Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Indicadores de Segurança

REUNIÃO MENSAL DE INDICADORES DE SEGURANÇA

Apresentação: Outubro de 2024
Referência: Setembro de 2024

cogetic.

COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

CONFIDENCIAL

TLP:AMBER+STRICT

As informações contidas nesse documento são confidenciais e restrita. Para compartilhar qualquer informação deste material com terceiros, será necessário autorização expressa do Coordenador do SSIC – Serviço de Segurança da Informação e Comunicações da COGETIC.

cogetic.

COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

Princípios da Segurança

Secure by default	*Segurança por padrão*
Keep security simple	*Mantenha segurança simples*
Minimize attack surface área	*Minimizar a área de superfície de ataque*
Segregation of duties	*Segregação de funções*
Least privileges	*Menor privilégio*
Defense in depth	*Defesa em profundidade*
Zero trust	*Confiança zero*
Security documentation	*Documentação de segurança*
Based on reference Frameworks	*Basear-se em Frameworks de referência*



PAUTA

REUNIÃO DE
INDICADORES
DE SEGURAÇA

1. Risk Index: Vision One
2. E-mail Sec: E-mail Security
3. Cloud Sec: CAS
4. Network Sec: DDI e Fortinet
5. Endpoint Sec: Apex One e Workload Security
6. Highlights – Pontos de Destaque
7. Pontos de Melhorias e Encaminhamentos

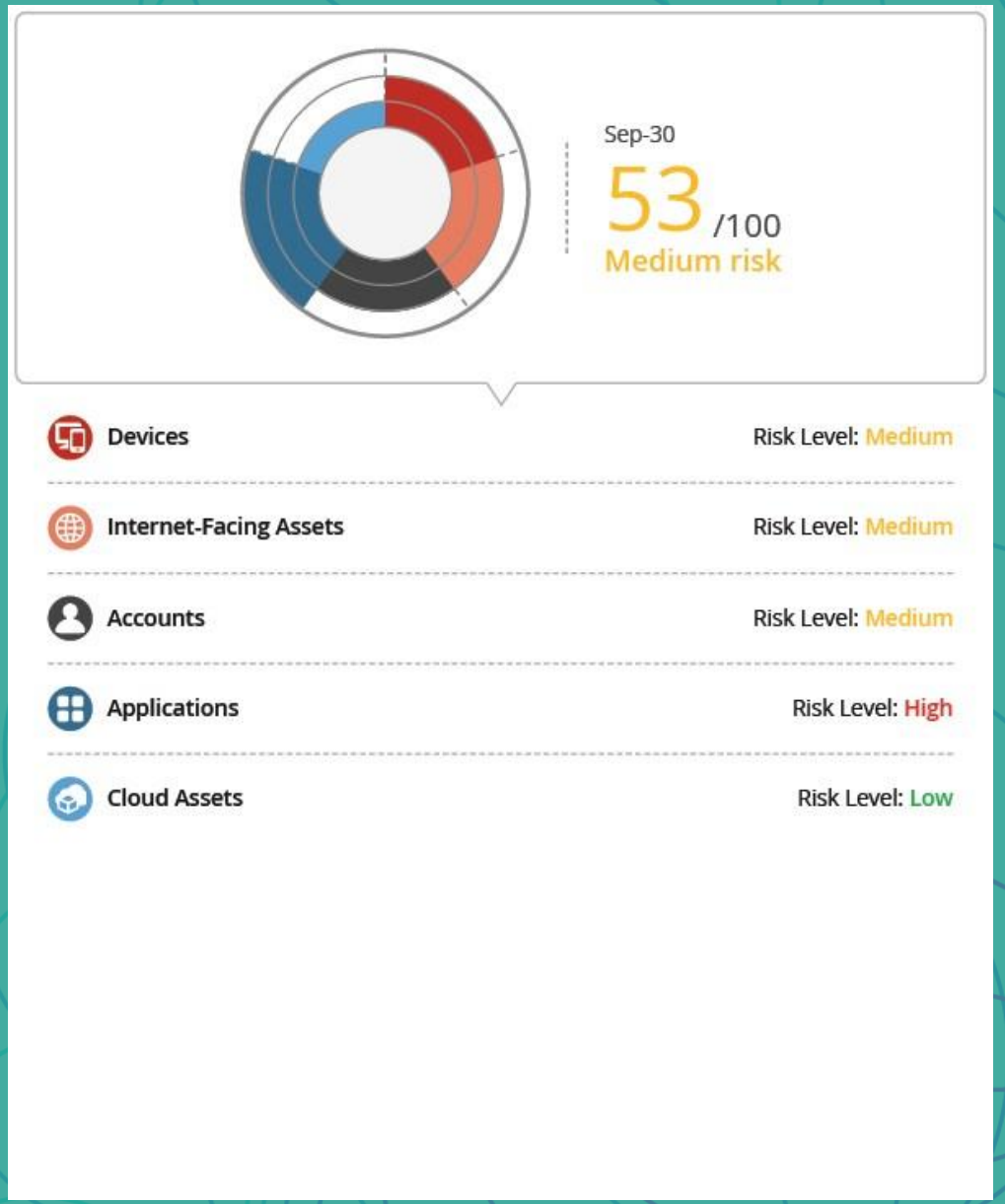
cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

Risk Index [TMVO]

RISK OVERVIEW

01/07	01/08	01/09	01/10
62	58	60	53

cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

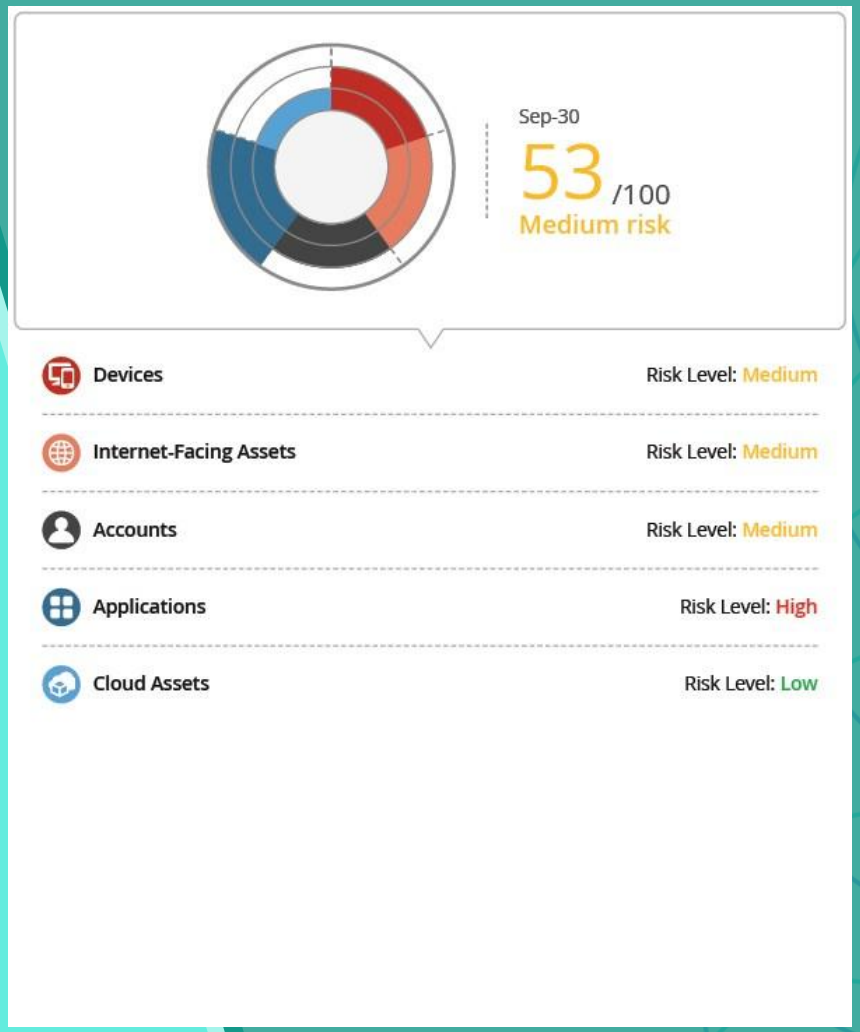


Risk Index [TMVO]

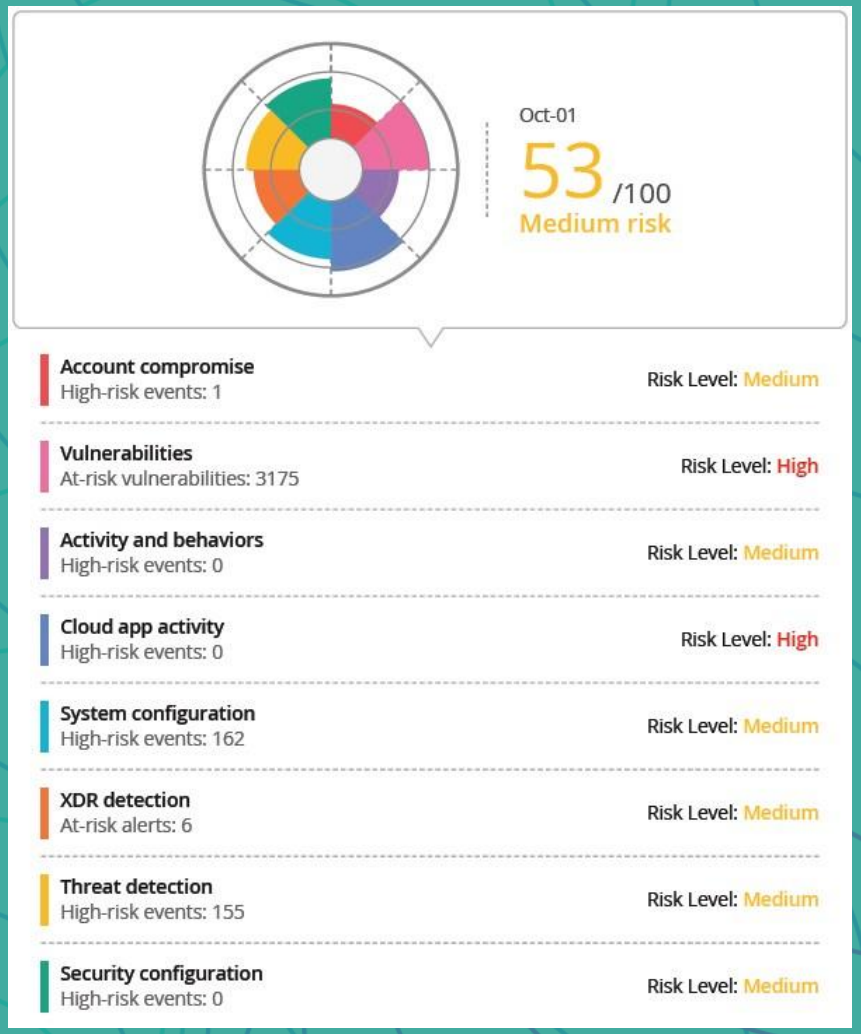
RISK OVERVIEW

cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

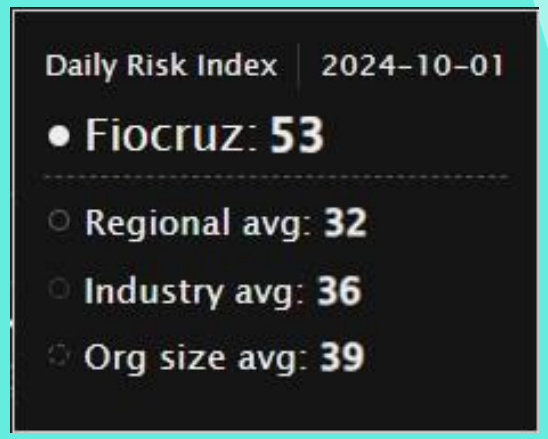
Risk Index



Risk Factors



Risk Index [TMVO]



cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

Principais ações percebidas:

1) Configurações no Vision One

2) Tratamento das **Unidades** em máquinas infectadas

3) Tratamento das **Unidades** em agentes problemáticos

Risk Index

[DETECÇÕES EM CAMADAS]

cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

Email Sec
223.863
+59,44%

NDR
NA
NA%

CASB
1.608
-02,62%

Firewall
3.481.132
+20,59%

Desktop Security
8.661
-85,22%

Sala Cofre

Server Security
4.456.102
+37,37%

S E G U R A N Ç A E M C A M A D A S

Dados Críticos

Internet

Filtragem entre redes

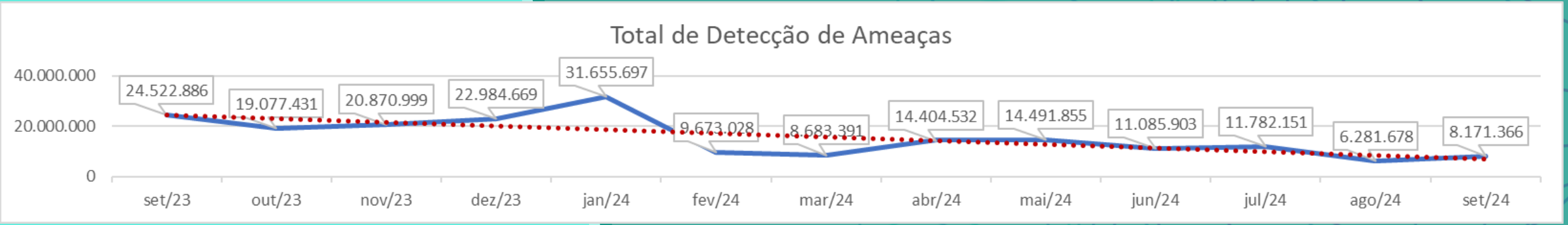
Rede Interna

Segurança Física

Risk Index [TMVO]

DETECÇÕES EM CAMADAS

Detecções	jun-24	jul-24	ago-24	set-24
Email Sec	58.567	84.729	90.801	223.863
Cloud App Security	4.339	3.007	1.567	1.608
NDR	62	232	264	NA
Firewall	8.060.404	7.259.350	2.886.664	3.481.132
Apex One	28.339	18.201	58.584	8.661
Workload Security	2.934.192	4.416.632	3.243.798	4.456.102
TOTAL	**11.085.903**	**11.782.151**	**6.281.678**	**8.171.366**
	-23,50%	+6,28%	-46,68%	+30,08%



ATTACK SURFACE DISCOVERY [TMVO]

LOCAL APPS



cogetic.

ATTACK SURFACE DISCOVERY [TMVO]

LOCAL APPS

Linux OS
All Risk Score

Local app	Version	Operating system	Vendor	App risk score ↓	Devices	Highly exploitable CVEs
tomcat	7.0.54	Linux	CentOS	73	1	9
apache2-bin	2.4.38-3+deb10u4	Linux	Debian Apache Maintain...	71	1	9
apache2-data	2.4.38-3+deb10u4	Linux	Debian Apache Maintain...	71	1	9
apache2-utils	2.4.38-3+deb10u4	Linux	Debian Apache Maintain...	71	1	9
apache2	2.4.38-3+deb10u4	Linux	Debian Apache Maintain...	71	2	9
libwebpdemux2	0.6.1-2ubuntu0.18....	Linux	Ubuntu Developers <ub...	69	1	1
libwebp6	0.6.1-2.1	Linux	Jeff Breidenbach <jab@d...	69	2	1
libvpx6	1.8.2-1build1	Linux	Ubuntu Developers <ub...	69	1	1
libwebp6	0.6.1-2.1+deb11u1	Linux	Jeff Breidenbach <jab@d...	69	2	1
libwebp7	1.2.2-2	Linux	Ubuntu Developers <ub...	69	4	1
libwebpdemux2	1.2.2-2	Linux	Ubuntu Developers <ub...	69	2	1
libwebpmux3	1.2.2-2	Linux	Ubuntu Developers <ub...	69	2	1
libwebp6	0.6.1-2ubuntu0.18....	Linux	Ubuntu Developers <ub...	69	2	1
libwebpmux3	0.6.1-2ubuntu0.18....	Linux	Ubuntu Developers <ub...	69	2	1

cogetic.

ATTACK SURFACE DISCOVERY [TMVO]

LOCAL APPS

All OS
High Risk Score

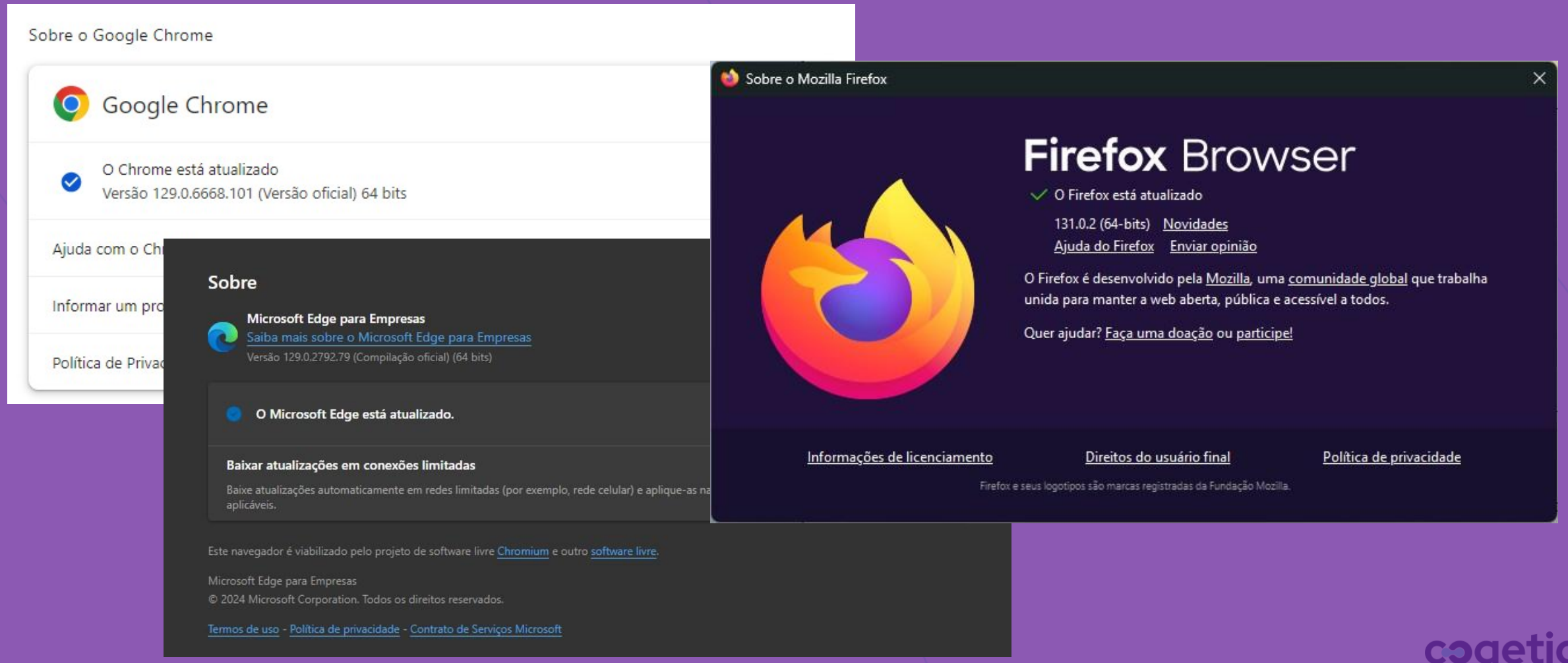
Local app	Version	Operating system	Vendor	App risk score	Devices	Highly exploitable ... ↓
Google Chrome	63.0.3239.132	Windows	Google	73	2	197
Google Chrome	85.0.4183.102	Windows	Google LLC	73	1	126
Google Chrome	85.0.4183.121	Windows	Google LLC	73	41	126
Google Chrome	86.0.4240.75	Windows	Google LLC	73	1	125
Google Chrome	87.0.4280.88	Windows	Google LLC	73	5	114
Google Chrome	87.0.4280.141	Windows	Google LLC	73	6	113
Google Chrome	89.0.4389.90	Windows	Google LLC	73	5	103
Google Chrome	90.0.4430.93	Windows	Google LLC	73	4	98
Google Chrome	90.0.4430.212	Windows	Google LLC	73	5	97
Google Chrome	91.0.4472.106	Windows	Google LLC	73	2	94
Google Chrome	91.0.4472.124	Windows	Google LLC	73	5	93
Google Chrome	91.0.4472.114	Windows	Google LLC	73	4	93
Google Chrome	91.0.4472.164	Windows	Google LLC	73	7	91
Google Chrome	92.0.4515.107	Windows	Google LLC	73	4	90

ATTACK SURFACE DISCOVERY [TMVO]

LOCAL APPS

All OS

High Risk Score



cogetic.

ATTACK SURFACE DISCOVERY [TMVO]

DOMAIN LIST

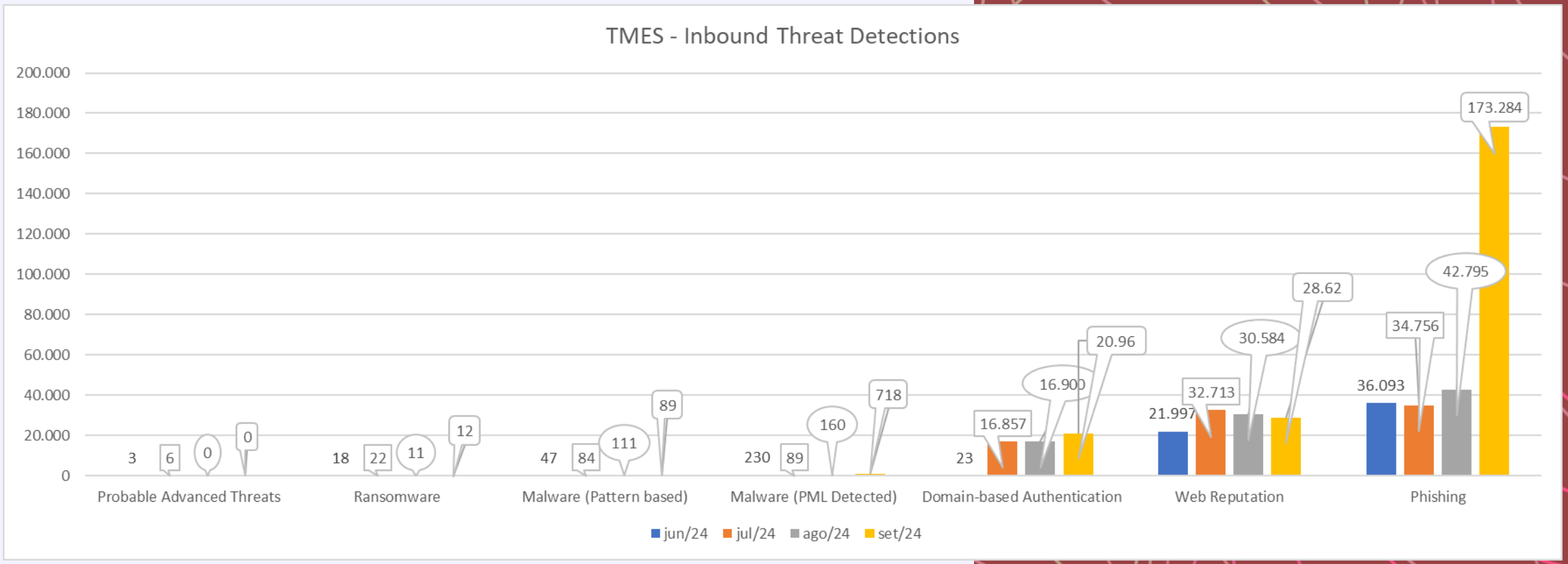
Host	Asset risk score ↓	Public IPs	Services	Ports
asfoc.fiocruz.br ★	73	1	DNS, HTTP, HTTPS, MySQL	53, 80, 443, 2000, 3306
glpi.campusvirtual.fiocruz.br	69	1	HTTP, HTTPS	80, 443
correio.cdts.fiocruz.br	69	1	HTTPS	443
dplnx-a.incqs.fiocruz.br	69	1	HTTPS	443
cloud.ensp.fiocruz.br	69	1	HTTP, HTTPS	80, 443
helpdesk.matogrossodosul.fiocruz.br	69	1	HTTPS	443
www.dichistoriasaude.coc.fiocruz.br	69	2	HTTP, HTTPS	80, 443
poc.eleicoes.fiocruz.br	69	1	HTTP, HTTPS	80, 443
rt-bl5-dtc-01.incqs.fiocruz.br	69	1	HTTP, HTTPS	80, 443
teste.ouvidoria.fiocruz.br	69	1	HTTP, HTTPS	80, 443
solucoes.agora.fiocruz.br	69	1	HTTP, HTTPS	80, 443
sagittarius.coc.fiocruz.br	69	1	HTTP, HTTPS	80, 443
periodicoshomol.fiocruz.br	69	1	HTTP, HTTPS	80, 443
own.procc.fiocruz.br	69	1	HTTP, HTTPS	80, 443
sisproj.fiocruz.br	69	1	HTTP, HTTPS	80, 443

ATTACK SURFACE DISCOVERY [TMVO]

DEVICE LIST

Device name	Asset risk sc... ↓	Highly exploita...	Devic...	Operating system	IP address
everolimo ★	80	61	Server	Windows Server, version 1809 10.0 (Build 17763)	10.2.2.72, 172.20.0.1, 172.31.32.1
EPSJV-SB-MOODLE	80	75	Server	Windows Server 2012 R2 6.3 (Build 9600)	157.86.173.251
EPSJV-N-LATEC	78	150	Desktop	Windows 10 10.0 (Build 19043)	169.254.187.146, 169.254.33.141, 169.254.205.118, 192.168.0.111, 169.254.13.198
157.86.252.9	78	0	Server	CentOS 7 3.10.0	-
csegsff35186	77	192	Desktop	Windows 10 10.0 (Build 18362)	157.86.170.134, 169.254.196.33, 169.254.100.137, 169.254.244.154
naff29165	76	189	Desktop	Windows 10 10.0 (Build 17134)	10.99.60.47
CSEGSFF35343	76	174	Desktop	Windows 10 10.0 (Build 18362)	157.86.169.73, 169.254.195.190, 169.254.143.251, 169.254.63.107, 169.254.54.193
cestehf28772	76	390	Desktop	Windows 10 10.0 (Build 19044)	10.99.7.203
seplamf29166	76	188	Desktop	Windows 10 10.0 (Build 18362)	10.99.30.24
CESTEHF35360	76	171	Desktop	Windows 10 10.0 (Build 18362)	169.254.151.236, 169.254.19.45, 169.254.24.151, 10.99.7.153, 169.254.168.86
csegsff35594	76	631	Desktop	Windows 10 10.0 (Build 17763)	169.254.168.102, 157.86.170.103, 192.168.137.1, 169.254.241.32
CESTEHF157346	76	76	Desktop	Windows 10 10.0 (Build 19045)	169.254.145.28, 169.254.92.222, 169.254.38.23, 10.99.7.32
CLAVESF29276	76	161	Desktop	Windows 10 10.0 (Build 18362)	157.86.162.103
CESTEHF35350	76	175	Desktop	Windows 10 10.0 (Build 18363)	169.254.57.73, 169.254.43.242, 10.99.7.187, 169.254.73.246

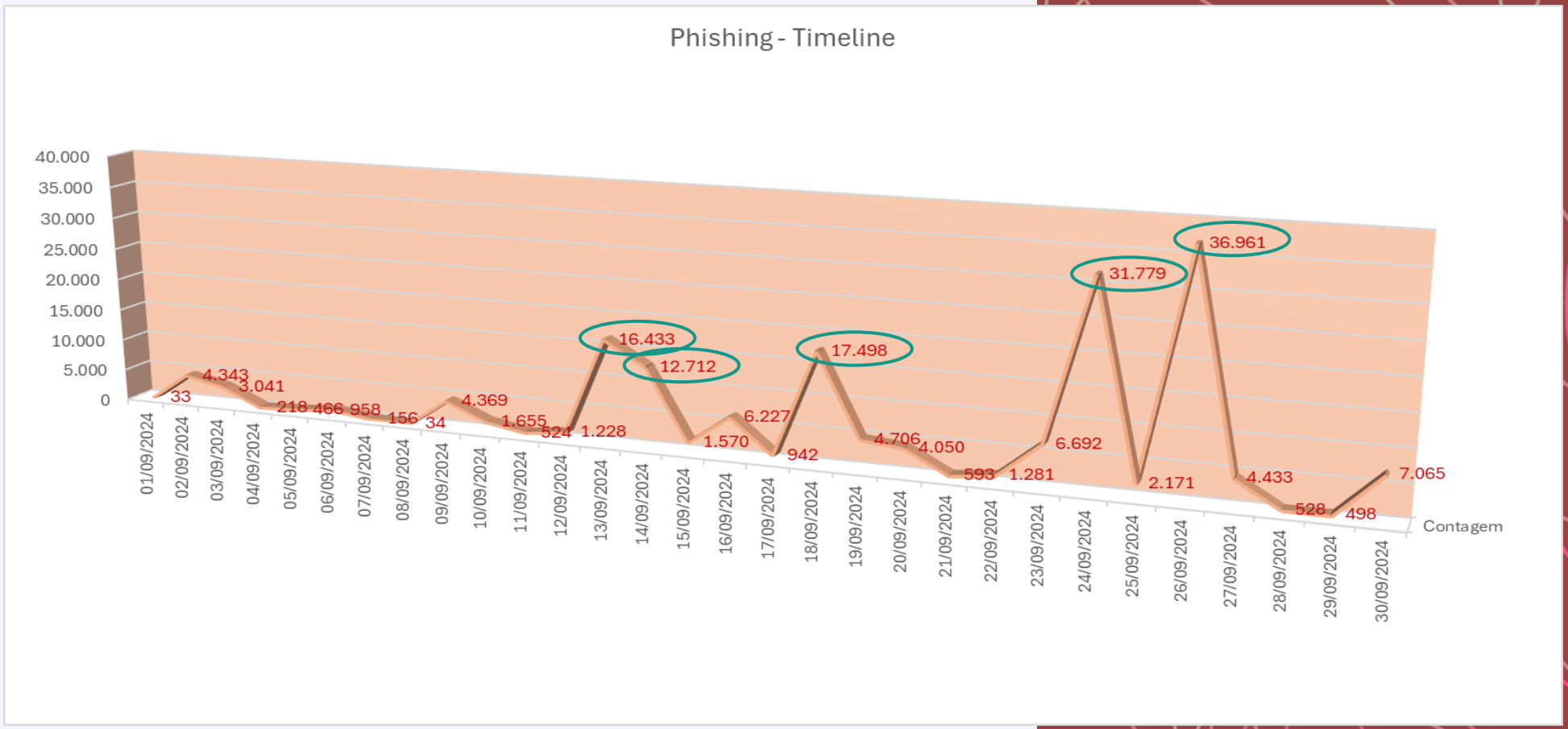
Email Sec [TMES]



