



# CERT-MZ

## **Pesquisa sobre o Ciber Ataque aos Domínios gov.mz de fevereiro 2022**

**(“Mass defacement gov.mz”)**

26 fevereiro 2022

**Andre Tenreiro**

[andre@cert.mz](mailto:andre@cert.mz)

PGP: 41A21D52

[www.cert.mz](http://www.cert.mz)

# Introdução

Recentemente no dia 21 fevereiro 2022, foram partilhadas imagens nas redes sociais onde mostravam cerca de 30 sites do governo de Moçambique invadidos por atacantes reivindicando ser do **Yemeni Cyber Army** ou Y.C.A.

As listas de sites invadidos incluem os seguintes domínios do governo:

URL
<a href="https://crepcd.gov.mz">https://crepcd.gov.mz</a>
<a href="https://www.adnap.gov.mz">https://www.adnap.gov.mz</a>
<a href="https://www.ane.gov.mz">https://www.ane.gov.mz</a>
<a href="https://www.ara-sul.gov.mz">https://www.ara-sul.gov.mz</a>
<a href="https://assembleia-provincial.inhambane.gov.mz">https://assembleia-provincial.inhambane.gov.mz</a>
<a href="https://www.bip.gov.mz/index.html">https://www.bip.gov.mz/index.html</a>
<a href="https://crepcd.gov.mz">https://crepcd.gov.mz</a>
<a href="https://crepg.gov.mz">https://crepg.gov.mz</a>
<a href="https://crepi.gov.mz">https://crepi.gov.mz</a>
<a href="https://crepm.gov.mz/index.html">https://crepm.gov.mz/index.html</a>
<a href="https://www.crepm.gov.mz">https://www.crepm.gov.mz</a>
<a href="https://crepman.gov.mz">https://crepman.gov.mz</a>
<a href="http://crept.gov.mz">http://crept.gov.mz</a>
<a href="https://crepz.gov.mz">https://crepz.gov.mz</a>
<a href="https://crescendoazul.museusdomar.gov.mz">https://crescendoazul.museusdomar.gov.mz</a>
<a href="https://csirt.gov.mz">https://csirt.gov.mz</a>
<a href="https://csmj.gov.mz">https://csmj.gov.mz</a>
<a href="https://csrecm.gov.mz">https://csrecm.gov.mz</a>
<a href="https://gabinfo.gov.mz">https://gabinfo.gov.mz</a>
<a href="https://ics.gov.mz">https://ics.gov.mz</a>
<a href="https://inatter.gov.mz">https://inatter.gov.mz</a>
<a href="https://www.infosaude.gov.mz">https://www.infosaude.gov.mz</a>
<a href="https://www.ingd.gov.mz">https://www.ingd.gov.mz</a>
<a href="https://maefp.gov.mz">https://maefp.gov.mz</a>
<a href="https://mdn.gov.mz">https://mdn.gov.mz</a>
<a href="https://www.micultur.gov.mz">https://www.micultur.gov.mz</a>
<a href="https://www.mophrh.gov.mz">https://www.mophrh.gov.mz</a>
<a href="https://mta.gov.mz">https://mta.gov.mz</a>
<a href="https://www.senami.gov.mz">https://www.senami.gov.mz</a>

A página principal dos websites, foi alterada para mostrar a seguinte imagem:



Figura 1 A página inicial dos sites foi alterada por esta imagem.

# Analise do Ataque

## Yemeni Cyber Army (Y.C.A)

O grupo Y.C.A reivindica ser um grupo de *hacktivistas* baseados no Iémen que esteve recentemente nos últimos meses envolvido em vários ataques a países como Emirados Árabes Unidos (E.A.U), França, Estados Unidos da América (E.U.A) e Israel. Inclusive, recentemente partilhou centras de informação confidencial tais como passaportes relacionados com oficiais do governo do E.A.U.

O grupo mantém um grupo publico do **Telegram**, onde nele partilha alguns dos ataques que vai fazendo recentemente.

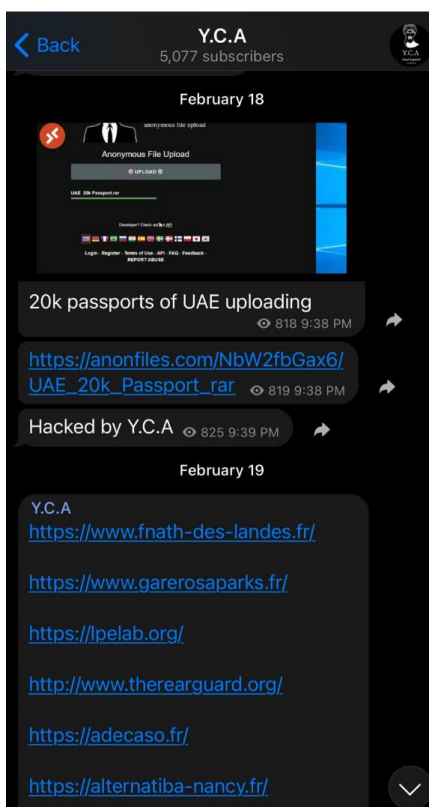
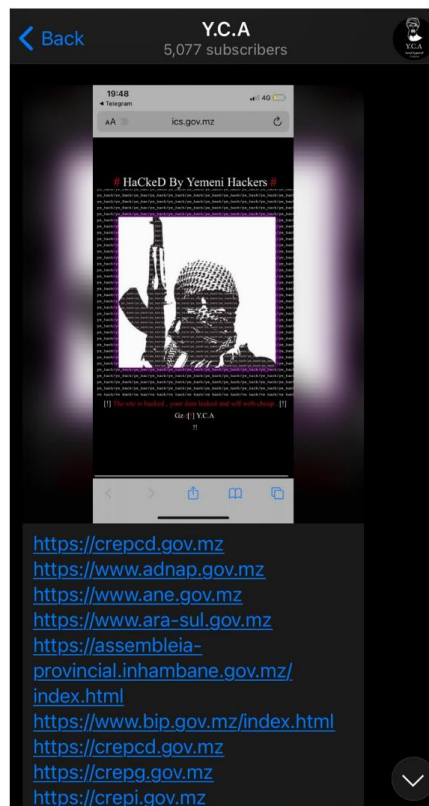


Figura 2 Grupo oficial e publico do Y.C.A no Telegram

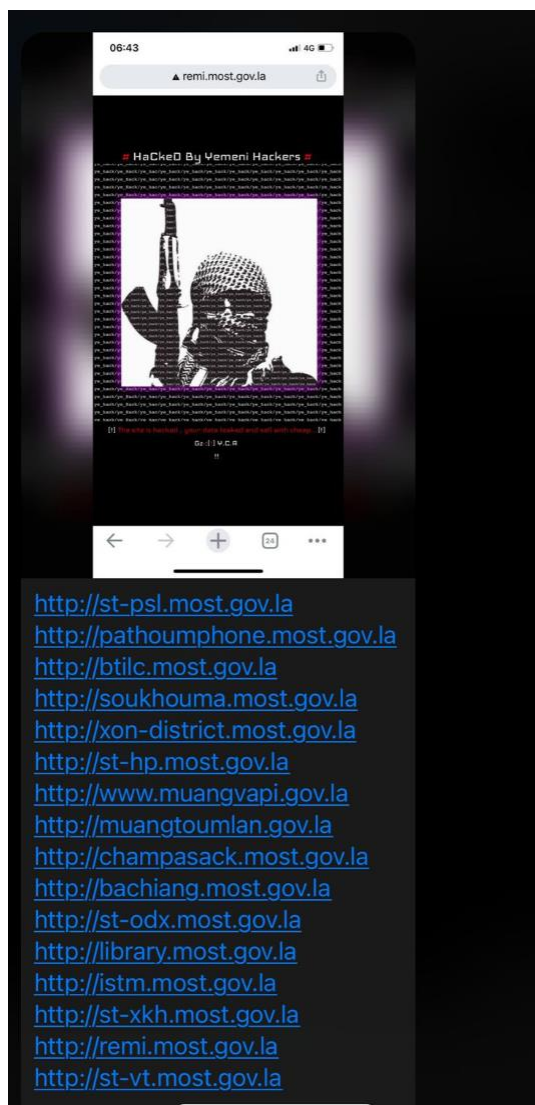
Não há nenhuma certeza de que este grupo seja o mesmo que o *Yemen Cyber Army* (Y.C.A) que reivindicou alguns ataques ao ministério dos negócios estrangeiros da Arabia Saudita em 2015, e vazou os seus dados no WikiLeaks. No mundo do *Hacktivismo*, por vezes há grupos que fazem invasões em nome de outros de forma a confundir a origem e atribuição dos ataques. Caso o grupo seja o mesmo, também há suspeitas que os mesmos sejam [Iranianos](#) e não do Iémen.

O ataque ao gov.mz foi inicialmente publicado pelo Y.C.A no dia 20/02/2022 as 22h11 de Maputo.



*Figura 3* Publicação do ataque ao gov.mz no canal do Telegram

Num novo *post* do dia 26/02/2022 às 8h44 (Maputo / UTC+2), denotamos um *screenshot* a reivindicar um novo ataque contra sites governamentais da República Democrática Popular do Laos (domínio .la)



*Figura 4* Novo "mass defacement" ao Governo de Laos.

Algo a destacar, foi que o *screenshot* demonstra a hora de **06h43**. Pode-se questionar se o mesmo foi publicado um minuto depois de ter sido tirado. Se sim, a hora no telemóvel corresponde a um país que esteja a menos 2 horas que Moçambique (UTC+0).

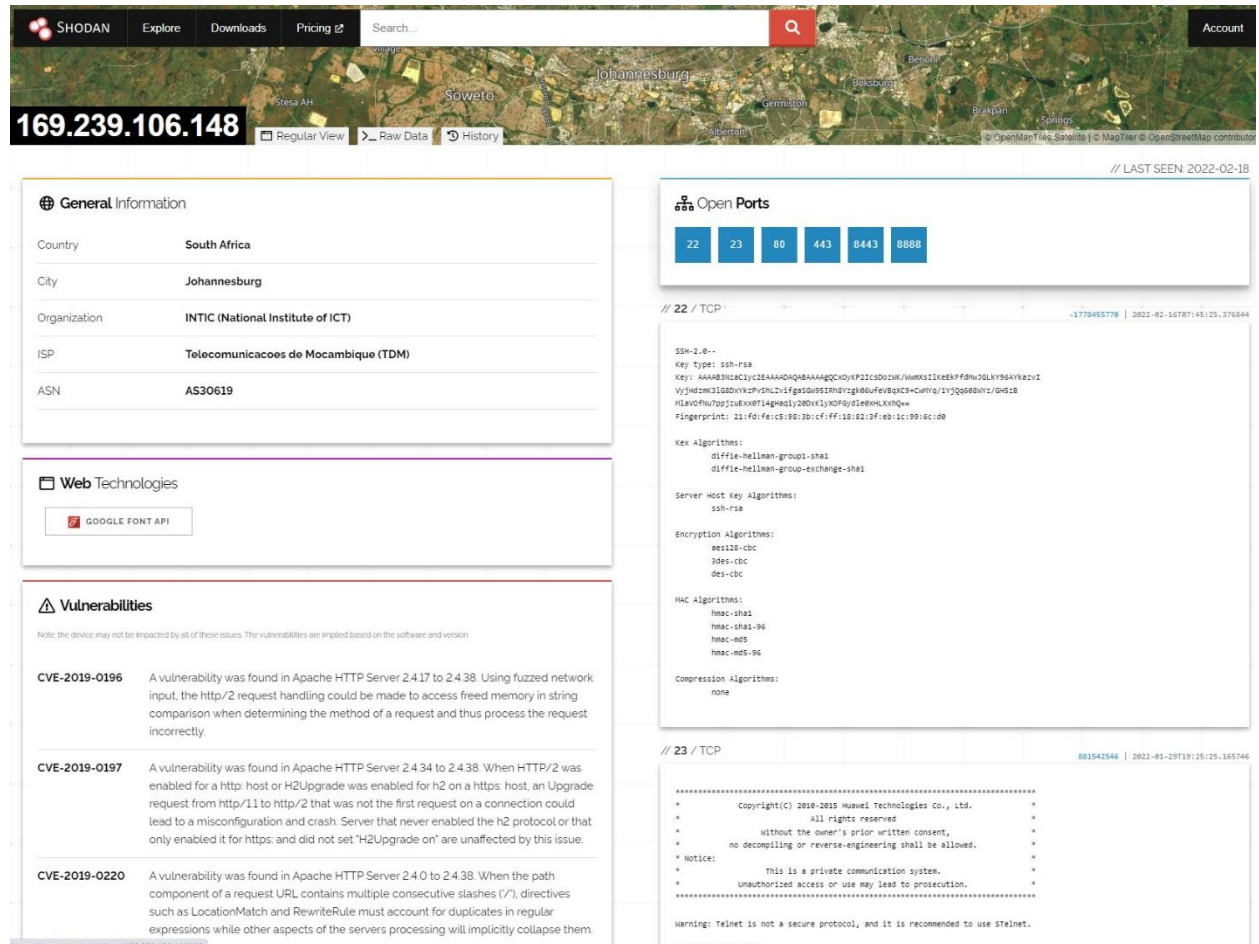
Algo também interessante, foi o facto de o *screenshot* do telemóvel demonstrar o ícone de 4G. Numa pesquisa no Google, consegue-se perceber que o 4G ainda não está massificado no Iémen segundo a publicação do [Yemen News Agency](#) (SABA) e pelo mapa de [cobertura 4G](#) da capital.

Esta informação por si não é suficiente para poder afirmar a **atribuição do ataque**.

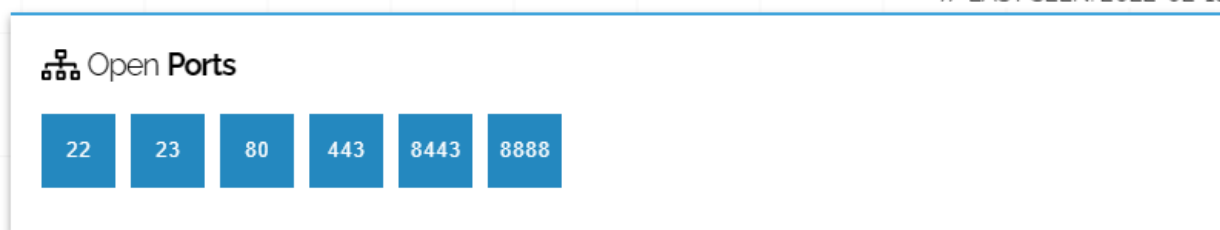
## Servidor afetado

Fazendo uma análise a todos os domínios afetados, tudo indica que o ataque foi a uma infraestrutura de alojamento partilhado (*shared hosting*) que utiliza o endereço de IP 169[.]239[.]106[.]148

Apenas utilizando fontes publicas de informação, vulgo ***opensource Intelligence*** (OSINT), utilizamos o site de pesquisa [Shodan](#) para visualizar informação do endereço IP, tais como portos abertos.

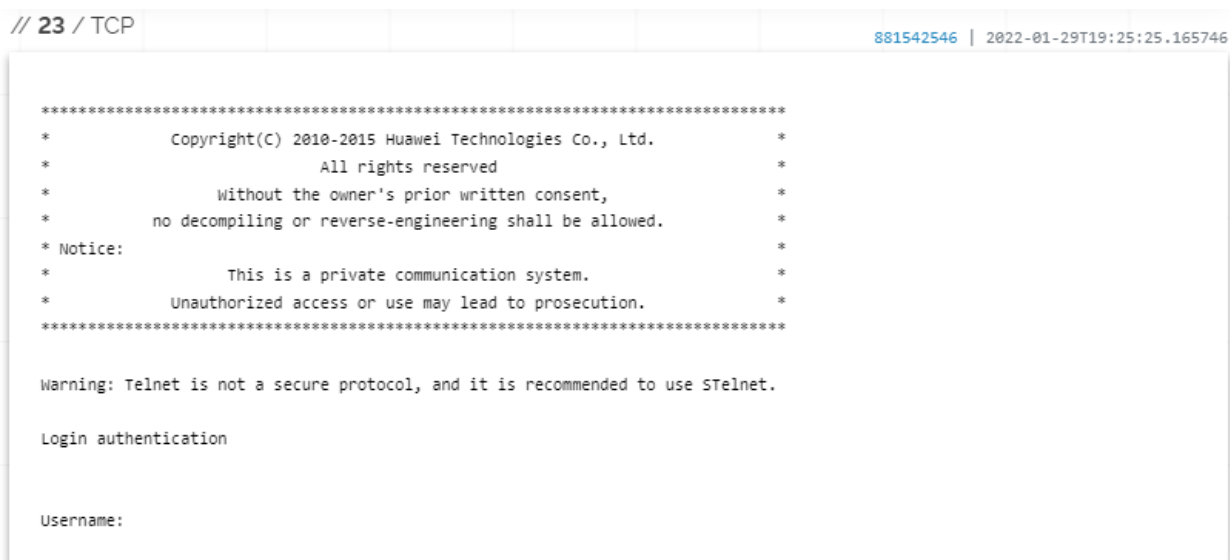


**Figura 5** Informação pública do IP comprometido.



*Figura 6 Portos abertos do servidor*

Pode-se destacar, que alguns desses portos não deveriam estar abertos ao mundo, tais como o **Telnet**.



*Figura 7 Porto telnet (23) aberto, aparentemente um equipamento de rede Huawei.*

Pudemos também destacar, que o servidor possui algumas vulnerabilidades identificadas pelo Shodan, entre com a seguinte severidade:

- Crítico: 1
- Alto: 6
- Médio: 7

As vulnerabilidades identificadas, foram reportadas publicamente entre 2017-2019 e podem ser encontradas na base de dados do [NIST](#).



## Vulnerabilidades identificadas pelo Shodan

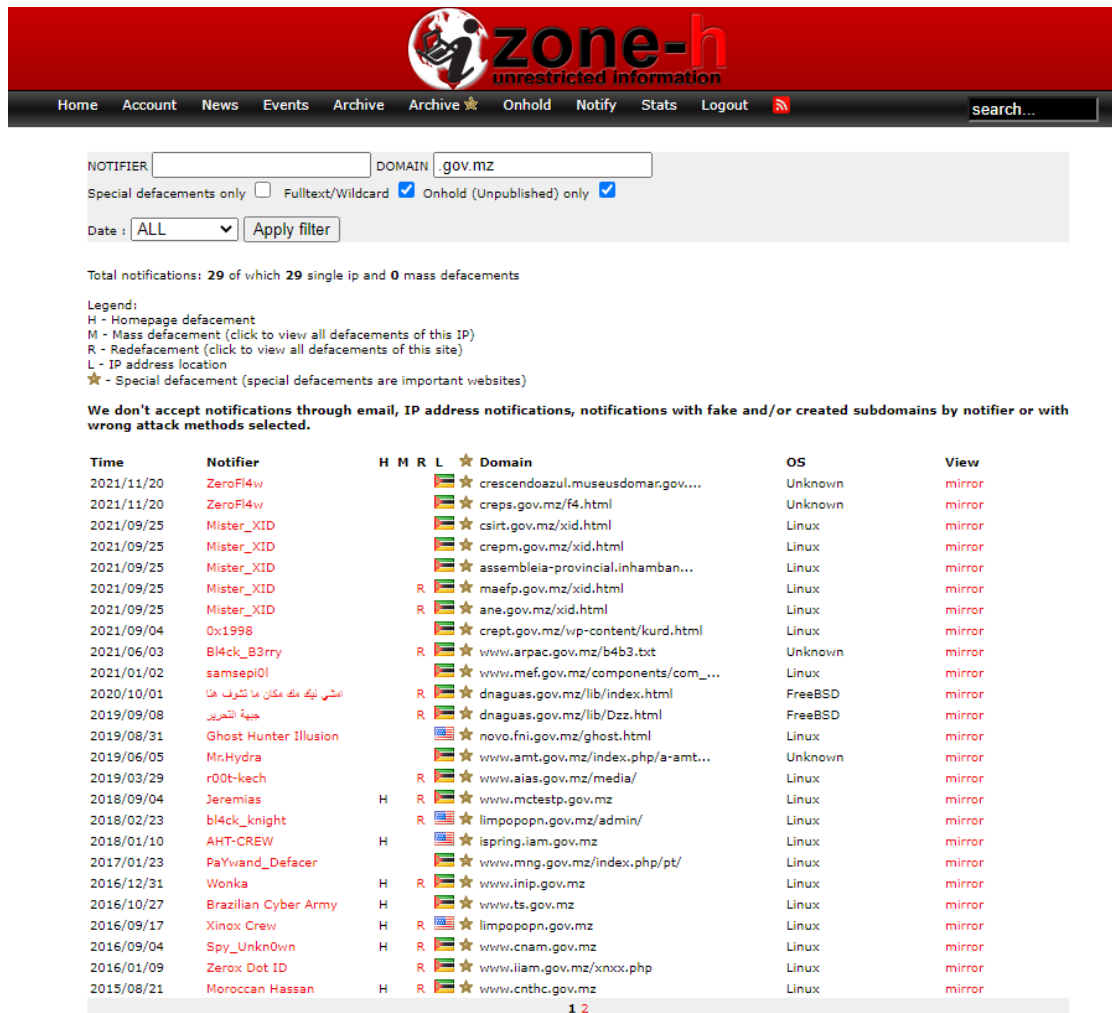
As vulnerabilidades identificadas pelo Shodan são relacionadas com o web server(s) disponível no servidor, que tudo indica parece ser apache v2.4.29 que foi lançada em 2017.

CVE	Impacto	Descrição (Inglês)	Ano publicação
CVE-2018-1312	<b>Crítico</b>	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.	2018
CVE-2019-0211	Alto	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the priv	2019
CVE-2017-15710	Alto	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.	2017
CVE-2018-1303	Alto	A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache	2018
CVE-2017-15715	Alto	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '\$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are externally blocked, but only by matching the trailing portion of the filename.	2017
CVE-2018-1333	Alto	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).	2018
CVE-2018-17199	Alto	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.	2018
CVE-2018-1301	Médio	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.	2018
CVE-2019-0196	Médio	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed	2019

		memory in string comparison when determining the method of a request and thus process the request incorrectly.	
CVE-2019-0197	Médio	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.	2019
CVE-2019-0220	Médio	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.	2019
CVE-2018-1283	Médio	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.	2018
CVE-2018-1302	Medio	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.	2018
CVE-2018-11763	Medio	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.	2018

## Analise histórica do IP

Fazendo uma análise histórica do **IP comprometido** na base de dados de *defacements* [Zone-h](#), poderemos constatar que não é a primeira vez que o mesmo foi comprometido. Existiram **múltiplas invasões** do tipo “defacement” que ocorreram nos últimos meses.



zone-h  
unrestricted information

Home Account News Events Archive Archive ★ Onhold Notify Stats Logout search...

NOTIFIER  DOMAIN

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☒

Date:  Apply filter

Total notifications: 29 of which 29 single ip and 0 mass defacements

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
L - IP address location  
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	★ Domain	OS	View
2021/11/20	ZeroFI4w					★ crescendozul.museusdomar.gov...	Unknown	mirror
2021/11/20	ZeroFI4w					★ creps.gov.mz/f4.html	Unknown	mirror
2021/09/25	Mister_XID					★ csirt.gov.mz/xid.html	Linux	mirror
2021/09/25	Mister_XID					★ crepm.gov.mz/xid.html	Linux	mirror
2021/09/25	Mister_XID					★ assembleia-provincial.inhamban...	Linux	mirror
2021/09/25	Mister_XID					★ maefp.gov.mz/xid.html	Linux	mirror
2021/09/25	Mister_XID					★ ane.gov.mz/xid.html	Linux	mirror
2021/09/04	0x1998					★ crept.gov.mz/wp-content/kurd.html	Linux	mirror
2021/06/03	bl4ck_B3rry					★ www.arpac.gov.mz/b4b3.txt	Unknown	mirror
2021/01/02	samsepi0l					★ www.mef.gov.mz/components/com_...	Linux	mirror
2020/10/01	امشي نيك ملك مكان ما تشوف هنا					★ dnaguas.gov.mz/lib/index.html	FreeBSD	mirror
2019/09/08	جبهة التحرير					★ dnaguas.gov.mz/lib/Dzz.html	FreeBSD	mirror
2019/08/31	Ghost Hunter Illusion					★ novo.fni.gov.mz/ghost.html	Linux	mirror
2019/06/05	MrHydra					★ www.amt.gov.mz/index.php/a-amt...	Unknown	mirror
2019/03/29	r00t-kech					★ www.aias.gov.mz/media/	Linux	mirror
2018/09/04	Jeremias	H				★ www.mctestp.gov.mz	Linux	mirror
2018/02/23	bl4ck_knight					★ limpopopn.gov.mz/admin/	Linux	mirror
2018/01/10	AHT-CREW	H				★ ispring.iam.gov.mz	Linux	mirror
2017/01/23	PaYvand_Defacer					★ www.mng.gov.mz/index.php/pt/	Linux	mirror
2016/12/31	Wonka	H				★ www.inip.gov.mz	Linux	mirror
2016/10/27	Brazilian Cyber Army	H				★ www.ts.gov.mz	Linux	mirror
2016/09/17	Xinox Crew	H				★ limpopopn.gov.mz	Linux	mirror
2016/09/04	Spy_Unkn0wn	H				★ www.cnam.gov.mz	Linux	mirror
2016/01/09	Zer0x Dot ID	R				★ www.iliam.gov.mz/xnxx.php	Linux	mirror
2015/08/21	Moroccan Hassan	H				★ www.cnthc.gov.mz	Linux	mirror

1 2

Figura 8 Alguns dos defacements de sites gov.mz disponiveis no Zone-h.

Passaremos a destacar ataques prévios ao IP 169[.]239[.]106[.]148

Data	URLs	Grupo
20/11/2021	http://crepg.gov.mz http://crescendoazul.museusdomar.gov.mz ...	ZeroFI4w
14/11/2021	https://infosaude.gov.mz https://csrecm.gov.mz https://crepn.gov.mz https://crepman.gov.mz https://www.mozambiqueexpo2020.gov.mz ...	KrdSec
25/09/2021	http://csirt.gov.mz http://senami.gov.mz http://seje.gov.mz http://portalcidadao.gov.mz http://crepm.gov.mz http://assembleia-provincial.inhambane.gov.mz http://maefp.gov.mz http://ane.gov.mz ...	Mister_XID
21/09/2021	https://www.micultur.gov.mz	KrdSec
04/09/2021	https://crept.gov.mz	KrdSec

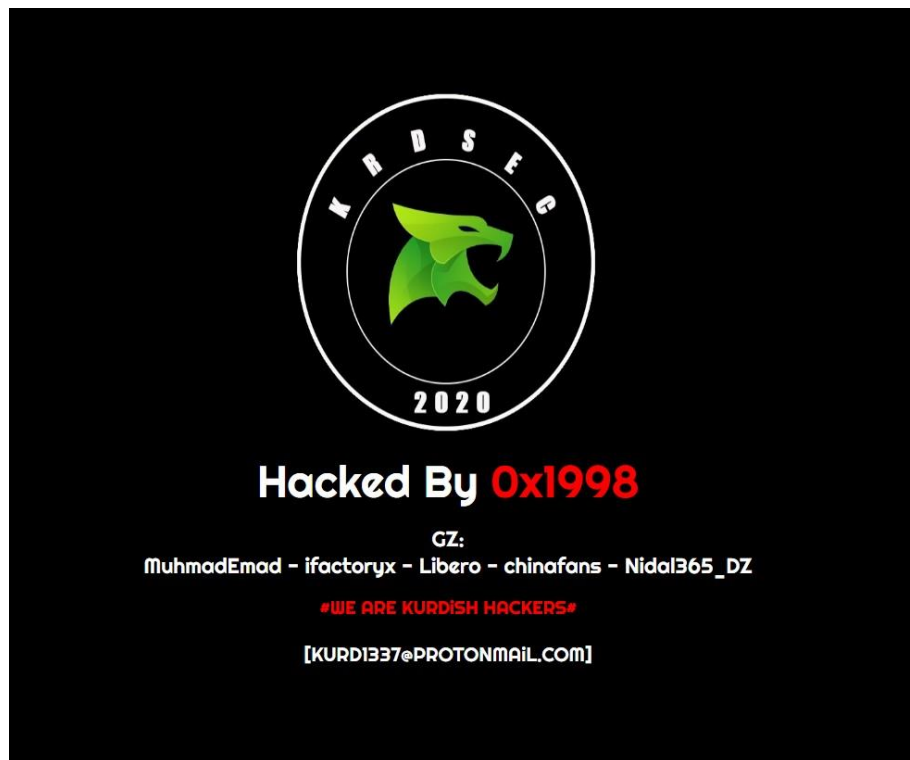


Figura 9 Defacement ao site www.micultur.gov.mz no dia 21 setembro 2021

## Nova Intrusão

Num novo ataque, vários sites do governo voltaram a estar indisponíveis.

Na nota deixada os atacantes dizem que infiltraram cerca de 34 ministérios do governo de Moçambique e pedem cerca de 20 mil dólares (crê-se americanos) para não publicar dados oficiais do governo.



Figura 10 Defacement do INATTER.GOV.MZ com pedido de extorsão.

Analisando o endereço Bitcoin “3FeFeloLRiGhXmvwW6UYowWEt8PZjCab8W” deixado pelos *hackers*, não foi possível detetar nenhuma transação no momento de elaboração desta pesquisa.

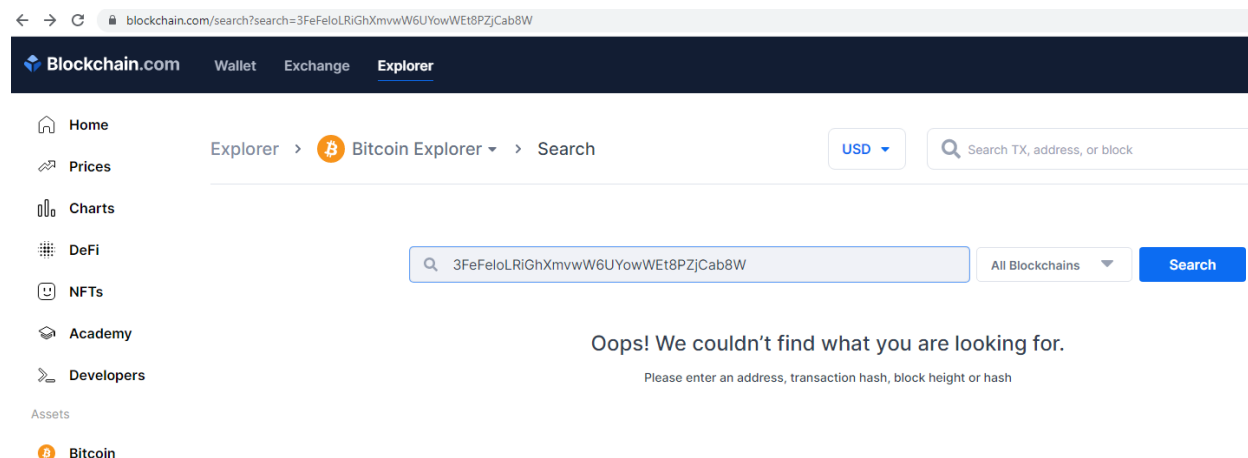


Figura 11 O endereço Bitcoin não dispõe de nenhum movimento até ao momento.

É de salientar, que pedidos de extorsão por Bitcoin começam a ser pouco comuns devido à falta de privacidade por detrás do sistema Bitcoin. Em vez disso, a cripto moeda **Monero** tem sido mais utilizado por criminosos sofisticados, como gangs de *Ransomware*.

## Data Leak

No canal **Telegram** do Y.C.A, no dia 23/02/2022 às 21h15 de Maputo, os mesmos publicaram um *screenshot* que parece ser um *dump* da base de dados de um *Content Management System* (CMS) ligado ao ataque. Contudo, isto não pode ser validado.



The screenshot displays a database interface with a list of tables on the left and a table view for 'ptwoc\_users' on the right. The 'ptwoc\_users' table contains columns for '#', 'id', 'name', 'username', and 'email'. Several rows of data are visible, with the 'name' and 'email' columns redacted with white boxes. The 'username' column contains various email addresses. The 'id' column shows values like 874, 877, 881, 878, 879, 880, 882, 883, 884, 885, 886, 887, 888, and 889. The 'name' column contains various names, some of which are redacted. The 'email' column contains various email addresses, some of which are redacted. The 'username' column contains various email addresses, some of which are redacted. The 'id' column shows values like 874, 877, 881, 878, 879, 880, 882, 883, 884, 885, 886, 887, 888, and 889. The 'name' column contains various names, some of which are redacted. The 'email' column contains various email addresses, some of which are redacted. The 'username' column contains various email addresses, some of which are redacted.

#	id	name	username	email
Edit 874				@gmail.com
Edit 877				mail.com
Edit 881				mdn.gov.mz
Edit 878				dn.gov.mz
Edit 879				mdn.gov.mz
Edit 880				65@gmail.com
Edit 882				ud.com
Edit 883				o3@gmail.com
Edit 884				mach.co.mz
Edit 885				ho@inage.gov.mz
Edit 886				camp.com
Edit 887				gmail.com
Edit 888				mpt.com
Edit 889				77a99...n

Query:

```
SELECT * FROM 'ptwoc_users' LIMIT 0,30
```

Figura 12 Database dump de utilizadores (informação sensível ocultada)

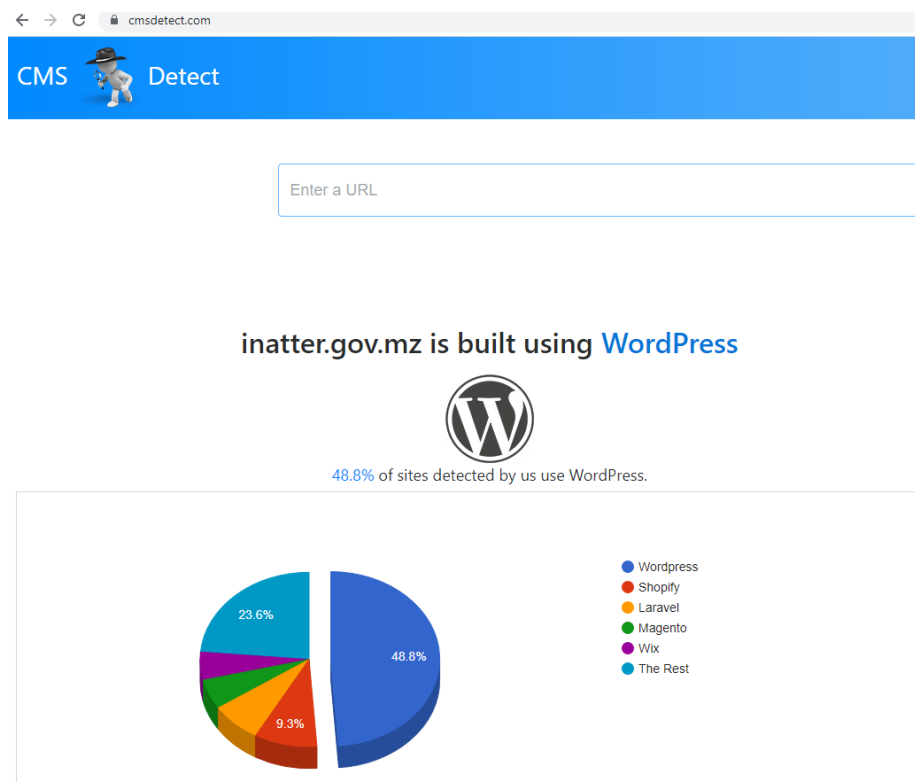
No *dump* da base de dados, é possível visualizar uma tabela “ptwoc\_users\*” contendo a seguinte informação:

- Nome
- Username
- Email
- Password (hashed)

Utilizando *fingerprinting* dos nomes das tabelas, esta base de dados parece corresponder ao **Joomla!** Contudo não é possível validar devido a falta de mais informação.

## Analise do CMS

Uma breve análise de *fingerprint* utilizando o [CMS detect](https://cmsdetect.com), permite identificar que sites os invadidos estão assentes na plataforma **WordPress**. Infelizmente, não é possível correlacionar o *dump* em cima mencionado com a plataforma de Wordpress ou Joomla!

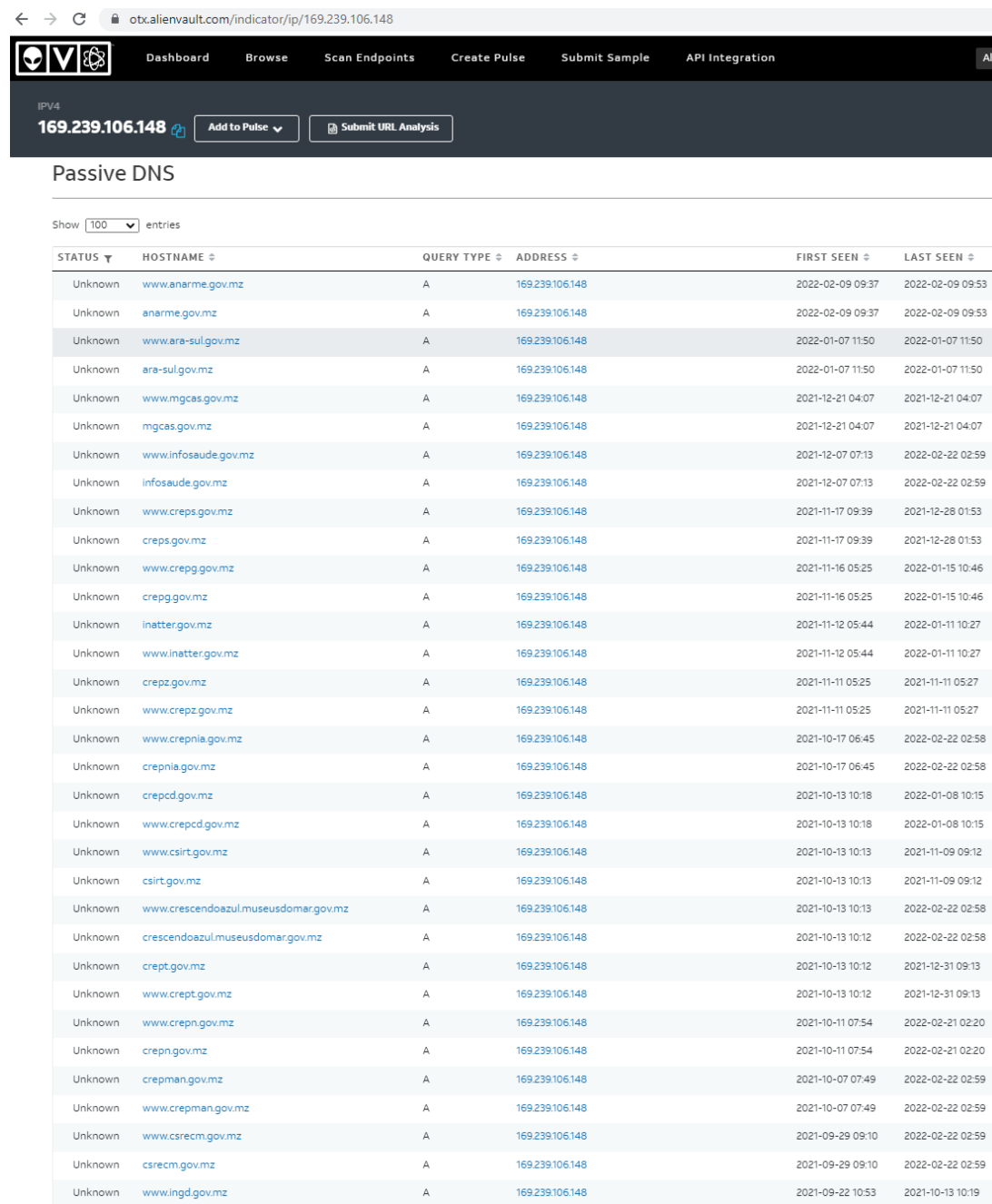


**Figura 13** Analise fingerprinting ao site do INATTER, mostra estar assente na plataforma Wordpress.

## Passive DNS

Fazendo uma análise de **Passive DNS** utilizando o [AlienVault OTX](#), foi possível obter cerca de **74** **entradas DNS** que resolvem o endereço de IP 169[.]239[.]106[.]148

**⚠ Atenção!** De forma alguma se pode deduzir com isto, que todos estes domínios foram comprometidos.



STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN
Unknown	www.anarme.gov.mz	A	169.239.106.148	2022-02-09 09:37	2022-02-09 09:53
Unknown	anarme.gov.mz	A	169.239.106.148	2022-02-09 09:37	2022-02-09 09:53
Unknown	www.ara-sul.gov.mz	A	169.239.106.148	2022-01-07 11:50	2022-01-07 11:50
Unknown	ara-sul.gov.mz	A	169.239.106.148	2022-01-07 11:50	2022-01-07 11:50
Unknown	www.mgcas.gov.mz	A	169.239.106.148	2021-12-21 04:07	2021-12-21 04:07
Unknown	mgcas.gov.mz	A	169.239.106.148	2021-12-21 04:07	2021-12-21 04:07
Unknown	www.infosaude.gov.mz	A	169.239.106.148	2021-12-07 07:13	2022-02-22 02:59
Unknown	infosau.de.gov.mz	A	169.239.106.148	2021-12-07 07:13	2022-02-22 02:59
Unknown	www.creps.gov.mz	A	169.239.106.148	2021-11-17 09:39	2021-12-28 01:53
Unknown	creps.gov.mz	A	169.239.106.148	2021-11-17 09:39	2021-12-28 01:53
Unknown	www.crepg.gov.mz	A	169.239.106.148	2021-11-16 05:25	2022-01-15 10:46
Unknown	crepg.gov.mz	A	169.239.106.148	2021-11-16 05:25	2022-01-15 10:46
Unknown	inatter.gov.mz	A	169.239.106.148	2021-11-12 05:44	2022-01-11 10:27
Unknown	www.inatter.gov.mz	A	169.239.106.148	2021-11-12 05:44	2022-01-11 10:27
Unknown	crepz.gov.mz	A	169.239.106.148	2021-11-11 05:25	2021-11-11 05:27
Unknown	www.crepz.gov.mz	A	169.239.106.148	2021-11-11 05:25	2021-11-11 05:27
Unknown	www.crepnia.gov.mz	A	169.239.106.148	2021-10-17 06:45	2022-02-22 02:58
Unknown	crepnia.gov.mz	A	169.239.106.148	2021-10-17 06:45	2022-02-22 02:58
Unknown	crepcd.gov.mz	A	169.239.106.148	2021-10-13 10:18	2022-01-08 10:15
Unknown	www.crepcd.gov.mz	A	169.239.106.148	2021-10-13 10:18	2022-01-08 10:15
Unknown	www.csirt.gov.mz	A	169.239.106.148	2021-10-13 10:13	2021-11-09 09:12
Unknown	csirt.gov.mz	A	169.239.106.148	2021-10-13 10:13	2021-11-09 09:12
Unknown	www.crescendoazul.museusdomar.gov.mz	A	169.239.106.148	2021-10-13 10:13	2022-02-22 02:58
Unknown	crescendoazul.museusdomar.gov.mz	A	169.239.106.148	2021-10-13 10:12	2022-02-22 02:58
Unknown	crept.gov.mz	A	169.239.106.148	2021-10-13 10:12	2021-12-31 09:13
Unknown	www.crept.gov.mz	A	169.239.106.148	2021-10-13 10:12	2021-12-31 09:13
Unknown	www.crepn.gov.mz	A	169.239.106.148	2021-10-11 07:54	2022-02-21 02:20
Unknown	crepn.gov.mz	A	169.239.106.148	2021-10-11 07:54	2022-02-21 02:20
Unknown	crepman.gov.mz	A	169.239.106.148	2021-10-07 07:49	2022-02-22 02:59
Unknown	www.crepman.gov.mz	A	169.239.106.148	2021-10-07 07:49	2022-02-22 02:59
Unknown	www.csrecm.gov.mz	A	169.239.106.148	2021-09-29 09:10	2022-02-22 02:59
Unknown	csrecm.gov.mz	A	169.239.106.148	2021-09-29 09:10	2022-02-22 02:59
Unknown	www.ingd.gov.mz	A	169.239.106.148	2021-09-22 10:53	2021-10-13 10:19

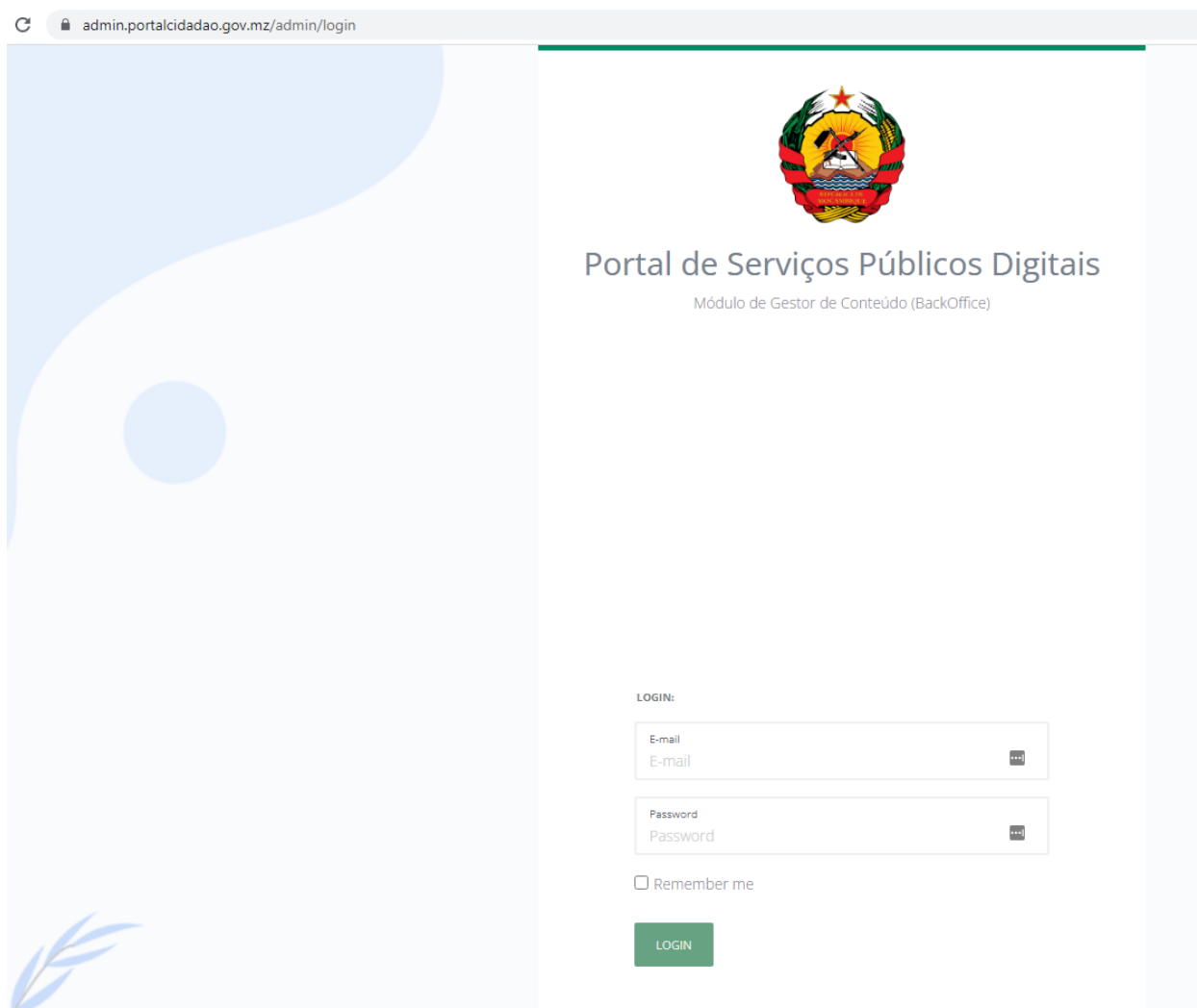
**Figura 14** Alguns domínios/hostnames resolvidos pelo endereço de IP 169[.]239[.]106[.]148




Contudo, há dois sites que merecedores de atenção:

Unknown	<a href="http://portalcidadao.gov.mz">portalcidadao.gov.mz</a>	A	169.239.106.148
Unknown	<a href="http://admin.portalcidadao.gov.mz">admin.portalcidadao.gov.mz</a>	A	169.239.106.148

Acedendo ao último site, parece ser um portal de acesso restrito:



admin.portalcidadao.gov.mz/admin/login



Portal de Serviços Públicos Digitais

Módulo de Gestor de Conteúdo (BackOffice)

LOGIN:

E-mail  
E-mail

Password  
Password

☐ Remember me

LOGIN

**Figura 15** Acesso admin ao Portal do Cidadão

Caso este portal seja de acesso restrito e com informação sensível, o mesmo não deveria ser acedido via internet e o protegido com *2 Factor Authentication* (2FA) sempre que possível. O mesmo portal também permite autenticação em canal não cifrado (porto 80).

# Conclusões e Recomendações

Por razões éticas quiçá legais, apenas foi analisada informação publicamente disponível do IP e do ataque. Não foi feito nenhum teste de intrusão ao endereço de IP em causa.

Não é possível dizer com precisão, o vetor de ataque utilizado pelo Y.C.A para a intrusão. Contudo o método mais comum para casos similares normalmente é explorando uma vulnerabilidade do CMS (ou de algum plugin) ganhando desta forma controlo sobre a infraestrutura de alojamento.

O endereço de IP em causa, dispõe de inúmeras vulnerabilidades de severidade crítica e alta. Pelo que se recomenda o seguinte:

## Recomendações:

1. Deve-se considerar que todos os dados do servidor foram comprometidos. Aconselha-se a reinstalação da máquina do zero, utilizando sistemas operativos e versões de software mais recentes e atualizadas.
2. Caso a máquina tenha um Content Management System (CMS), reinstalar a última versão e rever todos os *plugins*.
3. Instalar uma *Web Application Firewall* (WAF) de forma a mitigar ataques, tais como SQLi, XSS, etc.
4. Recomenda-se o *hardening* da infraestrutura, nomeadamente fechar portos de rede não encriptados como o Telnet.
5. Rever os processos de incidente. Existiram múltiplos incidentes ocorridos nos últimos meses, podendo ou não ter a mesma origem.
6. Mudar todas as passwords, quer de sistema operativo, quer do CMS. As mesmas contam podem estar a ser utilizadas também noutras plataformas.
7. Nunca utilizar emails pessoais (e.g: Gmail) como email oficial do governo.
8. Correr aplicações tipo anti rootkit de modo a detectar algum *trojan* que possa ter sido instalado no SO e/ou no CMS.
9. Não correr nenhum CMS com privilégios elevados.
10. Ter segregação de conteúdos, para no caso de intrusão, outros portais do governo não sejam comprometidos.
11. Não se recomenda o pagamento de extorsões. Não há nenhuma garantia que os invasores cumpram a palavra.
12. Utilizar autenticação por 2 fatores, também chamado de *2 Factor Authentication* / *Multi-Factor Authentication* sempre que possível.