

# Identifying Additional Insights on Cyber Adversaries: A ThreatConnect Customer Success Story

ſ

!

\*



### Customer's Problem:

A small threat intelligence team needed additional insights on several cyber adversaries that posed a risk to their organization. The customer reached out to the ThreatConnect's Customer Success and Research teams seeking additional information.

CUSTOMER'S TWO PRIMARY OBJECTIVES:

- Validate their own findings regarding the adversaries they were tracking.
- Identify any known intelligence and operations gaps in analysis that pose a risk to themselves and their environment.

## ThreatConnect's Solution

The ThreatConnect Research Team created a private community for the customer to enhance collaboration regarding their adversaries. The customer shared the information about the adversary that they were tracking with the Research team to do their own validation.

Creating a private community allowed the customer to interact with the ThreatConnect Research team and provide comments and analytical notes on the threats, adversaries, and infrastructure involved - all while working within the ThreatConnect Platform. Working within the private community allows only invited users to participate in the effort.

# Results

The ThreatConnect Research Team was able to identify additional adversarial assets including social media accounts and forum handles that were previously unknown to the customer's team.

- After a thorough analytical review of the customer's indicators, the ThreatConnect Research team identified a subset of threat activity previously identified within six ThreatConnect Communities and eight ThreatConnect Sources, including the ThreatConnect Intelligence feed and Technical Blogs and Reports source.
- The ThreatConnect Research team provided their finished analysis to the customer and provided best analytical practices on how to correlate and pivot for specific threats across the different sources within ThreatConnect.
- The additional findings from the Research team provided the customer with additional rules and signatures for network detection while simultaneously enhancing their knowledge of specific threats and adversaries.

	MY THREATCONNECT (8) 🔻		Security Director Dashboard				i		
	1.5 of		Playbooks Financial Savings Rules Deployed (SIEM / EDR / Firewall)			37 Recently Observed Indicators			
A	Summary Owner Due Date					Summary 🗢	Threat 🗢 Observ		
		_ /	·			209.99.40.223	420 204		
	Next Montris PIR Updates System VT Threat Hunting Results System 02-22-2019	57,100		-		72.52.4.119	484 153	-	
	A Investigate latest Pancy Bear Incl. System 02:20:019	_ /				188.29.165.194	389 136	-	
	A Create Playbook for spearphishing System 02-21-2019 O2-21-2019	_						95.7	
	ers Groene engyddole fan spearsening i gysterne i Sweartword	01-31-2019 02-01-2019 02-02-2019 02-03-2019	02-04-2019 02-05-2019 02-06-2019			81.241.108.114	389 119		
		01-3 02-0 02-0	02-0			193.137.92.201	389 102	-	
	>>> Popular Tags (This Week)					209.99.40.222	453 51	12	
	dedicated server			0 500	1,000	72.52.178.23	389 34	-	
	suspicious name	Latest Incidents		Active Phishing Incidents					
	aviation		1-10 of 104 Results				_		
	retail	Type © Summary © C	Dwner 🌣 Added 🗢	87	18	14	10		
	registrant email	1 Incid 201901178: Domain Th	hreatCo 01-17-20	PHISHING	BANKING	FINANCE	RUSSIA		
	mirage	11 Incid 20190117A: Amazo Th	01.17.20			_			
	apt28	iti incid 20190117A. Ainazo In	irealigo 01-17-20	9	9	8	7		
	finance	11 Incid 20190117A: Amazo Th	hreatCo 01-17-20	ADVANCED PERSIS	DOMAIN SQUATTING	SPOOFED	MIDDLE EAST		
		1 Incid 20190115A: Obinna Th	hreatCo 01-15-20						
	>>> Popular Tags (This Week)			6	6				

### What They Are Able To Do With ThreatConnect



#### About 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.



3865 Wilson Blvd. | Suite 550 | Arlington, VA 22203 sales@threatconnect.com P: 1.800.965.2708

**ThreatConnect.com** Copyright © 2019 ThreatConnect, Inc.