WHITE PAPER

HUNTING RATS

WRITTEN BY MATTHEW HAYNES
OF ASKARI BLUE

Introduction

Security professionals must continue to ask themselves, are they doing enough? Are they continuing to develop their knowledge and defences? Are they successfully staying ahead of cybercriminals? And even if the answer is *yes*, how do they know they will continue to stay ahead tomorrow? Systems are built, security protocols are established but then, in many cases, development stops and new defences are not implemented to mitigate new threats. What may have once been secured, will soon likely fail to keep new threats and vulnerabilities at bay as cybercriminals increase both their capability and volume of attacks.

To prevent an attack, an organisation may maintain a good patch management cycle and updated rulesets. Some may even go further to adopt threat intelligence feeds, although, it is argued this can be counterproductive. When threat intelligence is used correctly, it can deliver an early warning of likely threats, enabling ample time to adjust defences accordingly.

Defence teams are tasked with monitoring within a SOC, safeguarding the business, and winning every engagement with the enemy. On the other hand, threat actors or penetration testers only need to succeed once to win. But this works both ways, as investigators only need to identify one misstep by cybercriminals.

Hunting and identifying a threat actor may provide an opportunity to understand the enemy and learn better methods in defending against them. Cyber security professionals may not have the jurisdiction of Law enforcement and most definitely do not have the legal rights to *hack back*. But they can learn what new controls are required, even before a threat actor envisions their new tool, technique or procedure (TTP).

Goal of this paper

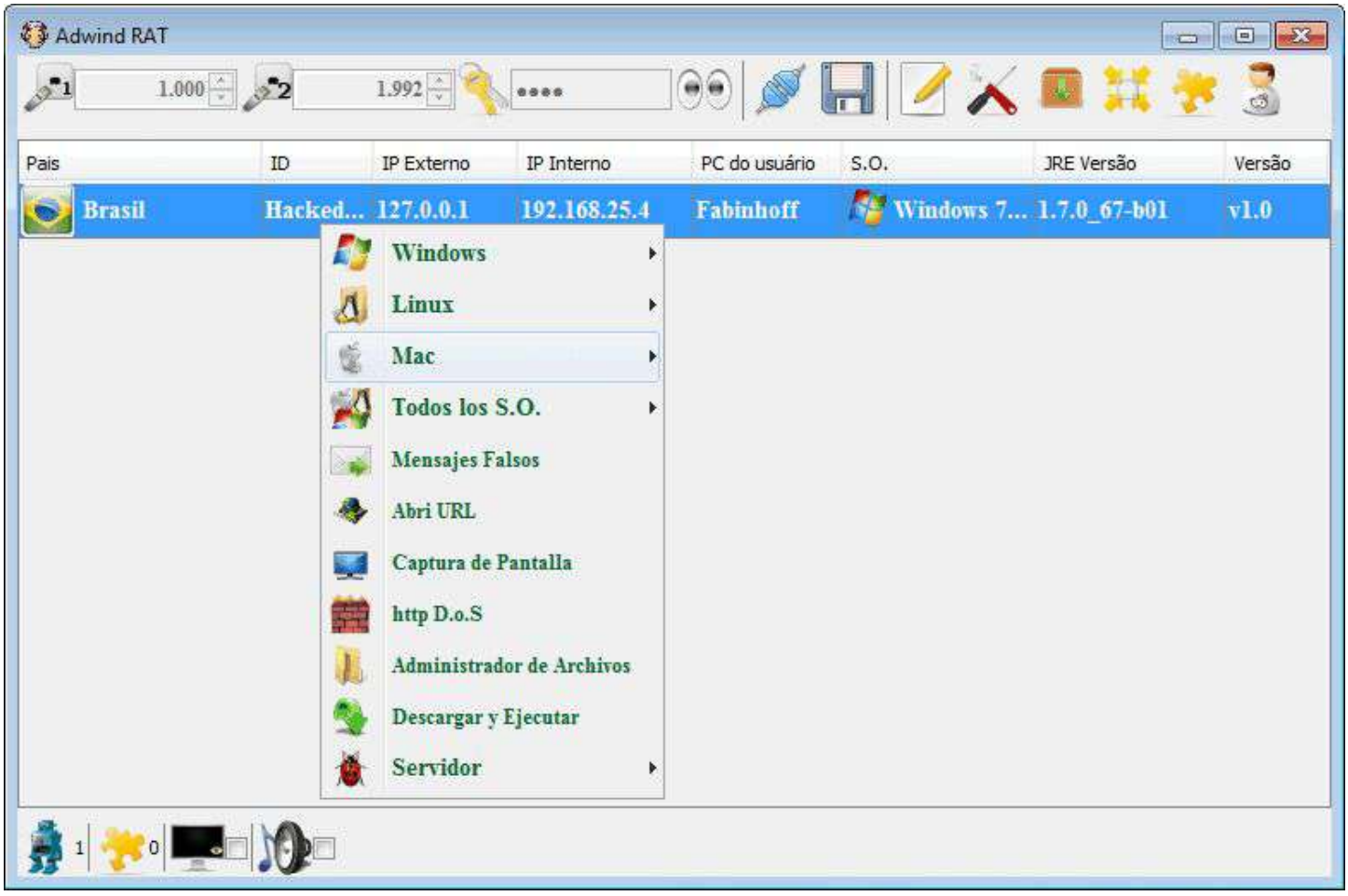
To aid security professionals in the use of powerful threat investigation tools such as DomainTools' Iris, so that they can further defend their business from cybercriminals through increased understanding of a given threat.

What is a RAT?

A Remote Access Trojan (RAT) is a very common tool used by many criminal groups and individuals across the world. This tool is often considered to be malware, but its functionality can be used for legitimate purposes. As an example, TeamViewer is a remote administration tool used by many system administrators to manage the corporate estate. Such functionality can include, but is not limited to; remote control, desktop sharing, file transfer, microphone access, camera access, keyboard input capture.

Adwind RAT v3.0 Operator Console

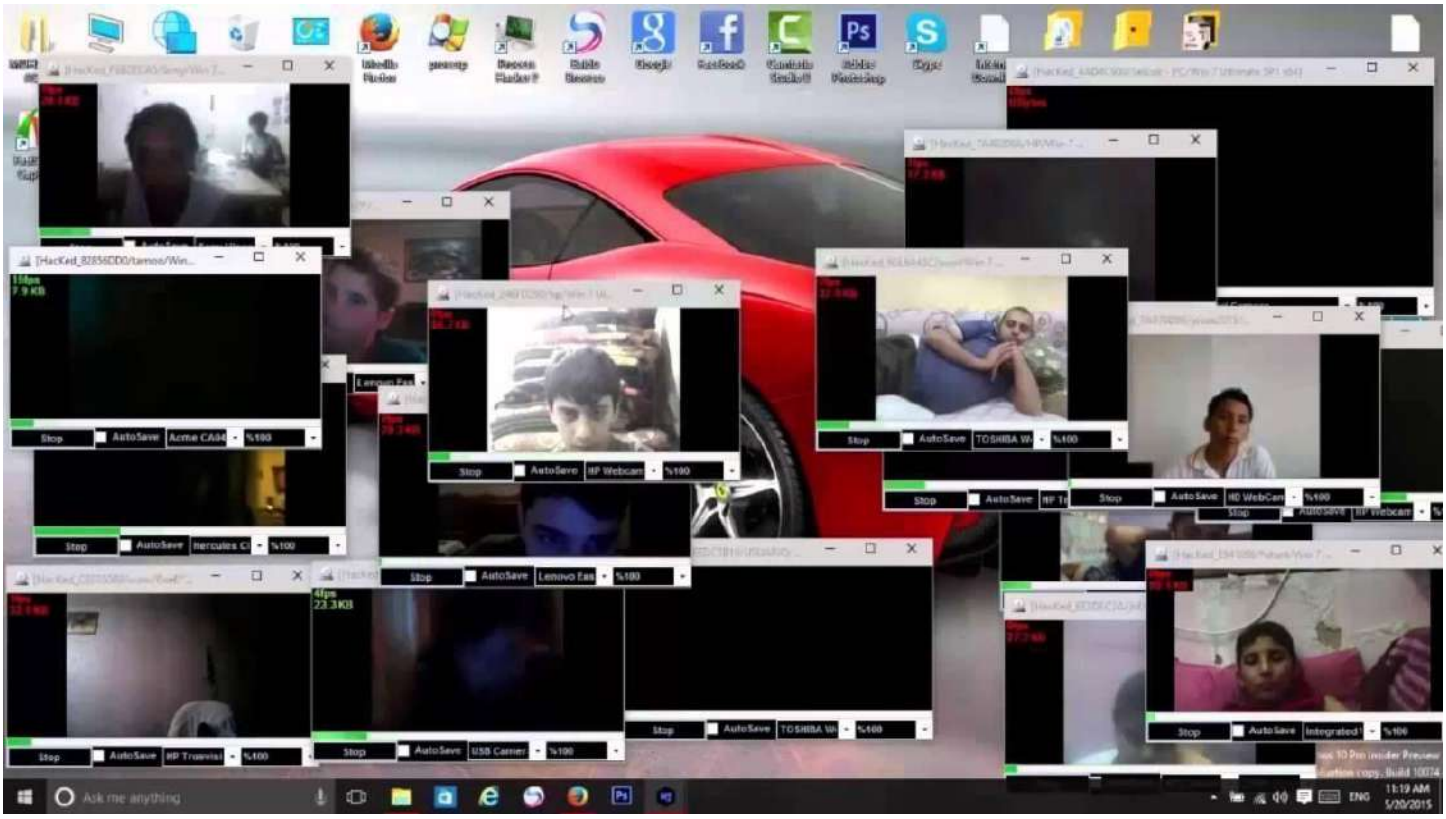
Source:
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07195002/KL_AdwindPublicReport_2016.pdf&psig=AOvVaw0tdnSNrO9Eh5X2Fc-Ild72&ust=1572366153652583



Adwind RAT Operator Console

Source:
https://www.connect-trojan.net/2014/09/adwind-rat-v10.html&psig=AOvVaw08r3pNgFqDTsaAe2XrT6sb&ust=1572366240698978

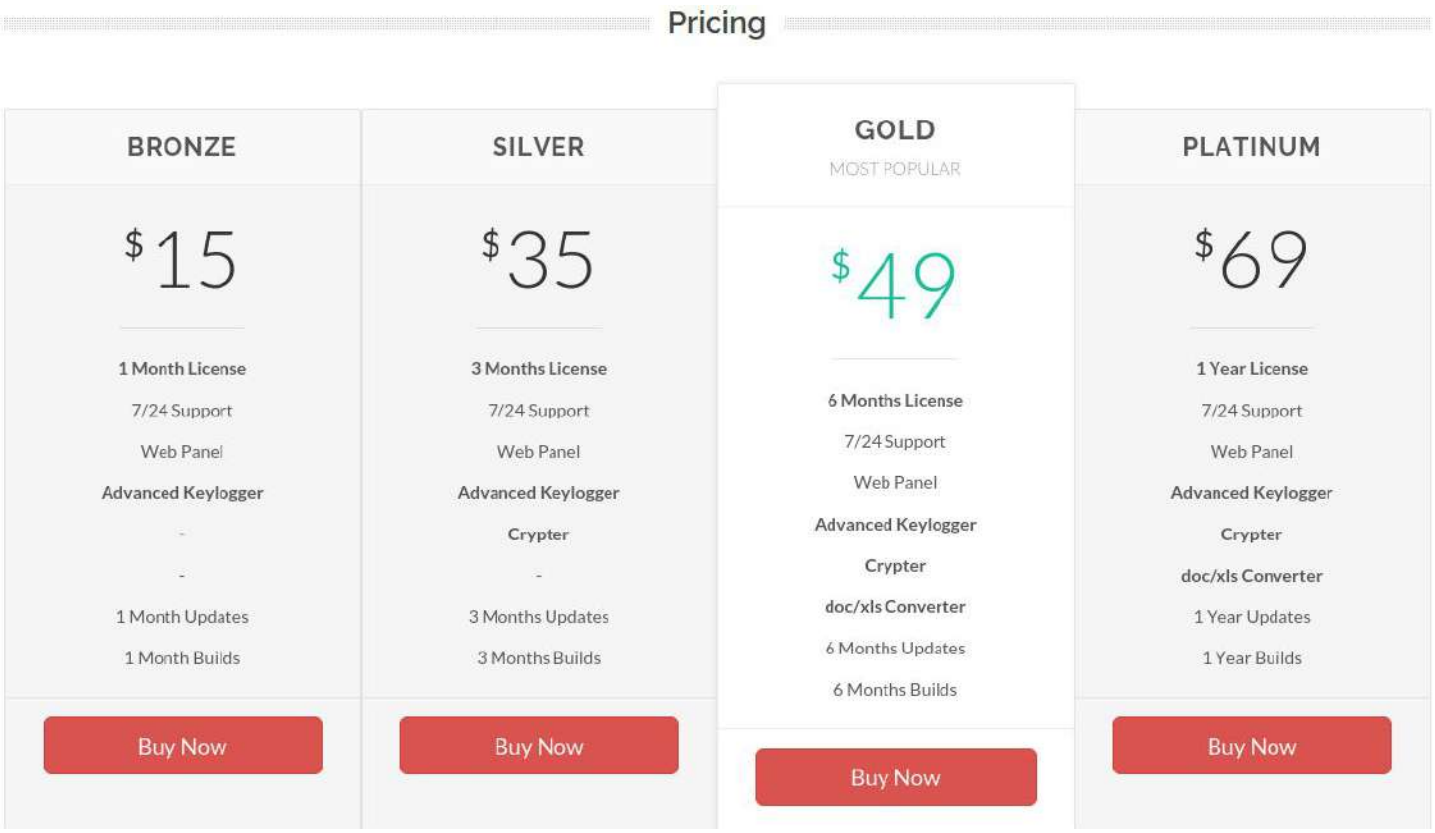
RATs are easy to use and simple to acquire. Very simplistically, a RAT server, otherwise known as a C2 (Command and Control) is installed on a computer. The console is typically user friendly and looks like any other normal Windows program. The operator uses the RAT to generate additional malware that will be installed on a victim's machine. Once installed, it will talk back to the C2 and allow the operator to control the victim remotely. Much of this process is relatively easy, the difficult aspect is successfully installing the malware on to the victim, bypassing any antivirus or other defensive controls along the way.



Njrat example of attack

Source: https://www.youtube.com/watch?v=ZB3A2nnIqpI

While many older RAT variants are accessible free of charge (and often contain a backdoor), many newer versions are available at low cost and purchased through a Crime-as-a-Service (CaaS) offering. The cat and mouse game of antivirus providers and malware developers has existed for a long time. In simplistic terms, when malware is created, antivirus programs do not recognise the sample and therefore mark it as benign. Such samples are eventually discovered by investigations, although this could take several days, weeks or longer. Once identified, antivirus programs are updated and begin blocking the malware sample. The same malware must be re-written so that antivirus programs do not identify it, but eventually it will be discovered, and the process reiterates. For older RATs most samples are now known and therefore, threat actors use CaaS to pay for services that distribute their malware and evade detection.



Crime-as-a-Service pricing page.

Source: https://krebsonsecurity.com/tag/nanocore-rat/

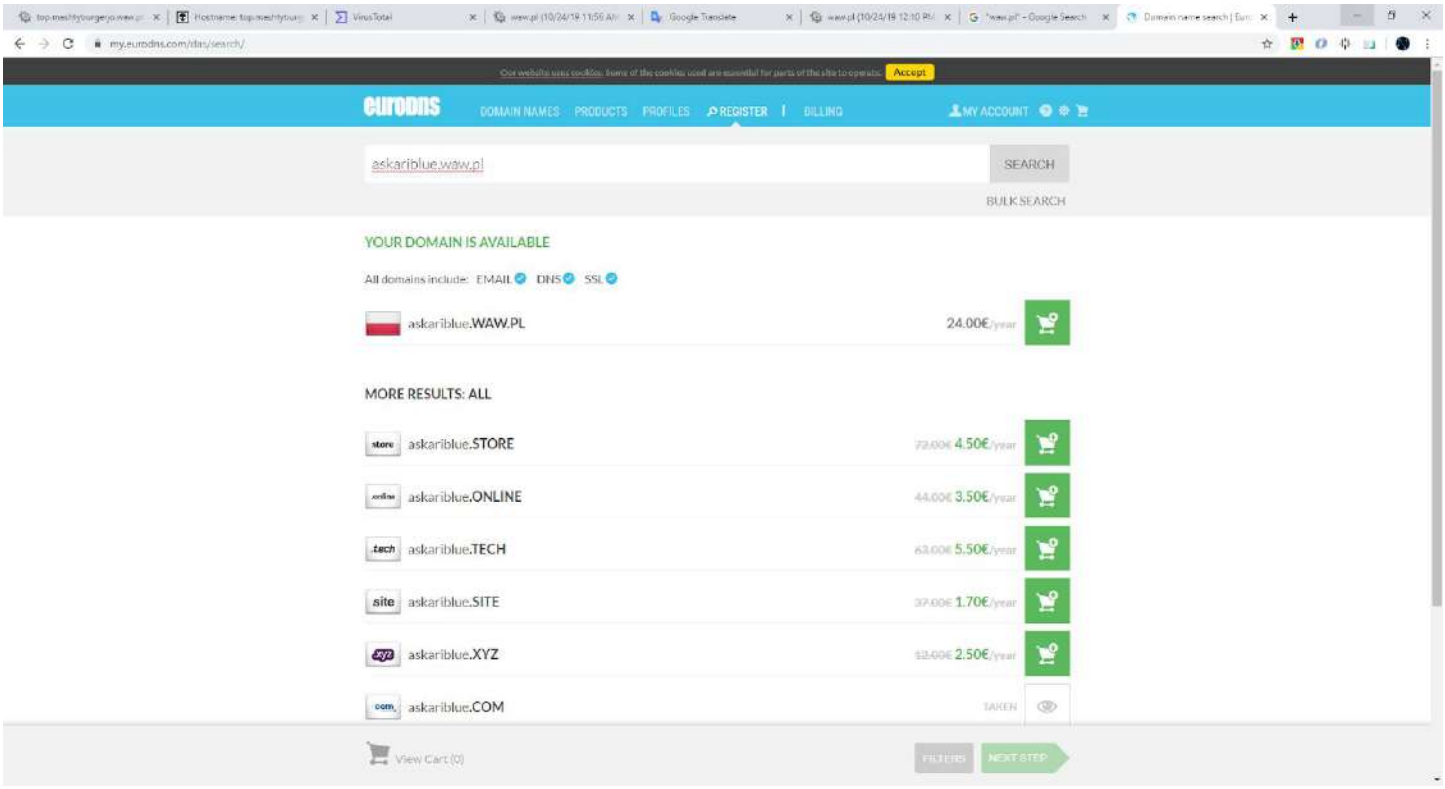
Original source: agenttesla[.]com

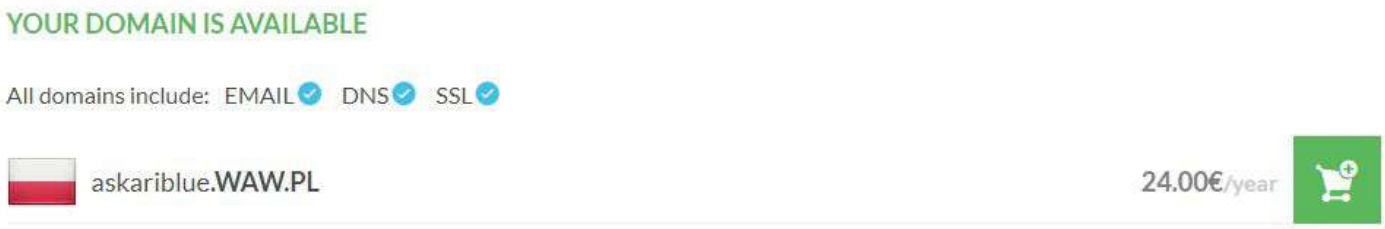
Investigation with an IOC

The investigation begins with a C2 domain address. Such addresses can be acquired post an incident response, as part of intelligence or obtained from a list on one of the many threat exchanges. This exercise will use the following domain IOC (Indicator of Compromise):

top.mashtyburgerjo.waw[.]pl

This IOC was highlighted as a Remcos RAT C2 from a Threat Exchange. On initial inspection, the domain *waw.pl* is available as a suffix with subdomains purchased for 24.00EUR/year. Given the volume of malicious subdomains found within *waw.pl* and naming patterns such as **top**.mashtyburger**jo**.waw[.]pl and **top**.multigaming**jo**.waw[.]pl it indicates a script has been used to generate the domain names.





What is Dynamic DNS?

The IOC example used throughout this guide is speculated to be using dynamic DNS, as do a large proportion of C2 RATs. Services such as DuckDNS or DDNS offer legitimate dynamic DNS services to aid network addressing. As an example, the website *www.huntingrats.com* is hosted from a home PC. Every time the PC is connected to the internet, the ISP (Internet Service Provider) assigns a new IP address for the website *www.huntingrats.com*. This new address must be updated to reflect the new IP address and Dynamic DNS services are ideal for such scenarios.

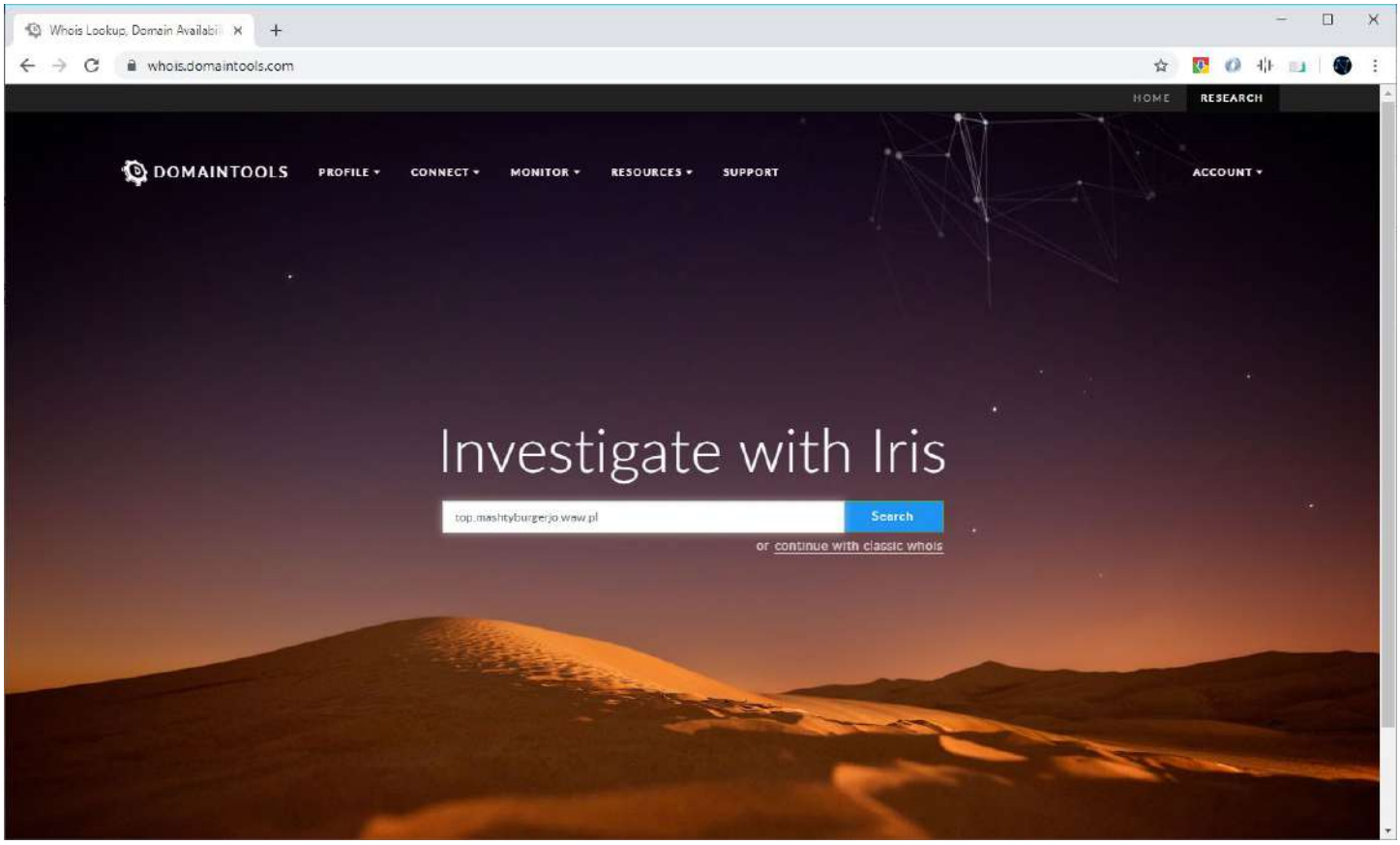
This service can be used for nefarious reasons, a threat actor uses an online hosting service for their C2. Often these domains are taken down by an ISP or Law enforcement as they are inevitably flagged for criminal activity. Subsequently the threat actor will move the C2 to a new location. The threat actor requires a method to inform all victim machines to connect to the new C2 location and like before, Dynamic DNS is ideal.

Many RAT operators can be classed as *script kiddies*. A term used for a *hacker* who has limited understanding of the mechanics of the tools they use. Criminal *script kiddies* can become very reliant on CaaS. As you'd expect, *script*

kiddies often make mistakes and it's OPSEC (operational security) failures that an investigation is searching for. One typical mistake by threat actors, is running the dynamic DNS service from their own machine prior to using a VPN or proxy.

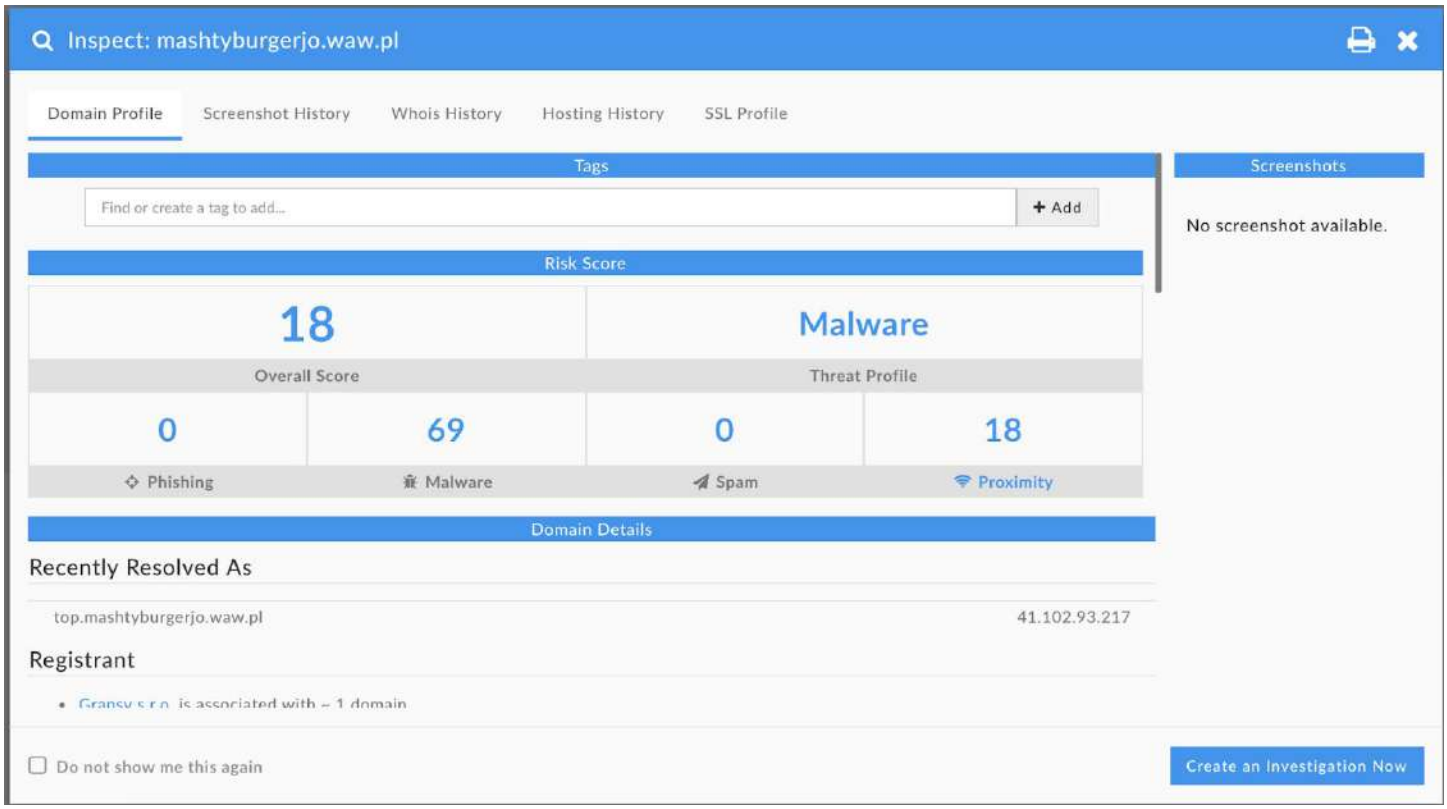
Hunting Guide

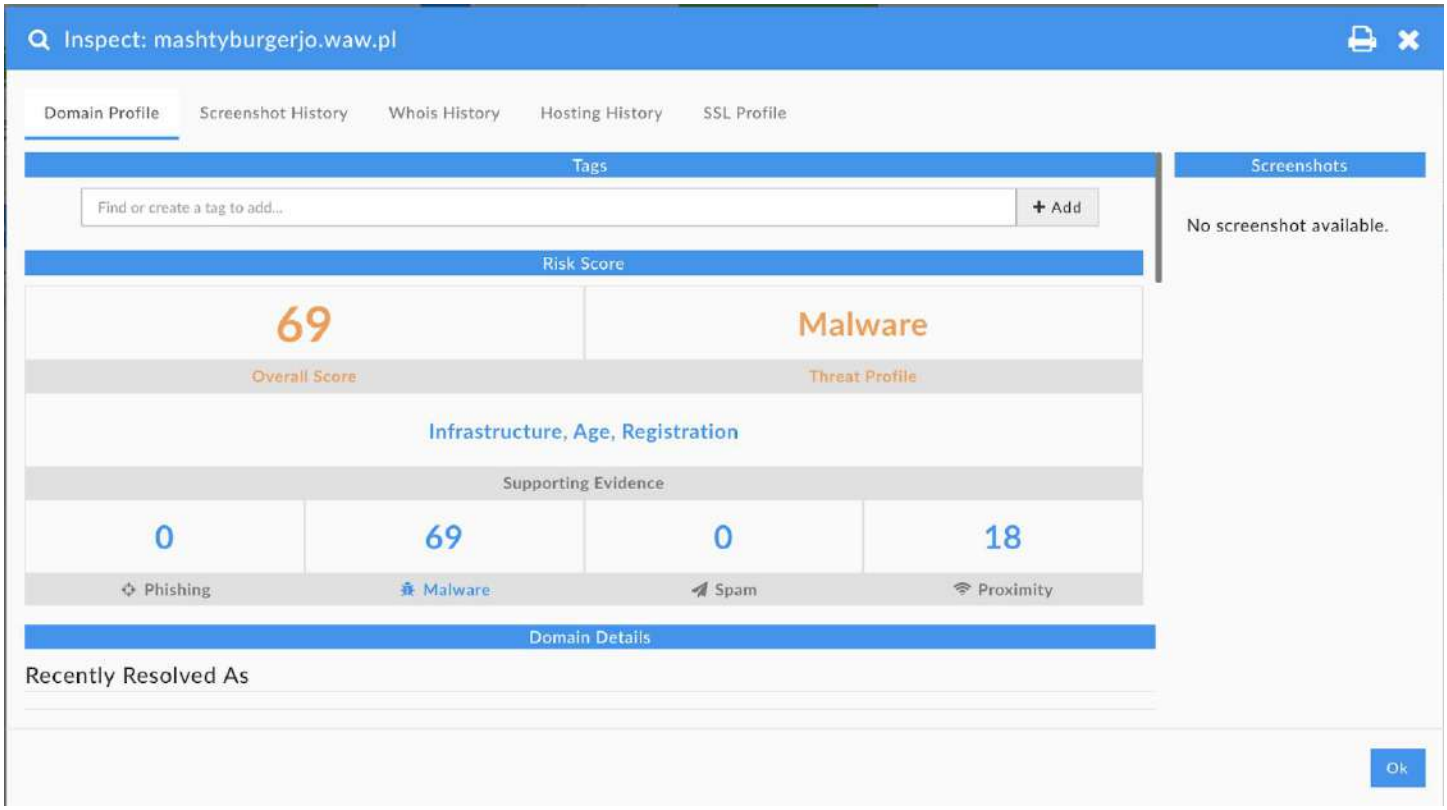
1. Open a browser, navigate to research.domaintools.com and login.
2. A search bar will be presented.
3. The search bar will direct requests to Iris which is DomainTools' investigation platform.
4. Enter the domain IOC into the search bar and click **search**.



Example: *top.mashtyburgerjo.waw.pl*

5. A print-friendly and PDF Inspect View will appear. This view provides a quick overview of the artifact in a printable form. Click **Create an Investigation Now**.



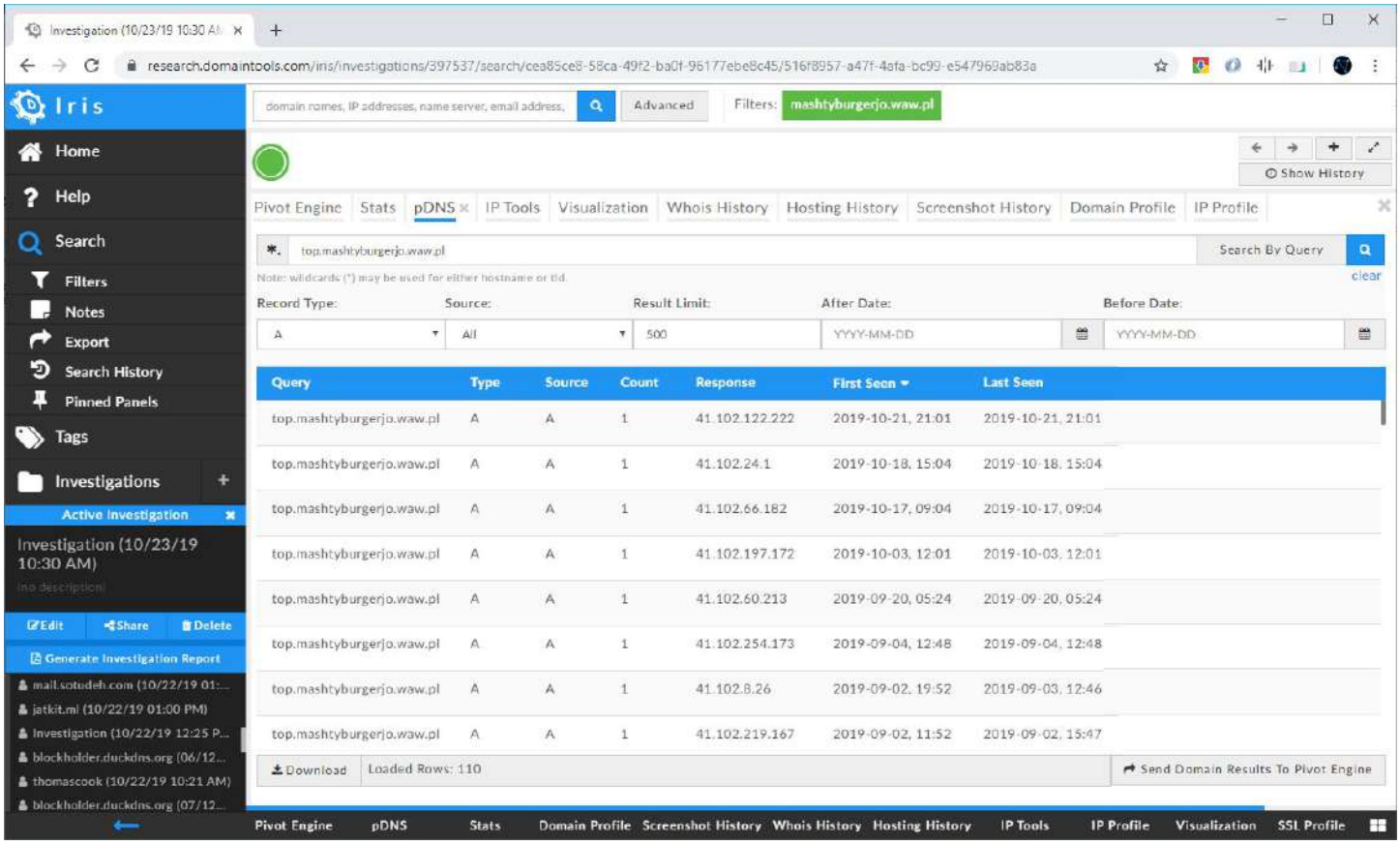


6. The Iris workspace will appear, here is an overview of each panel:

a. Across the top is the **search and filter bar**. Enter the IOC values to query and further filter with additional values, such as email addresses.
b. The next section down is the **search history** display. This tracks an investigation and allows analysts to quickly go back and forth throughout the investigation.
c. On the left is the **navigation bar** that provides additional controls, including those outside each investigation.
d. The main area contains the **data panels**. Here are multiple panels to view information and further an investigation. Each panel within can be altered, removed or added independently of others.

For a quick visual walk through of Iris, visit: https://www.domaintools.com/resources/user-guides/iris

7. Select the **pDNS** tab from the main area.

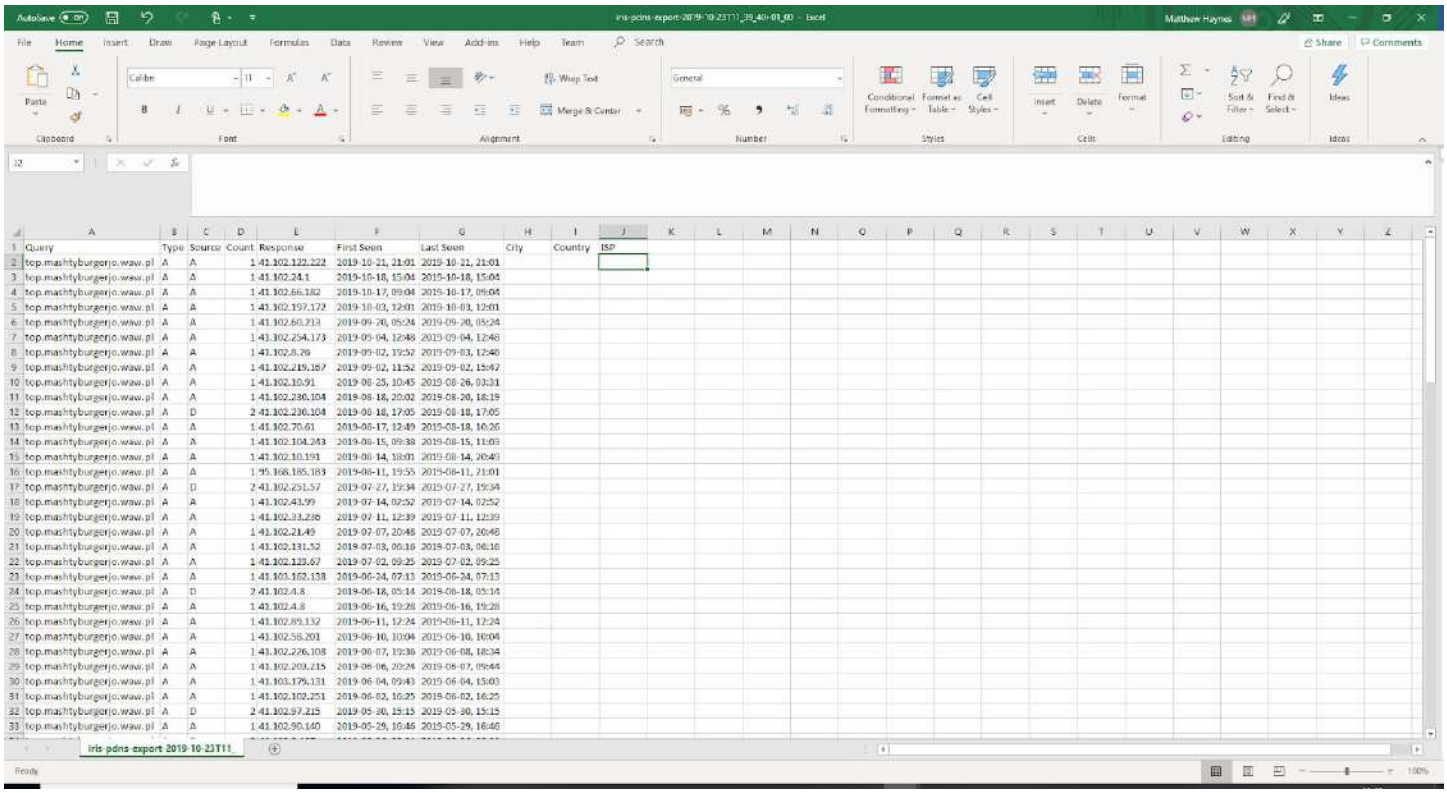


8. The pDNS tab shows the passive DNS records of the queried artifact. Within the main panel are the following headers:
    1. IOC queried
    2. DNS record type. This can be one of the following:
        a. A
        b. AAAA
        c. NS
        d. SOA
        e. MX
        f. CNAME

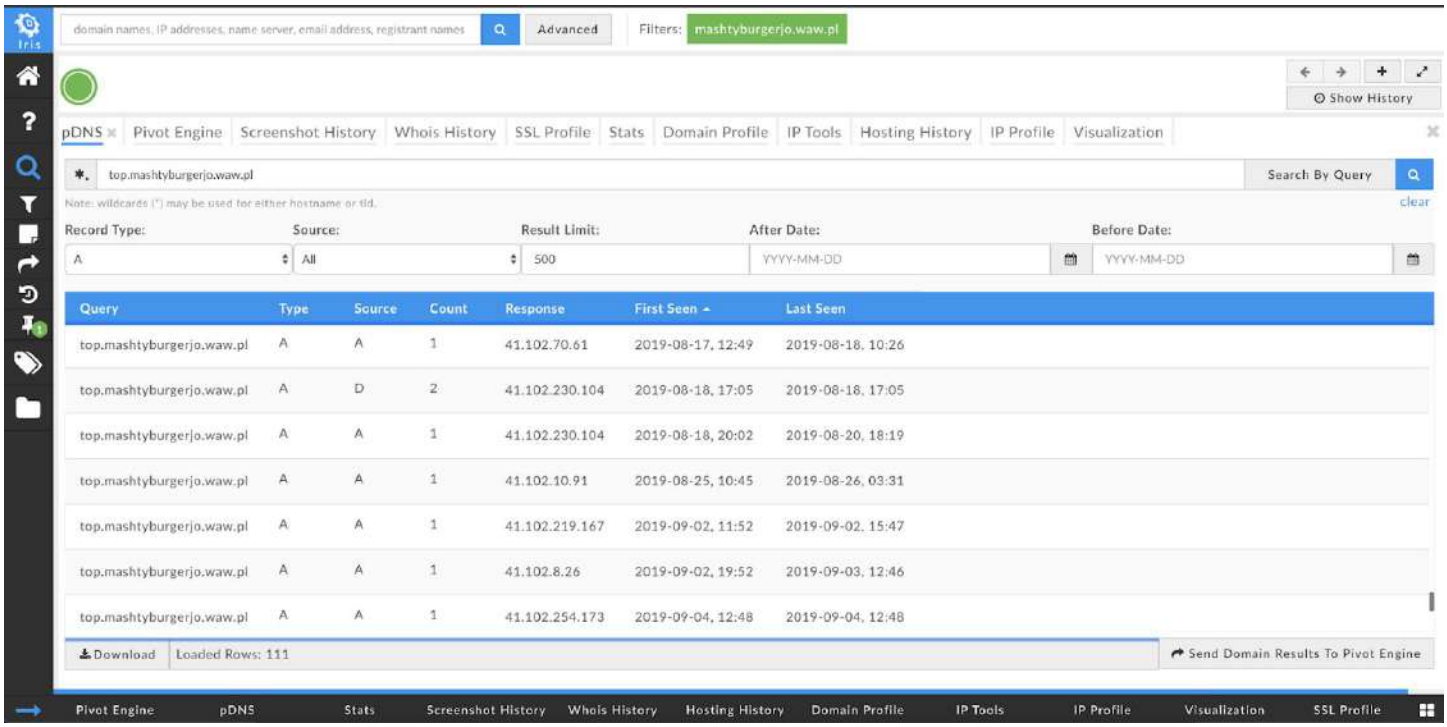
   g. TXT
3. Source
4. Count
5. Response. This is typically the IPv4 address of the queried domain IOC.
6. When it was first seen
7. When it was last seen

Different elements support varying investigations. Such that a particular NS (Name Server) may be under criminal control or a pattern indicator of a threat actor's behaviour. Records such as MX (Mail Exchange) identify mail services are or have been present, while TXT records can supply various indicators of activity. Knowing when an artifact became active can further support investigations on how far malicious activities may have occurred and how far an investigation may be required to trawl back logs. By leveraging various elements strengthens the success of an investigation.

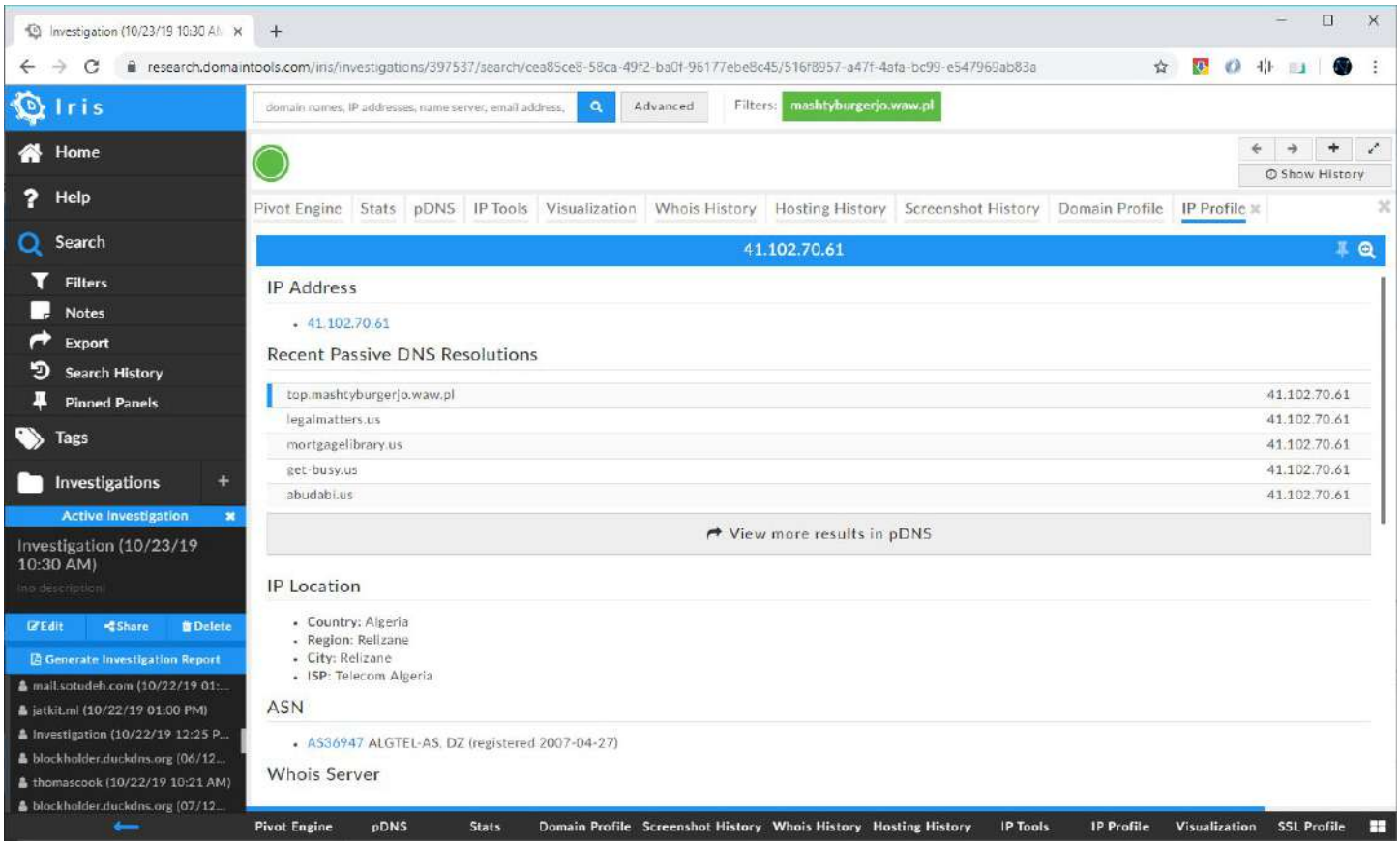
9. Download the full dataset and correlate the information within a spreadsheet processor. Select **download** from the bottom of the page to acquire the file.
10. Open the file in a spreadsheet processor. The example uses Microsoft Excel, but other programs such as LibreOffice Calc will suffice.
11. The data will mirror what was observed in the pDNS tab; Query, Type, Source, Count, Response, First Seen, Last Seen.
12. In row 1 for columns H, I, and J, enter **City**, **Country**, and **ISP** respectively.



13. Leave the spreadsheet open and put it to one side, then go back to your browser with DomainTools Iris.
14. Find the first response (i.e. IPv4 address), right click and select **IP Profile**.



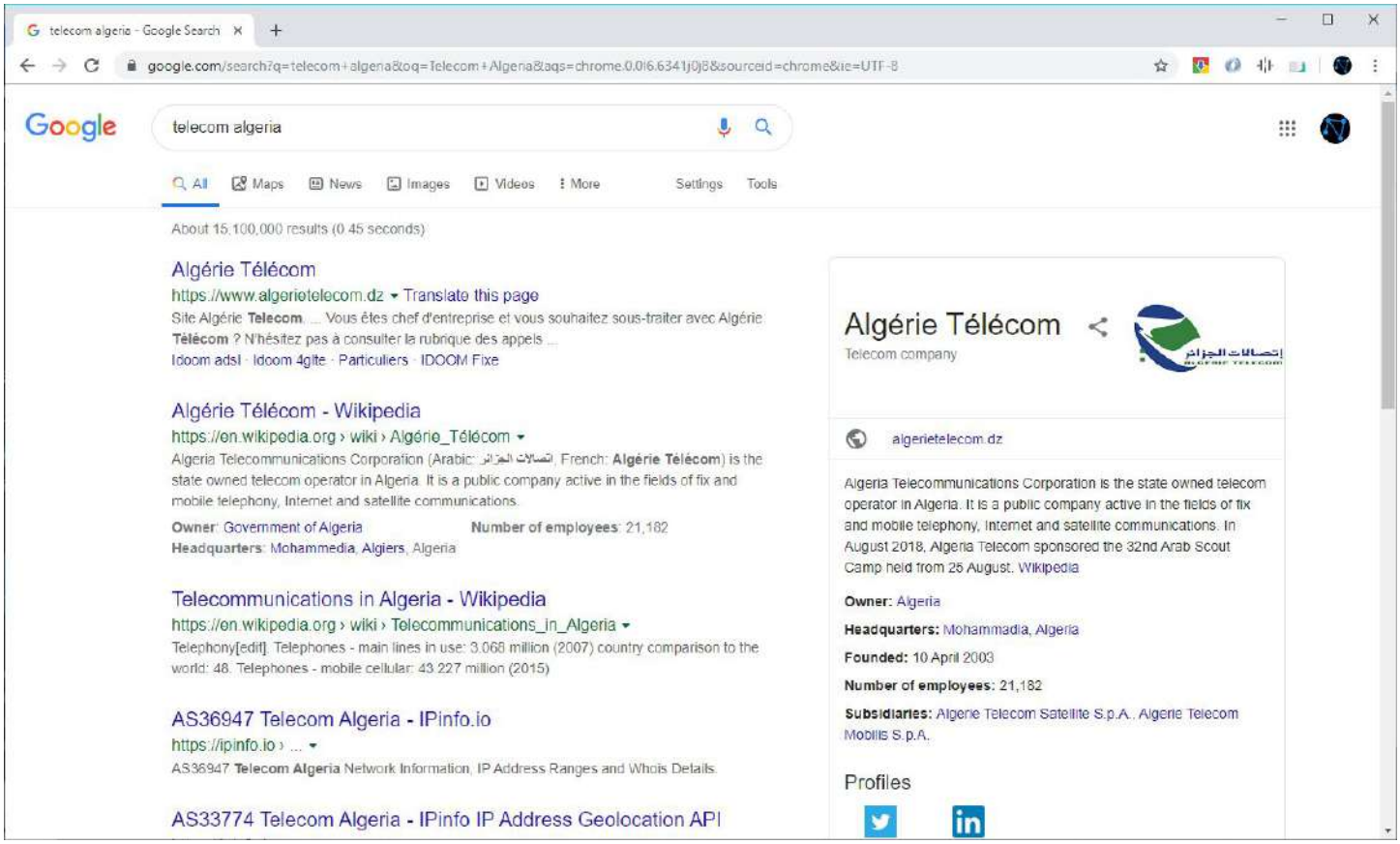
15. This will navigate to the IP Profile tab using that IPv4 response.



16. The panel is broken down into six headers:
    a. **IP Address**. This is the artifact being queried.
    b. **Recent Passive DNS Resolutions**. These are snapshots of DNS A records that have been used by this IPv4 address.
    c. **IP Location**.
    d. **ASN**. The autonomous system number is a unique number assigned to an autonomous system (AS) by the Internet Assigned Numbers Authority (IANA).
    e. **Whois Server**. The authoritative node that owns the whois record.
    f. **Whois Record**. Information pertaining to the current registrant.
17. Capture the **Country**, **City** and **ISP** from the **IP Location** section and populate your spreadsheet.
18. Click back on your browser to return to the pDNS list.
19. Right click the next unique response (IPv4 address) and select **IP Profile**.
20. Repeat the steps until all addresses are captured. **NOTE:** Analysts familiar with IPv4 addressing, can note IPv4 blocks belong to the same city, country and ISP. This will help speed up the processing of information.
21. Improve the cosmetics of the list, such as adding a query filter, colours and use visual styles.

Query	Typ	Sourc	Cou	Response	First Seen	Last Seen	City	Country	ISP	Comment
top.mashtyburgerjo.waw.pl	A	A	1	41.102.122.222	2019-10-21, 21:01	2019-10-21, 21:01	Relizane	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.24.1	2019-10-18, 15:04	2019-10-18, 15:04	Tiaret	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.66.182	2019-10-17, 09:04	2019-10-17, 09:04	Oued Rhiou	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.197.172	2019-10-03, 12:01	2019-10-03, 12:01	Oued Rhiou	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.60.213	2019-09-20, 05:24	2019-09-20, 05:24	Chlef	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.254.173	2019-09-04, 12:48	2019-09-04, 12:48	Tissemsilt	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.8.26	2019-09-02, 19:52	2019-09-03, 12:46	Oued Rhiou	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.219.167	2019-09-02, 11:52	2019-09-02, 15:47	Sougueur	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.10.91	2019-08-25, 10:45	2019-08-26, 03:31	Chlef	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.230.104	2019-08-18, 20:02	2019-08-20, 18:19	Theniet El Had	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	D	2	41.102.230.104	2019-08-18, 17:05	2019-08-18, 17:05	Theniet El Had	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.70.61	2019-08-17, 12:49	2019-08-18, 10:26	Relizane	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.104.243	2019-08-15, 09:38	2019-08-15, 11:03	ain Deheb	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	41.102.10.191	2019-08-14, 18:01	2019-08-14, 20:49	Chlef	Algeria	Telecom Algeria	All
top.mashtyburgerjo.waw.pl	A	A	1	95.168.185.183	2019-08-11, 19:55	2019-08-11, 21:01	London	United Kingdom	Leaseweb Uk Limited	Hosting provider
top.mashtyburgerjo.waw.pl	A	D	2	41.102.251.57	2019-07-27, 19:34	2019-07-27, 19:34	Boukadir	Algeria	Telecom Algeria	All

22. Once complete, Analysts may begin to notice patterns. Certain countries are used more frequently due to their large datacentres, high speed links, low hosting costs and bulletproof hosting. Countries such as Germany, the Netherlands, France, the United States of America, and Russia will likely appear. Any country in the world can legitimately host services, so further information is required to identify probable concerns.
23. Research each ISP from the list to determine what they offer. For example. business connectivity lease, domestic internet, hosting services.
24. Search the ISP in a search engine and note what services are being offered.



25. Some ISPs may prove difficult and offer multiple services. For example, **telecom Algeria** which is a backbone telecoms provider is highly likely to provide the primary infrastructure to alternative smaller

providers which in turn offer an array of services. Analysts will note what they can and later hypothesise on gaps.

26. There is now a lot of data and the following is noted of the investigation:
    a. The domain is being used as a Remco RAT C2.
    b. The address has been operating out of varying IPv4 addresses.
    c. It is known which addresses are using hosting providers and which are not.

Analysis

Once data is collated and analysed, analysts should develop one or more hypothesis. Such a hypothesis may include:

1. Addresses used by domestic providers are an indication of an infected victim and the threat actor is operating their C2 from a victim.
    a. All addresses are either compromised or owned by the threat actor.
    b. None indicate the operator's geographical location.
2. Addresses used at hosting providers are hosting malicious services operated and owned by the threat actor and/or are proxy addresses used to route traffic to the C2.
    a. Devices at these addresses maybe compromised services, once benign but now used to host malicious services.
    b. Addresses used at domestic providers are the direct endpoint of the threat actor.
    c. A failure in OPSEC (Operational Security) has occurred and the dynamic DNS service which exists on the threat actor's device has updated the address prior to a VPN and/proxy being used. This indicated the geographical location of the Threat Actor.
3. A threat actor is using the domestic addresses to mislead security researchers.
    a. While this aligns to option 2, motivations are different.
    b. This approach is not by design but by technique (TTP).
4. Unknown.

Intelligence is a team sport and requires further scrutiny. The following are the reasoning behind each hypothesis and encourage additional review:

1. This is a hypothesis that was raised during an intelligence workshop. Participants determined the addresses could have been from victim machines. But this is very unlikely. Knowing what we know about RATs, a victim is rarely used as a C2. While some have the capability to act as a reverse proxy, this is typically used to tunnel into a local network. In addition, the dynamic address would have to be updated to match the victim, possible but finicky with little value gained. As well as the added risk the victim will go offline at any time and cause loss of control to the botnet.
2. This remains the most likely, with an assessment of highly likely. It is expected behaviour to host a C2 from a hosting provider due to redundancy, good latency and overall management ease. This too is true for hosting providers acting as a VPN or proxy gateway, providing all the benefits mentioned above as well as increasing anonymity. A small quantity of domestic addresses all residing in a similar location further strengthens the argument OPSEC has occurred and the threat actor exists in this geographical location. A large quantity of domestic addresses indicates the threat actor disregards OPSEC entirely.

- While this hypothesis is possible, it is almost uncertain. The majority of RAT operators target the lowest hanging fruit, such as home users or small businesses. State-sponsored threat actors have been reported to use RATs, but this is rare due to high risk of detection.
- Cumulatively options 1-3 has significant potential, which leads me to determine while there is the possibility the correct scenario has not been theorised, it is very unlikely not one of the first three options. We do not know what we do not know and therefore, this will remain as a catch-all and on this occasion will provide a generous 5% likelihood.

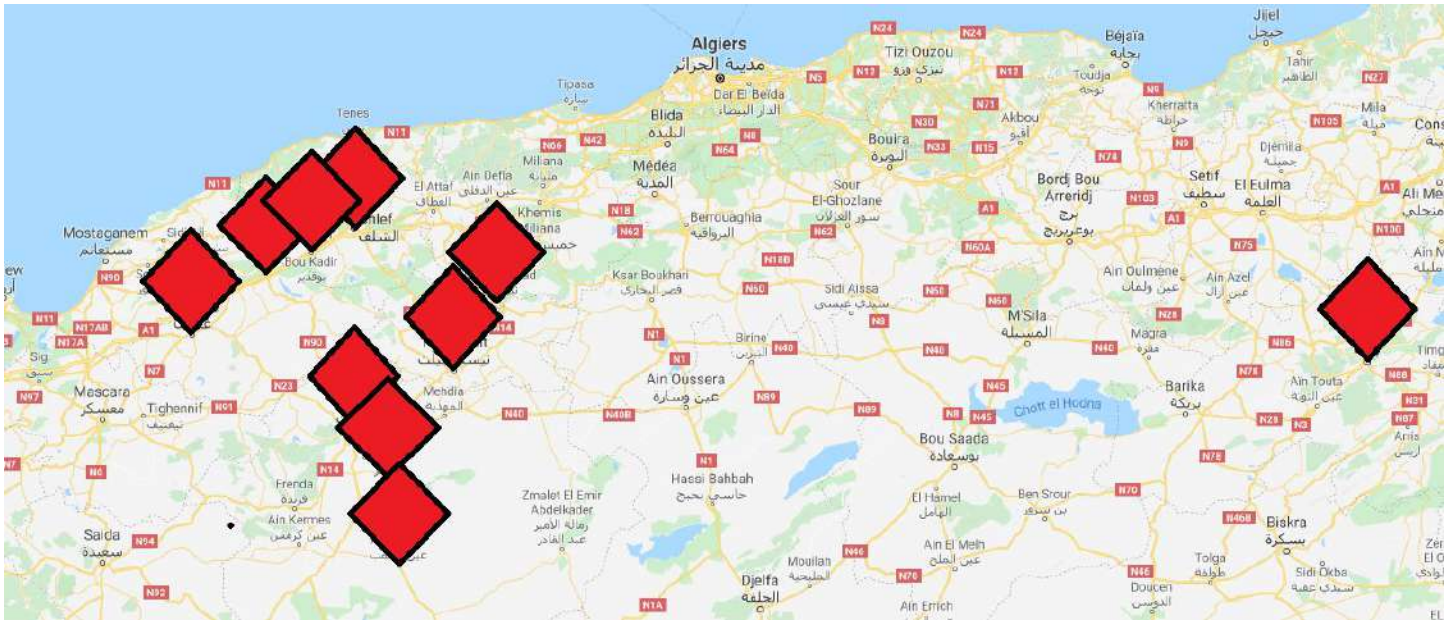
Further evidence is required for any investigation. Analysts are encouraged to answering such questions to aid their investigation greatly:

1. Who is the malware targeting?
2. What type of malware is it?
3. What threat groups typically use this malware?
4. What further evidence from the campaigns can you find? i.e. phishing emails/websites.
5. What potential goals is the threat actor trying to accomplish?
6. Would you consider the threat actor to be advanced? If so/not, then why?
7. What might be the motivations behind the threat actor?

Further Analysis

The example IOC was used by a Remco RAT which is typically used by unsophisticated threat actors. It is used for its ease and can be acquired for free. Therefore, the investigation will focus on individuals or smaller groups of cybercriminals who fit this modus operandi.

Map of Northern Algeria

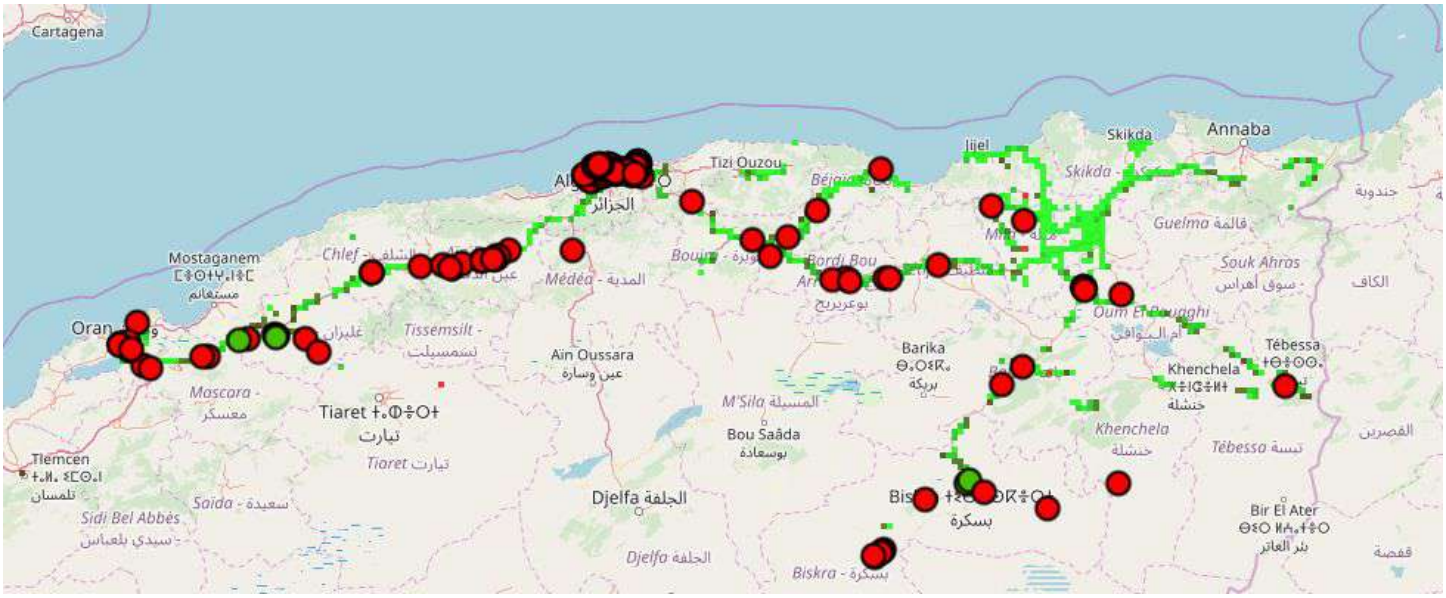


Geolocation of IP addresses laid over a map of Algeria

Mapping the geolocations of the IPv4 addresses, a distinctive area within Algeria begins to form. It is important to note that geolocation can be misleading as telecoms can route traffic through varying endpoints due to a number

of reasons, such as latency and traffic use. As an example, when end users visit certain websites or services, it can incorrectly display they're in a different part of the country.

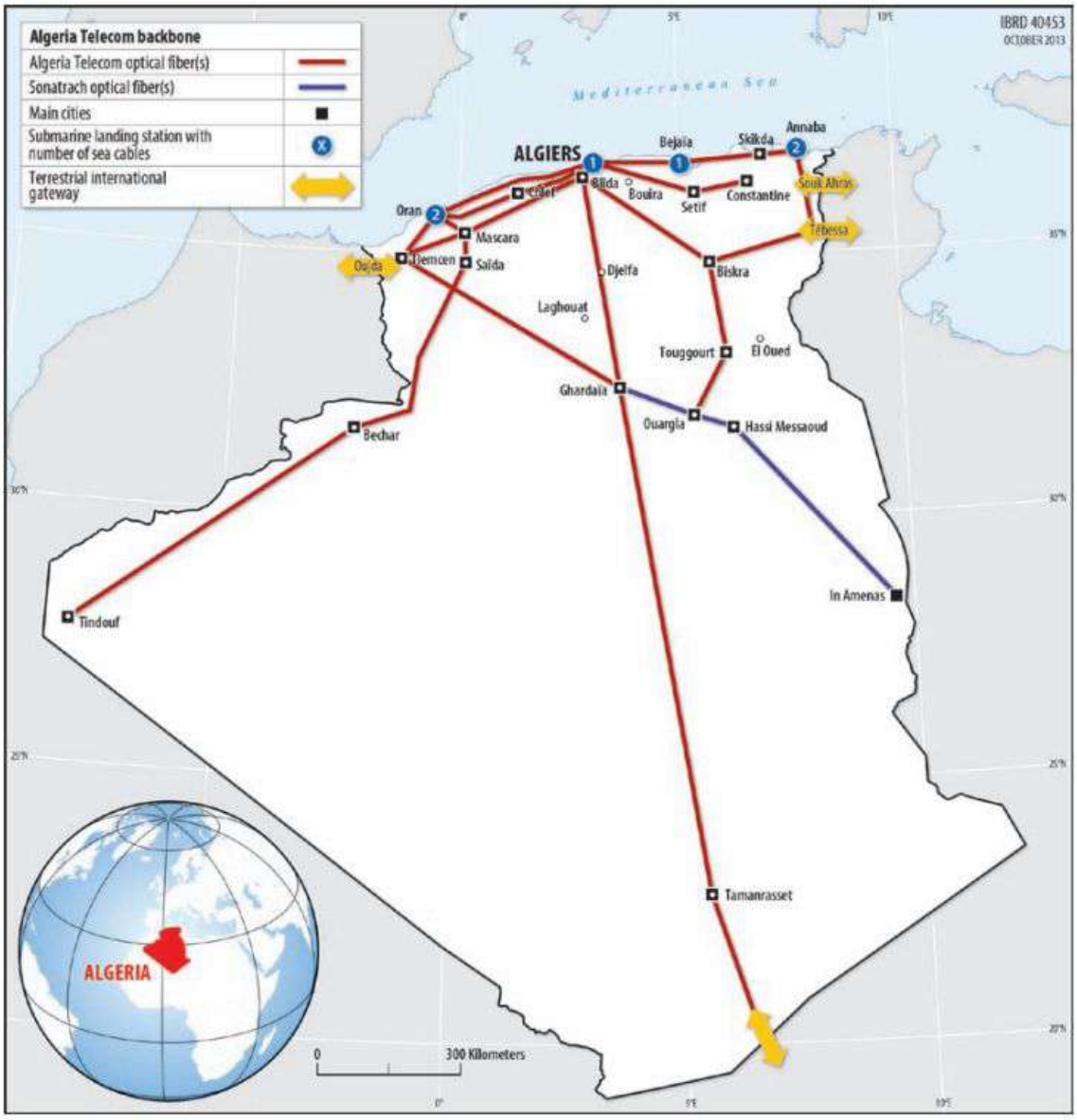
2G - Nedjma



3G – Nedjma

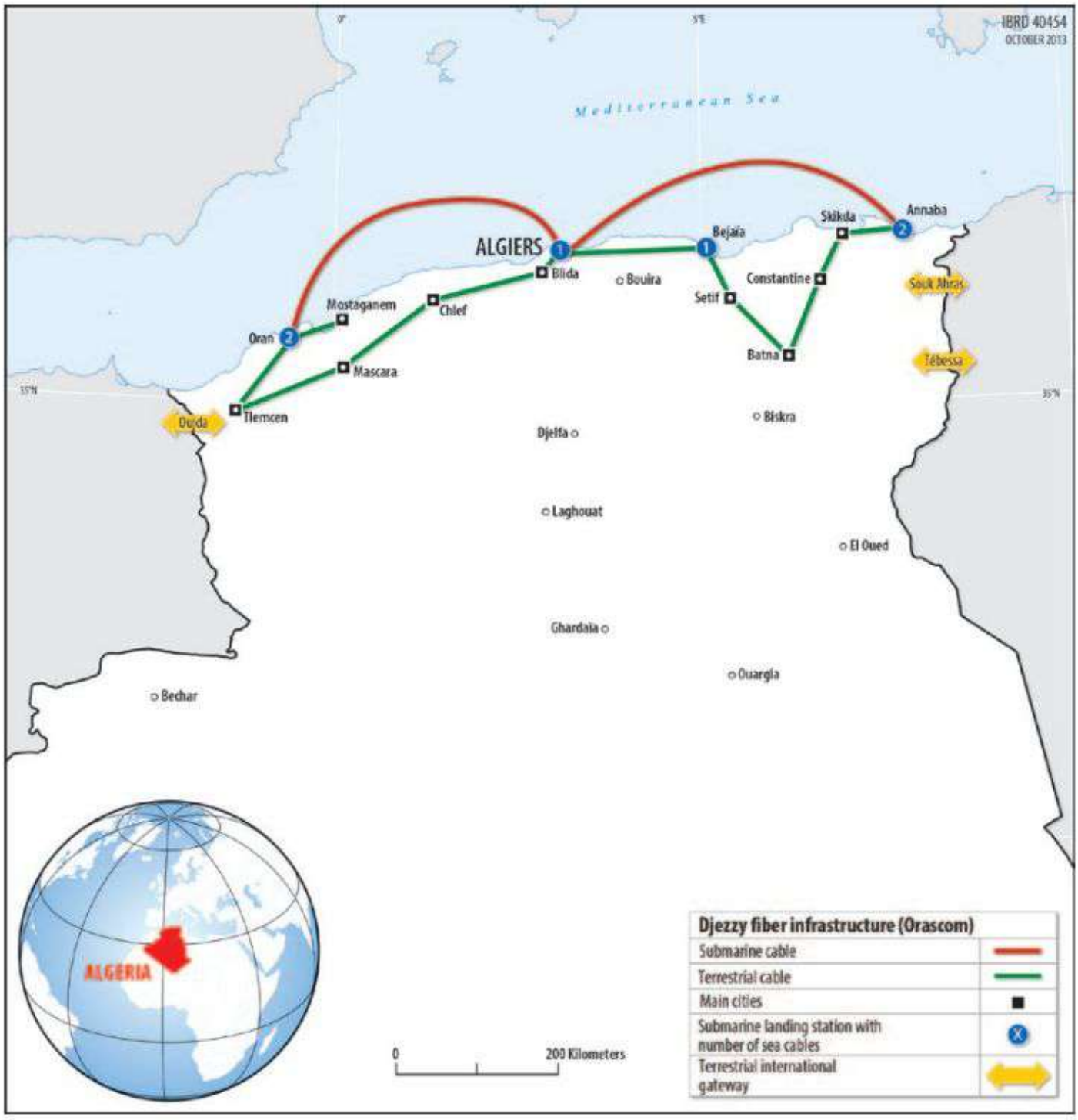
Source:
https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/Broadband_MENA_annexes.pdf

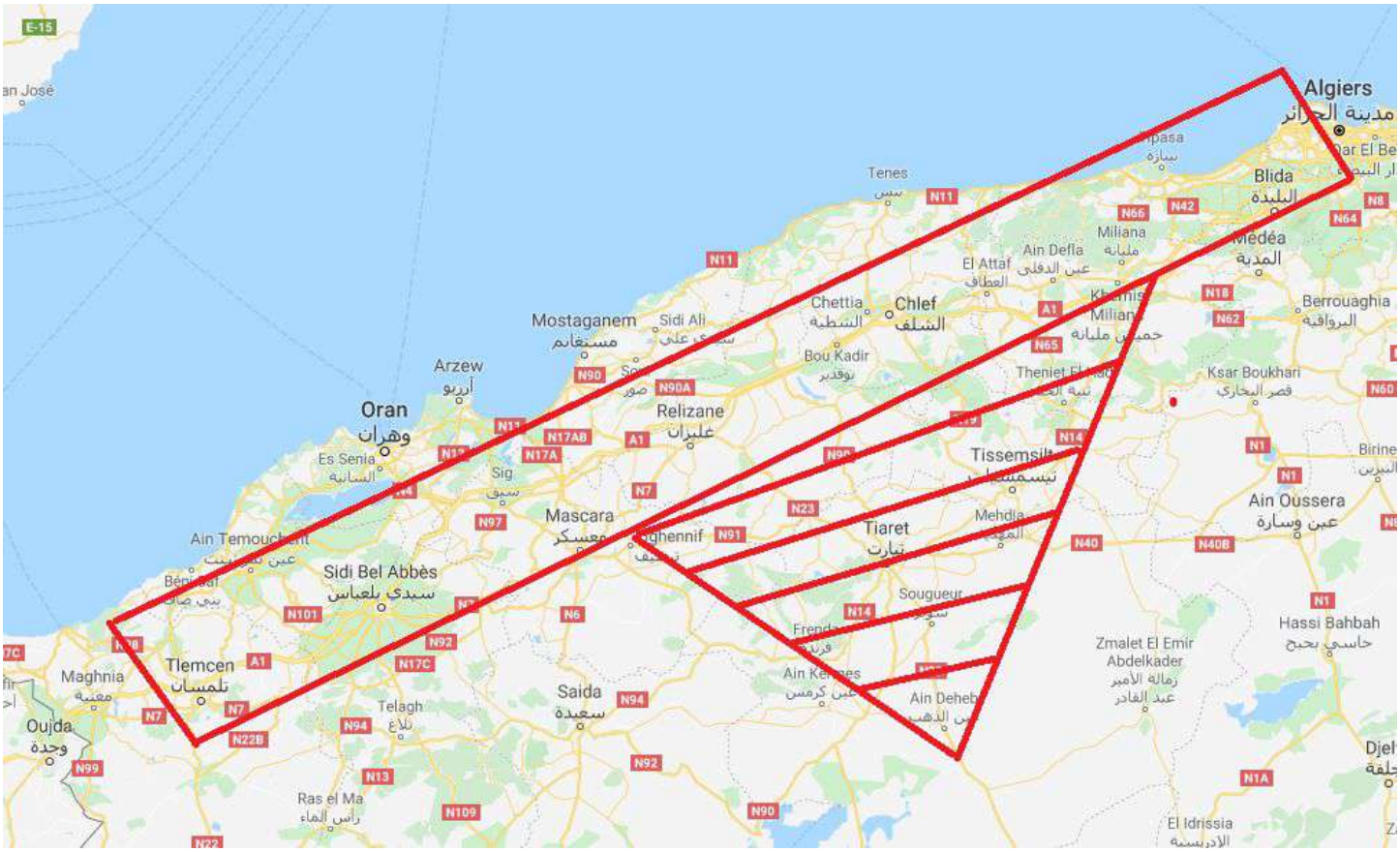
Map A.19 Main Links of Algeria Telecom's National Fiber Backbone



Source: World Bank.

Map A.20 Main Links of Djezzy's National Fiber Backbone





Algeria's telecom infrastructure has main lines that feed between the major cities of Algiers and Oran. Due to the infrastructure existing within the red rectangle between Algiers and Oran as an infrastructure backbone of Algeria, it is expected behaviour for the majority of traffic within this region to exit here.

However, many of the IPv4 addresses recorded also exited within the hatched triangle that is centred on Tiaret, adjacent to the red rectangle and goes out past Ain Deheb. Therefore, this indicates that any IPv4 addresses originating from this location more likely exists physically within this area. It must be noted that further information is required to build confidence in this hypothesis or debunk it if appropriate.

Culture Analysis

Algeria cybercrime as one of its largest concerns, with over 30% of computers in the country infected with malware. It has been identified as the country with the lowest rating for cybercrime preparation and legislation that reflects this new domain. However, little is raised regarding cybercrime when compared to other countries such as Nigeria which is notorious.

Identifying a threat actor in Nigeria can provide additional understanding into their motives, techniques and end goal. Given the similarities in this Algerian example to that of operators within Nigeria, it is assessed with moderate confidence the threat actor is likely unsophisticated, focusing on easily exploitable targets and accepting of low currency theft. The route of payment remains unknown. Organised entities in Nigeria are well structured to use mule networks in other countries but there remains an even chance this threat actor is using similar routes. Further investigation is required to identify fraudulent currency flows.

Summary

Businesses, organisations and individuals are under attack. Threat actors are increasing sophistication, frequency, and volume of strikes. Cyber security professionals are required to adapt and develop to changing threats of the future. And in order to do so, they must understand their enemy to defend effectively.

The investigation helped demonstrate a specific threat. By identifying a C2 address and using it as the focal point of an investigation, a threat actor can be hunted and analysed. During the demonstration, data was collated from various sources, analysed, and a hypothesis was developed on the likelihood of the geographical location of the attacker.

The goal, however, is not to catch the perpetrator. Law enforcement have that responsibility and importantly jurisdiction. And unfortunately for Law enforcement, further work is required. In addition to the substantial difficulties of operating across borders, such as legalities, they will be required to collect more data for analysis and to build confidence and corroborate current findings.

As cyber security professionals not associated with Law enforcement, the objective is to understand the enemy. Continuing on from the example, practitioners are encouraged to build threat profiles, understand capabilities, motivations and just as important, their limitations. To go further, identify where threat actors are not winning and determine what they must do to win. What TTP must they develop that lies within their capabilities? These are just some of the paths of investigation and analysis that can be taken. By identifying probable new avenues an attacker may take, provides the opportunity to assess their next move before they take it.

The next steps for many may be to reduce the difficulty of this example. The task of manually populating a spreadsheet is time consuming and ideal for automation. As an example, DomainTools offers an API that can greatly speed up the process of data collection, reducing an analyst's time and cost.

Analysts should repeat this approach to data analysis and hypothesis accordingly. They should identify patterns, research typical criminal equipment and further theorise the benefits or limitations threat actors have. By understanding what a threat actor needs to do to adapt and subvert current defence controls, an analyst can counter future attacks. By performing such types of investigations, defences will greatly strengthen, and criminals will be more easily identified.

ASKARI BLUE

Cyber Security

This white paper was written as a follow-up to the sold-out UK-wide 2019 workshop titled: 'WTF is CTI?' Designed for the Cyber Security community, the workshop and associated content aim to raise awareness of the field of Threat Intelligence and its benefits.

Here at Askari Blue we specialise at empowering decision makers, from SOC analysts to senior stakeholders. By delivering effective focused intelligence, we enable an organisation to enhance their defences and safeguard against cyber threats.