



Possibilities

#CiscoLive

Email Security Appliance Integration with Cisco Threat Response

Akieba Alexander – Technical Consulting Engineer (ESA)

Cassy Edgar – Technical Consulting Engineer (ATS)

DGTL-TSCSEC-501



#CiscoLive





Agenda

- Introduction
- Cisco Threat Response Overview
- What ESA Offers Independently
- ESA/CTR Integration Demo
- Investigation Demo
- Remediation Opportunities
- Conclusion

Meet the Engineers

- Akieba Alexander is based in our RTP office in North Carolina. She joined Cisco in 2014 as an Intern in the CX Lab, where she later transitioned into a full-time employee. She joined the Email Security Team in 2016, where she has worked on the TAC team until now. She has become one of our go-to engineers for handling high profile customers ensuring that they are taking full advantage of the product.
- Cassy Edgar has established herself as a senior engineer of the Advanced Threat Solutions team. While working as a Security Engineer with a Cisco Partner, she gathered an extensive understanding of various antivirus products including a solid grasp of Amp for Endpoints. She has played a vital role with our larger customers and ensuring that they are taking full advantage of the product and ultimately keeping them protected from malware. Outside of work, she likes to travel, spend time with her friends and family, and the occasional glass of wine.

Introduction

Welcome to A&E Industries – a small start-up company that just landed its first million-dollar contract.

Marley, one of the email administrator, just got word that the **CEO just receive an email with a malicious attachment that has left his computer unusable and the email is slowly spreading through to the rest of the company.**

It took Marley and the security team a total of 14 days to be able to review and rectify the threat, due to the several other security devices within their organization and outside third-party tools having to be checked.

During the Tech Strategy meeting, the conversation on how to remediate threats sooner came up and Marley brought up the idea of integrating the ESA with CTR. CTR can be added at no additional cost since AMP for Endpoints is already slated to be deployed for use.


**** A&E industries currently employs 250 people and has 2 ESAs currently deployed in their environment.****

Cisco Threat Response (CTR) Overview

Threat Response is an application that automates and aggregates threat intelligence sources and data from multiple security technologies – Cisco and third-party – into a central interface. So you can simplify and accelerate critical security operations functions:

1. Detection
2. Investigation
3. Remediation

What the ESA currently provides?

Message Details		
Envelope and Header Summary		
Received Time:	20 May 2020 03:07:00 (GMT +05:00)	
MID:	59	
Message Size:	99.91 (KB)	
Subject:	Invoice Due	
Envelope Sender:	khouse@aeindustries.com	
Envelope Recipients:	jmiller@aeindustries.com	
Message ID Header:	<150a5207-6fcf-bf96-4100-7a30967130ca@aeindustries.com	
SMTP Auth User ID:	N/A	
 Attachments:	AE_Industries2020-AnualReport.pdf	
Sending Host Summary		
Reverse DNS Hostname:	mail3.spammer.com	(verified)
IP Address:	10.82.246.5	
SBRs Score:	rfc1918	

Integration Benefits

- View message tracking details originating from multiple appliances within your organization
- Identify, investigate and remediate threats observed in the message tracking
- Remediate the identified threats rapidly and provide recommended actions to take against the identified threats
- Remediation time is down from **DAYS** to **HOURS** now
- Document the investigation of the threats in the portal to support collaboration of information among other devices on the portal



Demo

ESA/CTR Configuration

CISCO *Live!*

#CiscoLive






Supported Observables

Observable:	Syntax:
SHA-256 hash of attachments	sha256:"fb024742e...3a91a597"
IP address	ip:"10.82.246.5"
Domains	domain:"aeindustrial.com"
Email message-ID headers	email_messageid:"150a52...@aeindustries.com"
Email subject	email_subject:"Invoice Due"
Sender Email address	email:khouse@aeindustries.com
File name	file_name:"AE_Industries2020-AnnualReport.pdf"
Cisco ESA MID	cisco_mid: "59"

Oh No! A user interacted with the file?

DESKTOP-7SU3QQQ detected AE_Industries2020-AnnualReport.pdf.gfoug5m.partial as W32.FB0274E2CB-95.SBX.TG

Medium



Quarantine: Successful

2020-05-20 12:23:01 EDT

File Detection

Detection

W32.FB0274E2CB-95.SBX.TG

Connector Info

Fingerprint (SHA-256)

fb0274e2...3a91a597

Comments

File Name

AE_Industries2020-AnnualReport.pdf.gfoug5m.partial

File Path

C:\Users\ATS-User\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\AE_Industries2020-AnnualReport.pdf.gfoug5m.partial

File Size

72.07 KB

Parent Fingerprint (SHA-256)

ee7174ee...e7a7c895

Parent Filename

MicrosoftEdgeCP.exe

Analyze

Restore File




All Computers

Add to Allowed Applications

File Trajectory

Win10v1.kaboom.lcl detected AE_Industries2020-AnnualReport.pdf as W32.FB0274E2CB-95.SBX.TG

Medium



Quarantine: Successful

2020-05-20 10:39:34 EDT

File Detection

Detection

W32.FB0274E2CB-95.SBX.TG

Connector Info

Fingerprint (SHA-256)

fb0274e2...3a91a597

Comments

File Name

AE_Industries2020-AnnualReport.pdf

File Path

C:\Users\ATS-User\Downloads\AE_Industries2020-AnnualReport.pdf

Parent Fingerprint (SHA-256)

3f000138...c5a82d4d

Parent Filename

explorer.exe

Analyze

Restore File

All Computers

Add to Allowed Applications

File Trajectory

- If the user interacts with the file attached to the email, AMP for Endpoints will quarantine this file
- This will show you the SHA-256 of the file that is considered malicious and you can utilize the SHA-256 in CTR for investigation

Searching for File Names in CTR

- Need to add file_name:"AE_Industries2020-AnualReport.pdf" and the SHA-256 of the file: fb0274e2cbfef4aa4001805004aa637f303294dada91e2f8260e98843a91a597
- This will pull information on where the email came from and the indicators on the file that is malicious
- If you only have file_name:"AE_Industries2020-AnualReport.pdf" this will only show information about the email and not information about the file in question
- Need to make sure there aren't any spaces between type and value as this is not supported:
 - Example: **email_subject: "Invoice Due"**
 - Spaces are not interpreted correctly by matching patterns and will result in zero observables

Demo 2

CTR Threat Investigation



#CiscoLive



Completed Investigation

3 Targets

2 Observables

4 Indicators

0 Domains

1 File Hash

0 IP Addresses

0 URLs

5 Modules

Investigation 2 of 2 enrichments complete

sha256:"fb0274e2cbfef4aa4001805004aa637f303294dada91e2f8260e98843a91a597"

file_name:"AE_Industries2020-AnualReport.pdf"

Investigate

Clear

Reset

What can I search for?

Relations Graph · Filters: Show All, Simplified · Showing 15 of 23 nodes

Sightings

My Environment Global

21 Sightings in My Environment

First Seen: May 19, 2020 22:07:00 UTC

Last Seen: May 20, 2020 16:23:01 UTC

Observables

List View

fb0274e2cbfe... Malicious SHA-256 Hash

AE_Industries2... File Name

fb0274e2cbfef4aa4001805004aa637f3...

Malicious SHA-256 Hash

20 Sightings in My Environment

First Seen: May 20, 2020 14:24:28 UTC

Last Seen: May 20, 2020 16:23:01 UTC

Judgements (59) Verdicts (3) Sightings (21) Indicators (4)

Module	Observable	Disposition	Reason
AMP File Reputation	SHA256: fb0274e2...	Malicious	AMP ProtectDB Convictor
VirusTotal	SHA256: fb0274e2...	Malicious	Rising 25.0.0.25 (updated)
VirusTotal	SHA256: fb0274e2...	Malicious	BitDefenderTheta 7.2.377!
VirusTotal	SHA256: fb0274e2...	Malicious	SentinelOne 4.3.0.0 (update)

Remediation Opportunities

Using the CTR Query, we can acquire the following specific message details

- Sender
- Recipient(s)
- Sending Domain
- Sending IP address

We can then apply the above details to numerous areas of the ESA including Sender Groups, Content Filters and Message Filters to block further instances of this message.

Conclusion

Recovering from the last threat that targeted the CEO of AE Industries, they learned that the scarcest security feature is time.

With the integration of CTR with the Email Security Appliance, Marley and his team were able to simplify threat investigations through rapid, coordinated incident response. AE Industries are now better equipped to handle any potential threats of the future by lowering their mean time to respond and remediate these threats.

Thank you



Possibilities

#CiscoLive