WHITE PAPER

DISRUPTING ADVERSARY INFRASTRUCTURE

ThreatConnect Tactics to Encourage Internet Service Provider and State Entity Collaboration

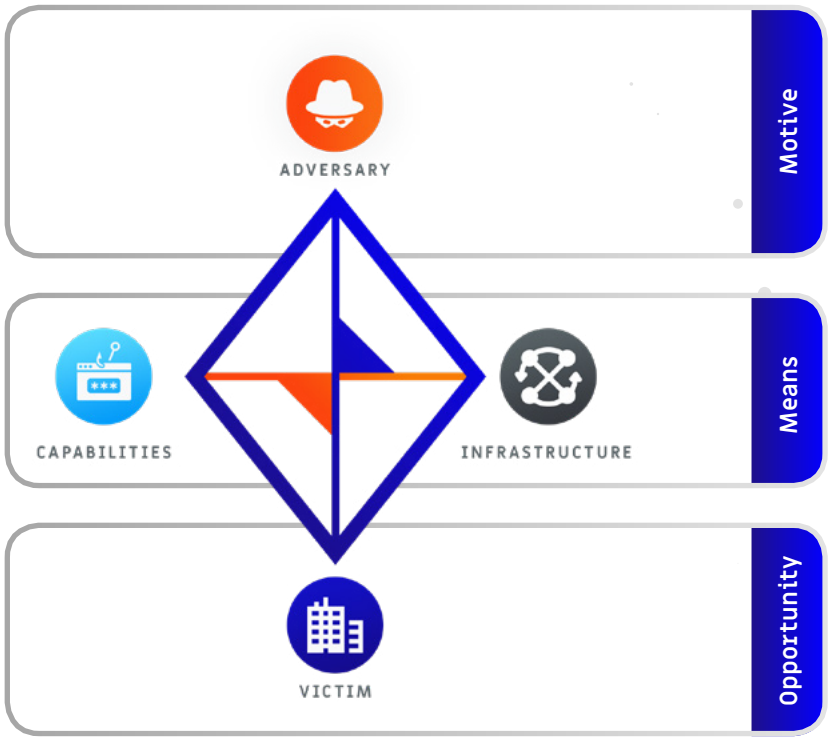
ThreatConnect™

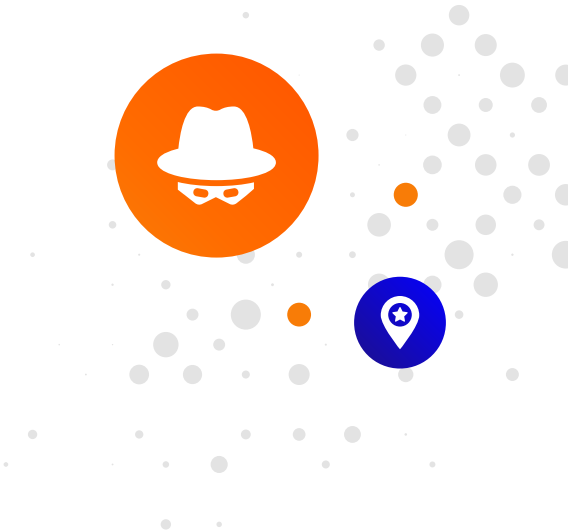
www.ThreatConnect.com

Obligations to Disrupt Adversary Infrastructure

Organizations relentlessly battle *adversaries* to maintain adequate levels of Cyber Mission Assurance (CMA), while Threat Analysts remain consumed with researching and can only hypothesize who the next *victim* may be. This unfortunate state of affairs is a consequence of motivated enemies who seemingly operate with impunity, wielding their offensive *capabilities* to weaponize Internet *infrastructure* by exploiting a vast landscape of vulnerabilities or dipping into private funds to lease servers. As illustrated by the Diamond Model (Figure 1), without infrastructure, an adversary's *means* to exploit an *opportunity* is severely degraded, if not eliminated.[1] Without infrastructure, an enemy's motivation to commit harm through cyberspace dwindles.

