





CLASSIFICAÇÃO DE INCIDENTES

João Machado RCTS CERT







QUESTÃO #1:



- Information Gathering Social Engineering
- 2) Fraud Phishing
- 3) Abusive Content Spam
- 4) Other Undetermined



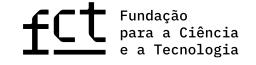


QUESTÃO #1:



- 1) Information Gathering Social Engineering
- 2) Fraud Phishing
- 3) Abusive Content Spam
- Other Undetermined





QUESTÃO #2:

CSIRT BOX

Host of attacker: pt 11 11 11 1 -> nat-alunos-n1-1.0000 | -> nat-aluno

```
Logfile entries (time is CE(S)T):
Wed Jan 6 16:33:45 2021: user: MikroTik service: ssh target:
Wed Jan 6 16:33:45 2021: user: MikroTik service: ssh target: source: source:
Wed Jan 6 16:32:51 2021: user: default service: ssh target:
Wed Jan 6 16:32:48 2021: user: default service: ssh target:
Wed Jan 6 16:32:48 2021: user: default service: ssh target: In the source: In the source:
Wed Jan 6 16:32:41 2021: user: default service: ssh target:
Wed Jan 6 16:32:40 2021: user: default service: ssh target:
Wed Jan 6 16:32:39 2021: user: default service: ssh target:
Wed Jan 6 16:32:37 2021: user: default service: ssh target:
Wed Jan 6 16:32:36 2021: user: default service: ssh target:
Wed Jan 6 16:32:33 2021: user: default service: ssh target:
Wed Jan 6 16:32:31 2021: user: default service: ssh target:
Wed Jan 6 16:32:31 2021: user: default service: ssh target: | Source: 
Wed Jan 6 16:32:30 2021: user: default service: ssh target:
Wed Jan 6 16:32:28 2021: user: default service: ssh target: Indiana source: Indiana source:
Wed Jan 6 16:32:28 2021: user: default service: ssh target:
Wed Jan 6 16:32:27 2021: user: default service: ssh target:
Wed Jan 6 16:32:26 2021: user: default service: ssh target:
Wed Jan 6 16:32:26 2021: user: default service: ssh target:
Wed Jan 6 16:32:25 2021: user: default service: ssh target: In the source: In the source: In the source is source.
Wed Jan 6 16:32:25 2021: user: default service: ssh target:
Wed Jan 6 16:32:25 2021: user: default service: ssh target:
Wed Jan 6 16:32:24 2021: user: default service: ssh target: In Inc. | Source: In Inc
Wed Jan 6 16:32:24 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:22 2021: user: default service: ssh target:
Wed Jan 6 16:32:22 2021: user: default service: ssh target:
Wed Jan 6 16:32:21 2021: user: default service: ssh target:
Wed Jan 6 16:32:21 2021: user: default service: ssh target: In the source: In the source:
Wed Jan 6 16:32:21 2021: user: default service: ssh target:
Wed Jan 6 16:32:20 2021: user: default service: ssh target:
Wed Jan 6 16:32:19 2021: user: default service: ssh target:
```

- L) Intrusion Attempts Login attempts
- 2) Information Gathering Scanning
- 3) Intrusion Unprivileged Account Compromise
- 4) Availability Denial of Service





QUESTÃO #2:

CSIRT BOX

Host of attacker: philing => nat-alunos-n1-1. philing => maying |
Responsible email contacts: abuse@philing | report@cert.rcts.pt
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts in our Network: philing | report@cert.rcts.pt |
Attacked hosts | rep

```
Logfile entries (time is CE(S)T):
Wed Jan 6 16:33:45 2021: user: MikroTik service: ssh target:
Wed Jan 6 16:33:45 2021: user: MikroTik service: ssh target: source: source:
Wed Jan 6 16:32:51 2021: user: default service: ssh target:
Wed Jan 6 16:32:48 2021: user: default service: ssh target:
Wed Jan 6 16:32:48 2021: user: default service: ssh target: In the source: In the source:
Wed Jan 6 16:32:41 2021: user: default service: ssh target:
Wed Jan 6 16:32:40 2021: user: default service: ssh target:
Wed Jan 6 16:32:39 2021: user: default service: ssh target:
Wed Jan 6 16:32:37 2021: user: default service: ssh target:
Wed Jan 6 16:32:36 2021: user: default service: ssh target:
Wed Jan 6 16:32:33 2021: user: default service: ssh target:
Wed Jan 6 16:32:31 2021: user: default service: ssh target:
Wed Jan 6 16:32:31 2021: user: default service: ssh target: | Source: 
Wed Jan 6 16:32:31 2021: user: default service: ssh target:
Wed Jan 6 16:32:30 2021: user: default service: ssh target:
Wed Jan 6 16:32:28 2021: user: default service: ssh target: Indiana source: Indiana source:
Wed Jan 6 16:32:28 2021: user: default service: ssh target:
Wed Jan 6 16:32:27 2021: user: default service: ssh target:
Wed Jan 6 16:32:26 2021: user: default service: ssh target:
Wed Jan 6 16:32:26 2021: user: default service: ssh target: In Jan 5 source: In Jan 6 land source:
Wed Jan 6 16:32:25 2021: user: default service: ssh target:
Wed Jan 6 16:32:25 2021: user: default service: ssh target:
Wed Jan 6 16:32:25 2021: user: default service: ssh target:
Wed Jan 6 16:32:24 2021: user: default service: ssh target: In Inc. | Source: In Inc
Wed Jan 6 16:32:24 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:23 2021: user: default service: ssh target:
Wed Jan 6 16:32:22 2021: user: default service: ssh target:
Wed Jan 6 16:32:22 2021: user: default service: ssh target:
Wed Jan 6 16:32:21 2021: user: default service: ssh target:
Wed Jan 6 16:32:21 2021: user: default service: ssh target: In the source: In the source:
Wed Jan 6 16:32:21 2021: user: default service: ssh target:
Wed Jan 6 16:32:20 2021: user: default service: ssh target:
Wed Jan 6 16:32:19 2021: user: default service: ssh target:
```

- .) Intrusion Attempts Login attempts
- 2) Information Gathering Scanning
- 3) Intrusion Unprivileged Account Compromise
- 4) Availability Denial of Service





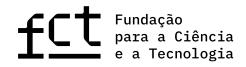
QUESTÃO #3:

```
Received: from wuhanmobilephone by hk2.cycom.asia with local (Exim 4.95)
    (envelope-from <support@wuhanmobilephonenumberlist.com>)
    id 1oHOUz-0002sG-G5
    for x;
    Fri, 29 Jul 2022 21:57:53 +0800
To: x
Subject: =?UTF-8?Q?Csomagja tart=C3=A1sban van!?=
X-PHP-Script: wuhanmobilephonenumberlist.com/wp-content/pluqins/jbntksx/LEAF.php for WH 11.1111
X-PHP-Originating-Script: 1167:LEAF.php
Date: Fri, 29 Jul 2022 13:57:53 +0000
From: =?UTF-8?Q?UPSDelivery=C2=AE?= <support@wuhanmobilephonenumberlist.com>
Message-ID: <829a
                                         8ae6@wuhanmobilephonenumberlist.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
   boundary="b1 829a76a4c087eabddc8bcd19748a8ae6"
Content-Transfer-Encoding: 8bit
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - hk2.cycom.asia
X-AntiAbuse: Original Domain - tmit.bme.hu
X-AntiAbuse: Originator/Caller UID/GID - [1167 994] / [47 12]
X-AntiAbuse: Sender Address Domain - wuhanmobilephonenumberlist.com
X-Get-Message-Sender-Via: hk2.cycom.asia: authenticated id: wuhanmobilephone/from h
X-Authenticated-Sender: hk2.cycom.asia: support@wuhanmobilephonenumberlist.com
X-Source:
X-Source-Args:
X-Source-Dir:
This is a multi-part message in MIME format.
--b1 829a76a4c087eabddc8bcd19748a8ae6
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
Tisztelt ÃSTqyfelÃ⅓nk,
Sajnos, nem lehetett kã©zbesã-teni a csomagot 514901185421.
Ha egy UPS szervizpont bã³l szeretne gyujteni, vagy mã;sik kã©zbesã-tã©si lehetosã©get szeretne vã;lasztani, Expressz Szã;llã-tã;si dã-j (362,74
HUF). Kérjük, kövesse a linket, erÅPUlsÃ-tse meg a kézbesÃ-tést.https://upsdelivery.com/tracknum514.421/
```



- 1) Abusive Content Spam
- Fraud Phishing
- Intrusion Attempts Login attempts
- Vulnerable Information Disclosure





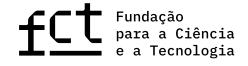
QUESTÃO #3:

```
Received: from wuhanmobilephone by hk2.cycom.asia with local (Exim 4.95)
    (envelope-from <support@wuhanmobilephonenumberlist.com>)
    id 1oHOUz-0002sG-G5
    for x;
    Fri, 29 Jul 2022 21:57:53 +0800
To: x
Subject: =?UTF-8?Q?Csomagja tart=C3=A1sban van!?=
X-PHP-Script: wuhanmobilephonenumberlist.com/wp-content/pluqins/jbntksx/LEAF.php for WH 11.1111
X-PHP-Originating-Script: 1167:LEAF.php
Date: Fri, 29 Jul 2022 13:57:53 +0000
From: =?UTF-8?Q?UPSDelivery=C2=AE?= <support@wuhanmobilephonenumberlist.com>
Message-ID: <829a
                                         8ae6@wuhanmobilephonenumberlist.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
   boundary="b1 829a76a4c087eabddc8bcd19748a8ae6"
Content-Transfer-Encoding: 8bit
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - hk2.cycom.asia
X-AntiAbuse: Original Domain - tmit.bme.hu
X-AntiAbuse: Originator/Caller UID/GID - [1167 994] / [47 12]
X-AntiAbuse: Sender Address Domain - wuhanmobilephonenumberlist.com
X-Get-Message-Sender-Via: hk2.cycom.asia: authenticated id: wuhanmobilephone/from h
X-Authenticated-Sender: hk2.cycom.asia: support@wuhanmobilephonenumberlist.com
X-Source:
X-Source-Args:
X-Source-Dir:
This is a multi-part message in MIME format.
--b1 829a76a4c087eabddc8bcd19748a8ae6
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
Tisztelt ÃSTqyfelÃ⅓nk,
Sajnos, nem lehetett kã©zbesã-teni a csomagot 514901185421.
Ha egy UPS szervizpont bã³l szeretne gyujteni, vagy mã;sik kã©zbesã-tã©si lehetosã©get szeretne vã;lasztani, Expressz Szã;llã-tã;si dã-j (362,74
HUF). Kérjük, kövesse a linket, erÅPUlsÃ-tse meg a kézbesÃ-tést.https://upsdelivery.com/tracknum514.421/
```



- **Abusive Content Spam**
- Fraud Phishing
- Intrusion Attempts Login attempts
- Vulnerable Information Disclosure





QUESTÃO #4:

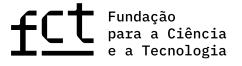
```
SenseLog id [80 1 017]
Message [ApacheWpXmlrpc]]style='padding:10px 20px; background:#e6e6e6;margin-bottom:10px'>Url: [numismaticaitaliana.net/xmlrpc.php]
Remote connection: [148446]
Headers: [arrav (
  'Host' = & gt; 'numismaticaitaliana.net',
  'Content-Type' = &qt; 'application/x-www-form-urlencoded; Charset=UTF-8',
  'Accept' =&qt; '*/*',
  'User-Agent' = & gt; 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)',
  'Content-Length' = > '193',
  'BN-Frontend' =&qt; 'captcha-https',
  'X-Forwarded-Port' = > '443',
  'X-Forwarded-Proto' => 'https',
  'BN-Client-Port' => '44739',
  'X-Forwarded-For' => '1994',
) ]
Post data: [Array
   [<methodCall&gt;&lt;methodName&gt;wp getUsersBlogs&lt;/methodName&gt;&lt;param&gt;&lt;param&gt;&lt;value&gt;&lt;string&gt;admin&lt;/string&gt;
   </value&gt;&lt;/param&gt;&lt;param&gt;&lt;value&gt;&lt;/meth
   odCall>] =>
]style='padding:10px 20px; background:#e6e6e6; margin-bottom:10px'>Url: [numismaticaitaliana.net/wp-login.php]
Remote connection: [144.114.148450]
Headers: [array (
  'Host' = & gt; 'numismaticaitaliana.net',
  'Content-Type' => 'application/x-www-form-urlencoded; Charset=UTF-8',
  'Accept' => '*/*',
  'User-Agent' =&qt; 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)',
  'Content-Length' => '42',
  'BN-Frontend' => 'captcha-https',
  'X-Forwarded-Port' => '443',
  'X-Forwarded-Proto' => 'https',
  'BN-Client-Port' => '44739',
  ) ]
Post data: [Array
   [log] => admin
                                             Intrusion - Exploration of known Vulnerability
   [pwd] =&qt; coronavirus
   [wp-submit] => Log In
```



]

- Abusive Content Spam
- Information Gathering Scanning
- Intrusion Attempts Login attempts





QUESTÃO #4:

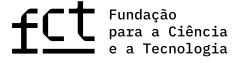
```
SenseLog id [80 1 017]
Message [ApacheWpXmlrpc]]style='padding:10px 20px; background:#e6e6e6;margin-bottom:10px'>Url: [numismaticaitaliana.net/xmlrpc.php]
Remote connection: [148446]
Headers: [arrav (
  'Host' = & gt; 'numismaticaitaliana.net',
  'Content-Type' = &qt; 'application/x-www-form-urlencoded; Charset=UTF-8',
  'Accept' =&qt; '*/*',
  'User-Agent' = & gt; 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)',
  'Content-Length' = > '193',
  'BN-Frontend' =&qt; 'captcha-https',
  'X-Forwarded-Port' = > '443',
  'X-Forwarded-Proto' => 'https',
  'BN-Client-Port' =&qt; '44739',
  'X-Forwarded-For' => '1994',
) ]
Post data: [Array
   [<methodCall&gt;&lt;methodName&gt;wp getUsersBlogs&lt;/methodName&gt;&lt;param&gt;&lt;param&gt;&lt;value&gt;&lt;string&gt;admin&lt;/string&gt;
   </value&gt;&lt;/param&gt;&lt;param&gt;&lt;value&gt;&lt;/meth
   odCall>] =>
]style='padding:10px 20px; background:#e6e6e6; margin-bottom:10px'>Url: [numismaticaitaliana.net/wp-login.php]
Remote connection: [144.114.148450]
Headers: [array (
  'Host' = & gt; 'numismaticaitaliana.net',
  'Content-Type' => 'application/x-www-form-urlencoded; Charset=UTF-8',
  'Accept' => '*/*',
  'User-Agent' =&qt; 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)',
  'Content-Length' => '42',
  'BN-Frontend' = & gt; 'captcha-https',
  'X-Forwarded-Port' => '443',
  'X-Forwarded-Proto' => 'https',
  'BN-Client-Port' => '44739',
  ) ]
Post data: [Array
   [log] => admin
                                             Intrusion - Exploration of known Vulnerability
   [pwd] =&qt; coronavirus
   [wp-submit] => Log In
```

- Abusive Content Spam
- Information Gathering Scanning
- **Intrusion Attempts Login attempts**





]



QUESTÃO #5:

```
style='padding:10px 20px; background:#e6e6e6:margin-bottom:10px'>{
"correlated logs":
"pr apacheaccess":
-- [25/Dec/2021:17:43:57 +1100] &guot: POST /profiles/minimal/index.php HTTP/1.1&guot: 200 50 &guot: http://sdahealth.org/profiles/minimal/index.php&guot: &guot: Mozilla/5.0 (Linux: U; Android 9: en-gb; Redmi 7A Build/PKQ1.190319.001)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/71.0.3578.141 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.9.8-g&guot: combined".
"pr wafaccess":
sdahealth.org -- [25/Dec/2021:17:43:58 +1100] " POST /profiles/minimal/index.php HTTP/1.0" 200 191 "http://sdahealth.org/profiles/minimal/index.php" "Mozilla/5.0 (Linux; U; Android 9; en-gb; Redmi 7A
Build/PKQ1.190319.001) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/71.0.3578.141 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.9.8-a&quot: &quot:client-port [30830]&quot:
"malware uploaded": "/home/sdaheal/public html/dzkpr/cache/oaytoglz.php",
"malware_name": "{SA-MD5}PHP.Backdoor.lhiacrfo"
}Url: [queennailslubbock.com/h7xafbm9.php]
Remote connection:
Headers: [array (
'Host' => 'queennailslubbock.com'.
'Connection' =&at: 'close'
'Referer' => 'http://queennailslubbock.com/h7xafbm9.php',
'Content-Length' => '32185',
'Content-Type' => 'application/x-www-form-urlencoded'
'Accept-Language' => 'en-US,en;q=0.8',
"User-Agent" =&gt: "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"
Post data: [Array
[kjcicw] =>
0818060817123c52175c56175d5943114b594f58465401574e0e5056420803214403765f44560041080e054f51590e0e1057035c510a46131f0a1c0a0c495d4a40006e440603441f070104434351140b27074453284f51594645575b0c5e4c3c505f5f170a7c6c7f617d4000
|style='padding:10px 20px; background:#e6e6e6;margin-bottom:10px'>Url: [queennailslubbock.com/991mzpu7.php]
Remote connection:
Headers: [array (
'Host' => 'queennailslubbock.com',
'Connection' => 'close'
'Referer' => 'http://queennailslubbock.com/991mzpu7.php',
'Content-Length' => '63833',
'Content-Type' => 'application/x-www-form-urlencoded'
'Accept-Language' => 'en-US,en;q=0.8',
'User-Agent' => 'Mozilla/5.0 (Linux; Android 8.1.0; SM-A260G) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Mobile Safari/537.36',
Post data: [Array
1213525912526f0246584e160a5b0f0e465646405f0e015156420751411356221404711502735451761d5207590a5a695e0717115315110506505f100a466a410c5347045143037715020279242d7b1d540e155771131d26460420080007585b443d16514108510c47045
]
```

- Intrusion Application Compromise
- Availability Denial of Service
- Information Gathering Sniffing
- Intrusion Attempts Exploration of Known Vulnerability





QUESTÃO #5:

```
{
"correlated logs":
"pr apacheaccess":
-- [25/Dec/2021:17:43:57 +1100] "POST /profiles/minimal/index.php HTTP/1.1" 200 50 "http://sdahealth.org/profiles/minimal/index.php" "Mozilla/5.0 (Linux; U; Android 9; en-gb; Redmi 7A Build/PKQ1.190319.001)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/71.0.3578.141 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.9.8-g&guot: combined".
"pr wafaccess":
sdahealth.org 💴 -- [25/Dec/2021:17:43:58 +1100] "POST /profiles/minimal/index.php HTTP/1.0" 200 191 "http://sdahealth.org/profiles/minimal/index.php" "Mozilla/5.0 (Linux; U; Android 9; en-gb; Redmi 7A
Build/PKQ1.190319.001) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/71.0.3578.141 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.9.8-a&quot: &quot:client-port [30830]&quot:
"malware uploaded": "/home/sdaheal/public html/dzkpr/cache/oaytoglz.php",
"malware_name": "{SA-MD5}PHP.Backdoor.lhiacrfo"
}Url: [queennailslubbock.com/h7xafbm9.php]
Remote connection:
Headers: [array (
'Host' => 'queennailslubbock.com'.
'Connection' =&at: 'close'
'Referer' => 'http://queennailslubbock.com/h7xafbm9.php',
'Content-Length' => '32185',
'Content-Type' => 'application/x-www-form-urlencoded',
'Accept-Language' => 'en-US,en;q=0.8',
"User-Agent" =&gt: "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"
Post data: [Array
[kjcicw] =>
0818060817123c52175c56175d5943114b594f58465401574e0e5056420803214403765f44560041080e054f51590e0e1057035c510a46131f0a1c0a0c495d4a40006e440603441f070104434351140b27074453284f51594645575b0c5e4c3c505f5f170a7c6c7f617d4000
|style='padding:10px 20px; background:#e6e6e6;margin-bottom:10px'>Url: [queennailslubbock.com/991mzpu7.php]
Remote connection:
Headers: [array (
'Host' => 'queennailslubbock.com',
'Connection' => 'close'
'Referer' => 'http://queennailslubbock.com/991mzpu7.php',
'Content-Length' => '63833',
'Content-Type' => 'application/x-www-form-urlencoded'
'Accept-Language' => 'en-US,en;q=0.8',
'User-Agent' => 'Mozilla/5.0 (Linux; Android 8.1.0; SM-A260G) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Mobile Safari/537.36',
Post data: [Array
1213525912526f0246584e160a5b0f0e465646405f0e015156420751411356221404711502735451761d5207590a5a695e0717115315110506505f100a466a410c5347045143037715020279242d7b1d540e155771131d26460420080007585b443d16514108510c47045
]
```

- Intrusion Application Compromise
- Availability Denial of Service
- Information Gathering Sniffing
- **Intrusion Attempts Exploration of Known Vulnerability**





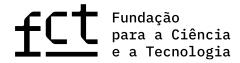
QUESTÃO #6:

```
rv:62.0) Gecko/20100101 Firefox/62.0&quot
- [04/Oct/2021:23:02:45 +0100] "POST /downloader//downloader/index.php HTTP/2" 404 16412 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0"
- [04/Oct/2021:23:05:28 +0100] "POST /downloader//downloader/index.php HTTP/2" 404 15911 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0"
Message [ApacheMagentoDownloader]]style='padding:10px 20px; background:#e6e6e6;margin-bottom:10px'>Url: [cn-plumbing.co.uk/admin/]
Remote connection:
Headers: [array (
'Host' => 'cn-plumbing.co.uk',
'User-Agent' =&qt; 'Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0',
'Content-Lenath' =&at: '491'.
'Content-Type' => 'multipart/form-data; boundary=0197f06d23908177bc3691b33f381930a53f28e0998034c51c020bff4970'
'Accept-Encoding' => 'gzip',
'Connection' =&at: 'close'.
'BN-Frontend' => 'captcha-https',
'X-Forwarded-Port' => '443',
'X-Forwarded-Proto' => 'https'.
'BN-Client-Port' => '36588'.
Post data: [Array
[password] => hemmingw
[redirect] => https://cn-plumbing.co.uk/admin//index.php?route=common/login
[username] =&at: admin
|Url: [www.handryersuk.co.uk/admin/]
Remote connection:
Headers: [array (
'Host' => 'www.handryersuk.co.uk',
'User-Agent' =&qt; 'Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0',
'Content-Length' => '495'
'Content-Type' =&qt; 'multipart/form-data; boundary=dffbab523ede0670fc40028aad027dcbd422fba18d7be6296af1d78ca36c',
'Accept-Encoding' => 'gzip',
'Connection' => 'close',
'BN-Frontend' =&at: 'captcha-https'
'X-Forwarded-Port' => '443',
'X-Forwarded-Proto' => 'https'.
'BN-Client-Port' =&at: '52448'.
'X-Forwarded-For' =&gt: '
Post data: [Array
[username] => admin
[password] =&at: brotherm
[redirect] => https://www.handryersuk.co.uk/admin//index.php?route=common/login
```

- Information Content Security Unauthorised Modification of Information
- Abusive Content Spam
- Information Gathering Scanning
- Vulnerable Information Disclosure



]



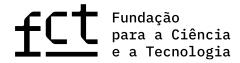
QUESTÃO #6:

```
rv:62.0) Gecko/20100101 Firefox/62.0"
- [04/Oct/2021:23:02:45 +0100] "POST /downloader//downloader/index.php HTTP/2" 404 16412 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0"
- [04/Oct/2021:23:05:28 +0100] "POST /downloader//downloader/index.php HTTP/2" 404 15911 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0"
Message [ApacheMagentoDownloader]]style='padding:10px 20px; background:#e6e6e6;margin-bottom:10px'>Url: [cn-plumbing.co.uk/admin/]
Remote connection:
Headers: [array (
'Host' => 'cn-plumbing.co.uk',
'User-Agent' =&qt; 'Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0',
'Content-Lenath' =&at: '491'.
'Content-Type' => 'multipart/form-data; boundary=0197f06d23908177bc3691b33f381930a53f28e0998034c51c020bff4970'
'Accept-Encoding' => 'gzip',
'Connection' =&at: 'close'.
'BN-Frontend' => 'captcha-https',
'X-Forwarded-Port' => '443',
'X-Forwarded-Proto' => 'https'.
'BN-Client-Port' => '36588'.
Post data: [Array
[password] => hemmingw
[redirect] => https://cn-plumbing.co.uk/admin//index.php?route=common/login
[username] =&at: admin
|Url: [www.handryersuk.co.uk/admin/]
Remote connection:
Headers: [array (
'Host' => 'www.handryersuk.co.uk',
'User-Agent' =&qt; 'Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:62.0) Gecko/20100101 Firefox/62.0',
'Content-Length' => '495'
'Content-Type' =&qt; 'multipart/form-data; boundary=dffbab523ede0670fc40028aad027dcbd422fba18d7be6296af1d78ca36c',
'Accept-Encoding' => 'gzip',
'Connection' => 'close',
'BN-Frontend' =&at: 'captcha-https'
'X-Forwarded-Port' => '443',
'X-Forwarded-Proto' => 'https'.
'BN-Client-Port' =&at: '52448'.
'X-Forwarded-For' =&gt: '
Post data: [Array
[username] => admin
[password] =&at: brotherm
[redirect] => https://www.handryersuk.co.uk/admin//index.php?route=common/login
```

- Information Content Security Unauthorised Modification of Information
- Abusive Content Spam
- **Information Gathering Scanning**
- Vulnerable Information Disclosure



]



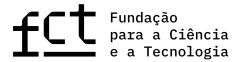
QUESTÃO #7:

UNIDADE DA FCT

```
Received: from mail-1... (unknown [#11.1841.19])
by av-mail (Postfix) with ESMTP id CF03A4254F17
for <x>: Tue, 28 Jun 2022 16:50:59 +0100 (WEST)
(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
(No client certificate requested)
by mail-1 (Postfix) with ESMTPSA id 9C8E38C23A2
for <x>; Tue, 28 Jun 2022 16:50:58 +0100 (WEST)
Date: Tue, 28 Jun 2022 12:51:00 -0300
Message-ID: <0070
From: "<Roberto Dosio> info.rete@stefan-mcds.it" <bolsas@ | | | | | | | |
To: "" <x>
Subject: RE: x
Content-Type: multipart/mixed;
boundary="----tX6LzxiaNaX4PpfalHPRAX40"
X-KLMS-Rule-ID: 1
X-KLMS-Message-Action: attachment removed, AntiVirus
X-KLMS-AntiSpam-Status: not scanned, disabled by settings
X-KLMS-AntiPhishing: Clean, bases: 2022/06/28 14:42:00
X-KLMS-AntiVirus: Kaspersky Security for Linux Mail Server, version 8.0.3.30, bases: 2022/06/28 09:08:00 #19868100
Return-Path: bolsas
X-MS-Exchange-Organization-Network-Message-Id: 3ccf6408-30e2-4a12-0105-08da591e0358
X-MS-Exchange-Organization-AuthSource: EX1.eqlt.equinoxlt.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Transport-EndToEndLatency: 00:00:00:2030213
X-MS-Exchange-Processed-By-BccFoldering: 15.01.2308.014
MIME-Version: 1.0
      -----tX6LzxjaNgX4PpfalHPRAX4o
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">
</head>
<body>
<br>
<br>
<br>
=0DPlease see attached
<br>
<br>
archive pass: 263<br>
<br>
<br>
Roberto Dosio < br>
info.rete@stefan-mcds.it
```



- 1) Malicious Code Infected System
- 2) Availability Sabotage
- 3) Vulnerable Vulnerable System
- 4) Malicious Code Malware Configuration



QUESTÃO #7:

Received: from mail-1... (unknown [#12.18841.19]) by av-mail (Postfix) with ESMTP id CF03A4254F17 for <x>: Tue, 28 Jun 2022 16:50:59 +0100 (WEST) (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate requested) by mail-1 (Postfix) with ESMTPSA id 9C8E38C23A2 for <x>; Tue, 28 Jun 2022 16:50:58 +0100 (WEST) Date: Tue, 28 Jun 2022 12:51:00 -0300 Message-ID: <0070 From: "<Roberto Dosio> info.rete@stefan-mcds.it" <bolsas@ | | | | | | | | To: "" <x> Subject: RE: x Content-Type: multipart/mixed; boundary="----tX6LzxiaNaX4PpfalHPRAX40" X-KLMS-Rule-ID: 1 X-KLMS-Message-Action: attachment removed, AntiVirus X-KLMS-AntiSpam-Status: not scanned, disabled by settings X-KLMS-AntiPhishing: Clean, bases: 2022/06/28 14:42:00 X-KLMS-AntiVirus: Kaspersky Security for Linux Mail Server, version 8.0.3.30, bases: 2022/06/28 09:08:00 #19868100 Return-Path: bolsas X-MS-Exchange-Organization-Network-Message-Id: 3ccf6408-30e2-4a12-0105-08da591e0358 X-MS-Exchange-Organization-AuthSource: EX1.eqlt.equinoxlt.com X-MS-Exchange-Organization-AuthAs: Anonymous X-MS-Exchange-Transport-EndToEndLatency: 00:00:00:2030213 X-MS-Exchange-Processed-By-BccFoldering: 15.01.2308.014 MIME-Version: 1.0 -----tX6LzxjaNgX4PpfalHPRAX4o Content-Type: text/html; charset="UTF-8" Content-Transfer-Encoding: quoted-printable <meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8"> </head> <body>

 =0DPlease see attached

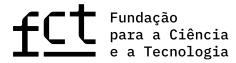
 archive pass: 263

 Roberto Dosio
 info.rete@stefan-mcds.it





- 1) Malicious Code Infected System
- 2) Availability Sabotage
- 3) Vulnerable Vulnerable System
- 4) Malicious Code Malware Configuration



QUESTÃO #8:

A couple of days ago, we opened case DIVD-2021-00030 to address a vulnerability known as CVE-2021-22205 in GitLab Community Edition (CE) and Enterprise Edition (EE), affecting all versions starting from 11.9. GitLab was not correctly validating image files passed to a file parser; this resulted in a remote command execution (RCE).

We have received a list of GitLab servers running a vulnerable version of GitLab from security researchers at Censys.io who previously wrote a blog post about this (https://censys.io/blog/cve-2021-22205-it-was-a-gitlab-smash/). We have validated these findings by manually verifying a representative sample, and are now sending out notifications.

The following server is on this list:

IP:

Port: 10101 Version: 13.7

Observed at: Nov 5, 2021, 3:54:23 PM

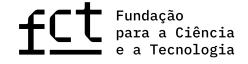
DNS names:

We advise you to upgrade your GitLab system to the latest version as soon as possible.

For more information: https://csirt.divd.nl/cases/DIVD-2021-00030/

- 1) Intrusion Application Compromise
- 2) Vulnerable Vulnerable System
- 3) Availability Misconfiguration
- 1) Information Gathering Sniffing





QUESTÃO #8:

A couple of days ago, we opened case DIVD-2021-00030 to address a vulnerability known as CVE-2021-22205 in GitLab Community Edition (CE) and Enterprise Edition (EE), affecting all versions starting from 11.9. GitLab was not correctly validating image files passed to a file parser; this resulted in a remote command execution (RCE).

We have received a list of GitLab servers running a vulnerable version of GitLab from security researchers at Censys.io who previously wrote a blog post about this (https://censys.io/blog/cve-2021-22205-it-was-a-gitlab-smash/). We have validated these findings by manually verifying a representative sample, and are now sending out notifications.

The following server is on this list:

IP:

Port: 10101 Version: 13.7

Observed at: Nov 5, 2021, 3:54:23 PM

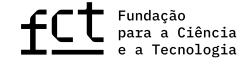
DNS names:

We advise you to upgrade your GitLab system to the latest version as soon as possible.

For more information: https://csirt.divd.nl/cases/DIVD-2021-00030/

- 1) Intrusion Application Compromise
- 2) Vulnerable Vulnerable System
- 3) Availability Misconfiguration
- 1) Information Gathering Sniffing





QUESTÃO #9:

Within the same week, I moved on with installing a Trojan virus in Operating Systems for all devices that you use to login to email. Frankly speaking, it wasn't a challenging task for me at all (since you were kind enough to click some of the links in your inbox emails before). Yeah, geniuses are among us.

Because of this Trojan I am able to gain access to entire set of controllers in devices (e.g., your video camera, keyboard, microphone and others). As result, I effortlessly downloaded all data, as well as photos, web browsing history and other types of data to my servers.

Moreover, I have access to all social networks accounts that you regularly use, including emails, including chat history, messengers, contacts list etc. My unique virus is incessantly refreshing its signatures (due to control by a driver), and hence remains undetected by any type of antiviruses.

Hence, I guess by now you can already see the reason why I always remained undetected until this very letter...

During the process of compilation of all the materials associated with you,

I also noticed that you are a huge supporter and regular user of websites hosting nasty adult content.

Turns out to be, you really love visiting porn websites, as well as watching exciting videos and enduring unforgettable pleasures.

As a matter of fact, I was not able to withstand the temptation, but to record certain nasty solo action with you in main role, and later produced a few videos exposing your masturbation and cumming scenes.

If until now you don't believe me, all I need is one-two mouse clicks to make all those videos with everyone you know, including your friends, colleagues, relatives and others.

Moreover, I am able to upload all that video content online for everyone to see.

I sincerely think, you certainly would not wish such incidents to take place, in view of the lustful things demonstrated in your commonly watched videos, (you absolutely know what I mean by that) it will cause a huge adversity for you.

There is still a solution to this matter, and here is what you need to do:

You make a transaction of \$950 USD to my account (an equivalent in bitcoins, which recorded depending on the exchange rate at the date of funds transfer), hence upon receiving the transfer, I will immediately get rid of all those lustful videos without delay.

After that we can make it look like there was nothing happening beforehand.

Additionally, I can confirm that all the Trojan software is going to be disabled and erased from all devices that you use. You have nothing to worry about, because I keep my word at all times.

That is indeed a beneficial bargain that comes with a relatively reduced price, taking into consideration that your profile and traffic were under close monitoring during a long time frame.

If you are still unclear regarding how to buy and perform transactions with bitcoins - everything is available online.

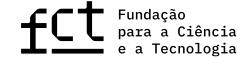
Below is my bitcoin wallet for your further reference: 1DnDfzKAjTYWcn6nCVfkXLh5RRaGBUZ7nE

All you have is 48 hours and the countdown begins once this email is opened (in other words 2 days).





- 1) Malicious Code Infected System
- 2) Fraud Phishing
- 3) Information Gathering Social Engineering
- 4) Abusive Content SPAM



QUESTÃO #9:

Within the same week, I moved on with installing a Trojan virus in Operating Systems for all devices that you use to login to email. Frankly speaking, it wasn't a challenging task for me at all (since you were kind enough to click some of the links in your inbox emails before). Yeah, geniuses are among us.

Because of this Trojan I am able to gain access to entire set of controllers in devices (e.g., your video camera, keyboard, microphone and others). As result, I effortlessly downloaded all data, as well as photos, web browsing history and other types of data to my servers.

Moreover, I have access to all social networks accounts that you regularly use, including emails, including chat history, messengers, contacts list etc. My unique virus is incessantly refreshing its signatures (due to control by a driver), and hence remains undetected by any type of antiviruses.

Hence, I guess by now you can already see the reason why I always remained undetected until this very letter...

During the process of compilation of all the materials associated with you,

I also noticed that you are a huge supporter and regular user of websites hosting nasty adult content.

Turns out to be, you really love visiting porn websites, as well as watching exciting videos and enduring unforgettable pleasures.

As a matter of fact, I was not able to withstand the temptation, but to record certain nasty solo action with you in main role, and later produced a few videos exposing your masturbation and cumming scenes.

If until now you don't believe me, all I need is one-two mouse clicks to make all those videos with everyone you know, including your friends, colleagues, relatives and others.

Moreover, I am able to upload all that video content online for everyone to see.

I sincerely think, you certainly would not wish such incidents to take place, in view of the lustful things demonstrated in your commonly watched videos, (you absolutely know what I mean by that) it will cause a huge adversity for you.

There is still a solution to this matter, and here is what you need to do:

You make a transaction of \$950 USD to my account (an equivalent in bitcoins, which recorded depending on the exchange rate at the date of funds transfer), hence upon receiving the transfer, I will immediately get rid of all those lustful videos without delay.

After that we can make it look like there was nothing happening beforehand.

Additionally, I can confirm that all the Trojan software is going to be disabled and erased from all devices that you use. You have nothing to worry about, because I keep my word at all times.

That is indeed a beneficial bargain that comes with a relatively reduced price,

taking into consideration that your profile and traffic were under close monitoring during a long time frame.

If you are still unclear regarding how to buy and perform transactions with bitcoins - everything is available online.

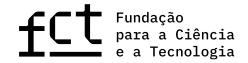
Below is my bitcoin wallet for your further reference: 1DnDfzKAjTYWcn6nCVfkXLh5RRaGBUZ7nE

All you have is 48 hours and the countdown begins once this email is opened (in other words 2 days).





- L) Malicious Code Infected System
- 2) Fraud Phishing
- 3) Information Gathering Social Engineering
- 4) Abusive Content SPAM

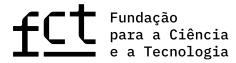


QUESTÃO #10:

```
2022-06-04 00:36:34.812354 IP (tos 0x28, ttl 44, id 59480, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.34454 > 216.52.148.x.27015; UDP, length 1458
0x0000: 4528 05ce e858 4000 2c11 cc82 c189 662e E(...X@......f.
0x0010: d834 942f 8696 6987 05ba 0f40 6100 0000 .4./..i....@a...
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.815545 IP (tos 0x28, ttl 44, id 61984, offset 0, flags [DF], proto UDP (17), length 1486)
0x0000: 4528 05ce f220 4000 2c11 c2ba c189 662e E(....@.,....f.
0x0010: d834 942f 7de2 6987 05ba 6cf4 0c00 0000 .4./\.i........
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.816516 IP (tos 0x28, ttl 44, id 62472, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.32226 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce f408 4000 2c11 c0d2 c189 662e E(....@.,....f.
0x0010: d834 942f 7de2 6987 05ba e4f3 9400 0000 .4./}.i......
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.820438 IP (tos 0x28, ttl 44, id 63996, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.32226 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce f9fc 4000 2c11 bade c189 662e E(....@.,....f.
0x0010: d834 942f 7de2 6987 05ba cbf3 ad00 0000 .4./}.i......
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.843397 IP (tos 0x28, ttl 44, id 7606, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.2772 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce 1db6 4000 2c11 9725 c189 662e E(....@.,..%..f.
0x0010: d834 942f 0ad4 6987 05ba 3f02 ad00 0000 .4./..i...?.....
0x0050: 0000 0000 0000 .....
             UNIDADE DA FCT
```



- 1) Other Undetermined
- 2) Information Content Security Data Loss
- 3) Availability Sabotage
- 4) Availability Denial of Service



QUESTÃO #10:

```
2022-06-04 00:36:34.812354 IP (tos 0x28, ttl 44, id 59480, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.34454 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce e858 4000 2c11 cc82 c189 662e E(...X@......f.
0x0010: d834 942f 8696 6987 05ba 0f40 6100 0000 .4./..i....@a...
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.815545 IP (tos 0x28, ttl 44, id 61984, offset 0, flags [DF], proto UDP (17), length 1486)
0x0000: 4528 05ce f220 4000 2c11 c2ba c189 662e E(....@.,....f.
0x0010: d834 942f 7de2 6987 05ba 6cf4 0c00 0000 .4./\.i........
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.816516 IP (tos 0x28, ttl 44, id 62472, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.32226 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce f408 4000 2c11 c0d2 c189 662e E(....@.,....f.
0x0010: d834 942f 7de2 6987 05ba e4f3 9400 0000 .4./}.i......
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.820438 IP (tos 0x28, ttl 44, id 63996, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.32226 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce f9fc 4000 2c11 bade c189 662e E(....@.,....f.
0x0010: d834 942f 7de2 6987 05ba cbf3 ad00 0000 .4./}.i......
0x0050: 0000 0000 0000 .....
2022-06-04 00:36:34.843397 IP (tos 0x28, ttl 44, id 7606, offset 0, flags [DF], proto UDP (17), length 1486)
102.46.2772 > 216.52.148.x.27015: UDP, length 1458
0x0000: 4528 05ce 1db6 4000 2c11 9725 c189 662e E(....@.,..%..f.
0x0010: d834 942f 0ad4 6987 05ba 3f02 ad00 0000 .4./..i...?.....
0x0050: 0000 0000 0000 .....
             UNIDADE DA FCT
```



- 1) Other Undetermined
- 2) Information Content Security Data Loss
- 3) Availability Sabotage
- 4) Availability Denial of Service







Obrigado!



