Indicators Over Cocktails: Exporting Indicators from Iris

domaintools.com/resources/blog/indicators-over-cocktails-exporting-indicators-from-iris

Introduction

Each month on our Indicators over Cocktails series, we take a look at some specific features of DomainTools products. We mainly focus on Iris, but the April edition also delved briefly into PhishEye. We do these mini-training-sessions with recent adversary campaign infrastructure as the example data, often expanding beyond published indicator lists to find new domains and IP addresses that are likely tied to identified campaigns (or clustered activities that may or may not have formal campaign classifications).

Oh, and we quaff tasty beverages too.

For May, the beverage was the delicious but often cheaply-made Mai Tai. Here's the recipe:

If you're like me, most of the Mai Tais you've had over the years were almost certainly made from a pre-mix which was probably about 85% sugar. The recipe above is from a speakeasy in New York called PDT, and they know how to make drinks the right way. Salud!

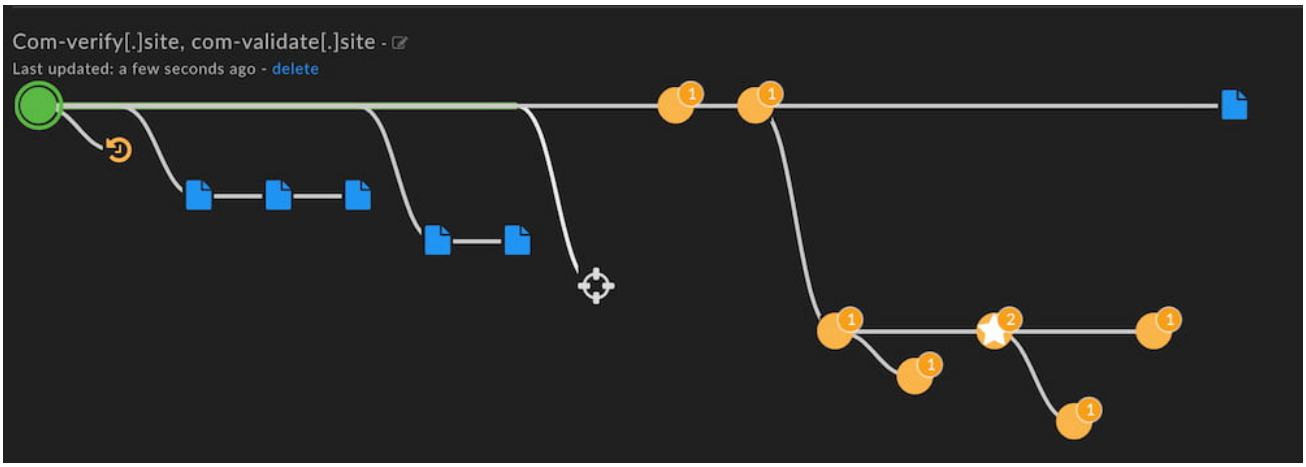
I've Finished My Investigation: Now What?

The training for May covered various ways to take the data you've developed in Iris and make it available for further actions, which could range from the defensive (building firewall/IPS rules, building detections) to the administrative (generating reports for management, GRC, etc) to the collaborative (sharing investigations with other Iris users, or sharing indicators with trust groups or law enforcement). Iris provides five distinct ways to share information.

To illustrate this, we looked at infrastructure related to a campaign FireEye has called "Ghostwriter," by a group they call UNC1151. It's a cyber espionage group targeting several specific countries, and a big part of their TTPs involves stealing credentials and then posing as the victims, posting on their social media accounts. They target victims of significance so as to spread their messages (mainly anti-NATO) as broadly as possible. We took a couple of indicators posted by Kyle Ehmke on May 13, and expanded from them to develop a list of dozens of domains that have a lot in common with confirmed UNC1151 infrastructure. Many of these domains have not at this point been put on block lists, but their nefarious purposes are pretty clear.

Breadcrumbs, But With a Difference

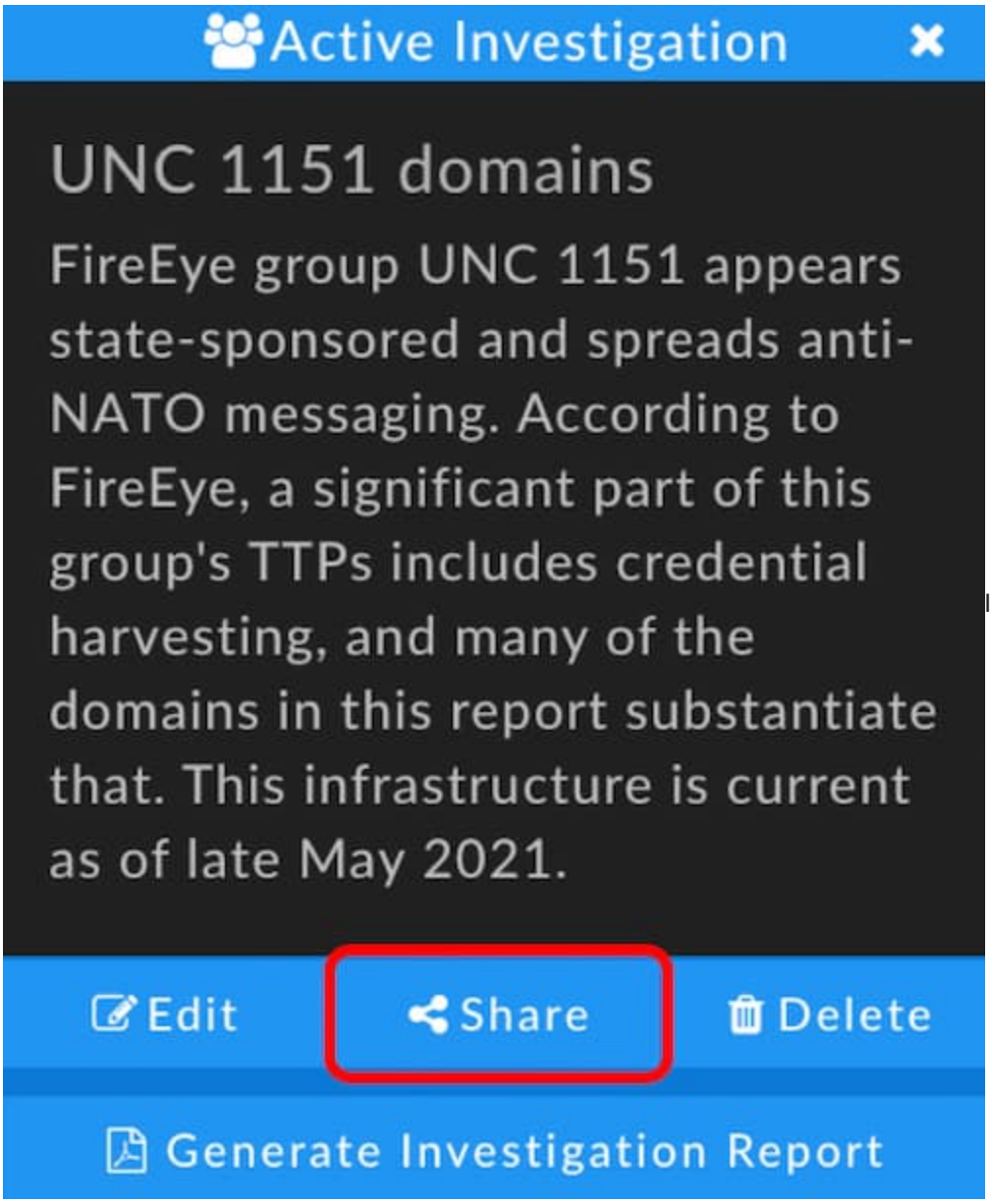
The screenshot below shows the Search History in Iris. It forms a sort of breadcrumb trail of each pivot or new search you take during the course of your investigation. The nodes of the trail can carry various pieces of information. In the example, we've got the first node in focus, which has the two domains that Kyle posted on the 13th. Some of the other nodes have a little number on them. That number shows one of the methods of sharing information in Iris: it represents the number of notes the investigator has pinned to that step of the investigation.



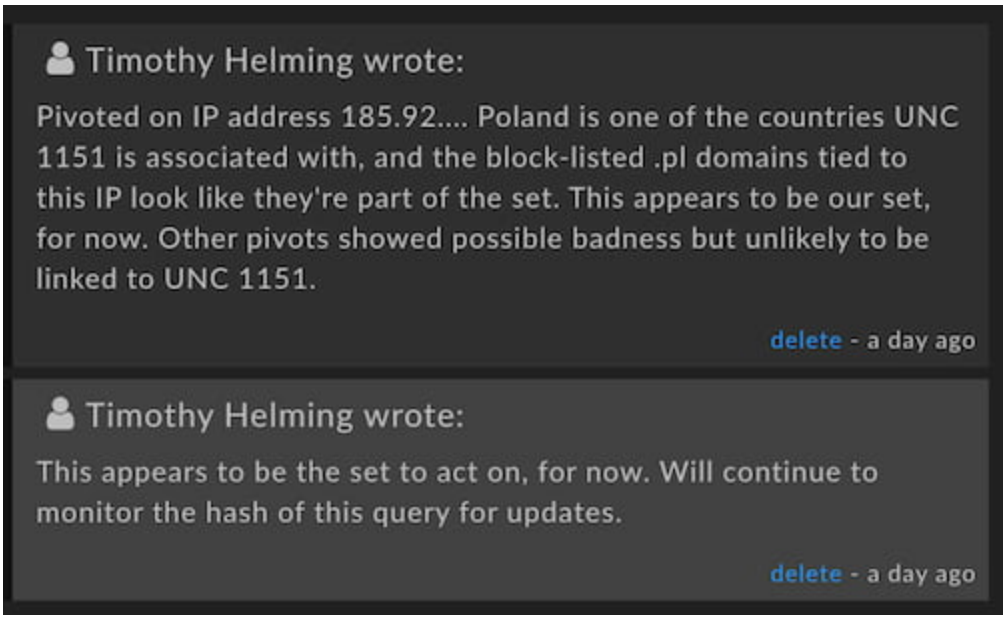
Iris Search History with annotated nodes

One of the nodes has the number 2 on it, and a star. The star can be added to any node to call it out as significant, and the two notes (which we'll see in a moment) give context on why that step of the investigation is useful.

"But wait," you might be thinking. "How is that *sharing*?" Here's how: Iris allows you to share an investigation with other Iris users in your DomainTools group. If you work on a team and more than one of you investigates infrastructure in Iris, the notes you create can be seen by your co-investigators.



Investigation Share Button

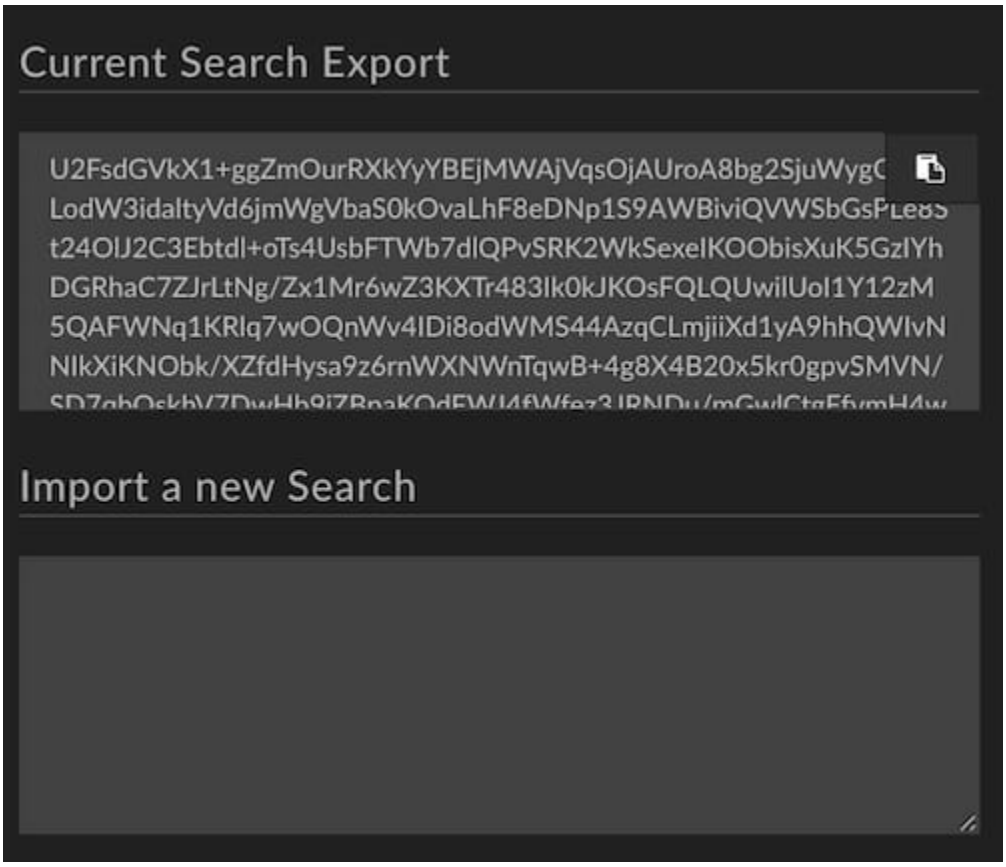


Notes for collaborators or for documentation

You can share the investigation as read-only, read+add, or read+add+delete, depending on how much control you want to give your colleagues.

Pass the Hash

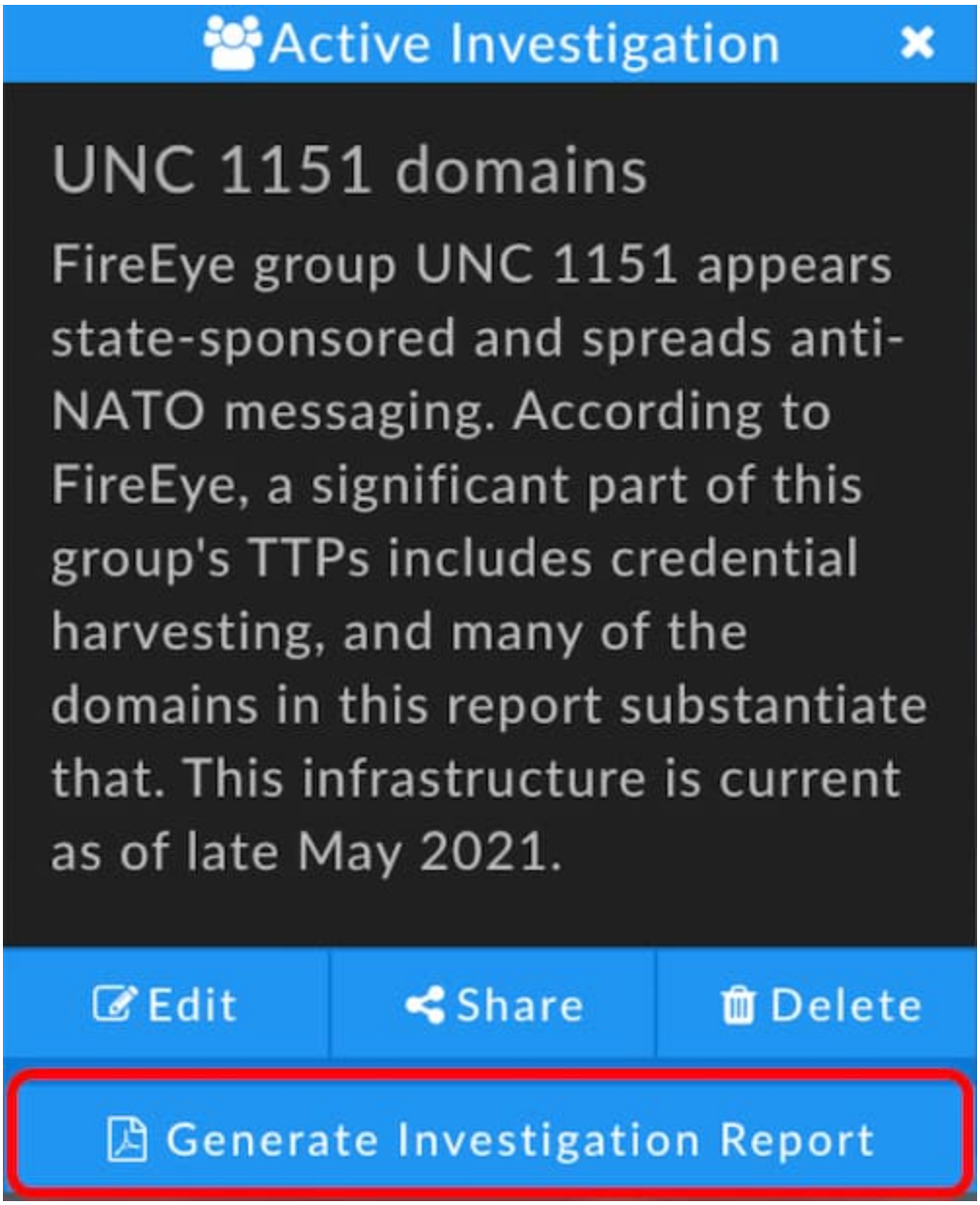
No, that's not a drug reference, nor is it a reference to a cyber adversary technique. Rather, Iris allows you to export a hash of any query, so that another Iris user who may not be part of your group can look at the same query that you ran. When you share in this way, the other party does not see investigation notes or any of your search history (breadcrumbs), but they do see the results of the same query that you had made.



Search hash export and import controls

Reporting for Duty

Sometimes a formal investigation report is required, whether for leadership, peers, or just as part of a documentation requirement in your organization. Iris allows you to generate a .pdf report that shows the investigative steps you took and various manifestations of the data you uncovered, including indicator lists, search hashes, and detailed domain information. The description of the investigation (which you can see in the screenshot below) as well as any notes you added along the way are recorded in the .pdf report. A sample report will be linked along with this blog for your perusal.



Machine-Readable Exports

You might also wish to share the indicators you developed in Iris with others who will use the data programmatically. Iris allows you to export the data to a .csv file, or to STIX versions 1.2 or 2.0. The latter is particularly useful for users in ISACs or other trust groups. The .csv export can be used for generation of detections or firewall rules. The .csv export's columns will show whatever columns you have active in the Pivot Engine. For some use cases, you might choose to show only the domain and IP address columns, and for others you might want everything.

inbox-admin.site	104.21.78.113	2021-03-23	100	https://whois.domaintools.com/inbox-admin.site	inactive		
incometaxindia-org.in	198.54.115.98	2021-05-12	97	https://whois.domaintools.com/incometaxindia-org.in	active	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY
international-indian.tech	198.54.115.98	2021-01-27	72	https://whois.domaintools.com/international-indian.tech	active		
jobes4u.com	198.54.115.98	2021-01-30	68	https://whois.domaintools.com/jobes4u.com	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
kamranshahriar.com	198.54.115.98	2021-04-12	79	https://whois.domaintools.com/kamranshahriar.com	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
login-inbox.online	104.21.64.156	2021-03-04	100	https://whois.domaintools.com/login-inbox.online	inactive		
login-mail.online	104.21.84.249	2021-03-02	100	https://whois.domaintools.com/login-mail.online	inactive		
login-telekom.online	104.21.79.247	2021-03-01	100	https://whois.domaintools.com/login-telekom.online	inactive		
login-verify.online	104.21.72.177	2021-03-04	99	https://whois.domaintools.com/login-verify.online	inactive		
logis-transport.com	198.54.115.98	2021-01-07	82	https://whois.domaintools.com/logis-transport.com	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
m-nd.co	185.107.56.200	2021-01-09	51	https://whois.domaintools.com/m-nd.co	active	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY
mail-validation.online		2021-04-19	100	https://whois.domaintools.com/mail-validation.online	active		
maitre-amanveba.com	198.54.115.98	2021-02-13	95	https://whois.domaintools.com/maitre-amanveba.com	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
mangatgroupinvestment.com	198.54.115.98	2021-02-24	80	https://whois.domaintools.com/mangatgroupinvestment.com	active	WhoisGuard Protected	WhoisGuard, Inc
maxinfotech.net	198.54.115.98	2021-05-16	49	https://whois.domaintools.com/maxinfotech.net	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
mayoladschools.com	198.54.115.98	2021-04-19	78	https://whois.domaintools.com/mayoladschools.com	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
mintoxworld.com	198.54.115.98	2021-03-30	72	https://whois.domaintools.com/mintoxworld.com	active	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
musicbook.email	198.54.115.98	2021-03-13	64	https://whois.domaintools.com/musicbook.email	active	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY
mypayee-new-confirmation.com	198.54.115.98	2021-04-08	100	https://whois.domaintools.com/mypayee-new-confirmation.com	inactive	Withheld for Privacy Purposes	Privacy service provided by Withheld for Privacy ehf
mytransfers-review.live	198.54.115.98	2021-03-30	98	https://whois.domaintools.com/mytransfers-review.live	inactive	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY
net-account.online	104.21.42.123	2021-02-24	100	https://whois.domaintools.com/net-account.online	inactive		
newpayee-cancel.co.uk	198.54.115.98	2021-01-16	100	https://whois.domaintools.com/newpayee-cancel.co.uk	active		
newrequestedapp-review.link	198.54.115.98	2021-05-10	99	https://whois.domaintools.com/newrequestedapp-review.link	active	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY

Iris results exported as .csv

Choose Your Export

Which way you export or share data from Iris depends on your needs and whom you're sharing the data with. Below is one way to think about it, but your own needs might rearrange some of the check marks.

	Leadership or GRC	Trust Group	Security Admins / DX Engineering	Law Enforcement	Business Ecosystem	Iris Users in Your Grou
.pdf Report						
.csv Export						
STIX Export						
Query Hash						
Investigation						

If you missed the live IOC webinar, you can revisit it here, and you can sign up for future installments here. Hope to see you there soon, and...cheers!

Watch the IOC Webinar