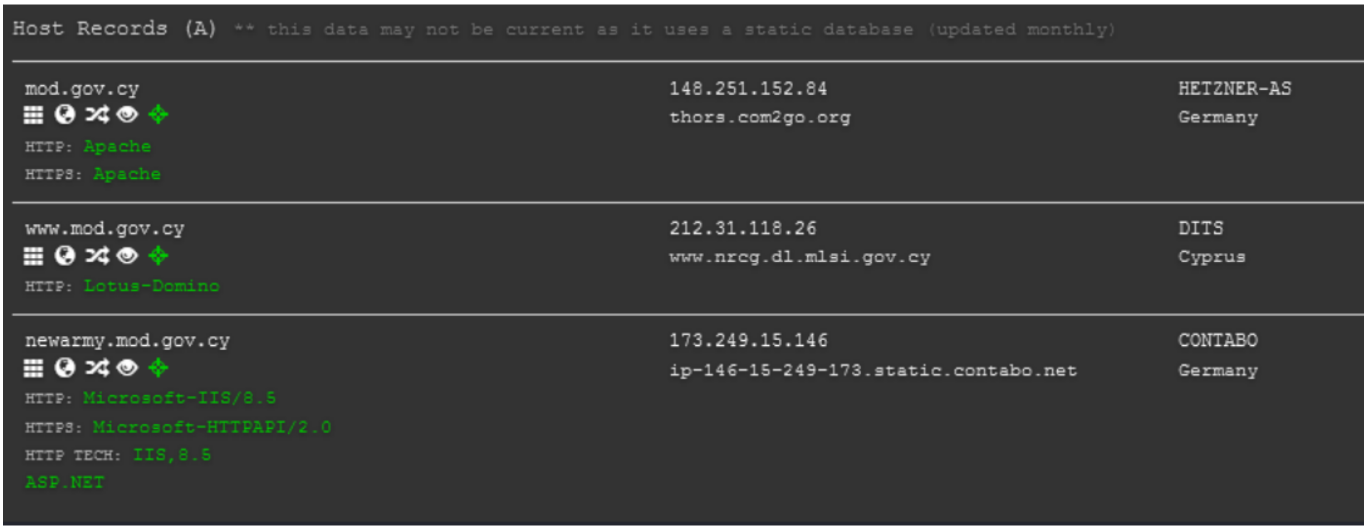
Open source intelligence investigation of Cyprus Ministry of Defense cyber attack

During the past couple of weeks there was a very subtle buzz about a cyber attack against the website of the Ministry of Defense by a well-known Turkish criminal hacking group. The original news article was published by SecNews.gr (https://amp.secnews.gr/331587/rootayyildiz-turkish-defacer-hacker-cyprus/) on the 24th of March 2021 and included a detailed analysis of the attack, along with photographic evidence of a sample of the data that was stolen. On the 29th of March 2021 the website Philenews.com, amongst others, published a 6 line article (https://www.philenews.com/koinonia/eidiseis/article/1157770/prospatheia-epithesis-apo-chaker-stin-istoselida-toy-ypam) mentioning that the attack against the Ministry was successfully blocked, no damage was done and that the Ministry was taking all the necessary measures to prevent similar actions from happening in the future.

Some would argue that Cypriot politicians are prone to sweeping under the rug major incidents caused by incompetence, indifference, negligence, profit, self-promotion and / or self-preservation (the Mari explosion, 2013 haircut on bank deposits, COOP and Laiki bankruptcies etc); hence, we have decided to lift the rug and expose the potential impact of the aforementioned cyber attack.

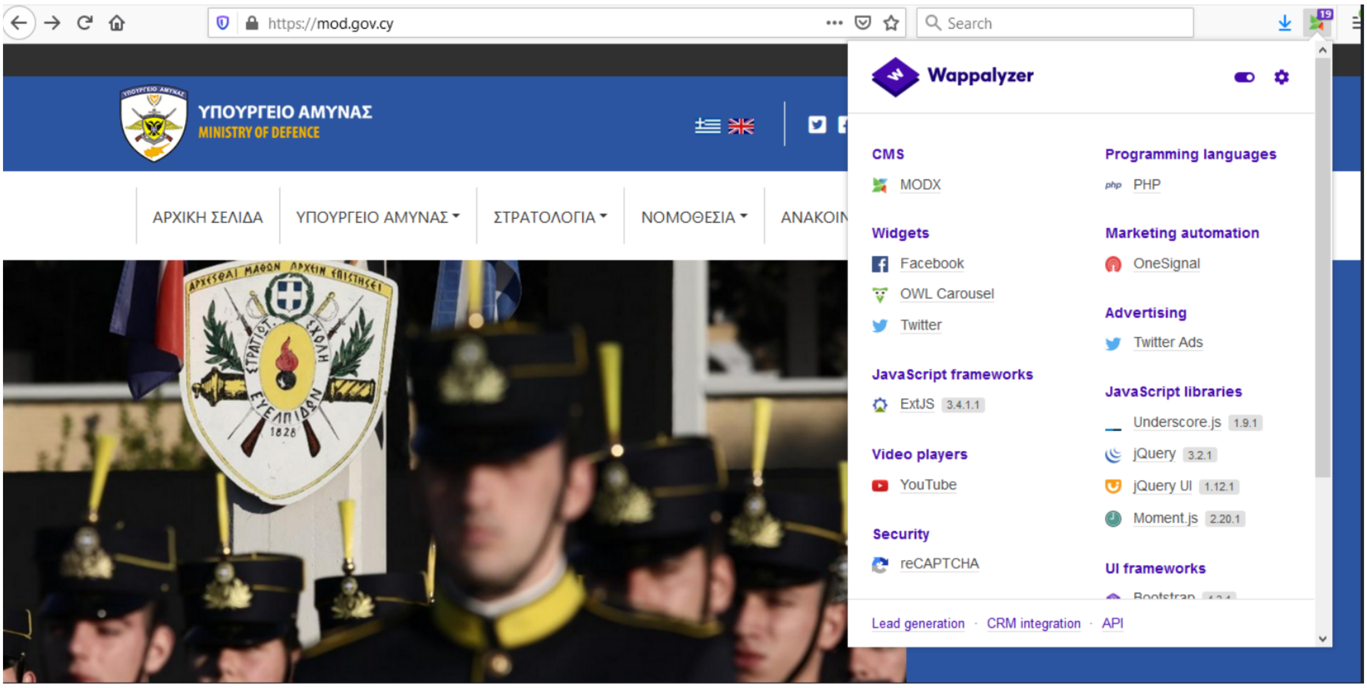
As per the SecNews article the attacker managed to compromise one of the Ministry of Defense websites. But which one? What information can we uncover about the attack through Open Source Intelligence (i.e. information that is available in the public domain)? A simple query on the DNSdumpster.com website can provide useful information about the public websites of the Ministry.



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

mod.gov.cy HTTP: Apache HTTPS: Apache	148.251.152.84 thors.com2go.org	HETZNER-AS Germany
www.mod.gov.cy HTTP: Lotus-Domino	212.31.118.26 www.nrcg.dl.mlsi.gov.cy	DITS Cyprus
newarmy.mod.gov.cy HTTP: Microsoft-IIS/8.5 HTTPS: Microsoft-HTTPAPI/2.0 HTTP TECH: IIS,8.5 ASP.NET	173.249.15.146 ip-146-15-249-173.static.contabo.net	CONTABO Germany

As per the image above we can try and visit the mod.gov.cy website to check if we can find any indicators of a compromise (IoC) or information that could lead to the conclusion that the site was compromised.



CMS
- MODX

Widgets
- Facebook
- OWL Carousel
- Twitter

JavaScript frameworks
- ExtJS 3.4.1.1

Video players
- YouTube

Security
- reCAPTCHA

Programming languages
- PHP

Marketing automation
- OneSignal

Advertising
- Twitter Ads

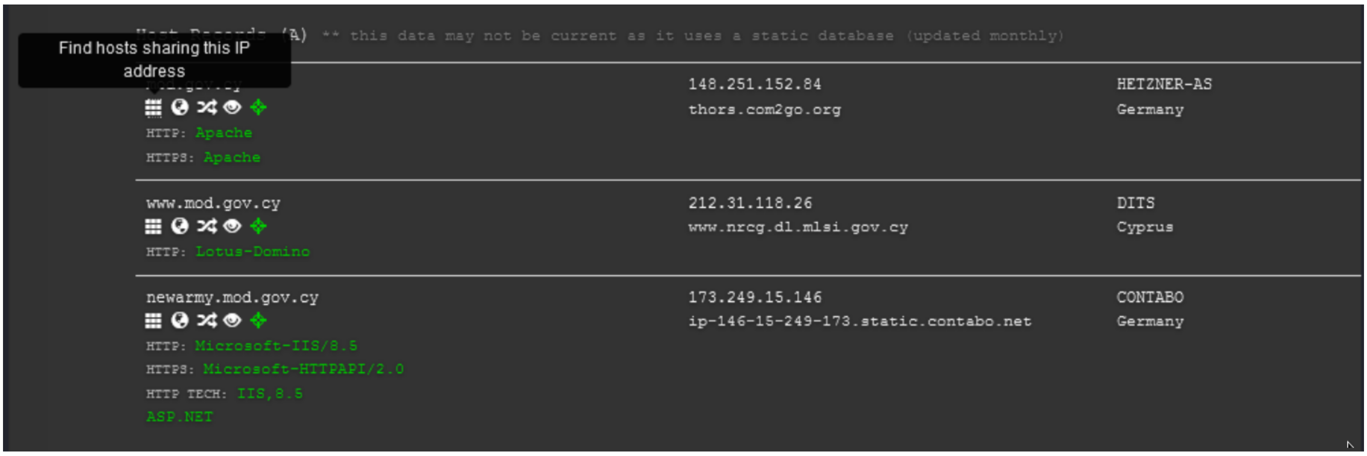
JavaScript libraries
- Underscore.js 1.9.1
- jQuery 3.2.1
- jQuery UI 1.12.1
- Moment.js 2.20.1

UI frameworks
- Bootstrap

Lead generation · CRM integration · API

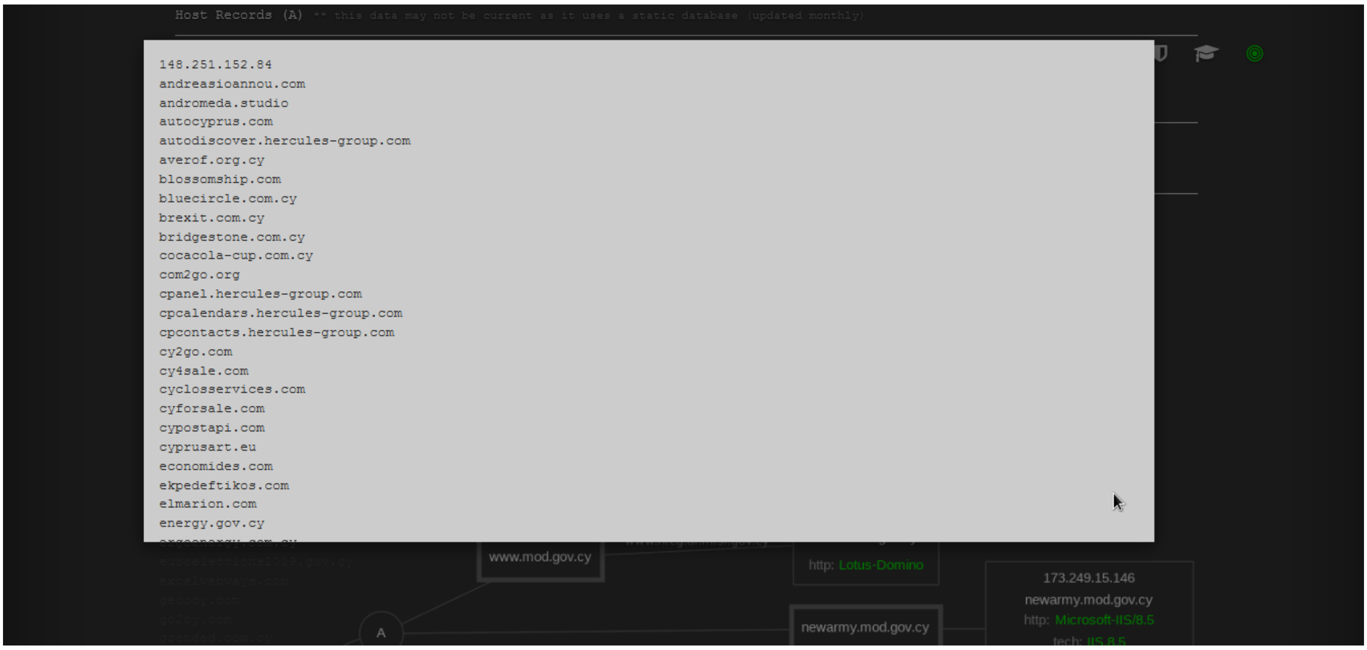
The image above shows that the website was built using the MODX Content Management System (CMS). This is a good indicator that this may be the compromised website because in some of the images published by the attacker, the exported database tables and website filenames begin with modx_ (e.g. modx_dashboard.csv). If this is the compromised website, what other government websites use the MODX CMS and have they also been compromised or could be in the near future?

A quick Google search shows that publications.gov.cy and www.pio.gov.cy could possibly be victims of the same attack since they may be affected by the same vulnerability as the MOD website. Even worse, the Com2Go developers/site administrators may use the same passwords to administer the above websites, access the websites’ databases or access their underlying operating system. If this is the case, more systems might be vulnerable to a potential compromise, something which is out of the scope of our investigatation. However, to get an idea of the number of websites that probably share the same server with the MOD website and have probably already been compromised during the attack, we simple clicked the “Find hosts sharing this IP address” link on the DNSsumpster.com website as per the image below.



```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

mod.gov.cy                        148.251.152.84                     HETZNER-AS
                                  thors.com2go.org                   Germany
HTTP: Apache
HTTPS: Apache

www.mod.gov.cy                    212.31.118.26                      DITS
                                  www.nrcg.dl.mlsi.gov.cy            Cyprus
HTTP: Lotus-Domino

newarmy.mod.gov.cy                173.249.15.146                     CONTABO
                                  ip-146-15-249-173.static.contabo.net   Germany
HTTP: Microsoft-IIS/8.5
HTTPS: Microsoft-HTTPAPI/2.0
HTTP TECH: IIS,8.5
ASP.NET
```

A sample of the list of 78 websites returned by the DNSsumpster.com website is shown below. Please bear in mind that evidence of their compromise has not been released by the hacker, hence there is a chance their data may not have been stolen.



```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

148.251.152.84
andreasioannou.com
andromeda.studio
autocyprus.com
autodiscover.hercules-group.com
averof.org.cy
blossomship.com
bluecircle.com.cy
brexit.com.cy
bridgestone.com.cy
cocacola-cup.com.cy
com2go.org
cpanel.hercules-group.com
cpcalendars.hercules-group.com
cpcontacts.hercules-group.com
cy2go.com
cy4sale.com
cyclosservices.com
cyforsale.com
cypostapi.com
cyprusart.eu
economides.com
ekpedeftikos.com
elmarion.com
energy.gov.cy
```

The complete list of websites on that server is included below in order to inform them of the possibly that their data may have been compromised and to initiate an investigation.

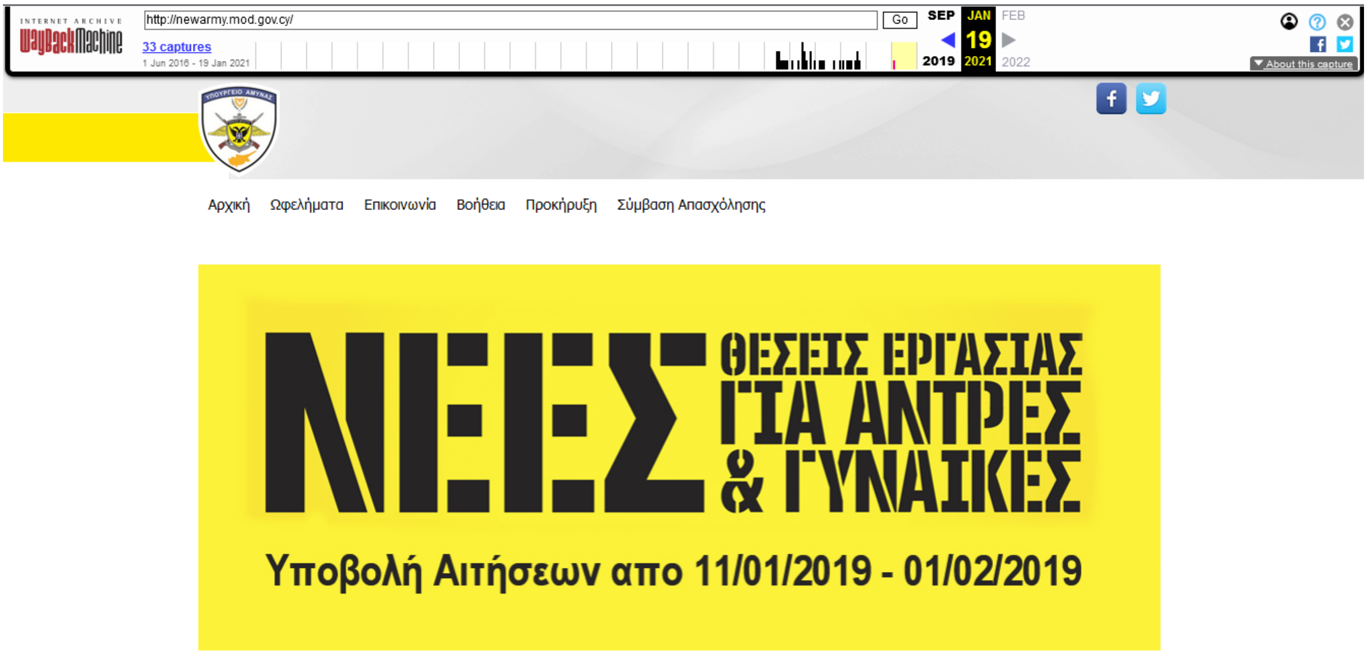
Table with 78 websites

andreasioannou.com	andromeda.studio	autocyprus.com
autodiscover.hercules-group.com	averof.org.cy	blossomship.com
bluecircle.com.cy	brexit.com.cy	bridgestone.com.cy
cocacola-cup.com.cy	com2go.org	cpanel.hercules-group.com
cpcalendars.hercules-group.com	cpcontacts.hercules-group.com	cy2go.com
cy4sale.com	cyclosservices.com	cyforsale.com
cypostapi.com	cyprusart.eu	economides.com
ekpedeftikos.com	elmarion.com	energy.gov.cy
ergoenergy.com.cy	euroelections2019.gov.cy	excelwebways.com
gecocy.com	go2cy.com	grandad.com.cy
grvisit.com	hercules-group.com	juniorkm-group.com
juniorkm.com	juniorkmgroup.com	limassolhills.com
mail.europadonna.com.cy	mail.hercules-group.com	mail.napolipizzacy.com
mail.petrosports.com.cy	mail.protelia.com.cy	mails.hercules-group.com
mod.gov.cy	mouflonfund.com	natasanirouyoga.com
nckglobal.com	novernaplus.com	panagiventilation.com
pegasos.com.cy	petrolinasolar.com.cy	petswelfarecy.com

pop.timinis.com	porsche.com.cy	regis.com.cy
santa2.me	santa2me.com	serano.com.cy
serano.gr	snackingood.com	theofanides.com
theophanides.com	thermofast.com.cy	thors.com2go.org
topaft2016.disy.org.cy	unilife.com.cy	universallife.com.cy
webdisk.hercules-group.com	webmail.hercules-group.com	webonu.com
www.centaur.com.cy	www.topaft2016.disy.org.cy	www.unilife.com.cy
www.universallife.com.cy		

What about the www.mod.gov.cy website? The DNSdumpster.com image indicates that it is running on a Lotus Domino webserver, but a visit to the site shows that it is down/unavailable. We should mention that the WayBackMachine (archive.org) website takes historical snapshots of publicly accessible websites on the Internet at specific time intervals. Querying the WayBackMachine automatically redirects us to a snapshot of the mod.gov.cy website which means that both domains (mod.gov.cy and www.mod.gov.cy) pointed to the same IP address and hence webserver until very recently (i.e. they were the same website).

This leaves us with the last remaining website on the DNSdumpster.com list, the newarmy.mod.gov.cy website which at the time of writing was not accessible. However, the WayBackMachine indicates that the last snapshot of the website was taken on the 19th of January 2021 and had the following content.



INTERNET ARCHIVE WayBackMachine

http://newarmy.mod.gov.cy/ Go

33 captures
1 Jun 2016 - 19 Jan 2021

SEP JAN FEB
19
2019 2021 2022

About this capture

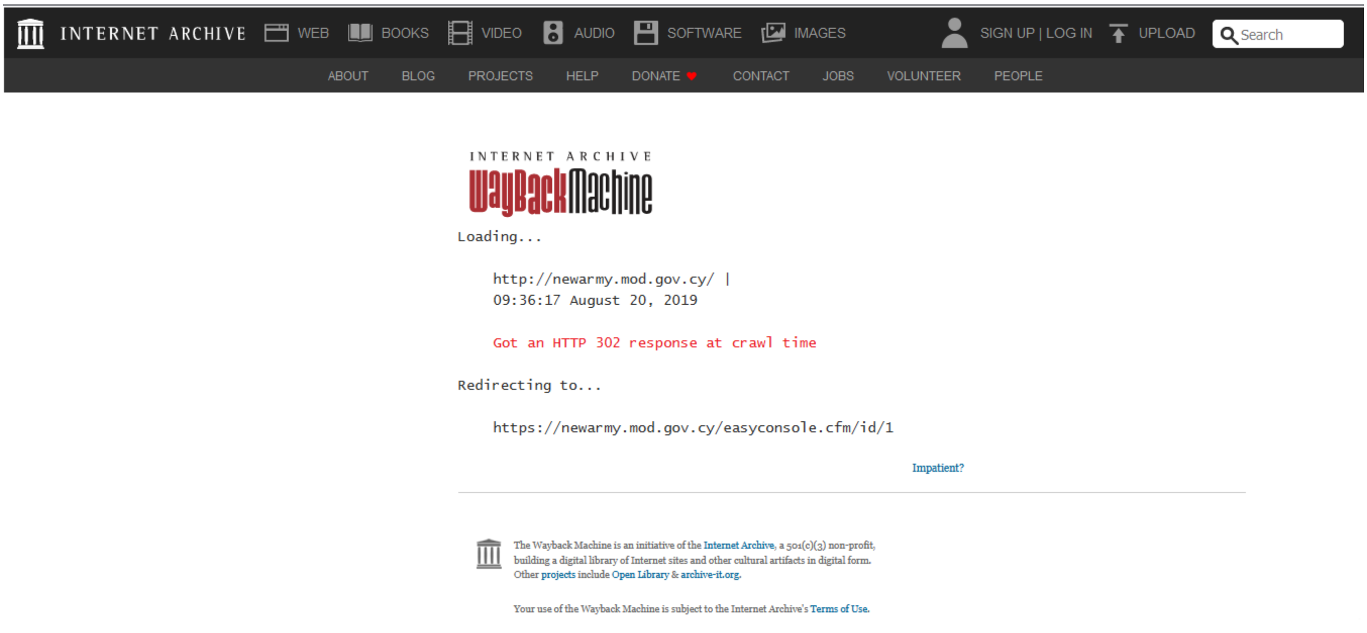
Αρχική Ωφελήματα Επικοινωνία Βοήθεια Προκήρυξη Σύμβαση Απασχόλησης

ΝΕΕΣ ΘΕΣΕΙΣ ΕΡΓΑΣΙΑΣ ΓΙΑ ΑΝΤΡΕΣ & ΓΥΝΑΙΚΕΣ

Υποβολή Αιτήσεων απο 11/01/2019 - 01/02/2019

At first glance, this may not seem to be a very important website; however, considering the fact that the personal information of applicants who tried to enlist in the National Guard (ΣΥΟΠ) may have been stolen, this should at least spur on the Commissioner of Personal Data Protection to inquire further. Furthermore, if the personal details of our professional soldiers has indeed been compromised, this could be a national security issue since they could be in the hands of a foreign nation state.

Let’s try and deduce the probability that this website was compromised. Opening the snapshot of the newarmy.mod.gov.cy taken on the 20th of August 2019, we are greeted with the below redirect message.



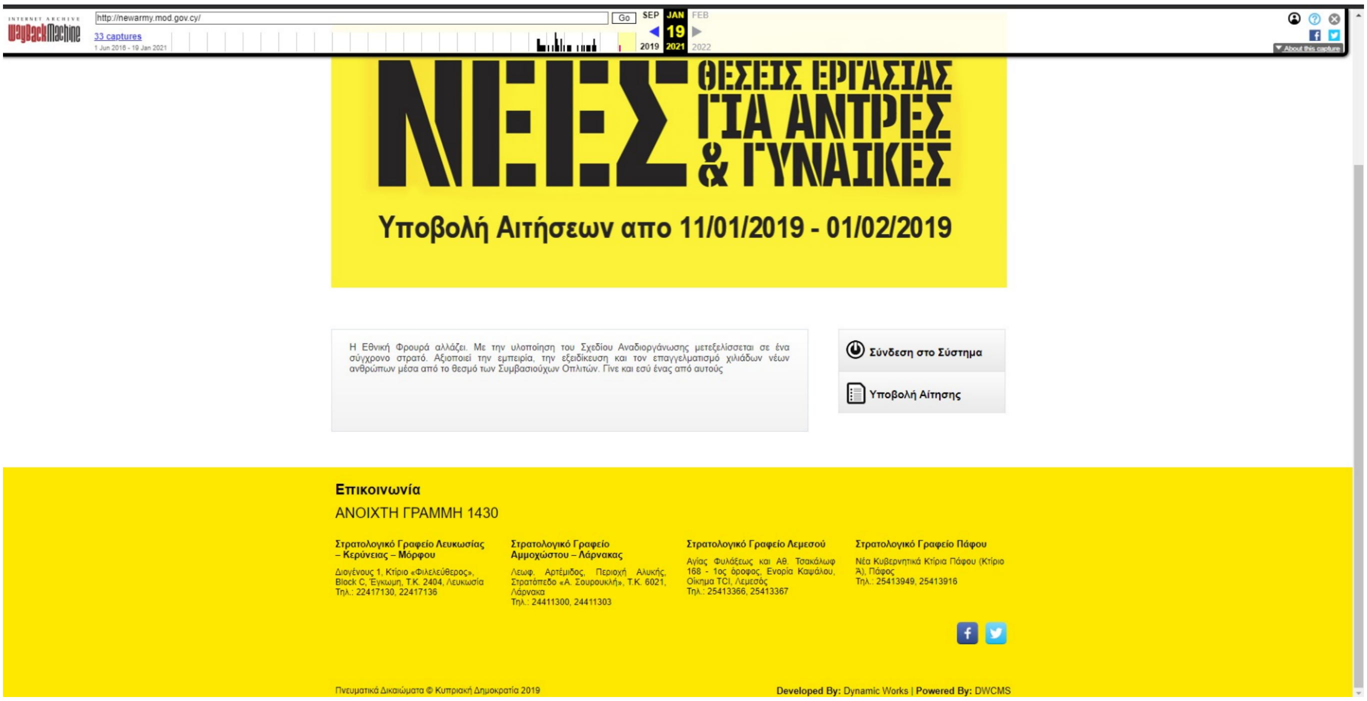
```
Loading...

    http://newarmy.mod.gov.cy/ |
    09:36:17 August 20, 2019

    Got an HTTP 302 response at crawl time

Redirecting to...

    https://newarmy.mod.gov.cy/easyconsole.cfm/id/1
```

Impatient?

The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of Internet sites and other cultural artifacts in digital form. Other projects include Open Library & archive-it.org.

Your use of the Wayback Machine is subject to the Internet Archive's Terms of Use.

A careful look at the redirection address reveals that the website was built using the EasyConsole CMS. A quick Google search shows that this is a proprietary CMS, developed by a Cyprus company called Dynamic Works. In addition to this, the snapshot of the website advertises the company who developed the site as Dynamic Works (hereafter referred to as DW).



Υποβολή Αιτήσεων απο 11/01/2019 - 01/02/2019

Η Εθνική Φρουρά αλλάζει. Με την υλοποίηση του Σχεδίου Αναδιοργάνωσης μετεξελίσσεται σε ένα σύγχρονο στρατό. Αξιοποιεί την εμπειρία, την εξειδίκευση και τον επαγγελματισμό χιλιάδων νέων ανθρώπων μέσα από το θεσμό των Συμβασιούχων Οπλιτών. Γίνε και εσύ ένας από αυτούς

Σύνδεση στο Σύστημα

Υποβολή Αίτησης

Επικοινωνία

ΑΝΟΙΧΤΗ ΓΡΑΜΜΗ 1430

Στρατολογικό Γραφείο Λευκωσίας – Κερύνειας – Μόρφου
Διογένους 1, Κτίριο «Φιλελεύθερος», Block C, Έγκωμη, Τ.Κ. 2404, Λευκωσία
Τηλ.: 22417130, 22417136

Στρατολογικό Γραφείο Αμμοχώστου – Λάρνακας
Λεωφ. Αρτέμιδος, Περιοχή Αλυκής, Στρατόπεδο «Α. Σουρουκλή», Τ.Κ. 6021, Λάρνακα
Τηλ.: 24411300, 24411303

Στρατολογικό Γραφείο Λεμεσού
Αγίας Φυλάξεως και Αθ. Τσακάλωφ 168 - 1ος όροφος, Ενορία Καψάλου, Οίκημα TCI, Λεμεσός
Τηλ.: 25413366, 25413367

Στρατολογικό Γραφείο Πάφου
Νέα Κυβερνητικά Κτίρια Πάφου (Κτίριο Ά), Πάφος
Τηλ.: 25413949, 25413916

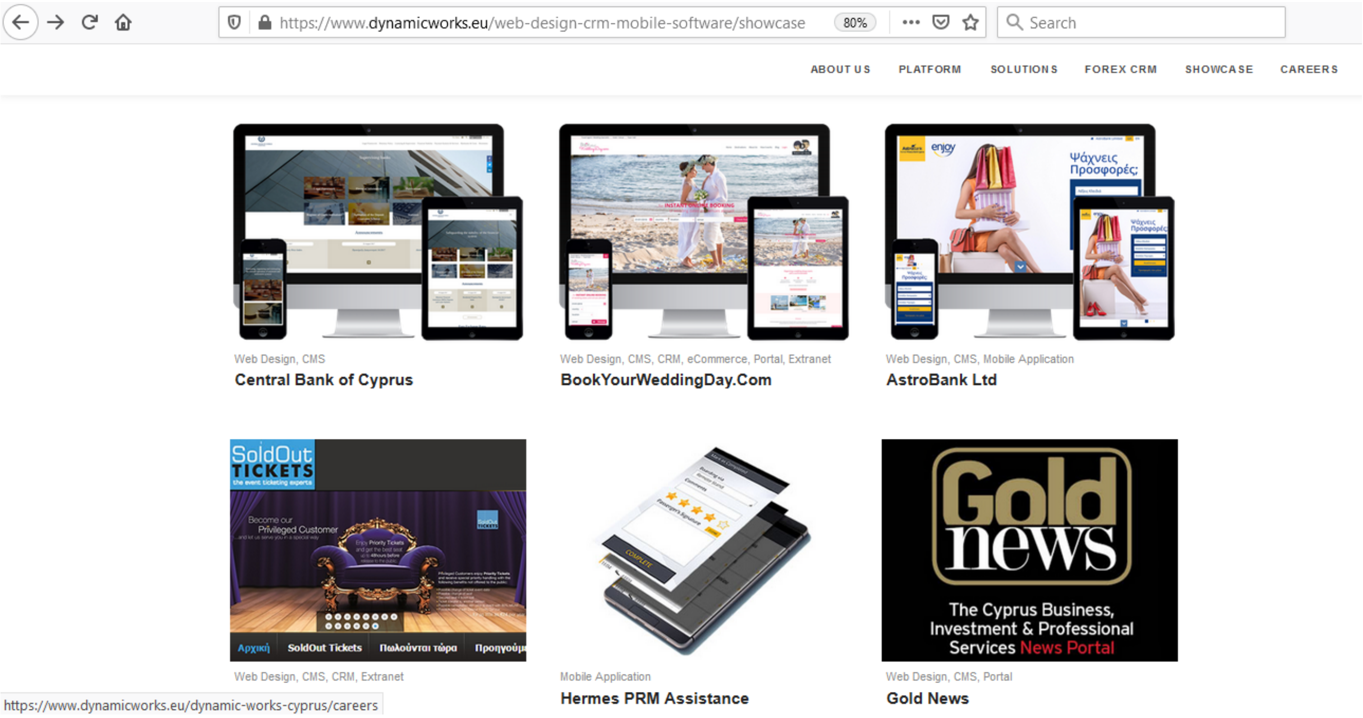
Πνευματικά Δικαιώματα © Κυπριακή Δημοκρατία 2019

Developed By: Dynamic Works | **Powered By:** DWCMS

Furthermore, DW's website, under the “Showcase” section, contains a list of client organizations whose websites or web-based applications they builtc Works. Some of them are:

- Central Bank of Cyprus
- AstroBank
- Hermes Airport
- Gold News
- PAFC Social Media

- Funding Programmes Portal (Government)
- HRD Authority (Government)
- The Cyprus Parliament (Government)
- Cyprus Institute of Neurology and Genetics
- OCECPR (Government)
- CNP Insurance
- Vassiliko Cement Works Public Company



https://www.dynamicworks.eu/web-design-crm-mobile-software/showcase

80%
Search
ABOUT US
PLATFORM
SOLUTIONS
FOREX CRM
SHOWCASE
CAREERS
SoldOut TICKETS
the event ticketing experts
Become our Privileged Customer
Αρχική
SoldOut Tickets
Πωλούνται τώρα
Gold news
The Cyprus Business, Investment & Professional Services News Portal

Web Design, CMS
Central Bank of Cyprus

Web Design, CMS, CRM, eCommerce, Portal, Extranet
BookYourWeddingDay.Com

Web Design, CMS, Mobile Application
AstroBank Ltd

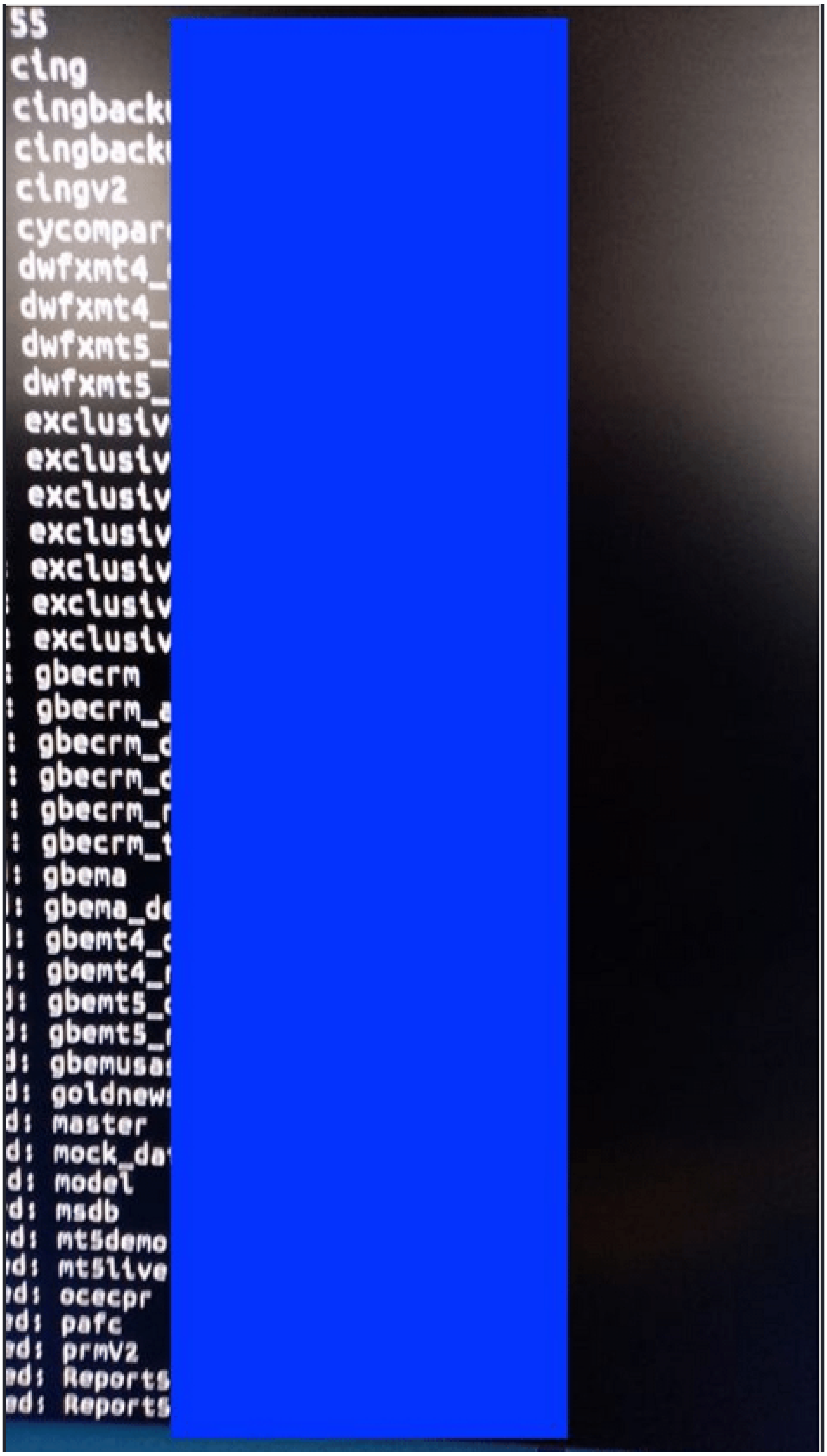
Web Design, CMS, CRM, Extranet

Mobile Application
Hermes PRM Assistance

Web Design, CMS, Portal
Gold News

https://www.dynamicworks.eu/dynamic-works-cyprus/careers

But have they been compromised? Included in the images released by the hacker is what looks like a list of MS SQL Server database instance names. This can be easily deduced by the default MS SQL database names “master”, “msdb” and “model” that are clearly shown in the image below.



[redacted]

```
55
cing
cingback
cingback
cingv2
cycompar
dwfxmt4_
dwfxmt4_
dwfxmt5_
dwfxmt5_
exclusiv
exclusiv
exclusiv
exclusiv
: exclusiv
: exclusiv
: exclusiv
: gbecrm
: gbecrm_a
: gbecrm_c
: gbecrm_c
: gbecrm_r
: gbecrm_t
: gbema
: gbema_de
: gbemt4_c
: gbemt4_r
: gbemt5_c
: gbemt5_r
d: gbemusa
d: goldnew
d: master
d: mock_da
d: model
d: msdb
d: mt5demo
d: mt5live
d: ocecpr
d: pafc
d: prmV2
d: Reports
d: Reports
```

Also included in the above image are the database names of some of the companies listed in the Dynamic Works showcase, or others that can easily be verified via a Google search. The list of private and public companies, and government entities that shared the same server as newarmy.mod.gov.cy are:

Dynamic Works database name	Company/Government Entity
cing	Cyprus Institute of Neurology and Genetics

Dynamic Works database name	Company/Government Entity
cycompare	OCECPR (ΓΕΡΗΕΤ/ΑΨΑ)
gbecrm	GBE Brokers Customer Relationship Management
gbemt4	GBE Brokers MetaTrader 4 Trading Platform
gbemt5	GBE Brokers MetaTrader 5 Trading Platform
goldnews	Gold News
ocecpr	OCECPR (ΓΕΡΗΕΤ/ΑΨΑ)
pafc	Pafos Aphrodite Festival Cyprus –Social Media

There is a very high likelihood that all these websites were compromised because they resided on the same server.

It should be noted that the Turkish hacker, as per the SecNews post, stated that he plans to “destroy Cyprus and will target banking and military systems”. From DW's portfolio and the databases listed, we can safely assume that the banking websites mentioned above are in the hacker’s crosshair or have already been compromised.

What's also very worrying is that two of the potentially compromised databases belong to the Office of the Commissioner of Electronic Communications & Postal Regulations under whose control and administration is the National Computer Security Incident Response Team (CY-CSIRT) and the Digital Security Authority (DSA). As per the DSA’s national legislation, it is the responsible authority for the security of digital networks and IT systems in Cyprus and the coordinator for the implementation of the national security strategy. In simple terms, it is responsible for the protection of the country’s critical infrastructure (e.g. Electricity Authority, Waterboards, Sewage Authorities, Banks, etc.), collects security-related information regarding the security weaknesses and defense mechanisms of organizes that are categorized as critical infrastructure, and has the power to set fines (financial and up to 3 years imprisonment) to companies and persons that fall under the Authority’s control.

The following questions regarding the incident arise:

1. Have Dynamic Works, Com2Go, the Ministry of Defense and the Deputy Ministry of Research, Innovation and Digital Policy, taken the necessary steps to notify the relevant authorities about the incident (e.g. Commissioner of Personal Data Protection)? If not, why?
2. Have all the clients of Dynamic Works and Com2Go been notified about the attack and the possibility of them being subsequently compromised?
3. Why was the incident undermined in public announcement issued by the Ministry of Defense to the media?
4. What is the true extent of the personal information leakage, taking into consideration all the clients in the list above?
5. This was not the first time that a cyber security incident affecting government systems occured, or was made public. Why did government not take the necessary steps to securely deploy the website (e.g. carrying out a penetration test, avoiding a shared hosting environment for sensitive information etc)?
6. Who are the persons responsible for the government’s cyber security procedures?

7. What information regarding Cypriot critical infrastructure was leaked from the OCECPR website? Why wasn’t it detected by them and what measures have they put in place to try and prevent the compromise of such data?

We believe that it has become a common practice in Cyprus to cover up cyber security intrusions; this has a detrimental effect on companies since they cannot see the real risk of attacks, therefore they are skpetical about the necessity of taking precautionary / proactive measures to protect themselves, until of course it is too late (as we have seen from our experiences time and again).

At the time of writing this whitepaper, SecNews.gr (secnews.gr/339663/hacked-larnaca-airport-hermesairports-rootayyil/), published an article about an attack on the website of Hermes Airports. Based on the Dynamic Works portfolio (secnews.gr/339663/hacked-larnaca-airport-hermesairports-rootayyil/) , the Hermes Airports PRM mobile application was developed by Dynamic Works. Unfortunately, the two attacks seem to be related since a screenshot from the SecNews.gr article showing the database names contains the PRM system. Initially we did not know which company this database belongs to, but after the Hermes Airport compromise it has been become obvious that the Turkish hackers inflicted more damage that it was initially estimated.

Therefore we would like to make the following recommendations towards the government in regards to its systems, policies and procedures:

1. Regarding any and all government information systems, security should be taken seriously by senior stakeholders, and not left as an afterthought.
2. The government should preform regular security reviews and penetration tests to identify and fix high-severity vulnerabilities; it should also continuously monitor its systems for p=ossible intrusions and have a plan in place for any such eventuality.
3. Appoint a contact person so that anyone who discovers a security weakness/vulnerability related to a governmental system can discloe it responsibly.
4. Implement a bug bounty program so Cypriot hackers (read: security practitioners) can legally test and report identified vulnerabilities on government systems and receive a financial reward for it.
5. Openly accept and report security incidents that affect government systems. We recommend a spokesperson be appointed for announcing such incidents to the public.
6. Vendors should be held accountable for gross negligence regarding how they manage vulnerabilities found in their products, if this can be proven.

All of the above recommendations also apply to private sector companies who should take the necessary steps to implement them. What was mentioned above is solely based on information we managed to collect from public resources and a proper investigation should be performed by the relevant authorities to confirm the above inferrences (which are based on our combined technical and professional experiences).

We apologize in advance to the affected companies if we have caused any reputational damage, but our intention was to responsibly inform the public and the persons whose personal information might have been compromised, since it was apparent that no one else was going to.