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/

To lessen an organization's burden, Internet Service Providers (ISPs) and local governments would ideally bring their own people, processes, and technologies to the conflict. Experts have written extensively about the utility of private-public partnerships for bolstering cybersecurity efforts. Security law professor Oren Gross suggested that "the growing challenges of cybersecurity incidents require streamlined processes for collaboration and exchange of information...and acknowledgement that every state, whether a source state for such incident or a state directly affected by the incident, must bear some responsibility to prevent, mitigate, manage, and ultimately recover from such incidents."[2] In the United States, local governments and federal institutions are indeed responsible for maintaining the territorial integrity of the Union to include the Internet infrastructure residing within their jurisdiction. In fact, the Department of Justice (DoJ) provides guidance for establishing State and major urban area cyber fusion centers suggesting collaboration with providers of internet services, website hosting, and mobile platforms.[3]

ISPs generally provide some level of cybersecurity protection, but researchers at the Institute for Homeland Security Solutions recognize that costly and legal barriers inhibit ISPs from doing more. Yet incentives offered by government regulation and subsidies, coupled with increased ISP engagement for victimized customers could certainly help.[4] Due to the routable IP addresses under their control, some ISPs accept their strategic role in countering malicious activity, but also acknowledge there's "no magic bullet."[5] To contain a botnet outbreak, one mid-sized ISP examined the efficacy of working more closely with its customers to quarantine infected devices into a "walled garden" instead of merely disseminating victim notification emails, an effort which resulted in a considerably high remediation rate.[6] Adopting a reference model for botnet mitigations, sharing intelligence with peers, and collaborating with law enforcement agencies is also prudent.[7] Without question, opportunities for cleaning up the Internet exist, but a robust Threat Intelligence Platform (TIP) is needed to detect and diminish the threat.

"the growing challenges of cybersecurity incidents require streamlined processes for collaboration and exchange of information...and acknowledgement that every state, whether a source state for such incident or a state directly affected by the incident, must bear some responsibility to prevent, mitigate, manage, and ultimately recover from such incidents."

OREN GROSS

2 Gross, O. (2015). "Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents," Cornell International Law Journal: Vol. 48 : Iss. 3 , Article 1. Retrieved from http://scholarship.law.cornell.edu/cilj/vol48/iss3/1

3 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

4 Rowe, B., Reeves, D., & Gallaher, M. (2009). The Role of Internet Service Providers in Cyber Security. Institute for Homeland Security Solutions. Retrieved from https://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf

5 Kan, Michael. (2017, February 23). Amid Cyberattacks, ISPs try to Clean Up the Internet. Retrieved from https://www.csoonline.com/article/3173274/amid-cyberattacks-isps-try-to-clean-up-the-internet.html

6 Cetin, O., Ganán, C., Altena, L., Kasama, T., Inoue, D., Tamiya, K., ... & van Eeten, M. (2019). Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai. Retrieved from https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-2_Cetin_paper.pdf

7 Pijpker, J., & Vranken, H. (2016, August). The Role of Internet Service Providers in Botnet Mitigation. In 2016 European Intelligence and Security Informatics Conference (EISIC) (pp. 24-31). IEEE. Retrieved from http://www.csis.pace.edu/~ctappert/papers/proceedings/2016EISIC/data/2857a024.pdf

Whether monitoring open source intelligence (OSINT) feeds for meaningful context or harnessing the power of **curated intelligence** published by ThreatConnect's Research Team, **ThreatConnect Query Language** (TQL) and **Dashboard** features facilitate "bubbling up" and visualizing compromised Internet infrastructure. To illustrate the point, the following vignette evaluates suspicious IP addresses presumably residing within New York's borders.

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

Evaluating "Empire State" Infrastructure

Advocating for the establishment of a "Office of Cyber Command" in New York City, Councilman Ritchie Torres warned, "It's often said New York City is the No. 1 terror target in the world — that statement is as true in cyberspace as it is in physical space."[8] Like virtually every other State in the Union, New York has experienced its share of breaches in recent months including unauthorized cryptocurrency mining[9] and disruptive ransomware.[10] Regardless of the nature of the compromise, attacks tend to traverse multiple ISPs, whether foreign or domestic, with the exception of an adversary who may assault an operational network exclusively from the inside. Therefore, it's in New York's best interest to regularly engage ISPs headquartered in the State to garner a mature understanding of their past successes and ongoing challenges. Using **TQL** filtering parameters (Table 1) and **Dashboards**, let's datamine ThreatConnect's existing IP address indicators to identify a potential candidate for future engagement.

TABLE 1 - TQL Filtering Parameters for Address Indicators

Parameter	Data Type
addressASN	Integer
addressCIDR	CIDR Expression
addressCity	String
addressCountryCode	String
addressCountryName	String
addressRegisteringOrg	String
addressState	String
addressTimeZone	String

8 Jorgensen, J. (2018, December 10). Exclusive: Councilman Proposes Creating 'Office of Cyber Command' for NYC to Combat Hackers. Retrieved from **https://www.nydailynews.com/news/politics/ny-pol-cyber-command-ritchie-torres-nyc-20181207-story.html**

9 Jerome, E. (2018, October 11). New York County Cyberattack Prompts State CIRT Response. Retrieved from **https://www.govtech.com/security/New-York-County-Cyberattack-Prompts-State-CIRT-Response.html**

10 Moench, M. (2019, April 1). Albany Cyber Attack Affecting Records, Police. Retrieved from **https://www.timesunion.com/news/article/Albany-police-can-t-access-scheduling-system-13730578.php**

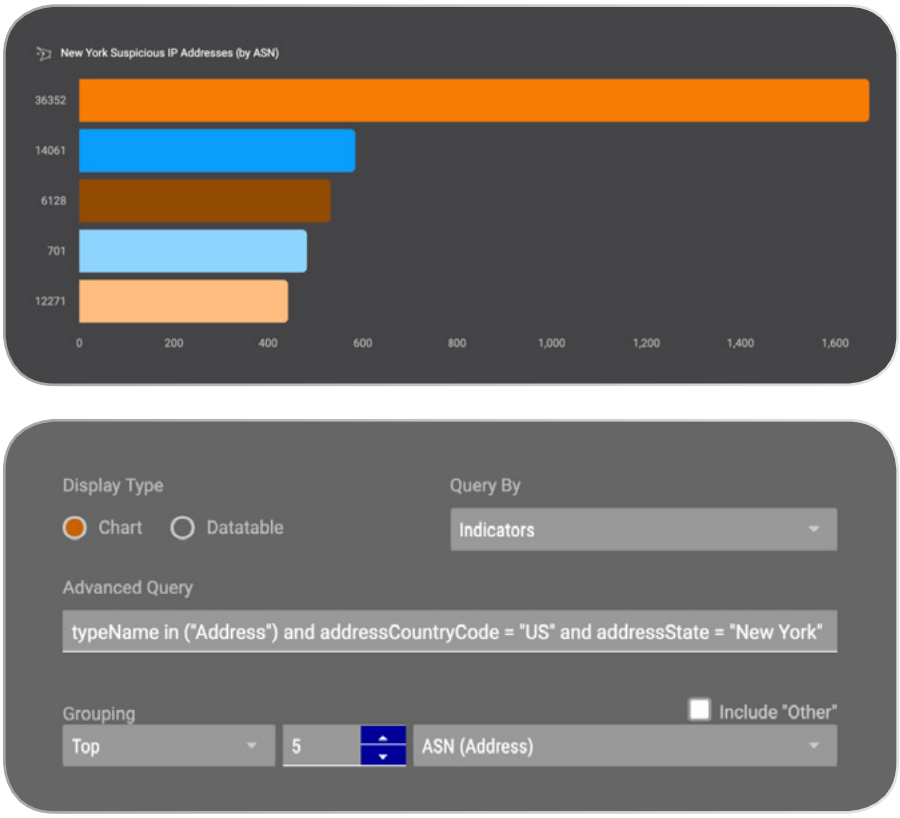
"It's often said New York City is the No. 1 terror target in the world — that statement is as true in cyberspace as it is in physical space."

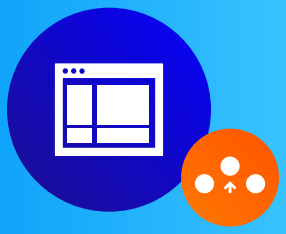
RITCHIE TORRES

For an initial analysis, a Dashboard card which counts all address indicators geolocated to New York and grouped by Autonomous System Number (ASN) will provide immediate situational awareness for determining which ISPs are hosting the highest quantity of suspicious indicators. Upon review, one ASN in particular immediately stands out, exhibiting more than double the amount of suspicious indicators when compared to the other four (Figure 2).

FIGURE 2 - New York Suspicious IP Addresses (by ASN)

TQL: typeName in (“Address”) and addressCountryCode = “US” and addressState = “New York”

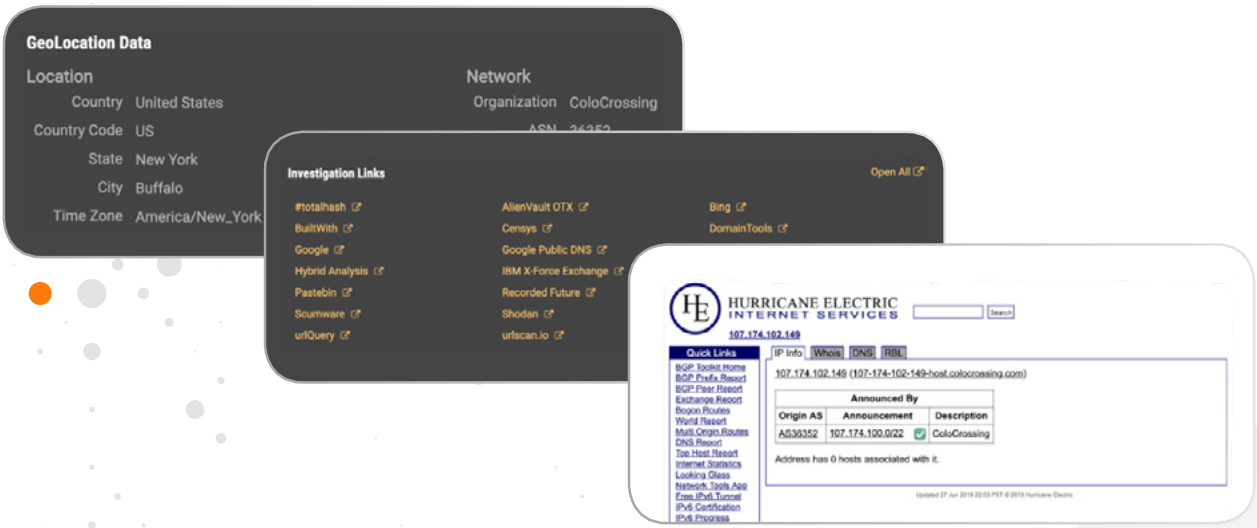




For an initial analysis, a Dashboard card which counts all address indicators geolocated to New York and grouped by Autonomous System Number (ASN) will provide immediate situational awareness for determining which ISPs are hosting the highest quantity of suspicious indicators.

Zeroing in on ASN 36352 data requires a simple click on the charted horizontal bar thereby opening a separate browser tab unveiling a **Browse** screen with nearly 1,600 IP addresses. By choosing the first IP address in the list, the **Details Screen** presents the indicator's IP Geolocation Data derived from **Automated Data Services**. If further confirmation is desired, investigative links permit analysts to immediately pivot to third-party sources such as Hurricane Electric Internet Services (Figure 3). The investigation uncovers ColoCrossing, an information technology services company headquartered in downtown Buffalo, as the owner of ASN 36352. Per their website, the business operates data centers in New York City, Dallas, Atlanta, Chicago, Seattle, Los Angeles, San Jose, and Buffalo.[11]

FIGURE 3 - Leveraging Automated Data Services and Investigation Links to Confirm ASN Ownership



With ColoCrossing headquartered in Upstate New York, members of the New York State Intelligence Center (NYSIC) could realistically establish a one-on-one engagement, or better yet a formal public-private partnership for **intelligence sharing** to collectively combat threats targeting statewide network infrastructure.[12] Before doing so, a few additional insights can be gleaned from the platform's contents.

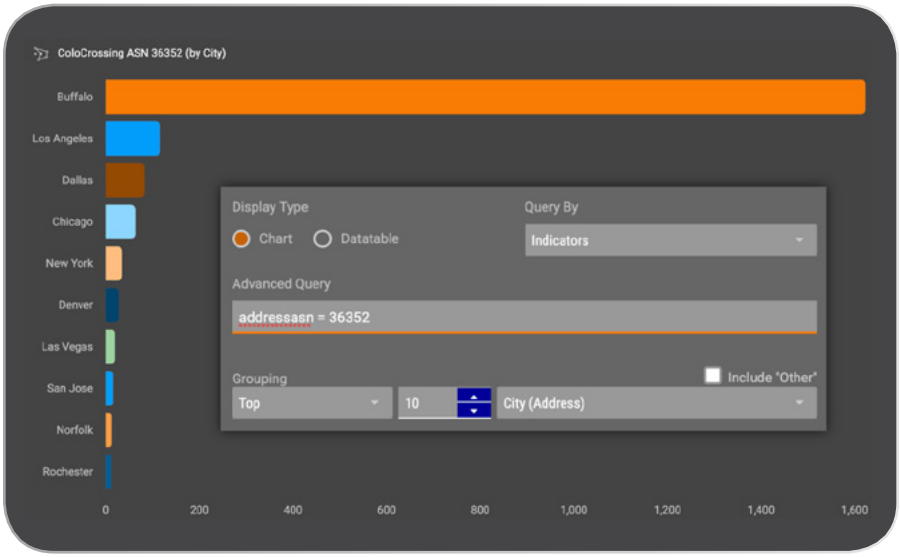
11 ColoCrossing. (2019). Our Company. Retrieved from **https://www.colocrossing.com/company/**

12 Bureau of Justice Assistance (BJA). Fusion Centers and Information Sharing. Retrieved from **https://www.ncirc.gov/documents/public/nysic_low_res.pdf**

Since ColoCrossing claims to have multiple U.S. data centers. it would be worth illuminating which cities predominantly exhibit threat activity. Perhaps one particular data center is experiencing an infectious outbreak. Maybe the outbreak is a consequence of a tenant's poor cybersecurity posture. Worse yet, a specific data center or tenant may have been directly targeted by an adversary. Using a simple TQL query such as ***addressasn = 36352*** and grouping the results by ***City***, it becomes immediately apparent that the city of Buffalo is the main source of anomalies to include New York City and Rochester (Figure 4).

If ColoCrossing confirms a previous or ongoing breach, the artifacts collected during the incident response process would surely generate native intelligence valuable for NYSIC operations. If warranted, local law enforcement personnel could offer assistance. If a foreign nexus is exposed, the Federal Bureau of Investigation (FBI)[13] or the International Criminal Police Organization (INTERPOL) Cybercrime unit could be called on.[14] Either way, an ISP such as ColoCrossing could leverage NYSIC's guidance and authorities to improve their condition. Lessons learned from the partnership could be applied elsewhere within the State.

FIGURE 4 - ColoCrossing ASN 36352 Suspicious IP Addresses Grouped by City



Since ColoCrossing claims to have multiple U.S. data centers. it would be worth illuminating which cities predominantly exhibit threat activity. Perhaps one particular data center is experiencing an infectious outbreak.

13 Federal Bureau of Investigation (FBI). (2019). Addressing Threats to the Nation's Cybersecurity. Retrieved from https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view

14 INTERPOL. (2019). Cybercrime. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

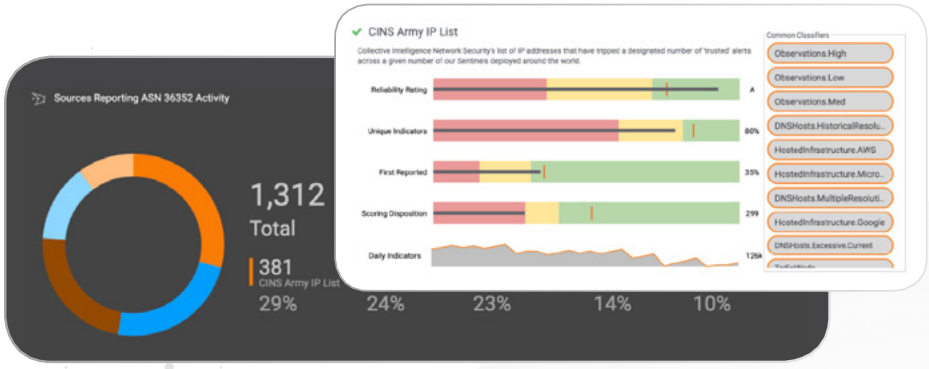
With ISP ownership and locality firmly established, additional context surrounding the nature of said suspicious activity is needed. By modifying the previous Dashboard card to group by ***Owner Name*** instead of *City*, and using an Advanced Pie Chart instead of a Horizontal Bar Chart, the card now shows various OSINT sources listed by percentage of coverage. With the CINS Army IP List reporting 29% of the activity, it's worth evaluating the reliability of the feed before confronting ColoCrossing with the findings.[15] Fortunately, ThreatConnect **Report Cards** provide the insight needed to characterize a feed by calculating its reliability, uniqueness, first reported, scoring disposition, daily indicator quantities, and common classifiers. In the case of the CINS Army IP List, it receives an "A" grade for reliability signifying a low False Positive (FP) rate. It's 80% uniqueness rating is also impressive, indicating that only 20% of the feed's indicators are found elsewhere in the platform (Figure 5). It's fair to say that ColoCrossing and the State of New York have valid cybersecurity challenges to tackle.

Setting aside the clear utility of evaluating data and information to identify risk, what about the intelligence? Luckily we have a TQL query for that! The **ThreatConnect Data Model** supports various Groups of intelligence. For the purpose of this exercise, ***Incident*** Groups will be the focus. Also, instead of fixating on one ColoCrossing ASN, the company may in fact have several. ASN 36352 just happened to exhibit the most suspicious indicators in New York during our initial evaluation. To expand the search, instead of using the ***addressASN*** parameter, the ***addressRegisteringOrg*** parameter will be used in its place.

Lastly, in order to present intelligence Groups associated with indicators instead of the indicators themselves, **nested queries** must be configured. Using the ***hasIndicator()*** keyword, the following TQL produces the cards in Figure 6:

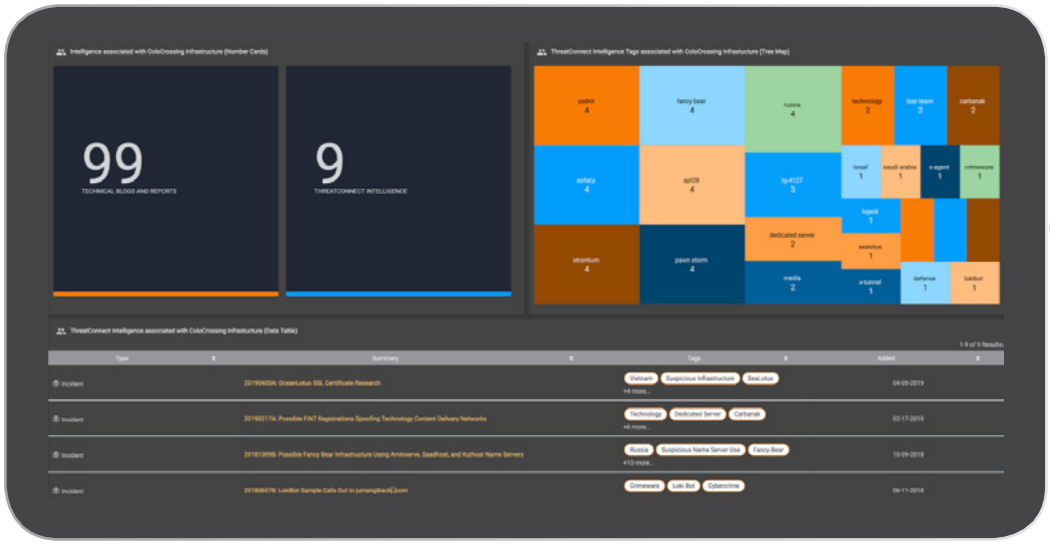
FIGURE 5 - Sources Reporting ASN 36352 Suspicious IP Addresses and Report Card Example

TQL: typeName in ("Incident") and hasIndicator(typeName = "Address" and addressRegisteringOrg = "ColoCrossing")

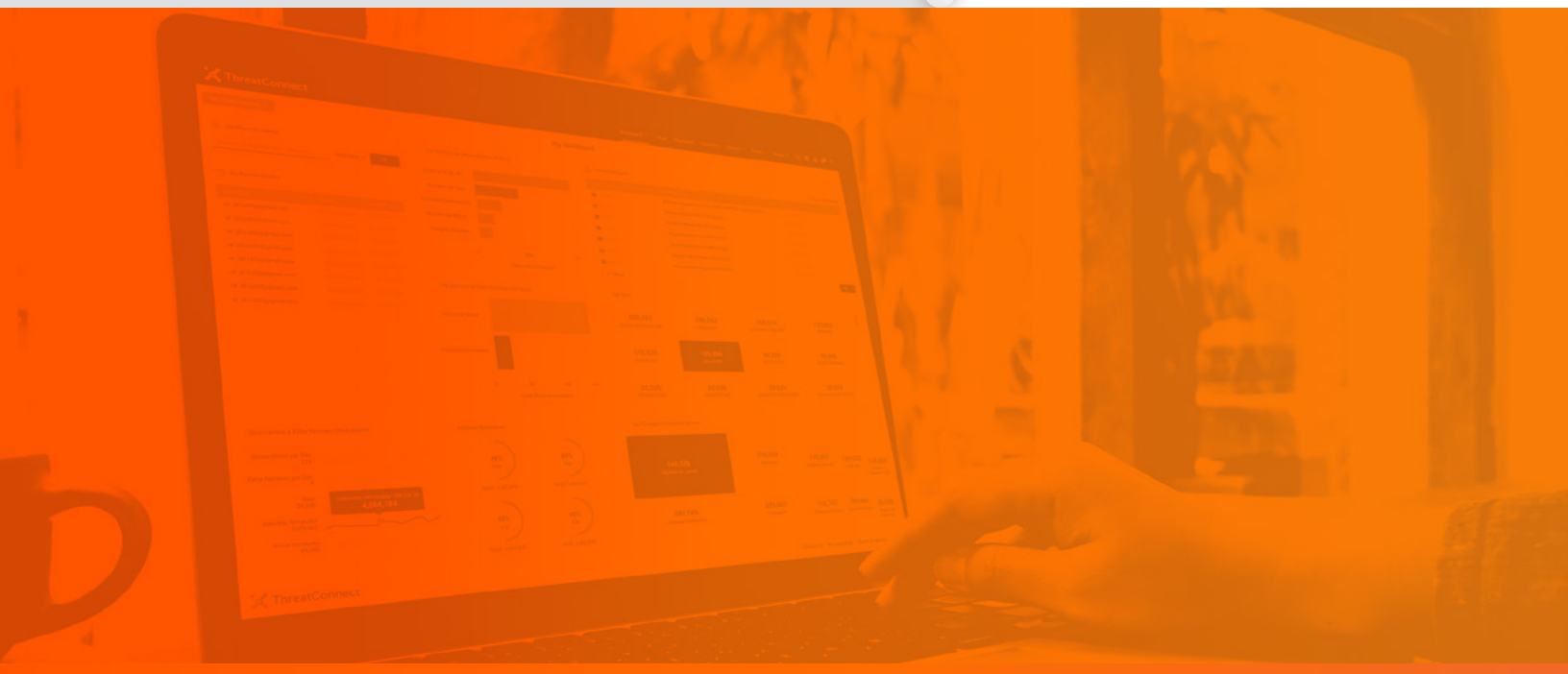


15 Collective Intelligence Network Security (CINS). CINS Army List. Retrieved from https://cinsarmy.com/list-download/

FIGURE 6 - Intel associated with ColoCrossing Infrastructure (Number Cards, Tree Map, & Data Table)

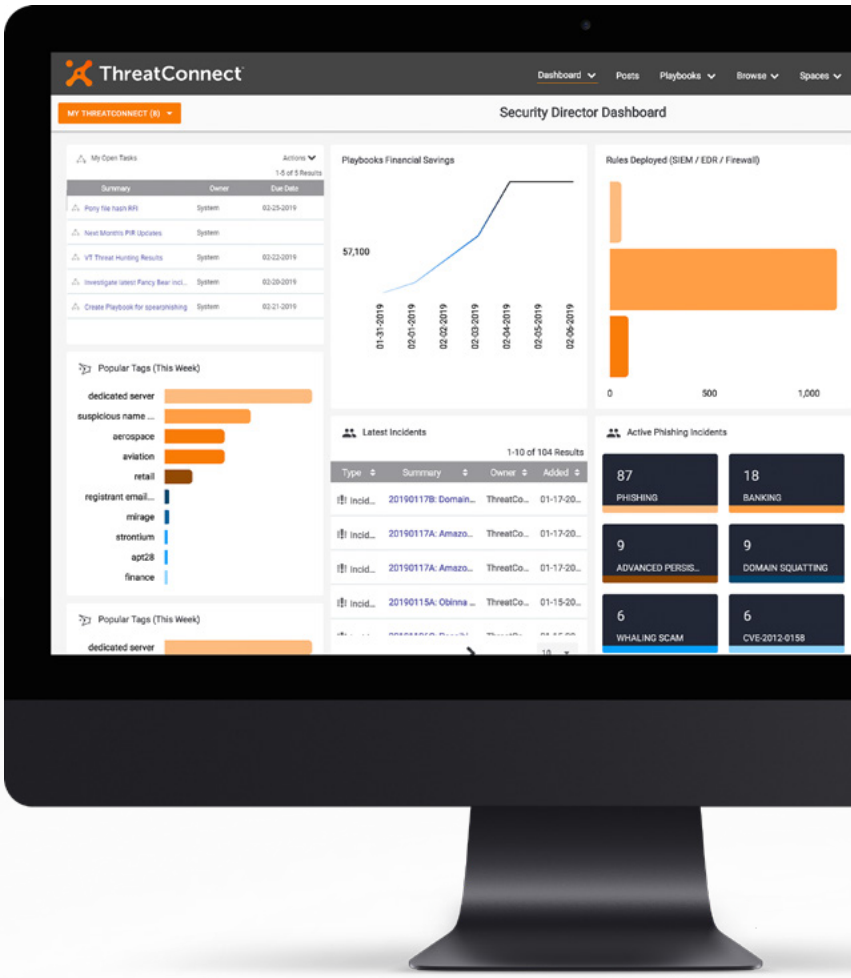


As the **Number Cards** in Figure 6 reveal, the **Technical Blogs and Reports** and **ThreatConnect Intelligence** sources contain Incidents correlated to ColoCrossing IP address indicators. Presented on the same Dashboard is a **Tree Map** of Tags and a **Data Table** of Incidents associated only with the ThreatConnect Intelligence source. At first glance, persistent threat actors such as Fancy Bear, FIN7, and OceanLotus may have commandeered or procured New York-based network infrastructure. Before raising alarm, performing additional analysis and assigning **threat/confidence ratings** is a judicious approach, particularly since IP addresses tend to be the most volatile indicators of compromise (IOCs).



Conclusion

Organizations need relief from the incessant cyber attacks that seem to originate from every corner of the Internet. The ThreatConnect tactics presented thus far are intended to encourage ISP and government collaboration with a keen focus on disrupting adversary infrastructure falling under their purview. By aggregating and assessing sources; geolocating and validating malicious infrastructure; and linking indicators to suspected threat actors, customers and citizens ultimately benefit from a less hostile cyberspace environment thanks to intensified intelligence sharing efforts. Despite the volatility of IP addresses, when evaluated within the context of ISP-owned ASNs and the authorities granted to State entities, more could be done and should be done.



ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit www.ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708

Copyright © 2019 ThreatConnect, Inc.