jornadas FCCN

fct csirt

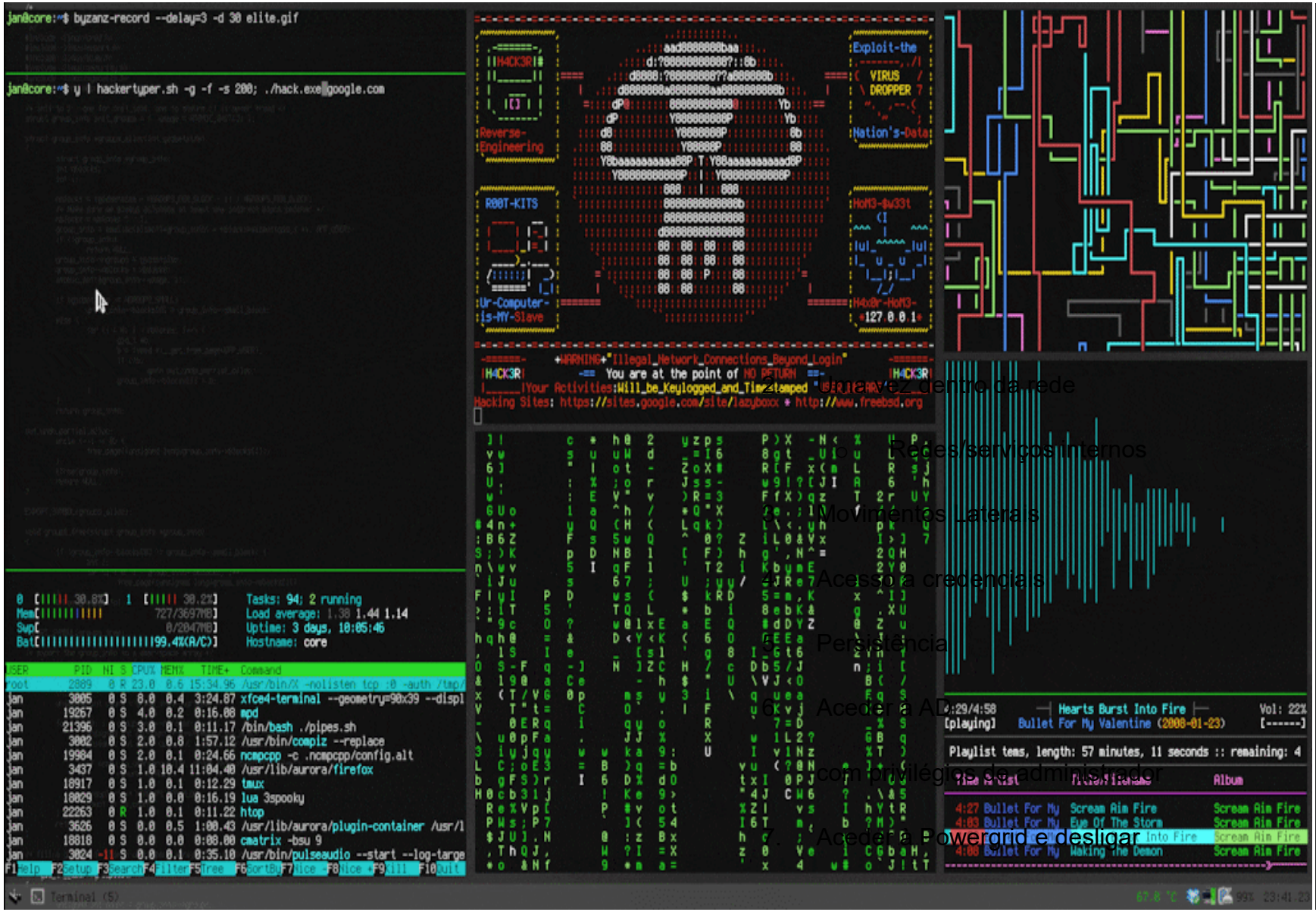
BLUE PILL, RED PILL

João Machado e Pedro Silva

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

JUST ANOTHER MONDAY

jornadas FCCN



[DarkWeb Private Chat – "SilentFox Messenger"]

ShadowWolf:

> Got eyes on GridCorp. Their employees are super click-happy.
> Thinking classic phishing.

ByteRider:

> Lol nice. What's the theme? Invoice? Password reset?

ShadowWolf:

> Better. Fake Office365 login page. Email looks like "Action Required: Password Expiring Soon."

ByteRider:

> Classic. You crafting the phishing page?

ShadowWolf:

> Already done. Cloned Microsoft login with SSL cert to look legit.
> Hosting it behind a fast-flux network.

ByteRider:

> Sweet. Mail server ready?

ShadowWolf:

> Yup. Spoofed "it-support@gridcorp.com" address. Gonna hit 300+ users at once.

ByteRider:

> Oof, that's gonna hurt. Payload or creds?

ShadowWolf:

> Focus on stealing credentials first.
> Later, maybe send a malware-laced attachment.

ByteRider:

> How you handling alerts? GridCorp has decent spam filters.

ShadowWolf:

> Using trusted domains for redirect chains to mask the phishing URL.

ByteRider:

> Solid. When do we launch?

ShadowWolf:

> Friday 8:30 AM. Early birds will fall for it.

ByteRider:

> Perfect. Let's make GridCorp our next trophy. 🏆

ShadowWolf:

> Stay low, stay silent. See you after the breach.

Já estás dentro da rede

Reconhecimento de Redes/serviços internos

Movimentos laterais

Acesso a credenciais

Persistência

Acedeu à AD

com privilégios de administrador

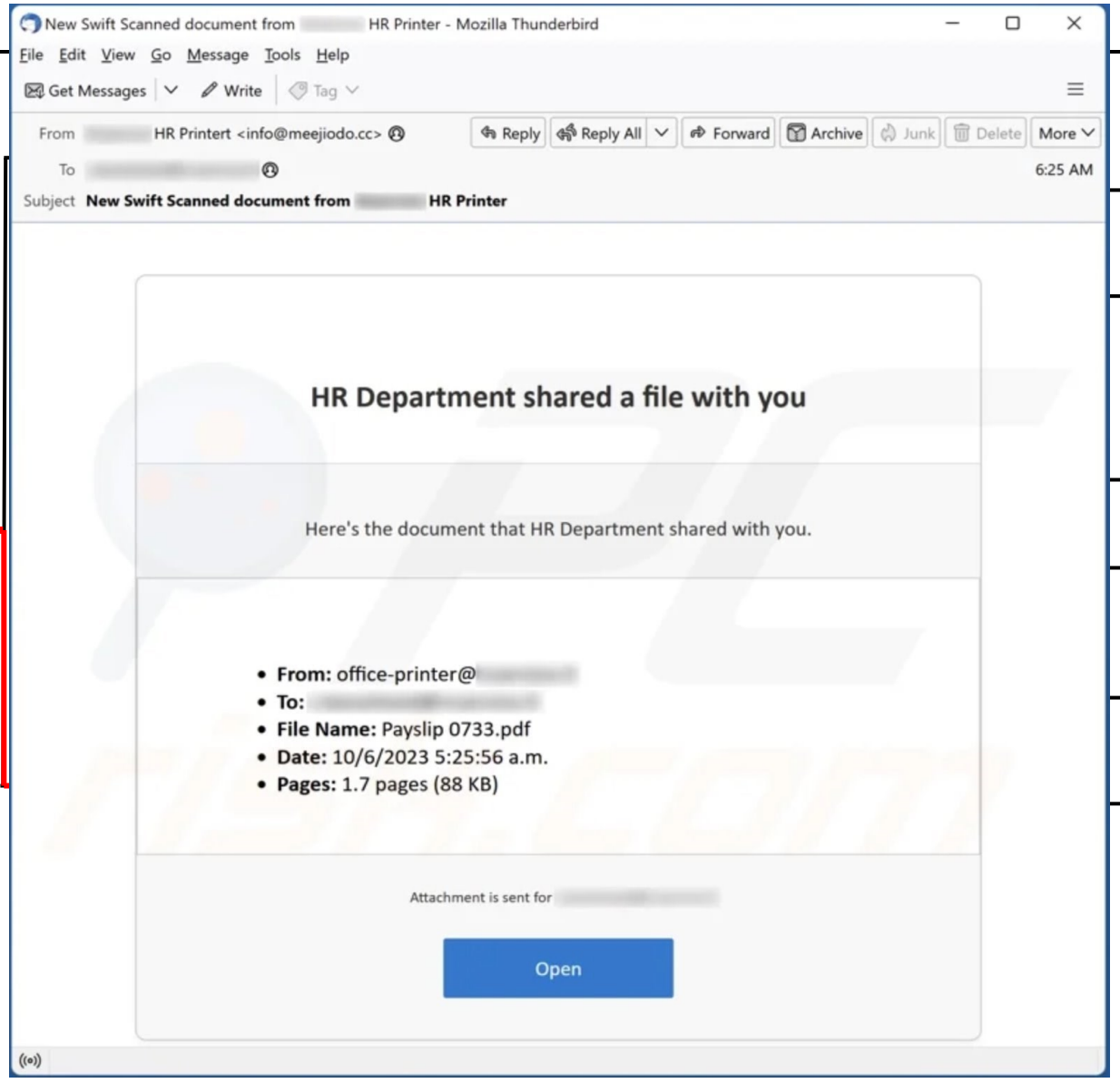
Acedeu à Powergrid e desligar

strador

REDE CORPORATIVA

INTERNET

1. Phishing Email
2. Instalar malware



Subnet 3

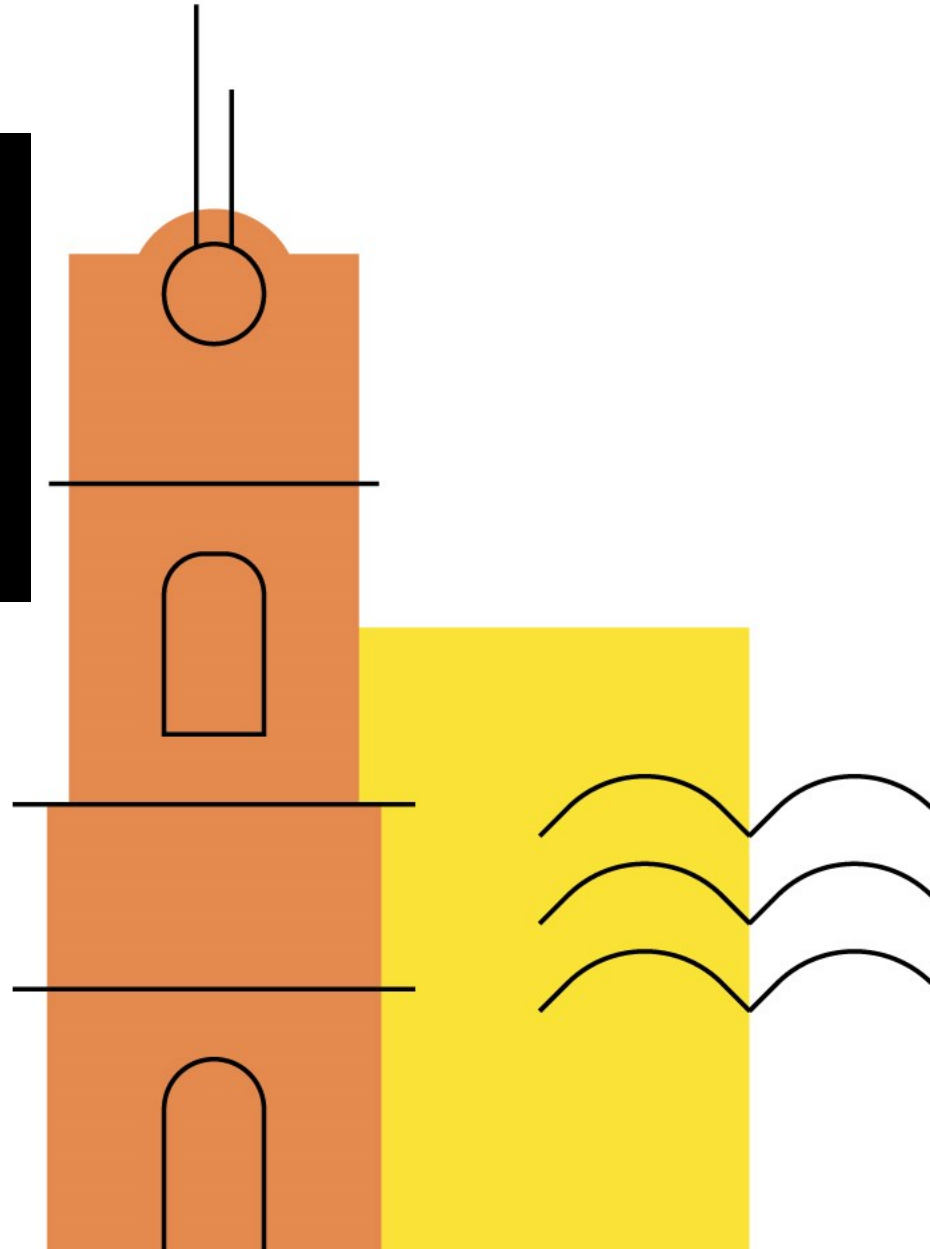
