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.

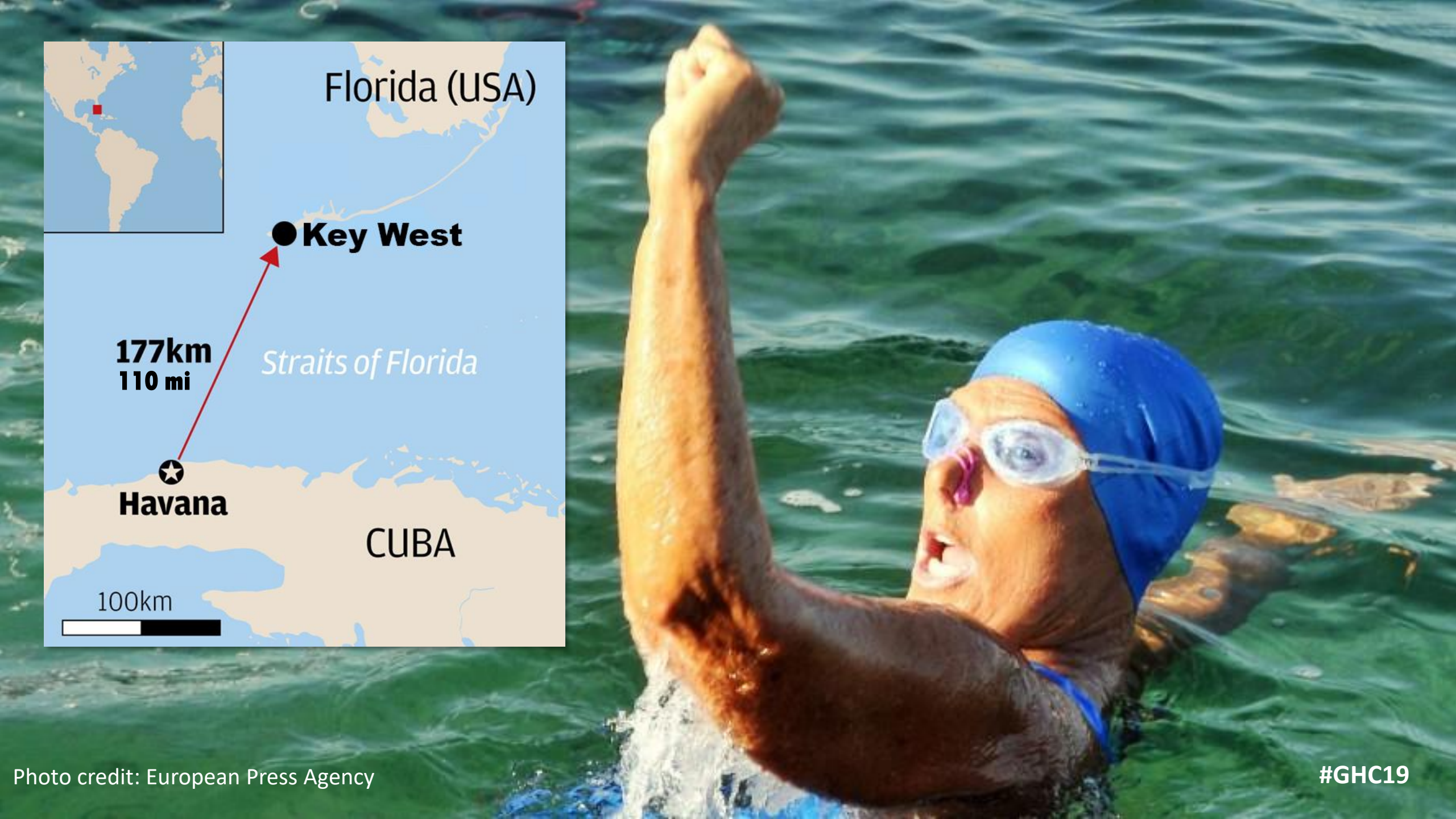


Photo credit: European Press Agency

#GHC19

Photo credit: Andy Newman

Photo credit: Ramon Espinosa

#GHC19

Attack landscape constantly evolving

Advanced Persistent Threats

Supply chain attacks

Ransomware

Unpatched Software

Data/IP Theft

Spyware/Malware

Malvertising

Wiper Attacks

Drive by Downloads

Phishing

Rogue Software

Man in the Middle

Botnets

DDoS

Credential compromise

Cryptomining

#GHC19

Power of a Global Footprint

#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?

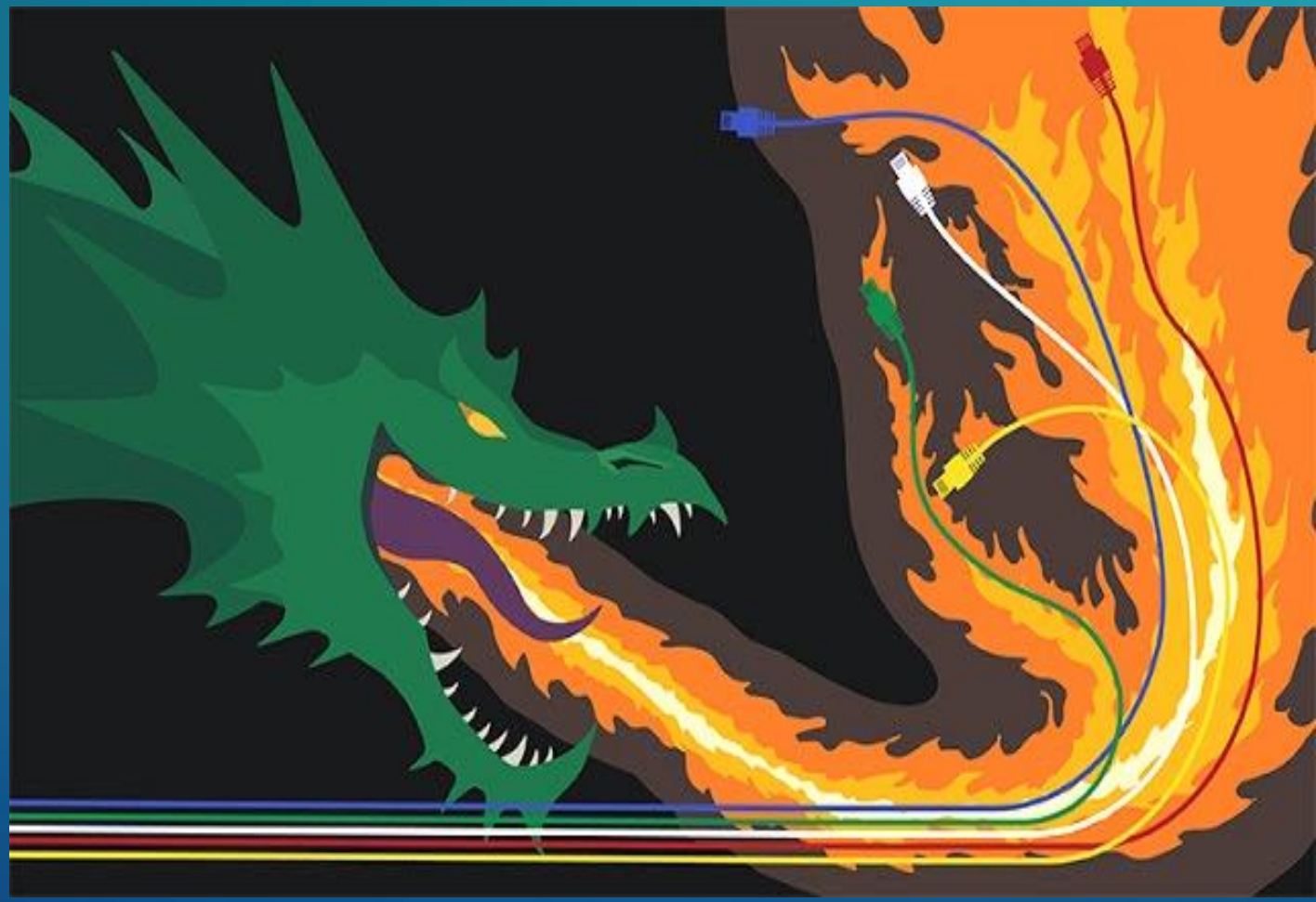
- Malicious code runs with **the same trust and permissions** as the trusted vendor app
- The infection **spreads laterally** across the network bypassing traditional protection

HOW TO DEAL WITH IT?

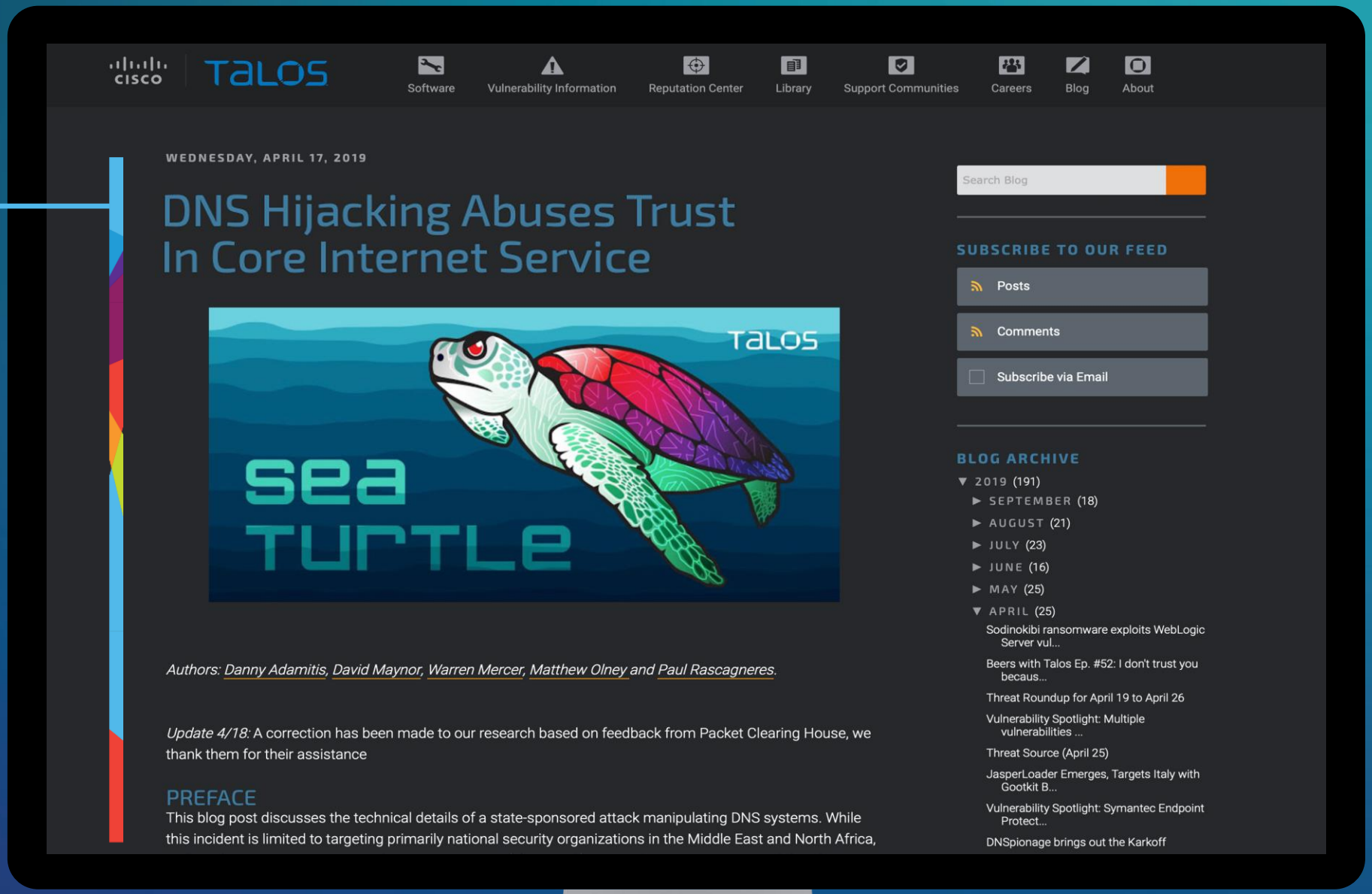
- **Known Attacks** - Threat Hunting, followed by investigation and response
- **Zero-Day Attacks** – Network and Endpoint behavior analytics

NotPetya (2016)

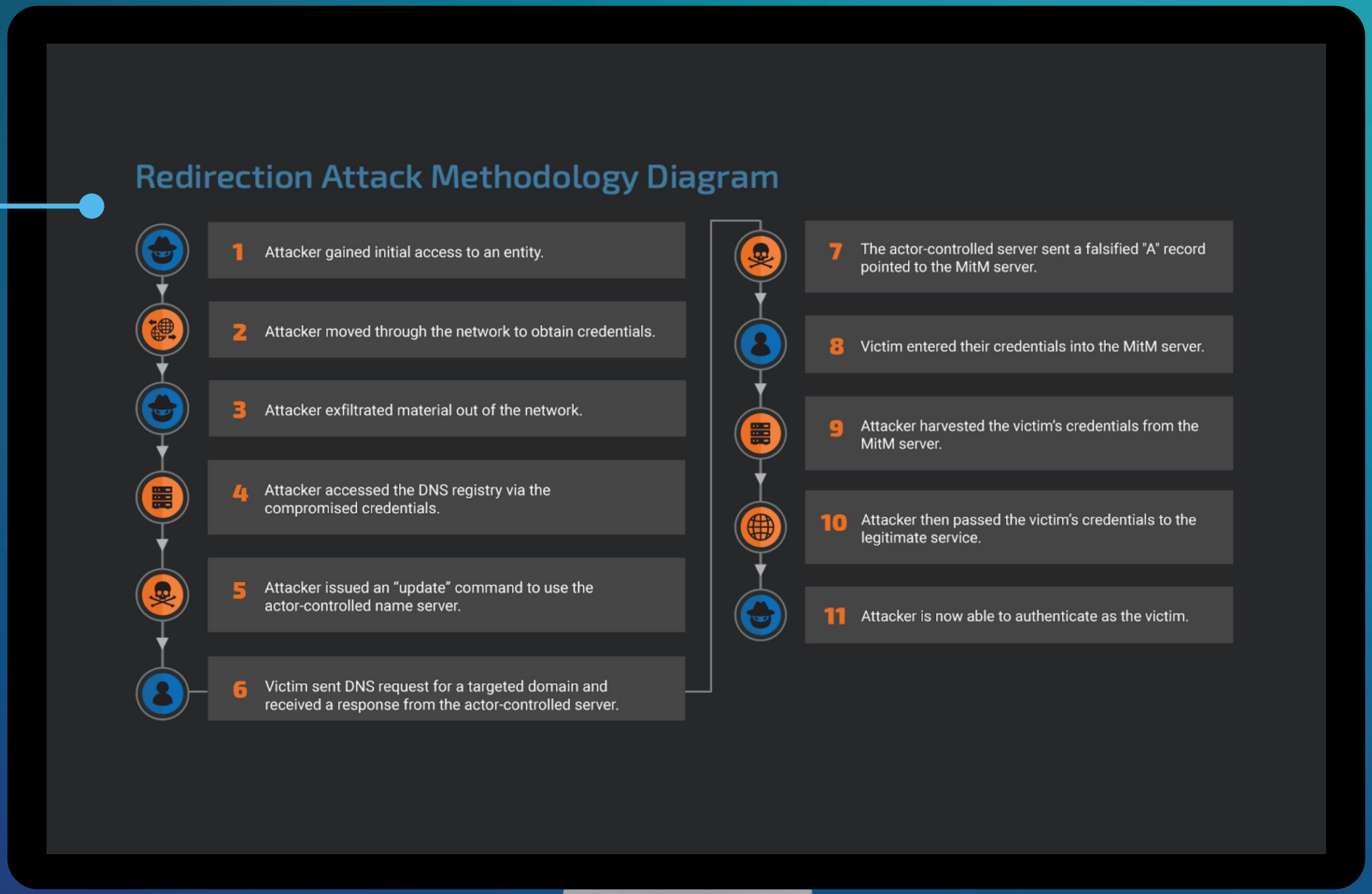
- Motivation: Geopolitical, Cyberwar
- Via update of a tax accounting package
- Paralyzed government, business operations worldwide
- Caused $10B in losses



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

1. Attacker gained initial access to an entity.
2. Attacker moved through the network to obtain credentials.
3. Attacker exfiltrated material out of the network.
4. Attacker accessed the DNS registry via the compromised credentials.
5. Attacker issued an “update” command to use the actor-controlled name server.
6. Victim sent DNS request for a targeted domain and received a response from the actor-controlled server.
7. The actor-controlled server sent a falsified "A" record pointed to the MitM server.
8. Victim entered their credentials into the MitM server.
9. Attacker harvested the victim’s credentials from the MitM server.
10. Attacker then passed the victim’s credentials to the legitimate service.
11. Attacker is now able to authenticate as the victim.

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

Indicators of Compromise

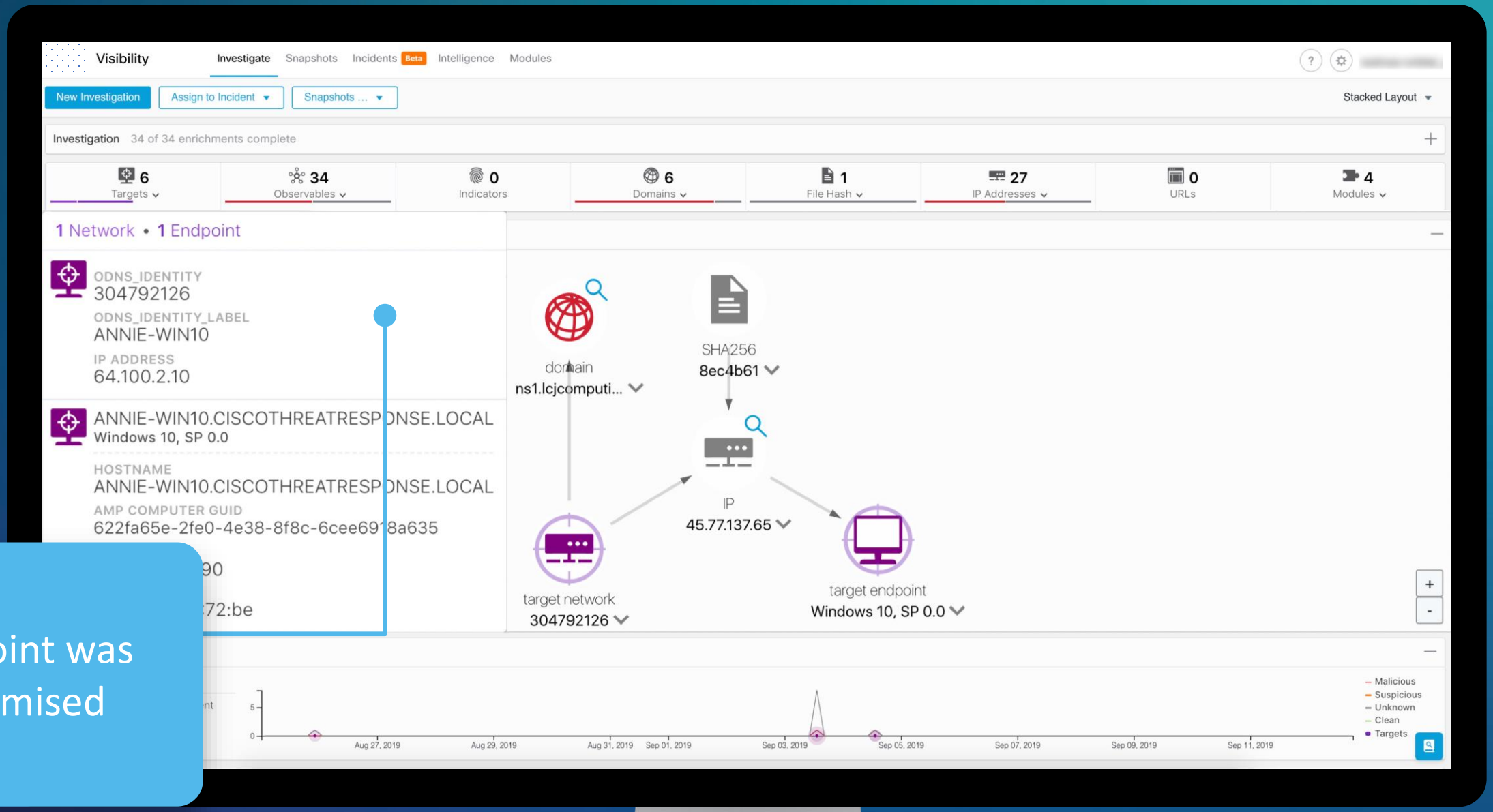
IP address	Month	Year	Country of targets
199.247.3.191	November	2018	Albania, Iraq
37.139.11.155	November	2018	Albania, UAE
185.15.247.140	January	2018	Albania
206.221.184.133	November	2018	Egypt
188.166.119.57	November	2018	Egypt
185.42.137.89	November	2018	Albania
82.196.8.43	October	2018	Iraq
159.89.101.204	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

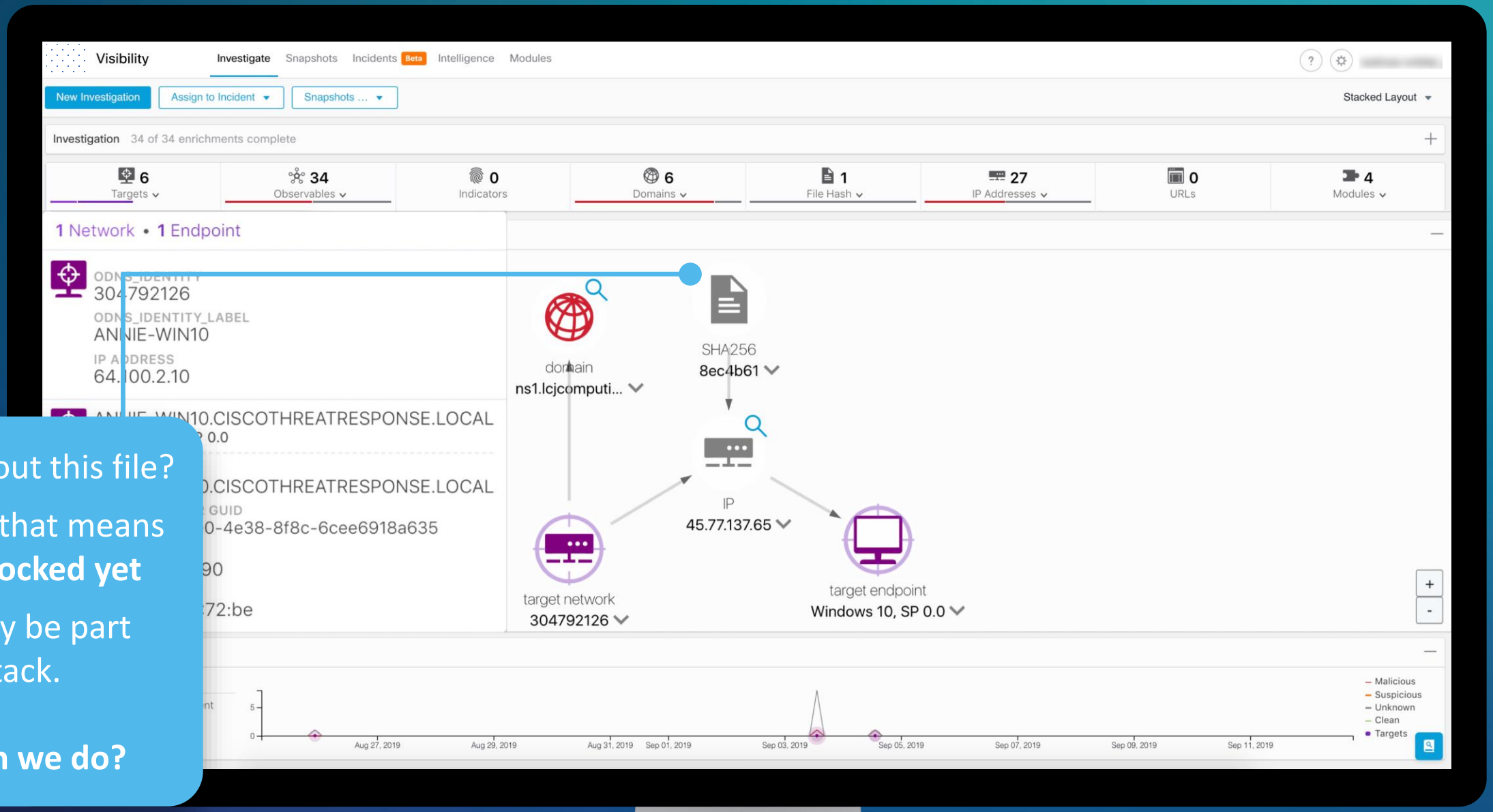
2

Perform Threat Hunting to identify internal targets



1 endpoint was compromised

#GHC19

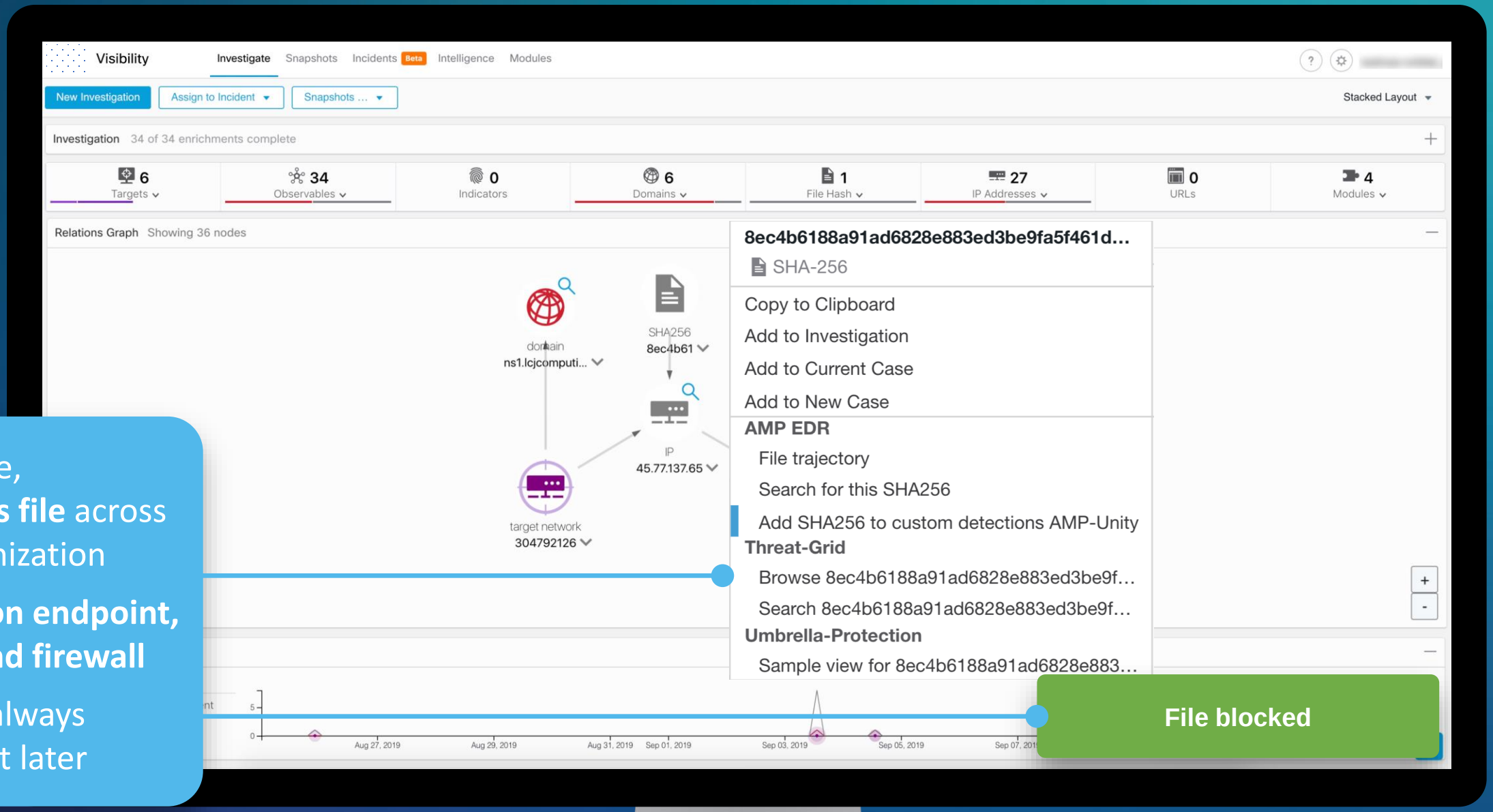


What about this file?

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

But it may be part of the attack.

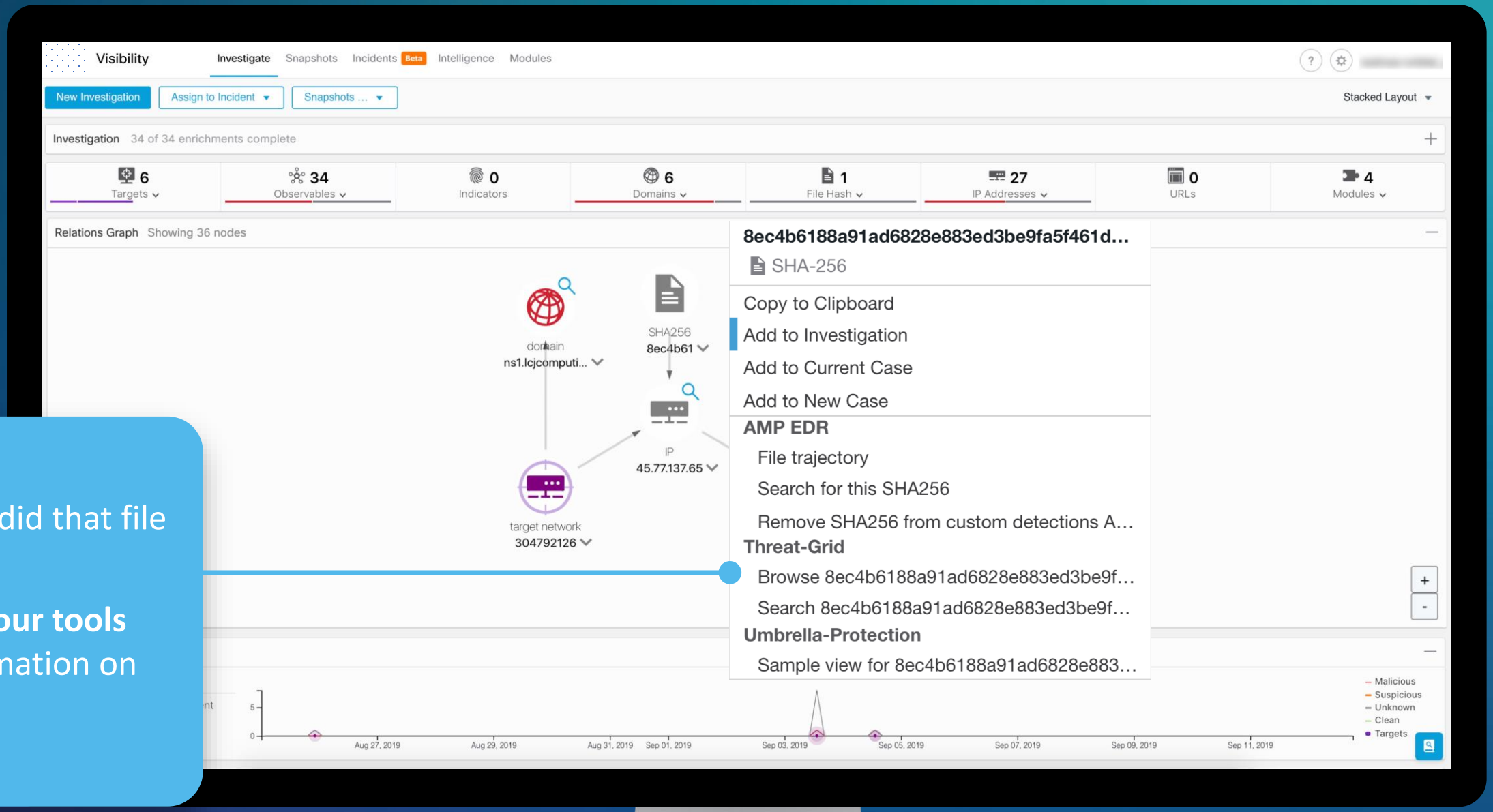
What can we do?



To be safe,
block this file across the organization

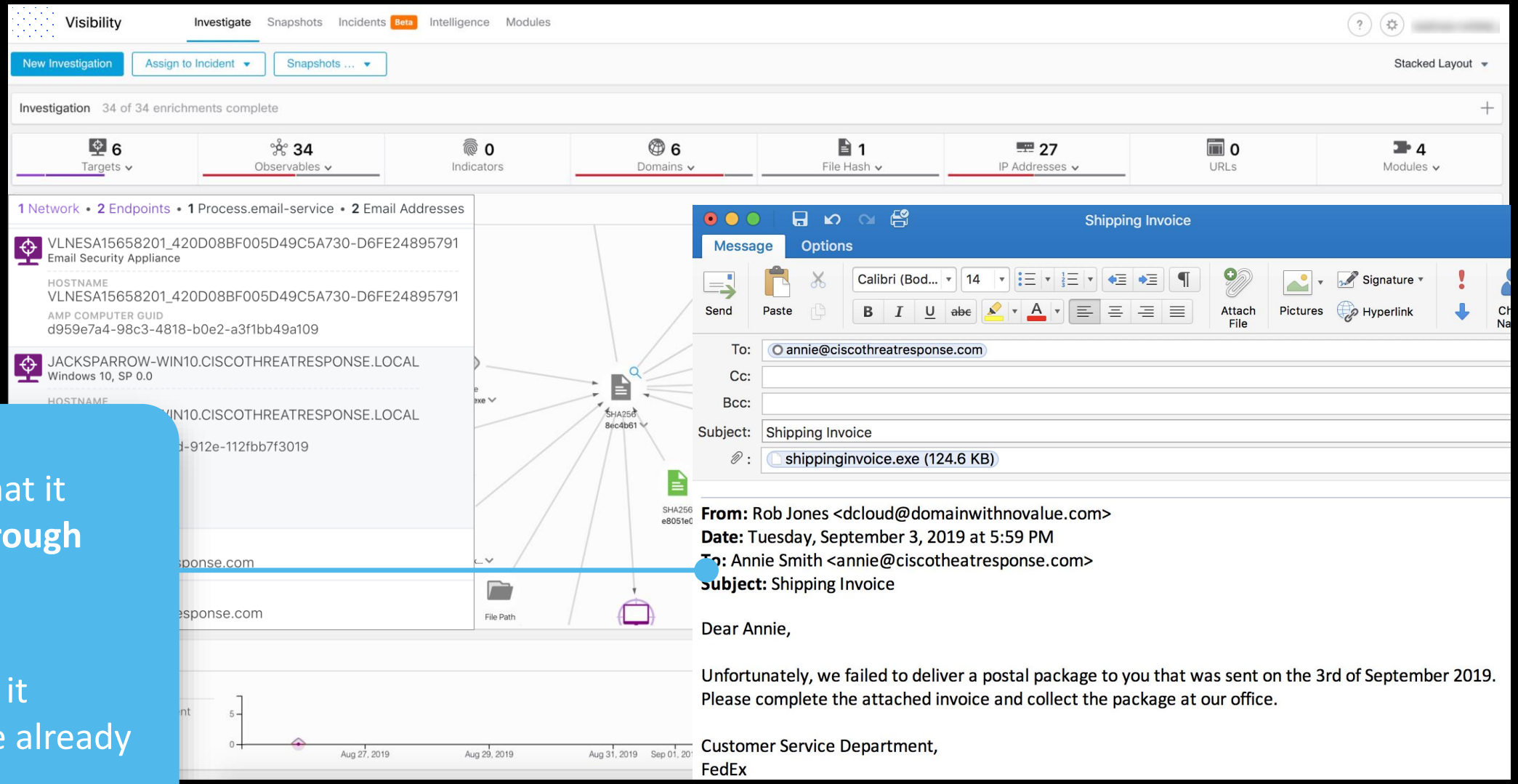
Block it on endpoint, email, and firewall

You can always unblock it later



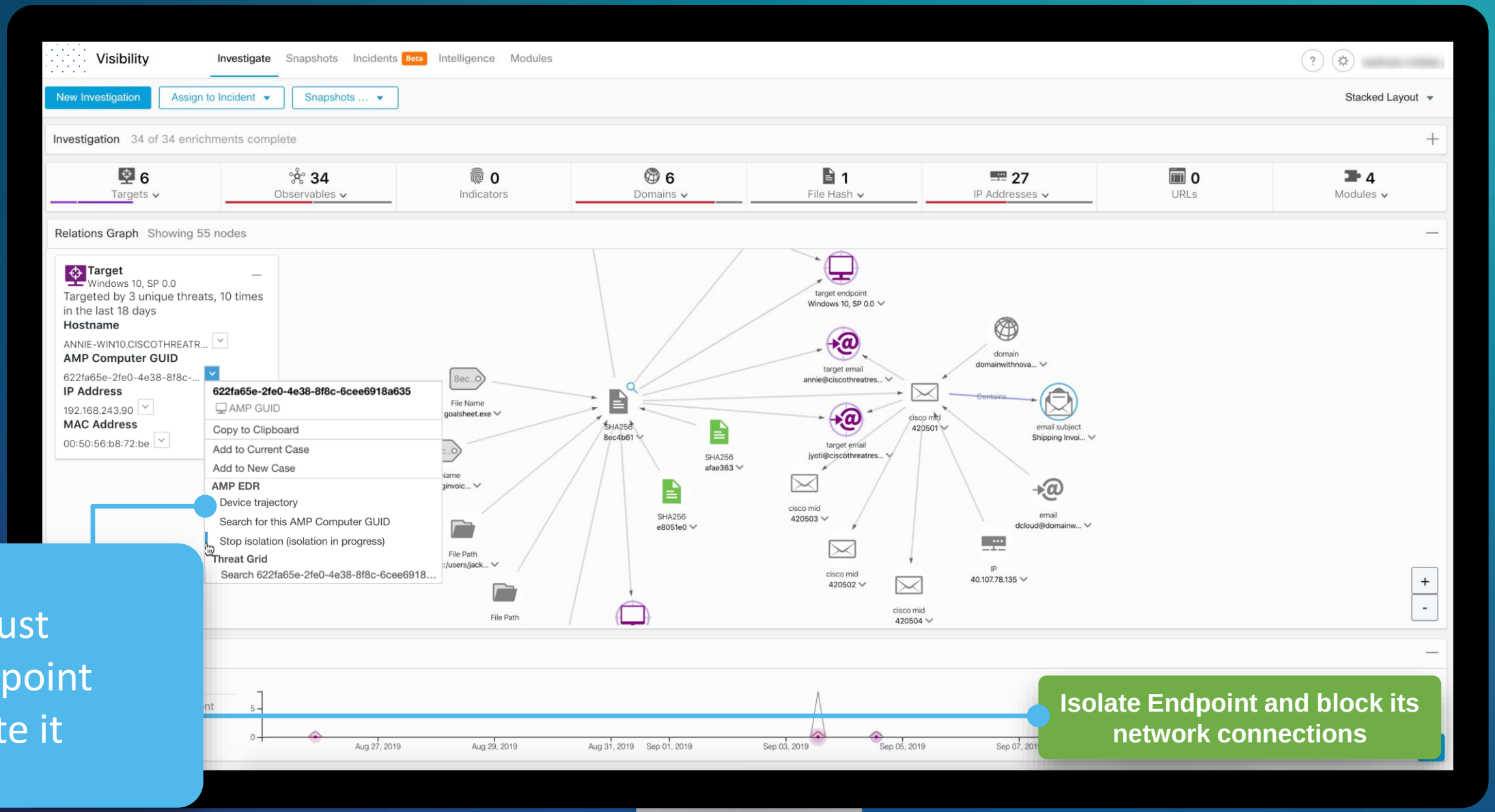
But how did that file get in?

Search your tools for information on this file



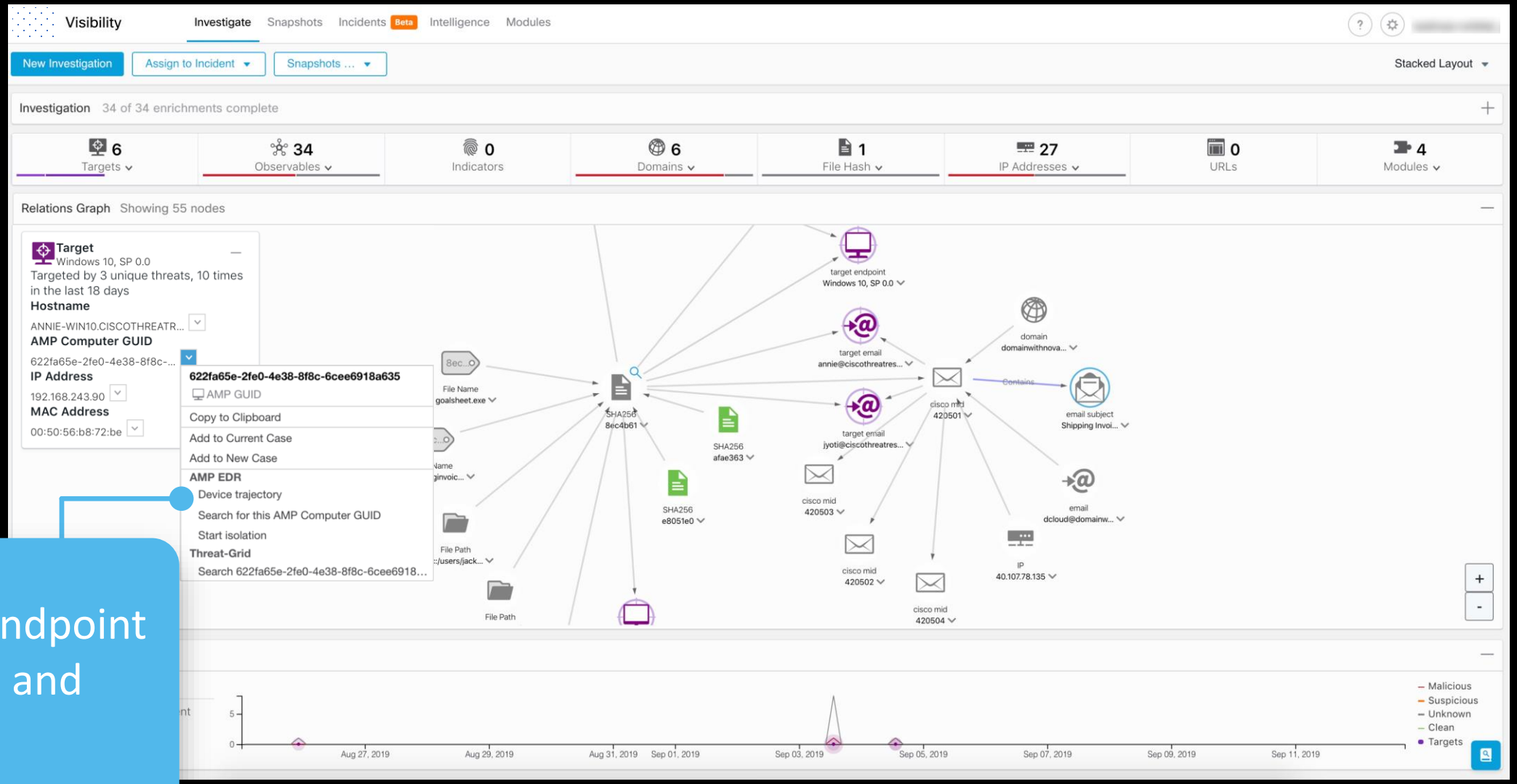
We learn that it **came in through email**

Good thing we blocked it everywhere already



Can't trust the endpoint so isolate it

Isolate Endpoint and block its network connections



Pivot to Endpoint Detection and Response

#GHC19

Endpoint Detection and Response

Dashboard | Analysis | Outbreak Control | Management | Accounts

Search

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.CISCOTHREATRESPONSE.LOCAL in group Orbital Group — No compromise events

Hostname	ANNIE-WIN10.CISCOTHREATRESPONSE.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

rbital | Take Forensic Snapshot | View Snapshot | Orbital Query | Events | View Changes

Start Isolation | Scan... | Move to Group...

Filters | Search Device Trajectory

5 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 2 3

AUG SEP

Capture **Forensic snapshot** of the endpoint

Forensic Analysis | Dashboard | Query | Jobs | Assets | Catalog | GraphQL | Node 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 -EJjrADpowR1OpScsPyTPg

programs

NAME	VERSION	PU
-EJjrADpowR1OpScsPyTPg		
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	Go
Cisco AMP for Endpoints Connector	6.5.1.11185	Ci
Google Update Helper	1.3.34.11	Go
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

#GHC19

Take away

TODAY
Study Up

- **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

3 MONTHS
Assess

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

6 MONTHS
Apply

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