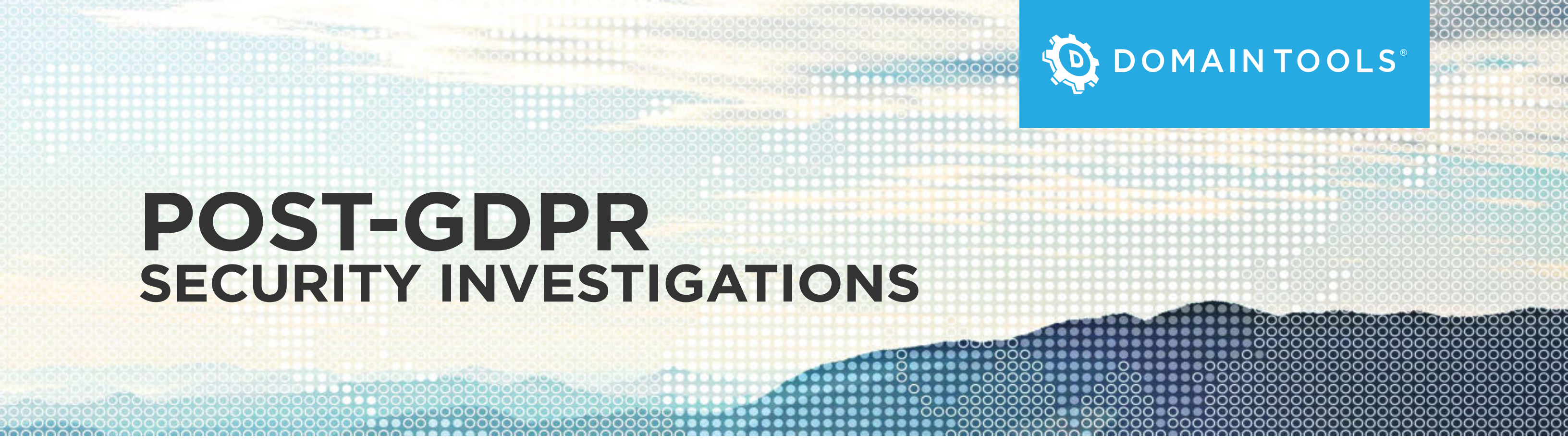


DOMAINTOOLS®

POST-GDPR
SECURITY INVESTIGATIONS

In May 2018, the General Data Protection Regulation (GDPR) went into effect and subsequently altered the way that cybersecurity analysts are able to perform their investigations. Where, previously, connections between incidents and attribution had often been tied to publicly available Whois data, there was now the word REDACTED hindering those linkages.

However, not all was lost with the implementation of GDPR and there are still numerous methods by which to conduct an incident investigation. In this report, we will identify four methods by which threat researchers can perform analysis using techniques that were not impacted by GDPR regulation, including Risk Score within DomainTools Iris platform, non-registrant based connections and attributions, OSINT-based methodologies, and information sharing.

Using these and other methods of investigations, analysts can still produce timely and relevant intelligence to defend their organizations, despite the roadblocks posed by GDPR.

4 POST-GDPR INVESTIGATION METHODS

In this report, we will identify four methods by which threat researchers can perform analysis using techniques that were not impacted by GDPR regulation.

RISK SCORE WITHIN DOMAINTOOLS IRIS PLATFORM

NON-REGISTRANT BASED CONNECTIONS & ATTRIBUTIONS

OSINT-BASED METHODOLOGIES

INFORMATION SHARING

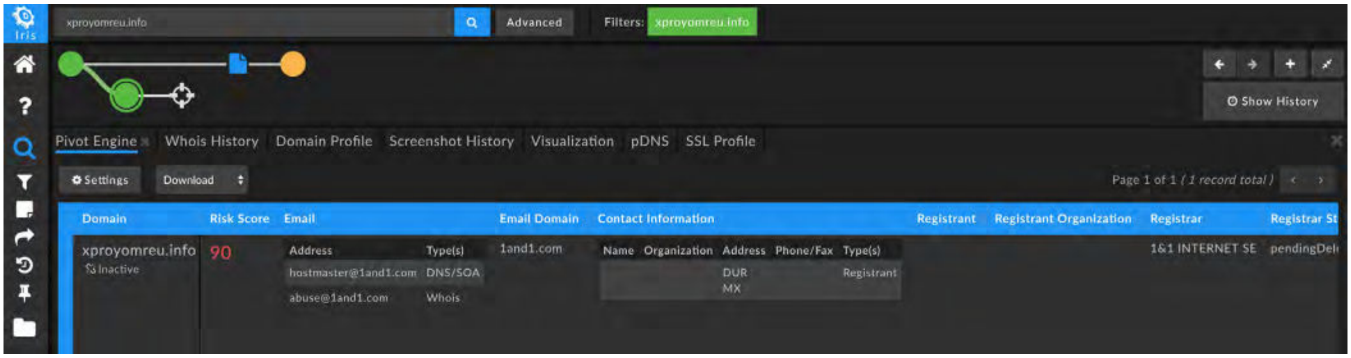
DOMAINTOOLS RISK SCORE

When conducting an investigation, it can be useful to determine the severity of an incident before spending a significant amount of time on analysis. Domain Risk Score can help give context and allow analysts to start off with an indication of how much attention they should pay to an indicator.

Drawing upon data points from more than 330 million current domains, Domain Risk Score predicts how likely a domain is to be malicious, often before it is weaponized. The score comes from two distinct algorithms: *Proximity* and *Threat Profile*. Proximity evaluates the likelihood a domain may be part of an attack campaign by analyzing how closely connected it is to other known-bad domains. Threat Profile leverages machine learning to model how closely the domain's intrinsic properties resemble those of others used for spam, phishing, or malware. The strongest signal from either of those algorithms becomes the overall Domain Risk Score.

DOMAINTOOLS RISK SCORE (CONT.)

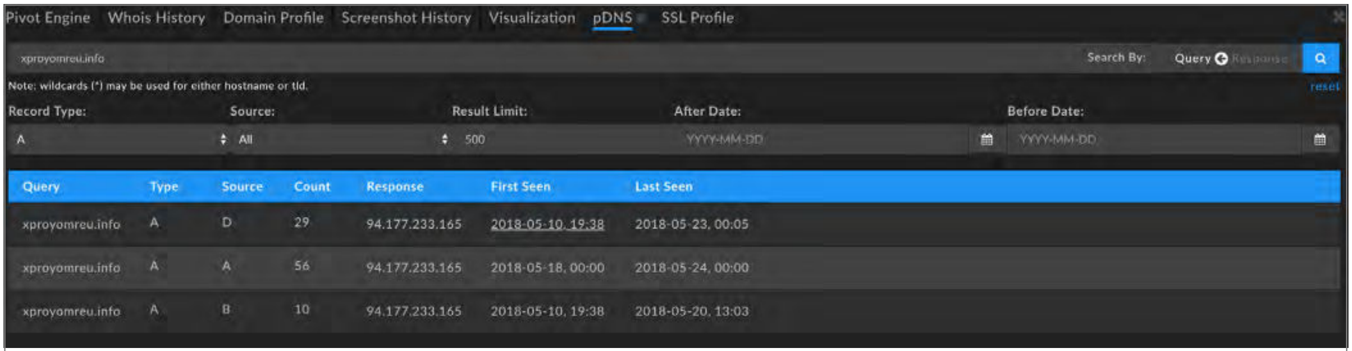
Domain Risk Score can be useful in identifying which domains warrant further research even in cases where little or no data is available about those domains. For example, during our research we came across a domain that was likely malicious, as it had a Domain Risk Score of 90 (domains that have a risk score of 70 or higher are considered suspect and warrant further research). There were no immediately obvious pivots or direct connections to malicious campaigns at first glance, but such a high Domain Risk Score indicated to us that this domain was worth a closer look.



Page 1 of 1 (1 record total)

Domain	Risk Score	Email	Email Domain	Contact Information	Registrant	Registrant Organization	Registrar	Registrar St
xproyomreu.info Inactive	90	Address — Type(s) hostmaster@1and1.com — DNS/SOA abuse@1and1.com — Whois	1and1.com	Name, Organization, Address, Phone/Fax, Type(s) Address: DUR MX — Type(s): Registrant			1&1 INTERNET SE	pendingDel

Reviewing the passive DNS records for this domain show an IP address that may be noteworthy.



xproyomreu.info

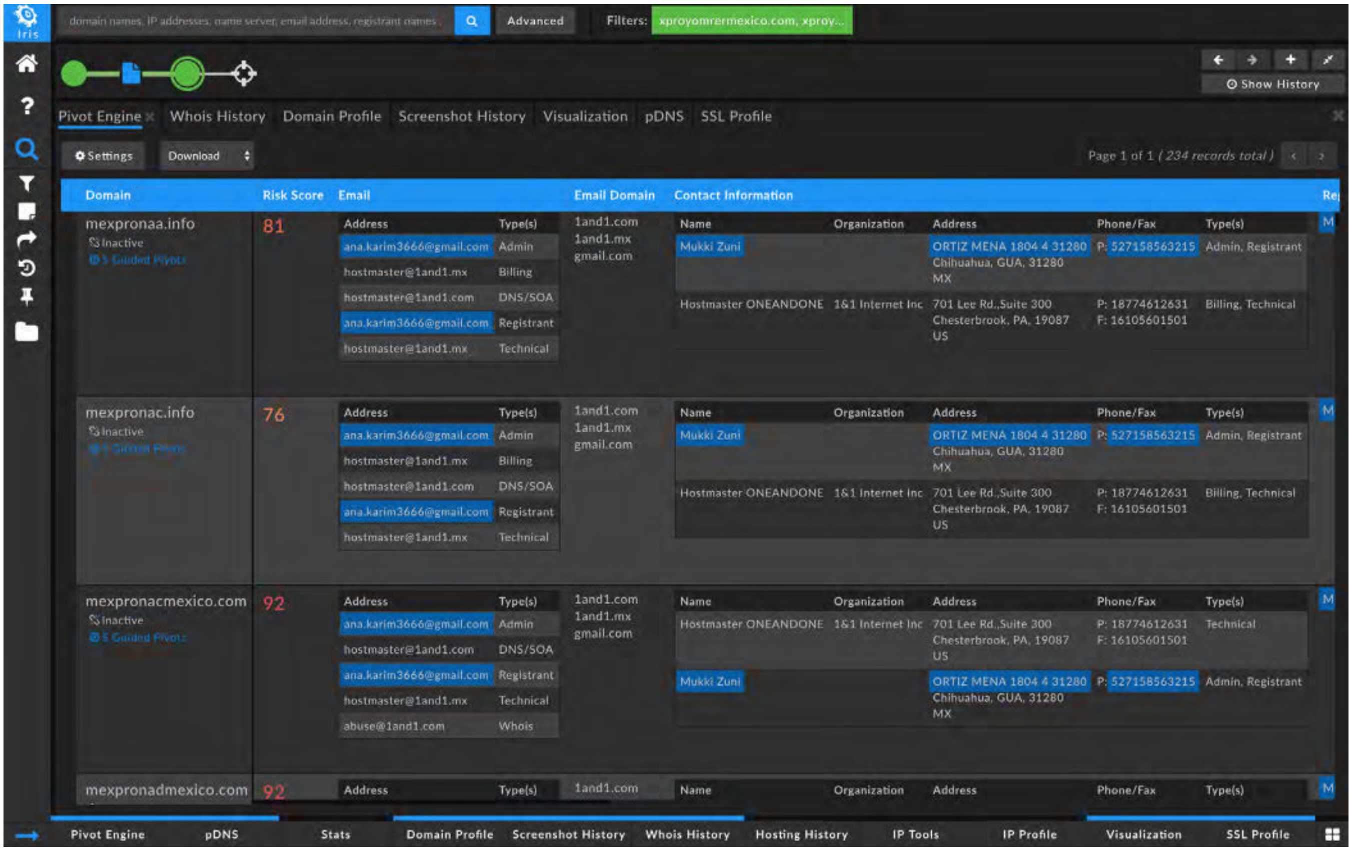
Note: wildcards (*) may be used for either hostname or tld.

Record Type: A
Source: All
Result Limit: 500
After Date: YYYY-MM-DD
Before Date: YYYY-MM-DD

Query	Type	Source	Count	Response	First Seen	Last Seen
xproyomreu.info	A	D	29	94.177.233.165	2018-05-10, 19:38	2018-05-23, 00:05
xproyomreu.info	A	A	56	94.177.233.165	2018-05-18, 00:00	2018-05-24, 00:00
xproyomreu.info	A	B	10	94.177.233.165	2018-05-10, 19:38	2018-05-20, 13:03

Pivoting on that IP, we can see that it has been associated with several domains, most of which also have high Domain Risk Score, indicating they too are likely malicious and may be a part of a campaign.

DOMAINTOOLS RISK SCORE (CONT.)



Domain	Risk Score	Email	Email Domain	Contact Information
mexpronaa.info Inactive 5 Guided Pivots	81	Address / Type(s) ana.karim3666@gmail.com / Admin hostmaster@1and1.mx / Billing hostmaster@1and1.com / DNS/SOA ana.karim3666@gmail.com / Registrant hostmaster@1and1.mx / Technical	1and1.com 1and1.mx gmail.com	Name / Organization / Address / Phone/Fax / Type(s) Mukki Zuni / ORTIZ MENA 1804 4 31280 Chihuahua, GUA, 31280 MX / P: 527158563215 / Admin, Registrant Hostmaster ONEANDONE / 1&1 Internet Inc / 701 Lee Rd.,Suite 300 Chesterbrook, PA, 19087 US / P: 18774612631 F: 16105601501 / Billing, Technical
mexpronac.info Inactive 5 Guided Pivots	76	Address / Type(s) ana.karim3666@gmail.com / Admin hostmaster@1and1.mx / Billing hostmaster@1and1.com / DNS/SOA ana.karim3666@gmail.com / Registrant hostmaster@1and1.mx / Technical	1and1.com 1and1.mx gmail.com	Name / Organization / Address / Phone/Fax / Type(s) Mukki Zuni / ORTIZ MENA 1804 4 31280 Chihuahua, GUA, 31280 MX / P: 527158563215 / Admin, Registrant Hostmaster ONEANDONE / 1&1 Internet Inc / 701 Lee Rd.,Suite 300 Chesterbrook, PA, 19087 US / P: 18774612631 F: 16105601501 / Billing, Technical
mexpronacmexico.com Inactive 5 Guided Pivots	92	Address / Type(s) ana.karim3666@gmail.com / Admin hostmaster@1and1.com / DNS/SOA ana.karim3666@gmail.com / Registrant hostmaster@1and1.mx / Technical abuse@1and1.com / Whois	1and1.com 1and1.mx gmail.com	Name / Organization / Address / Phone/Fax / Type(s) Hostmaster ONEANDONE / 1&1 Internet Inc / 701 Lee Rd.,Suite 300 Chesterbrook, PA, 19087 US / P: 18774612631 F: 16105601501 / Technical Mukki Zuni / ORTIZ MENA 1804 4 31280 Chihuahua, GUA, 31280 MX / P: 527158563215 / Admin, Registrant
mexpronadmexico.com	92	Address / Type(s)	1and1.com	Name / Organization / Address / Phone/Fax / Type(s)

Additional information allows a researcher to pro-actively protect their organization.

From this point, a researcher could pivot on any of the interesting pieces of information from those domains and uncover a network of badness. Most of the domains on this list had not yet been caught by any major blacklist, so by using Domain Risk Score to identify these as malicious a researcher can pro-actively protect their organization from these types of threats.

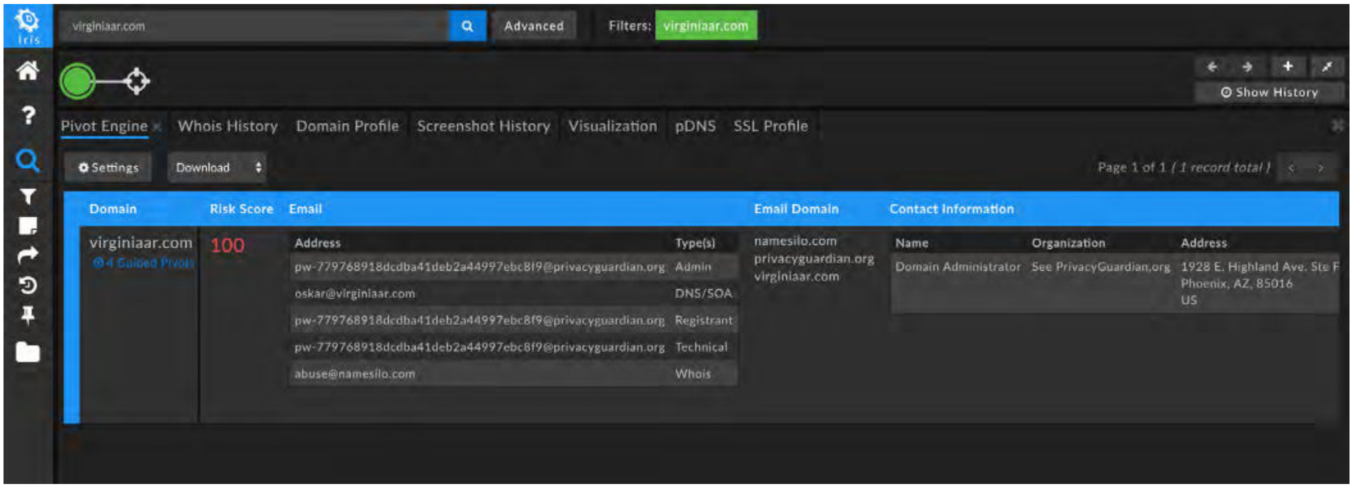
> *Domain Risk Score can help to*
> ***uncover a network of badness.***

NON-REGISTRANT BASED CONNECTIONS

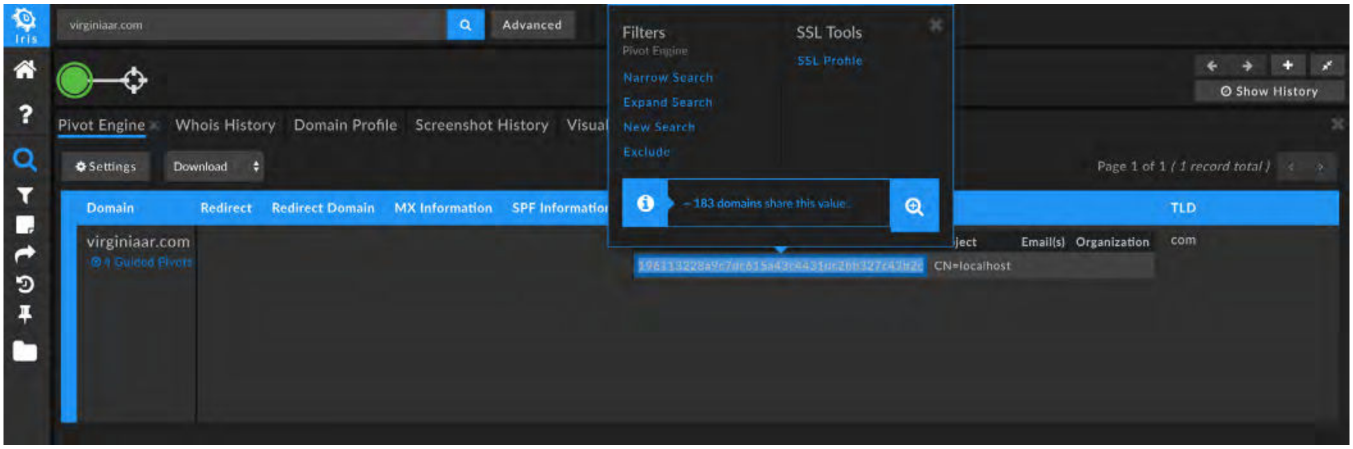
It's neither new nor novel, but it is worth remembering in this post-GDPR world that infrastructure isn't personally identifiable information (PII). This means that researchers can still make connections and attributions based on non-registrant based information using tools like DomainTools Iris.

Aside from Whois information, researchers know there are several other methods by which to tie domains to the same campaign or actor group. One such method is by linking shared infrastructure between domains. Oftentimes, lower level cyber criminals will often host multiple malicious domains on the same IP space or use the same SSL certificate.

For example, searching on a known APT-related domain and pivoting on the shared SSL certificate hash shows that there are over 180 other domains that are likely also tied to that same APT group.



Domain	Risk Score	Email		Email Domain	Contact Information		
		Address	Type(s)		Name	Organization	Address
virginiaar.com 4 Guided Pivots	100	pw-779768918dcdba41deb2a44997ebc8f9@privacyguardian.org	Admin	namesilo.com privacyguardian.org virginiaar.com	Domain Administrator	See PrivacyGuardian.org	1928 E. Highland Ave. Ste F Phoenix, AZ, 85016 US
		oskar@virginiaar.com	DNS/SOA				
		pw-779768918dcdba41deb2a44997ebc8f9@privacyguardian.org	Registrant				
		pw-779768918dcdba41deb2a44997ebc8f9@privacyguardian.org	Technical				
		abuse@namesilo.com	Whois				



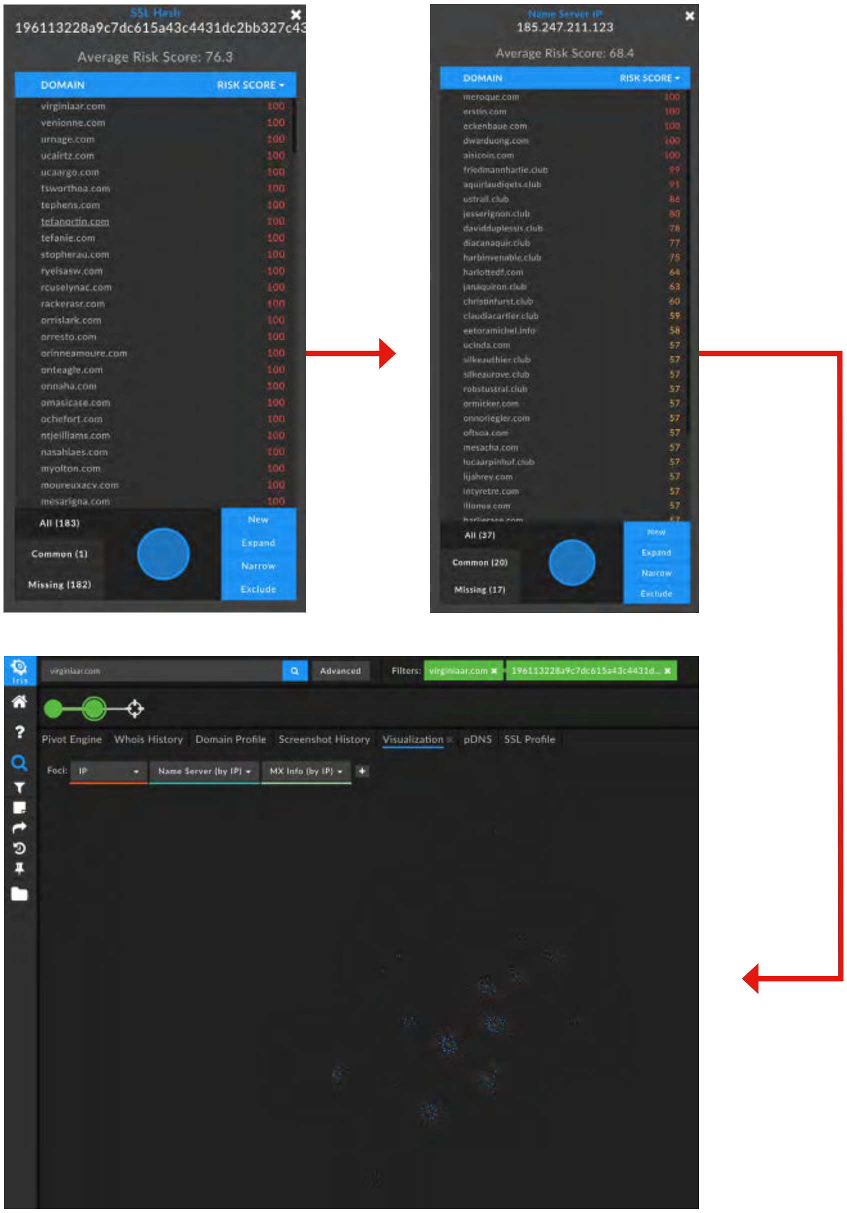
~183 domains share this value.

Domain	Redirect	Redirect Domain	MX Information	SPF Information				TLD
					ject	Email(s)	Organization	
virginiaar.com 4 Guided Pivots				196113228a9e7dc615a43c4431dc2bb327c43b2c	CN=localhost			com

Viewing those 180 domains shows that many of them are still active and aren't yet blacklisted, and might be worth further investigation or blocking.

NON-REGISTRANT BASED CONNECTIONS (CONT.)

It's also notable that many of these domains were not linked by any infrastructure other than SSL certificate - as the visualization of IP, mail server IP, and name server IP shows, these domains were otherwise disparate.



SSL Hash
196113228a9c7dc615a43c4431dc2bb327c43

Average Risk Score: 76.3

DOMAIN	RISK SCORE
virginiaar.com	100
venionne.com	100
urnage.com	100
ucairtz.com	100
ucaargo.com	100
tsworthoa.com	100
tephens.com	100
tefanortin.com	100
tefanie.com	100
stopherau.com	100
ryeisasw.com	100
rcuselynac.com	100
rackerasr.com	100
orrislark.com	100
orresto.com	100
orinneamoure.com	100
onteagle.com	100
onnaha.com	100
omasicase.com	100
ochefort.com	100
ntjeilliams.com	100
nasahlaes.com	100
myolton.com	100
moureuxacv.com	100
mesarigna.com	100

All (183)
Common (1)
Missing (182)

Name Server IP
185.247.211.123

Average Risk Score: 68.4

DOMAIN	RISK SCORE
meroque.com	100
erstin.com	100
eckenbaue.com	100
dwarduong.com	100
aisicoin.com	100
friedmannharlie.club	99
aquirlaudigets.club	91
ustrall.club	86
jesserignon.club	80
davidduplessis.club	78
diacanaquir.club	77
harbinvenable.club	75
harlottedf.com	64
janaquiron.club	63
christinfurst.club	60
claudiacartier.club	59
eetoramichel.info	58
ucinda.com	57
silkeauthier.club	57
silkeaurove.club	57
robstustral.club	57
ormicker.com	57
onnoriegler.com	57
oftsoa.com	57
mesacha.com	57
lucaarpinhuf.club	57
lijahrey.com	57
intyretre.com	57
illonea.com	57

All (37)
Common (20)
Missing (17)

virginiaar.com

Filters: virginiaar.com ✖ 196113228a9c7dc615a43c4431d... ✖

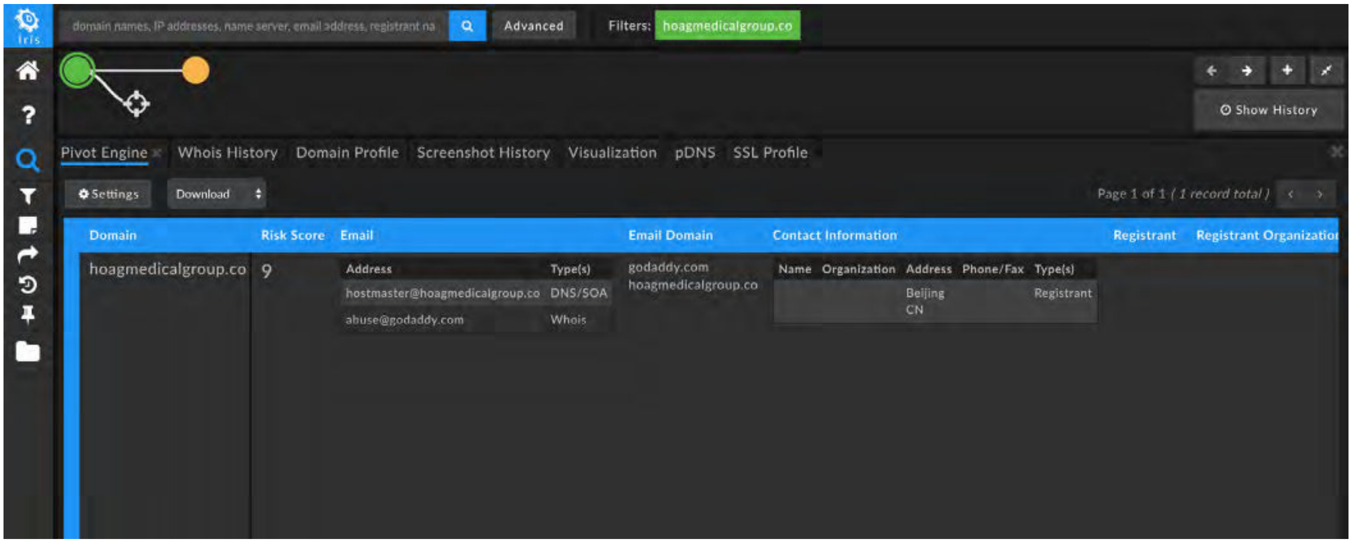
Foci: IP ▾ Name Server (by IP) ▾ MX Info (by IP) ▾ +

The mostly disparate nature of these domains allows for additional pivoting once they've been connected via SSL certificate. Pivoting on the Name Server IP of one of these domains reveals an additional 17 domains that hadn't been tied to the SSL certificate, which may potentially be linked to the same threat actor or campaign.

Threat actors try to hide their tracks when setting up and conducting malicious campaigns, but frequently leave behind a slew of clues that, when viewed together, form a sort of "digital fingerprint" that can help to identify their actions in the context of other related domains.

For example, in one particular observed instance, a threat actor registered numerous healthcare-related phishing domains on the same day. However, none of the domains had any obvious linkages to each other and searching for one of the domains in Iris looked to be a dead end.

NON-REGISTRANT BASED CONNECTIONS (CONT.)



domain names, IP addresses, name server, email address, registrant na

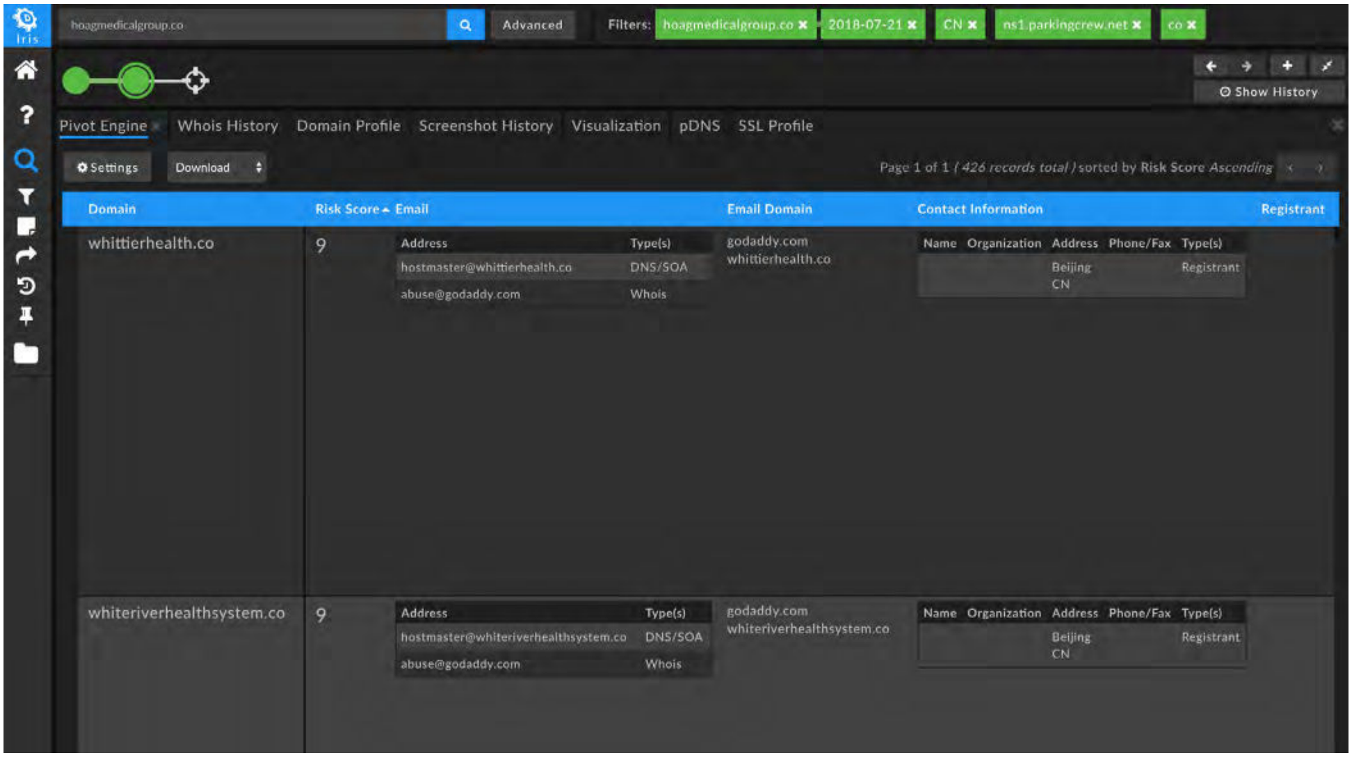
Filters: hoagmedicalgroup.co

Page 1 of 1 (1 record total)

Domain	Risk Score	Email	Email Domain	Contact Information	Registrant	Registrant Organizatio
hoagmedicalgroup.co	9	Address Type(s) hostmaster@hoagmedicalgroup.co DNS/SOA abuse@godaddy.com Whois	godaddy.com hoagmedicalgroup.co	Name Organization Address Phone/Fax Type(s) Beijing CN Registrant		

Example of a search based on specific attributes of a domain.

By expanding and narrowing the search based on specific attributes of the domain - such as create date, country code, name server, and TLD - we were able to identify approximately 400 domains that all appeared to be related to other healthcare institutions. Those attributes made up that particular campaign's "digital fingerprint," allowing us to pivot and find more potentially malicious domains related to the same actor and campaign.



hoagmedicalgroup.co

Filters: hoagmedicalgroup.co ✕ 2018-07-21 ✕ CN ✕ ns1.parkingcrew.net ✕ co ✕

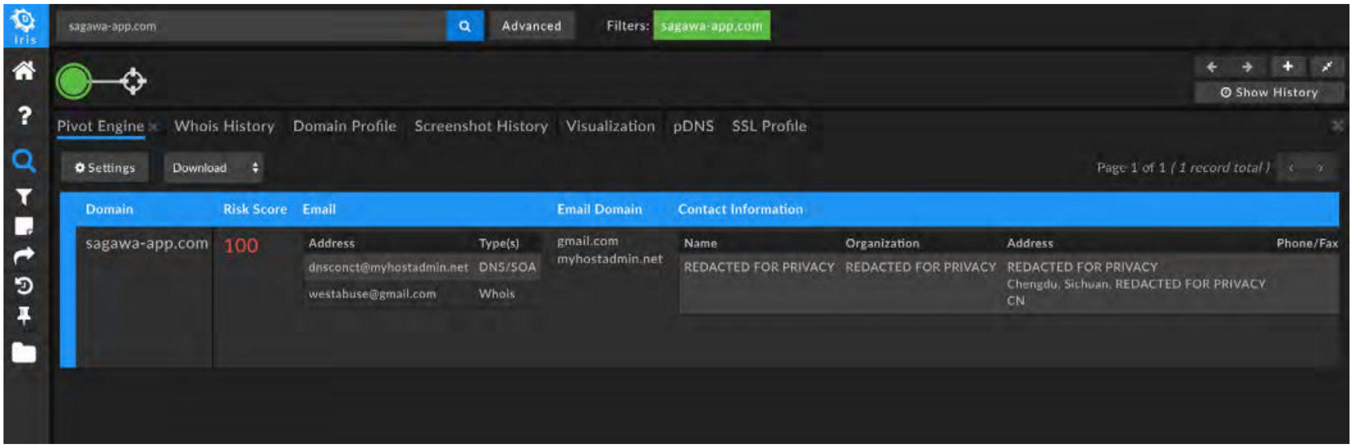
Page 1 of 1 (426 records total) sorted by Risk Score Ascending

Domain	Risk Score ▲	Email	Email Domain	Contact Information	Registrant
whittierhealth.co	9	Address Type(s) hostmaster@whittierhealth.co DNS/SOA abuse@godaddy.com Whois	godaddy.com whittierhealth.co	Name Organization Address Phone/Fax Type(s) Beijing CN Registrant	
whiteriverhealthsystem.co	9	Address Type(s) hostmaster@whiteriverhealthsystem.co DNS/SOA abuse@godaddy.com Whois	godaddy.com whiteriverhealthsystem.co	Name Organization Address Phone/Fax Type(s) Beijing CN Registrant	

Example of an expanded and narrowed search query, yielding additional malicious domains.

NON-REGISTRANT BASED CONNECTIONS (CONT.)

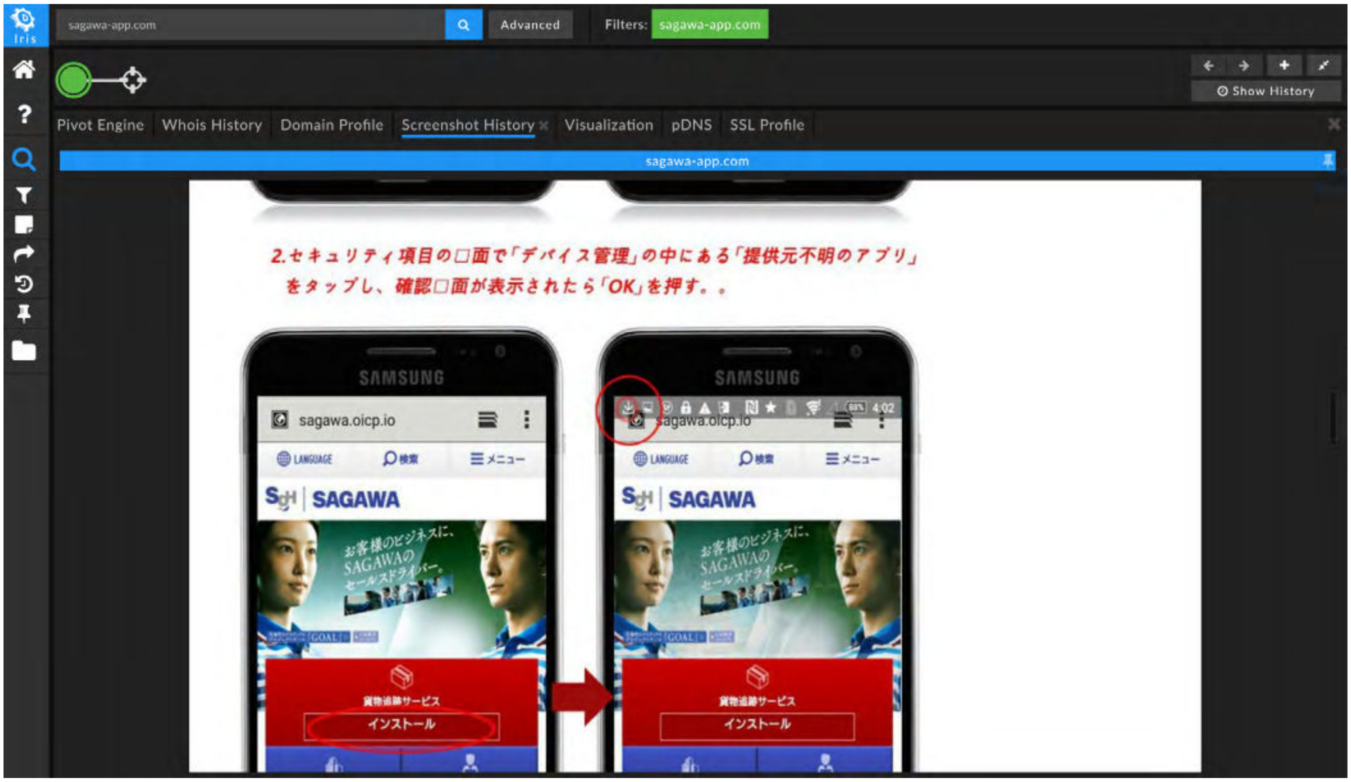
As researchers, we're used to looking for the obvious connections between domains, but sometimes linkages may be more uncommon. In one instance, a particular malicious domain didn't seem to have any useful pivots to additional maliciousness. It did, however, have a screenshot history.



Domain	Risk Score	Email	Email Domain	Contact Information
sagawa-app.com	100	Address / Type(s) dnsconct@myhostadmin.net / DNS/SOA westabuse@gmail.com / Whois	gmail.com myhostadmin.net	Name: REDACTED FOR PRIVACY Organization: REDACTED FOR PRIVACY Address: REDACTED FOR PRIVACY Chengdu, Sichuan, REDACTED FOR PRIVACY CN Phone/Fax

Sometimes obvious connections between domains may be more uncommon.

Reviewing the screenshot revealed that the webpage had instructions for the user to download malicious software onto their phone and included phone screenshots with a different domain in the address bar of the phone.

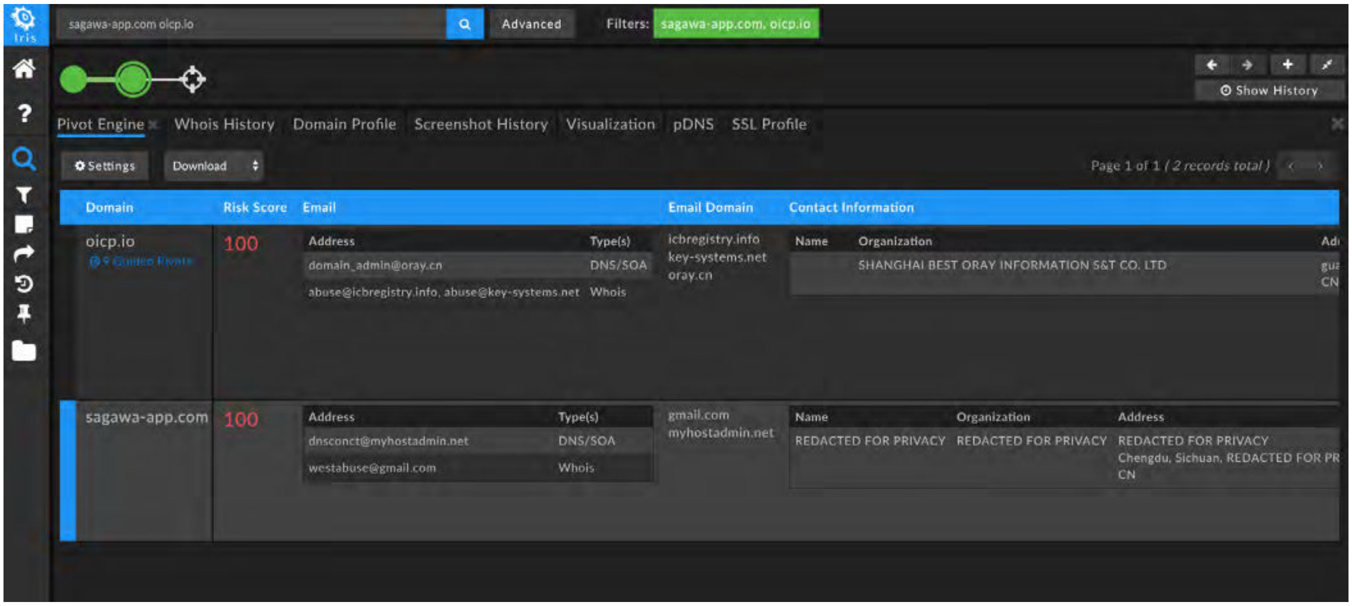


2.セキュリティ項目の□面で「デバイス管理」の中にある「提供元不明のアプリ」をタップし、確認□面が表示されたら「OK」を押す。。

This example shows a webpage with instructions for the user to download malicious software onto their phone.

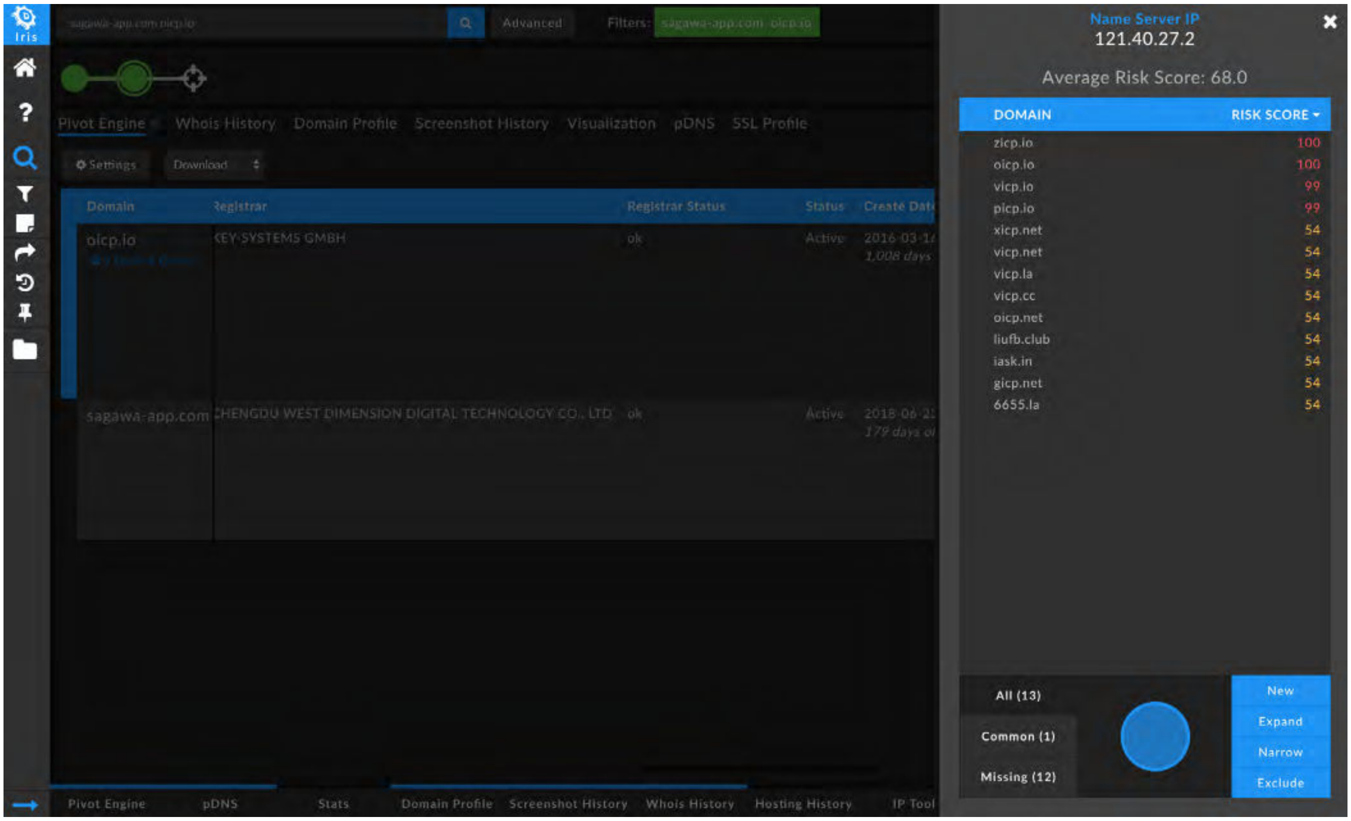
NON-REGISTRANT BASED CONNECTIONS (CONT.)

Searching on that domain reveals multiple other malicious domains tied to the same campaign.



Page 1 of 1 (2 records total)

Domain	Risk Score	Email		Email Domain	Contact Information		
		Address	Type(s)		Name	Organization	Ad
oicp.io	100	domain_admin@oray.cn	DNS/SOA	icbregistry.info key-systems.net oray.cn		SHANGHAI BEST ORAY INFORMATION S&T CO. LTD	gua CN
		abuse@icbregistry.info, abuse@key-systems.net	Whois				
		Address	Type(s)		Name	Organization	Address
sagawa-app.com	100	dnsconct@myhostadmin.net	DNS/SOA	gmail.com myhostadmin.net	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY Chengdu, Sichuan, REDACTED FOR PR CN
		westabuse@gmail.com	Whois				



Domain	Registrar	Registrar Status	Status	Create Dat
oicp.io	KEY-SYSTEMS GMBH	ok	Active	2016-03-1 1,008 days
sagawa-app.com	CHENGDU WEST DIMENSION DIGITAL TECHNOLOGY CO., LTD	ok	Active	2018-06-2 179 days o

Name Server IP
121.40.27.2

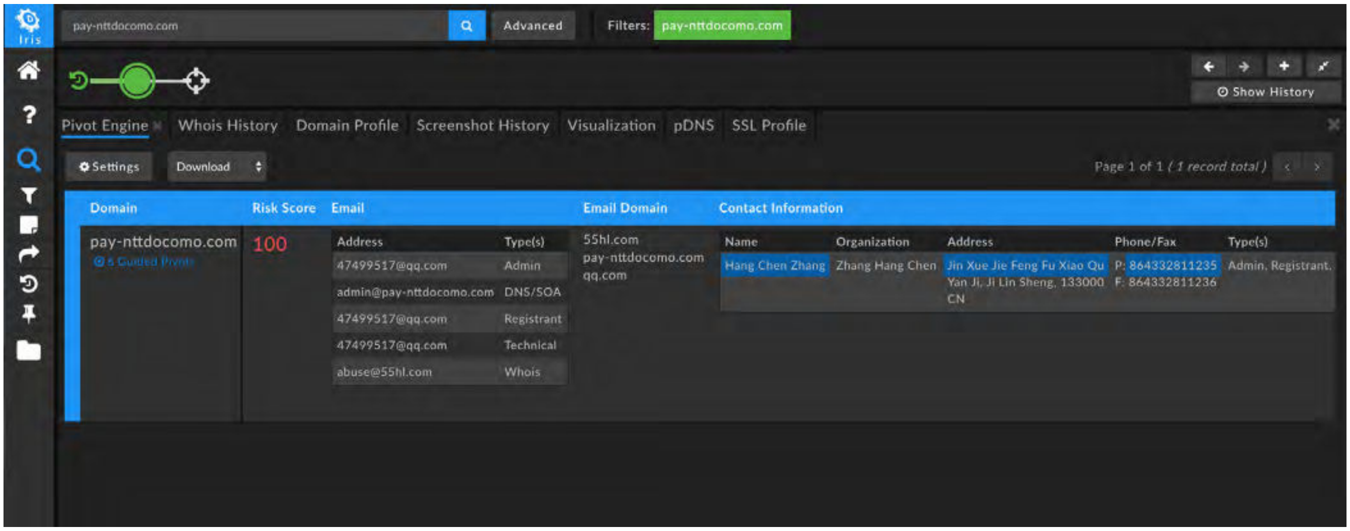
Average Risk Score: 68.0

DOMAIN	RISK SCORE
zicp.io	100
oicp.io	100
vicp.io	99
picp.io	99
xicp.net	54
vicp.net	54
vicp.la	54
vicp.cc	54
oicp.net	54
liufb.club	54
iask.in	54
gicp.net	54
6655.la	54

All (13)
Common (1)
Missing (12)

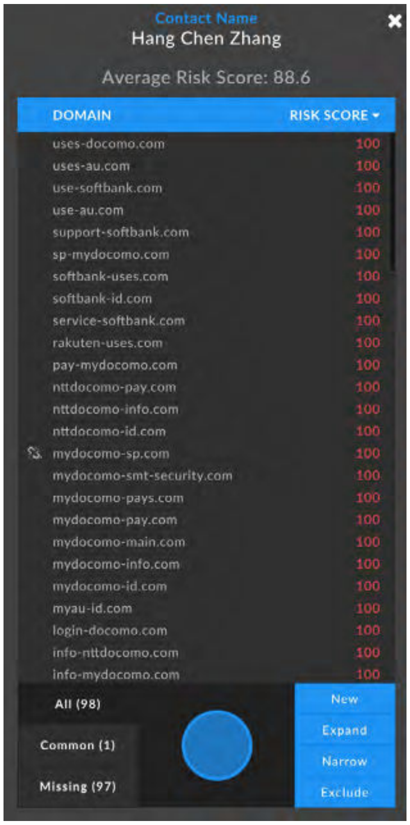
NON-REGISTRANT BASED CONNECTIONS (CONT.)

Finally, it is worthy to note that not all registrants have fully adhered to GDPR regulations, especially those that are based elsewhere than the European Union. When conducting an investigation, it may still be beneficial to check Whois information, as beneficial pivots may still be available. Additionally, historical Whois information in Iris may still contain registrant information that had been exposed at some point in time, even if it is private now, and may be useful for finding connections between malicious sites.



Domain	Risk Score	Email		Email Domain	Contact Information				
		Address	Type(s)		Name	Organization	Address	Phone/Fax	Type(s)
pay-nttdocomo.com	100	47499517@qq.com	Admin	55hl.com pay-nttdocomo.com qq.com	Hang Chen Zhang	Zhang Hang Chen	Jin Xue Jie Feng Fu Xiao Qu Yan Ji, Ji Lin Sheng, 133000 CN	P: 864332811235 F: 864332811236	Admin, Registrant,
		admin@pay-nttdocomo.com	DNS/SOA						
		47499517@qq.com	Registrant						
		47499517@qq.com	Technical						
		abuse@55hl.com	Whois						

These examples show that it may still be worthwhile to check Whois information, as beneficial pivots may still be available.



Contact Name
Hang Chen Zhang

Average Risk Score: 88.6

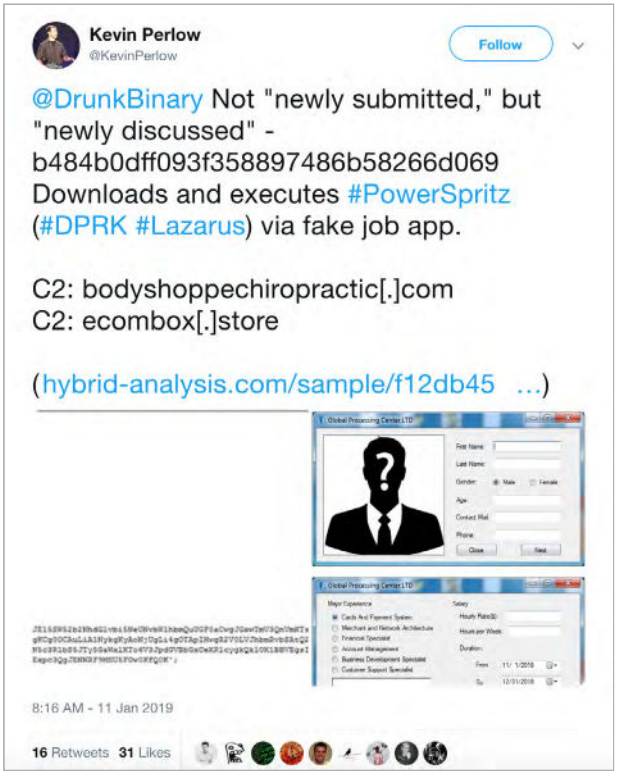
DOMAIN	RISK SCORE
uses-docomo.com	100
uses-au.com	100
use-softbank.com	100
use-au.com	100
support-softbank.com	100
sp-mydocomo.com	100
softbank-uses.com	100
softbank-id.com	100
service-softbank.com	100
rakuten-uses.com	100
pay-mydocomo.com	100
nttdocomo-pay.com	100
nttdocomo-info.com	100
nttdocomo-id.com	100
mydocomo-sp.com	100
mydocomo-smt-security.com	100
mydocomo-pays.com	100
mydocomo-pay.com	100
mydocomo-main.com	100
mydocomo-info.com	100
mydocomo-id.com	100
myau-id.com	100
login-docomo.com	100
info-nttdocomo.com	100
info-mydocomo.com	100

In this example, you can see that just from the Whois data available, there are potentially beneficial pivots on the registrant Name, Address, and Phone Number. Pivoting on Name shows 97 other malicious and potentially malicious domains.

These examples show that Whois information redacted by GDPR regulation have not truly hindered the intelligence and analysis process. With a little ingenuity, beneficial pivots can still be made to uncover campaigns or threat actors.

OPEN SOURCE INTELLIGENCE (OSINT) RESOURCES

Open source tools and methods have always been important to researchers, and many of these routes were not impacted by GDPR at all. Social media platforms like Twitter, vendor reports, indicator sharing platforms, phishing feeds, and tools posted to GitHub are just a few of the many ways that intelligence analysts can continue investigations into incidents.



Kevin Perlow
@KevinPerlow

@DrunkBinary Not "newly submitted," but "newly discussed" - b484b0dff093f358897486b58266d069 Downloads and executes #PowerSpritz (#DPRK #Lazarus) via fake job app.

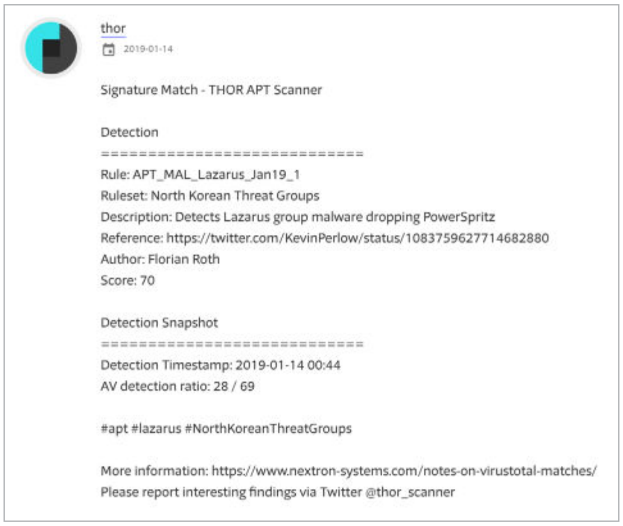
C2: bodyshoppechiropractic[.]com
C2: ecombox[.]store

(hybrid-analysis.com/sample/f12db45 …)

8:16 AM - 11 Jan 2019

16 Retweets 31 Likes

Twitter is an industry favorite for discussing current security trends and is a hotbed of activity.



```
thor
2019-01-14

Signature Match - THOR APT Scanner

Detection
==============================
Rule: APT_MAL_Lazarus_Jan19_1
Ruleset: North Korean Threat Groups
Description: Detects Lazarus group malware dropping PowerSpritz
Reference: https://twitter.com/KevinPerlow/status/1083759627714682880
Author: Florian Roth
Score: 70

Detection Snapshot
==============================
Detection Timestamp: 2019-01-14 00:44
AV detection ratio: 28 / 69

#apt #lazarus #NorthKoreanThreatGroups

More information: https://www.nextron-systems.com/notes-on-virustotal-matches/
Please report interesting findings via Twitter @thor_scanner
```

Detection Snapshot from https://www.nextron-systems.com

Twitter is an industry favorite for discussing current security trends and is a hotbed of activity. Security researchers will routinely post otherwise undocumented IOCs and investigation findings, so it's usually a worthwhile endeavor to search Twitter for IOCs related to your current case. Depending on the sensitivity of your investigation you may even consider asking the community for any information they may have.

Well-known vendors, government resources (**US-CERT**), and the **SANS Internet Storm Center (ISC)** are continuously keeping up with the latest threats and do a fine job posting analyses in a timely manner. While your investigation may not currently be attributed to any larger campaigns it's definitely worth checking recent industry reports for similar behavior or indicators.

Malware analysis services such as **VirusTotal**, **Malwr**, and **Hybrid Analysis** are a treasure trove of community-sourced data. These reports often contain community commentary attempting to enrich the automated analysis already provided. Keep in mind you don't need to search these platforms with only a file hash, but can search on IP addresses and domains as well. VirusTotal in particular is known to have plenty of friendly bot accounts whose sole purpose is to tag uploaded files with enrichments.

When investigating a domain it's important to check if it has a digital certificate, as the data they contain may allow you to link an actors infrastructure together (as seen above in "Non-Registrant Based Connections"). Sites like **Censys** and **crt.sh** are valuable resources for certificate information. Certificates may help provide some details for linking actor assets, as they may use the same information in separate places.

There's such an array of OSINT tools out there it would be an intensive effort to try and cover them all, but resources like the **OSINT Framework** and the **Awesome OSINT** list on Github are fantastic jumping off points for investigations.

INFORMATION SHARING

One of the most important ways that cyber security professionals should be getting information is by involvement in various information sharing groups and the usage of Threat Intelligence Platforms. By actively participating in these groups, researchers can share and receive valuable intelligence that might otherwise be unavailable to them. Private-sector groups like ISACs, government groups like Infragard, and member-operated sharing groups are all valuable sources of information.

While the first two categories of groups are easy to find and join, the category of small member-operated sharing groups is purposefully more hidden. The best way to identify these types of groups is by networking - go to conferences, trainings, and meetups to find out what groups may be beneficial to join.

On a technical level most of these relationships involve STIX/TAXII feeds and/or Threat Intelligence Platforms such as **MISP** and the **Alienvault Open Threat Exchange**. The strength in these platforms is their ability to allow programmatic data sharing between organizations using tiered access (such as the Traffic Light Protocol). If your organization is currently lacking a threat sharing platform you may be missing a treasure trove of security data. Even if you have a paid threat intelligence platform free tools like MISP are extremely likely to have different data sets and more flexibility for sharing data with other groups. Keep in mind these platforms are also your opportunity to contribute to the security community.

CONCLUSION

While GDPR affected the way that many analysts have historically conducted investigations, there are still several methods to uncover threat actors' tracks. By using Domain Risk Score, non-registrant based indicators, OSINT, and participating in information sharing organizations, analysts can identify useful indicators to produce intelligence and defend their organizations.

Tools & Resources

VIRUSTOTAL: https://www.virustotal.com/#/home/upload

MALWR: https://malwr.com/

HYBRID ANALYSIS: https://www.hybrid-analysis.com/

CENSYS: https://censys.io/

CRT.SH: https://crt.sh/

OSINT FRAMEWORK: https://osintframework.com/

AWESOME OSINT: https://github.com/jivoi/awesome-osint

MISP: https://www.misp-project.org/

ALIENVAULT OPEN THREAT EXCHANGE: https://www.alienvault.com/open-threat-exchange

ABOUT DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at **http://www.domaintools.com** or follow us on **Twitter: @domaintools**.