Domain Controller

Powergrid

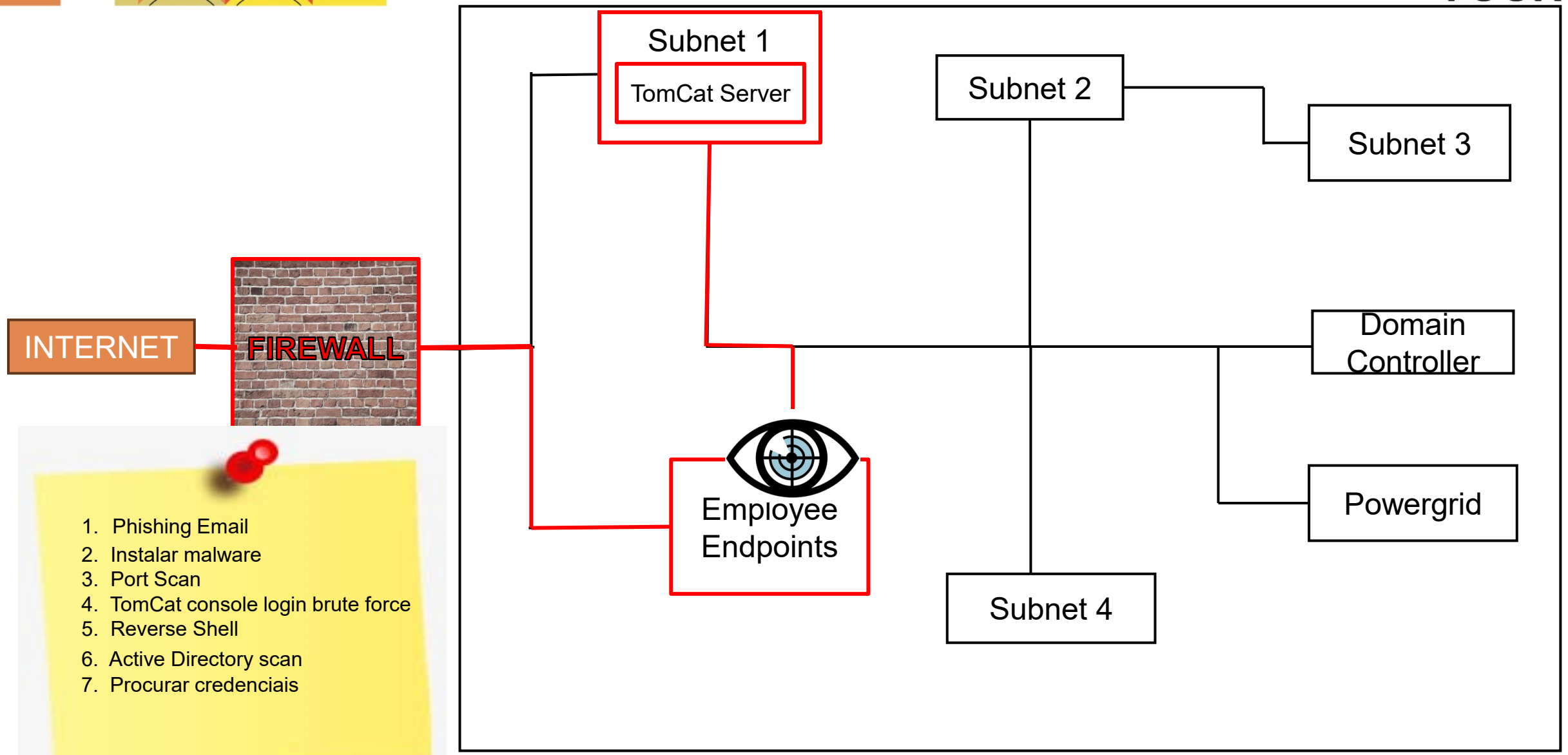
jornadas FCCN

LOADING...

00 : 00 : 05 : 00



REDE CORPORATIVA



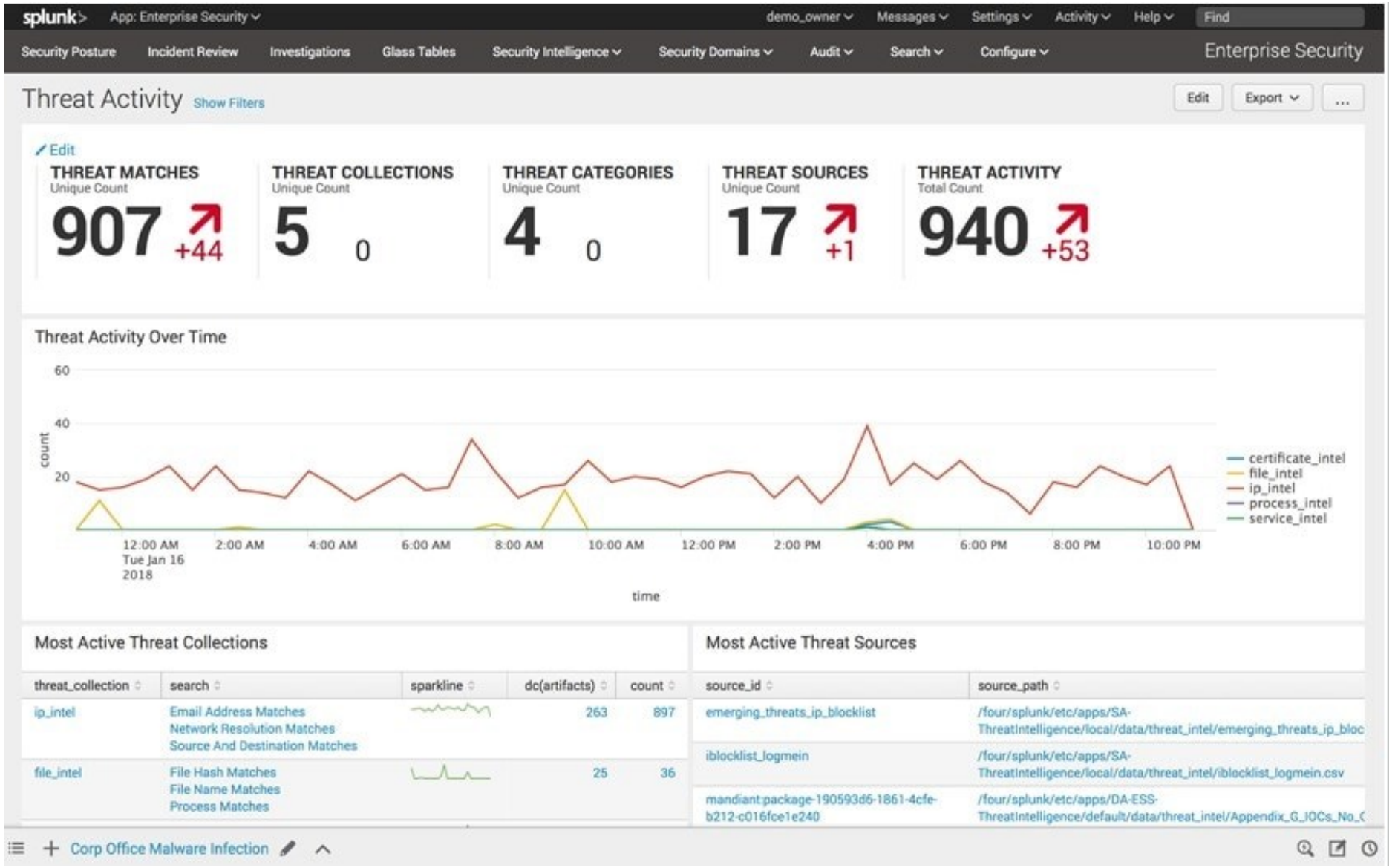
1. Phishing Email
2. Instalar malware
3. Port Scan
4. TomCat console login brute force
5. Reverse Shell
6. Active Directory scan
7. Procurar credenciais

ALERTAS, ALERTAS E MAIS ALERTAS...

Time	Alert	Priority	Status
7:30 am	Port Scan ALERT	Low (3)	Pending Investigating
7:55 am	User Reported: <HR Report Attached>	High (1)	Pending
8:00 am	User Reported: <Survey to be filled>	Low (3)	Pending
8:30 am	Port Scan across several machines	Low(3)	Pending
8:32 am	Active Directory – User Accounts Locked Out	Medium (2)	Pending
8:35 am	Active Directory – Windows Admin Credentials	Medium (2)	Pending

Showing 6 of 500

ANÁLISE DO E-MAIL - SIEM



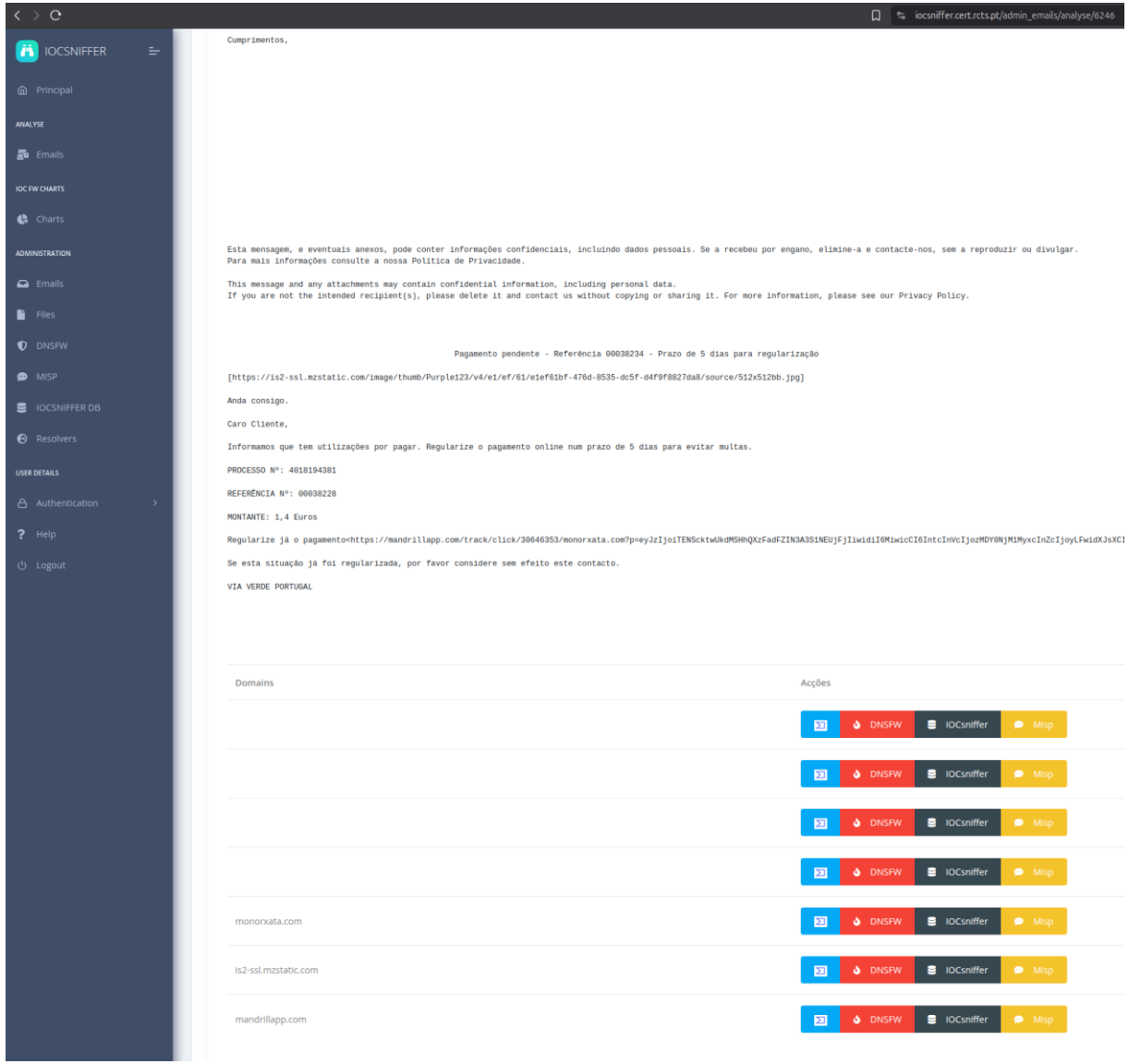
ALERTAS, ALERTAS E MAIS ALERTAS...

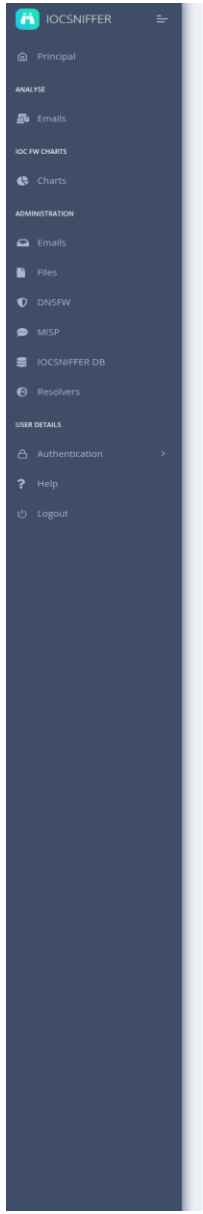
jornadas FCCN

Time	Alert	Priority	Status
7:30 am	Por Scan ALERT	Low (3)	Completed
7:55 am	User Reported: <HR Report Attached>	High (1)	Pending Investigating
8:00 am	User Reported: <Survey to be filled>	Low (3)	Pending
8:30 am	Port Scan across several machines	Low(3)	Pending
8:32 am	Active Directory – User Accounts Locked Out	Medium (2)	Pending
8:35 am	Active Directory – Windows Admin Credentials	Medium (2)	Pending