cogetic.

Email Sec [TMES]

Phishing



cogetic.

Email Sec [TMES]

Dias 13, 14, 18, 24 e 26
= 115.383 e-mails

Phishing

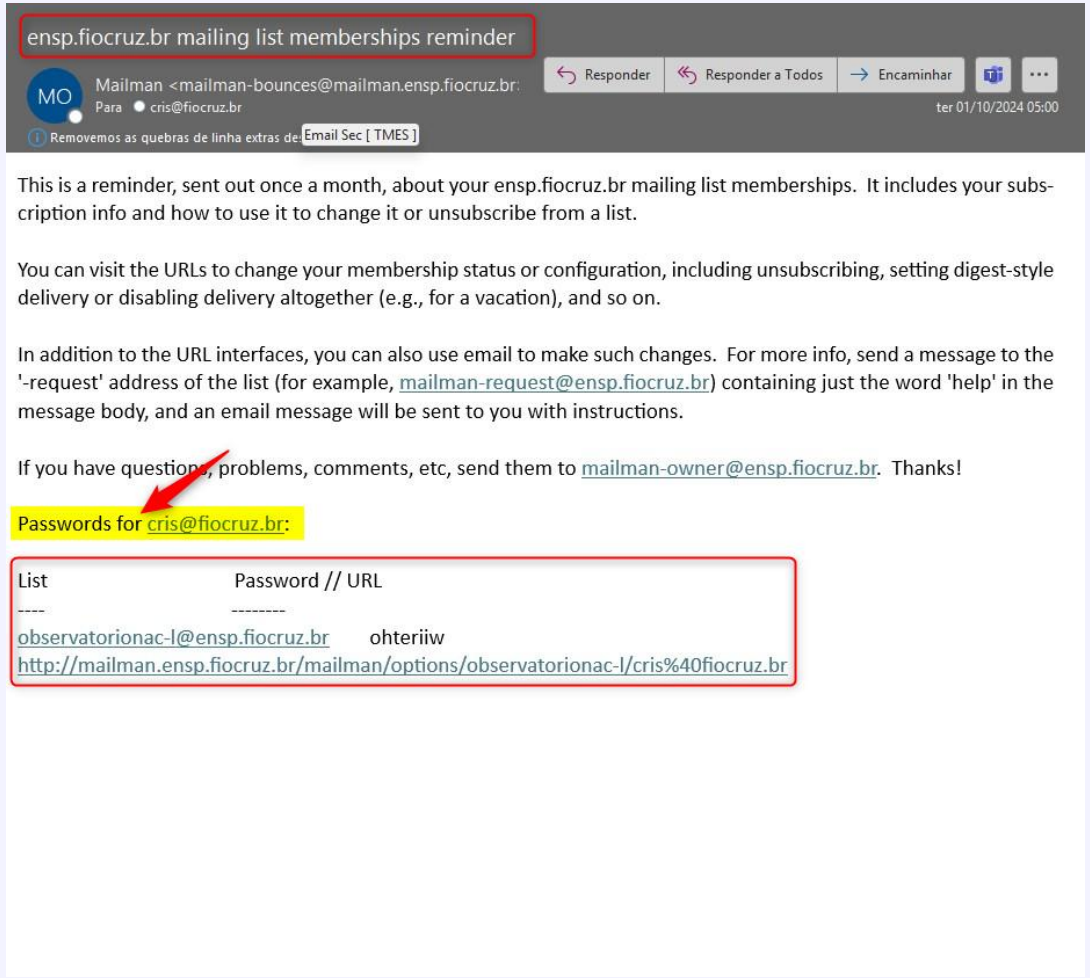
	Remetente	Qtd
1	mailman-bounces@mailman.ensp.fiocruz.br	6.510
2	nao-responder@0886escritorio.mysolutionscompany.com	468
3	nao-responder@empresarial891.departamentomails.team	456
4	nao-responder@escritorio344.mysolutionscompany.com	419
5	nao-responder@centroprodutivo12.pontozip.capital	409
6	nao-responder@escritorio406.mysolutionscompany.com	379
7	nao-responder@89escritorio.mysolutionscompany.com	378
8	daniela.soares@centroprodutivo23.pontozip.capital	367
9	nao-responder@39escritorio.mysolutionscompany.com	366
10	nao-responder@centroprodutivo866.pontozip.capital	352
11	nao-responder@empresarial552.departamentomails.team	352
12	condutor1380@denatranservicos2069.certificadovirtual.lease	348
13	caixa-postal33-ecac@hugodias69.adm-fort.partners	347
14	crlv82@portaldenatran1.sistemasoperant.band	347
15	financeiro66@denatranservicos065.certificadovirtual.lease	347
16	marina.garbossa717@7962qualytec.gestoronlinecompanies.org	347
17	nao-responder@centroprodutivo7.pontozip.capital	339
18	nao-responder@centroprodutivo23.pontozip.capital	330
19	nao-responder@empresarial928.departamentomails.team	328
20	nao-responder@231escritorio.mysolutionscompany.com	322

	Assunto	Qtd
1	(vazio)	13.220
2	ensp.fiocruz.br mailing list memberships reminder	4.221
3	mailman.ensp.fiocruz.br mailing list memberships reminder	1.575
4	Chegou seu documento - Revise assinatura - 18/09/2024	1.359
5	lembrete de membros da lista de discussão mailman.ensp.fiocruz.br	714
6	Netflix - Sua conta foi bloqueada. Revise seus dados.	233
7	ENC:Currículo	140
8	Nota Fiscal Eletrônica Emitida.	111
9	Notificação de Novo Processo Trabalhista	79
10	Nota Fiscal de Serviços Eletrônica - NFS-e	72
11	Your package number #540005452 is waiting to be processed at our facility.	29
12	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 219157388	19
13	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 657763722	19
14	Envio de Currículo e Disponibilidade Imediata	18
15	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 226622442	17
16	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 873238977	17
17	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 685265905	15
18	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 619937691	13
19	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 1498643	12
20	Bem vindo ao BRADESCO PRIME DIGITAL! Protocolo: 296615974	11

Email Sec [TMES]

Dias 13, 14, 18, 24 e 26
= 115.383 e-mails

Phishing



ensp.fiocruz.br mailing list memberships reminder

Mailman <mailman-bounces@mailman.ensp.fiocruz.br>
Para cris@fiocruz.br
Responder | Responder a Todos | Encaminhar
ter 01/10/2024 05:00
Removemos as quebras de linha extras de Email Sec [TMES]

This is a reminder, sent out once a month, about your ensp.fiocruz.br mailing list memberships. It includes your subscription info and how to use it to change it or unsubscribe from a list.

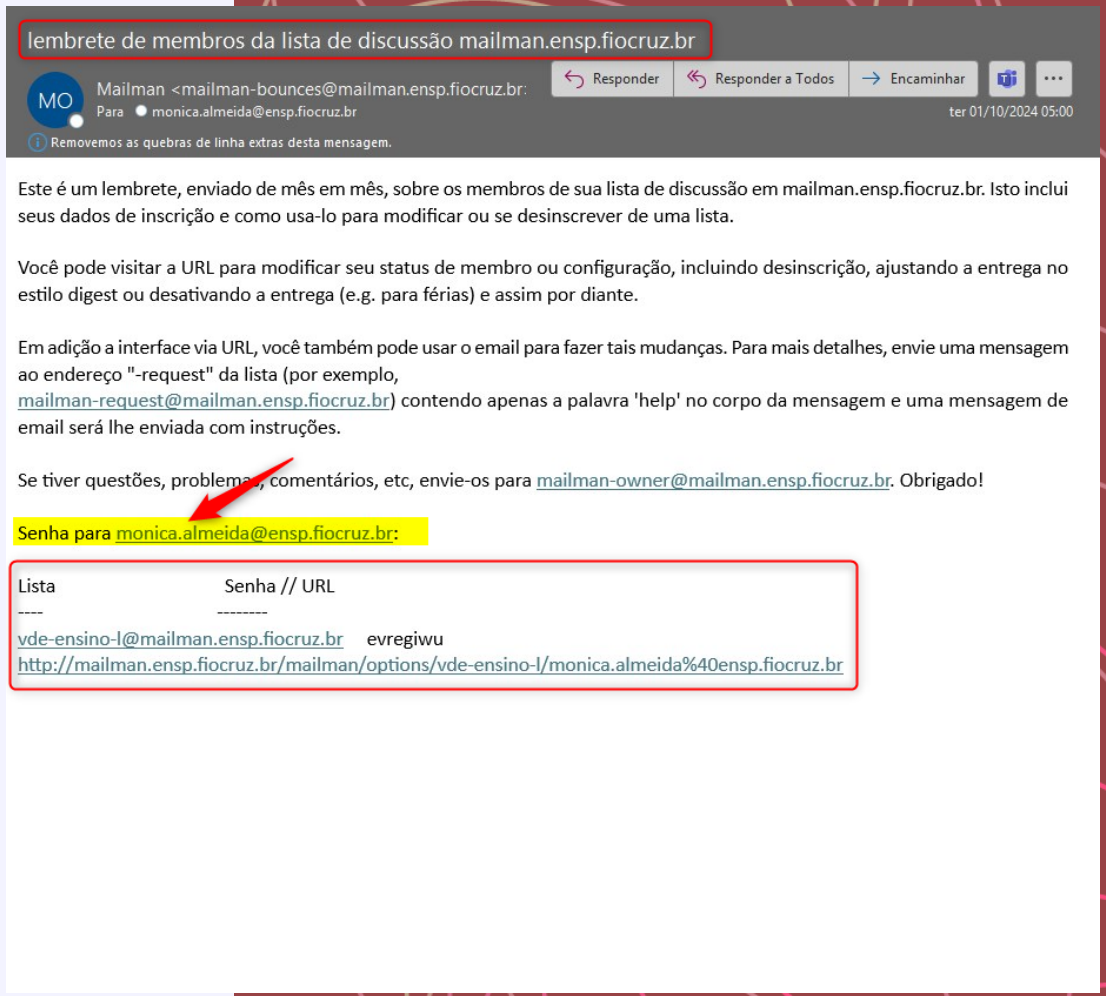
You can visit the URLs to change your membership status or configuration, including unsubscribing, setting digest-style delivery or disabling delivery altogether (e.g., for a vacation), and so on.

In addition to the URL interfaces, you can also use email to make such changes. For more info, send a message to the '-request' address of the list (for example, mailman-request@ensp.fiocruz.br) containing just the word 'help' in the message body, and an email message will be sent to you with instructions.

If you have questions, problems, comments, etc, send them to mailman-owner@ensp.fiocruz.br. Thanks!

Passwords for cris@fiocruz.br:

List	Password // URL
observatorionac-l@ensp.fiocruz.br	ohteriiw
http://mailman.ensp.fiocruz.br/mailman/options/observatorionac-l/cris%40fiocruz.br	



lembrete de membros da lista de discussão mailman.ensp.fiocruz.br

Mailman <mailman-bounces@mailman.ensp.fiocruz.br>
Para monica.almeida@ensp.fiocruz.br
Responder | Responder a Todos | Encaminhar
ter 01/10/2024 05:00
Removemos as quebras de linha extras desta mensagem.

Este é um lembrete, enviado de mês em mês, sobre os membros de sua lista de discussão em mailman.ensp.fiocruz.br. Isto inclui seus dados de inscrição e como usa-lo para modificar ou se desinscrever de uma lista.

Você pode visitar a URL para modificar seu status de membro ou configuração, incluindo desinscrição, ajustando a entrega no estilo digest ou desativando a entrega (e.g. para férias) e assim por diante.

Em adição a interface via URL, você também pode usar o email para fazer tais mudanças. Para mais detalhes, envie uma mensagem ao endereço "-request" da lista (por exemplo, mailman-request@mailman.ensp.fiocruz.br) contendo apenas a palavra 'help' no corpo da mensagem e uma mensagem de email será lhe enviada com instruções.

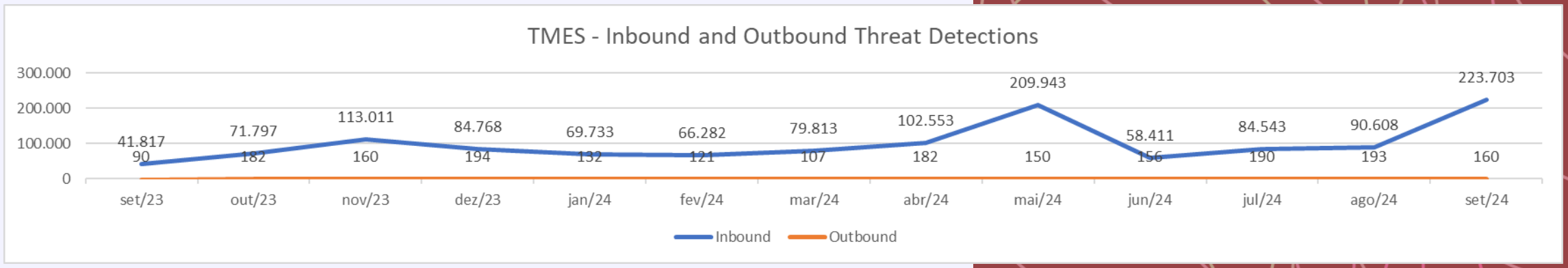
Se tiver questões, problemas, comentários, etc, envie-os para mailman-owner@mailman.ensp.fiocruz.br. Obrigado!

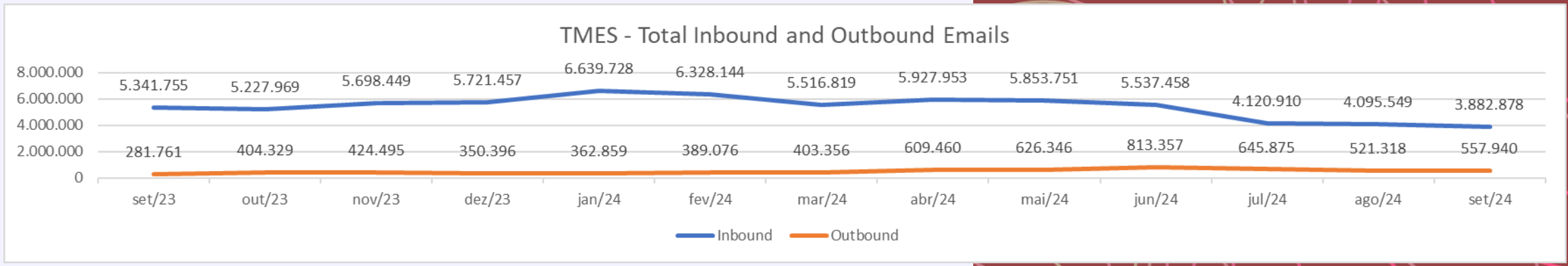
Senha para monica.almeida@ensp.fiocruz.br:

Lista	Senha // URL
vde-ensino-l@mailman.ensp.fiocruz.br	evregiwu
http://mailman.ensp.fiocruz.br/mailman/options/vde-ensino-l/monica.almeida%40ensp.fiocruz.br	

cogetic.

Email Sec [TMES]

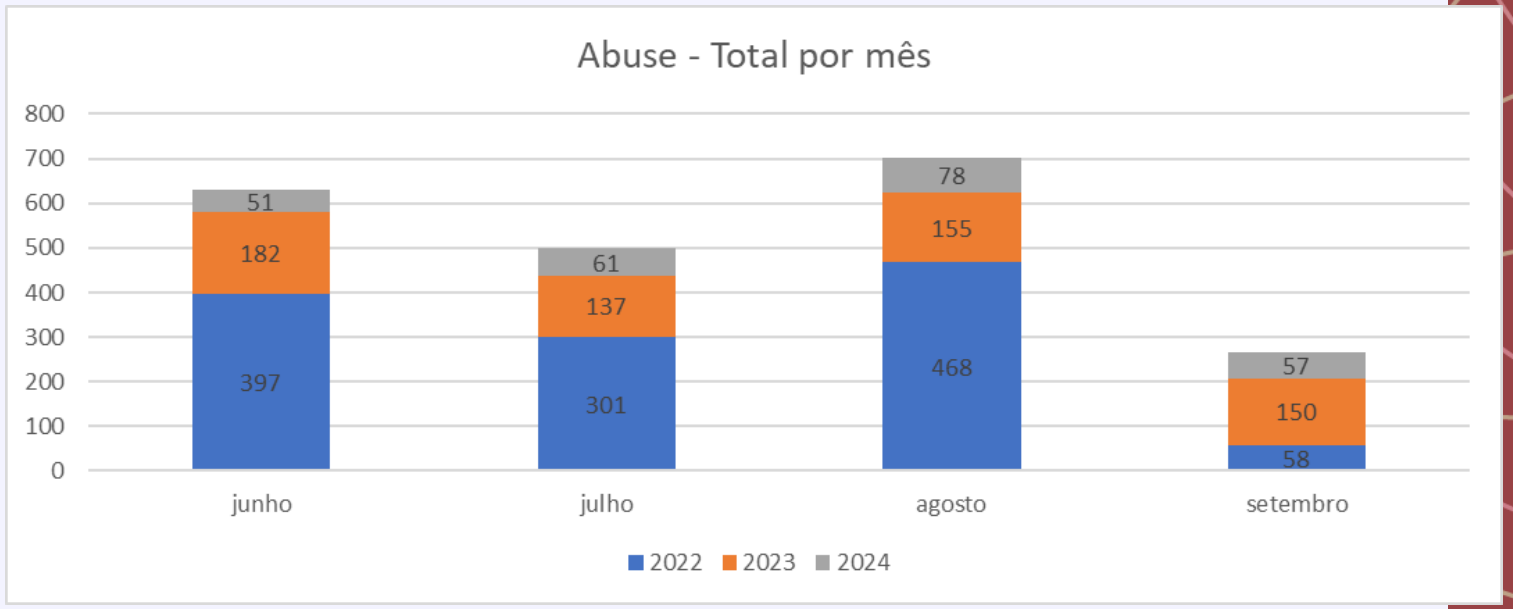


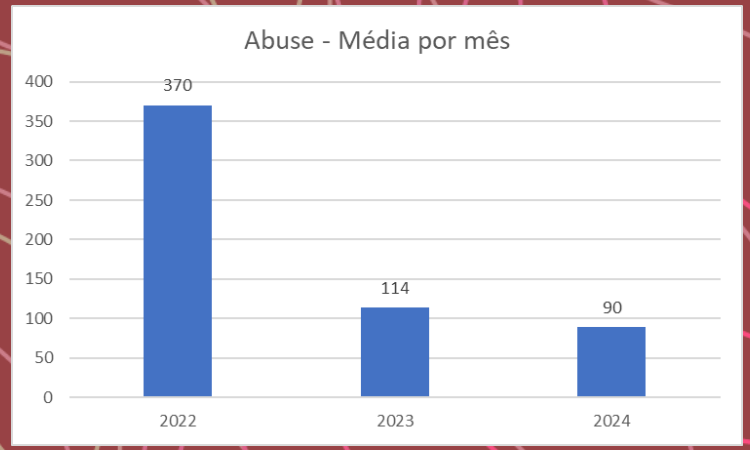


cogetic.

Email Sec
[Abuse]

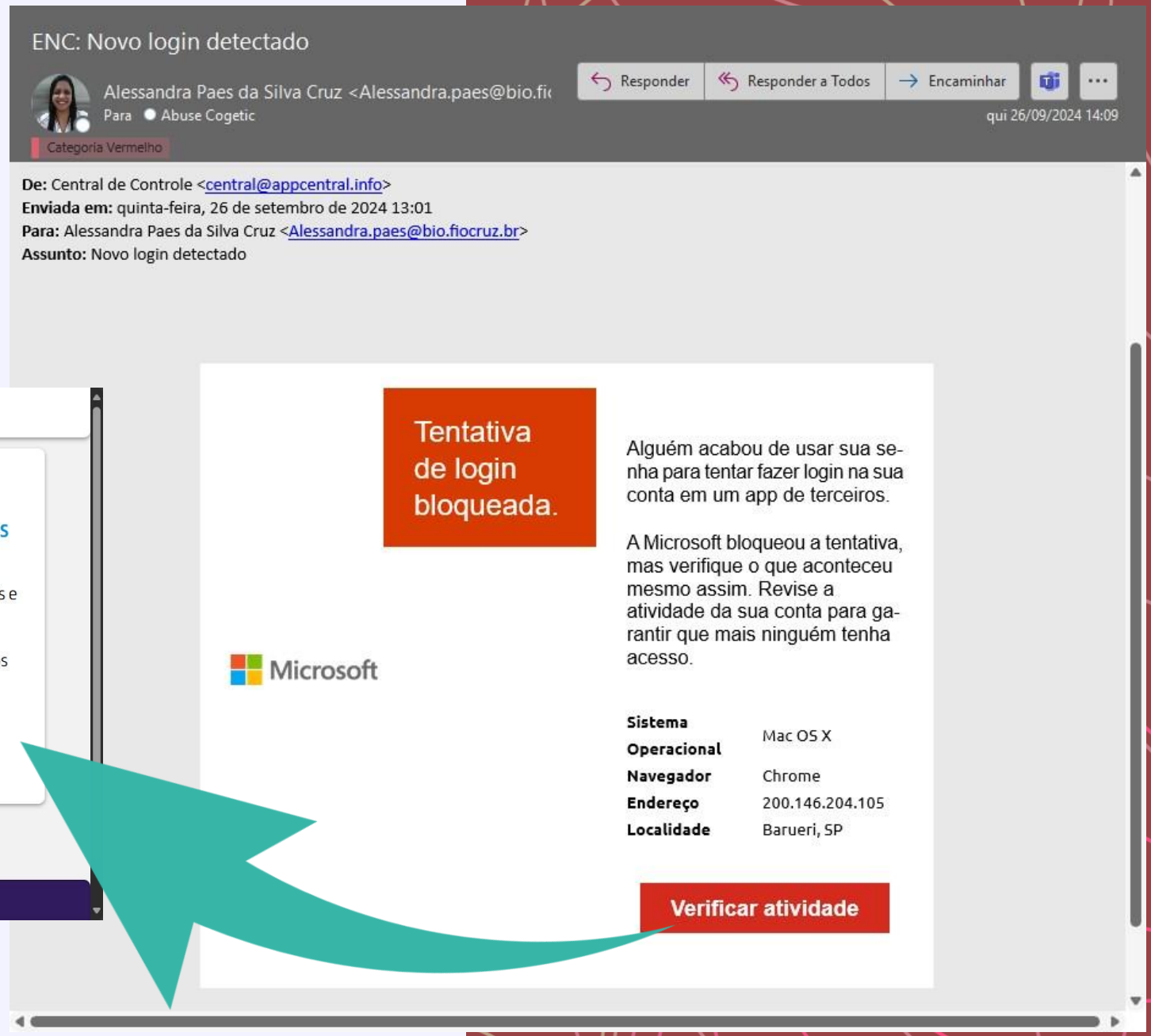
Abuse	jun-24	jul-24	ago-24	set-24
Total	51	61	78	57

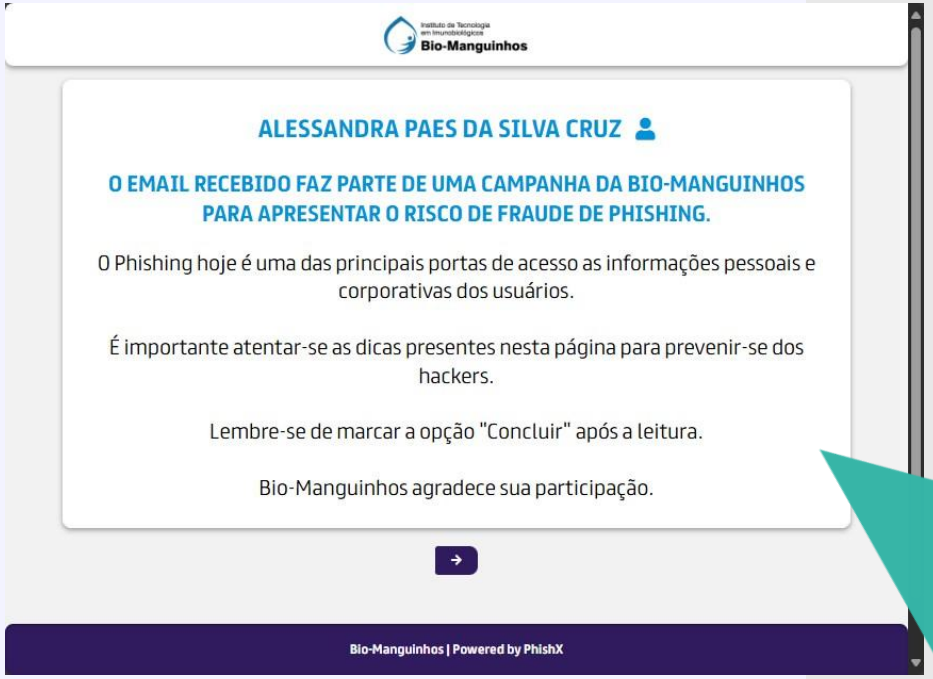




cogetic.

Email Sec
[Abuse]

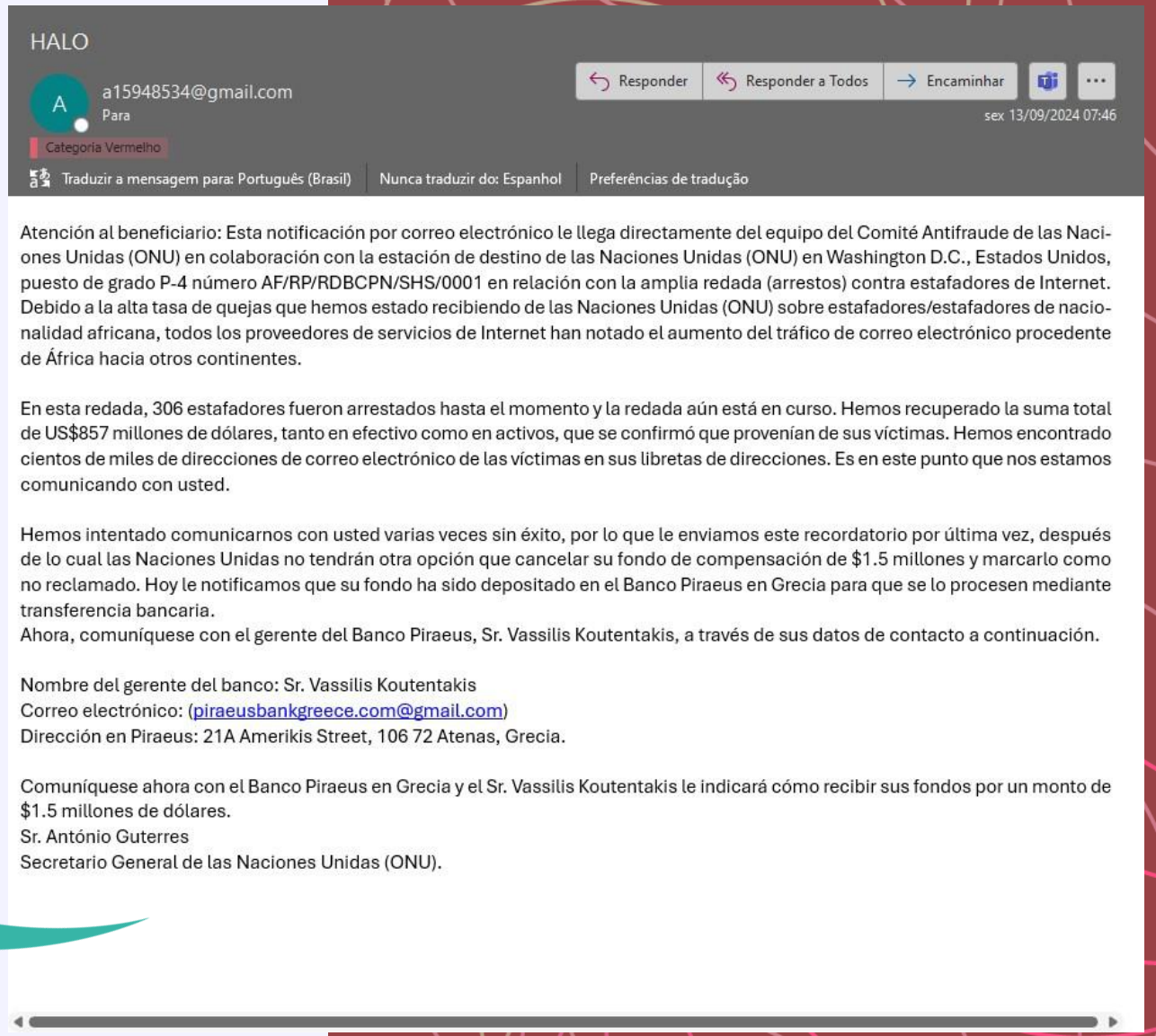




cogetic.

Email Sec [Abuse]

Tentamos entrar em contato com você várias vezes sem sucesso. Por isso, estamos enviando este lembrete *pela última vez*, após o qual as Nações Unidas não terão outra opção a não ser *cancelar seu fundo de compensação* de US$ 1,5 milhão e marcá-lo como não reclamado.



HALO

A a15948534@gmail.com
Para

Responder | Responder a Todos | Encaminhar

sex 13/09/2024 07:46

Categoria Vermelho

Traduzir a mensagem para: Português (Brasil) | Nunca traduzir do: Espanhol | Preferências de tradução

Atención al beneficiario: Esta notificación por correo electrónico le llega directamente del equipo del Comité Antifraude de las Naciones Unidas (ONU) en colaboración con la estación de destino de las Naciones Unidas (ONU) en Washington D.C., Estados Unidos, puesto de grado P-4 número AF/RP/RDBCPN/SHS/0001 en relación con la amplia redada (arrestos) contra estafadores de Internet. Debido a la alta tasa de quejas que hemos estado recibiendo de las Naciones Unidas (ONU) sobre estafadores/estafadores de nacionalidad africana, todos los proveedores de servicios de Internet han notado el aumento del tráfico de correo electrónico procedente de África hacia otros continentes.

En esta redada, 306 estafadores fueron arrestados hasta el momento y la redada aún está en curso. Hemos recuperado la suma total de US$857 millones de dólares, tanto en efectivo como en activos, que se confirmó que provenían de sus víctimas. Hemos encontrado cientos de miles de direcciones de correo electrónico de las víctimas en sus libretas de direcciones. Es en este punto que nos estamos comunicando con usted.

Hemos intentado comunicarnos con usted varias veces sin éxito, por lo que le enviamos este recordatorio por última vez, después de lo cual las Naciones Unidas no tendrán otra opción que cancelar su fondo de compensación de $1.5 millones y marcarlo como no reclamado. Hoy le notificamos que su fondo ha sido depositado en el Banco Piraeus en Grecia para que se lo procesen mediante transferencia bancaria.
Ahora, comuníquese con el gerente del Banco Piraeus, Sr. Vassilis Koutentakis, a través de sus datos de contacto a continuación.

Nombre del gerente del banco: Sr. Vassilis Koutentakis
Correo electrónico: (piraeusbankgreece.com@gmail.com)
Dirección en Piraeus: 21A Amerikis Street, 106 72 Atenas, Grecia.

Comuníquese ahora con el Banco Piraeus en Grecia y el Sr. Vassilis Koutentakis le indicará cómo recibir sus fondos por un monto de $1.5 millones de dólares.
Sr. António Guterres
Secretario General de las Naciones Unidas (ONU).

cogetic.

Email Sec [Abuse]

win10

Environment-specific risk level	High — The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	VAN_WEB_THREAT.UMXX
Exploited vulnerabilities	-
Network connection	Management

Object 1 - https://tinyurl.com/mdhb564v/index.php?email=infraestrutura@fiocruz.br (URL)

File name	https://tinyurl.com/mdhb564v/index.php?email=infraestrutura@fiocruz.br
File type	URL
SHA-1	A78750110B9C08D899338B454944DE9420AE86C6
SHA-256	3919F42F159CDC57E39F8004E0FDD394880B3C0ECF83A09D2454B132A4634DFB
MD5	668634F899A21BFC9FC684490415EE07
TLSH	T1EFA0222B3388CF2BE23288CAA8CC300CA00303008C080008C00A0C0C
Risk level	High
Detection	VAN_WEB_THREAT.UMXX
Exploited vulnerabilities	-
Threat characteristics	Malformed, defective, or with known malware traits (1)

ENC: infraestrutura, 15:20 09/09/2024.

Guilherme Menezes dos Santos
Para Abuse Cogetic

Responder | Responder a Todos | Encaminhar

seg 09/09/2024 15:43

Categoria Vermelho

Se houver problemas com o modo de exibição desta mensagem, clique aqui para exibi-la em um navegador da Web.

,_15_19_09_09_2024..pdf
44 KB

FIOCRUZ

Casa de Oswaldo Cruz • Fundação Oswaldo Cruz

Tel.: +55 (21) 3865-2201

De: Sr(a) infraestrutura. <paloma.decote1@espiral.eng.br>
Enviado: segunda-feira, 9 de setembro de 2024 15:20
Para: Infraestrutura COC <infraestrutura@fiocruz.br>
Assunto: infraestrutura, 15:20 09/09/2024.

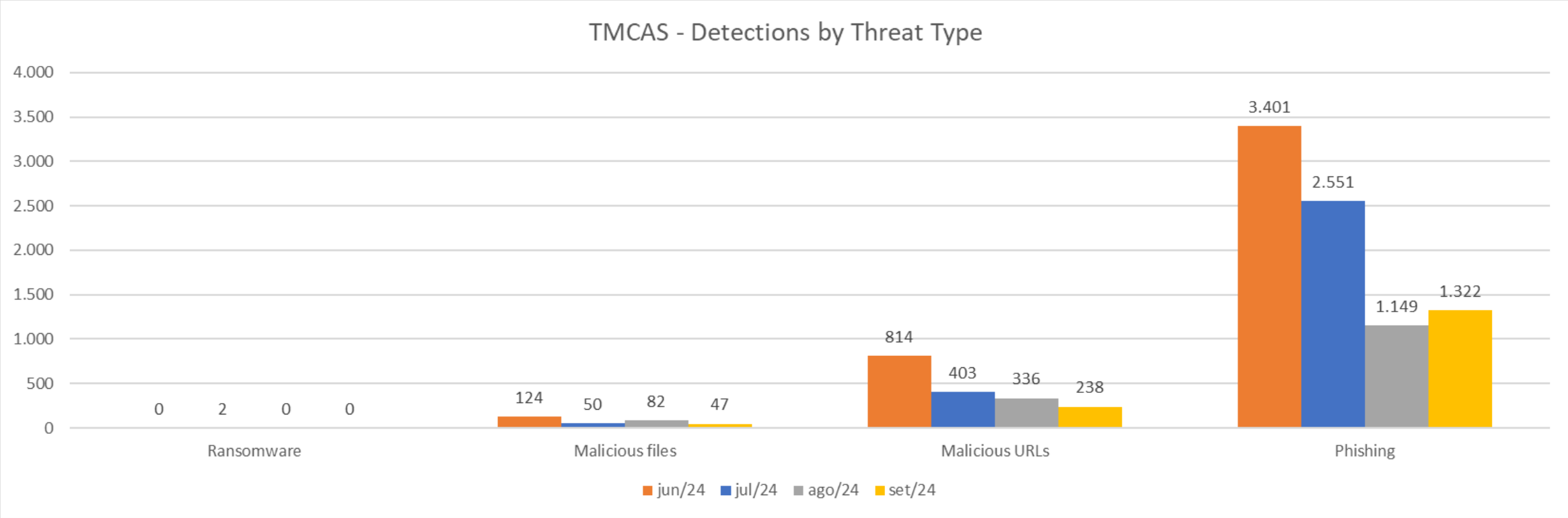
Aviso de Segurança: Renovação de Senha
Gostaríamos de informar que a senha associada ao seu endereço de e-mail infraestrutura está próxima de expirar.
Um novo código de segurança será gerado automaticamente em até 72 horas.
Para manter sua conta protegida, recomendamos que você atualize suas informações de registro o mais breve possível.
15:20 09/09/2024.

MANTER SENHA

cogetic.

Cloud Sec [TMCAS]

Threat Type	jun-24	jul-24	ago-24	set-24
Total	4.339	3.007	1.567	1.608



cogetic.

Network Sec [TMDDI]

Threat Detection Report	jun-24	jul-24	ago-24	set-24
Detected Events	62	232	264	NA
Attack Sources	6	15	13	NA
Event Types	2	4	3	NA
Affected Hosts	9	20	13	NA

cogetic.

Network Sec [FNT]

#	Ameaça CORP	jun/24	jul/24	ago/24	set/24
1	FG_MASTER (FG2K2ET920900331)	6.054.874	5.486.671	4.976.080	4.894.193
2	FW-FARMANGUINHOS	456.894	478.424	422.924	413.276
3	FG_Pernambuco	472.083	337.527	401.291	314.154
4	FG_CEARA (FG2K2ET920900292)	106.003	246.463	230.715	38.145
5	FG_ILMD	72.840	36.614	29.861	16.533
6	FGT_IRR	131	1.804	1.126	6.509
7	FG-MS	1.339	4.317	3.186	3.410
8	FG_Rondonia		1.865	3.769	3.138
9	FG_Parana	3.416	2.238	2.315	2.960
10	FG-Gereb	120.681	2.038	3.078	1.466
11	FG_Bahia	12.512	1.446	2.797	215
12	FG_MASTER (FG2K2ET920900371)				
13	FG_CEARA (FG2K2ET920900327)				
	TOTAL	**7.786.565**	**6.599.407**	**6.077.142**	**5.693.999**

#	Ameaça CORP	jun/24	jul/24	ago/24	set/24
1	SpywareCnC	7.588.872	6.352.516	5.817.493	5.409.622
2	CnC	188.021	240.620	257.489	278.426
3	InstallationTraffic	7.779	4.798	1.265	5.422
4	Lnkr	894	1.169	696	288
5	Sinkhole	185	93	73	95
6	APTAttack	717	187	112	54
7	PostInfectionTraffic	18	4	3	42
8	Wajam	7	14	9	24
9	W32/StartPage	72	4	2	16
10	Sunburst				8
11	Adware.InstallCore		2		2
12	Shlayer				
	Total	**7.786.565**	**6.599.407**	**6.077.142**	**5.693.999**

cogetic.

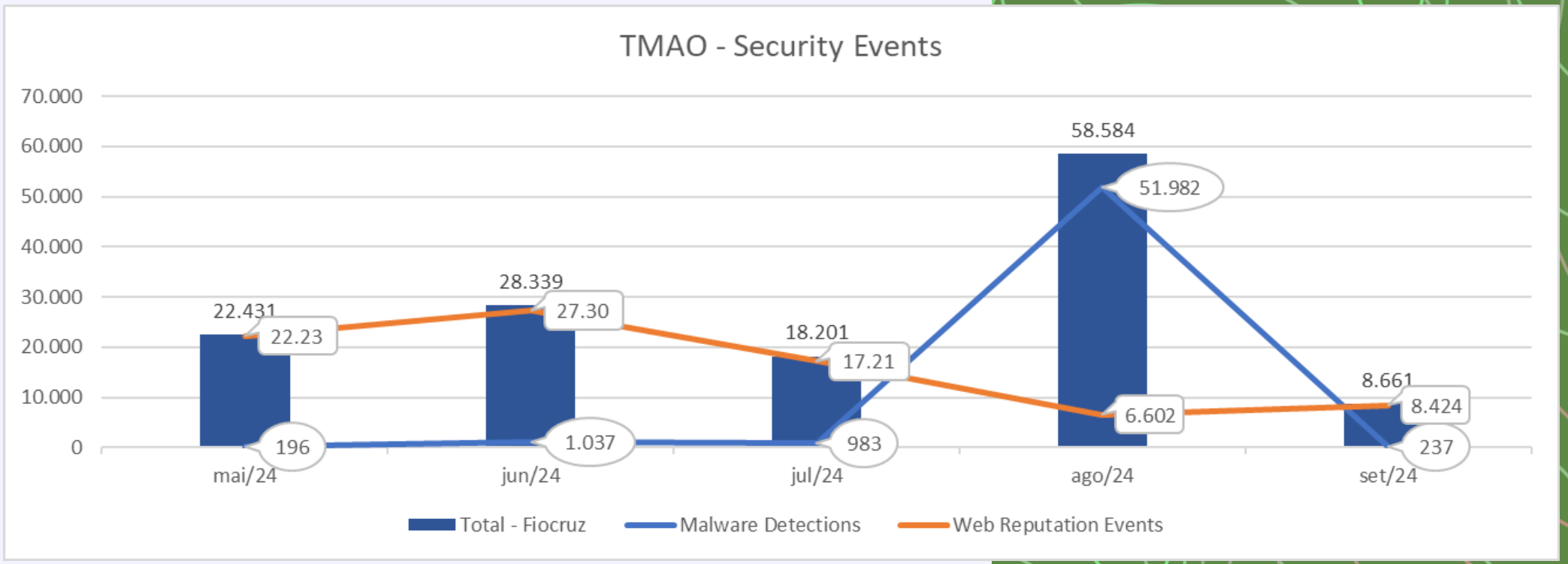
Network Sec [FNT]

#	Ameaça VISITANTE	jun/24	jul/24	ago/24	set/24
1	FG_MASTER (FG2K2ET920900331)	4.771.162	6.066.894	3.548.370	2.817.428
2	FG_CEARA (FG2K2ET920900292)	93.098	369.894	145.630	225.395
3	FG-Gereb	54.338	83.093	57.389	90.235
4	FG_Parana	78.702	84.763	26.653	47.233
5	FGT_IRR	18.814	19.064	40.340	11991
6	FG_Bahia	342	1.218		
7	FG_Pernambuco				
8	FW-FARMANGUINHOS				
9	FG_ILMD				
10	FG_Rondonia				
11	FG-MS				
12	FG_MASTER (FG2K2ET920900371)				
13	FG_CEARA (FG2K2ET920900327)				
	TOTAL	**5.016.456**	**6.624.926**	**3.818.382**	**3.192.282**

#	Ameaça VISITANTE	jun/24	jul/24	ago/24	set/24
1	SpywareCnC	5.013.399	6.620.221	3.912.134	3.189.419
2	CnC	2.494	4.154	5.504	2.604
3	Shlayer	12	2	9	136
4	InstallationTraffic	86	74	23	47
5	Wajam	26	44	112	37
6	Lnkr	132	10	2	25
7	APTAttack	12	24	17	14
8	Sinkhole	295	396	581	
9	NovaLite.Botnet		1		
	Total	**5.016.456**	**6.624.926**	**3.918.382**	**3.192.282**

cogetic.

Endpoint Sec [TMAO]



cogetic.

Endpoint Sec [TMAO]

1. Reiniciar todos os computadores pelo menos uma vez por semana.
2. Observar orientações de segurança.
3. Estabelecer rotina com agentes:

- Monitorar status do agente pela console
- Update Now
- Remover e reinstalar
- Garantir que GPO está aplicando script

CADÊNCIA COM AS UNIDADES

UNIDADES	DETECÇÕES	AGENTES	PROPORÇÃO
IGM	733	200	3,67%
COGETIC	3.694	1.620	2,28%
INI	1.993	877	2,27%
Fiocruz-CE	108	161	0,67%
CDTS	16	28	0,57%
Fiocruz-MS	6	11	0,55%
IGM-Cidacs	37	69	0,54%
EPSJV	158	357	0,44%
Canal Saúde	14	34	0,41%
IFF	162	418	0,39%
SaaS	***655***	***1.782***	***0,37%***
ICICT	102	325	0,31%
ICTB	58	191	0,30%
ENSP	170	606	0,28%
Bio-Manguinhos	487	1.816	0,27%
ILMD	14	55	0,25%
COC	66	293	0,23%
INCQS	16	77	0,21%
Gereb	53	259	0,20%
IRR	65	365	0,18%
FAR	22	131	0,17%
IAM	45	353	0,13%
Fiocruz-RO	8	68	0,12%
ICC	5	163	0,03%
Central Analítica	NA	57	0,00%
TOTAL	**8.687**	**10.316**	**0,84%**

cogetic.

Endpoint Sec [TMWS]

Threat Type	jun-24	jul-24	ago-24	set-24
Total	2.934.192	4.416.632	3.243.798	4.456.102



cogetic.

Endpoint Sec [TMWS]

25 Most Common Firewall Events Not Based on a Rule (Prevent Mode)

# of Packets	Rule
2,419 (64.1%)	Out Of Allowed Policy
663 (17.6%)	TCP SYN with Data
650 (17.2%)	Packet on Closed Connection
22 (0.6%)	Invalid Flags
18 (0.5%)	Dropped Retransmit

Top 25 Computers Ranked by Number of Firewall Events (Prevent Mode

# of Packets	Computer
774,839 (86.4%)	157.86.110.152 (157.86.110.152) Policy: Linux
120,090 (13.4%)	onlinecollectorfiocruzrj (157.86.218.60) Policy: Linux
759 (0.1%)	coc-linceu (157.86.56.45) Policy: Linux
594 (0.1%)	siga (157.86.152.36) Policy: Windows
10 (0%)	Eleicoes-WS_LB-02 (157.86.218.21) Policy: Linux (SS)
5 (0%)	Eleicoes-DB-01 (157.86.218.12) Policy: Linux (SS)
5 (0%)	Eleicoes-DB-02 (157.86.218.17) Policy: Linux (SS)

cogetic.

Endpoint Sec [TMWS]

1. SYN with Data: Recebido pacote com sinalizador SYN, mas contendo dados.
2. Packet on Closed Connection: Recebido pacote pertencente a uma conexão que já estava fechada.
3. Invalid Flags: Recebido pacote com sinalizador(es) inválido(s).
4. Dropped Retransmit: Recebido transmissão TCP cujo conteúdo é diferente do que foi enviado inicialmente.

25 Most Common Firewall Events Not Based on a Rule (Prevent Mode)	
# of Packets	Rule
2.419 (64,1%)	Out Of Allowed Policy
663 (17,6%)	*TCP SYN with Data*
650 (17,2%)	*Packet on Closed Connection*
22 (0,6%)	*Invalid Flags*
18 (0,5%)	*Dropped Retransmit*

cogetic.



Highlights – Pontos de Destaque

1. TM: Avançando com Cadências Técnicas (Cogetic, ICICT, IAM, ICC e IGM).
2. TM: Avanços com a inteligência do Vision One.
3. BioM: Palestra de Phishing

cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO



Pontos de Melhorias e Encaminhamentos

1. TM: Ampliação do DDI (NDR)
2. SC: Melhorias de infraestrutura e organização

cogetic.
COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

Obrigado

Comentários e Dúvidas

cogetic.

COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

As pessoas costumam dizer que a motivação não dura sempre. Bem, nem o efeito do banho, por isso recomenda-se diariamente.

Zig Ziglar

cogetic.

COORDENAÇÃO-GERAL DE GESTÃO DE TECNOLOGIA DE INFORMAÇÃO

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz