Projet financé par l'Union Européenne
Projet mis en œuvre par Expertise France

Basics of a CSIRT: Managerial Aspects and Software environment

Accra, August 9 – 13, 2021

Index

Introduction: The Trainer

- President, Founder, **The Security Brokers**
- Co-founder, **Swascan.com**
- Independent Special Senior Advisor on Cybercrime @ **UNICRI** (*United Nations Interregional Crime & Justice Research Institute*)
- Roster of Experts @ **ITU** (*UN International Telecomunication Union*)
- Former PSG Member, **ENISA** (*Permanent Stakeholders Group @ European Union Network & Information Security Agency*)
- Founder, @ **CLUSIT** (*Italian Information Security Association*)
- Steering Committee, **AIP/OPSI** (*Privacy & Security Observatory)*
- Board of Directors, **ISECOM** *(Institute for Security & Open Methodologies)*
- **OSSTMM** Key Contributor *(Open Source Security Testing Methodology Manual)*
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè, Scientific Committee, **APWG** European Chapter
- Former Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various security communities**

The right philosophy

- **Choose the** "**open source option(s)**" as much as you can, whenever you can, wherever you can do it
- It's not just about **budgets and saving money**: it's the **concept of "Security Community"**!
- Don't became the **cow of Vendors**
  - It will happen that your security vendor's product will turn you into **the attacker's entry point** (i.e. see Sonicwall, Fortinet, etc, just a few days ago)
  - **I will walk you through <u>0-days marketplaces</u>**

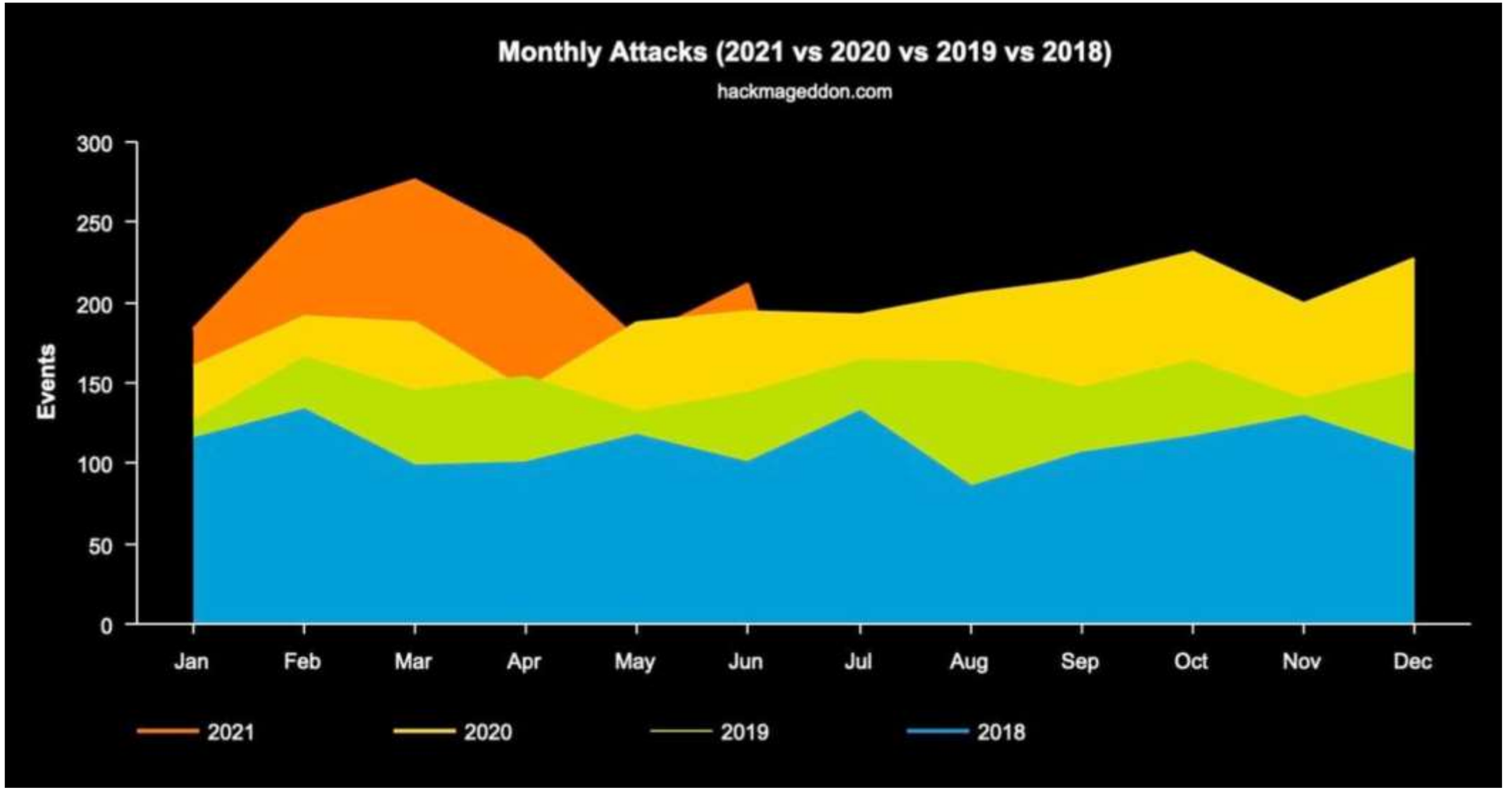
It's a dirty world out there…

- The cybercrime ecosystem
  - Multiple actors
  - Money driven
  - HPP (Hacker's Profiling Project by UNICRI and ISECOM)
    - Pls do remind I gotta show you this! (extras, if you'd need)

- **Everything is about the DATA. Never forget this.**

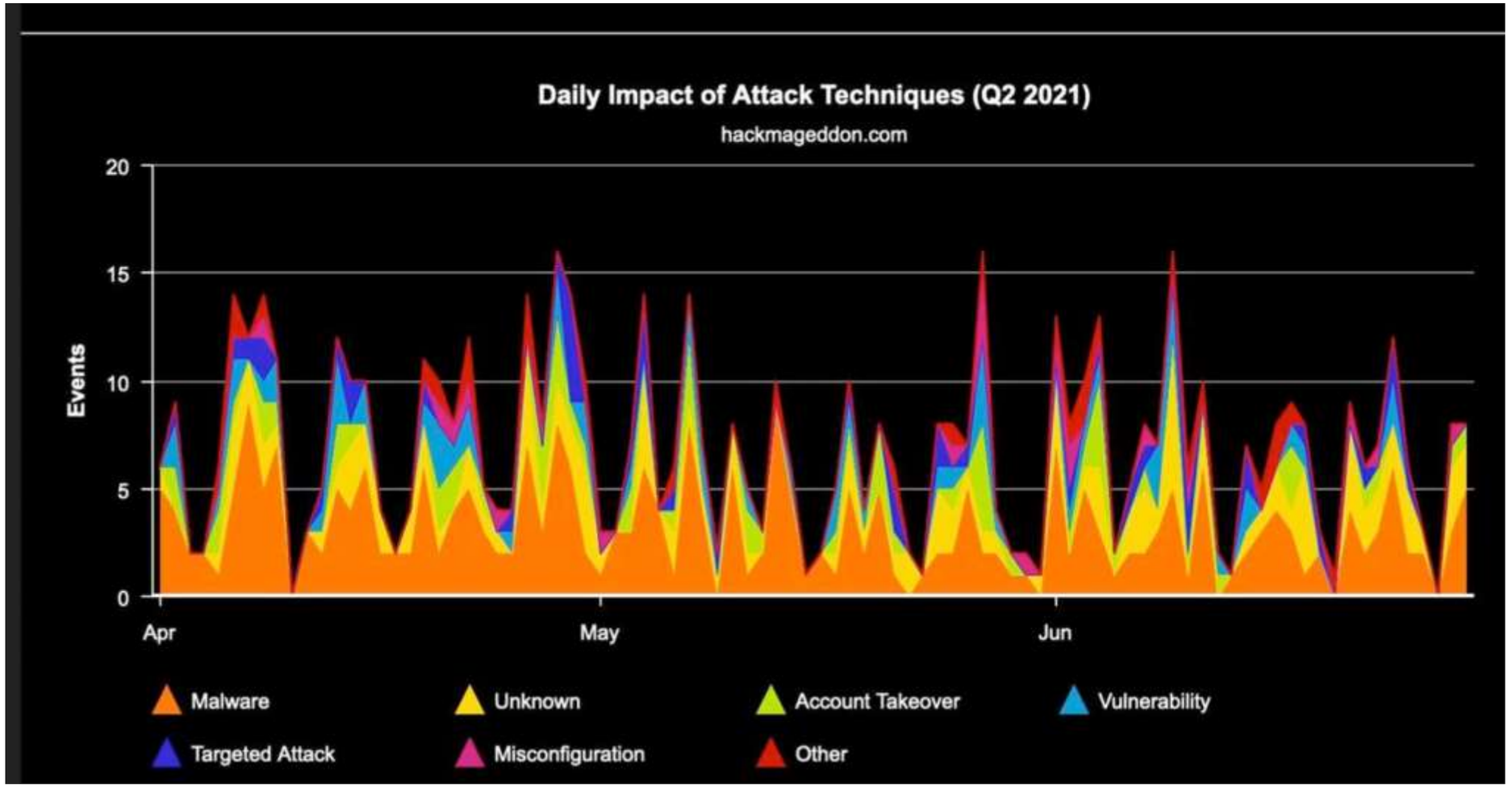
  - Hackmageddon.com (Paul Sparrows)
  - The WEF report(s)
  - EUROPOL operations
  - Vendors' reports (even if…)

Fresh data on Cyber Attacks!

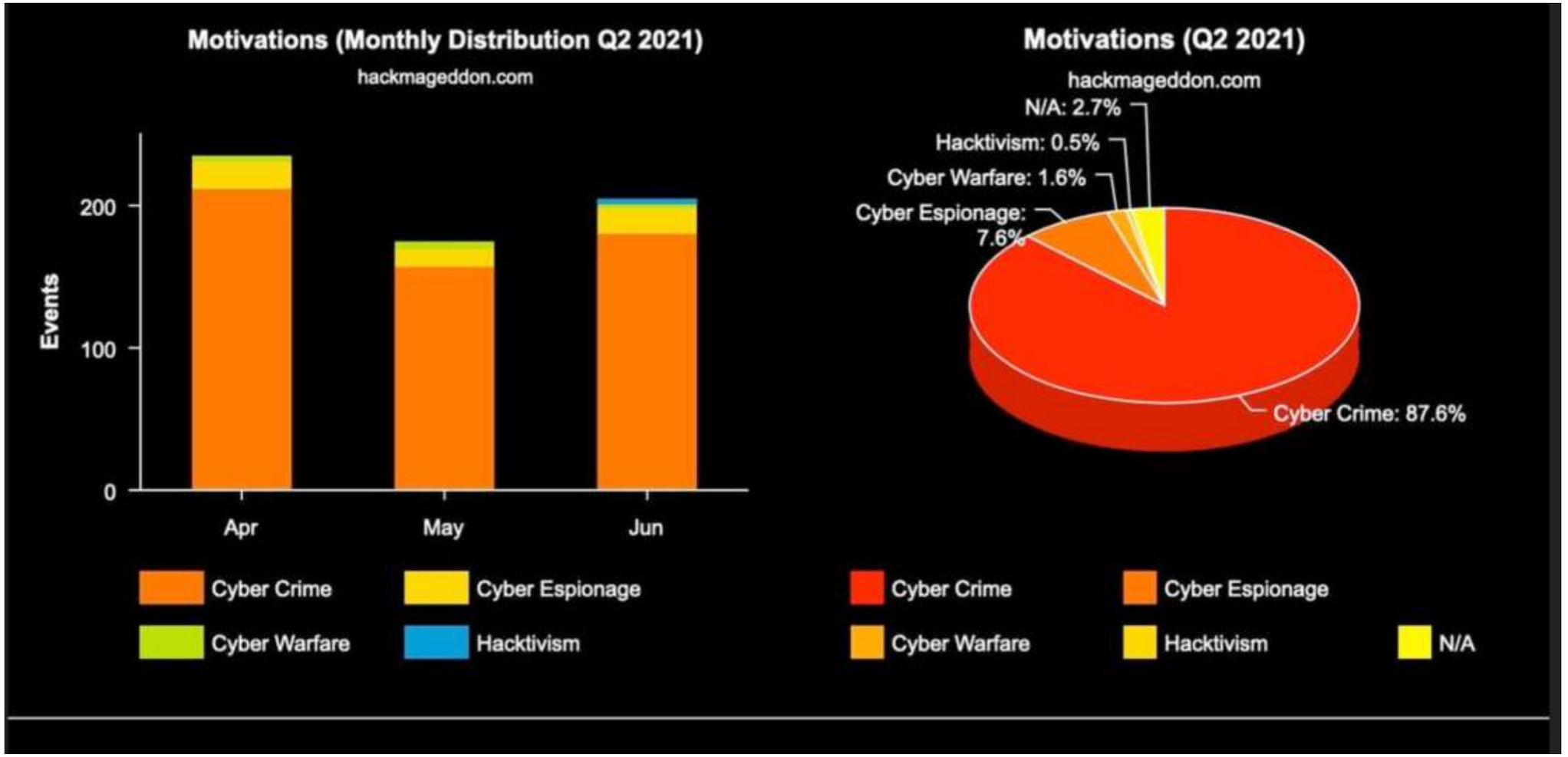


Managerial Aspects and Software environment

Fresh data on Cybercrime!

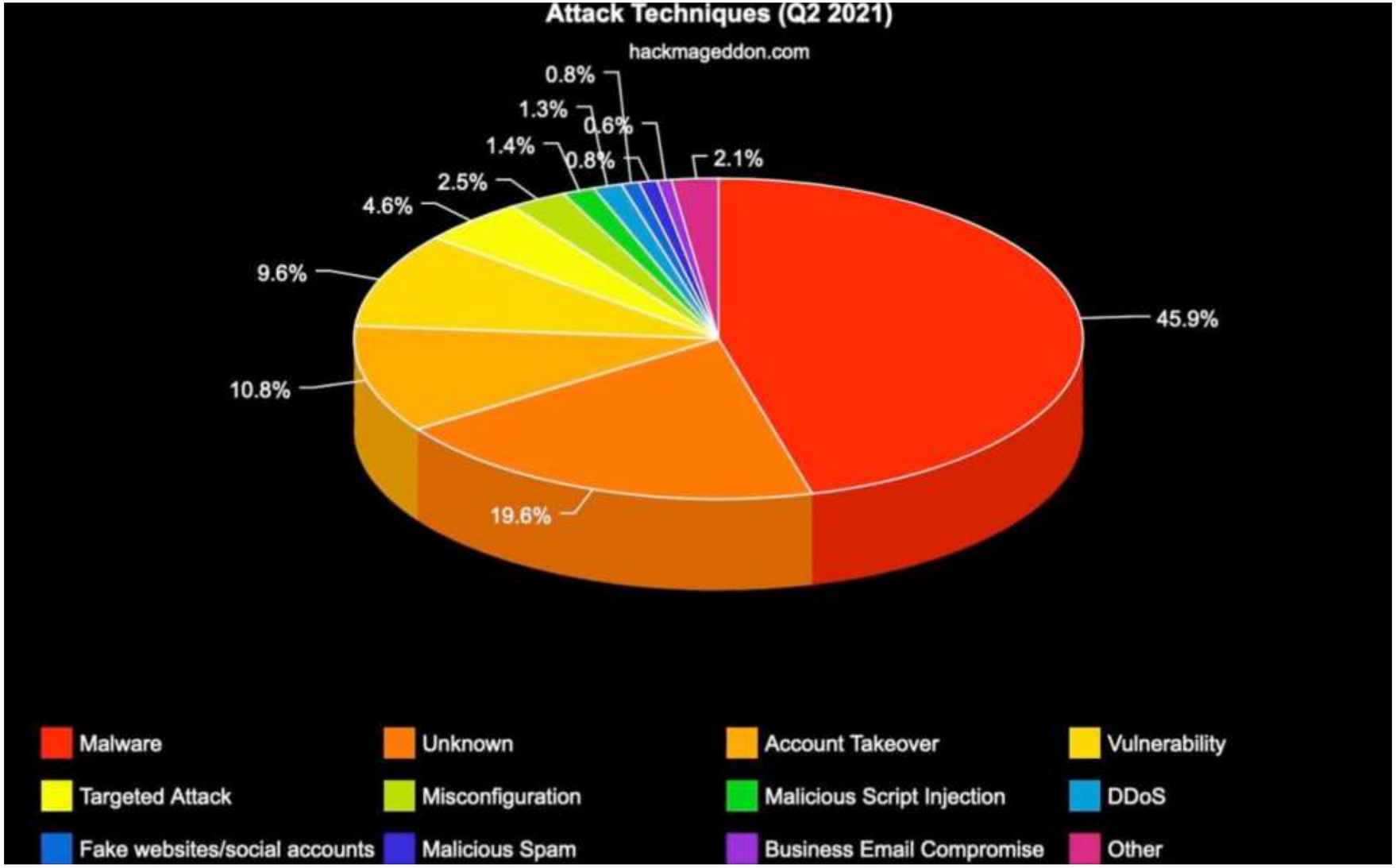


Fresh data on Cybercrime!



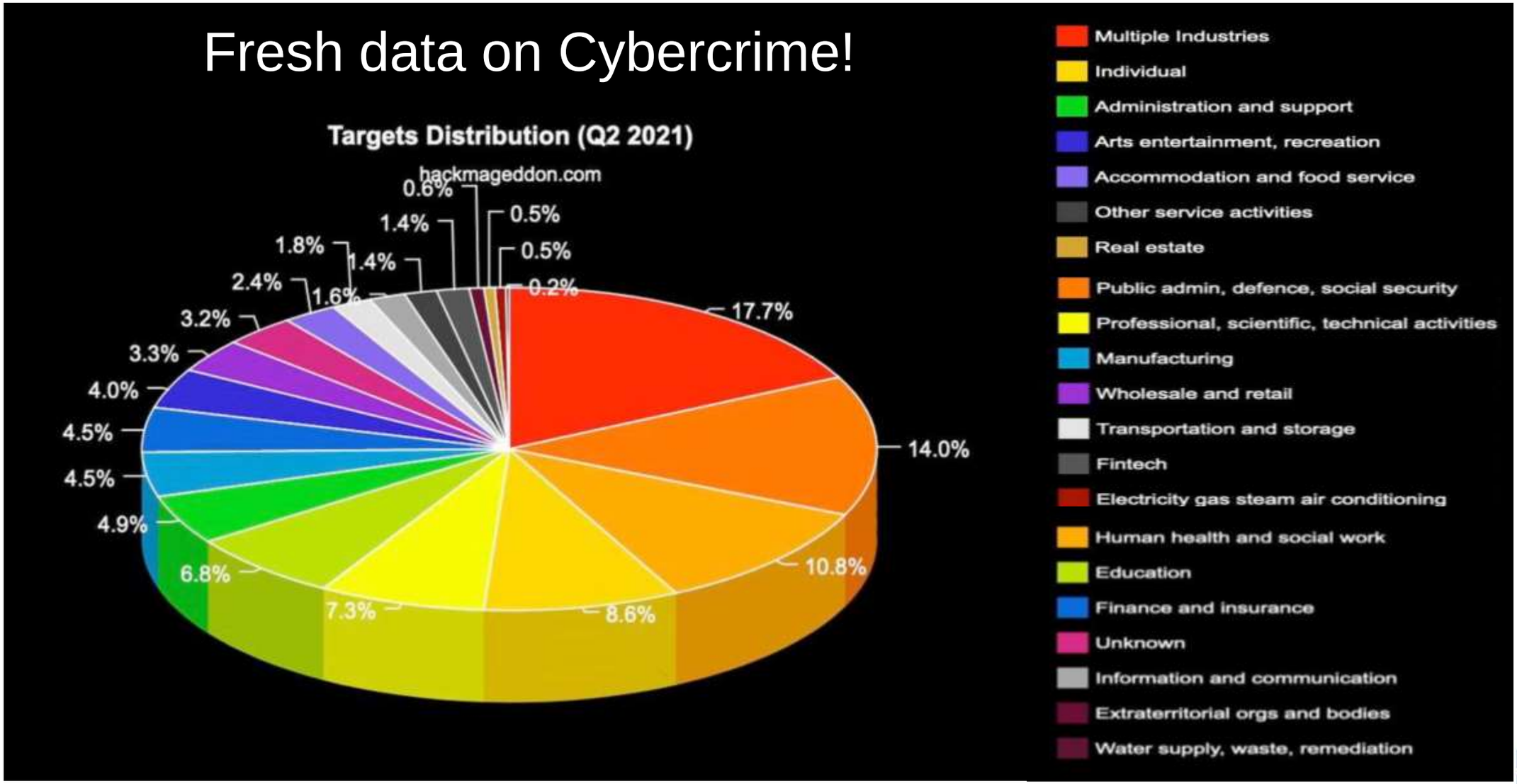
Managerial Aspects and Software environment

Fresh data on Cybercrime!

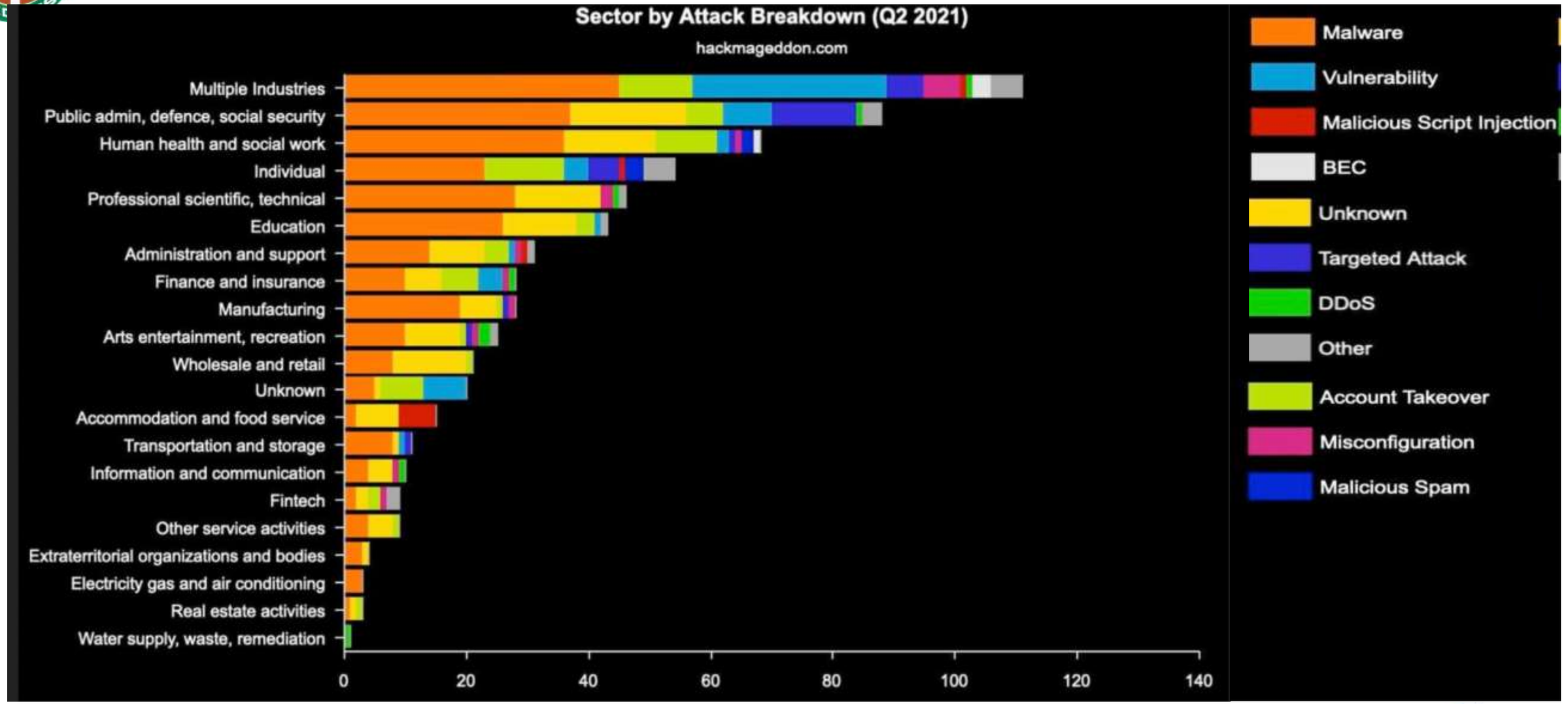


Managerial Aspects and Software environment

Fresh data on Cybercrime!



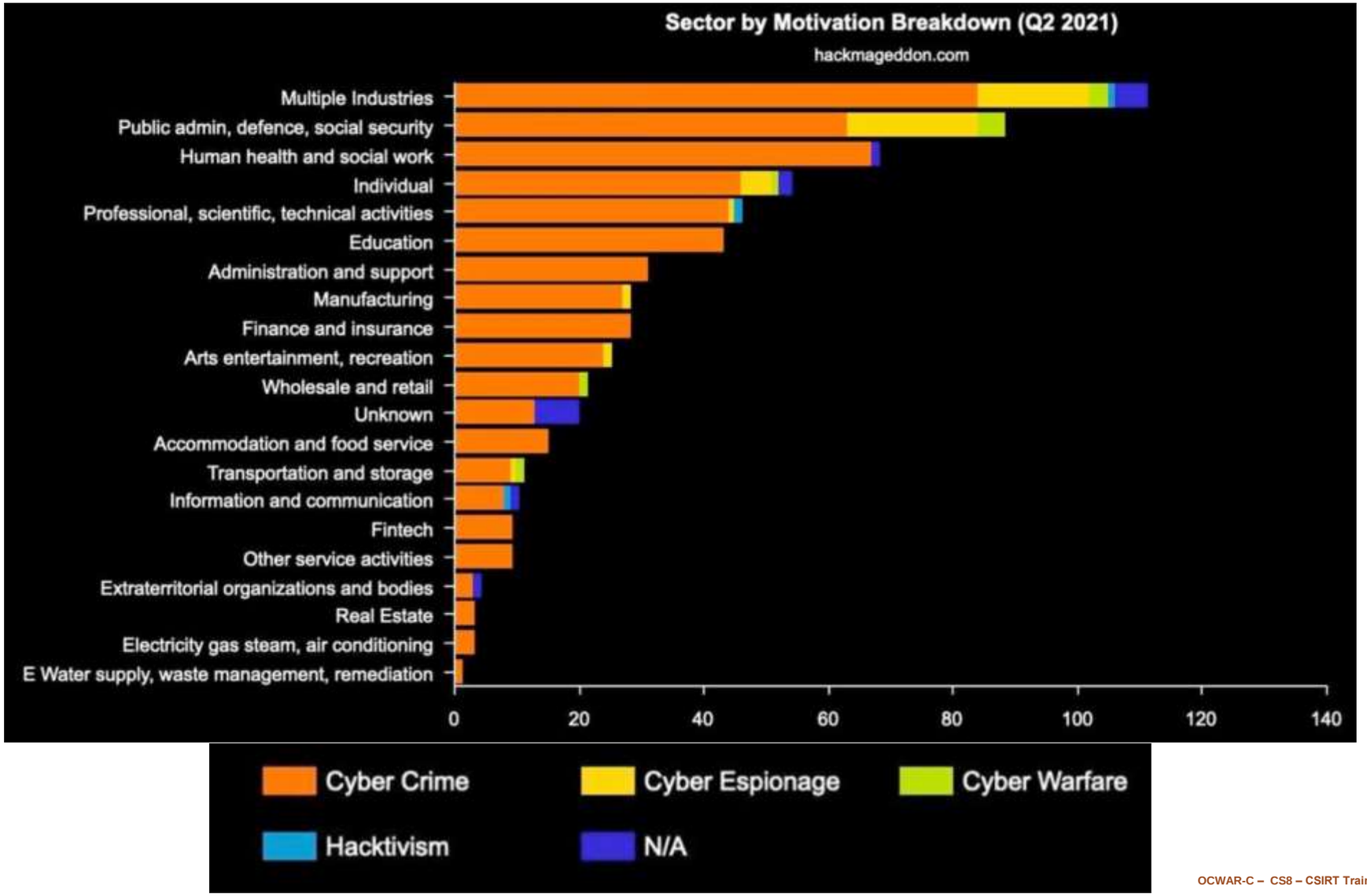
Managerial Aspects and Software environment



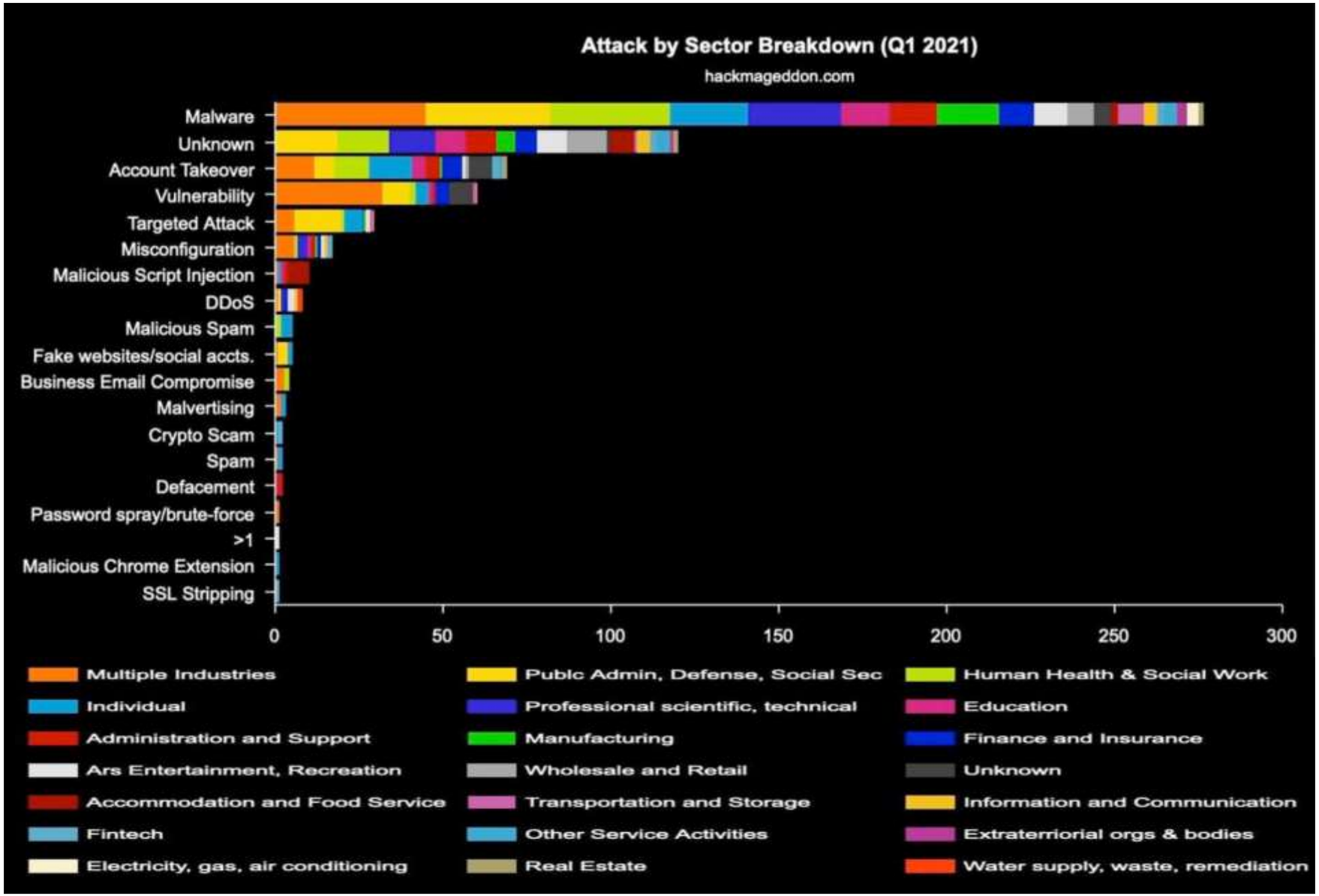
Fresh data on Cybercrime!

Managerial Aspects and Software environment

Fresh data on Cybercrime!



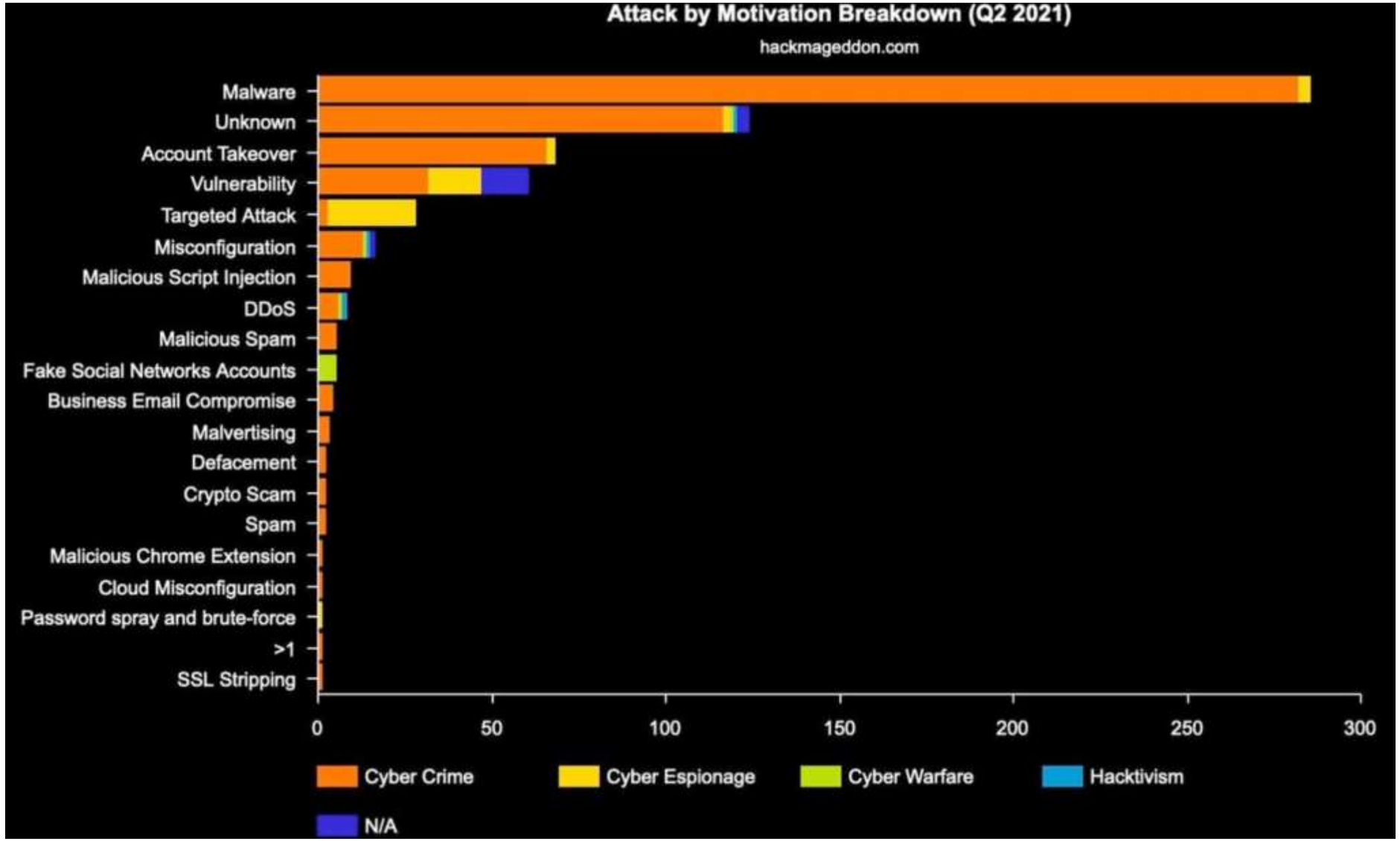
Managerial Aspects and Software environment



Fresh data on Cybercrime!

Managerial Aspects and Software environment

Fresh data on Cybercrime!



It's not just about "bit and bytes"

- Imagine if….. your country would be "cyber attacked" by cyber terrorists?
- **Who…what…how….why….when?**

- HACKMAGEDDON video! (not public)

Buzzwords / 1

- **IDS, IPS, SIEM**….
  - You must have this…
  - Seriously? CSIRTs' users should. The CSIRT itself should not (it's not "mandatory")

- **Packet capture and analysis, Malicious Traffic Detection, Log Processing and correlation…**
  - With the amount of today's data (coming from attacks and malicious traffic) it's not anymore a feasible approach
  - The REAL problem? The human resources
  - You can buy HW and SW. But you cannot buy expert analysts, if there's not enough of them around in your country

Buzzwords / 2

- Technology evolves very quickly
- And open source communities run miracles, somehow ☺
- Originally for this training:
  - Suricata, Zeek (Bro), Snort, AlienVault, OSSIM, SIEMonster, Elastic
  - SiLK, Malcolm, Maltrail (autopsy), apache-scalp, ELK (Elastic + LogStash + Kibana)
- Now:
  - Security Onion
  - Period ☺

Evolution of different approaches

- From the next slides I will **explain WHY the "capture & analyze" approach**, from a National Cybersecurity perspective, **doesn't work anymore**
- After that, **we may run anyway some exercises, rather than shifting to CTI-based** (cyber threat intelligence) **approach**, going on-line and playing with REAL data in REAL time
- We'll use the platform used by our +500 analysts in 5 continents

NOTE

- All of the following thoughts come from **insights and informal talks** among **techies** from **different CERTs** around **the world**.
- It's named "experience" and **it's priceless**.
- The concept is to not "**reinvent the wheel**", if we already have enough wheels.
- The thing here is: **where do I want to drive to**? How much fuel (resources) do I have **available**?
- **Let's be interactive and talk over such topics**, PLEASE!
- This is NOT a "regular" training…
- This people already tried most of the stuff you may think about on these days, and they **took different decisions**

NOTE /2 (stats)

- GARR.it
  - 20.000 Km fiber footprint
  - > 1000 “user’s” sites (GARR Consortium members)
  - > 1.5 Tbps aggregated capacity, > 3.5 Tbps backbone
- Traffic realtime statistics (aggregated on peering): gins.garr.it/Statistics/x_peering.php

NOTE /2 (stats)

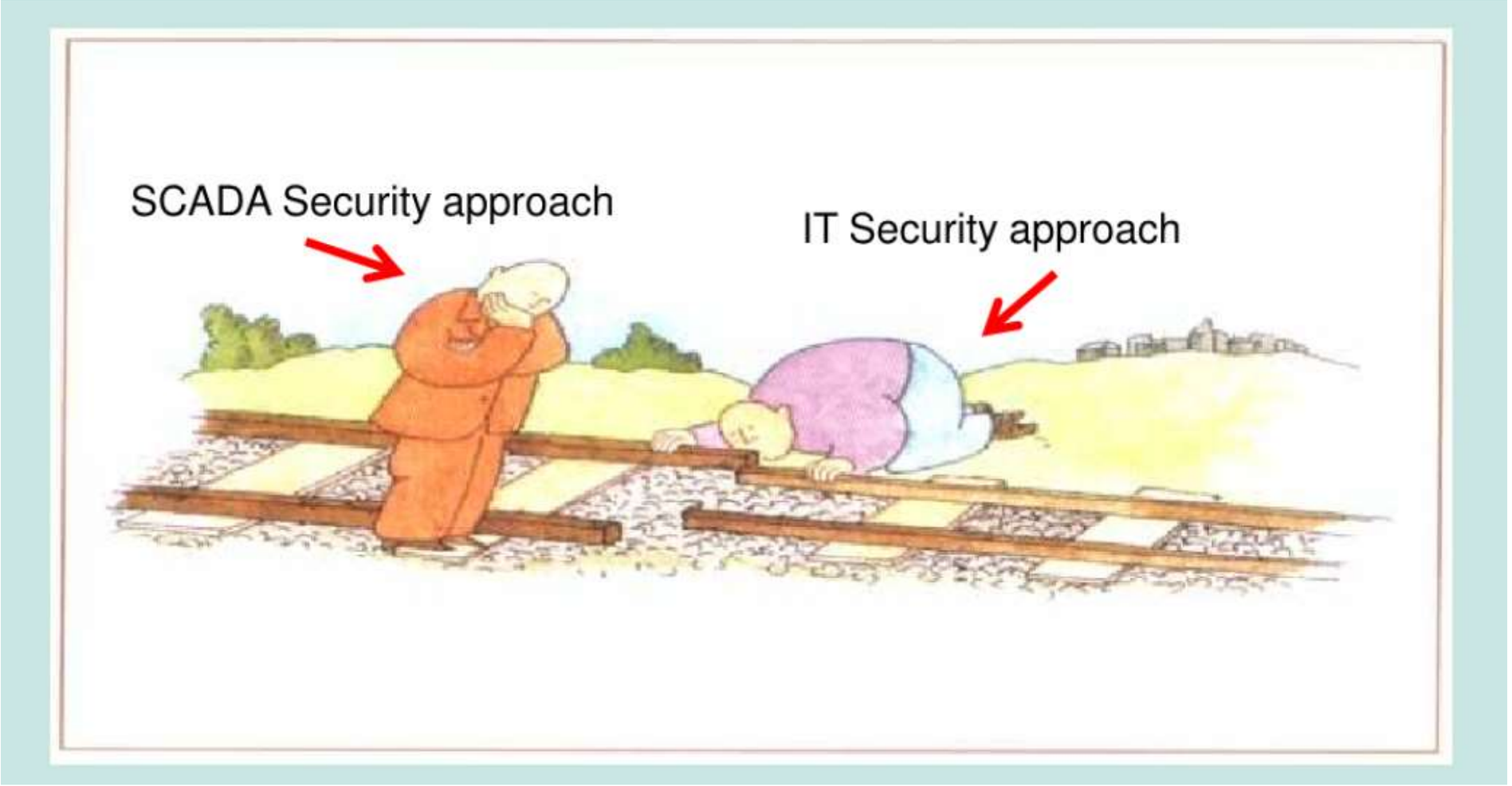
- Pls check with your own eyes: “GARR” environment VS UniBO (University of Bologna) one’s

https://gins.garr.it/Statistics/x_siteservice_viewer.php?target[]=siteservice_246&

[anyway, it’s “just” a 10 GB link, LOL ☺]

THE “OLD” APPROACH

Mindsets and techie's DNAs



SECURITY ONION

- The «less invasive» solution is **Security Onion**
  - It comes with most of the stuff already «on» when you boot the machine(s)
  - https://securityonionsolutions.com/software

- If your background(s) / operating environment includes Network Traffic Analysis as your «daily breed», then Security Onion (SO) is **the tool** for you!
- It’s a threat hunting platform, with SIEM aspects, and much more

Wazuh

- Otherwise, if you background(s) and operating environment, and your “DNA” it’s more a **SysAdm** approach, then wazuh is your tool.

- But, if then you will want to add to wazuh i.e. **the traffic between North and South of a given country**, then forget wazuh, and focus on SO.

Wazuh vs SO

- Everything you get with Wazuh, you find it in SO
- Furthermore:
  - An Incident Response platform (**The hive + Cortex**) *version 3*
  - An Automation Platform: **playbook**
  - A platform to check the health of the system (thanks to **Grafana's timeseries**)
  - A platform to analyze files: **strelka**
  - **mitre att&ck navigator**
  - **fleet server** to manage osquery's agents
  - **community id** to correlate those logs coming from different sources
  - Adopting **ECS** to normalize the data coming from different sources (suricata, zeek)
  - (if you can afford it) **full capture**
  - Full support of endpoint traffic (**osquery, autoruns, sysmon, winlogbeat**...)

Comments

- With SO, the interesting aspect is that **you won't get crazy** to have them **working correctly**.
- All of the tools already are perfectly **integrated**.
- There's also a wide **support for appliances**, i.e. Fortinet
- Each of the «objects» I listed on previous slide do represent **a world aside** (especially IDS):
  - Multiple issues with installation and tuning
  - Hardware, network resources
  - **(Human factor: we'll talk about this later, but keep it as an «overall» concept)**
  - You will need a lot of time to correctly «master» them

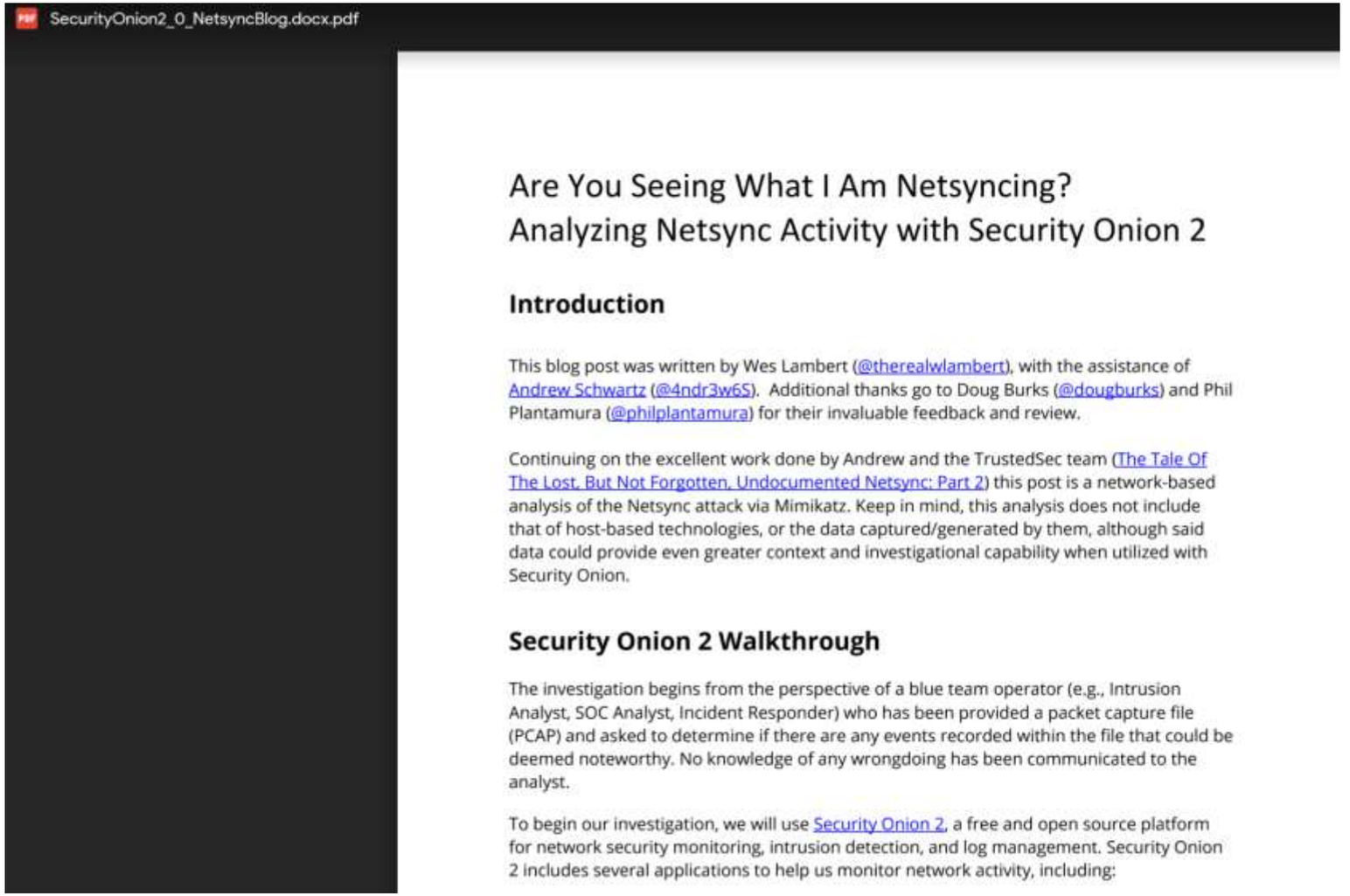
OK I got it… No, I don't need this Raoul, thank you…

- If you **do not have such needs**….
- But at the **same time**, you want to **analyze in a deep way** a **pcap** (Network Analysis Post Mortem, rather than Live Network Forensics, as Selene she will teach you tomorrow)….
- …and you would like to use something **more advanced** than **Wireshark**…
- Bingo! You can use SO in **Import Version**
- **Here you can find an example of the potentialities of SO:**

- https://drive.google.com/file/d/1xKuzWswUeDZrX3HPDZp74BUKQG5LoZ4S/view?usp=sharing

Managerial Aspects and Software environment

(intentionally, I'd prefer you all understanding such concepts starting from Security Onion 2)


SecurityOnion2_0_NetsyncBlog.docx.pdf

Are You Seeing What I Am Netsyncing?
Analyzing Netsync Activity with Security Onion 2

Introduction

This blog post was written by Wes Lambert (@therealwlambert), with the assistance of Andrew Schwartz (@4ndr3w6S). Additional thanks go to Doug Burks (@dougburks) and Phil Plantamura (@philplantamura) for their invaluable feedback and review.

Continuing on the excellent work done by Andrew and the TrustedSec team (The Tale Of The Lost, But Not Forgotten, Undocumented Netsync: Part 2) this post is a network-based analysis of the Netsync attack via Mimikatz. Keep in mind, this analysis does not include that of host-based technologies, or the data captured/generated by them, although said data could provide even greater context and investigational capability when utilized with Security Onion.

Security Onion 2 Walkthrough

The investigation begins from the perspective of a blue team operator (e.g., Intrusion Analyst, SOC Analyst, Incident Responder) who has been provided a packet capture file (PCAP) and asked to determine if there are any events recorded within the file that could be deemed noteworthy. No knowledge of any wrongdoing has been communicated to the analyst.

To begin our investigation, we will use Security Onion 2, a free and open source platform for network security monitoring, intrusion detection, and log management. Security Onion 2 includes several applications to help us monitor network activity, including:

Incident Response

- Now we come to **IR**
- When it got out, Hive 4 installation used to be a real nightmare.
  - Not anymore, now ☺
  - If you wanna try it, I advise to use Hive3 which it's into SO
  - In any case, it's **fully supported**
  - Consider that **Incident Response systems** and **Ticket Trouble Systems** are not really into the same «domain».

MISP and CTI platforms

- Speaking about **MISP** and **CTI** platforms (information sharing e cyber threat intelligence)….
- If you count to «just eat data», instead of misp I would go for **minemel** or **intelmq**, rather than taking a even stronger approach: **importing the feeds in the hive**!
- Otherwise, if you are planning to **share the data**, then choose for misp.
- Anyway, you will **also have to use TheHive**, if you also plan to **manage your incidents** (grin!)
- MISP communities goes much beyond «feeds». They are very interesting and give you access to excellent information

- **Such communities are not opened to everyone**
  - You must **request access**
  - Similar i.e. to my friends at **Spamhaus**, etc.

- **TIP**: adopting MISP+AIL is veryyyy interesting!
- I remember **AIL** can feed also TheHive. Its **github** contains many more interesting tools, such as **Social Network analysis tools**.

- https://github.com/MISP/MISP
- **AIL** is similar to one of the two CTI platform I will show you and it's from the friends at CERT Luxembourg.
- As a difference, with AIL you guys must find the feeds on your own. https://www.circl.lu/services/ail-training-materials/

Case Study: UNIBO

- Here's a useful example from friends at **University of Bologna** (see previous slide about their daily traffic)
- It's a nice case study, because of **economics**
- Architecture:
  - 3 links at 10GB
  - 3 "network port in monitor mode" for each link (I name this "network tap" or "TAP")
  - 9 storage nodes plus 1 master node
  - This little baby generates **5K log per second**
  - When working with **10G links, a zeek probe should have at least 24 core and 64GB RAM.**
    - **Suricata it depends on how many signatures you load into it. But that's the average HW need if you plan to build such a baby**
    - Their appliances are very interesting, especially because they look much more "smaller" (LOL)
    - I don't know the pricing
  - **But consider that a 10G tap, no matter from which Vendor, costs around 80K EUR**
  - **With SO, you can make it with less than 3K EUR**
  - Then as I said, Security Communities we do run!
  - i.e. SO 2.3 already was much more performant than SO 2.0
- Spare thoughts:
  - Do you have a LAB at your CSIRT where to run such benchmarks?
  - Unless you have a kind of "big budget" for hardware stuff…. Try to built something internally
  - **Don't relay on Vendors too much, please!**

SO 2.3
(and the tale of Security Onion conference)

- During the last Security Onion Conference (OCT 2020) version 2.3 was presented.
- I was there, along with folks and friends from different **EU CERTs and CSIRTs**
- There's the **streaming available**, here:
  - https://blog.securityonion.net/2020/10/security-onion-conference-2020.html
  - Or, for short: https://securityonionsolutions.com/conference
- SO is now "labeled" (it can be seen) as a "mix" of Distro and Respository
- Pros: easy to use, easy to manage

SO 2.3: what's new (and why you should be interested)

- When I told you before "far beyond Wazuh", here's some of the reasons of my statement

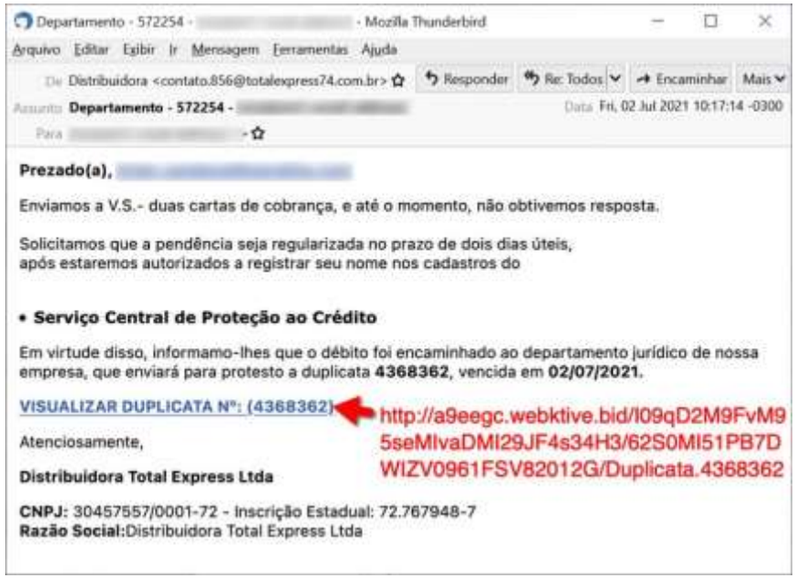
- Along with the "usual" detection engine (zeek and suricata), SO folks added the following, sexy stuff:
  - They changed the **full capture engine**, in order to **handle and manage IPv6**
  - An **IR** system (Incident Response: the hive + cortex)
  - An **automation** system (playbook)
  - A **threat hunting** system (soc)
  - A **file analysis** system (strelka)
  - **Mitre att&ck** (analysis and correlation)
  - **Integrating** what we call «North-South traffic» (servers <-> clients traffic) and East-West traffic (inside the data centers)
  - **Community id** to **correlate logs** from **different sources**, and **different tools**
  - **Log normalization** using ECS from elk-fleet + osquery, and much more…

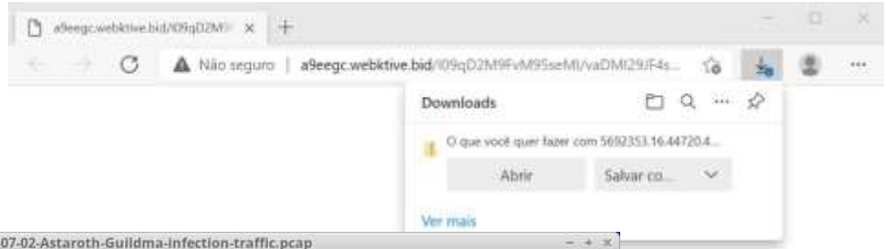
Choosing “what” depends on “who” (you are)

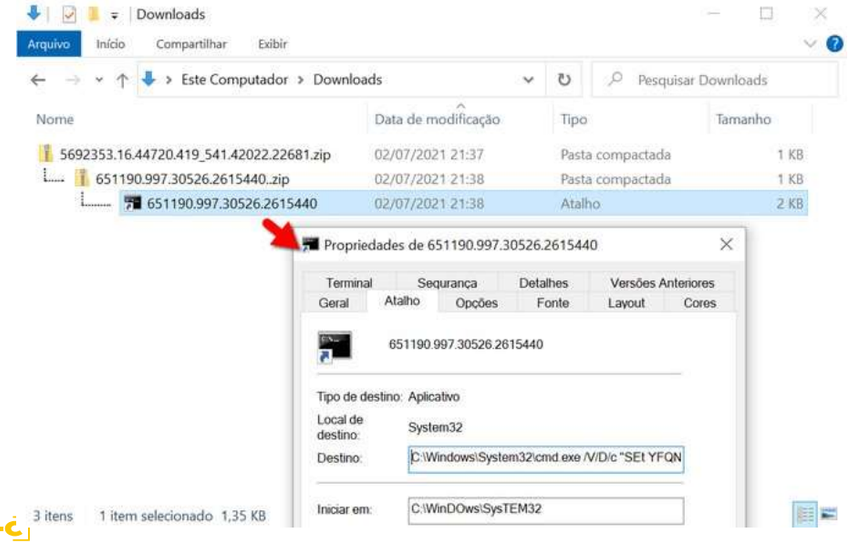
- If you belong to a Blue team…
- if your daily job is Cybersecurity..
- If you do not have those hundreds of thousands EUR to spend…
- Then you will find in SO a very serious, alternative solution
- **SO is totally open source**
- I strongly invite you to watch the conference recordings
- Further info on SO 2:
  - https://blog.securityonion.net/2020/10/security-onion-2-has-reached-general.html

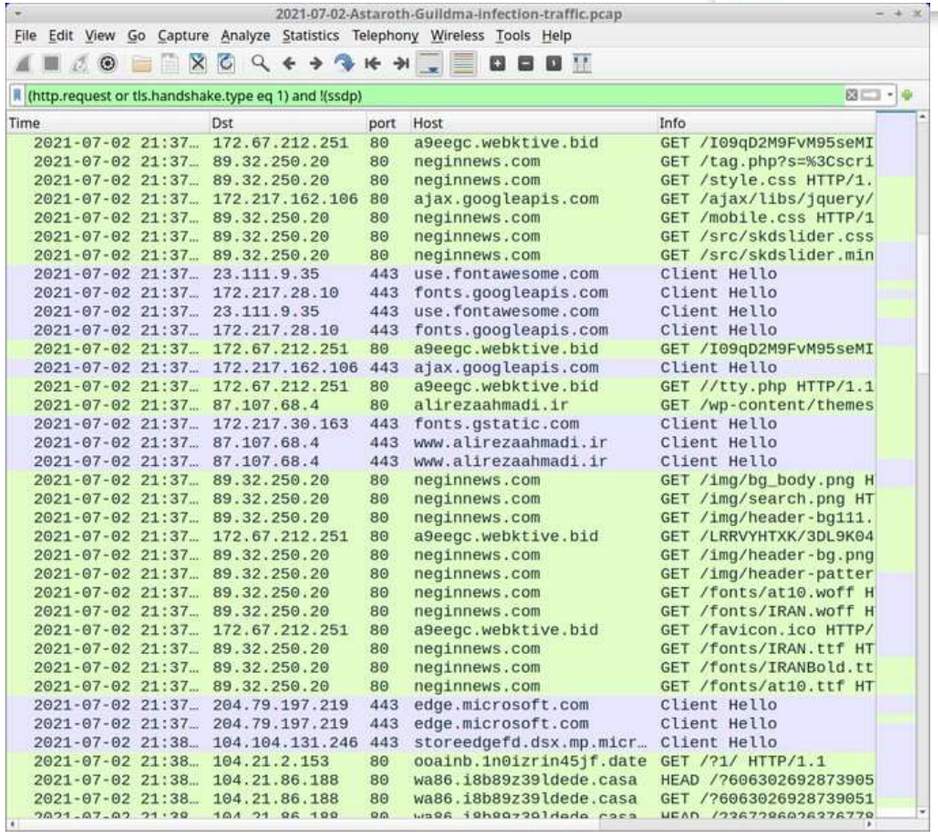
Managerial Aspects and Software environment

How does it look like, when you use it?









Managerial Aspects and Software environment

How does it look like, when you use it?

	Count ▼	rule.name
🔔	526	ET DNS Query to a .tk domain - Likely Hostile
🔔	9	ET DNS Query to a *.top domain - Likely Hostile
🔔	5	ET INFO HTTP POST Request to Suspicious *.ga Domain
🔔	5	ET INFO HTTP Request to a *.ga domain
🔔	4	ET INFO DNS Query for Suspicious .gq Domain
🔔	3	ET INFO DNS Query for Suspicious .cf Domain
🔔	3	ET INFO DNS Query for Suspicious .ga Domain
🔔	3	ET INFO DNS Query for Suspicious .ml Domain
🔔	1	ET INFO EXE - Served Attached HTTP
🔔	1	ET INFO HTTP POST Request to Suspicious *.gq domain
🔔	1	ET INFO HTTP Request to a *.date domain
🔔	1	ET INFO HTTP Request to a *.gq domain
🔔	1	ET INFO PowerShell Hidden Window Command Common In Powershell Stagers M1
🔔	1	ET MALWARE Likely Malicious Windows SCT Download MSXMLHTTP AX M2
🔔	1	ET POLICY PE EXE or DLL Windows file download HTTP

Managerial Aspects and Software environment

How does it look like, when you use it?

Count	event.module ▲	event.dataset	http.virtual_host
15	zeek	http	neginnews.com
8	zeek	http	wa86.i8b89z39ldede.casa
5	zeek	http	a9eegc.webktive.bid
1	zeek	http	4b0ddc0f8956802871583519f0383b5b.mifahfjheijjgfoosdspdsfjeummcsde.ga
1	zeek	http	4c0d1fa067186f2e5db94bffa7f05fb4.mifahfjheijjgfoosdspdsfjeummcsde.ga
1	zeek	http	ajax.googleapis.com
1	zeek	http	alirezaahmadi.ir
1	zeek	http	b389d4484a3df27544c79cd0e2ccc436.mifahfjheijjgfoosdspdsfjeummcsde.ga
1	zeek	http	c26f48940a185559ca2e5cbf35e10136.mifahfjheijjgfoosdspdsfjeummcsde.ga
1	zeek	http	db32f60504be4e233be92d895ef0c516.bhisfieahahprfjhchpjbcipuuhopfeb.gq
1	zeek	http	f8db5951fcc6d67d9cba15cf0d1c4307.mifahfjheijjgfoosdspdsfjeummcsde.ga
1	zeek	http	ooainb.1n0izrin45jf.date

Managerial Aspects and Software environment

How does it look like, when you use it?

Count	event.module	event.dataset
5,002	zeek	dns
2,167	zeek	conn
565	suricata	alert
145	zeek	file
38	zeek	ssl
37	zeek	http
33	zeek	x509
8	zeek	notice
2	zeek	pe

Managerial Aspects and Software environment

How does it look like, when you use it?

```
GET /7606382692872985125833851280071134 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.8
Host: wa86.i8b89z28ldede.casa
Cookie: cidade=CFXX; estado=CFXX; pais=BR; PHPSESSID=ipk708kubt9lp5012vavd6r45j

HTTP/1.1 200 OK
Date: Fri, 02 Jul 2021 21:38:58 GMT
Content-Type: application/octet-stream
Content-Length: 2853888
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Disposition: attachment; filename="vbnhopunpc.zip"
Content-Transfer-Encoding: binary
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=QqofWQf6ragMrA3Sh4xz%2F1untiUFPtU48r3KV4QaJ3b1titZehL2%2BetHPnbbKbedfQ9UJS4aV4yzBAFVOAtlKXnlYJXippZzCl2FL1jG5vB94MuzCFSs9GXDITlkIPwR502Oxrerk%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 668b05f7afe221b5-MIA
alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400

MZP.....@.....!..L.!..This program must be run under Win32
$7.....PE..L.
....`.....$.....#.....$...@.....P,.....%.....%.V.....
L.....%.,.....%.{.....%.....
.....text.....#.....#.....itext.....#.....#.....data...(B....$..D....$.....@....bss.....e....%.....idata..
V.....%.....$.....@....didata.....%.....%.....@....edata.....%.....%.....@..@.rdata..E....%.....%.....@..@.reloc.....%.....%.....@..B.rs
rc....L.....L...@+.....@..@.....P,.....+.....@..@.....@....Boolean.....@..False.True.
System....4.@...AnsiChar.....P.@...Char.....h.@...ShortInt.....@...SmallInt.....@...Integer.....@...Byte.....@...Word.....
@...Cardinal.....@...Pointer.....@...Int64.....$.@...UInt64.....X.@...NativeInt.....t.@..
NativeUInt.....@...Single.....@...Extended.....@...Double.....@...Comp.....@...Currency.....@...ShortString.....@...PAnsiChar0.@.....@...PWideChar1.@.....@...ByteBoo
l.....[.@..False.True.System...\.@...WordBool.....X.@..False.True.System.....@...LongBool.....@..False.True.System.....@...string.....@..
WideString.....@.
```

A few words of buzzwords like SIEMs, etc

- Ok, now let's stop for a moment.
  - Before we began this lesson, I'm sure that words such as "SIEM", "correlating data", "xIDS", "network taps", etc were **into your mind**, isn't it?
- A SIEM (Security Information and Event Management) by definition is a **trashcan** on which **you put «stuff»**.
  - Credits: «some security-addicted guys inside GARR community» **Now, «what you should do» with this «stuff»? It's up to take this decision…**
- Just like all of the SIEMs, wazuh also has got a set of rules/policies/check/etc.
  - Average speaking, all of this **works pretty good**, **helping** you covering **80%-90% of scenarios**.
  - But, those **remaining 20%-10%** it is **up to you.**

SIEMs – axioms and lesson learnt

1. You don’t have enough time to train a SIEM?
   - Then, you don’t need a SIEM
2. Wazuh is too much difficult / holistic?
   - Any kind of commercial SIEM won’t be less.

SIEMs – axioms and lessons learnt

1. **Wazuh makes too much "noise"?**
   - Any kind of SIEM makes noise.
   - Why? Because the collection of "basic events"builds the ground from which you can **deduct the anomaly** (and most of all, **detect it**!).
   - If you take a look at **Wazuh app** on **kibana**, you will notice many stuff "you cannot understand". Thus, you may think "it's useless" or "I don't need it".
   - **WRONG!**

2. Let's pick up **an easy scenario: a brute-force attack.**
   - **The very first step** is to collect all the login tries (the "failed" ones, of course). To be more clear:
     - **Wrong password**
     - **Username not existing**
     - **Misconfigurations**
     - **etc**

Then, **second step** will be to **extract a behaviour** from these events.

Here's when and where SIEM gets in!

A Rule will create the Alert when such pattern will be recognized.

3. **Something else** a SIEM can do is: generating an answer to an incident (**Remediation**).
   - **Which "Type of Answer" will (or, "should") this be?**
   - **YOU decide this, basing on the SCENARIO, and the ENVIRONMENT which has been impacted.**

4. **What's the truth?**

- There's not a "magic solution".
- There's not a unique answer.
- From my field experiences:
- Different scenarios and different environments = different reactions
- Along with… different tools, different Mos, different resources, different risks, thus different budgets.
- What I mean is that for the same given problem, all of you will probably adopt different strategies. No one is the right one or the wrong one.

SIEMs – axioms and lessons learnt /2

1. **Wazuh doesn't solve my problem.**
   - A SIEM is an **object which alerts on issues and problems.**
   - The **reaction to the problem** must be **understood**, then **engineered**.
   - **Wazuh has a wonderful engine for hardening/assessment ("sca**", even better if along with / next to **osquery**).
   - **If that's not enough for you, then you can expand with open-scap and cis-cat: these two tools are really powerful, created by NIST and CIS.**

2. Let's pick up **another example: patching issues.**
   - **Since "paranoia is a virtue", at least in Cybersecurity, everyday we do all patch our systems, right?**
   - This scenario should let all of us kinda of "**relaxed**".
   - If **this is what you think**, well… then SIEM will tell **you are wrong**!
   - There are (many) vulns which do not have a patch, yet. Different reasons. **(We'll see 0days market later, don't worry!** ☺
   - i.e. **Vulnerability Detector** alerts you on this, and even tells you of the pagch exists.
   - **SCA** tells you if there are "config" issues, and advises you on **how to handle them**.
   - **This isn't enough?**
   - Use **open-scap** (which is partially already configured in **Wazuh**), BUT **forget** "tips and advices" in such a case.
   - The **good thing** here is that you can **choose the check-level** (more or less "deep / strong").
   - **Still not enough??**
   - **Then BUY the license for cis-cat, BUT be aware of performances!**
   - **And, do pay attention to file permissions….. !!!**
   - Thanks to **Wazuh,** we **discovered a machine on which the gem installation was made in a «too much permissive manner»: the code was writable to everyone!!** ☹
   - **Now, such a functionality can be deployed in 1000 different ways…. But all of this can fit into a unique consolle.**

SIEMs – axioms and lessons learnt /3

1. **Yeah but.. Whatever Wazuh does, I can make it with a |grep**
   - Using “grep” is very useful on those scenarios with a **very few machines, and a few logfiles**.
   - Using **ELK to digest data** means running queries which are **much more effective** rather than a “grep”.
   - It also means to **speed up the research timings** by a x100 factor (!).
   - Using **analytics components of ELK** means bringing the **SIEM to alert new anomalies**, more or less dangerous.
   - If this is the case, then you will **train your SIEM to mitigate this**.

2. **Wazuh can be compromised.**
   - **If a machine is compromised, then everything running on it, it’s compromised.**
   - **After the «hack» of the machine, next steps for the attackers would be to keep silent every kind of objects which may alert the compromise (Anti Virus & co).**
   - **To silent Wazuh the attacker needs to change the policies, without Wazuh-manager to notice this.**
   - **It’s not so easy, since the agent alerts for «important» changes on the machine (thus, if a policy has been modified).**
   - **I’m not saying Wazuh is «invincible», but it’s not so easy to force him sleeping.**

I would have **many many more examples** and **lessons I learned** (i.e.: **with Snort, open source VS commercial products, SSLPP topic [**SSL Dynamic Pre-Processor**], analyzing encrypted traffic, ntopng [**ja3, ja3s, hashssh, and many detection algos**],** rather than **a specific idea** from my friends at different CERTs and CSIRTs, which brings us at the end of this section, opening a **new world** by using a **totally new** and **different approach** – **which is the one that me and Selene we use** (next slide).

All around, take a look at this, I love it:

https://www.ntop.org/ndpi/how-encryption-changed-network-traffic-monitoring-finally/

SIEMs – axioms and lessons learnt /4

1. **Let's think for a "unbeteable" solution.**
   - Let's use **Security Onion** with **Bro** and **Suricata**. And let's use also **Ntopng**.
   - **Still, not enough for me, sorry. Why??**
   - Because **each** one of these products **does thing better than others**.
   - Moreover, **we got too much data**, and we have to learn on **how to correlate them** (**Data Analytics**).
   - And, we may use also **IP Reputation**, because often different playgrounds produces different **false positives**.

Then, what's the solution?

What you learn 'till now will probably be USELESS, I'm sorry.

«Nice theory, nice tools, everything cool but… this is NOT the way.» (Raoul Chiesa)

This brings me to the next and last part of this session, which is about a CTI-based approach.

Keywords:

✓ **Cyber Threat Intelligence**

✓ **MISP**

✓ **AIL**

<u>Time is never enough</u>, so i'll walk you through on LIVE sessions, with REAL DATA.

A few words about Security Communities

- I'm a member of some of them. It's just **the right thing to do.**
- And, often you will find:
  - Next-generation approaches
  - Niche topics you ever thinked about
  - A bunch of experts like you, sharing the same passion for InfoSec
  - Closed networks of experts (and expertise)

Benefits from Security Communities: examples

- APWG.org (and APWG.eu)
  - Anti-Phishing working Group
- The best ever **knowledge of insights of Cybercrime** when dealing with "**phishing**"
- An **operational approach** to the problem(s)
- Open minded, humble specialists (like Peter Cassidy)
- Let's see a very fresh (JUL 2021), **practical example**:

PhishFarm Block List Latency Monitoring Program Proposal

APWG APPLIED RESEARCH

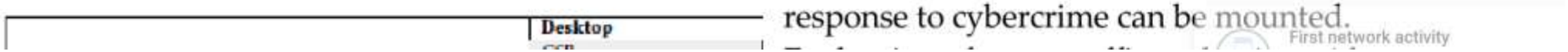
PhishFarm Block List Latency Monitoring Program Proposal
An APWG Applied Research Counter-Cybercrime Data Logistics Initiative

Block List Performance and the Global Confrontation with Cybercrime

Browser block list efficacy is one of the greatest public-health challenges on the World Wide Web today: Independent, academic studies and industrial analyses have found widely variable block list performance with failure rates (e.g. omission in adding reported URLs) of scale, in a number of scenarios, that apparently leave large proportions of users open to the most deviously designed phishing websites.

APWG PHISHFARM
APPLIED RESEARCH

Each block list has its own strengths and weaknesses,[1] but the larger point is that without consistent metrics for performance measurement of common cybercrime-response infrastructure, such as browser block lists, no coherent dialog about whole-of-ecosystem response to cybercrime can be mounted.



Managerial Aspects and Software environment

PhishFarm
Block List
Latency
Monitoring
Program
Proposal

		Desktop	
		GSB	
Experiment	Batch	Coverage	Median Speed
Experiment A (Baseline)		92.9%	00:57 (hh:mm)
Experiment B (Basic Evasion)	JavaScript Cloaking	88.3%	01:03
	Mobile Cloaking	100.0%	00:55
Experiment C (Typical Evasion - Redirection)	bit.ly Redirection - Lure	86.1%	01:25
	bit.ly Redirection - Landing	86.1%	02:58
	.com Redirection - Lure	83.3%	01:44
	.com Redirection - Landing	88.9%	02:48
	.com Redirection w/ .htaccess	80.2%	01:36
	.com Redirection w/ .htaccess - Landing	84.3%	02:43
Experiment D (Domain re-use)	bit.ly Redirection - Lure	96.3%	01:09
	bit.ly Redirection - Landing	97.2%	02:03
	.com Redirection - Lure	95.7%	01:10
	.com Redirection - Landing	98.1%	02:10
	.com Redirection w/ .htaccess - Lure	93.8%	01:13
	.com Redirection w/ .htaccess - Landing	95.4%	02:17
Experiment E (Discovery)	Reported to APWG	98.1%	02:47
	Reported to PayPal	16.2%	01:06
Experiment F (Emerging Evasion)	Mouse Movement Cloaking	0.0%	-
	CAPTCHA Cloaking	0.0%	-
	Notification Cloaking	0.0%	-
	.htaccess Cloaking	100.0%	01:37
	Mouse Movement Cloaking w/.htaccess		
	CAPTCHA Cloaking w/.htaccess		
	Notification Cloaking w/.htaccess		
Experiment G (Reporting Methods)	Standard URL Report	20.4%	00:38
	Chrome Suspicious Site Reporter (CSSR)	90.7%	10:13

Figure 1 *PhishTime: Continuous Longitudinal Measurement of Effectiveness of Anti-phishing Blacklists (Table 4). 'Coverage' addresses percentage of phishing URLs reported that are actually lodged on tested block lists. Google Safe Browsing coverage and speed to block report from PhishTime paper shown above.*

Managerial Aspects and Software environment

PhishFarm
Block List
Latency
Monitoring
Program
Proposal

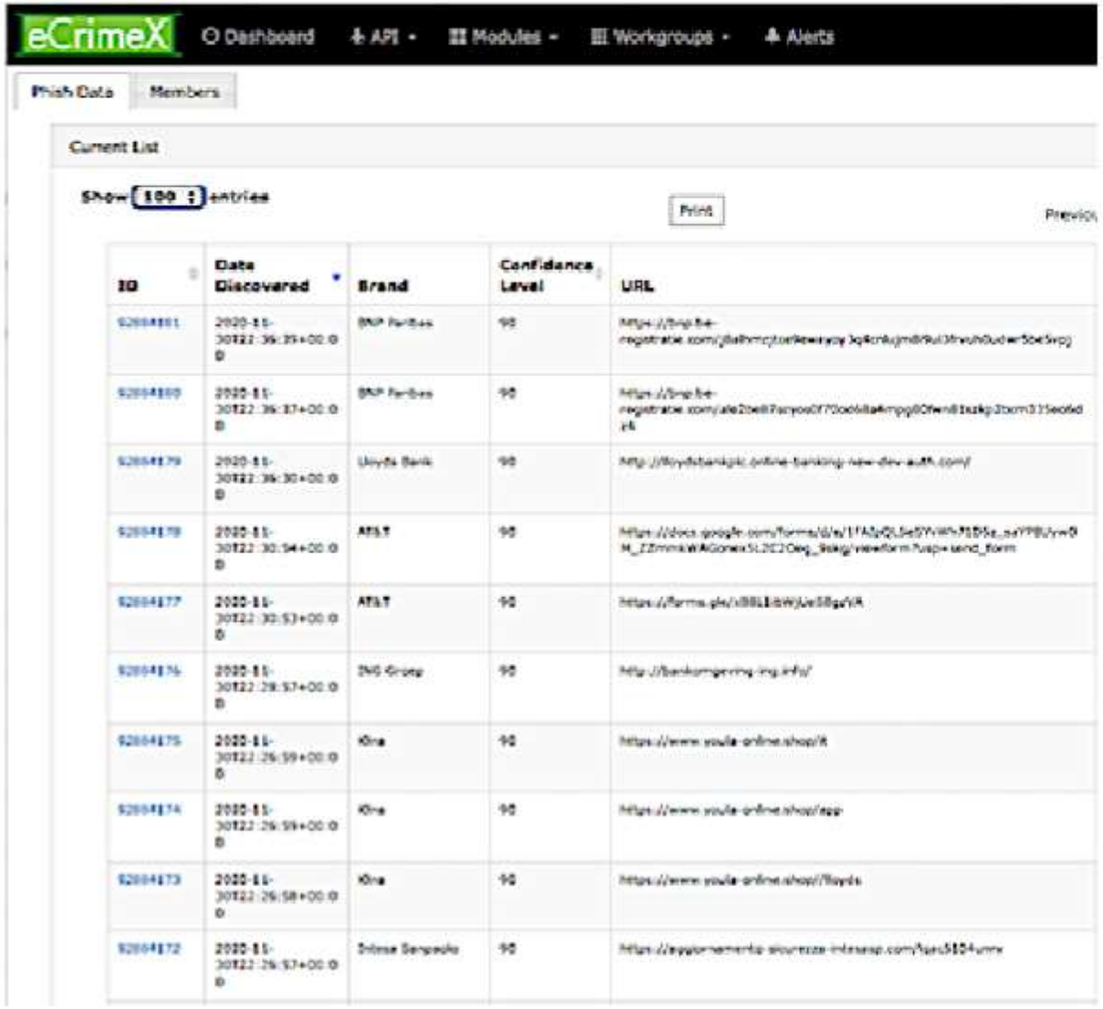


Figure 2 The eCrime eXchange and its progenitors have been clearing cybercrime machine event data for APWG members and correspondents without interruption since 2004

PhishFarm Block List Latency Monitoring Program Proposal

Rigging APWG eCrime eXchange for Continuous Blocklist Monitoring

The PhishFarm monitoring system as it is currently deployed at Arizona State University's Center for Cybersecurity and Digital Forensics is an experimentation platform developed by researchers to examine the efficacy of browser block list systems for their capacity to negotiate the cloaking and evasion techniques that are increasingly employed by cybercrime gangs to prevent their phishing websites from being detected. That successful years-long program of research in its largest study, however, ran a sample of some 4,000-plus experimenter-created, artificial phishing websites' URLs through the reporting mechanisms of major browser block lists. The prototype will be substantially augmented for continuous monitoring of latency of

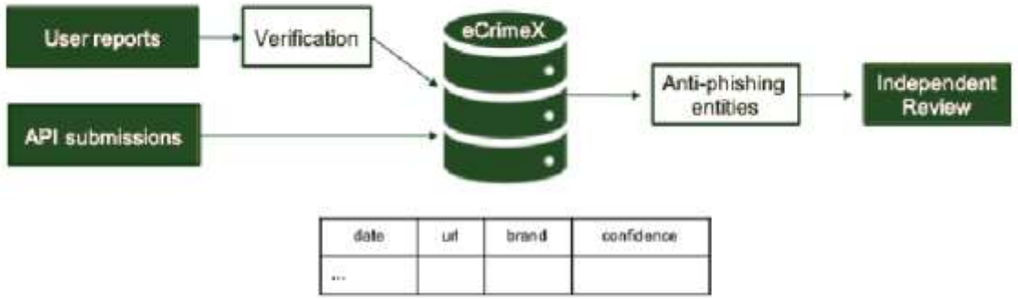
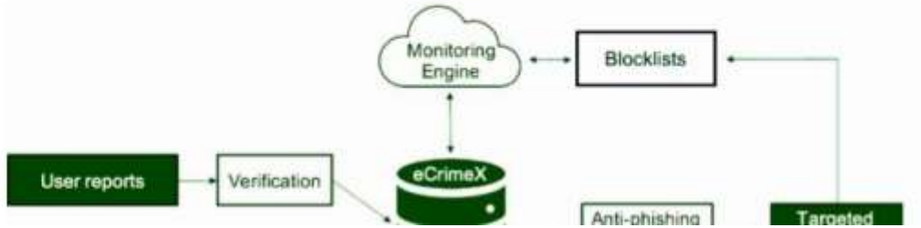


Figure 3 *The APWG eCrime eXchange time stamps phishing URLs at time of submission with other meta data for programmatic interventions and investigative routines managed by forensic professionals*

With these metrics, industry can establish conventions of accountability for the data



PhishFarm Block List Latency Monitoring Program Proposal

APWG PHISHFARM APPLIED RESEARCH METRICS TECH

- Who is supporting us now?

PayPal RSA facebook HITACHI Inspire the Next Hitachi Systems

- Are you interested? Contact me privately, and I'll walk you through this, introducing you to the right people at APWG: you will love them! ☺
- Why should you be interested? Because we all need an offensive, operational approach when fighting Cybercrime.
- And, **we must think ahead: we cannot just sit down on our chairs and analyze logs and data traffic…. !!!**

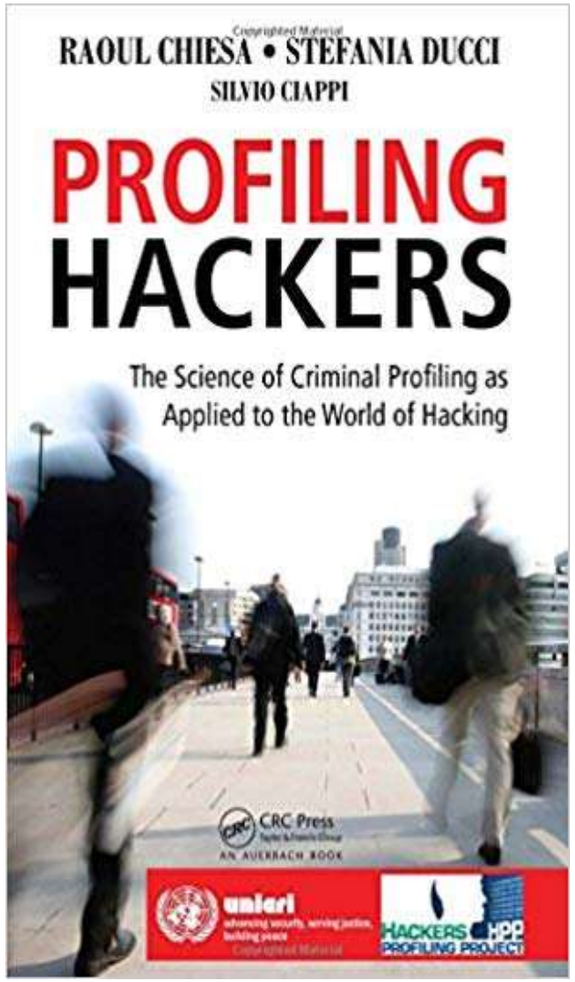
Benefits from Security Communities: examples

- **ISECOM.org**
  - Institute for Security and Open Methodologies (USA, EU)
- The best ever **knowledge of insights on Penetration Testing**
- **We wrote the OSSTMM (Open Source Security Testing Methodology Manual). Period.**
- **Got a CEH? Forget it.. it's lame ☹**
  - **See ISECOM's OPST, OPSA, OPSE, OWSE, etc**
- Learn from **OSSTMM v3** (public) and v4 (under Peer Review) different views such as:
  - RAVs and RAV Calculator
  - Security Metrics
  - STAR sheet
  - Interconnected security domains when pentesting
    - Including **Physical Security** and **Web Applications**!

Books

- Not forgetting that Security Professionals must keep on and update their knowledges!
- And… reading books is a good way to.

Hackers Profiling



- Applied Research started back in 2004
- Field research started in 2006 (still on-going)
- Law Enforcement Officers and Government Agencies loved our profiling approach
- FBI Academy Library in Quantico (VA)
- Special Agents (cybercrimes) must-read book
- Translated in different languages
- Cutting-edge milestone from the previous “Black-hat / White-hat” approach

Managerial Aspects and Software environment

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

The 9 profiles

Managerial Aspects and Software environment

PROFILE	MAY BE LINKED TO	WILL CHANGE ITS BEHAVIOR?	TARGET	(NEW) MOTIVATIONS & PURPOSES
Wanna Be Lamer		**No**		
Script Kiddie	Urban hacks	**No**	**Wireless Networks, Internet Café, neighborhood, etc..**	
Cracker	Phishing Spam Black ops	**Yes**	**Companies, associations, whatever**	**Money, Fame, Politics, Religion, etc…**
Ethical Hacker	Massive Vulnerabilities	**Probably**	**Competitors (Telecom Italia Affair), end-users**	**Big money**
Quiet, Paranoid, Skilled Hacker	Black ops	**Yes**	**High-level targets**	**Hesoteric request (i.e., hack "Thuraya" for us)**
Cyber-Warrior	CNIs attacks Gov. attacks	**Yes**	**"Symbols": from Dali Lama to UN, passing through CNIs and business companies**	**Intelligence ?**
Industrial Spy		**Yes**	**Business company / Corporation**	**For profit**
Government Agent		**Probably**	**Government / Suspected Terrorist/ Strategic company/ Individual**	**Espionage/ Counter-espionage Vulnerability test Activity-monitoring**
Military Hacker		**Probably**	**Government / Strategic company**	**Monitoring / controlling / crashing systems**

Managerial Aspects and Software environment

DETERRENCE EFFECT OF:	LAWS	CONVICTIONS SUFFERED BY OTHER HACKERS	CONVICTIONS SUFFERED BY THEM	TECHNICAL DIFFICULTIES
Wanna Be Lamer	NULL	NULL	ALMOST NULL	HIGH
Script Kiddie	NULL	NULL	HIGH: they stop after the 1st conviction	HIGH
Cracker	NULL	NULL	NULL	MEDIUM
Ethical Hacker	NULL	NULL	HIGH: they stop after the 1st conviction	NULL
Quiet, Paranoid, Skilled Hacker	NULL	NULL	NULL	NULL
Cyber-Warrior	NULL	NULL	NULL	NULL: they do it as a job
Industrial Spy	NULL	NULL	NULL	NULL: they do it as a job

Managerial Aspects and Software environment

- **Leonardo “Leo” Lanzi**, GARR-CERT (IT)
- Dr. Prof. **Mrs**. **Adriana “auntie” Franca,** The Security Brokers (IT)
- All of the **Network and Cybersecurity people** at University of Bologna (IT)
- **Mrs. Rabiyatou “Rabi” BAH**, (FR), for making this training happened
- **Almerindo Graziano** and **Lawrence Ikhabi Muchilwa** @ SilenSec, for the **Cyber Ranges** courtesy: kudos!
- **Benjamin Delphy** aka **Gentilkiwi**, author or **Mimikatz** (aka *kdll, kdllpipe, katz, mimikatz*) (FR)
- **Paul Sparrows** (Paolo Passeri) (IT)
- **Kevin “The Condor” Mitnick**
- **Pete Herzog**, ISECOM (USA, ES)
- **Peter Cassidy**, APWG (USA)
- Multiple security communities:
  - ✓ ISECOM
  - ✓ OWASP
  - ✓ ICANN
  - ✓ APWG
  - ✓ INTERPOL
  - ✓ TEAM CYMRU
  - ✓ Hackmageddon.com
  - ✓ Operation Trust / OPS-T

Credits

End of story

Now that we have all this useful information, **it would be nice to do something with it**. (Actually, it can be emotionally fulfilling just to get the information. This is usually only true, however, if you have **the social life of a glass of water**.)

Unix Programmer's Manual
ISECOM's mantra (Pete Herzog, Director).

Managerial Aspects and Software environment

Thank you

Contact:

Raoul Chiesa

Cybersecurity Expert

rc@security-brokers.com

OCWAR-C
12 Charles de Gaulle Street Asokoro,
Abuja - NIGERIA
contact@ocwarc.eu