Showing 6 of 500

ANÁLISE DO E-MAIL - HEADERS

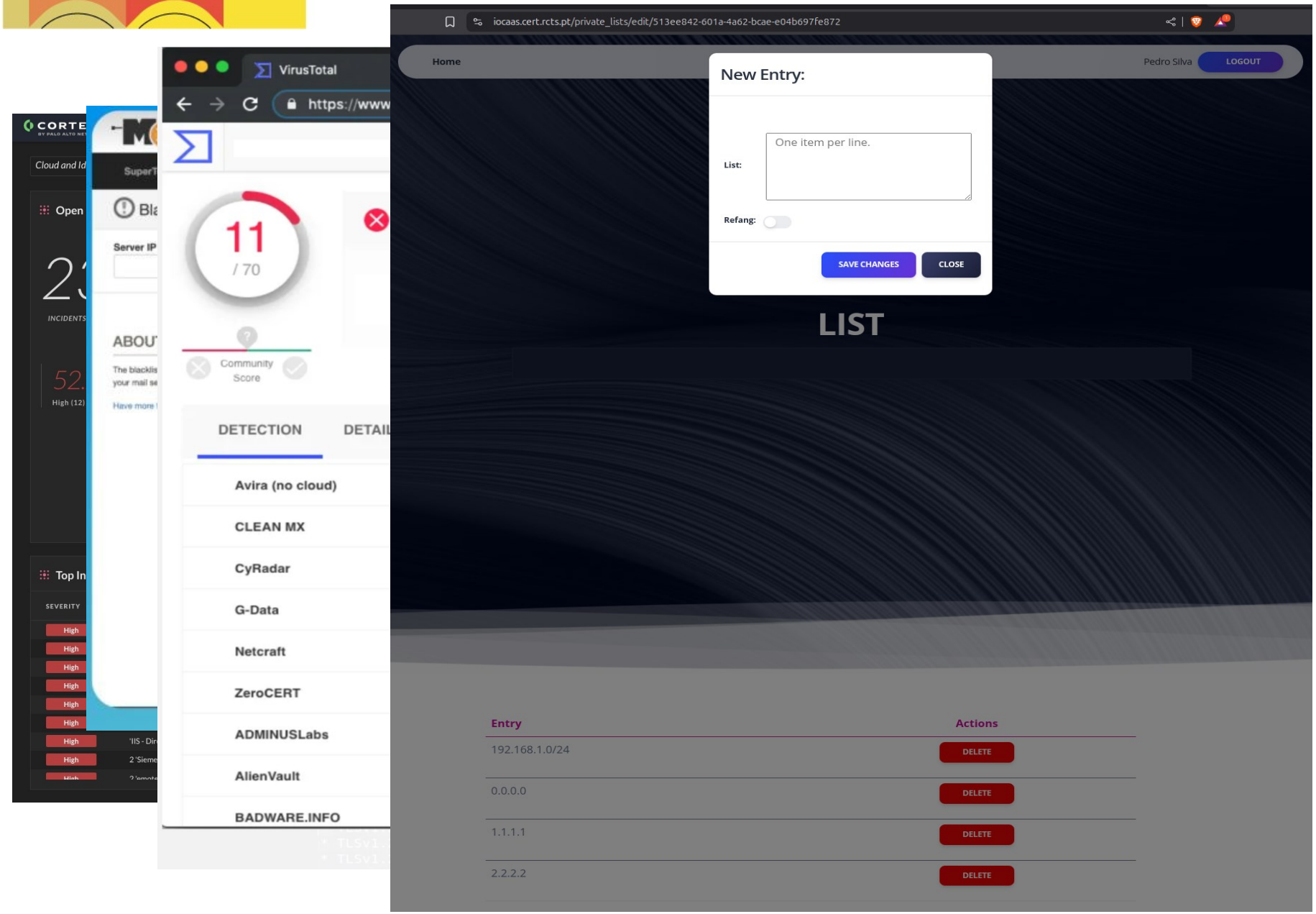




Raw email:

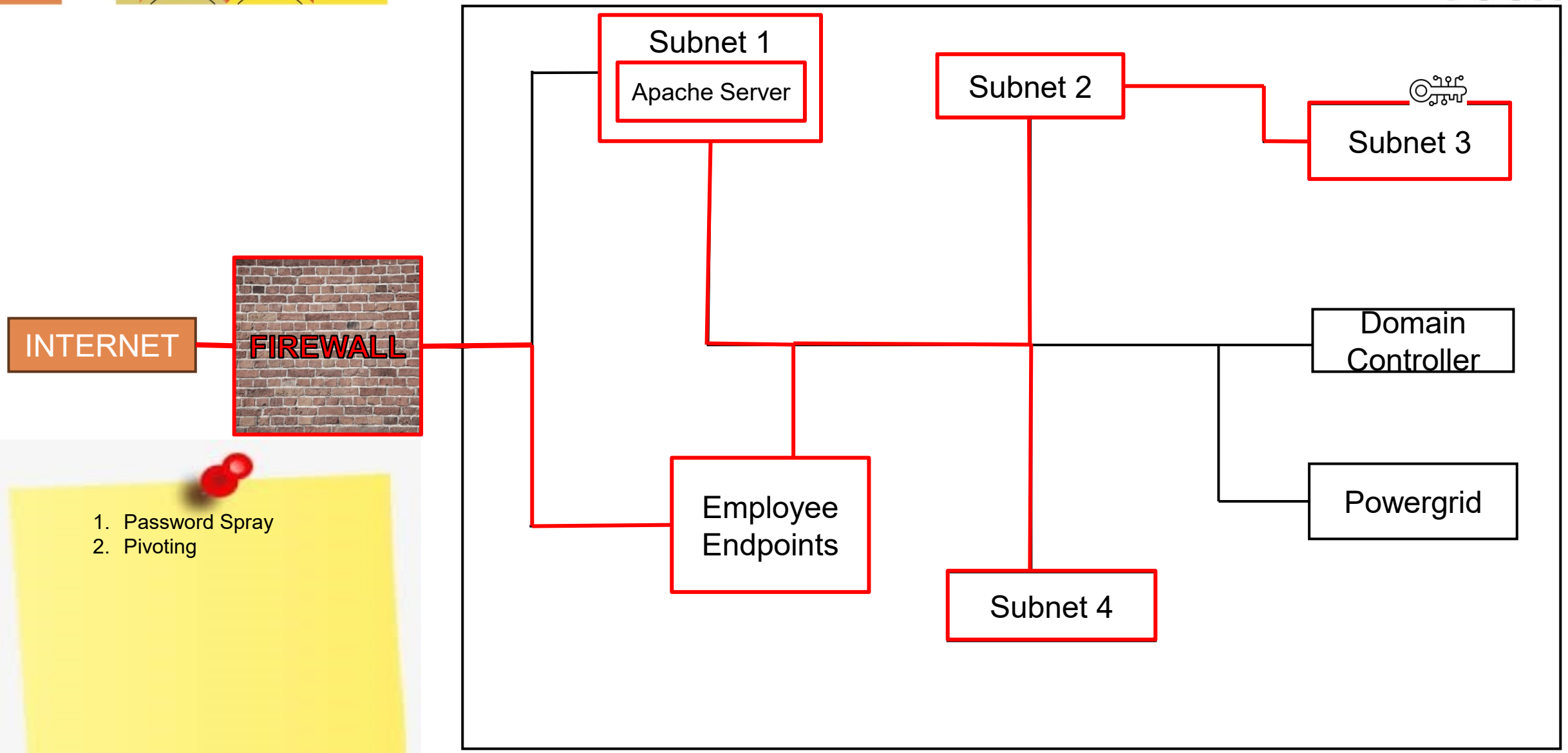
```
Return-Path: <prvs=1189275d16=                t>
Delivered-To:
Received: from
        by
        id OmuRODzh72fKUyMAzi5QSQ
        (
        fo                                    Apr 2025 14:40:12 +0100
X-Spam-Checker-Version: SpamAssassin 3.4.4 (2020-01-24) on
X-Spam-Level:
X-Spam-Status: No, score=1.0 required=50.0 tests=DKIM_SIGNED,DKIM_VALID,
        DKIM_VALID_AU,HTML_FONT_LOW_CONTRAST,HTML_MESSAGE,RCVD_IN_MSPIKE_H4,
        RCVD_IN_MSPIKE_WL,SPF_HELO_NONE,URIBL_GREY autolearn=no
        autolearn_force=no version=3.4.4
X-Spam-Report:
        *  1.1 URIBL_GREY Contains an URL listed in the URIBL greylist
        *      [URIs: mandrillapp.com]
        *  0.0 RCVD_IN_MSPIKE_H4 RBL: Very Good reputation (+4)
        *      [193.137.198.39 listed in wl.mailspike.net]
        *  0.0 SPF_HELO_NONE SPF: HELO does not publish an SPF Record
        *  0.0 HTML_FONT_LOW_CONTRAST BODY: HTML font color similar or
        *      identical to background
        *  0.0 HTML_MESSAGE BODY: HTML included in message
        *  0.1 DKIM_SIGNED Message has a DKIM or DK signature, not necessarily
        *      valid
        * -0.1 DKIM_VALID Message has at least one valid DKIM or DK signature
        * -0.1 DKIM_VALID_AU Message has a valid DKIM or DK signature from
        *      author's domain
        *  0.0 RCVD_IN_MSPIKE_WL Mailspike good senders
X-Spam-Score: 1.0
Received: from                (
        (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
         key-exchange X25519 server-signature ECDSA (P-256) server-digest SHA256)
        (No client certificate requested)
        by           .  .Postfix) with ESMTPS id B306BD08EB
        for                .     Fri,  4 Apr 2025 14:40:12 +0100 (BST)
Authentication-Results:            t; dmarc=pass (p=reject dis=none) h
Authentication-Results:            t;
        dkim=pass (2048-bit key; secure)
        dkim=pass (2048-bit key; unpr                                                                                    3wsmx/6;
        dkim-atps=neutral
Received: from
        by s                  :h ESMTP id 534DeBEF020789-534DeBEG020789
        for                  :>; Fri, 4 Apr 2025 14:40:11 +0100
Received: from EUR05-VI1-obe.outbound.protection.outlook.com (mail-vi1eur05lp2168.outbound.protection.outlook.com [104.47.17.168])
        (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
         key-exchange ECDHE (P-384) server-signature RSA-PSS (4096 bits) server-digest SHA256)
        (No client certificate requested)
        by                        with ESMTPS id 02D1A48E931
        for                  .  4 Apr 2025 14:40:11 +0100 (WEST)
ARC-Seal: i=1; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=none;
 b=gtq13EAuy/LFK4Ya99L6U3qZYWWsxfN3rePBeuKrHHahqd/nx2iZIA6hWlVtjUuBPR9vqa4NB0qpGJ7XQowyzE0T+j7FE+ZkskF1aQ2Gt9Lwwte6PMt8OLPCYVzSDs570626dTiFZ3(
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector10001;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:
 bh=Xxszu9rRSlaQrftxFlNrxP0ctjwEVnTxrjOYy54vf64=;
 b=Z5OUTXhloa62/NKtUo28Sc/wpnFj5Z0coD5t8svsRfU51yuCWVJeaNrcf+2Hx0ZwoN39ld7cb51lFO5nLuNr3ABq2z0ym78sPqp/BE7aNH8sRo9WjUadcqmNITJgQhLds3nkeh7uzC'
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass
 smtp.mai                                                                                                                                    .
 header.d=fccn.pt; arc=none
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; d=fccn.pt; s=default; c=relaxed/relaxed;
 h=from:to:subject:date:message-id:references:content-type:mime-version;
 bh=Xxszu9rRSlaQrftxFlNrxP0ctjwEVnTxrjOYy54vf64=;
 b=SROwLs0ZPmehO8T6sHpiUTeCnygA7Lh9s9HxM94T/cn612ZCoSl+s4jRBSqOosHVmDX3MeYaHdzW
        rxtkaX2GTXtuLMaaCW3X+tlwiYjLnE/Ev03TZi82n116yHFREYc7js6znpdbN/1M1+iyGElnx8rB
        5i/CWb10MWf57cTiVOx2v65dWoe+X5su+2NiQthjx23r3xnvbURj55UKQrWx1fZ7sM58YKv9P1z
        43XfPfwDTaOQEyPc13df8GuxAA61YUaixyI8sdWhLNqjOOudLj8hFZ/XxtSHDPWlmXnpz+XfklE/
        U/iKliuqDVDgXpbAI4pAAXhAPkAbfes3WdMQRg==
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relax                s=selector2;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
 bh=Xxszu9rRSlaQrftxFlNrxP0ctjwEVnTxrjOYy54vf64=;
 b=r8wsmx/6sPrx4JTF04GF4CtLShx2ayygeJh10QXCMEHYPUTENuyoZ8ZppYzbc4UoD9OLmDqOrZnrH/YJs84YxtD8dI/XZnQTNu3MrPlm27rrB0ICqcr/zQ+hdQNHjrTEFGAxKGzd8yM'
Received: from DU2P193MB2308.EURP193.PROD.OUTLOOK.COM (2603:10a6:10:2fb::21)
 by DBAP193MB0986.EURP193.PROD.OUTLOOK.COM (2603:10a6:10:1c3::24) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8632.11; Fri, 4 Apr
 2025 13:40:08 +0000
Received: from DU2P193MB2308.EURP193.PROD.OUTLOOK.COM
 ([fe80::a2b9:d94:ab79:208e]) by DU2P193MB2308.EURP193.PROD.OUTLOOK.COM
 ([fe80::a2b9:d94:ab79:208e%3]) with mapi id 15.20.8632.011; Fri, 4 Apr 2025
 13:40:08 +0000
From
To: '
Subject: FW: Pagamento Pendente - Ref:00038228
Thread-Topic: Pagamento Pendente - Ref:00038228
Thread-Index: AQHYnzg+XeuvzC6jTWB+3fXgkXxOTLOZj5Bg
Date: Fri, 4 Apr 2025 13:40:08 +0000
Message-ID:
 <DU2P193MB2308F0DDFCF0DA4C2F385DBCD5A92@DU2P193MB2308.EURP193.PROD.OUTLOOK.COM>
References: <1743770439.67efd34793879@gynecologist-near-me.ae>
In-Reply-To: <1743770439.67efd34793879@gynecologist-near-me.ae>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
authentication-results: dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.fr
x-ms-publictraffictype: Email
x-ms-traffictypediagnostic: DU2P193MB2308:EE_|DBAP193MB0986:EE_
x-ms-office365-filtering-correlation-id: cb6e6daf-216d-4abf-5e12-08dd737e3715
x-ms-exchange-atpmessageproperties: SL
x-microsoft-antispam: BCL:0;ARA:13230040|366016|8096899003|41050700001;
x-microsoft-antispam-message-info:
 =?utf-8?B?dmg5WWc0RzNjejZDTnlXYVZiNVBYK1RDdGZTV21BSWhtVUdLc3NJdFJkbTNs?=
 =?utf-8?B?NFJoS0JZVlFaY2RVcndWVjE5TBCUmkraTlXRkdCK0ltSXE0Z1RJS0p4TVhE?=
```

ANÁLISE DO E-MAIL - TOOLS



REDE CORPORATIVA

jornadas FCCN



1. Password Spray
2. Pivoting

ALERTAS, ALERTAS E MAIS ALERTAS...

jornadas FCCN

Time	Alert	Priority	Status
7:30 am	Por Scan ALERT	Low (3)	Completed
7:55 am	User Reported: <HR Report Attached>	High (1)	Completed
8:00 am	User Reported: <Survey to be filled>	Low (3)	Pending
8:30 am	Port Scan across several machines	Low(3)	Pending
8:32 am	Active Directory – User Accounts Locked Out	Medium (2)	Pending
8:35 am	Active Directory – Windows Admin Credentials	Medium (2)	Pending Investigating

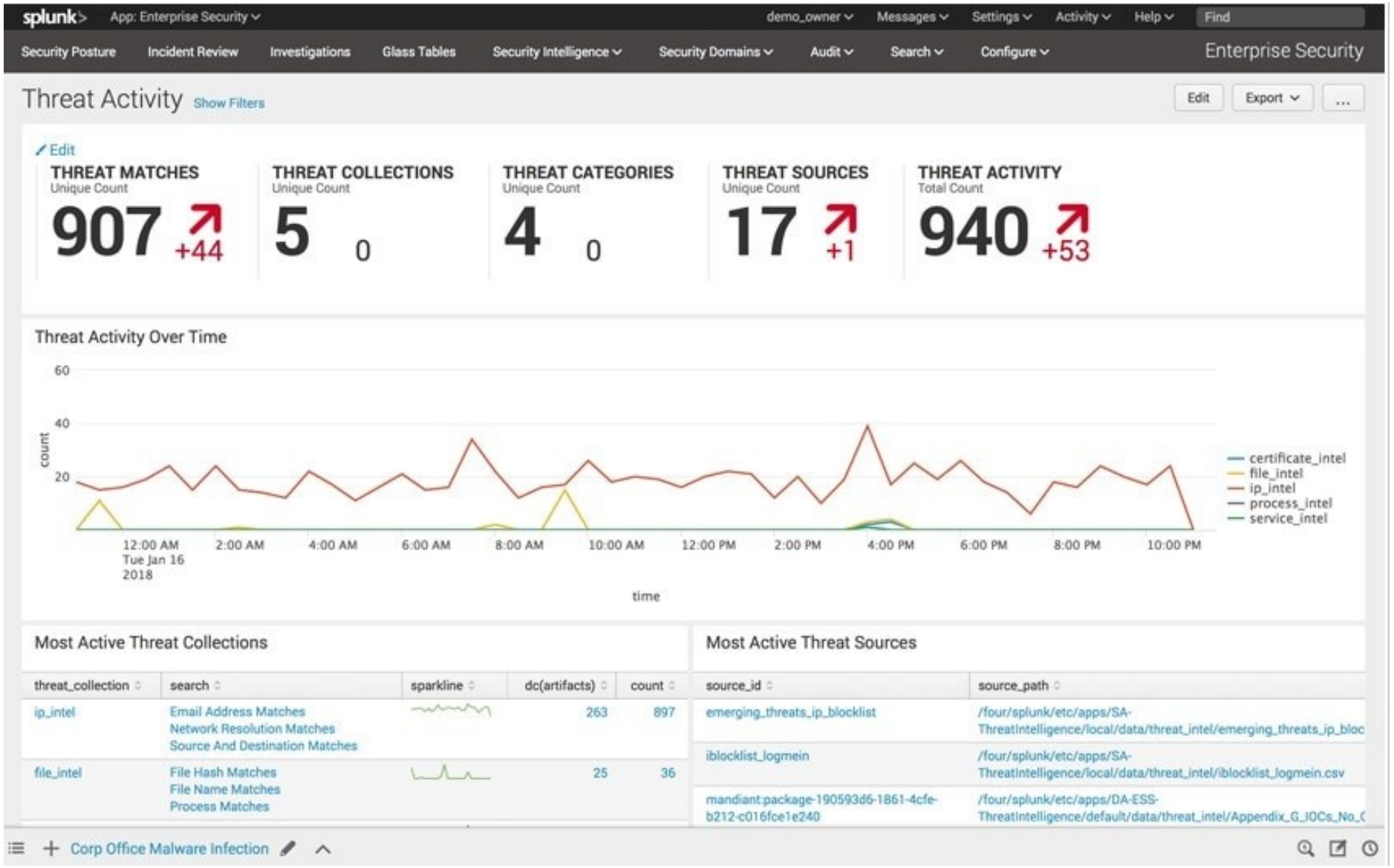
Showing 6 of 500

ALERTAS, ALERTAS E MAIS ALERTAS...

Time	Alert	Priority	Status
7:30 am	Por Scan ALERT	Low (3)	Completed
7:55 am	User Reported: <HR Report Attached>	High (1)	Completed
8:00 am	User Reported: <Survey to be filled>	Low (3)	Pending
8:30 am	Port Scan across several machines	Low(3)	Pending
8:32 am	Active Directory – User Accounts Locked Out	Medium (2)	Pending
8:35 am	Active Directory – Windows Admin Credentials	Medium (2)	Investigating
9:10 am	Active Directory – User Authentication failed	High (1)	Pending
9:12 am	Active Directory – User Authentication failed	High (1)	Pending

Showing 8 of 502

SIEM – TAKE 2


splunk> App: Enterprise Security
demo_owner Messages Settings Activity Help Find
Security Posture Incident Review Investigations Glass Tables Security Intelligence Security Domains Audit Search Configure
Enterprise Security
Threat Activity
Show Filters
Edit Export ...
Edit
THREAT MATCHES
Unique Count
907 +44
THREAT COLLECTIONS
Unique Count
5 0
THREAT CATEGORIES
Unique Count
4 0
THREAT SOURCES
Unique Count
17 +1
THREAT ACTIVITY
Total Count
940 +53
Threat Activity Over Time
60
40
20
count
12:00 AM Tue Jan 16 2018
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
time
certificate_intel
file_intel
ip_intel
process_intel
service_intel
Most Active Threat Collections
threat_collection search sparkline dc(artifacts) count
ip_intel Email Address Matches Network Resolution Matches Source And Destination Matches 263 897
file_intel File Hash Matches File Name Matches Process Matches 25 36
Most Active Threat Sources
source_id source_path
emerging_threats_ip_blocklist /four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_bloc
iblocklist_logmein /four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv
mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240 /four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_
Corp Office Malware Infection

REDE CORPORATIVA

jornadas FCCN

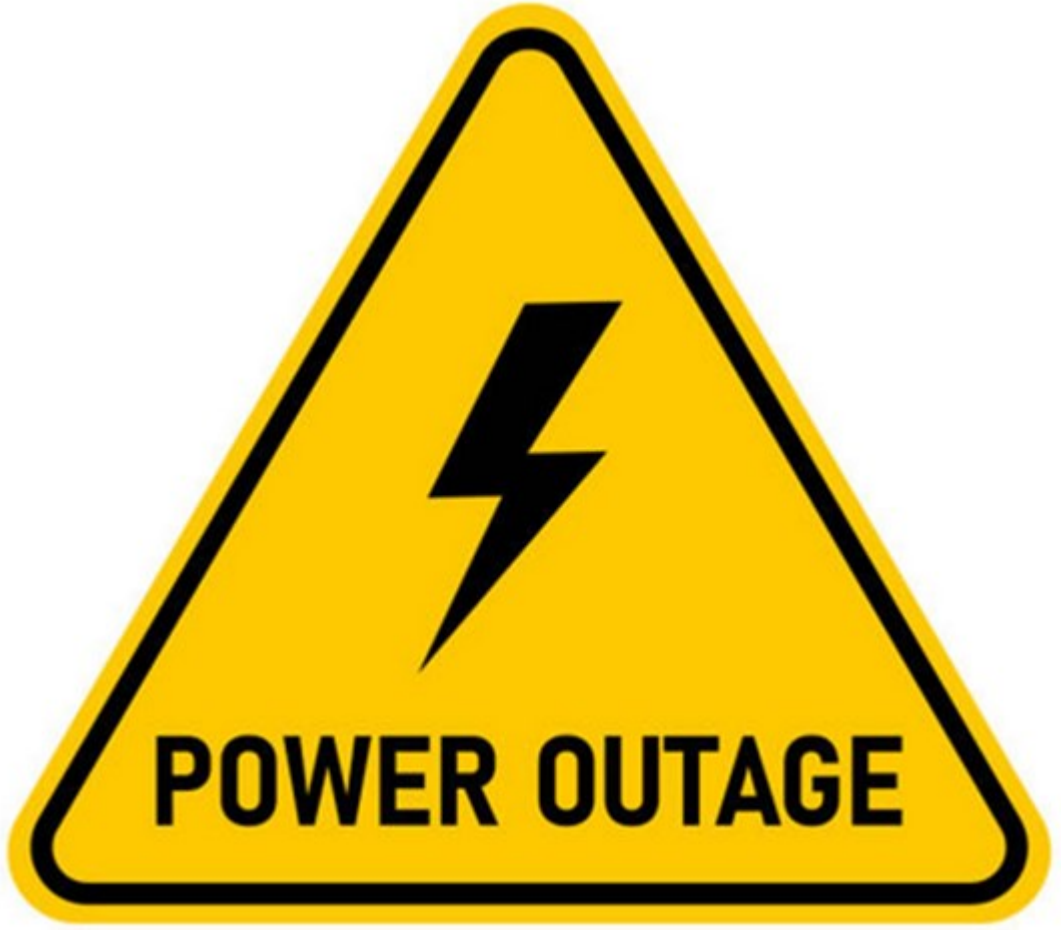
Subnet 1

Subnet 3

INTERNET

Domain Controller

Powergrid



1. Login na AD – HASH DUMP
2. Login na PowerGrid
3. Exfiltrar informação
4. Elimiar evidencias
5. Desligar a rede elétrica

ALERTAS, ALERTAS E MAIS ALERTAS...

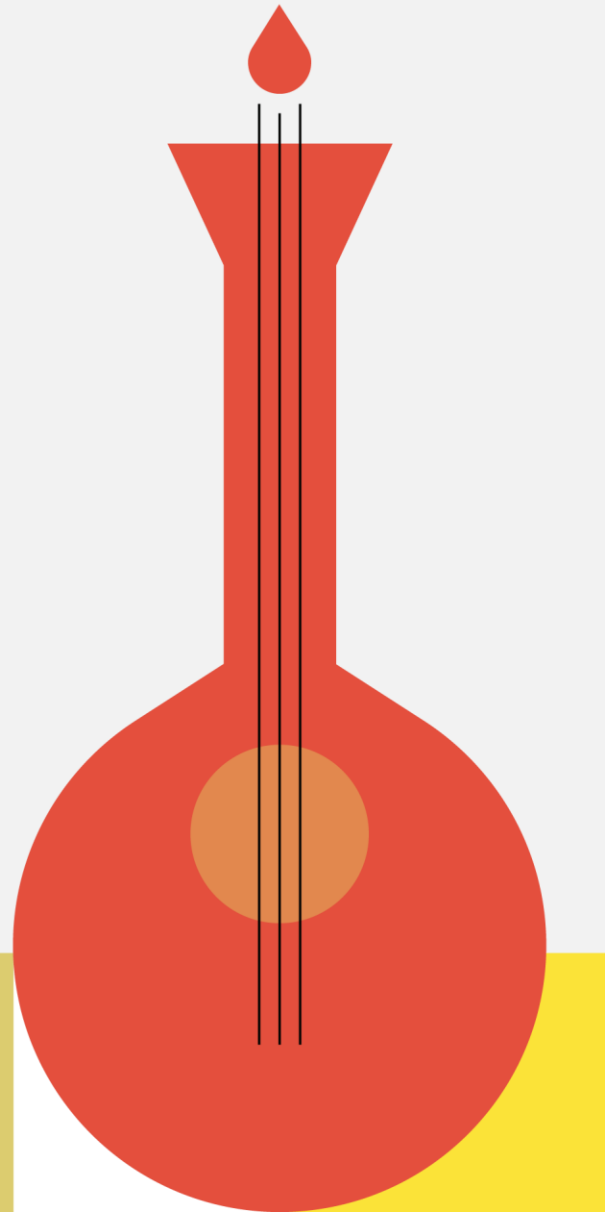
Time	Alert	Priority	Status
7:30 am	Por Scan ALERT	Low (3)	Completed
7:55 am	User Reported: <HR Report Attached>	High (1)	Completed
8:00 am	User Reported: <Survey to be filled>	Low (3)	Pending
8:30 am	Port Scan across several machines	Low(3)	Pending
8:32 am	Active Directory – User Accounts Locked Out	Medium (2)	Pending
8:35 am	Active Directory – Windows Admin Credentials	Medium (2)	Investigating
9:10 am	Active Directory – User Authentication failed	High (1)	Investigating
9:12 am	Active Directory – User Authentication failed	High (1)	Investigating
9:30 am	Active Directory – Suspicious Service Account used to Login do Domain Controller (RDP)	High (1)	Pending
10:00 am	PowerGrip down...	Critical (0)	Pending

Showing 10 of 504

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA