



Cisco Stealthwatch WannaCry Incident Response Guide

On Friday, May 12 organizations around the world faced a new and very dangerous ransomware threat dubbed “WannaCry.” Cisco’s industry-leading Talos threat intelligence team, captured WannaCry in the wild and examined it. In a [blog post](#), the Talos team describes how Internet users can use Cisco solutions to defend their networks and computers against this malware and its potential variants that are expected over the next weeks and months.

With this threat, as with any newly discovered threat, two of the most important questions for incident responders are:

1. What is my current and past exposure to this threat?
2. Can I effectively monitor and control my ongoing exposure?

As a component of the Cisco Ransomware Defense, [Network as a Sensor](#), and [Network as an Enforcer](#) solutions, [Cisco Stealthwatch](#) can be leveraged to address these questions.

Infection Detection

The initial strain of WannaCry malware relies on the Server Message Block (SMB) protocol to infect and propagate computers running Microsoft Windows on the network. Using Stealthwatch, network operators can monitor SMB activity inside the network.

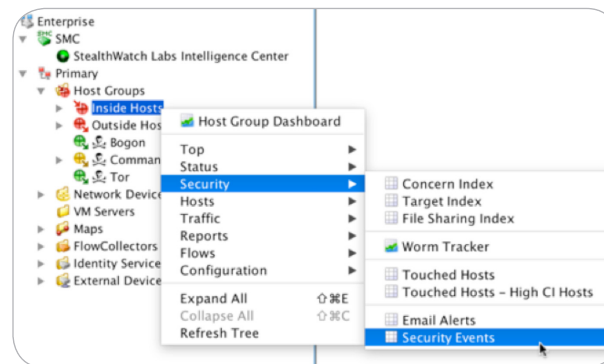
Propagation Detection

The initial strain of WannaCry malware will try to propagate inside the network laterally (from host to host) in an attempt to infect as many hosts as possible. This propagation action has been noted sometimes even before the malware triggers its ransomware payload. Stealthwatch is designed to detect lateral movements, especially between systems on the same subnet.

Assessing Current and Past Exposure

As discovered by [Cisco Talos](#), this malware checks the IP address of the infected machine and attempts to connect over TCP port 445 to other IP addresses reachable by the infected host. This is an extremely noisy and high-traffic activity – and something easily discoverable using Stealthwatch.

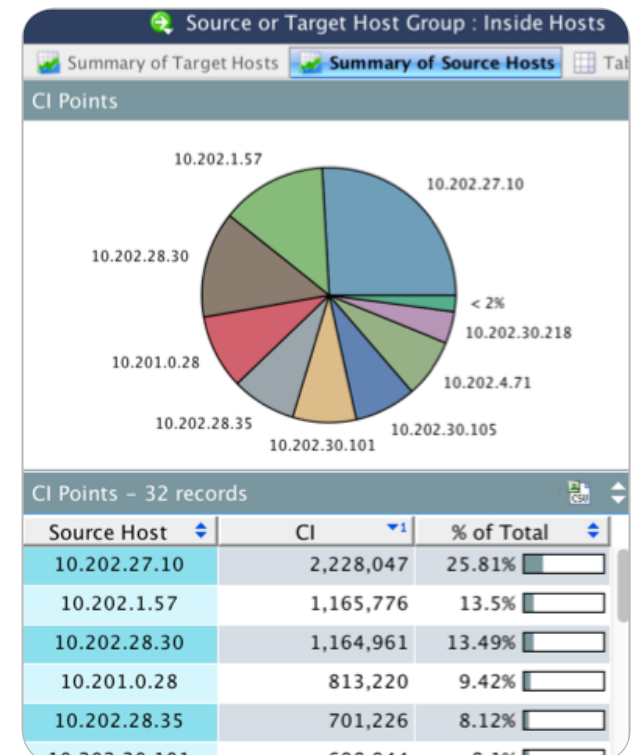
The quickest way to identify hosts that have been scanning subnets over TCP port 445 (the Server Message Block port) is to do a directed query against the Security Events for all Inside Hosts:



In the filter window, set the following conditions to identify the hosts exhibiting the most suspicious behaviors:

- Date/Time: Active time period = Today
- Hosts: Source = Inside Hosts
- Types: Filter by Type = Addr_Scan/tcp
- Ports: Filter on ports = 445/tcp

After completing the query, the resulting report “Summary of Source Hosts” will list out hosts that are actively scanning the network over TCP port 445 with the top host exhibiting the most SMB activity. These are the hosts that are using the same port and protocol as the malware, indicating past exposure to this threat. Note that Stealthwatch allows the user to change the date and time of the active time period in a query. This allows the user to go back and search data captured on the weekend immediately or the following Monday morning as news of the malware surfaced.



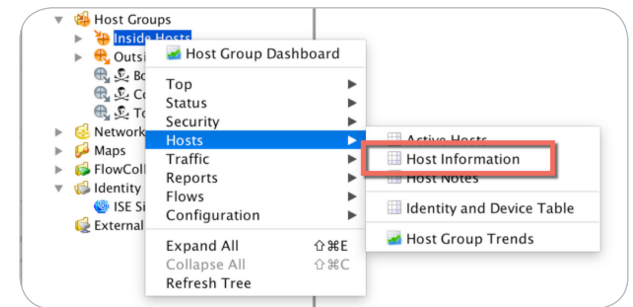
Correlation

Stealthwatch will correlate different activities observed on a specific host computer and consider that IP as suspect based on numerical scores related to each observation. The system then accumulates those scores under one index for each host IP address and raises an alarm called Concern Index. The higher this concern index numerical value rises advises, the more likely the host is engaging in malicious activity.

As an alternative method to get to a host list we can begin the search looking strictly for hosts with high SMB and scanning activity by utilizing the Host Information report. As always, Stealthwatch users should follow research and guidance from computer manufacturers and operating system and application vendors as to what protocols and ports are used by their applications. Based on guidance from Microsoft concerning port 445 is SMB over TCP. SMB traffic can also use NetBIOS over TCP (also known as NBT using ports 137 - name services, 138 - datagram services, and 139 - session services). For more guidance regarding SMB traffic, [click here](#).

In the filter conditions set the following:

- Date/Time: Active time period = Today
- Hosts: Source = Inside Hosts
- Server Applications: Filter by applications = smb (unclassified)
- Security Events:: Filter by Type = Addr_Scan/tcp



Host Groups	Host	Avera...	Total ...	Total ...	Total Traffic ...
Catch All	10.201.3.21	8.15M	82.12G	1.59G	83.72G
Catch All	10.10.30.23	2.96M	2.05G	28.38G	30.44G
Catch All	10.201.3.184	587.13k	4.94G	1.1G	6.03G
Catch All	10.201.3.43	339.48k	3.33G	156.51M	3.49G
Catch All	10.10.30.19	127.06k	48.43M	1.26G	1.31G

Scoping and Mitigation

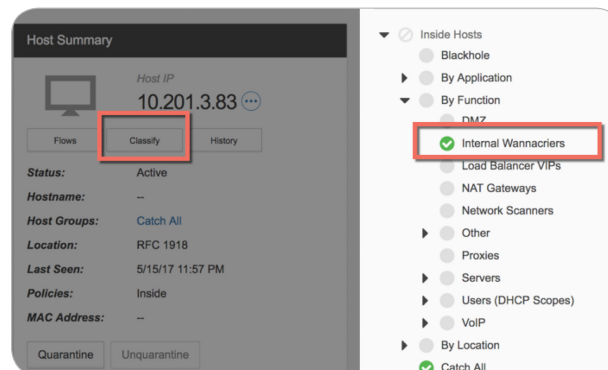
Using the Stealthwatch Management Center and dashboards, you can easily build a simple report to list all systems that indicated suspicious activity and possible infection. With Cisco Identity Services Engine (ISE) integration, you can then quarantine suspect machines, preventing further spread of WannaCry until the threat is remediated.

Effectively Monitoring and Controlling Ongoing Exposure

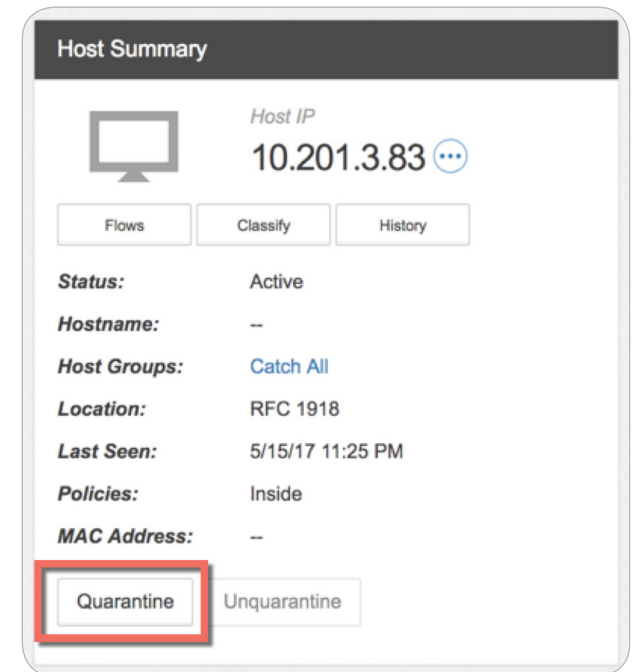
In this step of the incident response process, we are going to first neutralize any of the potentially infected hosts covered above as well as monitor our ongoing exposure to the external threats coming into our environment.

As an output of the investigation above, we generated a list of potentially infected hosts. The next step is to quarantine these hosts. Using technologies such as the [Cisco Identity Services Engine \(ISE\)](#) and [Cisco TrustSec](#), components of the Cisco Ransomware Defense Solution, this can be quickly accomplished.

First, after confirming that a host is infected with WannaCry, classify it into an appropriate host group to contextually monitor its ongoing interaction with your environment.



Immediately afterwards, quarantine the host:



The act of quarantining will use Cisco Platform Exchange Grid (pxGrid) protocol to instruct ISE to trigger a Change of Authorization (CoA) and assign the host to a new Security Group, preventing it from accessing network resources and hosts. The use of software-defined segmentation with technologies such as Cisco TrustSec can [help block the spread of malware](#) – both before and after the attack.

Success

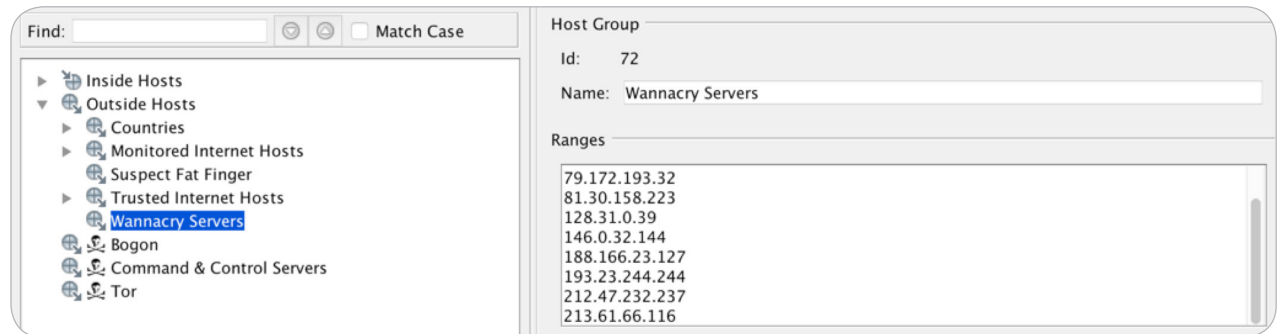
Quarantine request successfully sent to ISE. To view the current quarantine status of the host, you must go to the ISE appliance or contact your ISE administrator.

Ok

To learn more about how your organization can stay protected visit:

- [Cisco Stealthwatch](#)
- [Now What? Moving Forward After the WannaCry Attack](#)

Our last step is to classify the hosts outside our network that Talos has identified as known WannaCry servers. This is accomplished by creating a host group with the IP addresses and labelling it as such.



Summary

WannaCry was an amazingly effective malware campaign, and network owners and Internet users should be ready for possible WannaCry variants. The Cisco Ransomware Defense solution and its incorporated technologies can effectively detect, monitor, and control ongoing exposure to this threat.

Next Steps

Customers are encouraged to contact Stealthwatch Customer Success to help assess their current WannaCry exposure and monitor future risk, by:

- [Visiting the Customer Community](#)
- [Emailing Stealthwatch Customer Support](#)
- Calling Stealthwatch Customer Support at 1-800-838-6574