

Cyber Threat Intelligence

From 0 to h3r0

Nino Verde, PhD

Antonio Villani, PhD

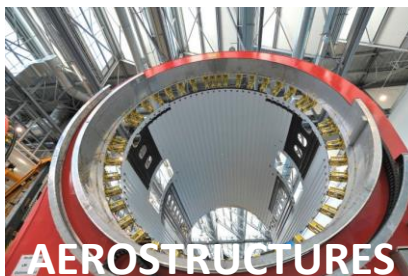
March 24th, 2021






Who are we?

- About Leonardo:
 - Aerospace, defence and security sector
 - One of the largest defence contractor in the world



- We work for the **Cyber Security Research Center – Product & Technology Development**

- About us:
 - Nino Verde, PhD:
 - Senior Cyber Security Architect
 - Cyber Threat Intelligence Analyst, Incident Reponse
 - Antonio Villani, PhD:
 - Senior Cyber Security Architect
 - Endpoint protection, Reverse Engineering

 @verdenino

 @t0nvi



WARNING

This is not a Webinar!!!

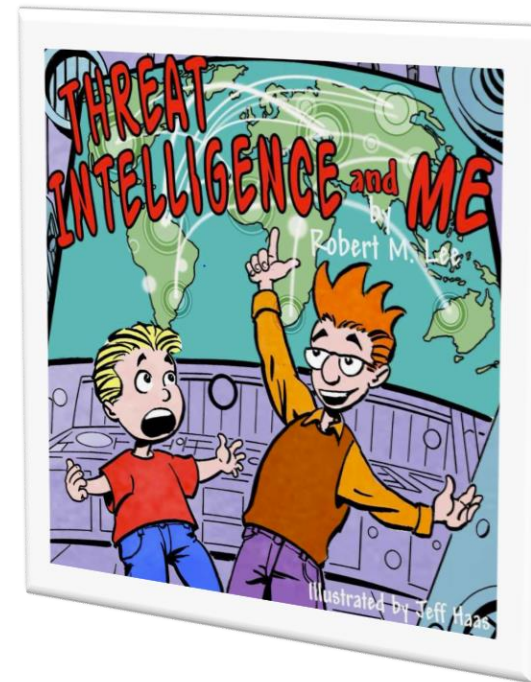


This is a gaminar!

- Open joinmyquiz.com with your mobile phone, desktop or notebook
- Enter the following join code: **342 815**
- Play with us!
- The winner will receive one of the best books about Threat Intelligence



When this icon appears on a slide it is time to play!



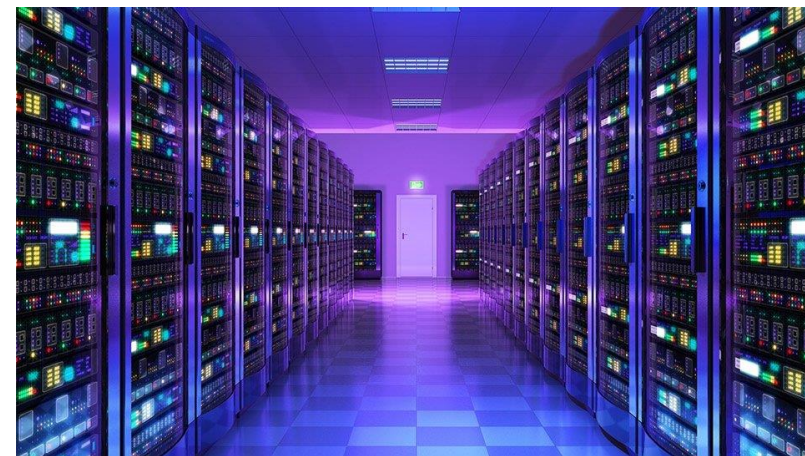
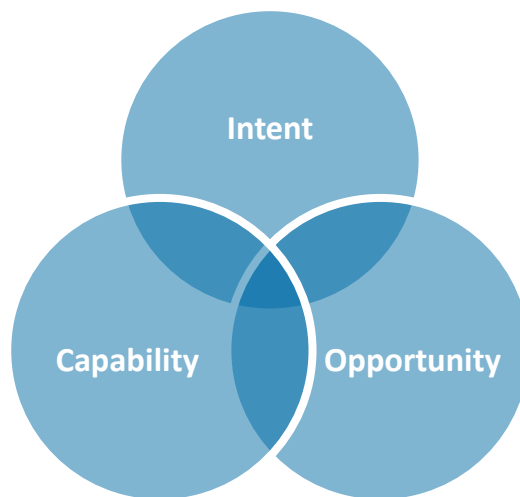


Cyber

Threat

Intelligence

“Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool – and therefore strange, spooky.” [New York magazine, Dec. 23, 1996]





Why do companies want threat intelligence?

Start from monitoring and response

Help C-level make good decisions – reduce uncertainty

TI doesn't address all existing problems



CTI Platforms





Finally... a definition of cyber threat intelligence

- Threat Intelligence is:
 - “Analyzed information about adversaries who have the Intent, Opportunity and Capability to do you harm.”
 - “Analyzed information about the hostile intent, capability, and opportunity of an adversary that satisfies a requirement”
 - “the products and processes across the intelligence cycle of assessing the capabilities, intentions, and activities – technical and otherwise – of potential adversaries and competitors in the cyber domain (with cyber counterintelligence as a sub-discipline).”
 - **Note:**
 - Actionability of an intelligence product is a must!
 - At the end, intelligence must reduce uncertainty
- Things to remember always:
 - The threat is another human!
 - The malware is just a capability of the adversary
 - Organization sharing their internal threat information with each other can help community understand the largest threat landscape
 - Be careful to not overvalue attribution!
 - It is determining who was responsible for a cyber attack
 - Mmm... isn't it always Russia or China?



Process Considerations: Organizational context



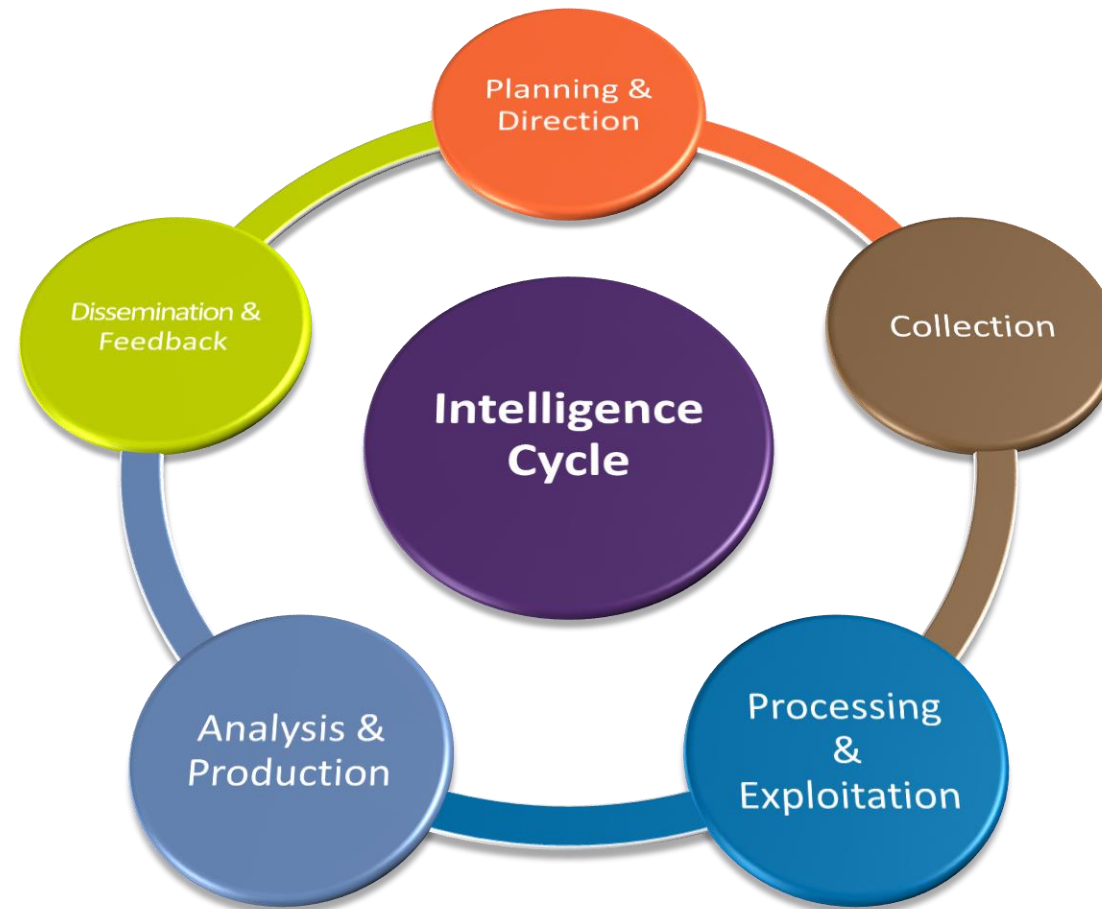
- Understand the **assets** of your organization **and their value**
- Identify **threat actors** motivated to access or harm your assets
- Determine **methods** common to relevant threat actors who may target your organization and its assets
- Establish **monitoring and hunting processes** aligned with the most likely avenues of compromise
- **Monitoring adversaries**, their activities, and interests continuously, and map these against your changing business activities that may alter your appeal as a target

Cyber Threat Intelligence

Concepts and models

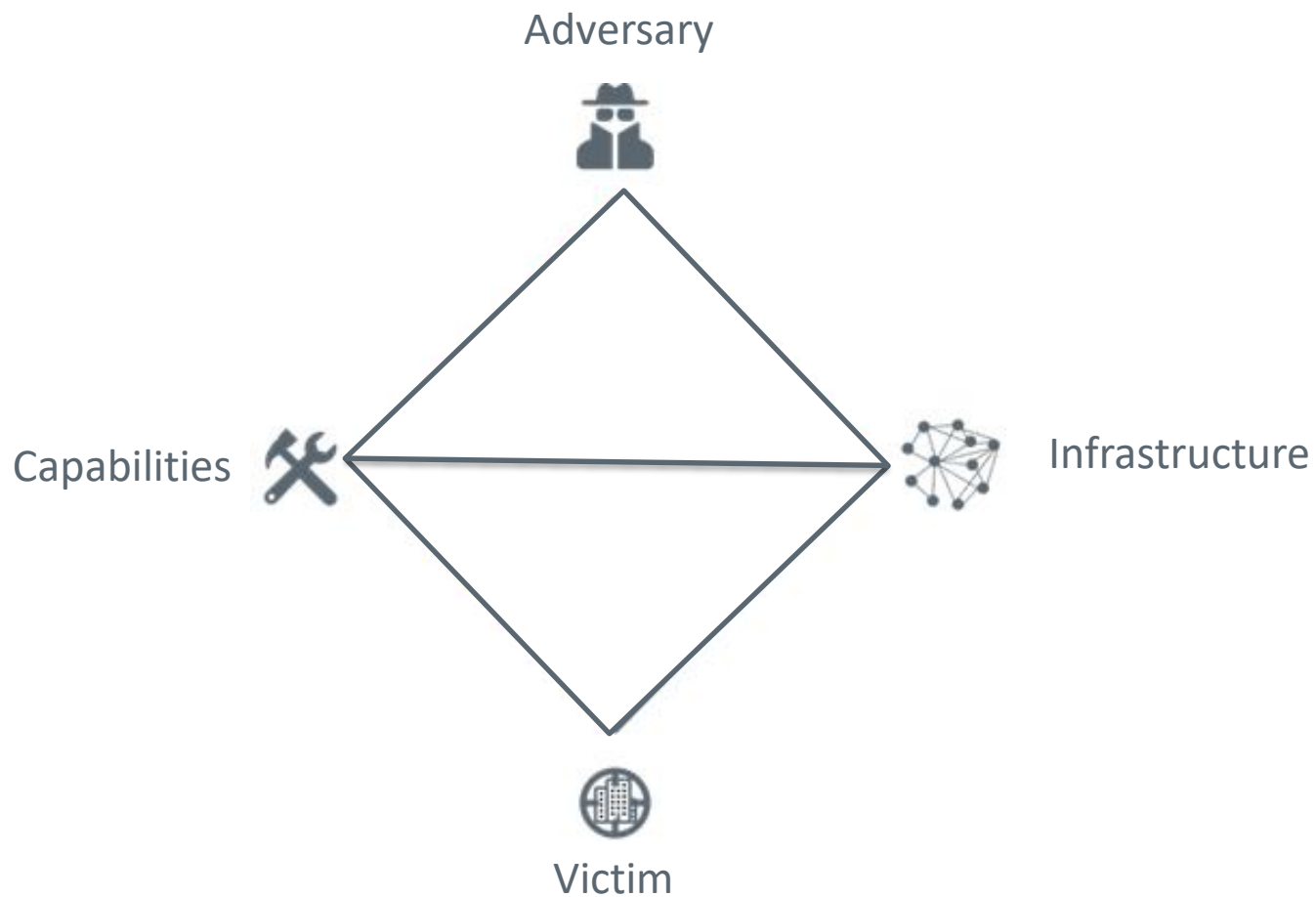


Please, welcome the intelligence cycle!





The diamond model of intrusion analysis

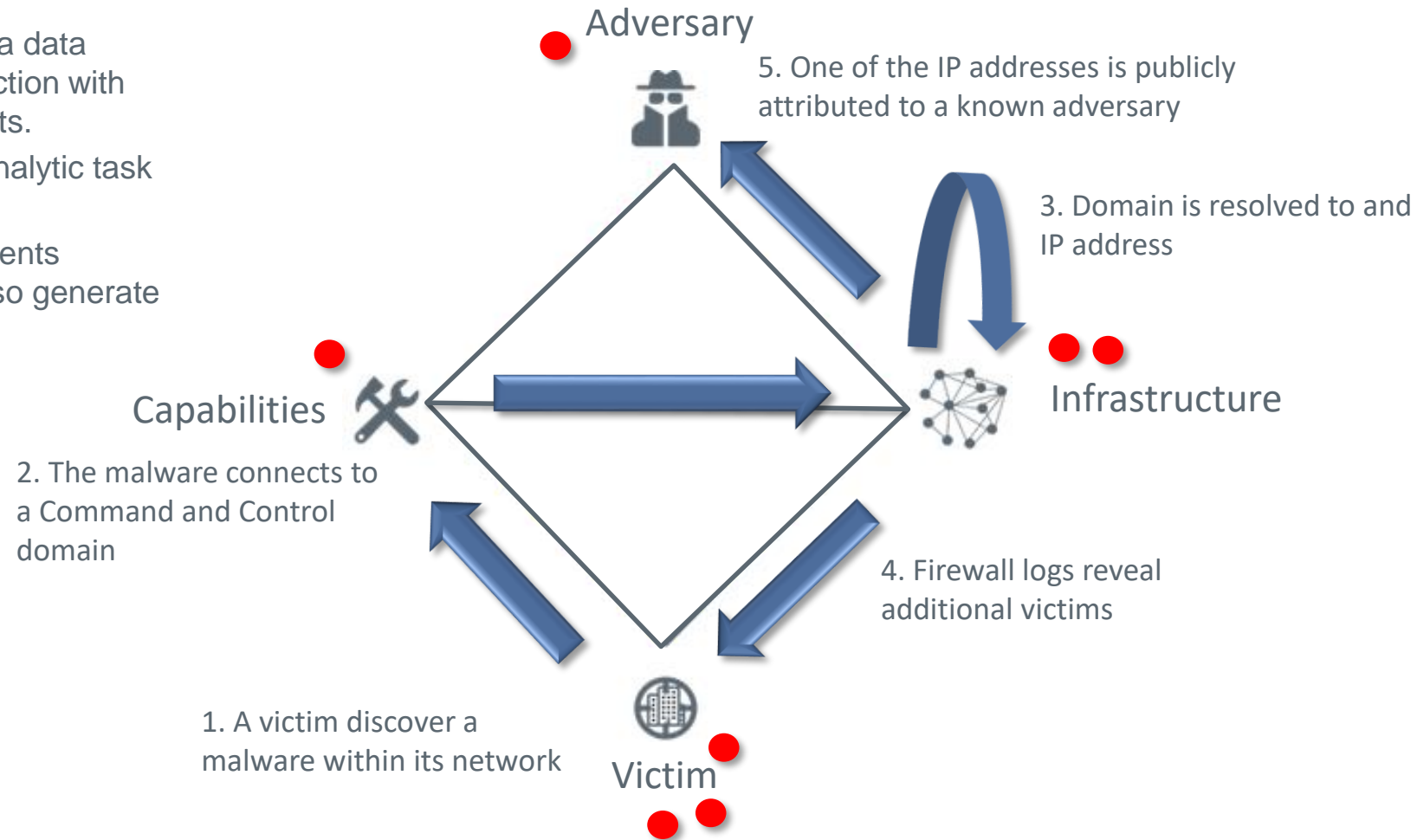


Sergio Caltagirone, Andrej Pendergast, Christofer Bets, <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>



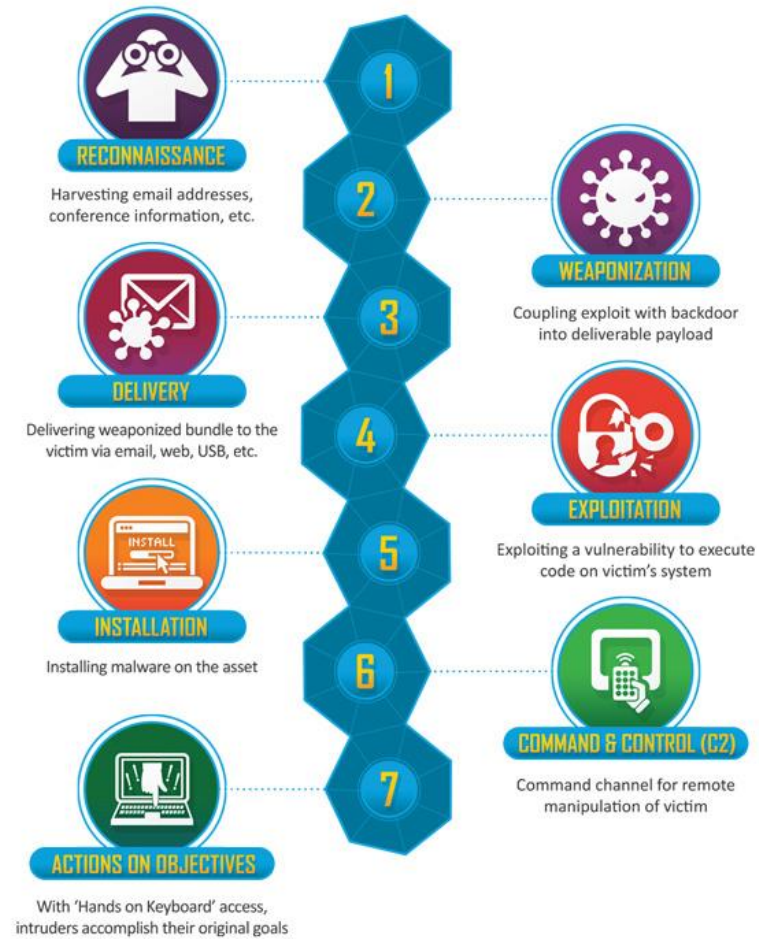
Pivoting

- Pivoting is the analytic technique of extracting a data element and exploiting that element, in conjunction with data sources, to discover other related elements.
- Ultimately, pivoting is about the fundamental analytic task of hypothesis testing.
- Pivoting is the task of discovering related elements (evidence) which inform the hypothesis and also generate new hypotheses themselves



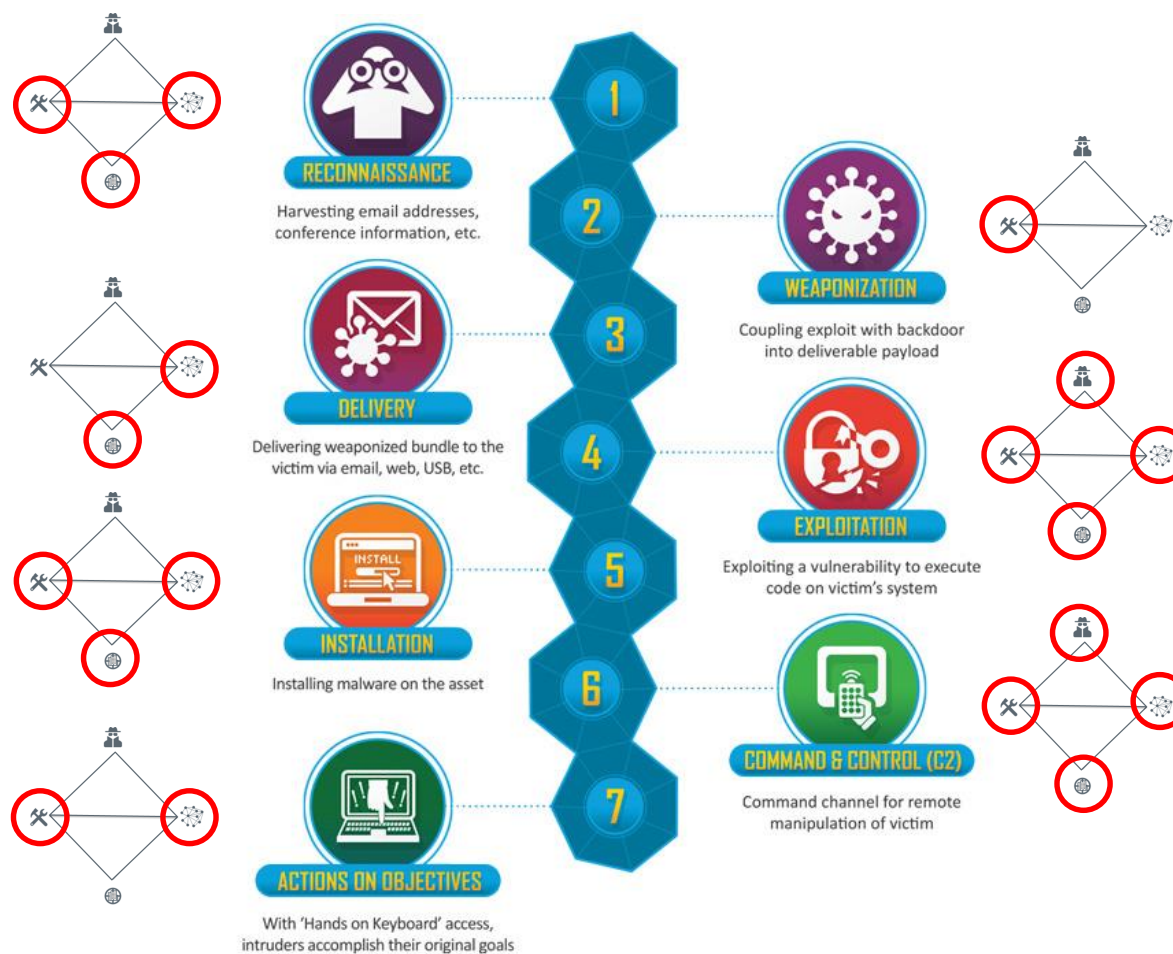


Killchain of intrusion analysis



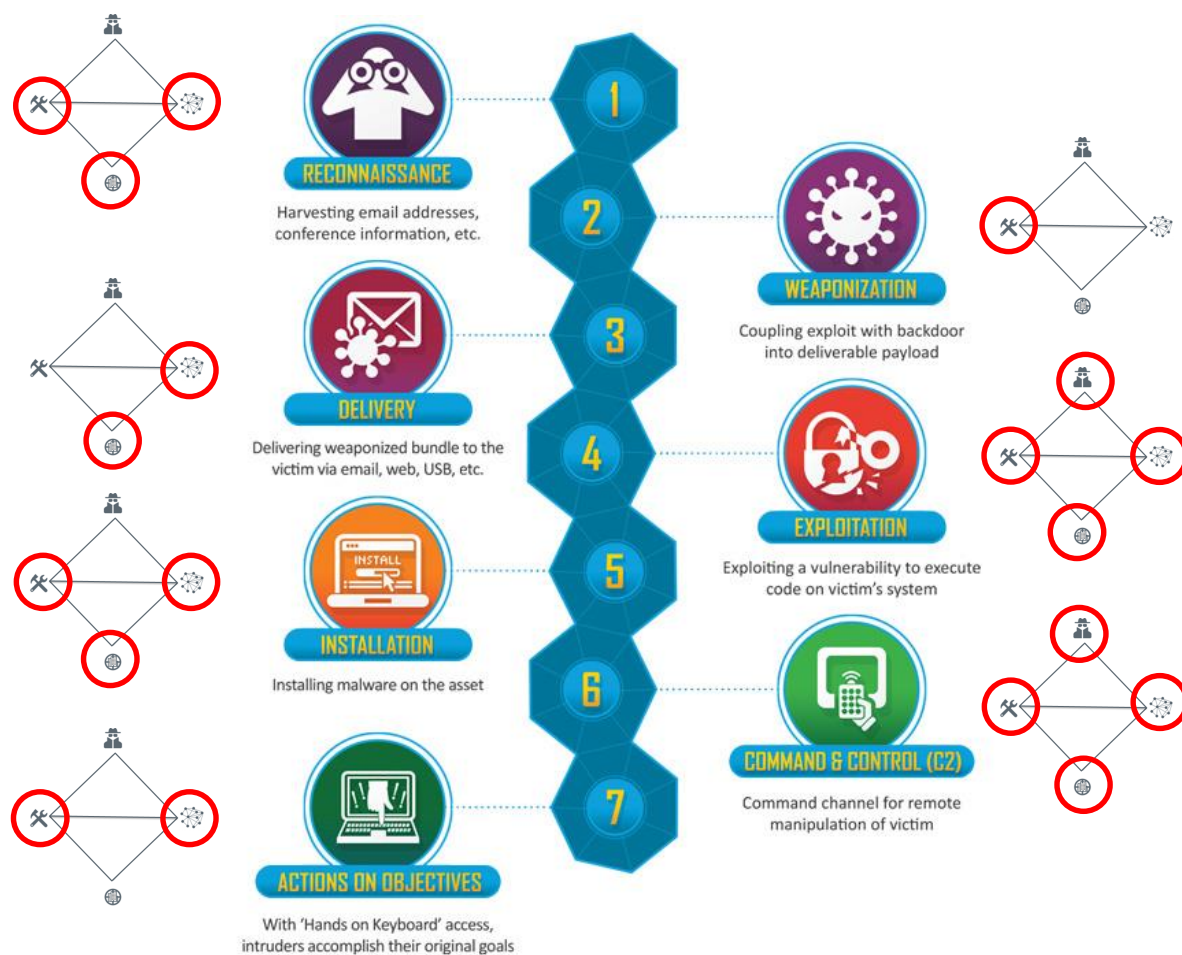


Organizing data into buckets





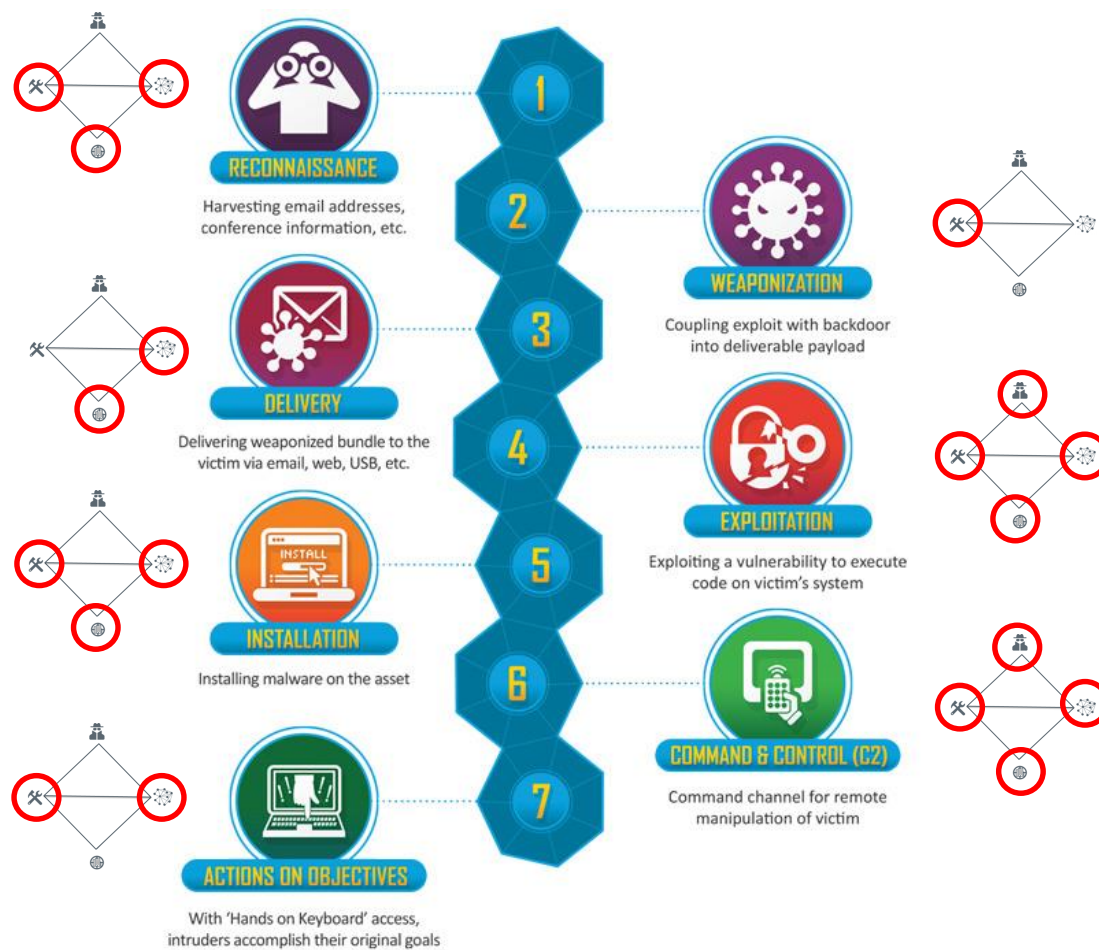
Organizing **more** data into buckets





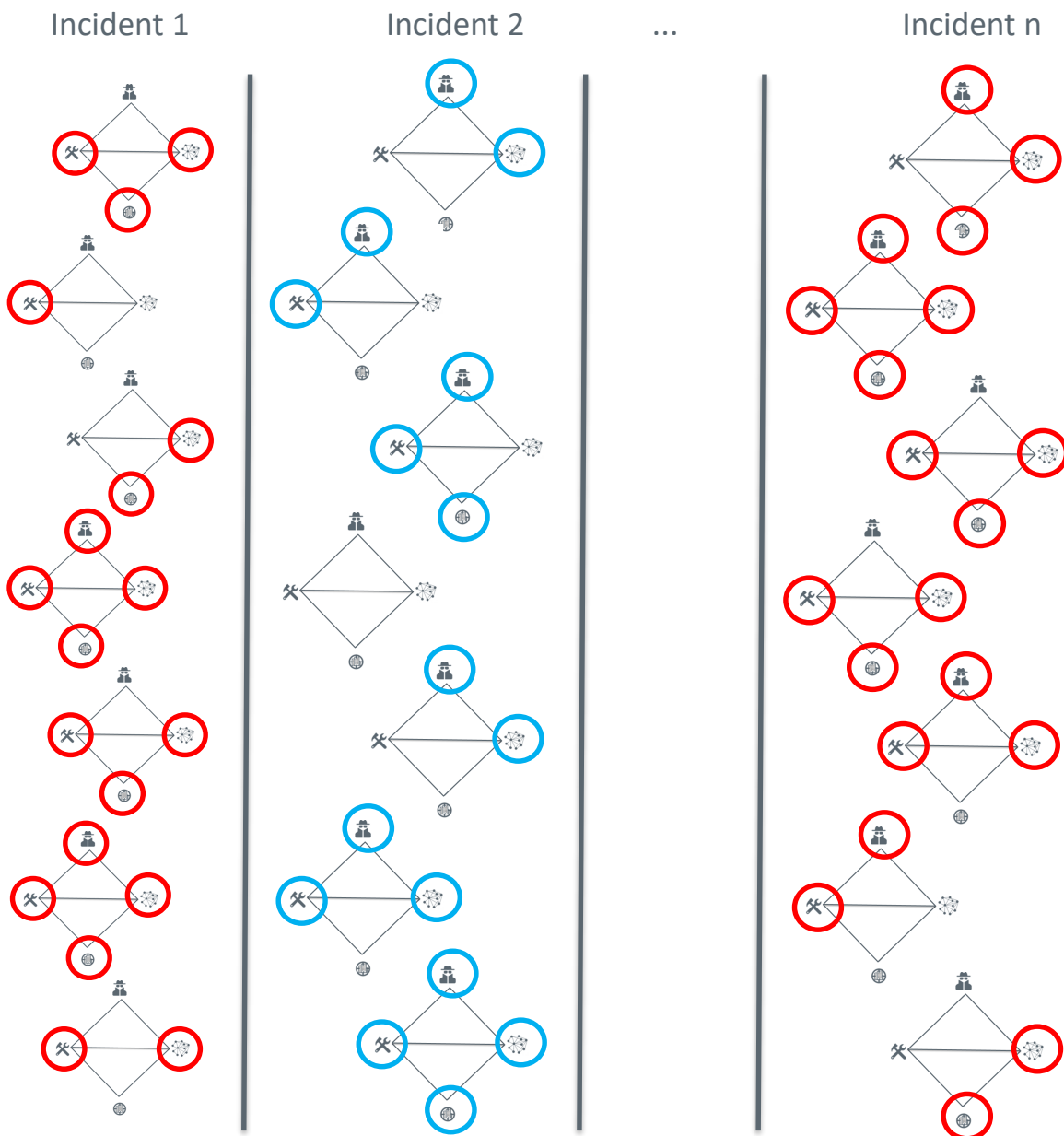
Incident 1

R
W
D
E
I
C
A





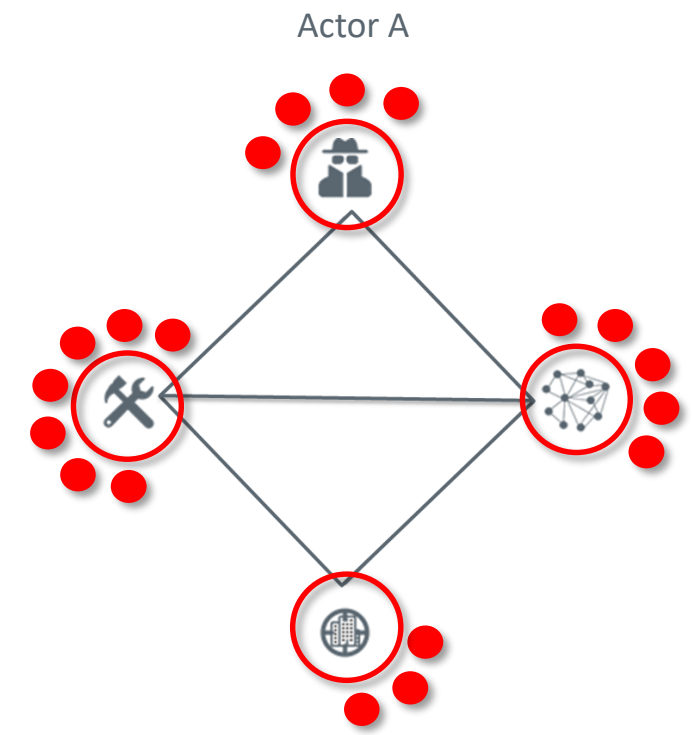
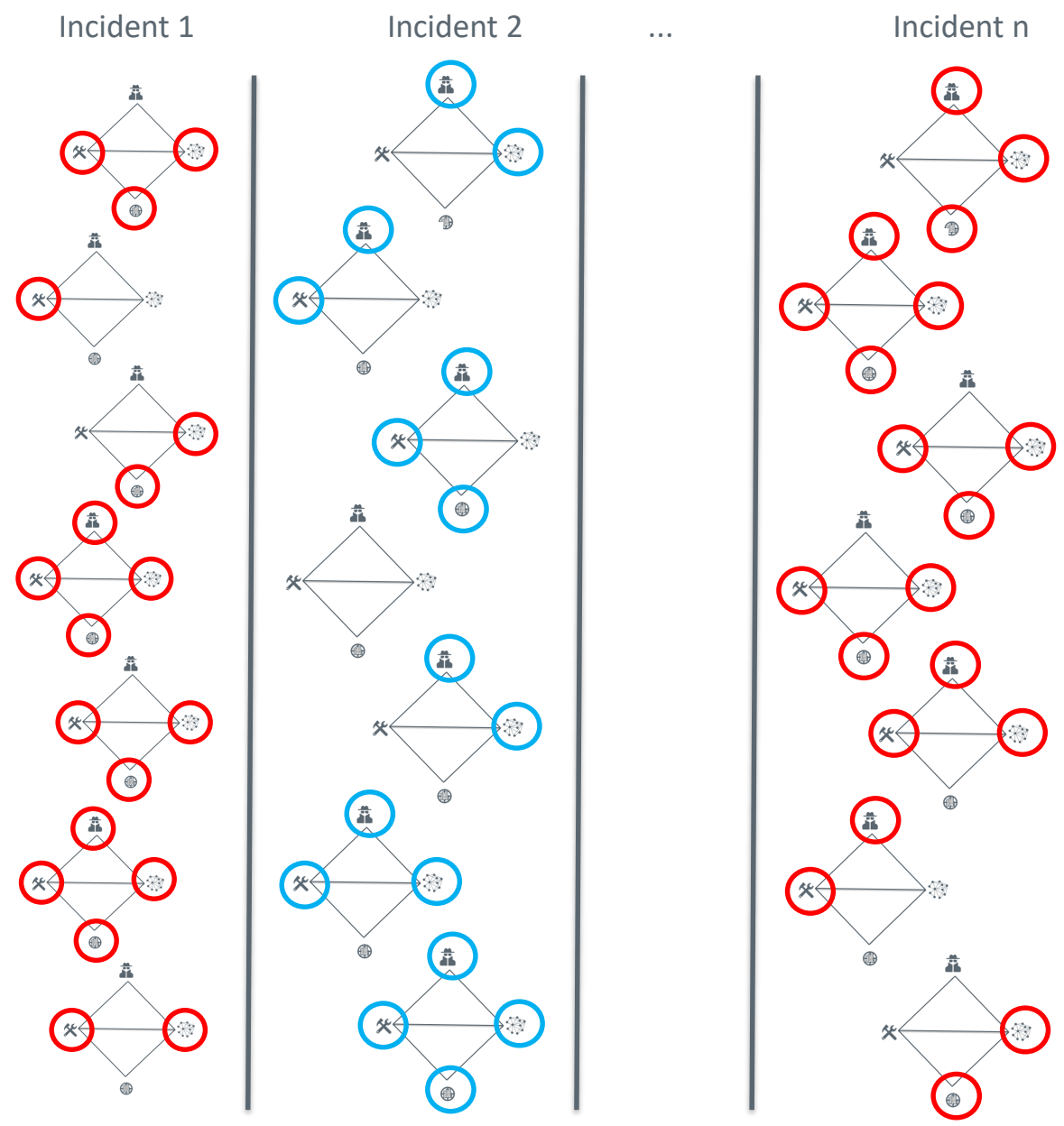
R W D E I C A



-  Suspected Actor A
-  Suspected Actor B



R W D E I C A



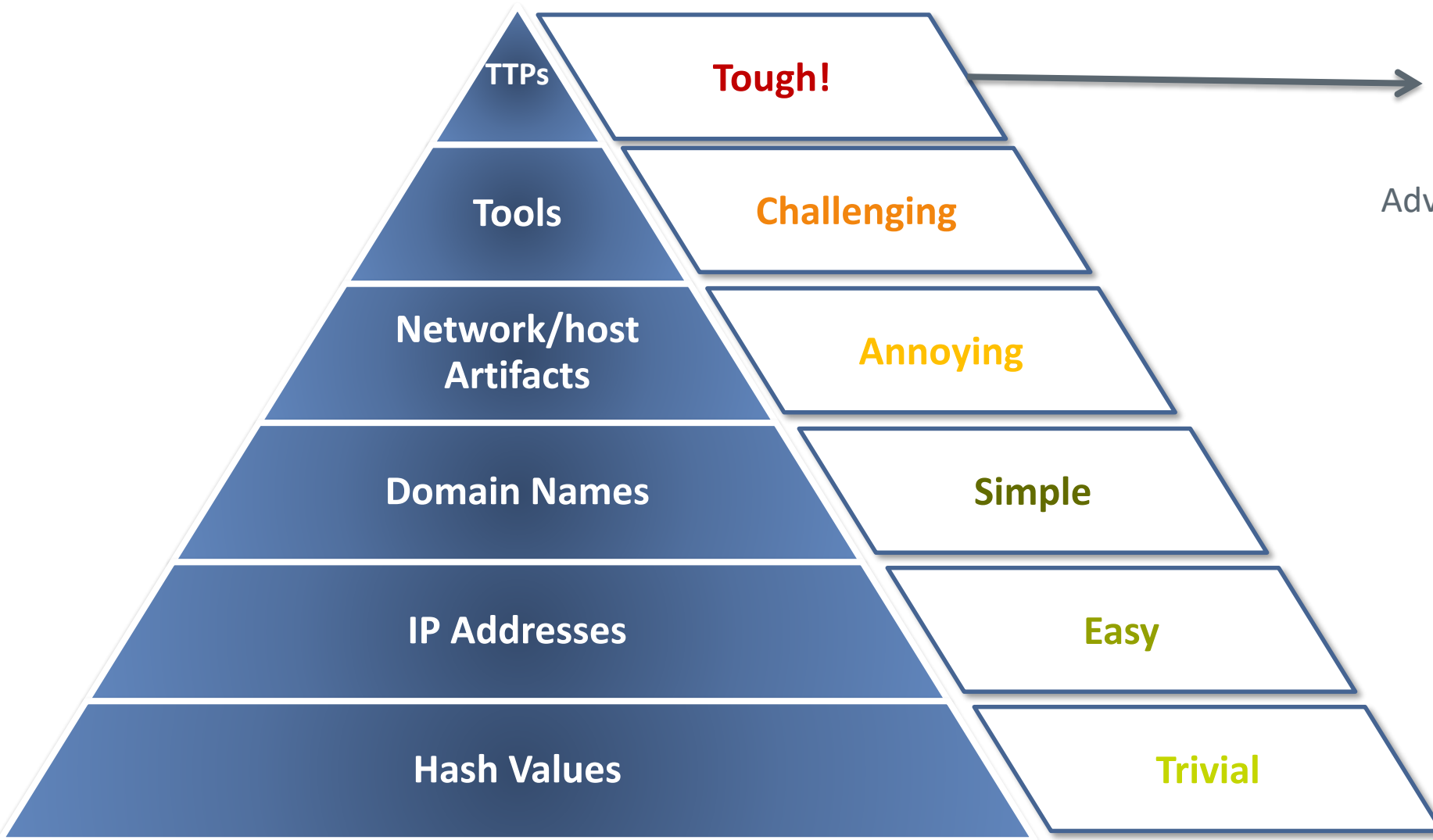
- Suspected Actor A
- Suspected Actor B



Actionable Intelligence

- We learned:
 - How important is to organize data with a structured model (es. diamond model and killchain)
 - How important is to investigate incidents leveraging well defined models and processes (es. Pivoting)
 - How important is to work with internal data
- At this point we should be able to collect and organize data
- How to use this knowledge?
 - Try to answer the following Information Requests:
 - Is our organization a possible target of actor X?
 - Which are the attackers we should take care of?
 - Do our network logs show any sign of compromise by Actor Z?
 - Are we prepared to defend ourselves from Actor Y?

Pyramid of pain



MITRE
ATT&CK™

Adversarial Tactics, Techniques
& Common Knowledge



MITRE Att&ck matrix



Techniques of Actor Y

Data sources available and detection rules deployed

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques
<div style="border: 1px solid red; padding: 2px;">Active Scanning (2)</div> Gather Victim Host Information (4)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	<div style="border: 1px solid red; padding: 2px;">Account Discovery (4)</div>	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Auto Exfiltration
Gather Victim Identity Information (3)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Abuse Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Size
Gather Victim Network Information (6)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocols
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over Channel
Phishing for Information (3)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over Network Media
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Network Media
Search Open Technical Databases (5)	Supply Chain Compromise (3)	Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Media
Search Open Websites/Domains (2)	Trusted Relationship	Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Exfiltration Over Services
Search Victim-Owned Websites	Valid Accounts (4)	Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Permissions Modification (2)	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over System Channels
			Windows Management Instrumentation			Hide Artifacts (7)	OS Credential Dumping (8)	Hide Artifacts (7)		Data from Removable Media	Multi-Stage Channels	Schedule Task
						Hijack Execution Flow (11)	Steal Application Access Token	Hijack Execution Flow (11)		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account
						Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Impair Defenses (7)		Data Staged (2)	Non-Standard Port	
						Indicator Removal on Host (6)	Steal Web Session Cookie	Indicator Removal on Host (6)		Email Collection (3)	Protocol Tunneling	
						Indirect Command Execution	Two-Factor Authentication Interception	Indirect Command Execution		Input Capture (4)	Proxy (4)	
						Masquerading (6)		Masquerading (6)		Man in the Browser	Remote Access Software	
						Modify Authentication Process (4)		Modify Authentication Process (4)		Man-in-the-Middle (2)	Traffic Signaling (1)	
						Modify Cloud Compute Infrastructure (4)		Modify Cloud Compute Infrastructure (4)		Screen Capture	Web Service (3)	
						Modify Registry		Modify Registry		Video Capture		
						Modify System Image (2)		Modify System Image (2)				
						Network Boundary Bridging (1)		Network Boundary Bridging (1)				
						Obfuscated Files or Information (4)		Obfuscated Files or Information (4)				



How to learn more about CTI?

- There are several important topics we didn't speak about here:
 - Cognitive biases
 - Exploring hypothesis
 - Knowledge gaps
 - ... and many more!
- Professional training
 - SANS FOR578: CYBER THREAT INTELLIGENCE
 - Threat Intelligence Academy of Sergio Caltagirone
- Self study
 - Read books, and CTI reports – see suggested reading at the end of this presentation
 - Follow people from the CTI community
 - Take a look at Katie Nickels's suggestions on medium¹ - Twitter account: @likethecoins
- Gain experience as Security Operation Center operator, Incident Responder, Malware Analyst and then move to the CTI team

1. <https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a>

Cyber Threat Intelligence

Uncovering the traces of State Sponsored Threat Actors: A case study on Turla

Silvio La Porta, PhD

Nino Verde, PhD

Antonio Villani, PhD



Turla - Identikit of the adversary



WHO IS IT?  Russian based threat group active since 2004 at least

ALIASES  Snake – WhiteBear – Venomous Bear – Uroburos – Waterbug

THREAT TYPE  State Sponsored

SOPHISTICATION  Innovator

VICTIMOLOGY  Defense
Government
Embassies
Education
Research
Pharmaceutical Companies
More than 45 Countries

INTENT

To foster Russian interests and its foreign affairs

OPPORTUNITIES

Use any technological mean and discovered vulnerability.

CAPABILITIES

It is known for: leveraging satellites connections to hide their traces, conducting watering hole and spearphishing campaigns, in-house tools and malware.



Turla's - Features



Skilled Cyber Operators
Opsec masters!



Stealthiness
Steganography
Piggibacking



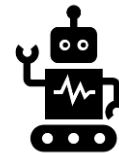
Compromised Servers
Targeting vulnerable hosting providers



Versatility
Adapting sophistication level



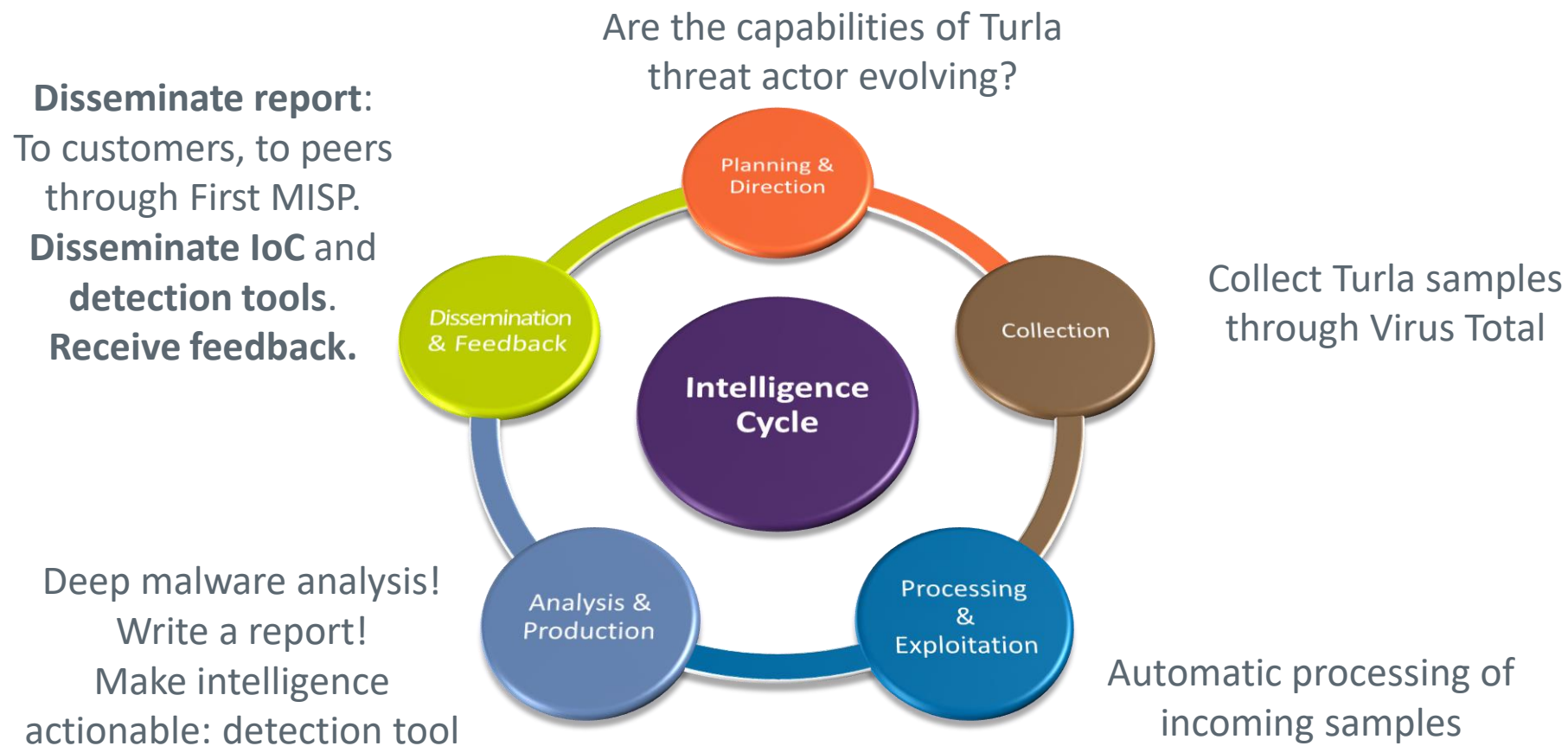
Anonimization Network
Peer-to-peer architecture
Satellites connections
Compromised mail servers



Several Implants
From rootkits to javascript



Continuous monitoring of Adversaries' Capabilities: an example





<https://bit.ly/2yZ1rKJ>

Once upon a time there was a "Penguin"

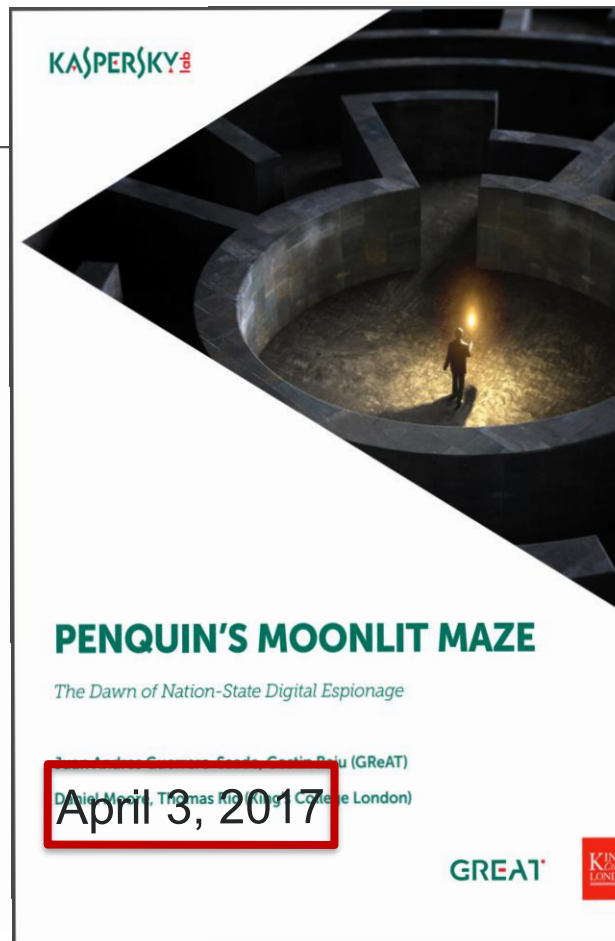
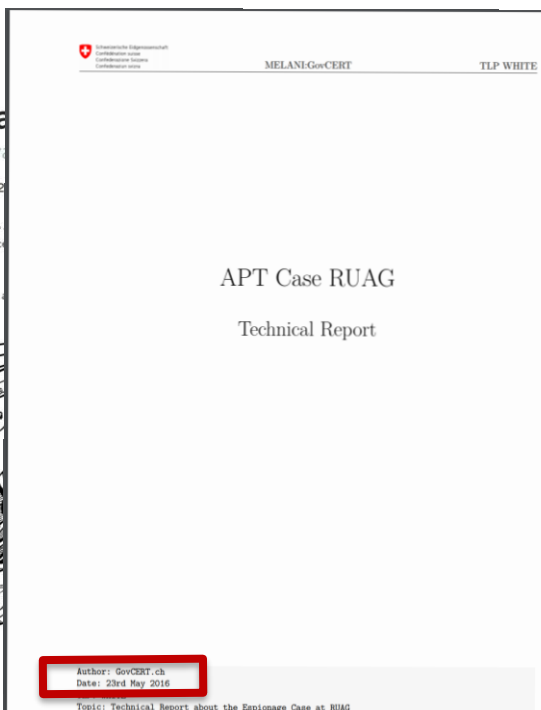
2014 → 2016 → 2017 → 2020

The 'Penguin' Turla

By Kurt Baumgartner, Costin Ralu on December 8, 2014

Recently, an interesting malicious sample was uploaded to because it appears to represent a previously unknown piece of complex APTs in the world.

We have written previously about the Turla APT with posts.



CYBER SECURITY DIVISION

MALWARE TECHNICAL INSIGHT TURLA "Penguin_x64"

Last update: May 29th 2020

The information contained in this document is proprietary to Leonardo S.p.a. This document and the information contained herein may not be copied, reproduced, used or disclosed in whole or in part in any form without the prior written consent of Leonardo S.p.a.
© Copyright Leonardo S.p.a. - All rights reserved

Cyber Threat Intelligence

Uncovering the traces of State Sponsored Threat Actors:
A case study on Turla

PART 2

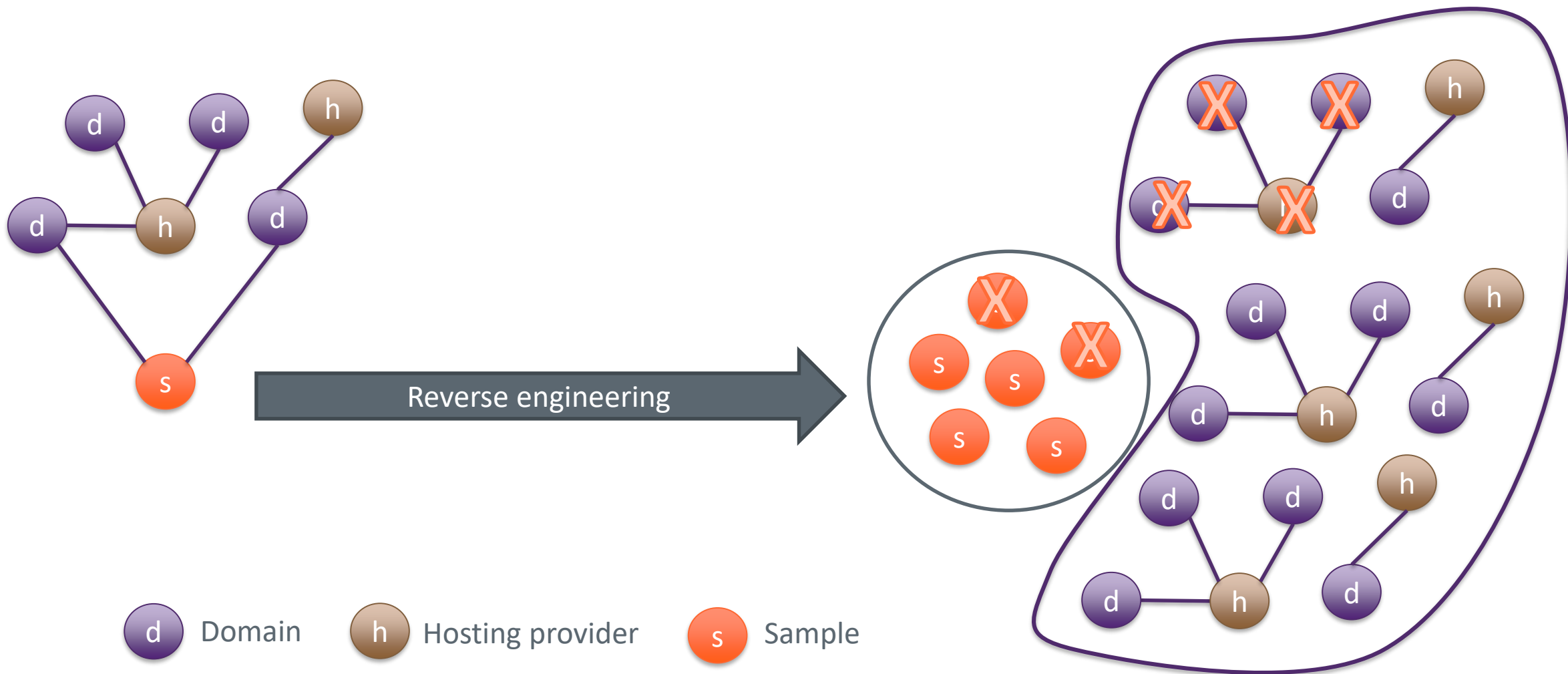
Silvio La Porta, PhD

Nino Verde, PhD

Antonio Villani, PhD

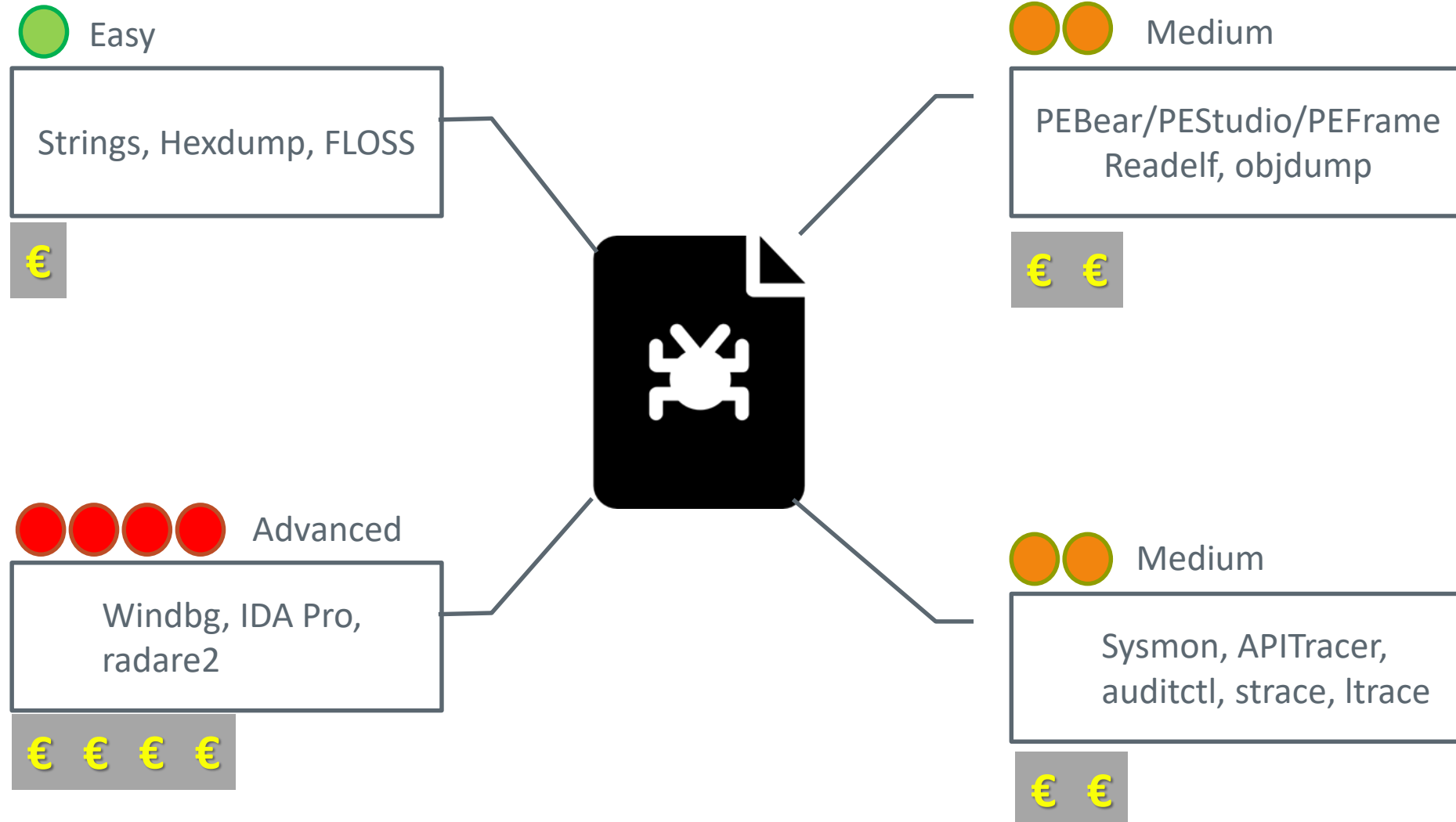


An example of the analysis process





The binary analysis tradeoff





To strings or not to strings

- With in-depth reverse engineering you can:
 - Understand the capabilities of the adversary
 - How advanced is his technical knowledge?
 - How is he using critical components such as encryption?
 - **XOR** vs **RC4** vs **SALSA** vs **AES** with modified S-Box vs Custom
 - How much effort did he put on the target
 - Uncover hidden corners
 - Environment-aware malware

Agenda

- Challenges
- Penguin Version comparison
- Timeline Exstimation
- Main commands description
- Activation packet
- Demo





Challenges that we had to face with



Evaluate the novelty of the collected samples

Why?

Turla operates since 2004 at least, they could be old samples resubmitted to Virus Total

Is it a problem?

ELF files (executables for Linux) do not have a compilation timestamp like windows executable

How?

Dig into our Knowledge Base

Find a way to estimate the build date



Provide a way to detect a well-engineered passive backdoor for Linux

Why?

To defend ourself, our customers and the entire community

Is it a problem?

Low visibility on Linux machines

Difficult to develop network signatures and probably not effective (low traffic)

Difficult to detect this backdoor through network scans

Several checks to identify well-formed packets

How?

Reverse Engineering the network protocol



Comparing Architecture and Capabilities

Penquins' main



Penquin_x86

- Passive
- Get cmd parameters (ID, INT)
- Use *command* function to process C2 received data



Penquin_2.0

- Active
- Hardcoded C2 IP
- It is the only Penquin which does not require *root* privileges
- Use *command* function to process C2 received data



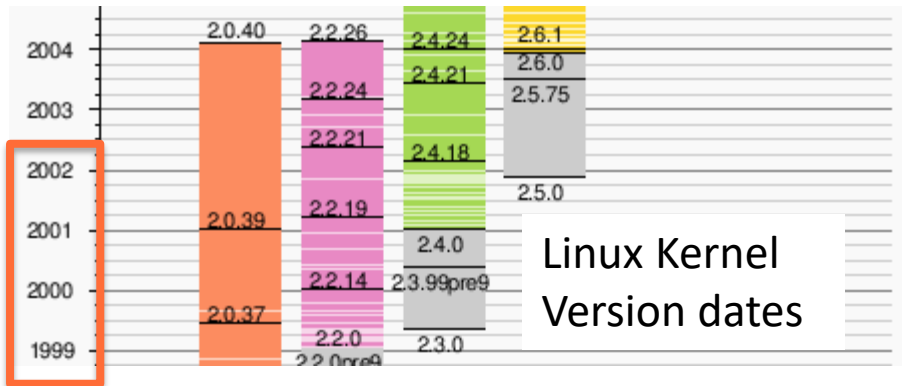
Penquin_x64

- Passive
- Hardcoded parameters (ID, INT)
- Drop/run cron (*/root/.sess*)
- Use *do_callback* function to process C2 received data



Build date estimation

- ABI Version
- Statically linked library
- Linux Distribution (cron)



ABI	Penquin_x86	Penquin_2.0	Penquin_x64
2.2.0		X	
2.2.5	X		
2.4.18			X

GCC	ABI	Release Date
3.4.6	2.6.8	March 6, 2006
4.4.4	2.6.15	April 29, 2010
4.8.2	2.6.24	October 16, 2013
4.9.1	2.6.32	July 16, 2014
6.2.0	2.6.32	August 22, 2016
6.3.0	2.6.32	December 21, 2016
7.2.0	3.2	August 14, 2017
7.3.0	3.2	January 25, 2018
7.5	3.2	November 14, 2019



Build date estimation

- ABI Version
- Statically linked library
- Linux Distribution (cron)



OpenSSL Version	Penquin_x 86	Penquin_2 .0	Penquin_x 64	Year
0.9.6	X			2000
0.9.7.e		X		2004
1.0.1j			X	2014



Build date estimation

- ABI Version
- Statically linked library
- Linux Distribution (cron) ←

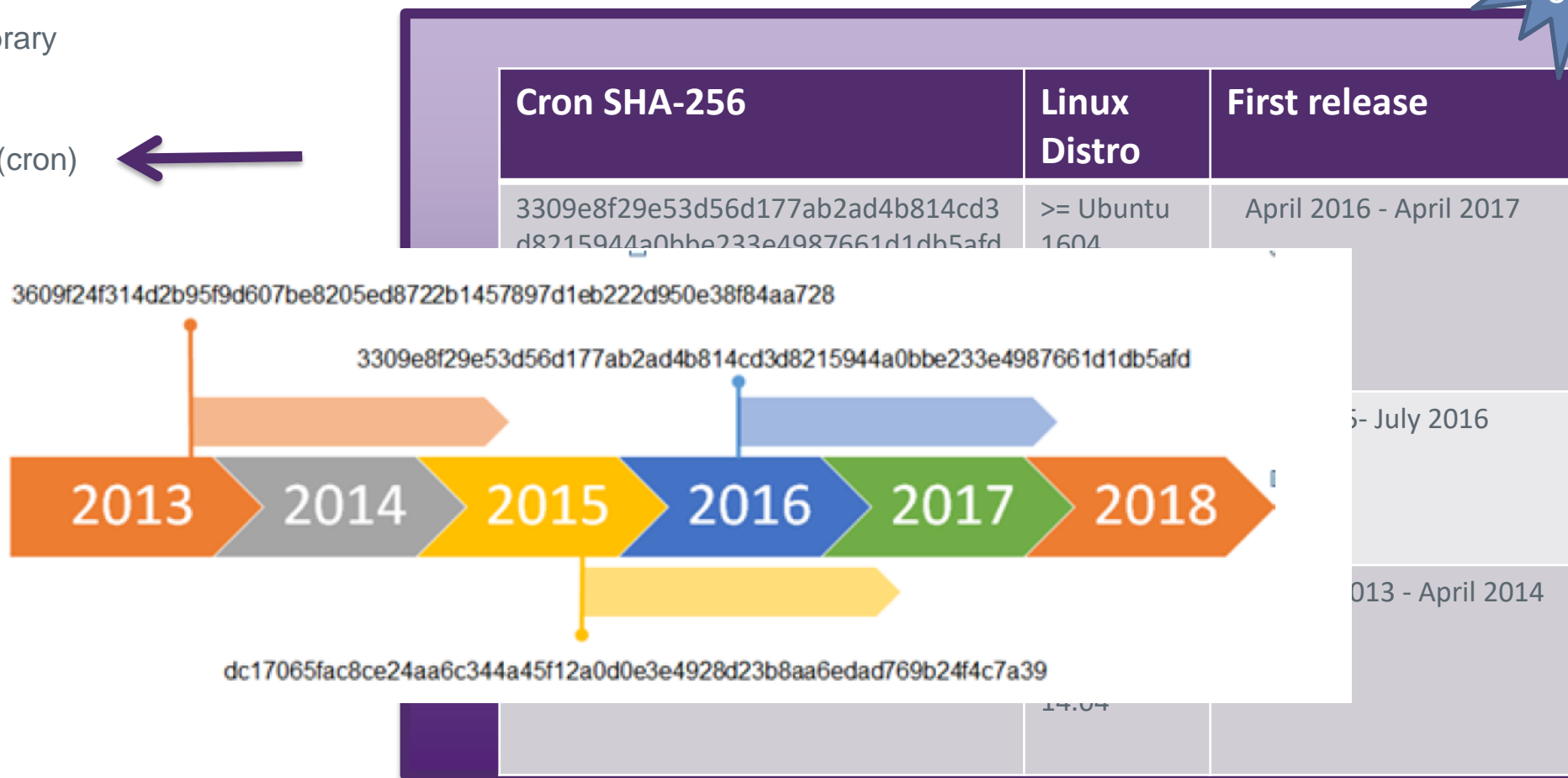


Cron SHA-256	Linux Distro	First release
3309e8f29e53d56d177ab2ad4b814cd3d8215944a0bbe233e4987661d1db5afd	>= Ubuntu 1604 <= Ubuntu 1704	April 2016 - April 2017
dc17065fac8ce24aa6c344a45f12a0d0e3e4928d23b8aa6edad769b24f4c7a39	Centos 6.7 Centos 6.8	Sep 2015- July 2016
3609f24f314d2b95f9d607be8205ed8722b1457897d1eb222d950e38f84aa728	Ubuntu 13.10 Ubuntu 14.04	October 2013 - April 2014



Build date estimation

- ABI Version
- Statically linked library
- Linux Distribution (cron) ←





The `do_callback` function

Download & execute

It is **not** present in `Penquin_2.0`

It is called after the packet activation process if it succeed in `Penquin_x64`, in the older version is not directly reachable

```
close(1);
if ( !fork_() )
{
    set_sid_();
    chdir("/root");
    uuencode("/root/.tmpware");
    v11 = &status;
    wait(&status);
    unlink(".tmpware");
    v4 = execli("/root/.x11-fifo", "w");
    v5 = prepare_output_str(v14);
    sprintf(v4, "%s\n", v5);
    sprintf(v4, "%ld\n", a2);
    fclose_caller(v4);
}
}
```

Penquin_x86

```
if ( !fork_call() )
{
    setsid();
    chdir("/root");
    uuencode_parse("/root/.session");
    wait(&stat_addr);
    unlink("/root/.session");
    v8 = run_cmd("/root/.hspcrfdata", "w");
    v9 = prepare_output_str(v11);
    fprintf_0(v8, "%s\n", v9);
    fprintf_0(v8, "%ld\n", v2);
    printf(v8, "%ld\n");
    sleep(5u);
    exit(0LL, "%ld\n");
}
}
```

Penquin_x64



The *do_callback* function

Download & execute

It is **not** present in
It is called after the

uuencode(1) - Linux man page

Name

uuencode, uudecode - encode a binary file, or decode its representation

Synopsis

uuencode [-m] [file] name
uudecode [-o outfile] [file]...

Description

Uuencode and *uudecode* are used to transmit binary files over transmission mediums that do not support other than simple ASCII data.

Uuencode reads *file* (or by default the standard input) and writes an encoded version to the standard output. The encoding uses only printing ASCII characters and includes the mode of the file and the operand *name* for use by *uudecode*. If *name* is */dev/stdout* the result will be written to standard output. By default the standard UU encoding format will be used. If the option *-m* is given on the command line **base64** encoding is used instead.

```
if (
{
set
chd
uud
v11
wai
unl
v4
v5
spr
spr
fcl
}
}
```

```
"w");
```

Penquin_x86

Penquin_x64

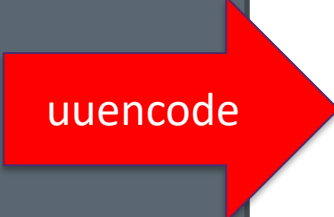


The `do_callback` function

Download & execute

```
t0@DESKTOP-LEI8HMJ:~$ head test_minio.sh
#!/bin/bash
set -x
out_folder="./"

host=$1
s3_key=$2
s3_secret=$3
...
...
...
```



```
t0@DESKTOP-LEI8HMJ:~$ uuencode test_minio.sh test.uuencoded
begin 755 test.uuencoded
M(R$O8FEN+V)A<V@*<V5T("UX"F]U=%]F;VQD97()(BXO(@H*:&]S=#T
D,0IS
M,U]K97D])#(*<S-?<V5C<F5T/20S"B-H;W-
T/2)M:6YI;RYA<F=O+FQA8CHY
M,#`P(@HC<S-?:V5Y/2)4:&ES27-4:&5-
:6YI;T%C8V5S<TME>2(*(W,S7W-E
M8W)E=#TB5&AI<TES5&AE36EN:6]396-
R971+97DB"@HC(%1H92!N86UE(&]F
M('1H92!T97AT(&9I;&4@8V]N=&%I;FEN9R!T:&4@97AP96-
T960@:&%S:`IH
M87-H7V9N86UE/2)T97-
T+FAA<V@B"FUS:5]F;F%M93TB4')O=&]!9V5N=$EN
M<W1A;&QE<BYM<VDB"F-E<G1?9FYA;64](G!R;W1O<V5R=F5R+F-
R="(*"F10
```

output. The encoding uses only printing ASCII
name for use by `uudecode`. If *name* is `/dev/std`
the standard UU encoding format will be used.
encoding is used instead.

Penquin_x86

Penquin_x64



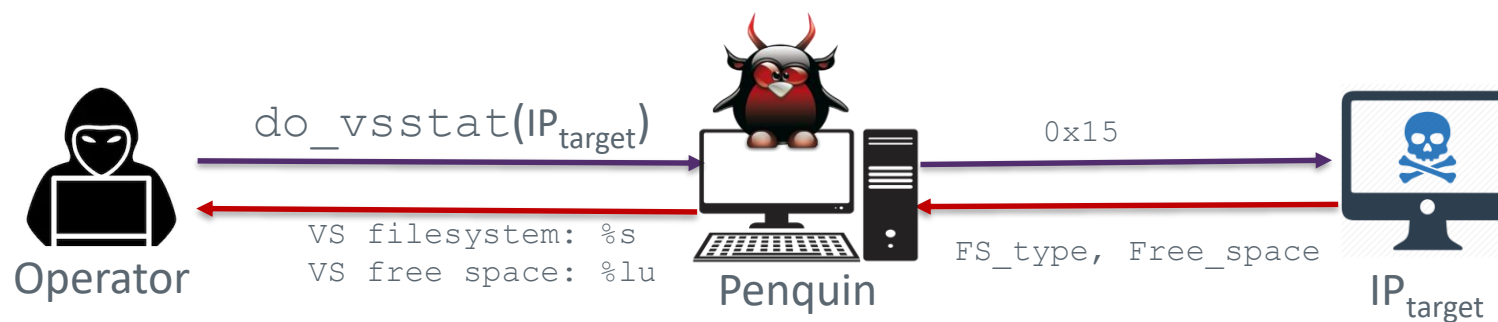
More and more commands...

Function Name	Description
do_exit	Exit returning 0
do_setenv	Set an <i>env</i> variable
do_cd	Re-implements the <i>cd</i> command logic
do_download	Download a file from C2
do_upload	Upload a file to C2
do_start	Download and execute a file from C2 getting pipes
do_exec	Download and execute a file from C2 in /tmp folder

Function Name	Description
do_vslist	Send a table to C2 containing specified peer's file information Description FileName Size Status
do_vsupload	Upload a local file to specified peer
do_vsdownload	Download a specified peer's file locally
do_vsstat	Get specified peer filesystem information and available disk space
do_vsshutdown	Likely delete a peer remote file
do_vsdelete	Just send a message containing a code to specified peer



More and more commands...

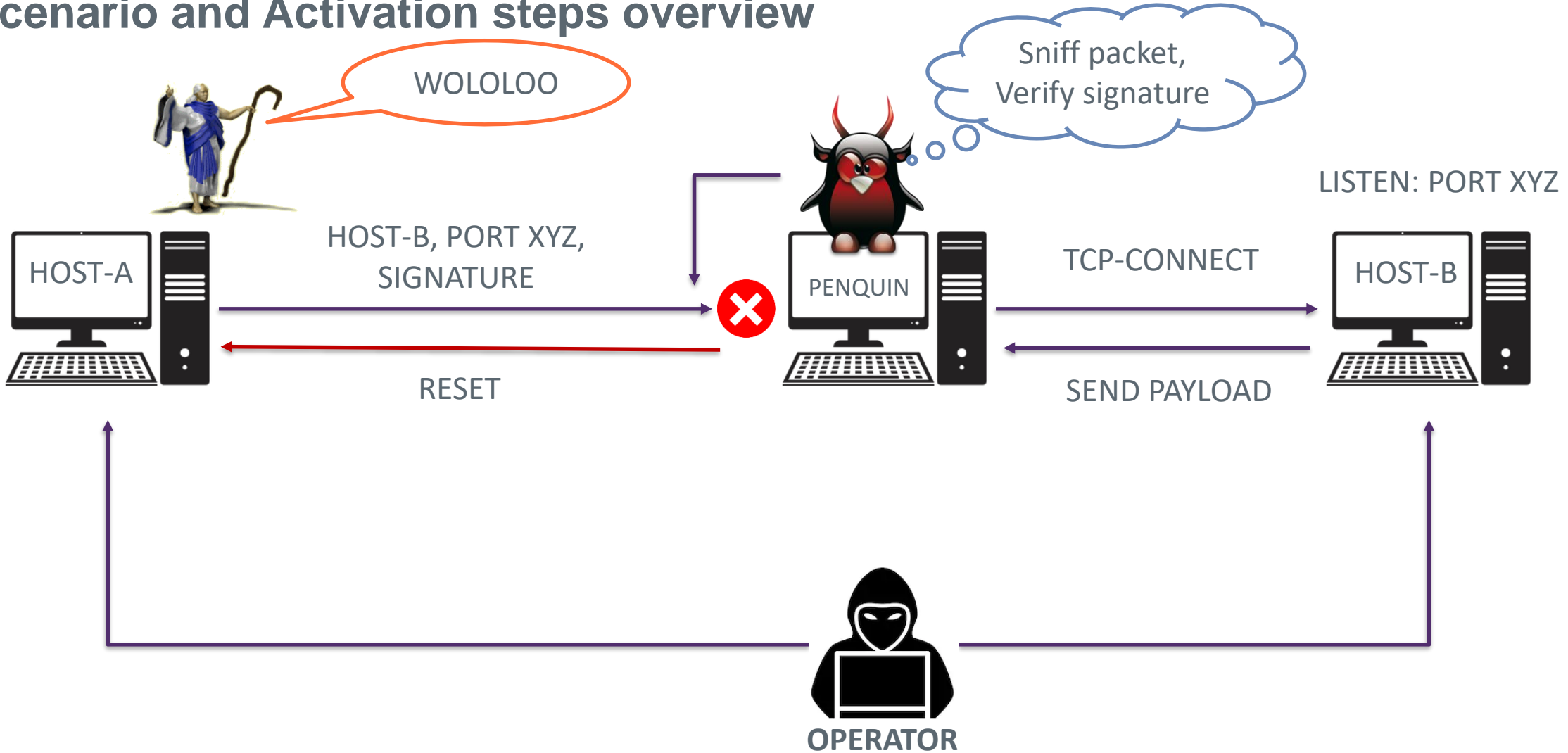


<code>do_upload</code>	Upload a file to C2
<code>do_start</code>	Download and execute a file from C2 getting pipes
<code>do_exec</code>	Download and execute a file from C2 in /tmp folder

<code>do_vsstat</code>	Get specified peer filesystem information and available disk space
<code>do_vsshutdown</code>	Likely delete a peer remote file
<code>do_vsdelete</code>	Just send a message containing a code to specified peer



Scenario and Activation steps overview





WOLOLOO

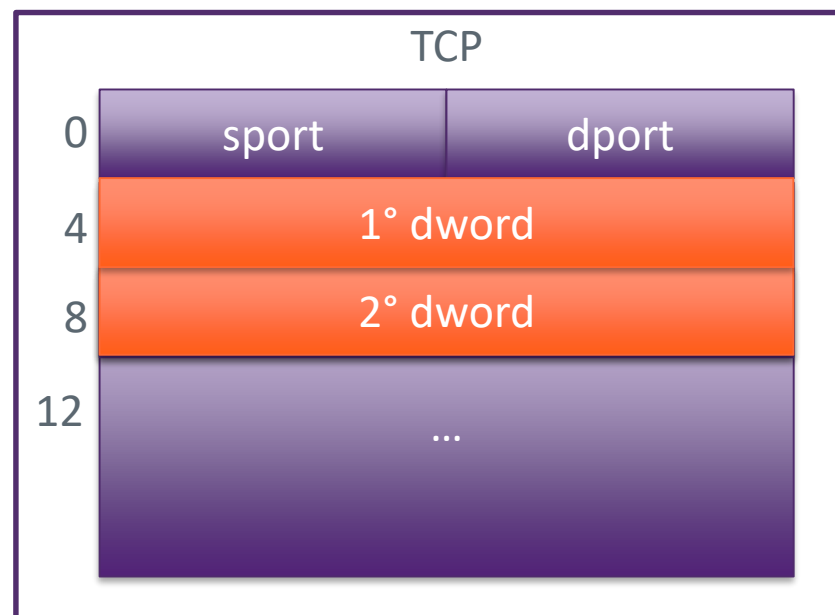
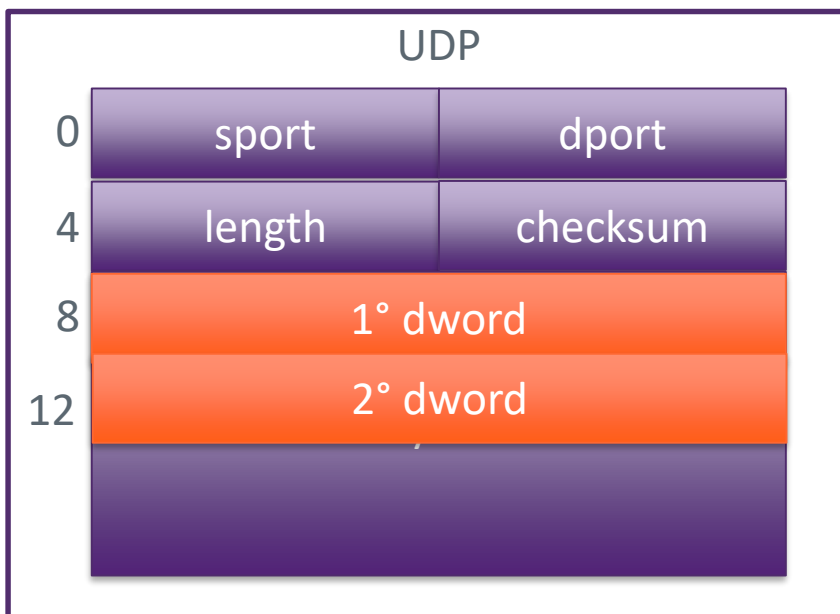
I wanna be a...



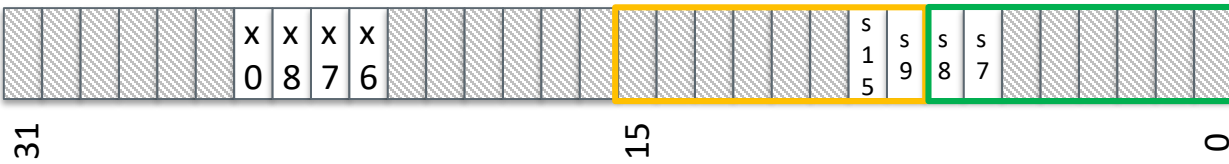
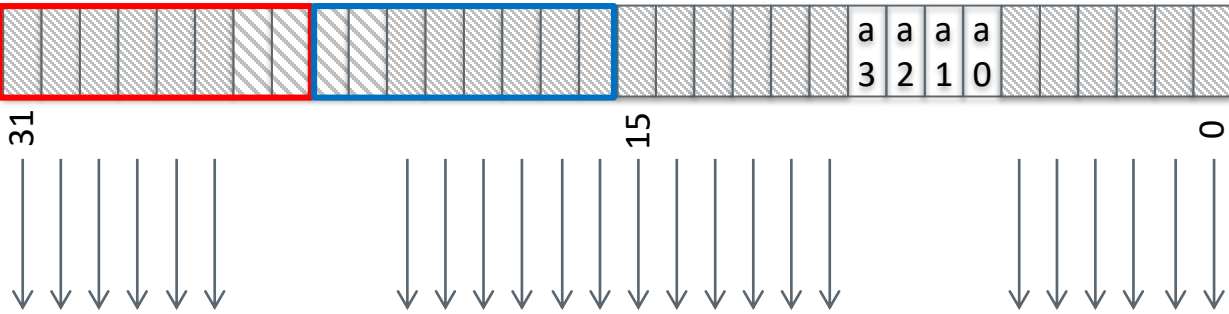
- PCAP Filter

```
(tcp[8:4] & 0xe007ffff = 0x6005bdbd) or (udp[12:4] & 0xe007ffff = 0x6005bdbd)
```

```
(tcp[8:4] & 0xe007ffff = 0x6005bebe) or (udp[12:4] & 0xe007ffff = 0x6005bebe)
```

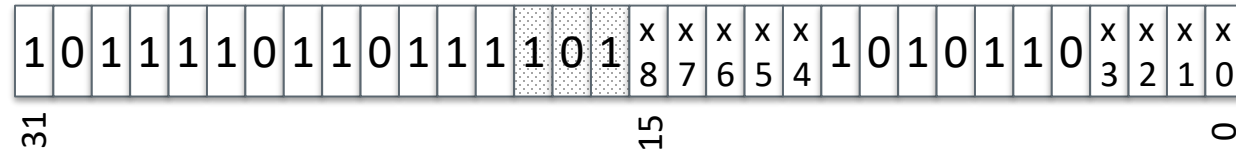


First Dword

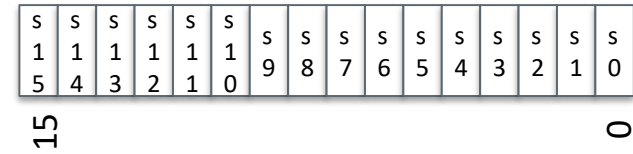


Final IP (endian-flipped)

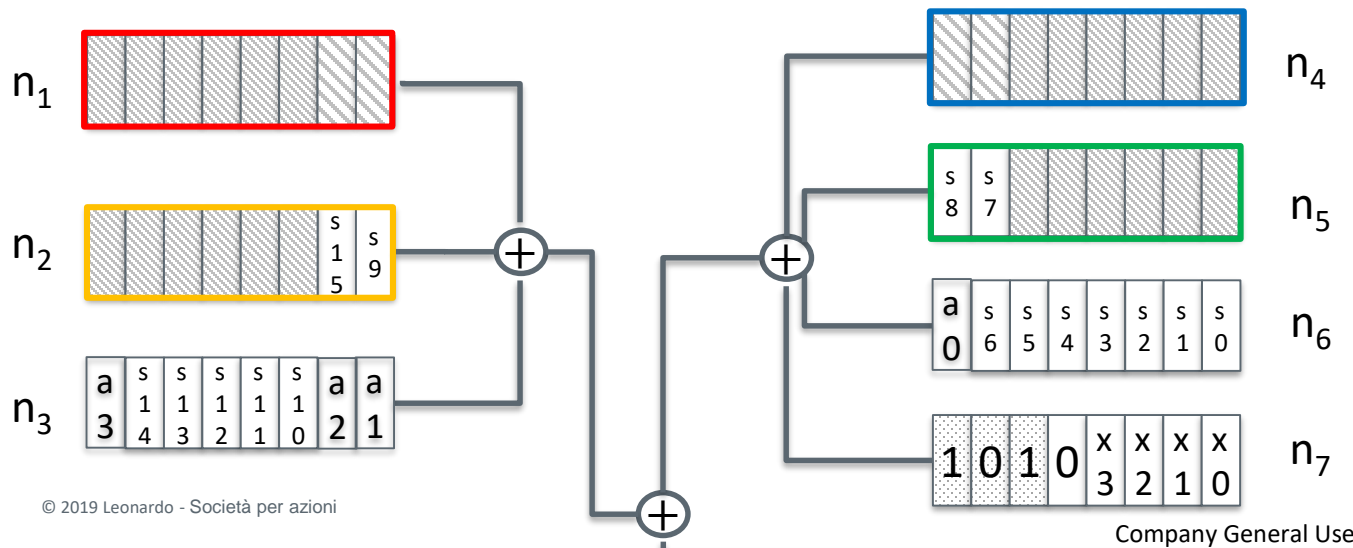
Second Dword (0xbdbd0560)



Source Port



DATA

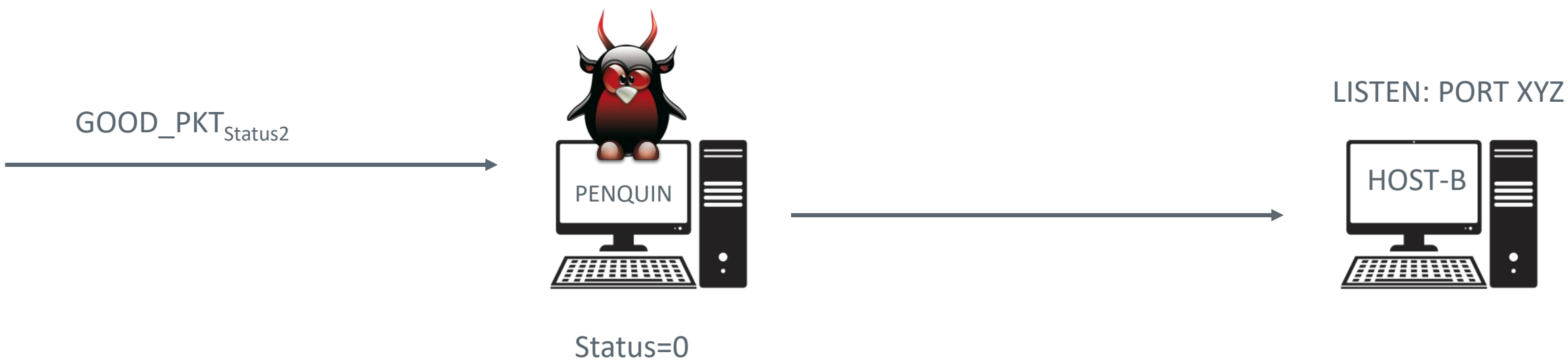


if $((n_1 \oplus n_2 \oplus n_3) \oplus (n_4 \oplus n_5 \oplus n_6 \oplus n_7)) == n_8$
return success

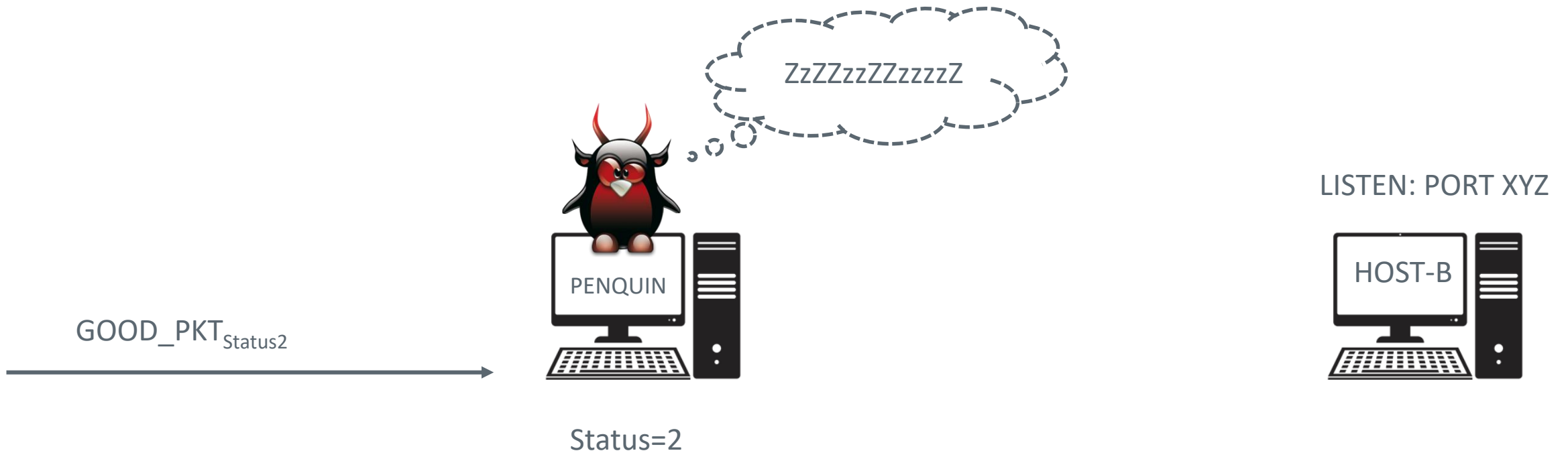
CONDITIONS



Internal status



Internal status



Ubuntu 1604 x64 - VMware Workstation

File Edit View VM Tabs Help

Ubuntu 1604 x64

root@ubuntu: ~/Desktop

root@ubuntu:~/Desktop# ./penquin_x64

Cattura da VMware Network Adapter VMnet1

File Modifica Visualizza Vaj Cattura Analizza Statistiche Telefonja Wireless Strumenti Aiuto

(tcp | udp) && | dns && | mdns && | ssh && | mnr && | nbs && | (tcp.port ==22) && | dhcp

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

t0@DESKTOP-LEI8HMJ: ~

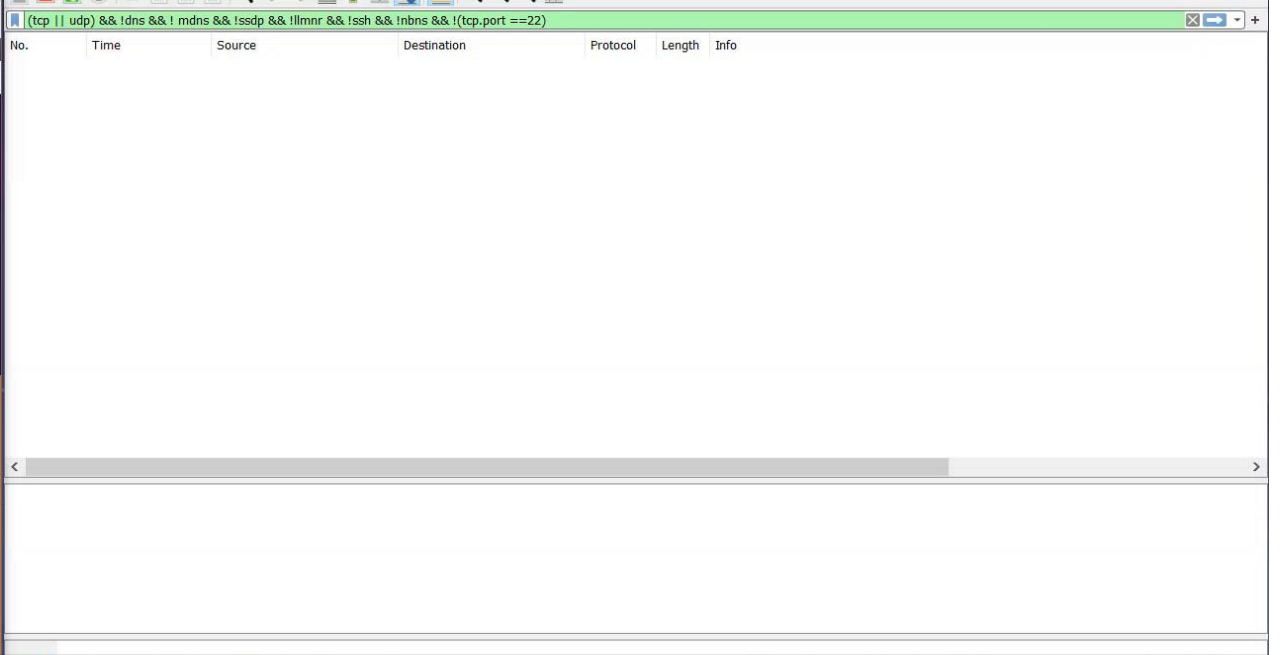
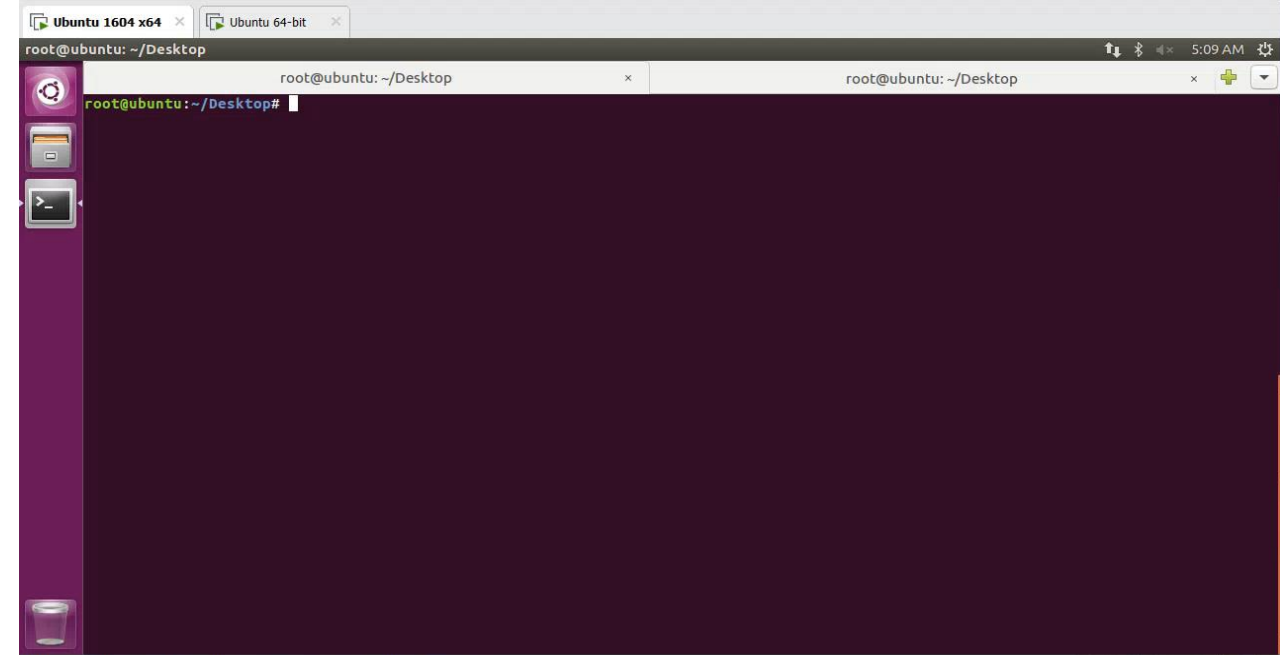
u@u:~\$ nc -l -p 12664

u@u:~\$ nc -l -p 12792

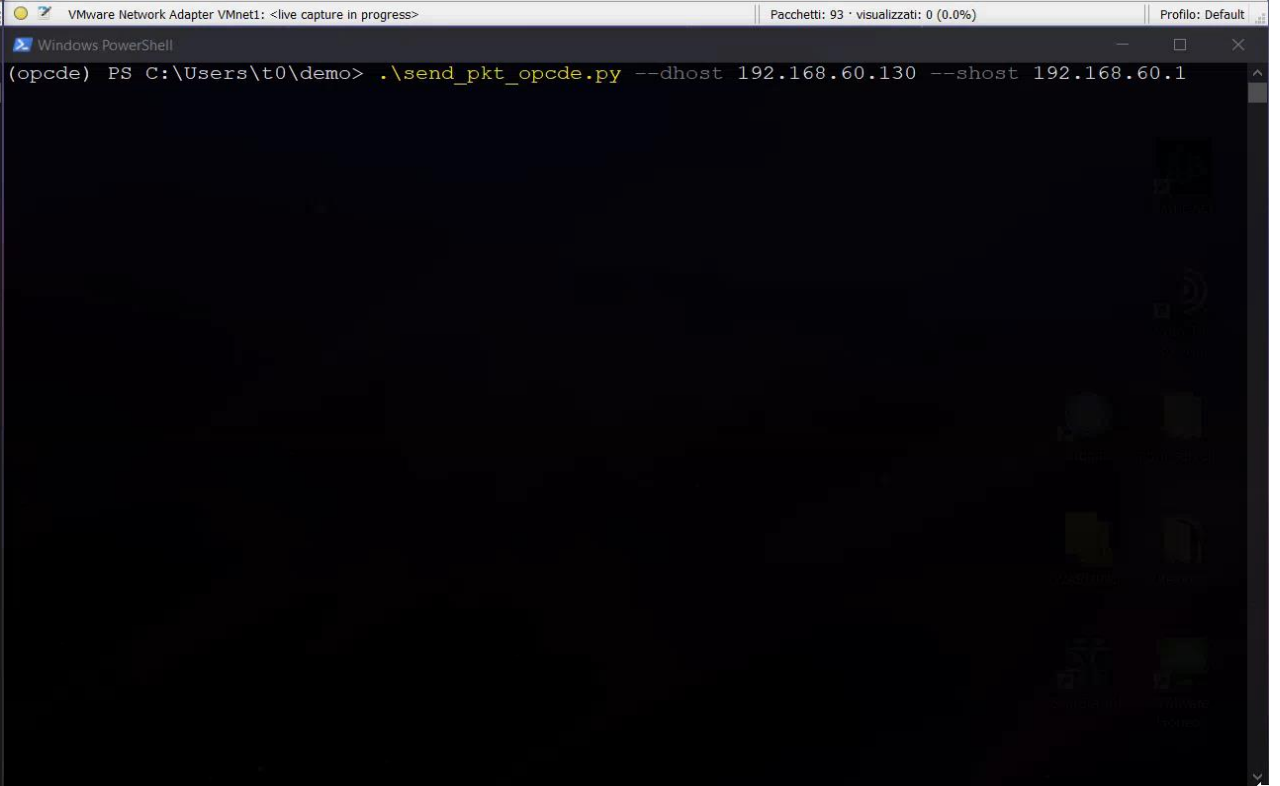
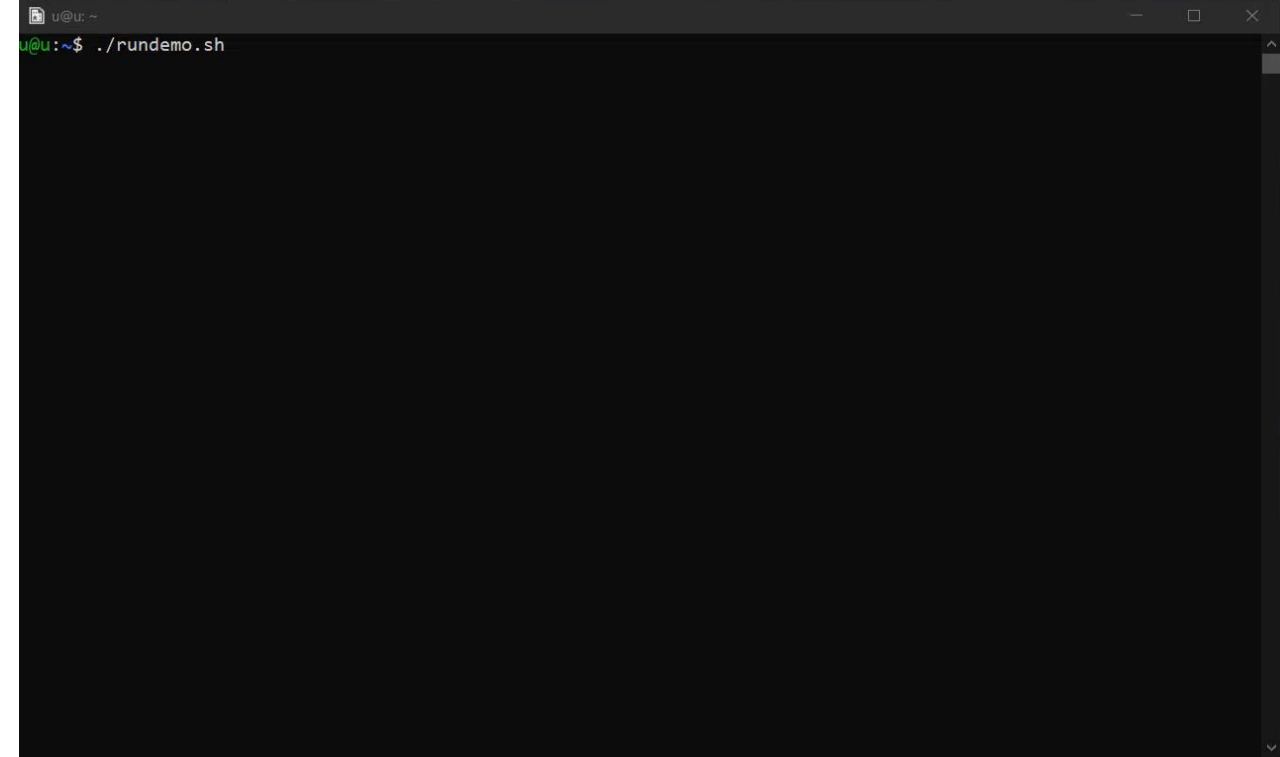
VMware Network Adapter VMnet1: <live capture in progress> Pacchetti: 68 · visualizzati: 0 (0.0%) Profilo: Default

Windows PowerShell

(opcde) PS C:\Users\t0\demo> .\send_pkt_opcde.py --dhost 192.168.60.130 --shost 192.168.60.1

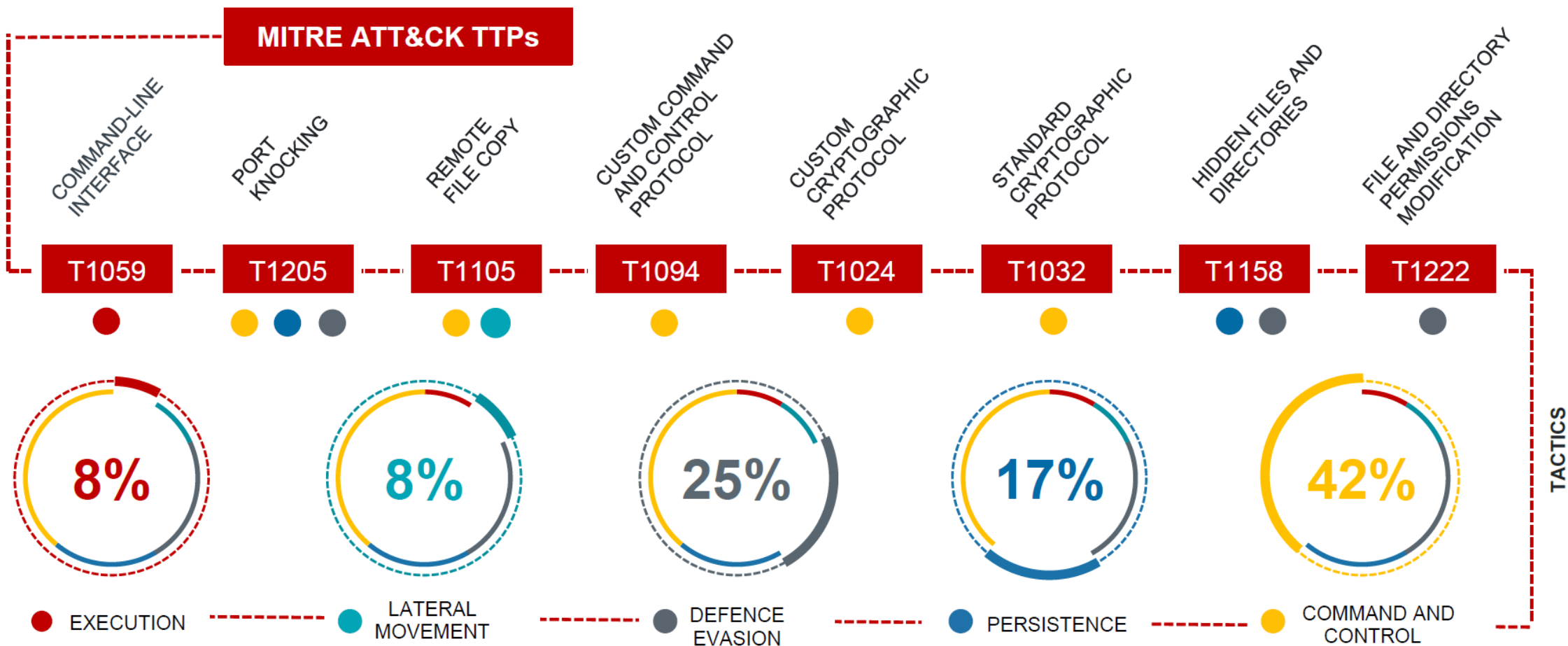


To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





Evaluation of "Penguin_x64" tactics and techniques





Penquin killchain phases



Credits to Antonio Rossi



Work with us

- We are hiring!
- Other collaborations:
 - Stage
 - Thesis
- Send your CV and collaboration proposal to:

cybersecurityrecruitment@leonardocompany.com

Specify your interests and the seminar that you attended

For the winner:

Send us a tweet with the screenshot of your result and we will send you the book!

 @verdenino

 @t0nvi



THANK YOU FOR YOUR ATTENTION





Suggested Readings

- Threat intelligence and me, Robert M. Lee
- Intelligence Driven Incident Response: Outwitting the adversary
- Watch [Week 6](#) of Chris Sanders' free Cuckoo's Egg course.
- **The Security Intelligence Handbook, Third Edition.** How To Disrupt Adversaries and Reduce Risk With Security Intelligence, Recorded Future
- APT1 - Exposing One of China's Cyber Espionage Units. Report by Mandiant (2004)