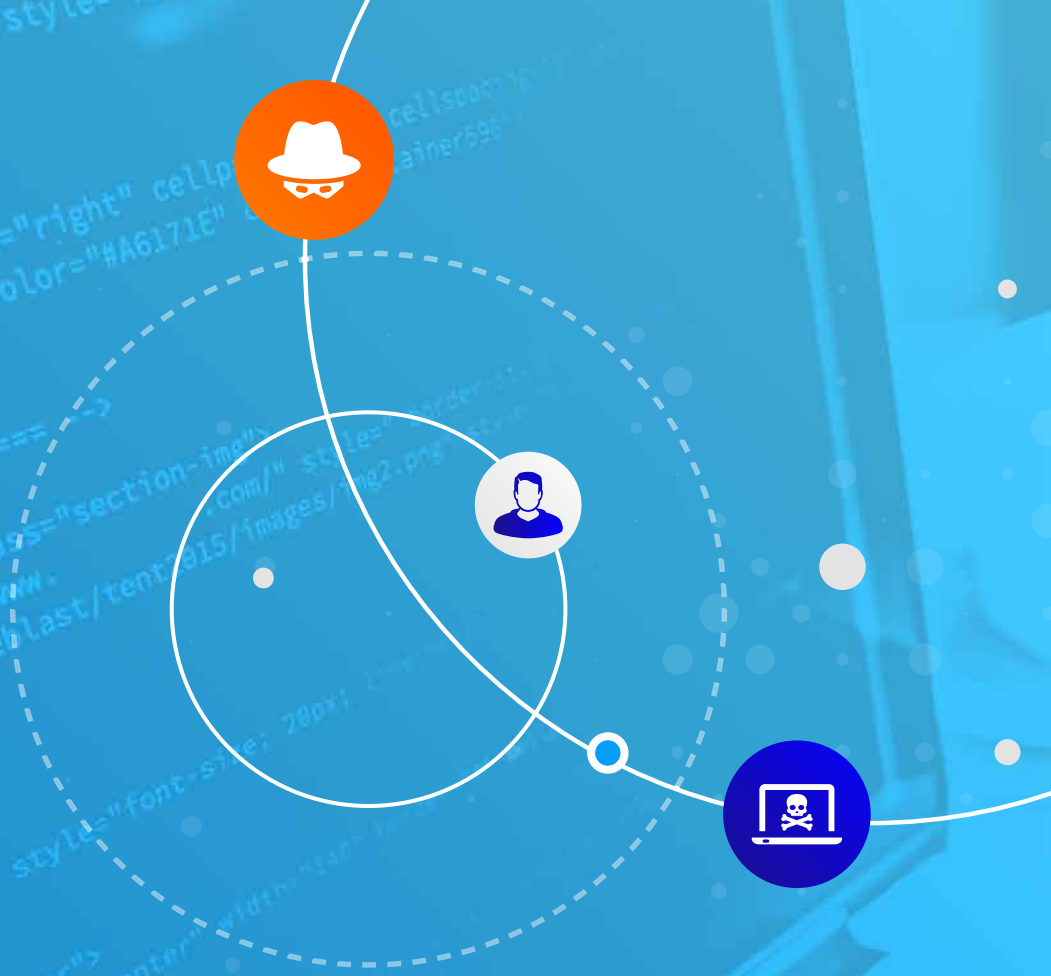
WHITE PAPER



Volume 2

DISRUPTING ADVERSARY INFRASTRUCTURE

ThreatConnect Tactics to Encourage Domain Registrar and State Entity Collaboration

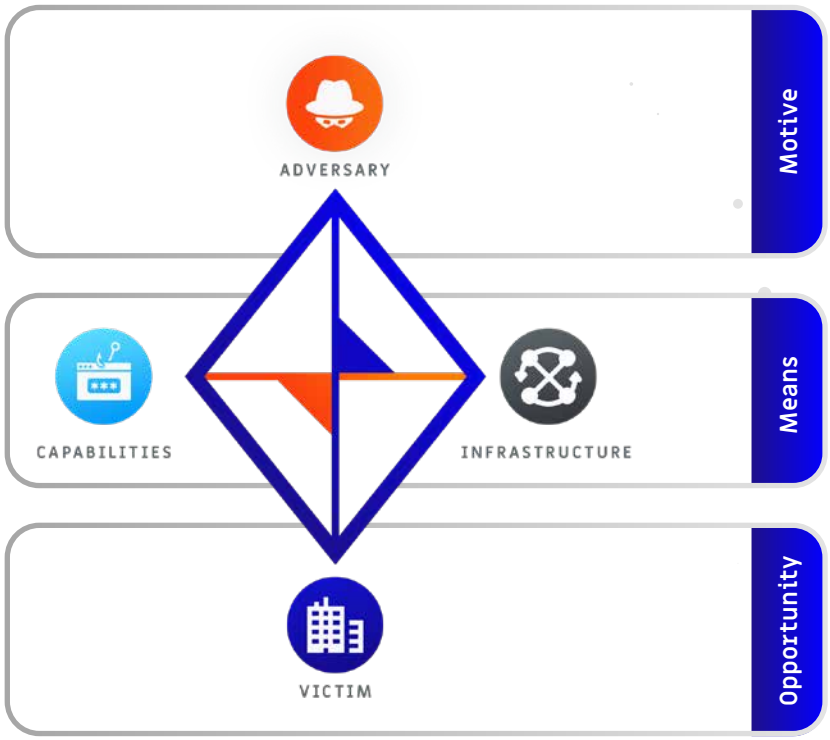
ThreatConnect™

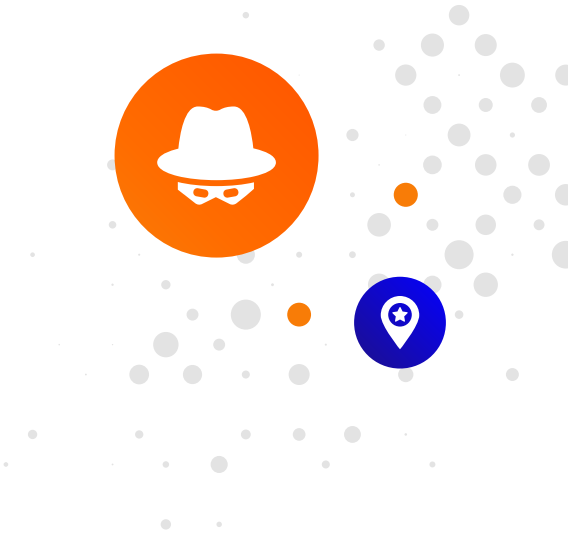
www.ThreatConnect.com

Adversarial Abuse of the Domain Name System

In a previous *Disrupting Adversary Infrastructure* white paper, we discussed the roles and obligations of Internet Service Providers (ISPs) and governments to identify and eliminate cyberspace assets used for malicious purposes, with a particular focus on IP addresses and Autonomous System Numbers (ASNs). Domain registrars and registrants, however, also play a critical role in disruptive efforts. As illustrated by the Diamond Model (Figure 1), *Adversaries* wield offensive *capabilities* to weaponize Internet *infrastructure* by exploiting vulnerable *victims*. Without infrastructure, an adversary's *means* to exploit an *opportunity* is severely degraded, if not eliminated[1]. Without infrastructure, an enemy's *motive* to commit harm through cyberspace dwindles. A *Domain* name, also referred to as *Host* name, is an infrastructure element which facilitates Internet-based communications by providing a human-readable object translated directly to a machine-based IP address. Hence why domain names are integral for both business owners and criminals to operate on the Internet.

FIGURE 1 - The Diamond Model of Intrusion Analysis





1 Caltagirone, S. & Pendergast, A. (2019, March 25). The Diamond Model: An Analyst's Best Friend. Retrieved from https://threatconnect.com/resource/the-diamond-model-an-analysts-best-friend/

Domains are registered by legitimate business owners and malevolent adversaries to host web content. Often, adversaries circumvent a victim's website security controls to host malware, effectively launching attacks from an otherwise legitimate domain. As a defensive measure, targeted third parties may report abuse to a Domain Registrar. In response, a registrar may suspend the domain's functionality until the nature of the abuse is identified and remediated by a Hosting Provider or registrant. Registry Operator (RO) abuse response options may include holding, locking, redirecting, transferring, or deleting the domain[2]. On the victim's compromised website, a warning similar to the one represented in Figure 2 may be presented to visitors, resulting in negative mission impact and perhaps even financial loss.

FIGURE 2 - Domain Suspension Notification

The aforementioned process is the consequence of a long-standing agreement between the Internet Corporation for Assigned Names and Numbers (ICANN) and accredited registrars. Registrars are expected to abide by the terms outlined in their Registrar Accreditation Agreement (RAA)[3]. If a domain is being abused, the ICANN, registries, registrars, and registrants are expected to manage the situation as follows:

> ICANN organization doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. Its agreements with registries and registrars does include obligations on the registries and registrars to investigate and report abuse and illegal activities. As a domain name registrant, you have certain obligations for your domain name registration and its usage, governed by your agreement with the registrar[4].

On the victim's compromised website, a warning similar to the one represented in Figure 2 may be presented to visitors, resulting in negative mission impact and perhaps even financial loss.

2 ICANN. (2017). Framework for Registry Operator to Respond to Security Threats. Retrieved from https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en

3 ICANN. (2013). Registrar Abuse Reports. Retrieved from https://www.icann.org/resources/pages/abuse-2014-01-29-en

4 ICANN. (2017). Spam, Phishing, and Website Content. Retrieved from https://www.icann.org/resources/pages/spam-phishing-2017-06-20-en

Activity defined as *abusive* is revealed by the Domain Abuse Activity Reporting (DAAR) project which focuses primarily on phishing domains, malware domains, Botnet Command-and-Control domains, and spam domains[5]. An illustration of the Domain Name Registration Process is provided in Figure 3.

FIGURE 3 - Domain Name Registration Process[6]

Economically speaking, domain abuse takes its toll, particularly on small business owners who may not have the fiscal resources to adequately protect their web infrastructure. Even for larger businesses, a few minutes of website outage time could result in millions of dollars lost. Ethically, individuals and organizations should be afforded the right to operate on the Internet without being subjected to criminal or state-sponsored maltreatment. Local governments would be keen to identify and evaluate the extent of adverse socioeconomic impact originating from cyber attacks within their area of responsibility. For example, upon discovering a malicious domain, States could directly engage the affected registry operators, registrars, resellers (web hosting companies), and registrants to assess impact, apply countermeasures, and gather artifacts. Fortunately, ThreatConnect offers capabilities to aggregate, analyze, and act during such scenarios.

Economically speaking, domain abuse takes its toll, particularly on small business owners who may not have the fiscal resources to adequately protect their web infrastructure. Even for larger businesses, a few minutes of website outage time could result in millions of dollars lost.

5 ICANN. (2019). Domain Abuse Activity Reporting. Retrieved from https://www.icann.org/octo-ssr/daar

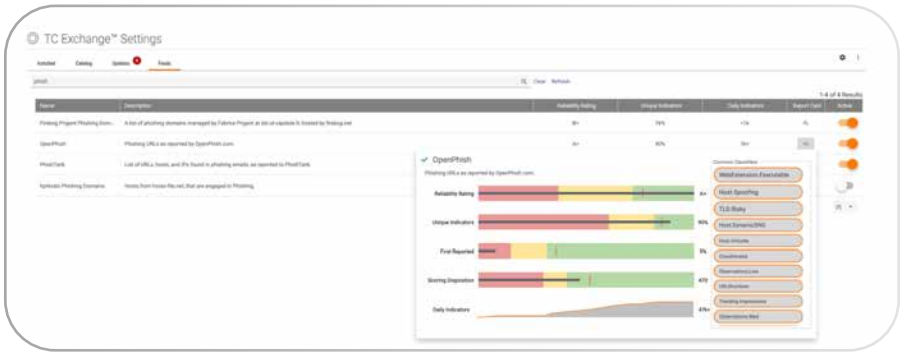
6 ICANN. (2017). Domain Name Registration Process. Retrieved from https://whois.icann.org/en/domain-name-registration-process

In the following example, we use the State of Arkansas, but this could apply to any state.

Phishing in the "Natural State" of Arkansas

Suppose the Arkansas State Fusion Center (ASFC) has an intelligence requirement to illuminate credential harvesting activity affecting Arkansas residents[7]. Phishing Kits are notorious for masquerading as legitimate business websites, only to steal email addresses and passwords from unsuspecting victims so adversaries can later utilize the stolen credentials for their nefarious deeds. With this in mind, by navigating to the TC Exchange Feeds page, a Collection Manager could search for "phish" related feeds, assess their quality via **Metrics and Report Cards**, and then begin collecting data by simply toggling the ***Active*** button. At this point, URL and/or Host indicators download into the platform (Figure 4).

FIGURE 4 - Search for "Phish" Feeds, assess Report Cards, and Activate



In order to pinpoint Hosts/Domains affiliated with Arkansas, reviewing registrant and registrar Whois information for *country* and *state* metadata is key. Despite trends towards the use of privacy services to mask personal information in Whois records, many registrants forgo its use or simply remain unaware of this offering. If privacy services are indeed implemented, geographic details of the registrar may be displayed in place of the registrant's. Either way, the goal is to identify a touchpoint for abused Domain names by identifying the registrar or registrant for future engagement. In ThreatConnect, one method is to manually click the Whois checkbox for each Host indicator to populate the ***Whois*** tab using **Automated Data Services**, but this can be cumbersome for Analysts wanting to quickly identify Arkansas affiliated domains. Orchestrating activities to automatically process each new indicator added to the platform is more ideal. In this case, **Playbooks** are the answer.

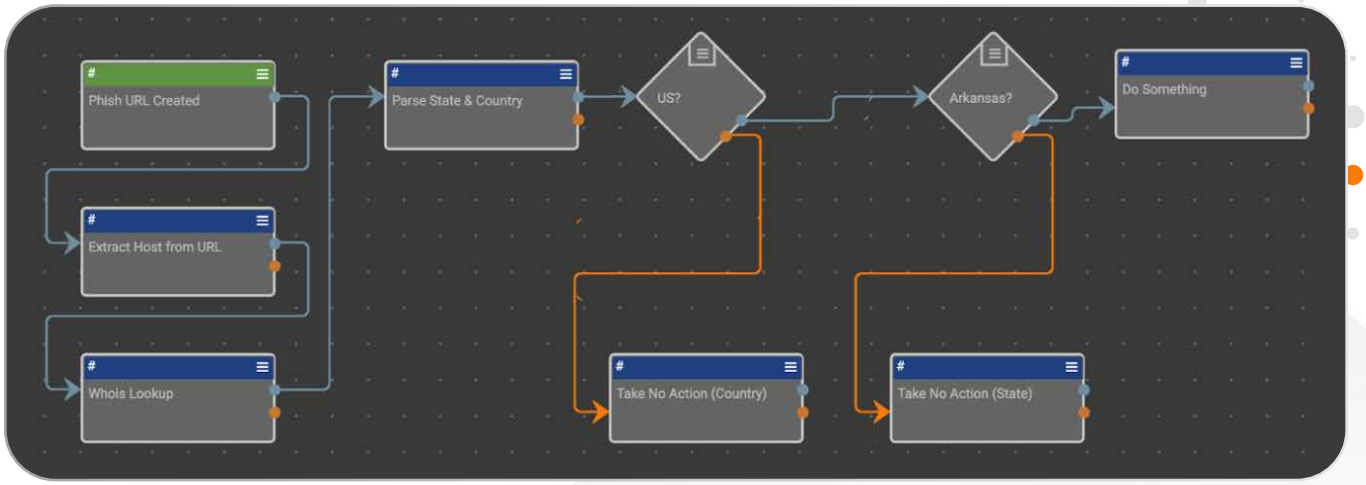
Phishing Kits are notorious for masquerading as legitimate business websites, only to steal email addresses and passwords from unsuspecting victims so adversaries can later utilize the stolen credentials for their nefarious deeds.

7 DHS. (2019). Fusion Center Locations and Contact Information. Retrieved from **https://www.dhs.gov/fusion-center-locations-and-contact-information**

A general Playbook workflow for identifying Arkansas-affiliated domains is illustrated in Figure 5. For each new phishing URL created in the platform, it *Triggers* the execution of the Playbook. The subsequent indicator processing actions are as follows:

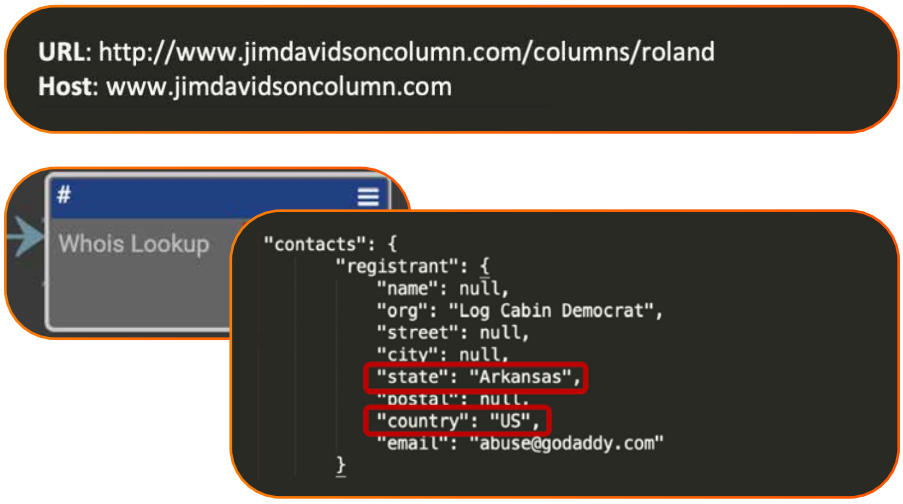
- Extract the Host/Domain name from the URL using Regular Expression (Regex) syntax
- Perform a Whois lookup for the extracted domain to retrieve its registration record
- Parse the State and Country from the returned Whois JavaScript Object Notation (JSON)
- If the registrant Country code is “US” then continue, otherwise take no action
- If the registrant State is “Arkansas” then continue (Do Something), otherwise take no action

FIGURE 5 - Evaluating Phishing Domain Whois Records containing an Arkansas Nexus



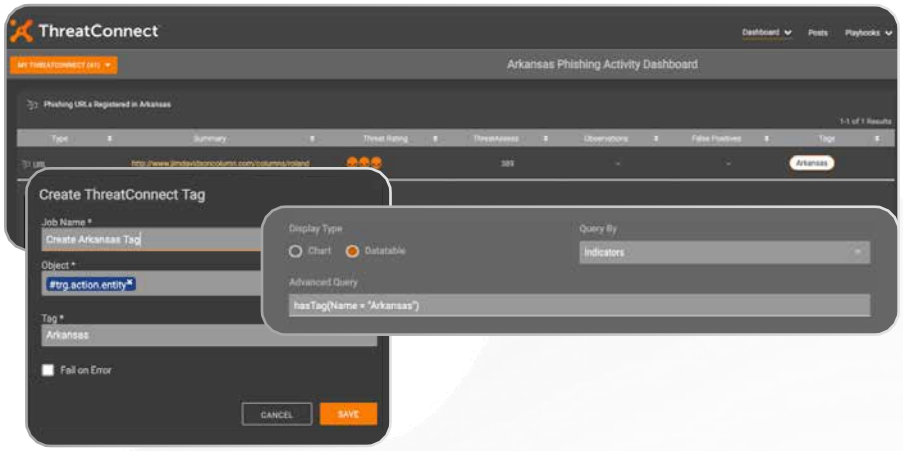
Perhaps over the course of several days, the Playbook finally discovers an Arkansas registered domain created by a phishing feed. As shown in Figure 6, a phishing URL triggered the Playbook; the host **www[.]jimdavidsoncolumn[.]com** was extracted; and a Whois Lookup was performed which generated JSON matching the Playbook's processing criteria. We now have an indicator candidate to "do something" with. But what to do?

FIGURE 6 - Automated Whois Lookup for Domain associated with Phishing Activity



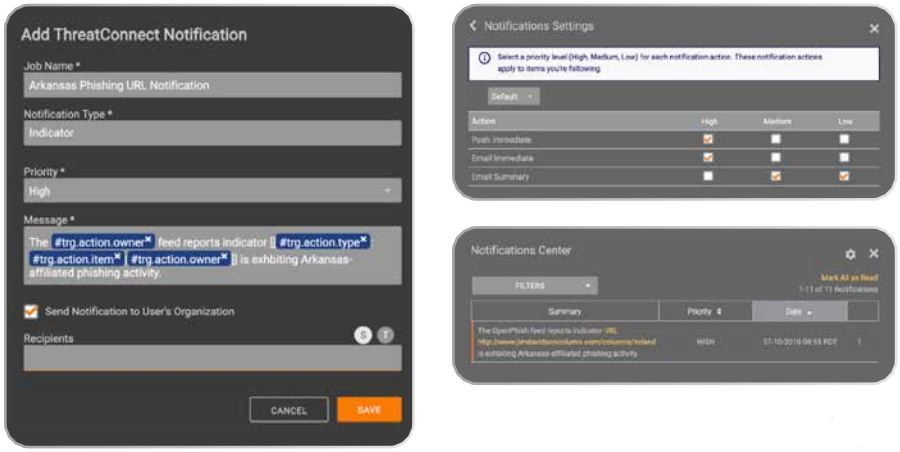
The beauty of a Playbook is that it's only limited by the user's imagination. In the above scenario, perhaps simply displaying the identified URL in a Dashboard by filtering on an "Arkansas" Tag using the ThreatConnect Query Language (TQL) is the extent of it. In which case, the Create ThreatConnect Tag app serves this purpose (Figure 7).

FIGURE 7 - Arkansas Phishing Activity Dashboard with Data Table Filtered by Tag



Due to the critical nature of the finding, immediately pushing a high priority notification may be required as well, in which case configuring the **Add ThreatConnect Notification** app to automatically interface with the **Notifications Center** is an option, along with a bit of **markup** to format the message (Figure 8).

FIGURE 8 - Configuring and Generating a Notification for Arkansas Phishing URLs



Between the Dashboard and Notifications Center, situational awareness concerning the newly discovered phishing URL is expediently disseminated to the platform's users. Follow-on activity may involve browsing to the URL's **Details Screen** and conducting manual analysis using third-party tools via the **Investigation Links** card. Alternatively, the Playbook's functionality could be expanded to include automated enrichment. Let's explore this possibility further.

A pillar of the ThreatConnect Platform is its ability to **integrate** with a variety of other platforms and tools. Since the focus of this demonstration is a phishing URL, using a "sandbox for the web" such as urlscan.io comes in handy[8]. A user can customize an integration by becoming familiar with the urlscan.io API and then developing **Playbook Components** to interface with it[9]. Deep-diving into the details of component creation is beyond the scope of this white paper, but suffice it to say that our goal is to automate the following activities:

- Generate an **Event Group** to capture phishing URL details for further triage and investigation
- Capture the Phishing Site image in a **Custom Attribute** named "Screenshot" using **markdown**
- Capture the victim's Home Page image in a "Screenshot" attribute
- **Associate** URL and Host indicators to the Event Group

8 Urlscan.io (2019). About urlscan.io. Retrieved from **https://urlscan.io/about/**

9 Urlscan.io (2019). Urlscan.io API v1. Retrieved from **https://urlscan.io/about-api/**

A pillar of the ThreatConnect platform is its ability to **integrate** with a variety of other platforms and tools. Since the focus of this demonstration is a phishing URL, using a "sandbox for the web" such as urlscan.io comes in handy[8].

By doing something "a little extra" with the Playbook, an Event is created using the **Create ThreatConnect Event** app; a Host indicator is created using the **Create ThreatConnect Host** app; the URL and Host indicators are associated to the Event group (Figure 9); and screenshots are added for the URL and Host indicators using the Create ThreatConnect Attribute app (Figures 10 & 11). Applying markdown Image formatting[10] to each attribute by referencing urlscan.io screenshots does the trick: **![Alt Text](url)**

FIGURE 9 - Playbook-generated Event with URL and Host indicator associations

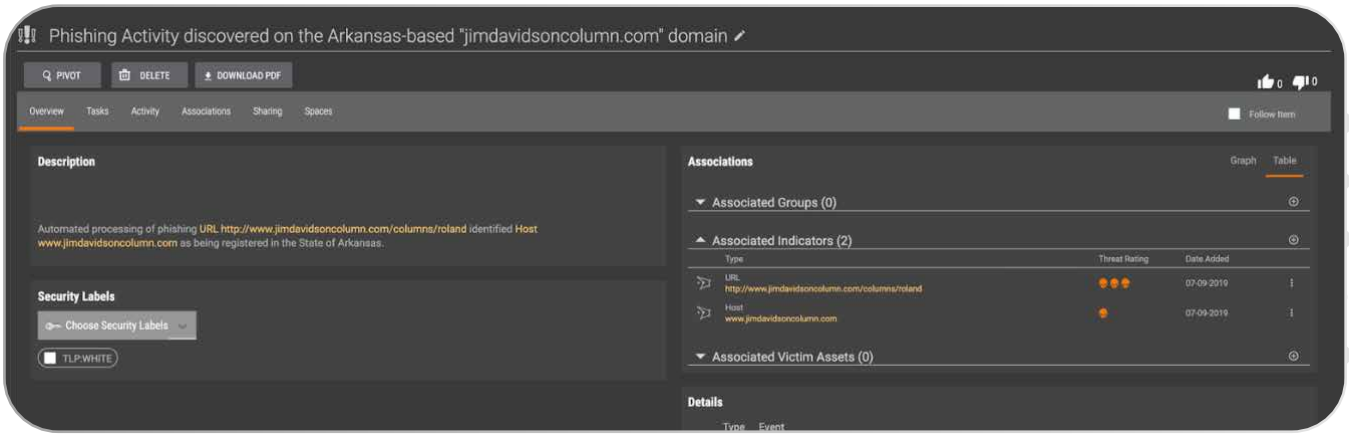
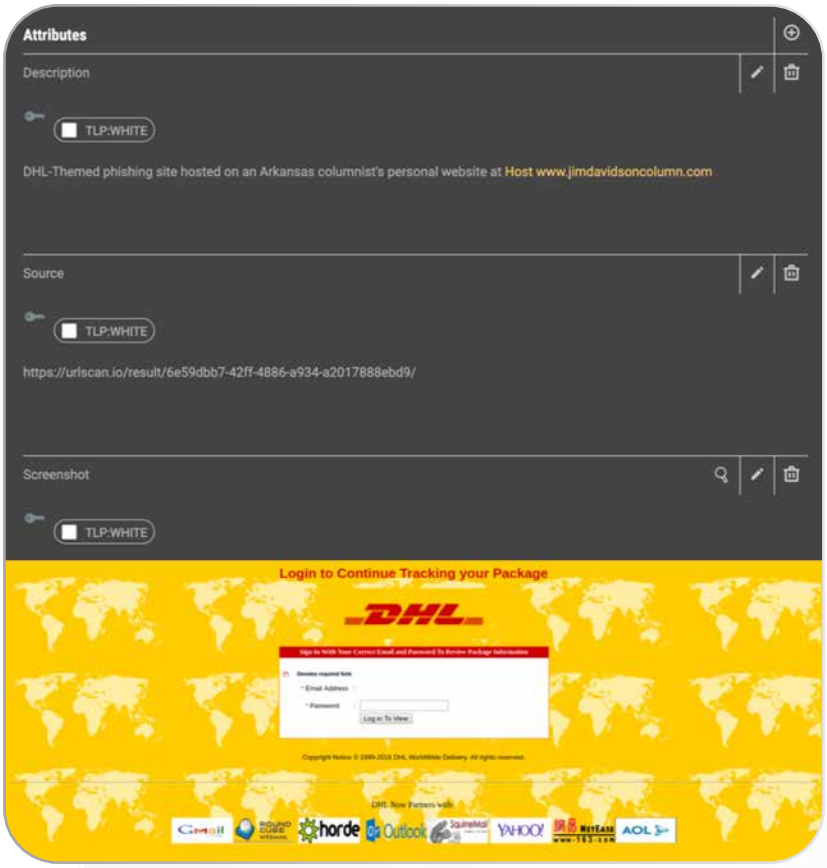
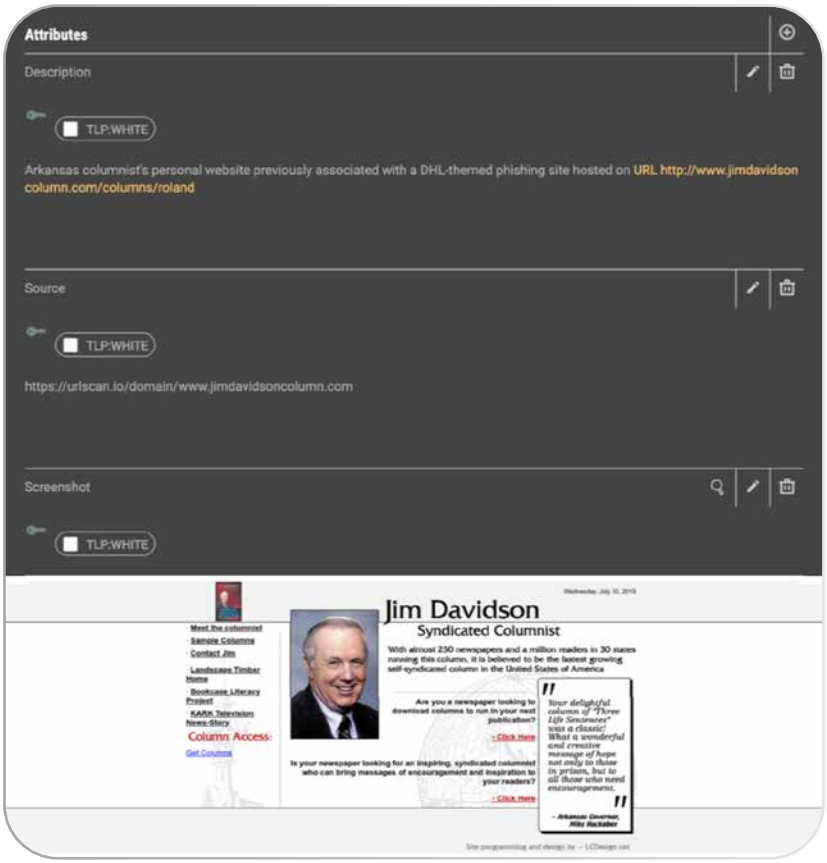


FIGURE 10 - URL indicator Attributes with Phishing Site Screenshot



10 Github Guides. (2014). Mastering Markdown. Retrieved from https://guides.github.com/features/mastering-markdown/

FIGURE 11 - Host indicator Attributes with Screenshot of Victim's Home Page



As the above figures reveal, an unauthorized DHL-themed phishing kit (Figure 10) is hosted on a compromised website belonging to Arkansas columnist Jim Davidson (Figure 11). It appears to be harvesting victim email address and password credentials. At this point, the Arkansas State Fusion Center could reach out to the website owner or domain registrar to takedown the phishing site. While certainly advisable at some point during the investigation, peeling back the onion a bit further to unveil additional artifacts is prudent.

While certainly advisable at some point during the investigation, peeling back the onion a bit further to unveil additional artifacts is prudent.

The phishing kit files residing on the compromised web server are likely coded to store and/or transmit the stolen credentials using server-side script (e.g. PHP). Unfortunately, only client-side script (e.g. JavaScript) is retrievable from a user's web browser (e.g. "View Page Source" in Google Chrome). Gaining direct access to these files would require permission from the hosting provider or registrant, a good topic to discuss during an engagement. Yet sometimes an adversary gets sloppy and leaves behind a preconfigured phishing kit archive (e.g., .zip file) which can be downloaded directly from the compromised website. This archive contains both client-side and server-side script. With some luck, a drop email account may be embedded in the code revealing the location where heavested creds are being sent. Luckily, in the case of the DHL phishing kit, its archive was left behind and its drop email account revealed (Figure 12).

FIGURE 12 - DHL Phishing Kit PHP Files, Code, and Drop Email Account

Aside from gaining direct access to the web server, acquiring operationalized phishing kits may be accomplished using scripts or third-party offerings. For example, at a premium cost, some vendors offer phishing kits previously extracted from known phishing sites[11]. Otherwise, various developers freely share scripting code such as Python-based StalkPhish[12], Analyst-Arsenal[13], and phish-collect[14] to name a few. More advanced ThreatConnect users may choose to develop their own custom Playbook App to collect phishing kits using the **App Builder** (the platform's native Python development environment). For further background concerning the collection and analysis of Phishing Kits, Duo Security[15] and PhishLabs[16] offer additional guidance.

11 OpenPhish. (2019). Phishing Feeds. Retrieved from https://openphish.com/phishing_feeds.html

12 StalkPhish by t4d. Retrieved from https://github.com/t4d/StalkPhish

13 Analyst-Arsenal by ecstatic-nobel. Retrieved from https://github.com/ecstatic-nobel/Analyst-Arsenal

14 Phish-Collect by Duo Labs. Retrieved from https://github.com/duo-labs/phish-collect

15 Duo Security. (2017). Phish in a Barrel; Hunting and Analyzing Phishing Kits at Scale. Retrieved from https://duo.com/assets/ebooks/phish-in-a-barrel.pdf

16 PhishLabs. (2013). How to Fight Back Against Phishing; a Guide to Mitigating and Deterring Attacks Targeting your Customers. Retrieved from https://info.phishlabs.com/hs-fs/hub/326665/file-558105945-pdf/White_Papers/How_to_Fight_Back_Against_Phishing_-_White_Paper.pdf

Leveraging State-level authorities, Arkansas may even consider engaging the email service provider associated with the Gmail-based drop email account, in this case Google. Individual users are able to audit their *Last Account Activity* to include session information, access type, and location (IP Address)[17]. As one can imagine, establishing an intelligence sharing relationship with Google which includes the gathering of these artifacts could contribute to the disruption and/or attribution of adversary activity. Reporting violations of Gmail Program Policies via their abuse form is a less formal approach[18]. In the end, drop email accounts, phishing kits, and compromised domains are another *means* for adversaries to wreak havoc on the Internet community.

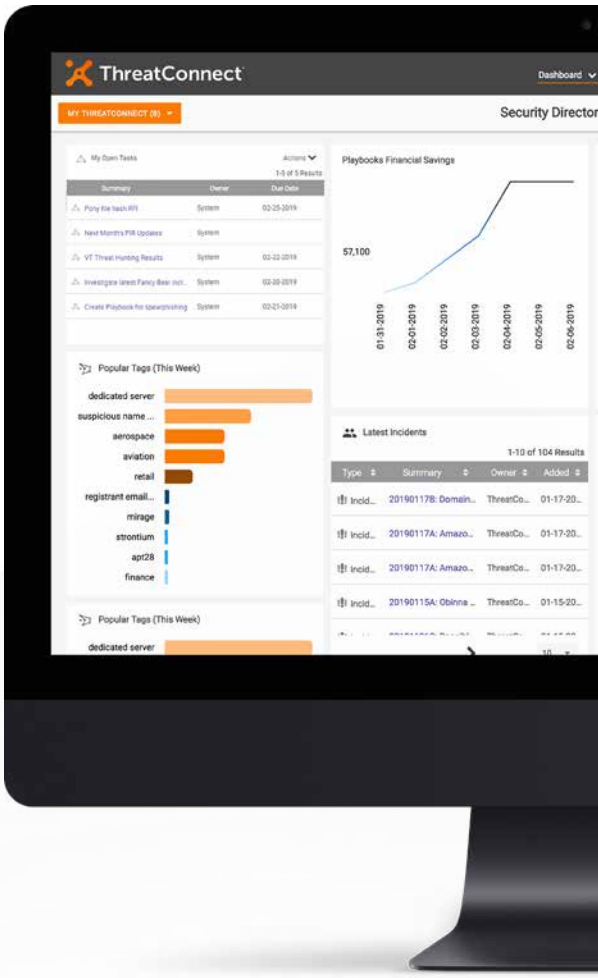
As one can imagine, establishing an intelligence sharing relationship with Google which includes the gathering of these artifacts could contribute to the disruption and/or attribution of adversary activity.

17 Google. (2019). GMail Help; Last Account Activity. Retrieved from https://support.google.com/mail/answer/45938?hl=en

18 Google. (2019). Gmail Program Policies. Retrieved from https://www.google.com/gmail/about/policy/

Conclusion

As State, Local, and Education (SLED) or State, Local, Tribal, and Territorial (SLTT) organizations ramp up their Cyber Fusion Center capabilities, ThreatConnect is without a doubt a mission-enabler[19]. New prospects to illuminate and disrupt adversary infrastructure is materializing, particularly for those governments willing to exert their public authorities on behalf of private communities and organizations. To help manage the risk, the platform's ability to aggregate, analyze, and act upon abused domain infrastructure is but one use case of many. Automation and collection via **Playbooks**, **Automated Data Services**, **Feeds**, and **Integrations**; situational awareness via **Dashboards**, **TQL**, and **Notifications**; and customization via **Tags**, **Attributes**, **markup**, **markdown**, and **App Builder** provide an endless amount of capabilities to enhance and streamline an organization's intelligence analysis workflow.



19 Department of Justice (DoJ). (2015, May). Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers. Retrieved from https://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers