processing... Success.
  
```



# DIFFERENT WAY OF THINKING #3

## SOC vs. 1 Malware Developer



Every org's wet dream



Benjamin Delpy – Author of Mimikatz



# LESSON #4

**EXPERTISE > NB. OF PEOPLE > TOOLS**

10 000 hours of training minimum, over 10 years

Every single domain of CYOPS

100% practical and focused on solving real-world problems



# SUMMARY: "Professionals" vs. APT

"PROFESSIONALS"	APT
Complex	Simple
Broad	Targeted
Long OODA loop	Short OODA loop
Large and slow-moving	Small and agile
Decision paralysis	Rapid decision making
Politics	Mission
Technology	Skills
Disorganised	Prioritized
Unclear	Clear

**Develop attitudes, mindsets and tradecraft similar to the APTs**



# CONTACT US

Benjamin Mossé

CEO, Mossé Security

[contact@mosse-security.com](mailto:contact@mosse-security.com)





# REFERENCES

1. <https://twitter.com/craiu/status/1301454498288799745>
2. <https://kapitanhack.pl/2019/05/09/czarne-biale-kapelusze/benjamin-delpy-gentilkiwi/>
3. <https://www.bbc.com/news/technology-29567782>
4. <https://www.cbinsights.com/research/cybersecurity-artificial-intelligence-startups-market-map/>