

**FCT**

Fundação para a Ciência e a Tecnologia  
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

**FCCN**

Computação  
Científica Nacional

# Resposta a Incidentes (II)

Pedro Silva



# Agenda

- Introdução
- Casos Práticos



# INTRODUÇÃO

# Enquadramento



BITNINJA



**CERT  
RCTS**

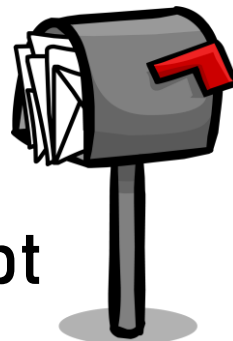


**NETPROTECT**



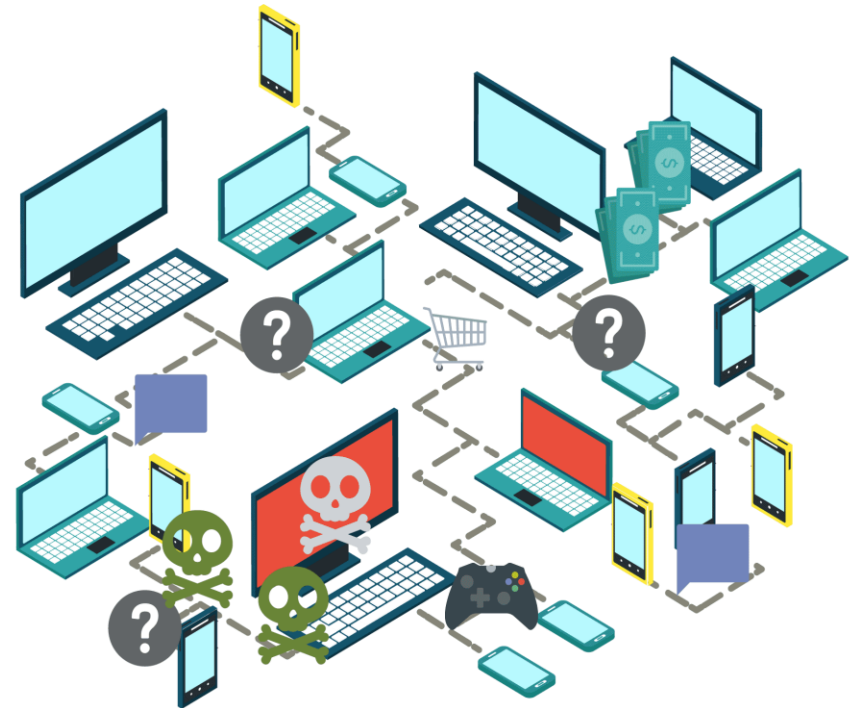
**abusix**

report@cert.rcts.pt



# Tipos de incidentes

- Malware
- Availability
- Information collection
- Intrusion
- Intrusion attempt
- Information Security
- Fraud
- Abusive content
- Vulnerability
- Other





