

GRACE HOPPER CELEBRATION



ANITA
B.ORG

Best Case Security for Worst Case Scenarios

Ever wonder how the most challenging cyber attacks are managed? In this session we'll walk through the critical stages of detection, investigation and response in a real-world supply chain attack.

about us

Jyoti Verma

Jyoti Verma is a Senior Technical Leader and Architect in Cisco's Security Business Group where she develops techniques to simplify security operations through applied research, standards and product engineering.



Bret Hartman

Bret Hartman is Vice President and Chief Technology Officer of Cisco's Security Business Group where he and his team are focused on the future direction of the industry and the role Cisco plays in preparing its customers for the security landscape of tomorrow.







Photo credit: Andy Newman

#GHC19



Photo credit: Ramon Espinosa

#GHC19

Attack landscape constantly evolving

Advanced Persistent Threats

Unpatched Software

Spyware/Malware

Wiper Attacks

Phishing

Man in the Middle

DDoS

Cryptomining



Supply chain attacks

Ransomware

Data/IP Theft

Malvertising

Drive by Downloads

Rogue Software

Botnets

Credential compromise

Advanced Persistent Threats

Power of a Global Footprint

Supply chain attacks

Unpatched Software

Ransomware

Spyware/Malware

Data/IP Theft

Wiper Attacks

Malvertising

Phishing

Drive by Downloads

Man in the Middle

Rogue Software

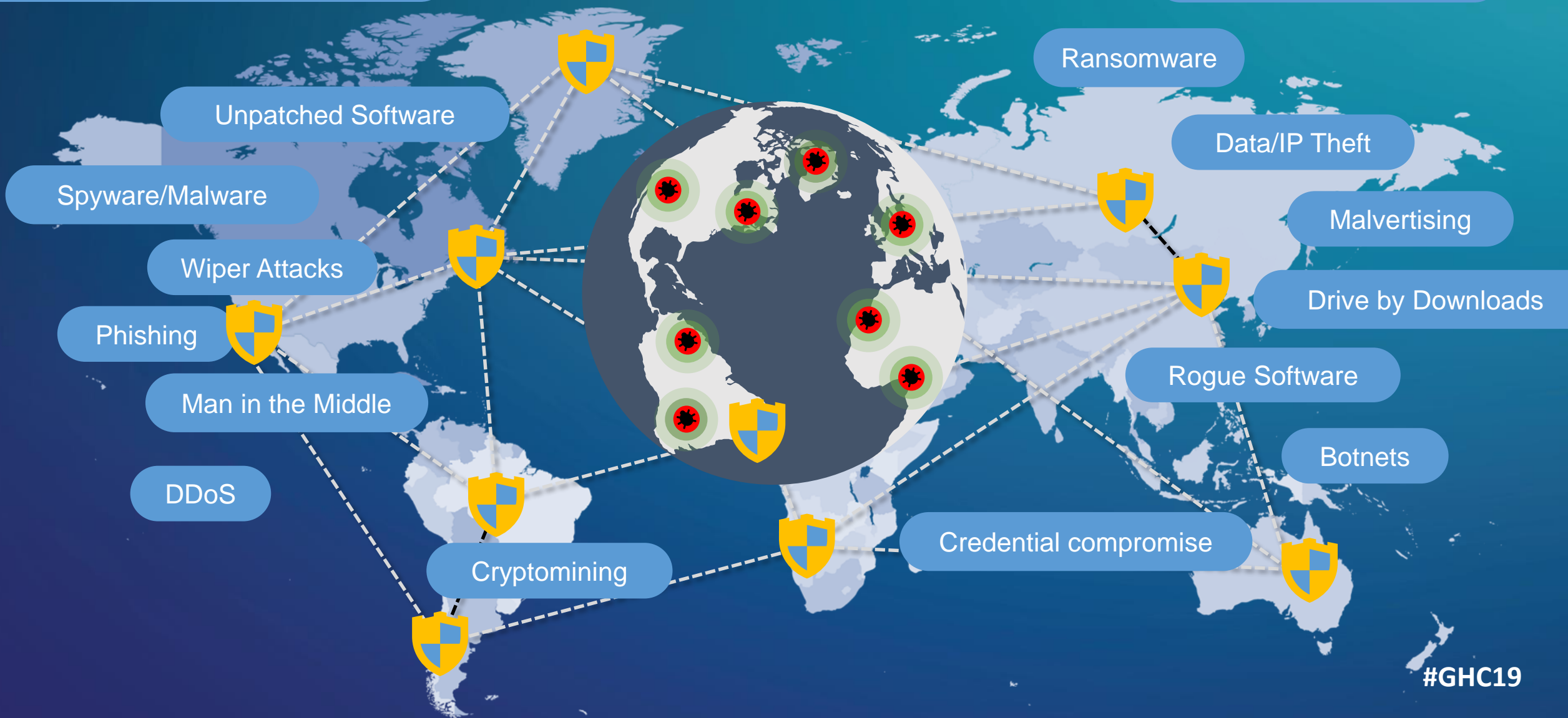
DDoS

Botnets

Cryptomining

Credential compromise

#GHC19



Supply Chain Attacks

WHAT IS A SUPPLY CHAIN ATTACK?

- **Exploit** the trust model
- **Target** unsecure network protocols
- **Hide malware** in build and update processes

HOW IT GETS IN?

- **Legitimate** software updates
- Email links from **seemingly trusted** vendors

WHY IS IT CHALLENGING?

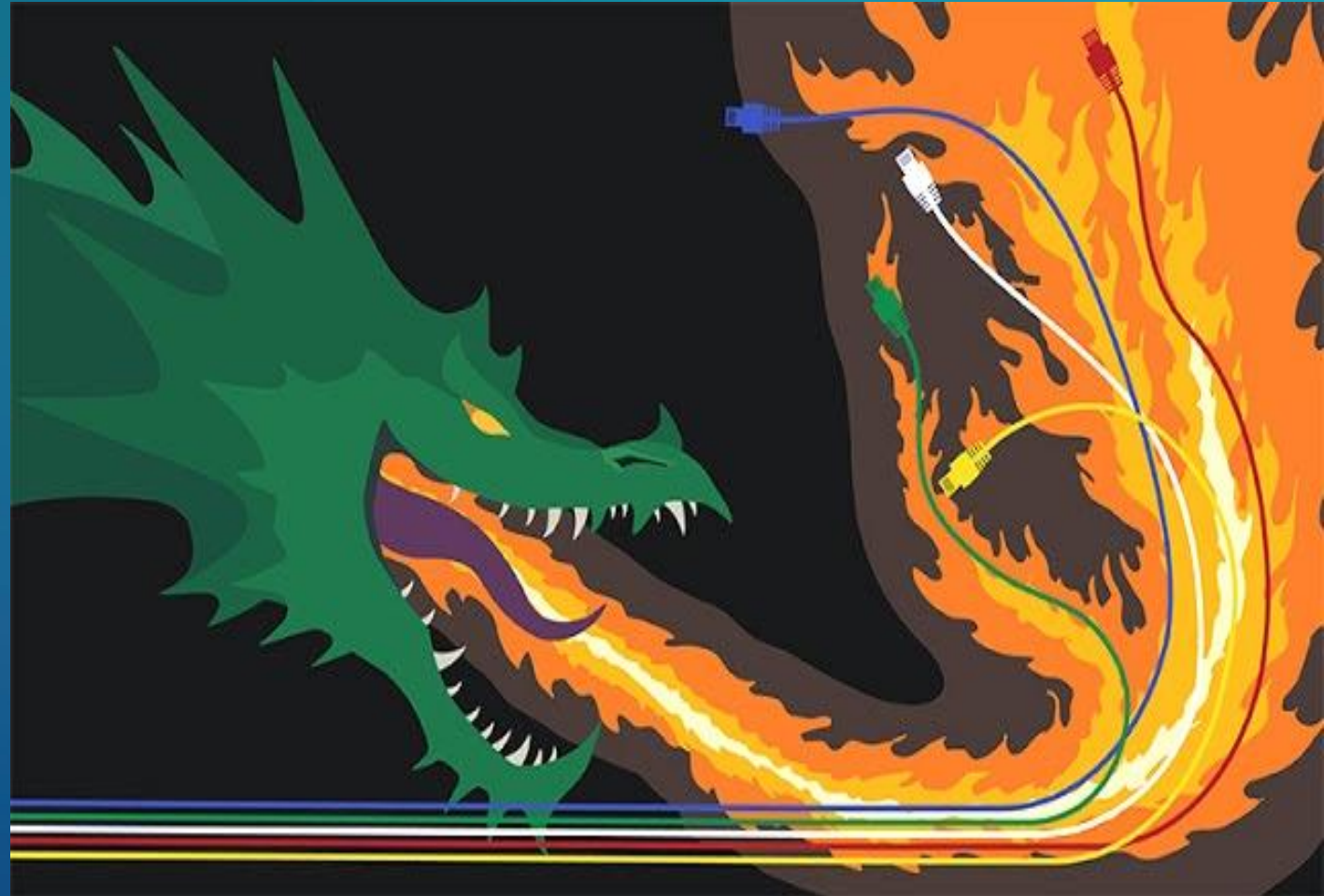
- Malicious code runs with **the same trust and permissions** as the trusted vendor app
- The infection **spreads laterally** across the network bypassing traditional protection

HOW TO DEAL WITH IT?

- **Known Attacks** - Threat Hunting, followed by investigation and response
- **Zero-Day Attacks** – Network and Endpoint behavior analytics

NotPetya (2016)

- Motivation: Geopolitical, Cyberwar
- Via update of a tax accounting package
- Paralyzed government, business operations worldwide
- Caused \$10B in losses

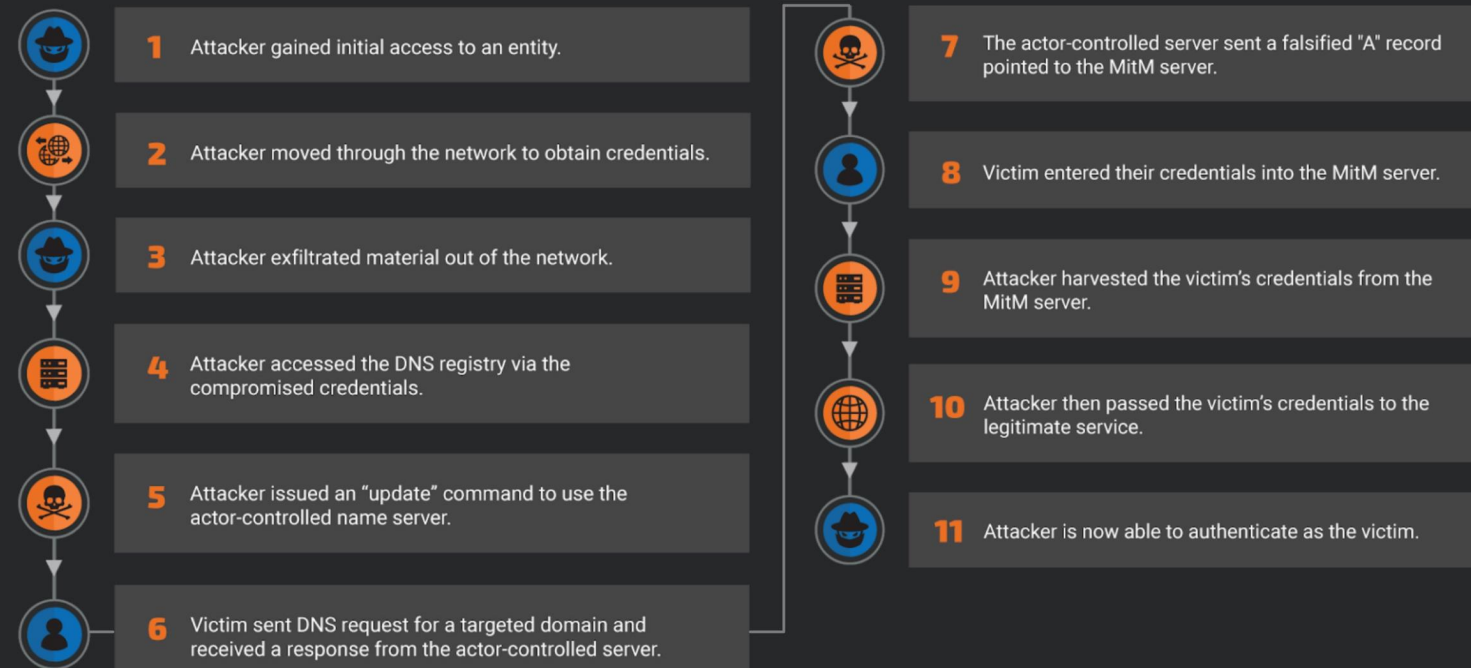


Need to **study**
multiple blog
posts to learn
what **Sea Turtle**
is all about

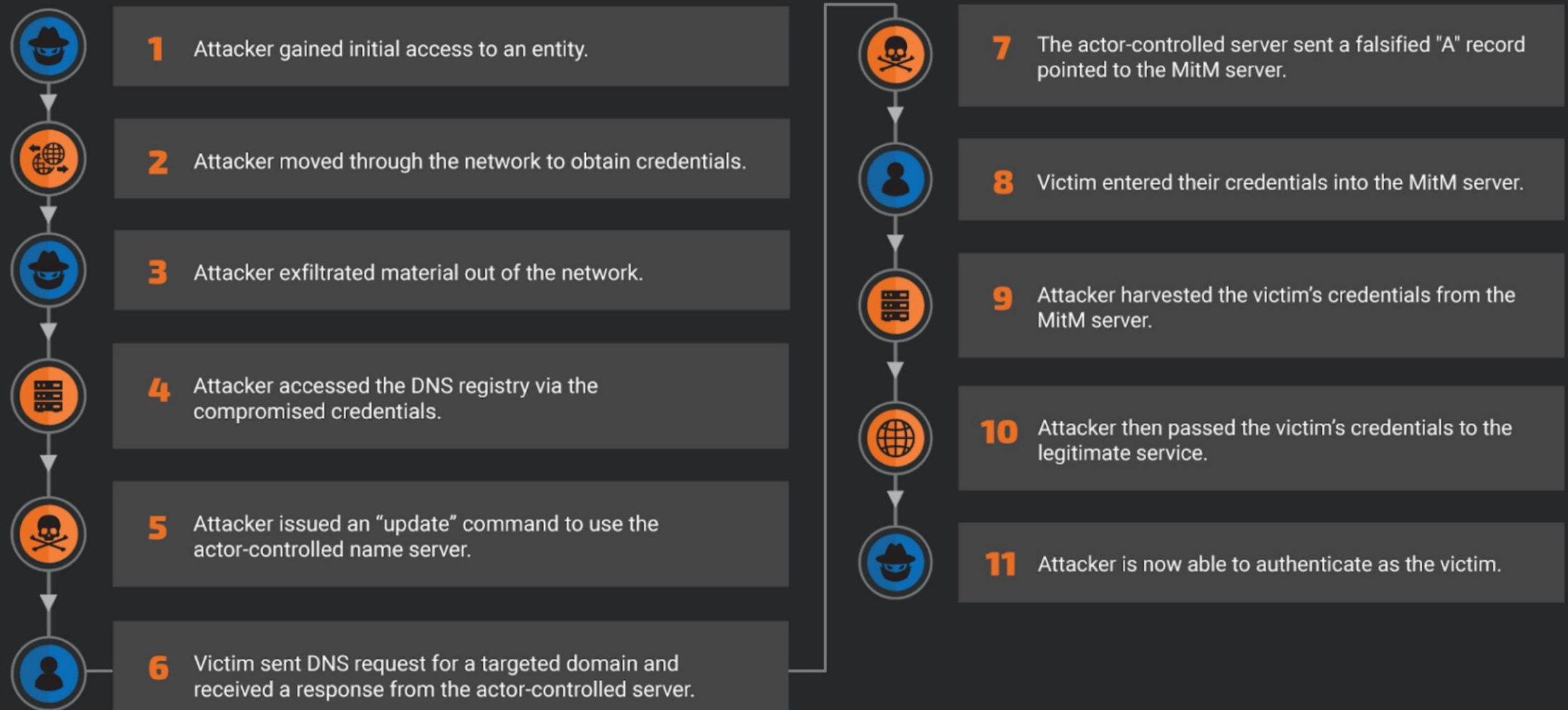


There is so much
we need to know
about Sea Turtle

Redirection Attack Methodology Diagram



Redirection Attack Methodology Diagram



Here is some threat intel on Sea Turtle that we can use

Indicators of Compromise

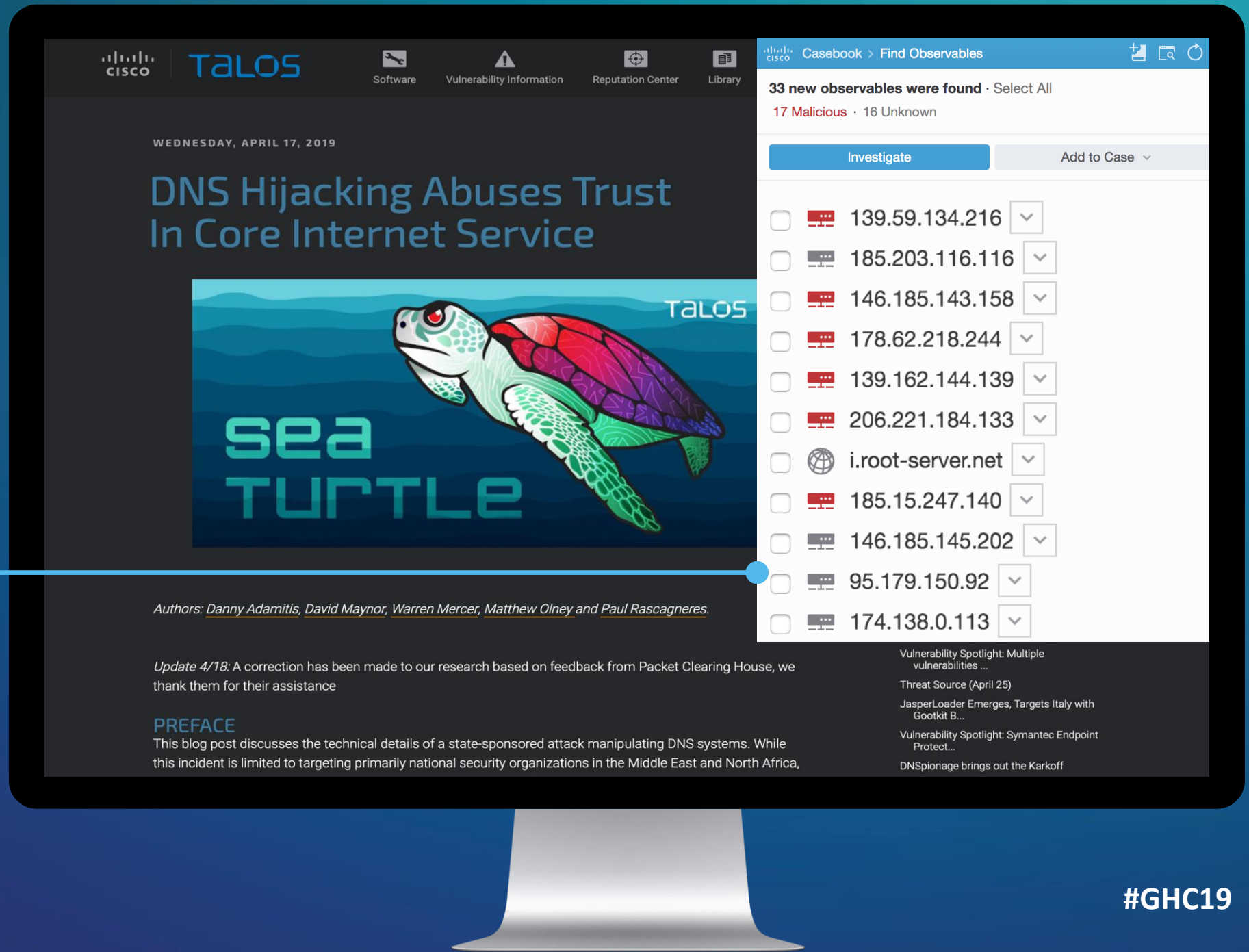
IP address	Month	Year	Country of targets
199.247.3.191	November	2018	Albania, Iraq
37.139.11.155	November	2018	Albania, UAE
185.15.247.140	January	2018	Albania
206.221.184.133	November	2018	Egypt
188.166.119.57	November	2018	Egypt
185.42.137.89	November	2018	Albania
82.196.8.43	October	2018	Iraq
159.89.101.204	December - January	2018-2019	Turkey, Sweden, Syria, Armenia, US
146.185.145.202	March	2018	Armenia
178.62.218.244	December - January	2018-2019	UAE, Cyprus
139.162.144.139	December	2018	Jordan
142.54.179.69	January - February	2017	Jordan
193.37.213.61	December	2018	Cyprus
108.61.123.149	February	2019	Cyprus
212.32.235.160	September	2018	Iraq
198.211.120.186	September	2018	Iraq
146.185.143.158	September	2018	Iraq
146.185.133.141	October	2018	Libya
185.203.116.116	May	2018	UAE
95.179.150.92	November	2018	UAE
174.138.0.113	September	2018	UAE
128.199.50.175	September	2018	UAE
139.59.134.216	July - December	2018	United States, Lebanon
45.77.137.65	March - April	2019	Syria, Sweden
142.54.164.189	March - April	2019	Syria
199.247.17.221	March	2019	Sweden

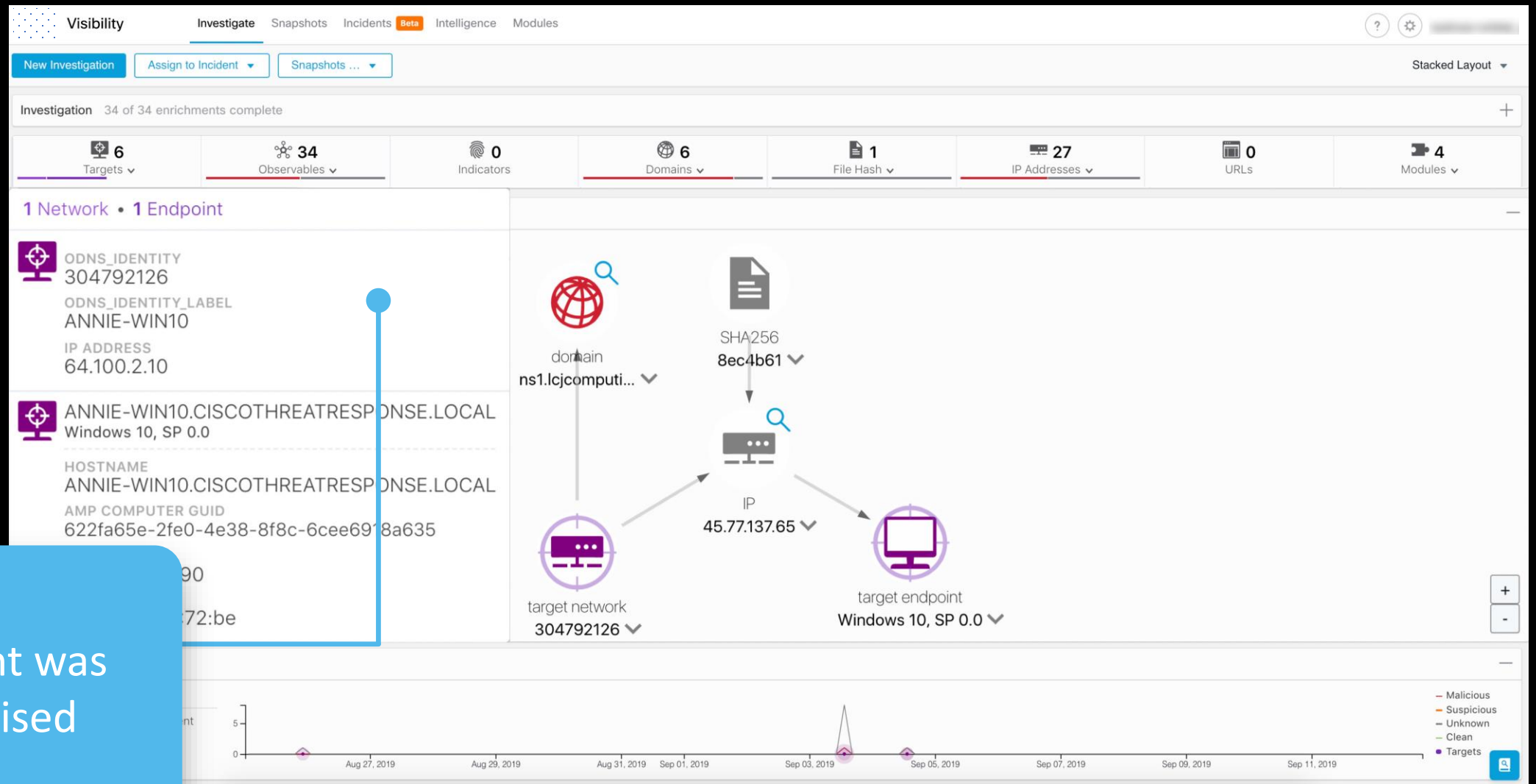
1

Block the
malicious
domains,
URLs and IPs

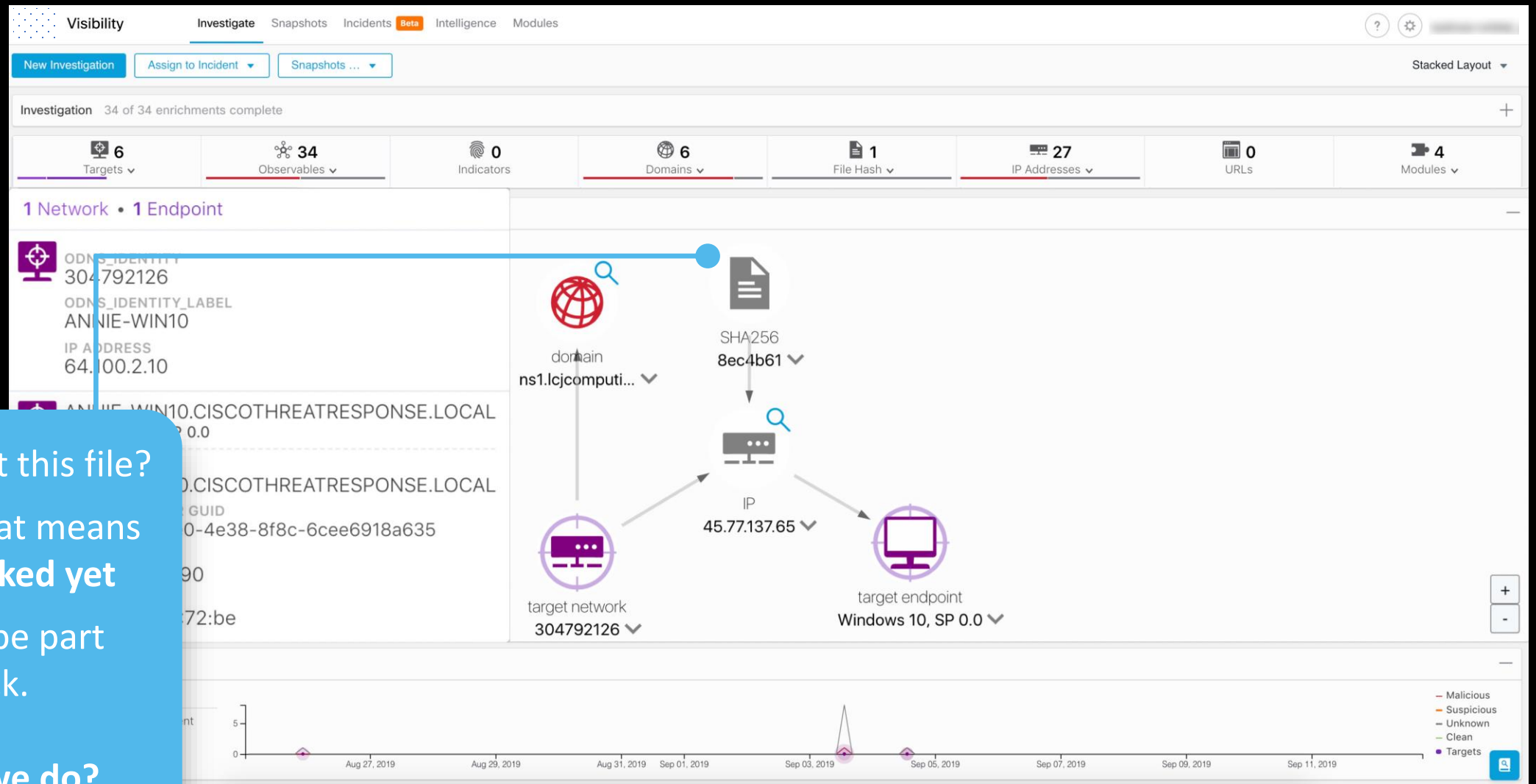
2

Perform
Threat Hunting
to identify
internal targets





1 endpoint was
compromised



What about this file?

It's gray; that means
it isn't blocked yet

But it may be part
of the attack.

What can we do?

To be safe,
block this file across
the organization

**Block it on endpoint,
email, and firewall**

You can always
unblock it later

The screenshot displays the AMP EDR interface. At the top, there are tabs for Visibility, Investigate, Snapshots, Incidents, Intelligence, and Modules. Below these are buttons for 'New Investigation', 'Assign to Incident', and 'Snapshots ...'. A status bar indicates 'Investigation 34 of 34 enrichments complete'. A navigation bar shows counts for various entities: 6 Targets, 34 Observables, 0 Indicators, 6 Domains, 1 File Hash, 27 IP Addresses, 0 URLs, and 4 Modules. The main area is titled 'Relations Graph Showing 36 nodes' and contains a graph with nodes for 'domain ns1.lccomputi...', 'SHA256 8ec4b61', 'IP 45.77.137.65', and 'target network 304792126'. A context menu is open over the SHA256 node, listing actions: 'Copy to Clipboard', 'Add to Investigation', 'Add to Current Case', 'Add to New Case', 'AMP EDR' (with sub-items 'File trajectory' and 'Search for this SHA256'), 'Add SHA256 to custom detections AMP-Unity', 'Threat-Grid' (with sub-items 'Browse 8ec4b6188a91ad6828e883ed3be9f...' and 'Search 8ec4b6188a91ad6828e883ed3be9f...'), and 'Umbrella-Protection' (with sub-item 'Sample view for 8ec4b6188a91ad6828e883...'). At the bottom, a timeline shows dates from Aug 27, 2019, to Sep 07, 2019. A green box labeled 'File blocked' is positioned over the timeline.

8ec4b6188a91ad6828e883ed3be9fa5f461d...

SHA-256

Copy to Clipboard

Add to Investigation

Add to Current Case

Add to New Case

AMP EDR

File trajectory

Search for this SHA256

Add SHA256 to custom detections AMP-Unity

Threat-Grid

Browse 8ec4b6188a91ad6828e883ed3be9f...

Search 8ec4b6188a91ad6828e883ed3be9f...

Umbrella-Protection

Sample view for 8ec4b6188a91ad6828e883...

File blocked

But how did that file
get in?

Search your tools
for information on
this file

Visibility Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Stacked Layout

Investigation 34 of 34 enrichments complete

6 Targets 34 Observables 0 Indicators 6 Domains 1 File Hash 27 IP Addresses 0 URLs 4 Modules

Relations Graph Showing 36 nodes

domain ns1.lccomputi... SHA256 8ec4b61 IP 45.77.137.65 target network 304792126

8ec4b6188a91ad6828e883ed3be9fa5f461d...
SHA-256

Copy to Clipboard
Add to Investigation
Add to Current Case
Add to New Case

AMP EDR
File trajectory
Search for this SHA256
Remove SHA256 from custom detections A...

Threat-Grid
Browse 8ec4b6188a91ad6828e883ed3be9f...
Search 8ec4b6188a91ad6828e883ed3be9f...

Umbrella-Protection
Sample view for 8ec4b6188a91ad6828e883...

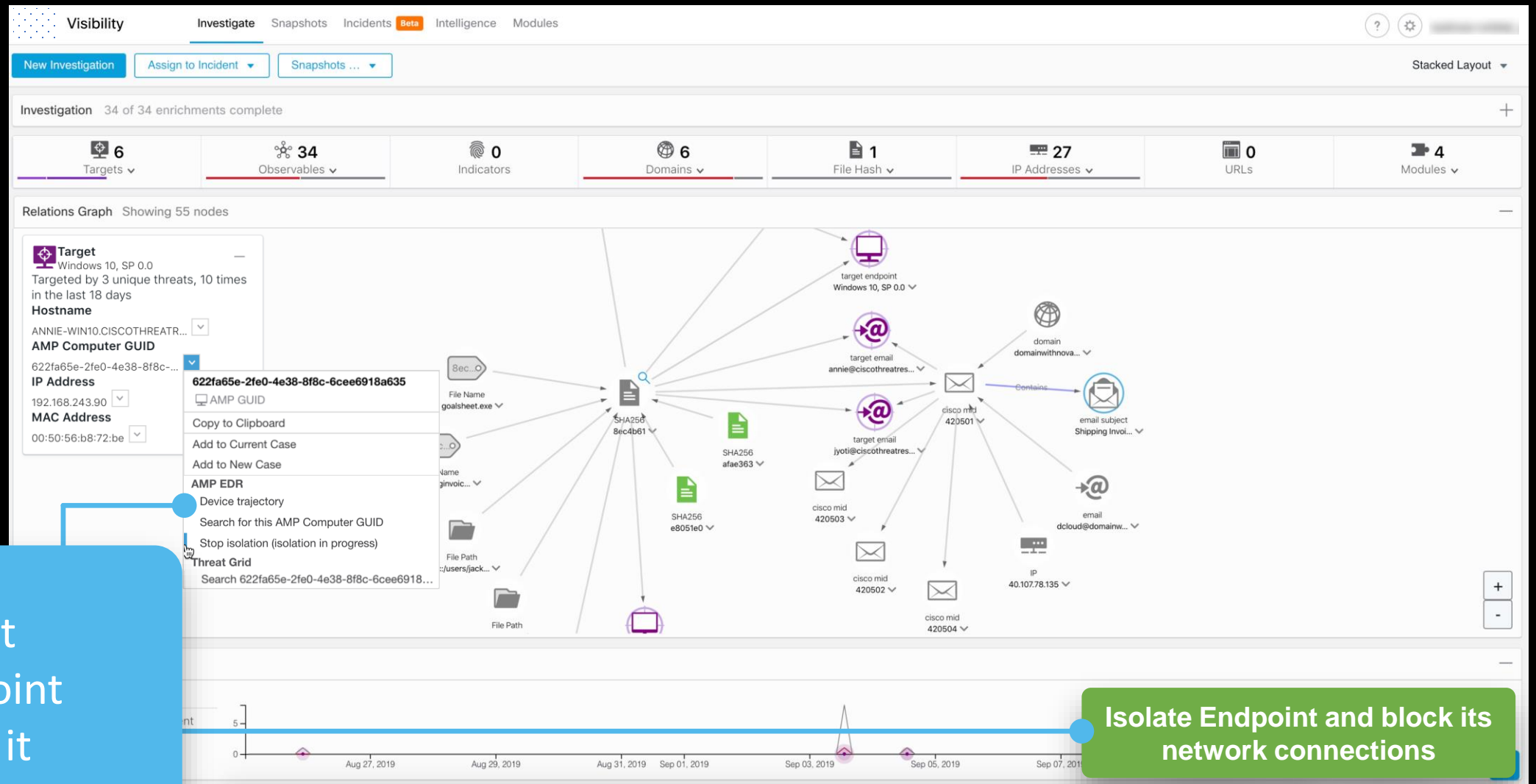
nt 5 0 Aug 27, 2019 Aug 29, 2019 Aug 31, 2019 Sep 01, 2019 Sep 03, 2019 Sep 05, 2019 Sep 07, 2019 Sep 09, 2019 Sep 11, 2019

Malicious Suspicious Unknown Clean Targets

We learn that it
came in through
email

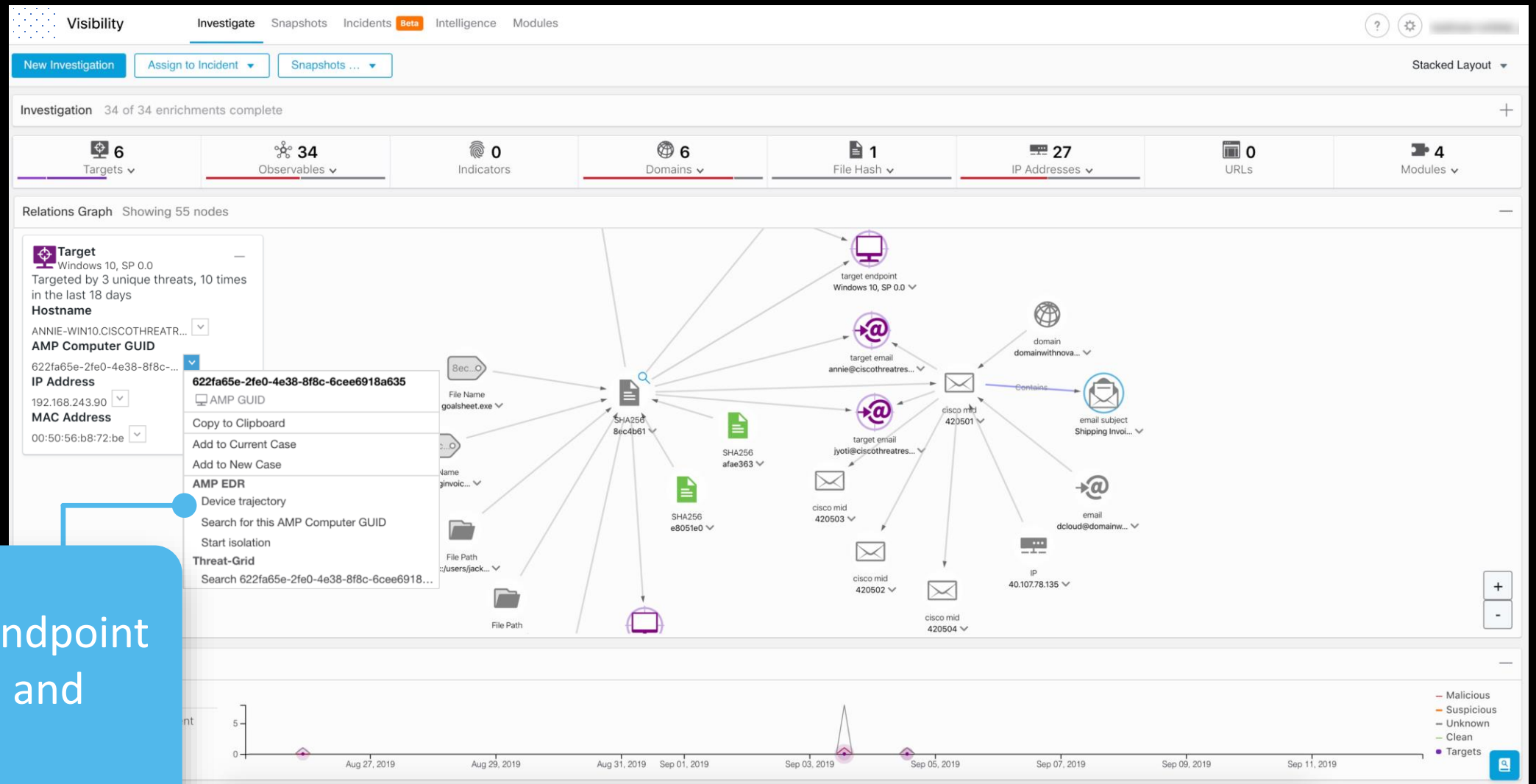
Good thing
we blocked it
everywhere already

The screenshot displays a security investigation interface with a top navigation bar including 'Visibility', 'Investigate', 'Snapshots', 'Incidents', 'Beta', 'Intelligence', and 'Modules'. Below the navigation bar are buttons for 'New Investigation', 'Assign to Incident', and 'Snapshots ...'. A status bar indicates 'Investigation 34 of 34 enrichments complete'. A dashboard shows various metrics: 6 Targets, 34 Observables, 0 Indicators, 6 Domains, 1 File Hash, 27 IP Addresses, 0 URLs, and 4 Modules. The main area features a network diagram with nodes for 'VLNESA15658201_420D08BF005D49C5A730-D6FE24895791' (Email Security Appliance) and 'JACKSPARROW-WIN10.CISCOTHREATRESPONSE.LOCAL' (Windows 10, SP 0.0). A central node is labeled 'SHA256 8ec4b61'. A blue line connects this node to an email message window titled 'Shipping Invoice'. The email message window shows the following details: To: annie@ciscothreatresponse.com, Cc: , Bcc: , Subject: Shipping Invoice, and an attachment 'shippinginvoice.exe (124.6 KB)'. The email body text reads: 'From: Rob Jones <dcloud@domainwithnovalue.com>', 'Date: Tuesday, September 3, 2019 at 5:59 PM', 'To: Annie Smith <annie@ciscothreatresponse.com>', 'Subject: Shipping Invoice', 'Dear Annie,', 'Unfortunately, we failed to deliver a postal package to you that was sent on the 3rd of September 2019. Please complete the attached invoice and collect the package at our office.', and 'Customer Service Department, FedEx'.



Can't trust
the endpoint
so isolate it

Isolate Endpoint and block its
network connections



Pivot to Endpoint
Detection and
Response

⚠ Planned changes to Cisco-Maintained Exclusions ✕

Starting on Wednesday, August 28th, the Cisco-Maintained exclusion sets will be updated in order to address CPU and Update issues. The sets that will be modified are: Microsoft Windows Default, N-Able Solarwinds Technology, and Docker. - If your environment is using any of these lists, please expect an influx of policy updates throughout the day. These updates will start after 23:00 UTC to minimize business impact.

Device Trajectory[Take a Tour](#) [Share](#) [Send Feedback](#) [Use Legacy Device Trajectory](#)

ANNIE-WIN10.CISCOTHEATRESPONSE.LOCAL in group Orbital Group

No compromise events

Hostname	ANNIE-WIN10.CISCOTHEATRESPONSE.LOCAL	Group	Orbital Group
Operating System	Windows 10, SP 0.0	Policy	Orbital Policy
Connector Version	6.5.1.11267	Internal IP	192.168.243.90
Install Date	2019-09-03 19:16:20 UTC	External IP	64.100.2.10
Connector GUID	622fa65e-2fe0-4e38-8f8c-6cee6918a635	Last Seen	2019-09-03 21:16:37 UTC
Definition Version	TETRA 64 bit (None)	Definitions Last Updated	None
Update Server	tetra-defs.amp.cisco.com		

Related Events

No incidents

Vulnerabilities

No known software vulnerabilities observed

[Orbital](#) [Take Forensic Snapshot](#) [View Snapshot](#) [Orbital Query](#)[Events](#) [View Changes](#)[Start Isolation](#) [Scan...](#) [Move to Group...](#)

Filters ▾

Search Device Trajectory

Q

5
AUG

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

1
SEP

2

3

Capture **Forensic snapshot** of the endpoint

Forensic Analysis

DashboardQueryJobsAssetsCatalogGraphQLNode Creation

🔍 Live Forensic Query

New

Targets

.amp:07f155d0-d3f6-4323-9961-2a1dd76832bf

SQL

SELECT name, version, publisher, install_date FROM programs WHERE name!="" OR publisher!=""

+

Catalog

Search

Browse...

▶ Query

Create Job

1 node

NODE -EJrADpowR1OpScsPyTPg

programs

NAME	VERSION	PL
-EJrADpowR1OpScsPyTPg		
Update for Windows 10 for x64-based Systems (KB4023057)	2.61.0.0	Mi
Update for Windows 10 for x64-based Systems (KB4480730)	2.53.0.0	Mi
VMware Tools	10.2.5.8068393	VM
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	9.0.30729.6161	Mi
Cisco AMP Orbital	0.8	Ci
Google Chrome	76.0.3809.100	Gc
Cisco AMP for Endpoints Connector	6.5.1.11185	Ci
Google Update Helper	1.3.34.11	Gc
Cisco Webex Meetings Desktop App	39.6.4.3	Ci
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	9.0.30729.6161	Mi
Microsoft OneDrive	19.123.0624.0005	Mi

Perform forensics on the endpoint

List of all the software installed on the machine

Next step: Block access to internal resources for the compromised endpoint

Response recap



Take away




TODAY
Study Up



3 MONTHS
Assess



6 MONTHS
Apply

- **NIST Cybersecurity Framework**
- **MITRE ATT&CK Framework**
- **OASIS Standards:**
 - Structured Threat Information Expression (STIX)
 - Collaborative Automated Course of Action Operations (CACAO)
 - OpenC2
- **JOIN OASIS:** 
 - dee.schur@oasis-open.org

Assess the detection and response systems within your own organization and determine if you have enough in place.

How would you **apply** what you have to a more automated environment?

“Never give up. And even if something looks like a solitary sport, it’s a team effort.”

- Diana Nyad

Thank you.

You can follow
us @



Jyoti Verma
Bret Hartman

Please remember to
complete the session
survey in the mobile
app.

GRACE HOPPER
CELEBRATION



#GHC19