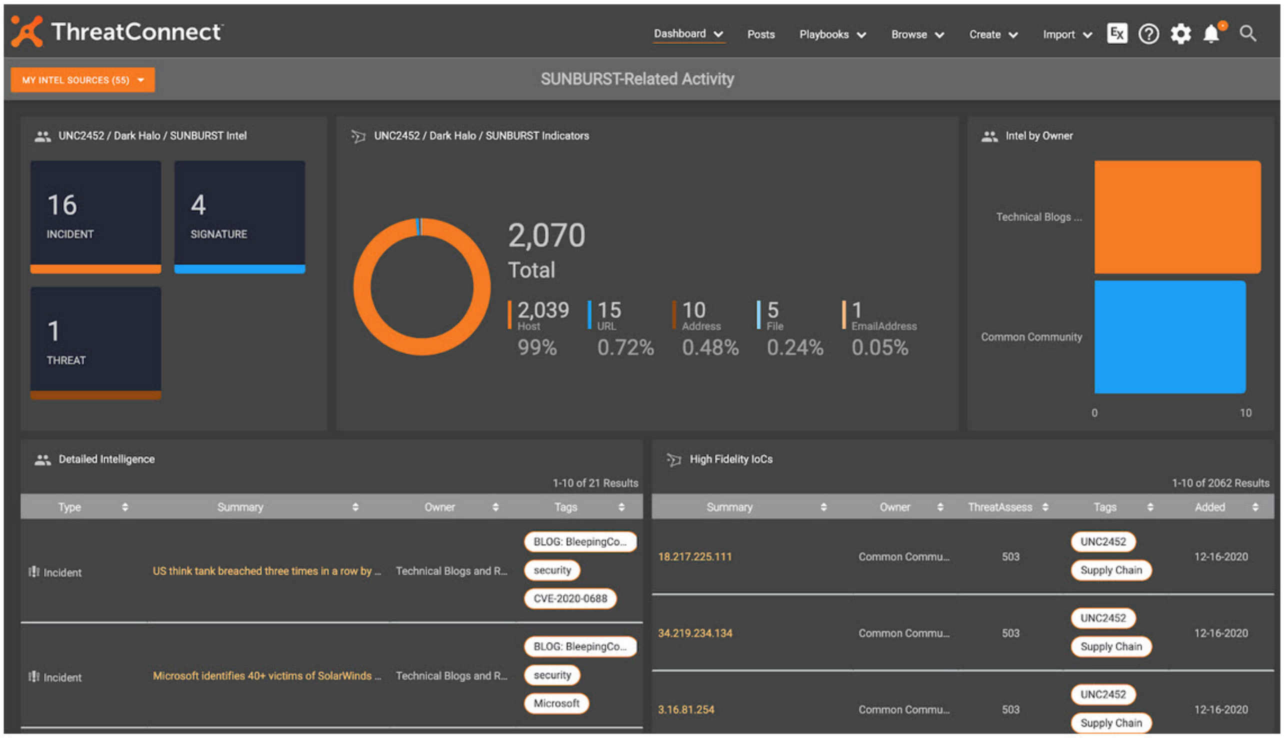
Tracking Sunburst-Related Activity with ThreatConnect Dashboards

December 18, 2020

Recently FireEye discovered that the SolarWinds Orion IT monitoring platform was compromised earlier this year. The threat actor used SolarWinds cryptographic keys to sign multiple backdoored files posing as Orion IT updates. These files contained a hidden backdoor that would communicate via HTTP to external servers after remaining dormant for up to 2 weeks. The malware disguised communications as legitimate data being sent to SolarWinds.

The number of organizations affected by this malware is what makes the attack remarkable. SolarWinds estimates approximately 18,000 customers installed these malicious updates, including private sector organizations, the US Departments of Treasury, Commerce and Homeland Security.

Available immediately to ThreatConnect users is a Dashboard that provides a single location to view relevant intelligence and indicators of compromise (IOCs) from across various sources related to the SolarWind event. The Dashboard helps consolidate intelligence that would otherwise take a large amount of time to identify in separate sources. Public Cloud users can now access a SUNBURST-Related Activity Dashboard by choosing clicking that link or navigating to ‘Dashboard’ and choosing it from the drop down.



UNC2452 / Dark Halo / SUNBURST Intel

16 INCIDENT

4 SIGNATURE

1 THREAT

UNC2452 / Dark Halo / SUNBURST Indicators

2,070 Total

2,039 Host	15 URL	10 Address	5 File	1 EmailAddress
99%	0.72%	0.48%	0.24%	0.05%

Detailed Intelligence

1-10 of 21 Results

Type	Summary	Owner	Tags
Incident	US think tank breached three times in a row by ...	Technical Blogs and R...	BLOG: BleepingCo... security CVE-2020-0688
Incident	Microsoft identifies 40+ victims of SolarWinds ...	Technical Blogs and R...	BLOG: BleepingCo... security Microsoft

High Fidelity IoCs

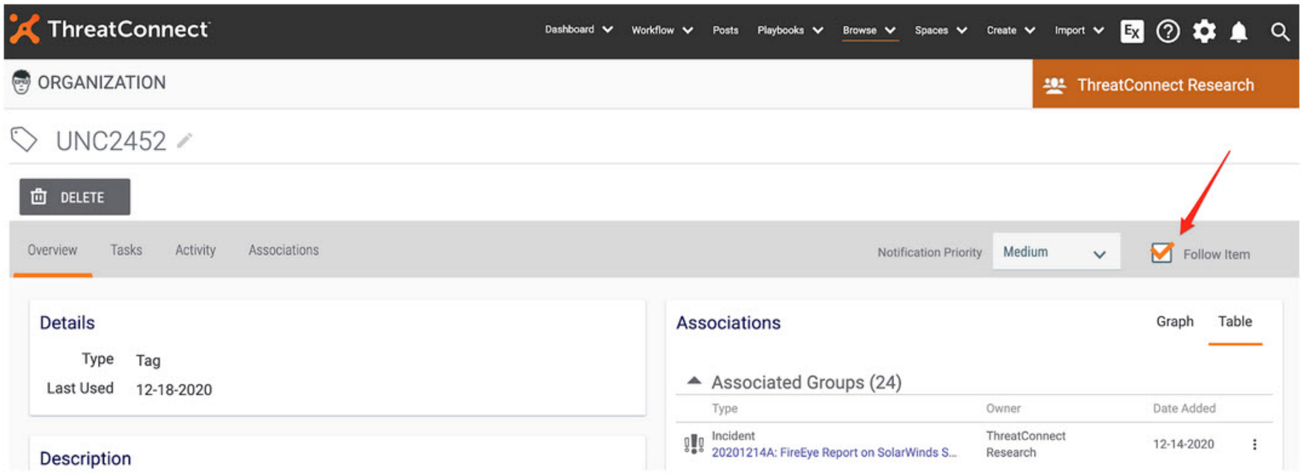
1-10 of 2062 Results

Summary	Owner	ThreatAssess	Tags	Added
18.217.225.111	Common Commu...	503	UNC2452 Supply Chain	12-16-2020
34.219.234.134	Common Commu...	503	UNC2452 Supply Chain	12-16-2020
3.16.81.254	Common Commu...	503	UNC2452 Supply Chain	12-16-2020

A Glimpse of the Activity Displayed on the SUNBURST-Related Activity Dashboard

For our customers leveraging our dedicated cloud or on-premises deployment options, the ThreatConnect Customer Success Team has built out instructions on how to create this dashboard in your own, private instance. Find a write-up outlining this process and how to create the necessary Dashboard cards in the ThreatConnect Learning Management System.

In addition to the Dashboard above, for individuals and organizations looking for proactive alerts to new intelligence and indicators related to this activity, ThreatConnect provides the Follow capability. Following tags like UNC2452, Dark Halo, or SUNBURST can generate an alert in the platform or to your email when that tag is applied to an indicator or group.



UNC2452

Notification Priority: Medium

☑ Follow Item

Details

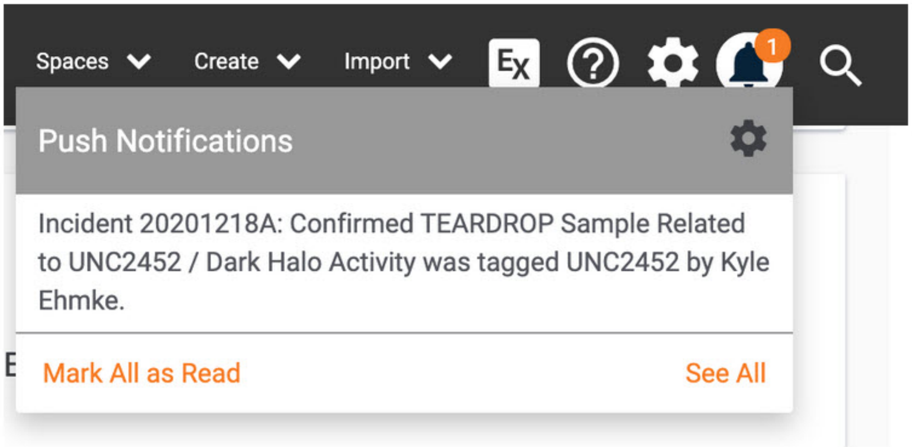
Type: Tag
Last Used: 12-18-2020

Description

Associations

Associated Groups (24)

Type	Owner	Date Added
Incident 20201214A: FireEye Report on SolarWinds S...	ThreatConnect Research	12-14-2020



Push Notifications

Incident 20201218A: Confirmed TEARDROP Sample Related to UNC2452 / Dark Halo Activity was tagged UNC2452 by Kyle Ehmke.

We hope that this information helps you answer some of the difficult questions around this recent series of attacks. Beyond just this specific instance, remember that you can modify these queries to create topical dashboards around whatever your high priority threats might be. TQL is your language for situational awareness.