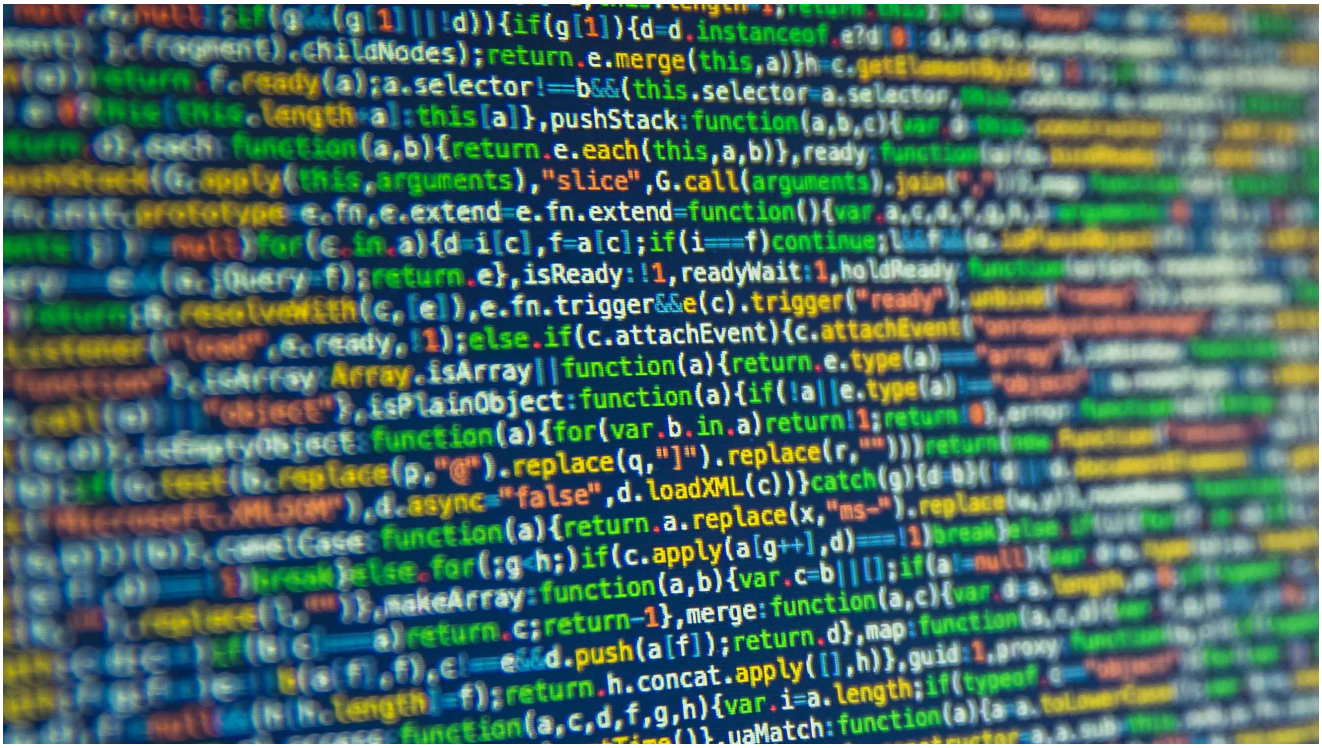
Hunt Case Study: Hunting Campaign Indicators on Privacy Protected Attack Infrastructure

domaintools.com/resources/blog/case-study-hunting-campaign-indicators-on-privacy-protected-attack-infrastr



As a researcher, when I find an attacker working, one of the first places I start to pivot is the command and control infrastructure. I do this because I want to see if I can find additional binaries, indicators of attack, or additional infrastructure being used by an adversary.

When looking at attacker infrastructure, one of the things that annoys analysts the most is attackers using Whois protection services for registering domains that are used as attack infrastructure. At first glance, many analysts will abandon an investigation when finding privacy protected domains. So, in this blog, I intend to show just how you can pivot on a privacy protected indicator of attack infrastructure, and ultimately find good intelligence data.

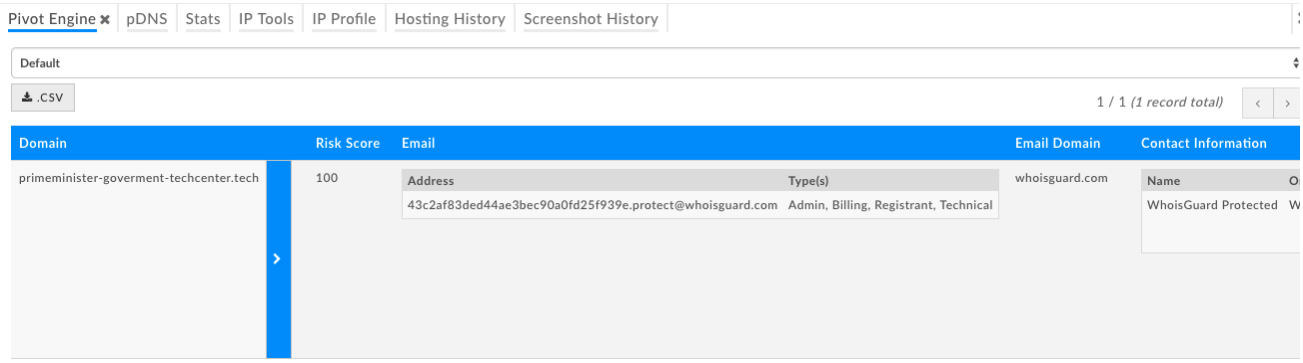
Please keep in mind, in this blog I will not be attributing this activity to any specific nation state. We have indicators that point to a specific actor group, but nation-state attribution is a tricky and near impossible endeavor, therefore we shy away from making any nation-state attribution claims.

Infrastructure Pivots

As part of my daily routine, I check several tools for any triggered YARA rules I'm running. One particular domain stood out, since it triggered on a specific rule looking for attacker infrastructure.

In this case, I looked at the domain in **DomainTools Iris Investigate**:

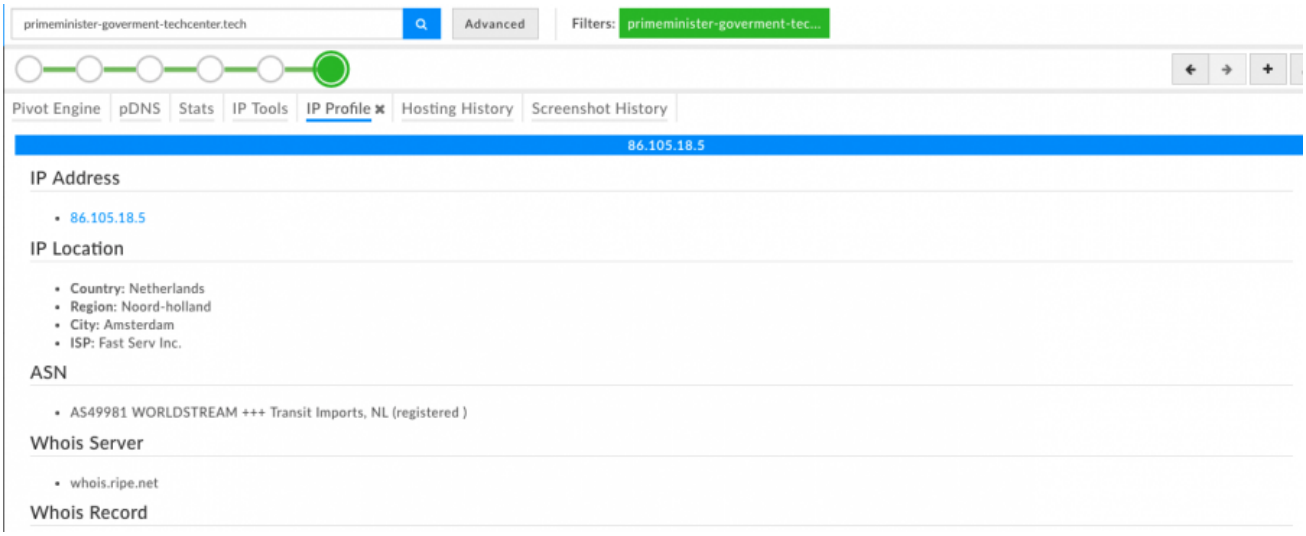
primeminister-goverment-techcenter[.]tech



When an attacker uses Whois protection, it prevents an analyst from pivoting off registrant information, making it more difficult to find additional infrastructure or files. But, there is a way to help offset this perplexing investigative nuisance.

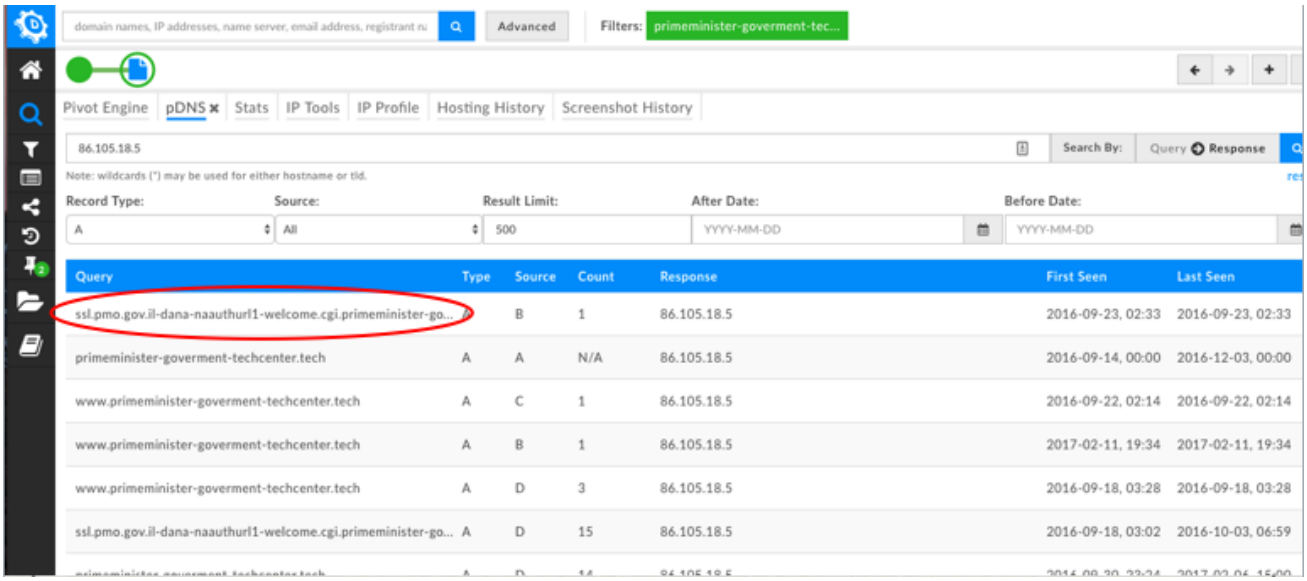
Because of the privacy protection on the Whois record, I looked to find the IP that the domain is hosted on. Keep in mind, finding the IP doesn't have to be the first pivot to execute. There are several potential pivots an investigator could start with. I began my first pivot with the IP first because I often scour infrastructure of the attacker before I move on to analyzing actor tools and procedures. Also, ideally we will see additional attacker infrastructure on that IP, regardless of who's hosting the domains. Pivoting off the IP of the hosting infrastructure can prove valuable, especially when the hosting provider and the privacy protection service are different entities.

Within the DomainTools Iris Investigate toolset, I quickly pulled and pivoted off the IP address of the hosting infrastructure- 86[.]105[.]18[.]5.



When pivoting within Passive DNS on the IP, several additional domains were identified. Out of those newly identified domains, one specific one piqued my interest.

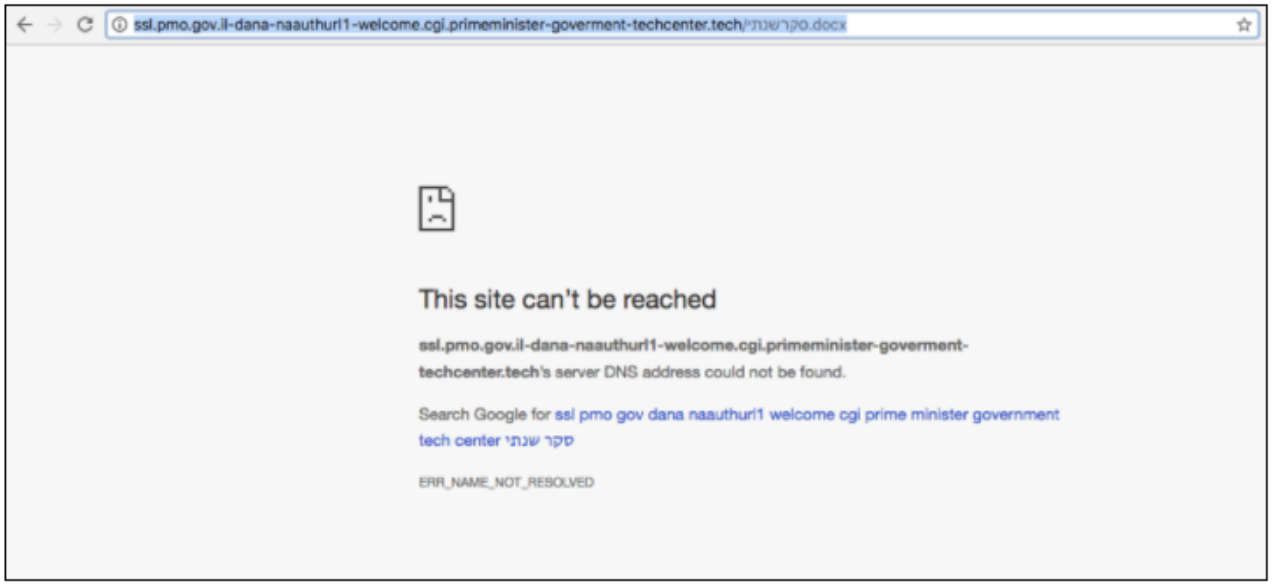
ssl.pmo.gov[.]il-dana-naauthurl1-welcome.cgi.primeminister-goverment-techcenter[.]tech



At this point, I Googled the domain and found that there could possibly be a Microsoft Word file hosted on the newly discovered URL.

http://ssl.pmo.gov.il-dana-naauthurl1-welcome.cgi.primeminister-goverment-techcenter.tech/%D7%A1%D7%A7%D7%A8%20%D7%A9%D7%A0%D7%AA%D7%99.docx

Converting the .docx file to a readable format, you are given a Hebrew file name סקרשנתי.docx, which when translated means “Annual Survey.docx.”

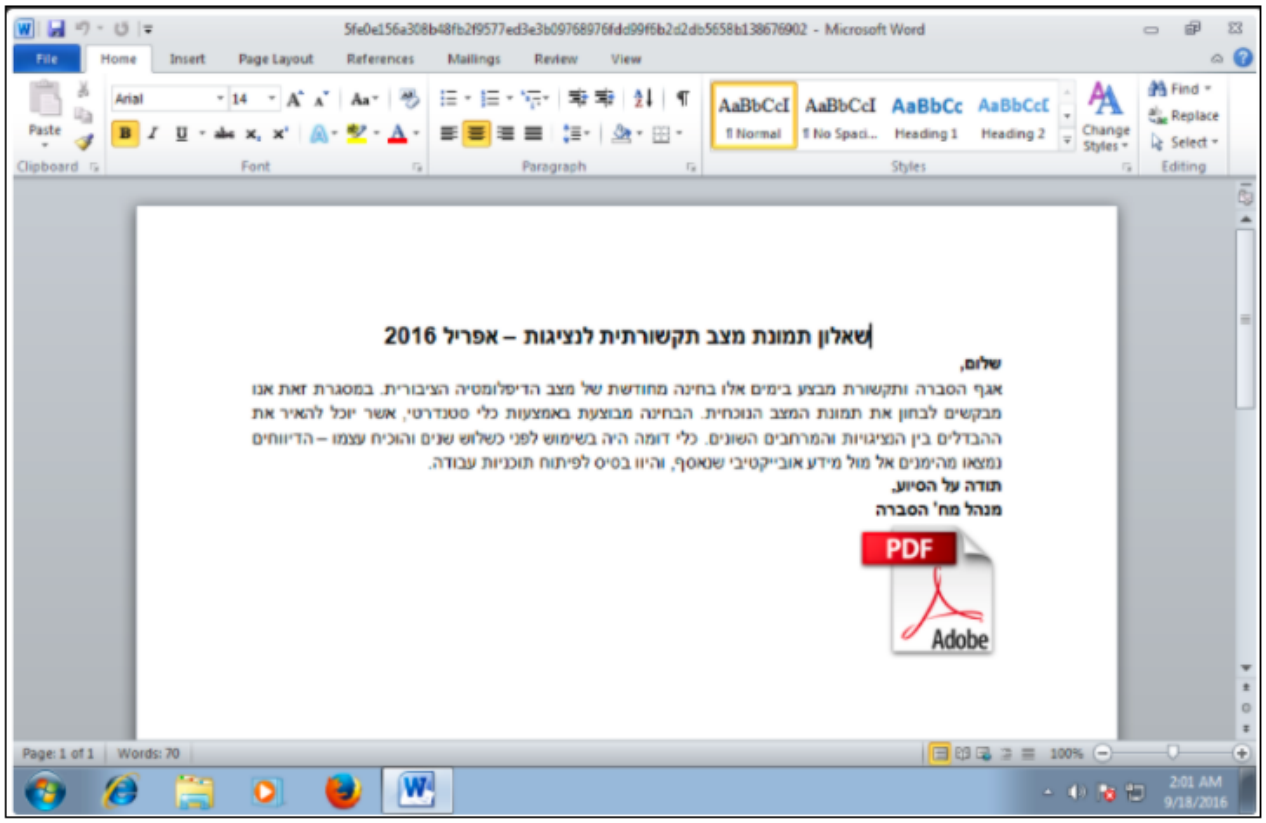


At this point, the hunt was on to find the actual DOCX file. I wanted to download the DOCX to not only find any possible communications that could be occurring, but also strings in the file, dropped files, possible build paths, and even communications. In addition, having the actual file allows us to pivot and write YARA rules to match any other files in the wild that may be related. (Possibly the same attacker/group or campaign)

Using the file name and C2, with the help of Google and some additional tools, I was able to subsequently locate and download the DOCX.

Annual_Survey.docx

Looking closer at the malware document, I noticed that it appeared to come from the Director of the Information Department. The document also makes reference to The Ministry of Communications, therefore possibly targeting the Israeli government's Ministry of Communications.



Looking at the Word document, there is an OLE object (oleObject1.bin) directly embedded within it, making it look like a PDF was actually embedded.

```
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: word/_rels/document.xml.rels
  inflating: word/document.xml
 extracting: word/media/image1.png
  inflating: word/embeddings/oleObject1.bin
  inflating: word/theme/theme1.xml
  inflating: word/settings.xml
  inflating: word/webSettings.xml
  inflating: docProps/core.xml
  inflating: word/styles.xml
  inflating: word/fontTable.xml
  inflating: docProps/app.xml
```

The OLE object, appearing to be an embedded PDF, and appears to be communicating to a C2.

static.dyn-usr[.]f-login-me.c19.a23.akamaitechnology[.]com

This domain has an IP of 212[.]199[.]61[.]51, which, according to pDNS data within Iris Investigate can also be attributed to 212.199.61.51.static.012.net[.]il. It's important to note that the Top Level Domain (TLD) .il is assigned to the country of Israel.

Within the strings of the original PDF file, there appears to be a build path (C:\Users\Administrator\Desktop\Files\mfa\mfaformann) and two file names - **fdp.exe** and **PDFOPENER_CONSOLE.exe.**

```
PDFOPENER_CONSOLE
PDFOPENER_CONSOLE.exe
mscorlib
System
kernel32.dll
user32.dll
PDFOPENER_CONSOLE
AppDomain
```

```
ASCII Strings:
==========
OLE Package
Package
mfaformann
fdp.exe
C:\Users\Administrator\Desktop\Files\mfa\mfaformann
fdp.exe
C:\Users\ADMINI
1\AppData\Local\Temp\mfaformann
fdp.exe
```

We didn't investigate these files further, but they could easily be analyzed further for additional pivot points.

Infection Vector

Looking closer at the domains and files involved in this campaign, while looking for infection vectors, with the help of Eyal Sela from ClearSky, we noticed that the domain *http://ssl[.]pmo.gov.il-dana-naauthurl1-welcome.cgi.primeminister-goverment-techcenter[.]tech/%* was in fact, the original phishing page to drop the Annual Survey.docx

This spear phishing page appears to be a near clone of the valid Israeli Prime Minister's office SSL VPN login page; except for a few changes that include the "Plugin installation initiated…", "Restitution of Jewish Property" and "Please login to start the installation."

Conclusion

There are additional pivots that one could perform on this dataset and possibly find other campaigns targeting Israeli interests. For the sake of this blog, we didn't go down every rabbit hole as this is a large campaign and can be further investigated.

Attribution is not something we typically get involved in. It is extraordinarily difficult to definitively state where an attacker originates. However, in this case, some of the indicators of compromise or attack attribute this activity to a well known attack group called CopyKitten*.

After reading this blog, one can see the power of pivots, especially off initially identified attacker infrastructure. This is even useful when an attacker uses privacy protection when registering domains as part of their infrastructure. As we continue to monitor attacker groups, it's important to pay attention to the importance of not just pivots, but the appropriate pivots to make. Ideally, using a tool like DomainTools can eliminate some of those manual processes, thus reducing the amount of dwell time on a network.

———————

*http://www.clearskysec.com/report-the-copykittens-are-targeting-israelis/

I'd like to personally thank Eyal Sela from ClearSky Cyber Security who assisted in providing intelligence as we both investigated this actor.

IOCs/IOAs referenced in this blog

Domains

- primeminister-goverment-techcenter[.]tech
- http://ssl.pmo.gov.il-dana-naauthurl1-welcome.cgi.primeminister-goverment-techcenter[.]tech
- static.dyn-usr.f-login-me.c19.a23.akamaitechnology[.]com
- 212.199.61.51.static.012.net[.]il

IPs

- 212[.]199[.]61[.]51
- 86[.]105[.]18[.]5

Files

- Annual Survey.docx and/or סקרשנתי.docx
  5fe0e156a308b48fb2f9577ed3e3b09768976fdd99f6b2d2db5658b138676902
- PDFOPENER_CONSOLE.exe:
  4d657793ddc9c49abe7e4afcf9abb43626e91a18a925223555070c53fd672b59

oleObject1.bin

7651f0d886e1c1054eb716352468ec6aedab06ed61e1eebd02bca4efbb974fb6