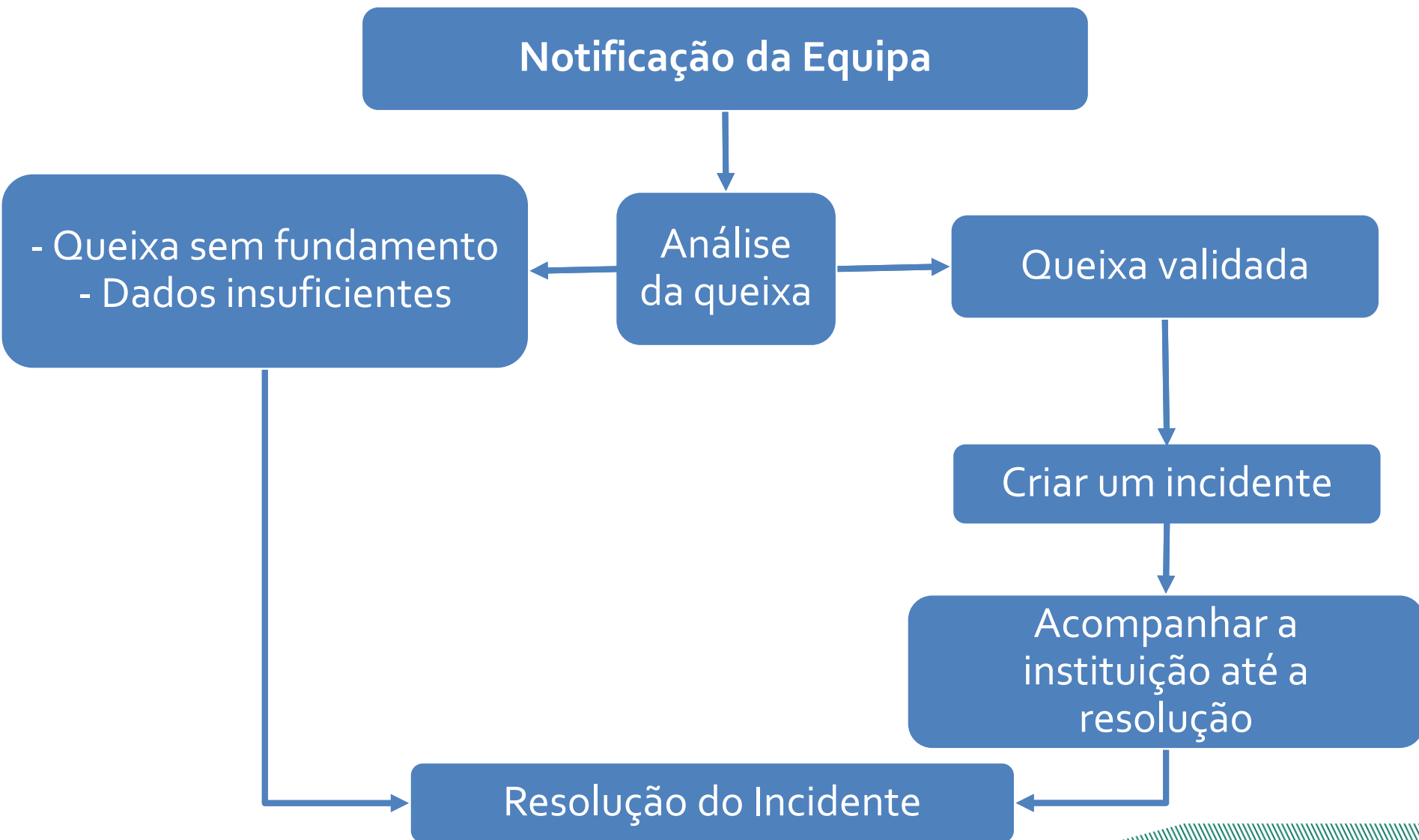
# Taxonomia

- Abusive Content
  - (Child) Sexual Information Gathering
  - Exploitation/Sexual/Social Engineering
  - Stalking/Intimidation



- Masquerade
- Phishing
- Unauthorized use of resources

# Tratamento de Incidentes: Prática



# CASOS PRÁTICOS



# Incidente I



Good morning,

we detected a DOS attack from your network.

Below the logs.

```
-----  
XXX.XXX.XXX.XXX - - [06/May/2021:18:24:53 +0200] "POST /xmlrpc.php HTTP/1.0" 403 1031 "-"  
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0"  
XXX.XXX.XXX.XXX - - [06/May/2021:18:43:27 +0200] "GET /wp-login.php HTTP/1.0" 200 1250 "-"  
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0"
```

(...)

```
XXX.XXX.XXX.XXX - - [07/May/2021:03:25:02 +0200] "POST /wp-login.php HTTP/1.0" 200 2049 "-"  
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0"  
XXX.XXX.XXX.XXX - - [07/May/2021:03:25:03 +0200] "POST /xmlrpc.php HTTP/1.0" 403 212 "-"  
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0"  
-----
```

Please take action as soon as possible. The destination IP of the attack from your network is:  
web.mercurio.vhosting-it.com

Kind regards  
Abuse Department  
VHosting Solutionz

**Classe de Incidente: Tentativa de Intrusão**  
**Tipo de Incidente: Exploitation of known vulnerabilities**

# Incidente II



From Abusix <noreply@abusix.org> ☆  
Subject [REPORT-CERT] Abusix Potentially Compromised Account Report  
To report@cert.rcts.pt ★



username	pw_sha1	source_ip	timestamp	human_date
123xxx@xxxxxx.pt	daf71	89.38.97.144	1614823226	2021-03-04T02:00:26.000Z
xpto3@xxxx.xxxx.pt	dd1a2	89.38.97.144	1614824085	2021-03-04T02:14:45.000Z
5678234@xxxxx.pt	aa876	89.38.97.144	1614824716	2021-03-04T02:25:16.000Z

usefulness of these reports to you.

This data is collected by observing hosts abusing our traps and sending SMTP AUTH credentials to external domains. Note that we do not store usernames and passwords, just the usernames.

**Classe de Incidente: Intrusions**  
**Tipo de Incidente: Unprivileged Account Compromise**

# Incidente III



Hello,

An attempt to brute-force account passwords over SSH/FTP by a machine in your domain or in your network has been detected. Attached are the host who attacks and time / date of activity. Please take the necessary action(s) to stop this activity immediately. If you have any questions please reply to this email.

Logfile entries (time is CE(S)T):

```
Sun Apr  4 03:41:40 2021: user: root service: ssh target: 178.250.10.10 source: xxx.xxx.xxx.xxx
Sun Apr  4 03:35:58 2021: user: root service: ssh target: 185.39.220.238 source: xxx.xxx.xxx.xxx
Sun Apr  4 02:19:33 2021: user: root service: ssh target: 178.250.9.170 source: xxx.xxx.xxx.xxx
Sun Apr  4 00:18:38 2021: user: ftpuser service: ssh target: 178.250.10.81 source: xxx.xxx.xxx.xxx
Sat Apr  3 15:53:44 2021: user: root service: ssh target: 37.228.156.147 source: xxx.xxx.xxx.xxx
Sat Apr  3 15:43:27 2021: user: admin service: ssh target: 77.75.254.104 source: xxx.xxx.xxx.xxx
Sat Apr  3 11:01:26 2021: user: ftpuser service: ssh target: 37.228.154.190 source: xxx.xxx.xxx.xxx
Sat Apr  3 04:27:08 2021: user: root service: ssh target: 178.250.15.203 source: xxx.xxx.xxx.xxx
Fri Apr  2 22:13:59 2021: user: root service: ssh target: 37.228.156.34 source: xxx.xxx.xxx.xxx
Fri Apr  2 18:26:31 2021: user: ubnt service: ssh target: 77.75.251.211 source: xxx.xxx.xxx.xxx
Fri Apr  2 14:25:51 2021: user: jojo service: ssh target: 85.158.183.141 source: xxx.xxx.xxx.xxx
Fri Apr  2 11:29:41 2021: user: root service: ssh target: 178.250.14.16 source: xxx.xxx.xxx.xxx
Fri Apr  2 10:44:16 2021: user: root service: ssh target: 37.228.155.157 source: xxx.xxx.xxx.xxx
Thu Apr  1 20:31:40 2021: user: ipko service: ssh target: 37.228.155.226 source: xxx.xxx.xxx.xxx
Wed Mar 31 11:42:19 2021: user: admin service: ssh target: 37.228.156.22 source: xxx.xxx.xxx.xxx
Wed Mar 31 10:54:53 2021: user: amx service: ssh target: 77.75.254.18 source: xxx.xxx.xxx.xxx
Wed Mar 31 07:02:42 2021: user: admin service: ssh target: 77.75.249.92 source: xxx.xxx.xxx.xxx
Wed Mar 31 02:24:57 2021: user: root service: ssh target: 37.228.154.153 source: xxx.xxx.xxx.xxx
Tue Mar 30 20:11:29 2021: user: admin service: ssh target: 77.75.255.133 source: xxx.xxx.xxx.xxx
Tue Mar 30 18:48:46 2021: user: admin service: ssh target: 185.39.220.151 source: xxx.xxx.xxx.xxx
Tue Mar 30 12:31:21 2021: user: admin service: ssh target: 77.75.255.139 source: xxx.xxx.xxx.xxx
Tue Mar 30 03:31:17 2021: user: vpn service: ssh target: 178.250.10.249 source: xxx.xxx.xxx.xxx
```

...

Regards,  
Profihost AG Team

**Classe de Incidente: Tentativa de Intrusão**

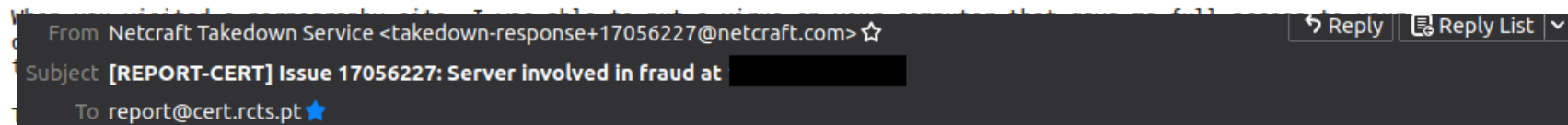
**Tipo de Incidente: Tentativa de login**

# Incidente IV



Greetings.

I monitored your device on the net for a long time and successfully managed to hack it.  
It was not difficult for me, as I have been in this business for a long time.



Hello,

We have discovered an email server on your network that is sending e-mail messages that are attempting to extort users.

The server has the IP address [redacted].

We have attached an example fraudulent e-mail demonstrating the e-mail server's involvement. Please close down this attack as soon as possible.

More information about the detected issue is provided at <https://incident.netcraft.com/e4303f5c4511/>

Many thanks,

Netcraft

Phone: +44(0)1225 447500  
Fax: +44(0)1225 448600  
Netcraft Issue Number: 17056227

I am also automatically notified when this email is opened.

If you do not know how to transfer money and what Bitcoin is. Then type "Buy Bitcoin" into Google

As soon as I receive a transfer of the required amount, the system will automatically inform me about the received payment and offer to delete from my servers all the data I received from you.  
And therefore, I will confirm the deletion.

Do not try to complain anywhere, as a purse does not track, mail from where the letter came, and is not tracked and created automatically, so there is no point in writing to me.  
If you try to share this email with anyone, the system will automatically send a request to the servers and they will proceed to upload all the data to social networks.  
Also, changing passwords in social networks, mail, device will not help you, because all the data is already downloaded to a cluster of my servers.

Good luck and don't do anything stupid.

Classe de Incidente Information Gathering  
Tipo de Incidente Phishing

# Incidente V



Hello,

This is a notification of unauthorized uses of systems or networks.

On July 19, 2021, a total of 1 IP addresses from your networks probed my servers for TCP open ports. Due to their dubious behavior, they are suspected to be compromised botnet computers.

The log of TCP port scans is included below for your reference (time zone is UTC). To prevent this mail from getting too big in size, at most 5 attempts from each attacker IP are included. Those connection attempts have all passed TCP's 3-way handshake, so you can trust the source IP addresses to be correct.

If you regularly collect IP traffic information of your network, you will see the IPs listed connected to various TCP ports of my server at the time logged, and I suspect that they also connected to TCP ports of many other IPs.

If a Linux system was at the attacker's IP, you might want to use the command "netstat -ntp" to list its active network connections. If there is still some suspicious connection, find out what PID/program/user ID they belong to. You might find something to help you solve this problem.

Please notify the victims (owners of those botnet computers) so that they can take appropriate action to clean their computers, before even more severe incidents, like data leakage, DDoS, and the rumored NSA spying through hijacked botnets, arise. This also helps prevent botnets from taking up your network bandwidth.






Classe de Incidente Information Gathering  
Tipo de Incidente Scanning

----- log of TCP port scans (time zone is UTC; sent to report@cert.rcts.pt) -----

(time in UTC)=2021-07-19T14:41:24 (attacker's IP)=xxx.xxx.xxx.xxx (IP being scanned)=150^116^77^189 (TCP port being scanned)=1433  
(time in UTC)=2021-07-19T17:19:00 (attacker's IP)=xxx.xxx.xxx.xxx (IP being scanned)=150^116^77^192 (TCP port being scanned)=1433  
(time in UTC)=2021-07-19T17:19:01 (attacker's IP)= xxx.xxx.xxx.xxx (IP being scanned)=150^116^77^192 (TCP port being scanned)=1433  
(time in UTC)=2021-07-19T17:19:03 (attacker's IP)= xxx.xxx.xxx.xxx (IP being scanned)=150^116^77^192 (TCP port being scanned)=1433  
(time in UTC)=2021-07-19T17:19:04 (attacker's IP)= xxx.xxx.xxx.xxx (IP being scanned)=150^116^77^192 (TCP port being scanned)=1433



# Em Resumo

-  Usar as mesmas credenciais em vários sistemas
-  Sistemas em produção e expostos à Internet
-  Sistemas actualizados
-  Antivírus / AntiMalware
-  Emails



# Obrigado