THREATCONNECT™

CASE STUDY

GO DEEPER AND DISCOVER NEW INTELLIGENCE WITH THREATCONNECT

SUMMARY:

This case study illustrates how an organization utilizing ThreatConnect® was able to develop a predictive network defense by taking a single indicator discovered from network traffic monitoring and finding additional indicators for more predictive analytics. This is a single example of a process that is repeatable for literally every known domain used for command and control of Trojan malware by the adversary. The organization utilizes ThreatConnect on a daily basis in this manner to keep ahead of threats by monitoring and tracking their infrastructure changes as they happen. In this study, we will show how the integration of services such as passive DNS (pDNS), Whois monitoring, and Reverse Whois Tracks within ThreatConnect enabled this organization to not only manage their threat intelligence knowledgebase, but to also grow their knowledge of network based threats in a dynamic manner.

Challenge

The organization's cyber threat team was charged with adding additional context and indicators to Security Operations Center (SOC) incident tickets. To do this effectively, the threat team needed to go to several sources to correlate information on a daily basis to provide relevant, accurate, and timely threat intelligence back to the SOC. This process did not scale, as it generated several tickets a day and analysis was static. There was also no way to know what threat movements occurred after the threat team had submitted the response to the ticket and moved to the next one.

What is ThreatConnect®?

ThreatConnect is the first and only Threat Intelligence Platform built to bridge incident response, defense, and threat analysis. Government agencies and Fortune 500 organizations worldwide leverage the power of ThreatConnect every day to aggregate, analyze, and act on their threat intelligence data. Available as both on-premise and in the cloud, ThreatConnect increases productivity and delivers dynamic knowledge management, high context indicators, and automated responses to counter sophisticated cyber-attacks.

Organization

Confidential

Industry

Government

Challenge

Organization had no way to aggregate the large influx of data on a daily basis to conduct deep analysis and produce actionable threat intelligence. Data was static and could not be updated in real-time.

Solution

ThreatConnect provided a dynamic knowledge and process management solution to create threat intelligence and discover new information.

Results

- One-Stop Shop
- Predictive Defense
- Dynamic Knowledge
- Management and Workflow

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 F +1.703.229.4489

THREATCONNECT™

CASE STUDY

Background

This government sector customer has a SOC with a small team dedicated to cyber threat analysis. The SOC provides intrusion detection tickets to the cyber threat team. Each ticket contains potential indicators of compromise found during SOC efforts. The cyber threat team is responsible for providing additional context and indicators back to the SOC to search for in their logs. ThreatConnect has been integrated into the Standard Operating Procedures (SOPs) of the cyber threat team to allow them to be more efficient in their daily duties.

Solution

The cyber threat team leveraged ThreatConnect to provide a dynamic knowledge management and a Threat Intelligence Platform to both store historic knowledge of threat indicators and the context around them, as well as provide multiple sources of intelligence within the platform to grow that knowledge. By pivoting on relationships between known threat indicators and newly discovered indicators, the team discovered new intelligence.

ThreatConnect also actively tracked infrastructure movements over time to keep defenses up long after the threat team provided the SOC with their initial intelligence. This helped keep the organization protected as the malicious infrastructure shifted.

Results

ONE-STOP SHOP

Without going to multiple sources, the threat team analyst was able to discover new email registrants, domains, subdomains, and IP address resolutions all related to the threat that was targeting them.

PREDICTIVE DEFENSE

The integration of DNS and Whois monitoring, pDNS, ReverseWhois Tracks, and registrant alerts into ThreatConnect was critical in creating situational awareness of known threat infrastructure activity, which enabled a predictive defensive posture against known persistent threats.

Dynamic Knowledge Management and Workflow

The cyber threat team was able to use ThreatConnect's workflow features and analytic tools to create threat profiles in ThreatConnect. These threat profiles were then continuously monitored for associated infrastructure. Context of all SOC tickets responded to, actions taken, and impact to the organization are all maintained within ThreatConnect to provide historical context and risk assessments of the threats.

DETAILS

The details of the events that occurred are masked due to operational considerations since the customer may still be a target of this adversary.

STEP 1

The intrusion detection (ID) analyst in the SOC came across suspicious connectivity to a domain while reviewing logs.

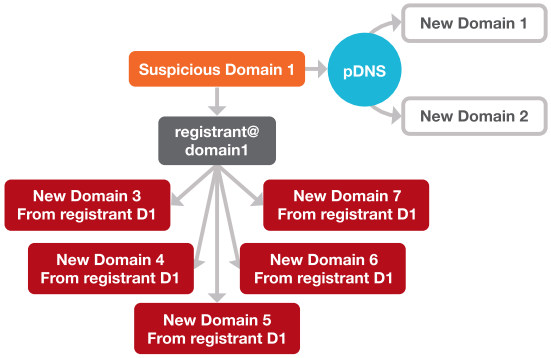
STEP 2

The intrusion detection (ID) analyst in the SOC came across suspicious connectivity to a domain while reviewing logs.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com
P 1.800.965.2708 F +1.703.229.4489

STEP 3

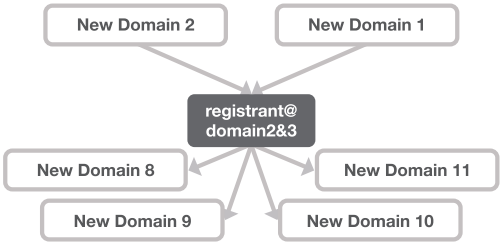
The cyber threat team entered the domain into ThreatConnect as a Host Indicator, and within seconds was able to find out who registered the domain as well as retrieved the passive DNS (pDNS) history on the additional domains. Using the Track feature with ThreatConnect to perform a Reverse Whois query, the registrant email address was linked to five additional suspicious domains with similar naming conventions. This discovery added to the confidence that these domains were all related to the same adversary. In addition, the pDNS history showed two additional domains that resolved to the same IP address. Both of these new domains had naming conventions which led the analyst to believe they were being used for malicious purposes.



STEP 4

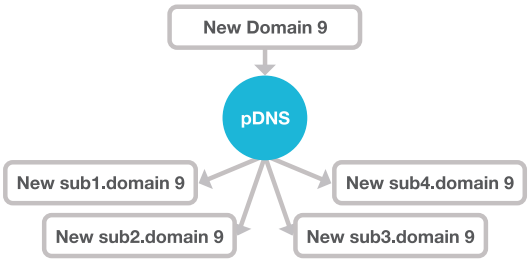
The cyber threat team was able to easily import the pDNS results as Indicators into their organization's account in ThreatConnect.

By using the Reverse Whois Track feature to query for additional domains using the same registrant email address of the domains found in the previous step, the team was able to reveal four additional domains that all appeared to be part ofthe adversary's infrastructure.



STEP 5

Upon further examination of "New Domain 9"*, the team was able to pivot by querying pDNS to discover another four subdomains. Two of the subdomains resolved to the same IP address.

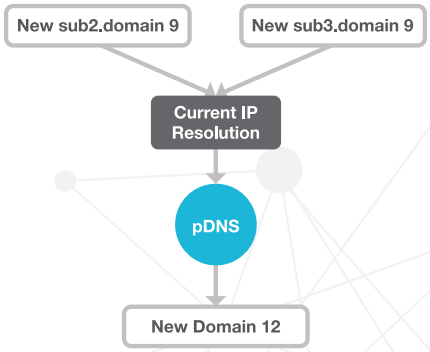


*"New Domain 9" was the only domain referenced in this case study. However, note that the same steps 5-7 were taken for all the newly discovered domains.

STEP 6

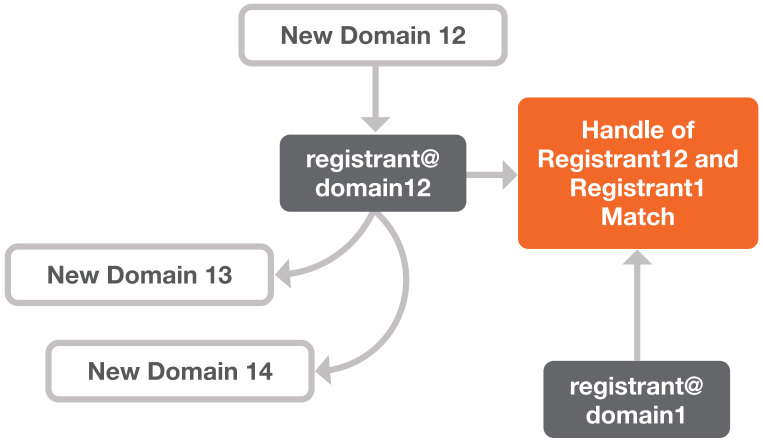
The analyst then conducted additional analysis on the IP address from sub2.domain9 and sub3.domain9, to discover three new results including New Domain 12.

This was the only additional domain resolving to that IP address and the naming convention was also deemed to be suspiciousby the cyber threat analyst reviewing this ticket.



STEP 7

With that information uncovered, a Reverse Whois Track was set up on the registrant information of “New Domain 12” which immediately found two additional domains to research and analyze. Further tying the activity together, the registrant handle of “New Domain 12” matches that of “New Domain 1”, showing a linkage that was previously not seen.



CONCLUSION

Cyber Threat Analysis today is often done manually and knowledge of threats is often kept in disconnected spreadsheets. This state of affairs does not scale and leaves troubling gaps in defenses. Whether performed by SOC members, malware analysts, incident responders, or full time cyber threat analysts; there is simply not enough time to research and keep up with the various network threats facing their organizations. All require a means to manage their knowledge of threats, make assessments on those threats, and keep up with them as they attempt to adapt to out maneuver current defenses.

ThreatConnect is the only commercial Threat Intelligence Platform that addresses these needs head on, increasing analyst efficiency, providing unique data through its multiple integrated data sets, allowing for team and community collaboration, and enabling direct action through defensive integrations with our powerful API. If you’d like to learn more about how ThreatConnect can enable dynamic Threat Intelligence for your organization, contact us at sales@threatconnect.com or sign up for a free trial here: http://www.threatconnect.com/platform/editions/#Community

CONNECT WITH US

Interested in learning more about how ThreatConnect can help unite your security team and protect your enterprise?

www.ThreatConnect.com

TOLL FREE: 1.800.965.2708
LOCAL: +1.703.229.4240
FAX: +1.703.229.4489