



# Aby vás infikované koncové zariadenie nestálo hlavu

Peter Mesjar  
Consulting Systems Engineer  
25.6.2019





# Mám sa obávať novoobjavenej kybernetickej hrozby?

“Otázka za milión” v kybernetickej bezpečnosti

TUESDAY, JUNE 4, 2019

# It's alive: Threat actors cobble together open-source pieces into monstrous Frankenstein campaign

## Našťastie nemusím 😊

**Threat Response** Investigate Snapshots Intelligence Modules

New Investigation Snapshots ...

**0** Targets **12** Observables **7** Indicators **3** Domains **6** File Hashes **0** IP Addresses **3** URLs **5** Modules

Investigation 12 of 12 enrichments complete with **1 Alert**

### Indicators of Compromise

**Hashes**  
 418379fbfe7e26117a36154b1a44711928f52e33830c6a8e740b66bcbe63ec61  
 50195be1de27eac67dd3e5918e1fc80acaa16159cb48b4a6ab9451247b81b649  
 6b2c71bf65d2a9514fb27a811d20155e4034b407f84c004570973a9620a81c6d0

Investigate Clear Reset What can I search for?

### Relations Graph

Showing 42 nodes

### Sightings Timeline

My Environment Global

**0** Sightings in My Environment

First: Last: Jun 24, 2019

### Observables

List View

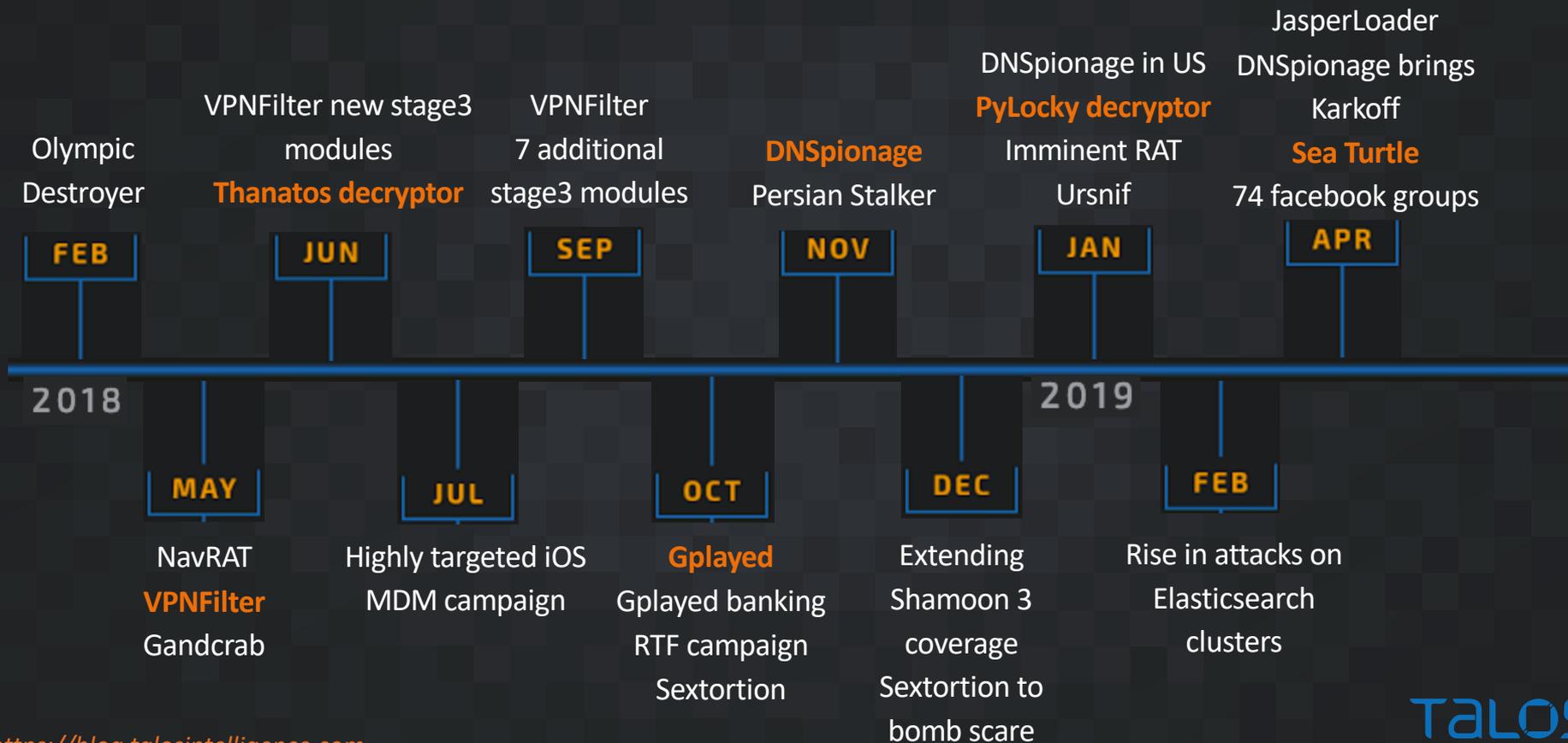
- b2600ac9b83e5b...**  
Malicious SHA256 Hash  
Last seen on May 31, 2019
- msdn.cloud**  
Malicious Domain
- droobox.online**  
Malicious Domain  
Last seen on Jun 10, 2019
- msdn.cloud**  
Malicious Domain  
Last seen on Jun 20, 2019
- search-bing.site**  
Malicious Domain  
Last seen on Jun 24, 2019
- 418379fbfe7e2611...**  
Malicious SHA256 Hash  
Last seen on Apr 9, 2019
- 6be18e3afeec482...**  
Malicious SHA256 Hash  
Last seen on May 7, 2019
- http://droobox.onli...**  
Malicious URL  
No Sightings
- http://search-bing...**  
Malicious URL  
No Sightings
- http://msdn.cloud/...**  
Malicious URL  
No Sightings

Module	Observable	Disposition	Reason
Umbrella	DOMAIN: msdn.cloud	Malicious	Poor Cisco Umbrella reputation st
Talos Intelligence	DOMAIN: msdn.cloud	Malicious	Poor Talos Intelligence reputation

25 per page 1-2 of 2

Previous Next

# What did TALOS find after Nyetya/Not Pyetya attack





“Houston” nemáme problém😊

Fáza pred útokom



Recycle Bin



Cisco AMP for Endpoint...



FileZilla Client



Stuff



Cisco AnyConne...



Firefox



Task Mgr



Windows Live Mail

Cisco AnyConnect Secure Mobility Client

**VPN:**  
Connected to dCloud.

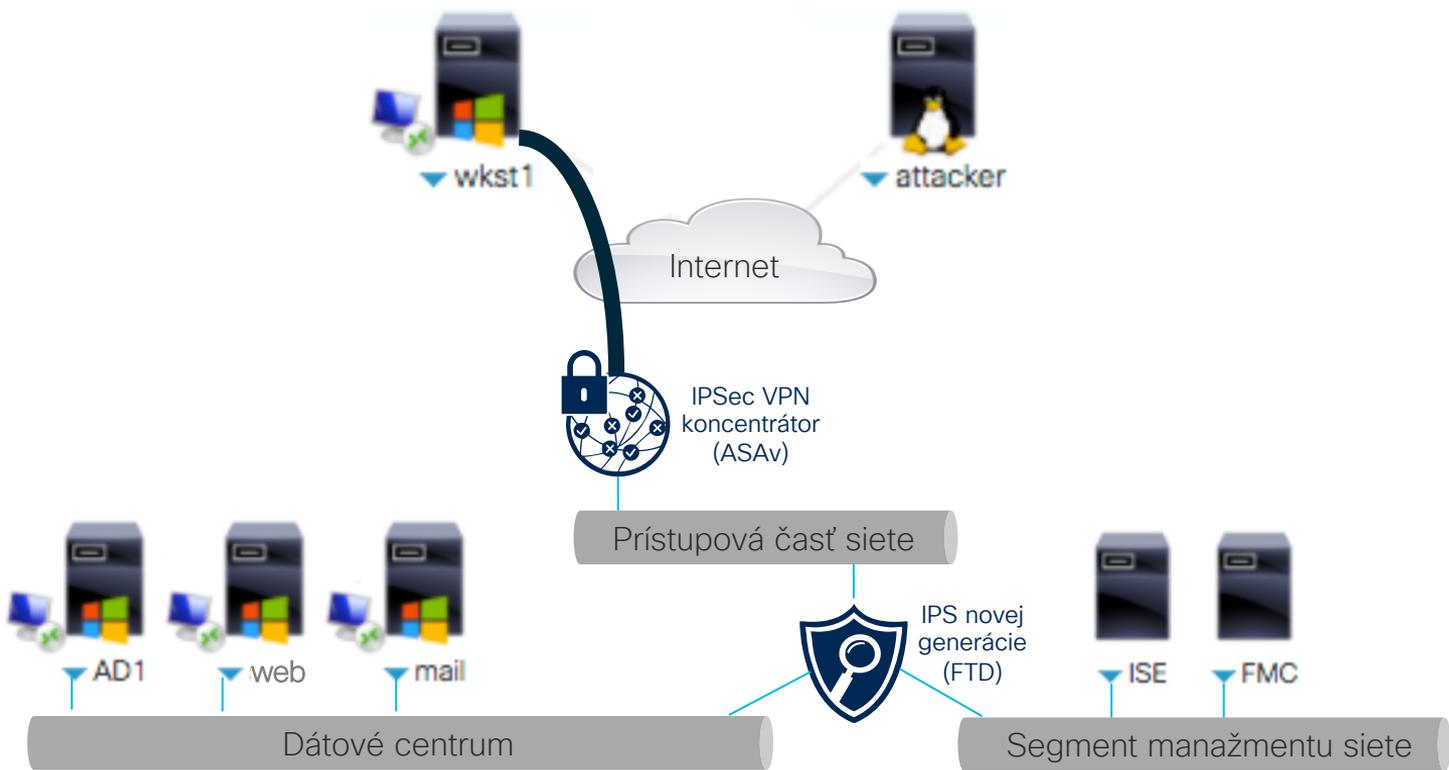
dCloud

00:13:06 IPv4

**Roaming Security:**  
You are protected by Umbrella.  
DNS queries are not encrypted.

© 2018 Cisco

# Typická počítačová sieť dnes



Search for a message



## ACTION REQUIRED!

Apple (support@apple.com) [Add contact](#)

4/29/2019 1:02 PM

To: manager@dcloud.cisco.com;



Dear User,

The following changes to your Apple ID, **manager@dcloud.cisco.com** were made today

### **Credit card updated: ACTION REQUIRED!**

Your credit card data may have been breached. In order to protect your security, you must immediately update your secure profile using the attached account update tool. Failure to comply will result in immediate suspension of your account, and you could be at risk of losing iCloud backup data including music, photos and backups

[Account Update Tool](#)

Sincerely, Apple Support

## ACTION REQUIRED!

General Details

Internet headers for this message:

```
Received: from esa.dcloud.cisco.com (198.19.10.146) by mail1
(198.19.10.2) with Microsoft SMTP Server id 14.1.438.0; Mon,
14:02:24 +0100
IronPort-SDR: GV1veQ3mXsZJ9JhsurIR4Vv20Q8HyoFD15DIH
Vgku6V/BZHJRHGnV++07vDIqswEqKB4JwSssCaVuoeD3C
HYUFX6yFFoEVqqCuDERPhctYtfoPouzg4lI9ayo1aLh8By4Ny
xPbCPpXjS9UoJw7Riq/3NbmICIKi8AV3T w6XMTnpPILFkyg
TDkrHXCrB4xWwy1nnTs2jxT+
X-Amp-Result: SKIPPED(no attachment in message)
Received: from attacker.dcloud.cisco.com (HELO attacker) [1:
by esa.dcloud.cisco.com with ESMTP; 29 Apr 2019 13:02:24
Received: from [::1] (helo=attacker.dcloud.cisco.com) by
(Exim 4.86) (envelope-from <support@apple.com>) id
manager@dcloud.cisco.com; Mon, 29 Apr 2019 09:02:23 -04C
Message-ID: <971914.697063284-sendEmail@attacker>
From: Apple <support@apple.com>
To: "manager@dcloud.cisco.com" <manager@dcloud.cisco.c
Subject: ACTION REQUIRED!
Date: Mon, 29 Apr 2019 13:02:23 +0000
```

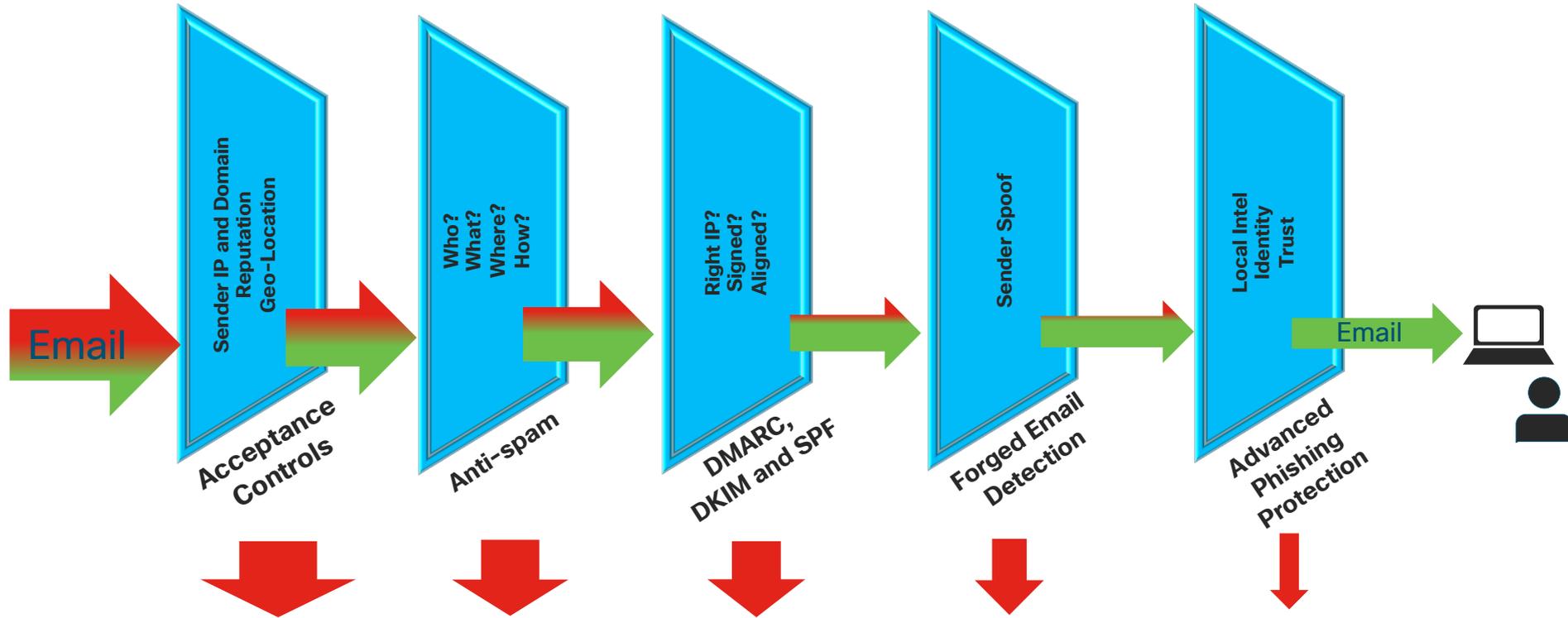
Message Source...

OK

Cancel

# Email je stále číslo 1 pre počítačové kompromitácie koncových zariadení!

# Securing Inbound Email: Layers of Defense





“Houston” máme problém!

Fáza počas útoku

File Edit View History Bookmarks Tools Help

Cisco Firepower Management | Identity Services Engine | New Tab

https://ise.dcloud.cisco.com/admin/#home

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Summary | Endpoints | Guests | Vulnerability | Threat

Click here to do visibility setup Do not show this again.

### METRICS

**Total Endpoints** 1

**Active Endpoints** 1

**Rejected Endpoints** 0

**Anomalous Behavior** 0

**Authenticated** 0

**AUTHENTICATIONS**

Identity Store Identity Group Network Device Failure Reason

ad1: [100%]

**ENDPOINTS**

Type Profile

workstations: [100%]

**BYOD ENDPOINTS**

Type Profile

No data available.

**ALARMS**

Severity	Name	Occu...	Last Occurred
	<input type="text" value="Name"/>		

ISE Authentication Inacti... 10270 14 mins ago

**SYSTEM SUMMARY**

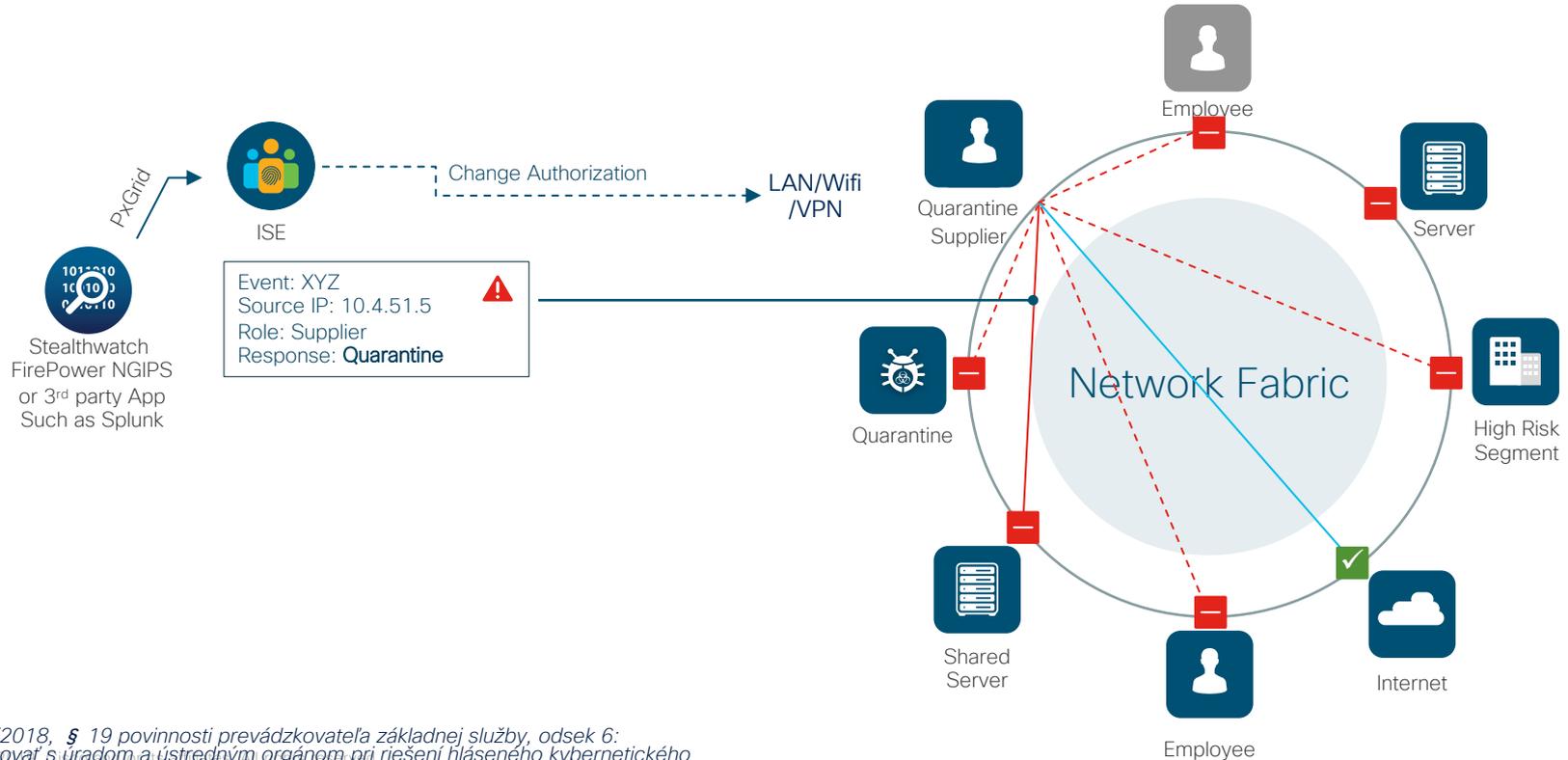
1 node(s) All 24HR

ise	CPU	Memory	Authentication Latency
<span style="color: green;">✔</span>			

2:44 PM 4/29/2019

# Cisco Integrovaná Kybernetická Bezpečnosť

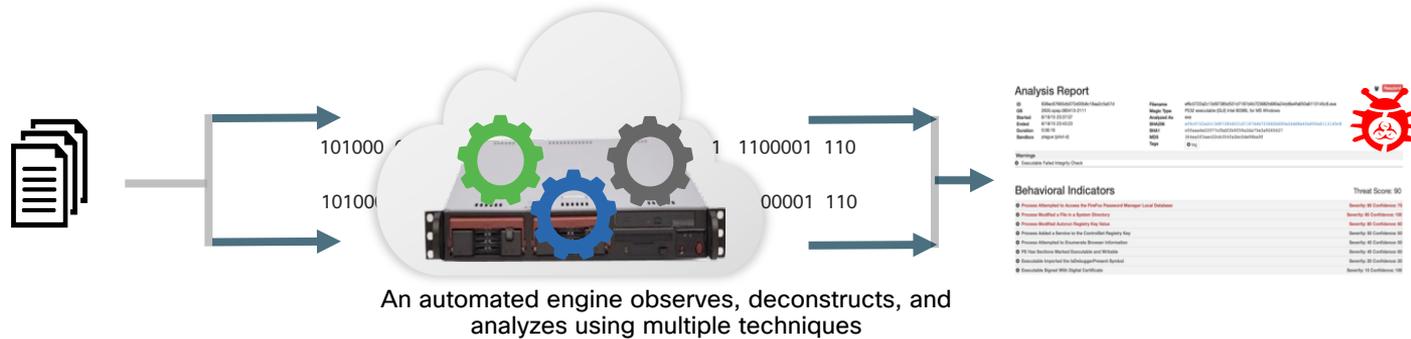
## Detekcia -> Karanténa -> Riešenie bezpečnostného incidentu



zákon č. 69/2018, § 19 povinnosti prevádzkovateľa základnej služby, odsek 6:  
c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

# Cisco Threat Grid = Sandbox + Threat Intelligence

## Malware Analysis / Threat Intelligence



### Malware Analysis

- Automated Analysis
  - Static
  - Dynamic
- Global Correlation



### Threat Intelligence

- Threat Score
- Behavior Indicators
- Observables
- Analysis Reports

Provides a single solution delivered multiple ways: through the cloud, as an on-premises solution, or integrated into security technologies such as AMP (Advanced Malware Protection).

# Threat Grid Integrations



## Supported Integrations & Partners

## Select Recipe Integrations



## Select Threat Feed Integrations





# “Houston” máme po probléme?

Fáza po útoku

# Cisco Threat Response - vyhl'adanie IoC (Indication of Compromise)

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate Clear Reset What can I search for?

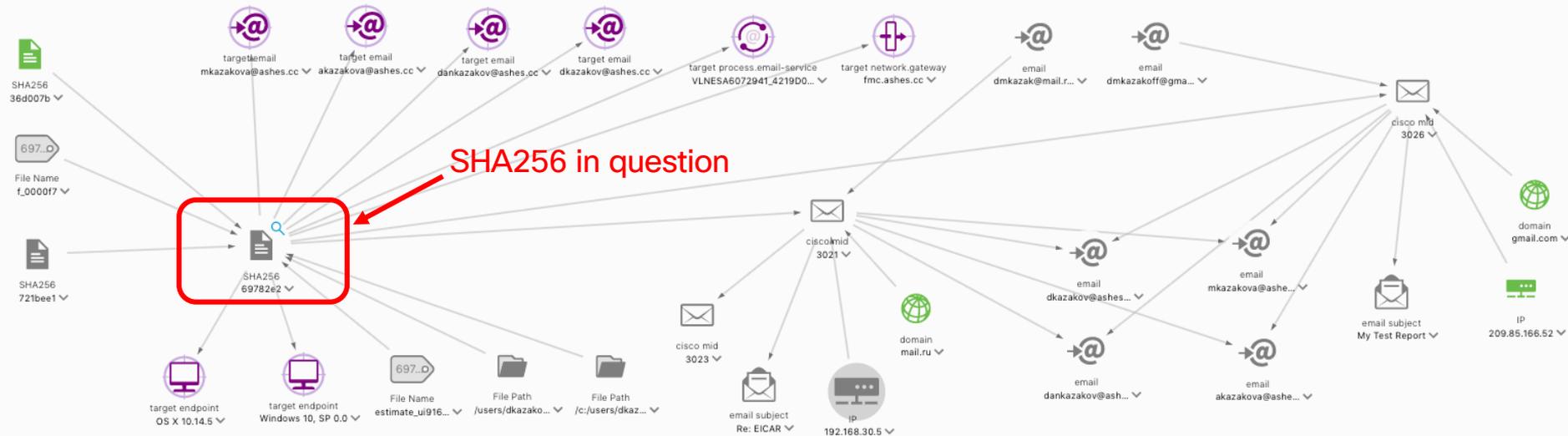
8 Targets

1 Observable

0 Indicators

0 Domains

1 File Hash



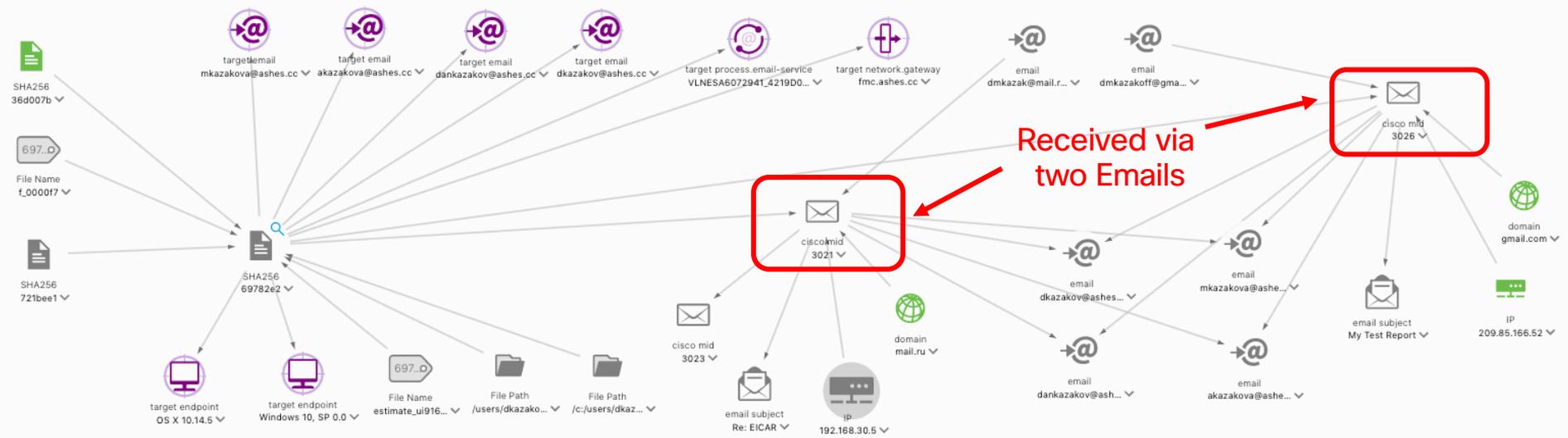
# Cisco Threat Response – trasovanie IoC cez sieť

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate Clear Reset What can I search for?

8 Targets 1 Observable 0 Indicators 0 Domains 1 File Hash



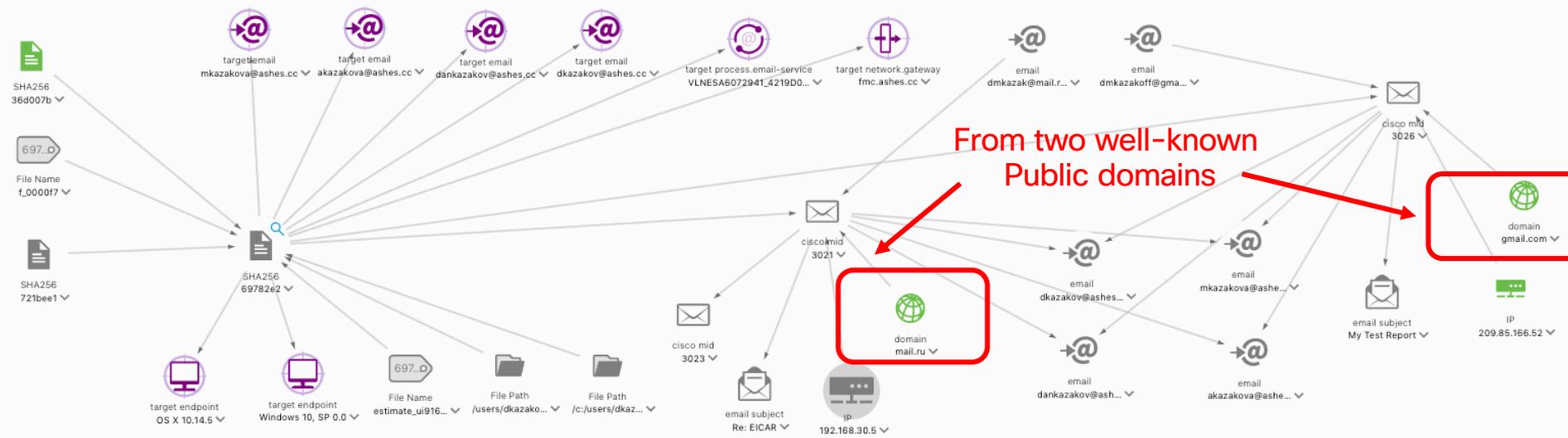
# Cisco Threat Response – trasovanie IoC cez sieť

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate Clear Reset What can I search for?

8 Targets 1 Observable 0 Indicators 0 Domains 1 File Hash



# Cisco Threat Response – trasovanie IoC cez sieť

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate

Clear

Reset

What can I search for?



8  
Targets



1  
Observable



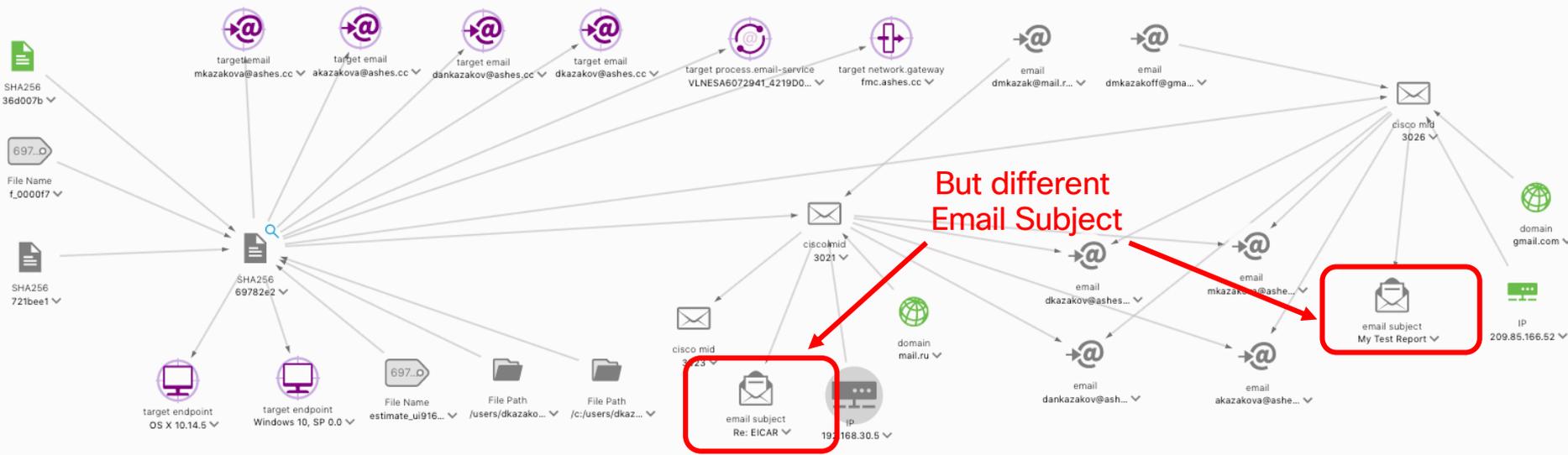
0  
Indicators



0  
Domains



1  
File Hash



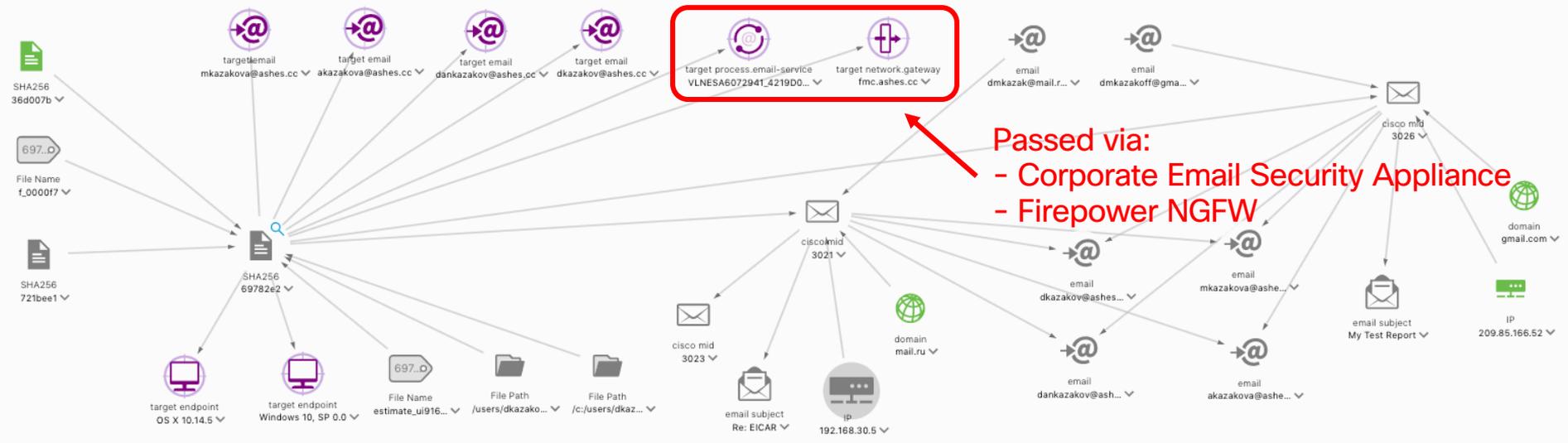
# Cisco Threat Response – trasovanie IoC cez sieť

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate Clear Reset What can I search for?

8 Targets 1 Observable 0 Indicators 0 Domains 1 File Hash



# Cisco Threat Response - analýza cieľa

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate Clear Reset What can I search for?

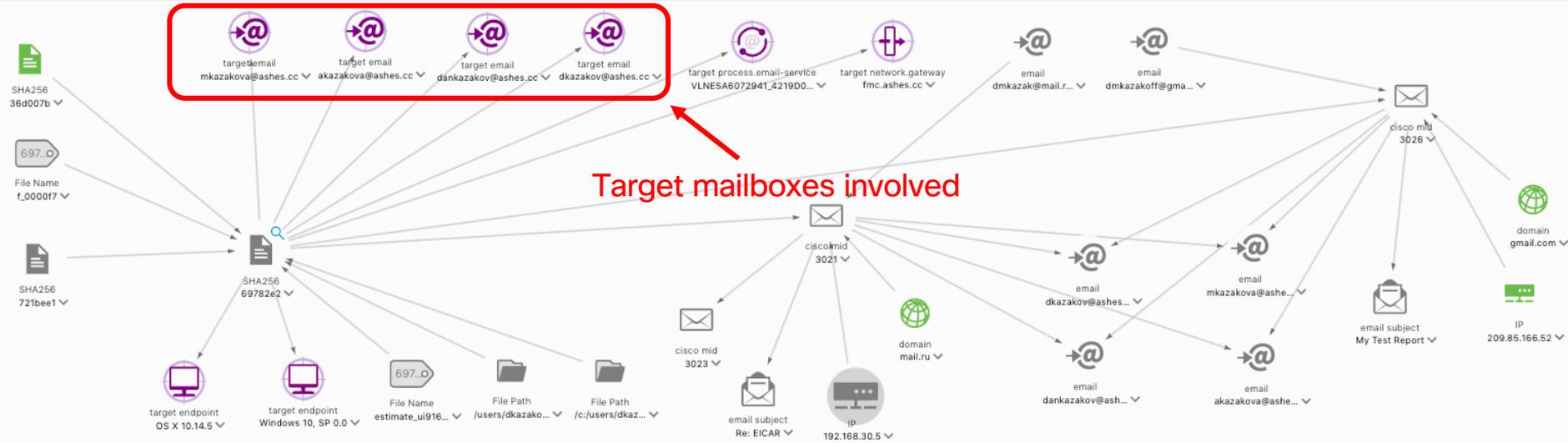
8 Targets

1 Observable

0 Indicators

0 Domains

1 File Hash



# Cisco Threat Response - analýza cieľa

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate Clear Reset What can I search for?

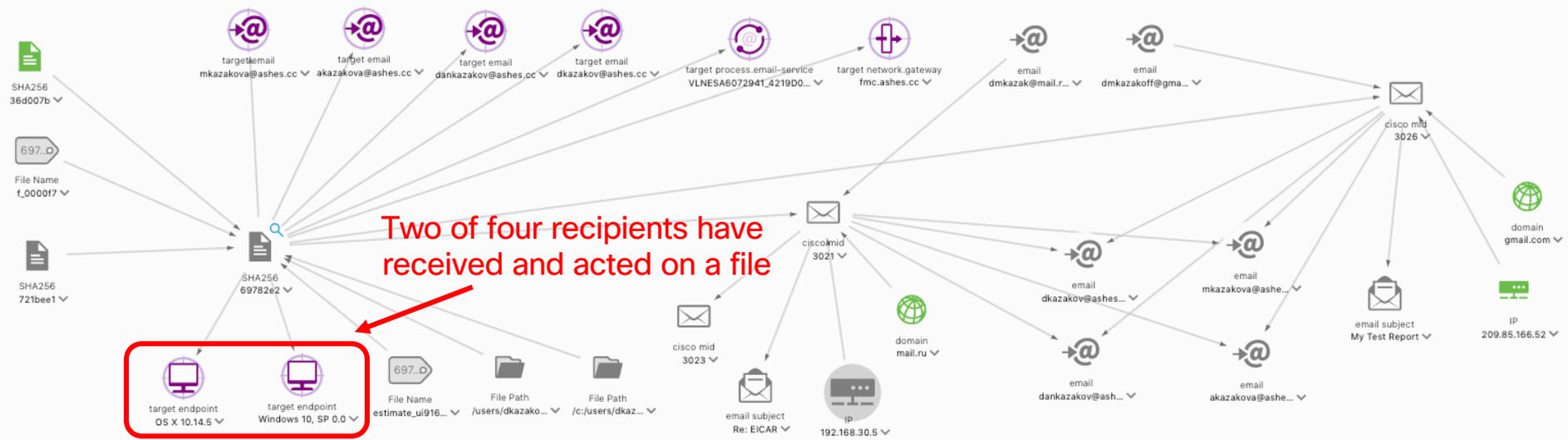
8 Targets

1 Observable

0 Indicators

0 Domains

1 File Hash



# Cisco Threat Response – sled udalostí v čase

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f   
SHA256 Hash

My Environment Global

8 Sightings in My Environment

First: May 30, 2019

Last: May 30, 2019



Judgement (1) Verdict (1) Sightings (8)

AMP for Endpoints	32 minutes ago	Created by Sighting	High	Unknown	endpoint	AMP Event 	<p>SHA256: 36d007b4...</p> <p>parent of</p> <p>SHA256: 69782e24...</p> <p>FILE NAME: f_0000f7</p> <p>file name of</p> <p>SHA256: 69782e24...</p> <p>FILE PATH: /c:/users/dkazakov/appda...</p> <p>file path of</p> <p>SHA256: 69782e24...</p>	<p>HOST NAME: ashes-vm-win.ashes.cc</p> <p>AMP COMPUTER GUID: 1c30c493-ca9a-4d76-a1fe-...</p> <p>IP: 192.168.99.19</p> <p>MAC ADDRESS: 00:0c:29:c9-13-1c</p> <p>IP: 169.254.54.30</p> <p>MAC ADDRESS: 02:00:4c:4f:4f:50</p>
AMP for Endpoints	32 minutes ago	Moved by Sighting	High	Unknown	endpoint	AMP Event 	<p>SHA256: 721bee11...</p> <p>parent of</p> <p>SHA256: 69782e24...</p> <p>FILE NAME: estimate-148565sn (1...</p> <p>file name of</p> <p>SHA256: 69782e24...</p> <p>FILE PATH: /users/dkazakov/download...</p> <p>file path of</p> <p>SHA256: 69782e24...</p>	<p>HOST NAME: DKAZAKOV-M-223W</p> <p>AMP COMPUTER GUID: e44be0be-eb6b-404f-a4fc-...</p> <p>MAC ADDRESS: ac:de:48:00:11:22</p> <p>MAC ADDRESS: 8c:85:90:a5:28:7d</p> <p>IP: 192.168.99.12</p> <p>MAC ADDRESS: 48:65:ee:16:de:d3</p>

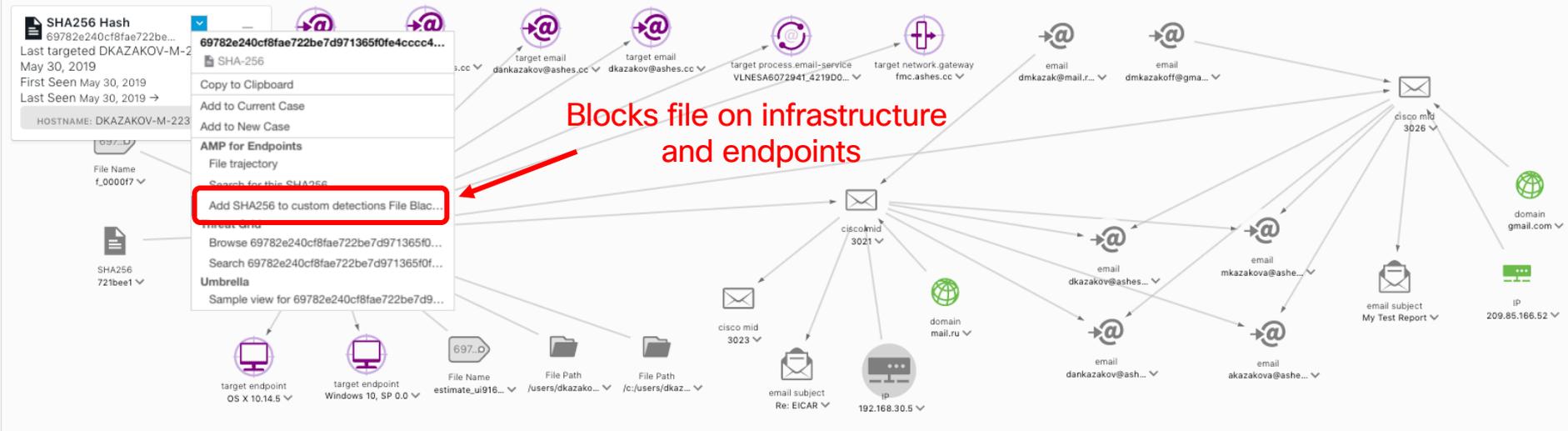
See the associated activities at the endpoint

Investigate deeper

Understand which hosts been involved

# Cisco Threat Response – bloknutie na pár klikov

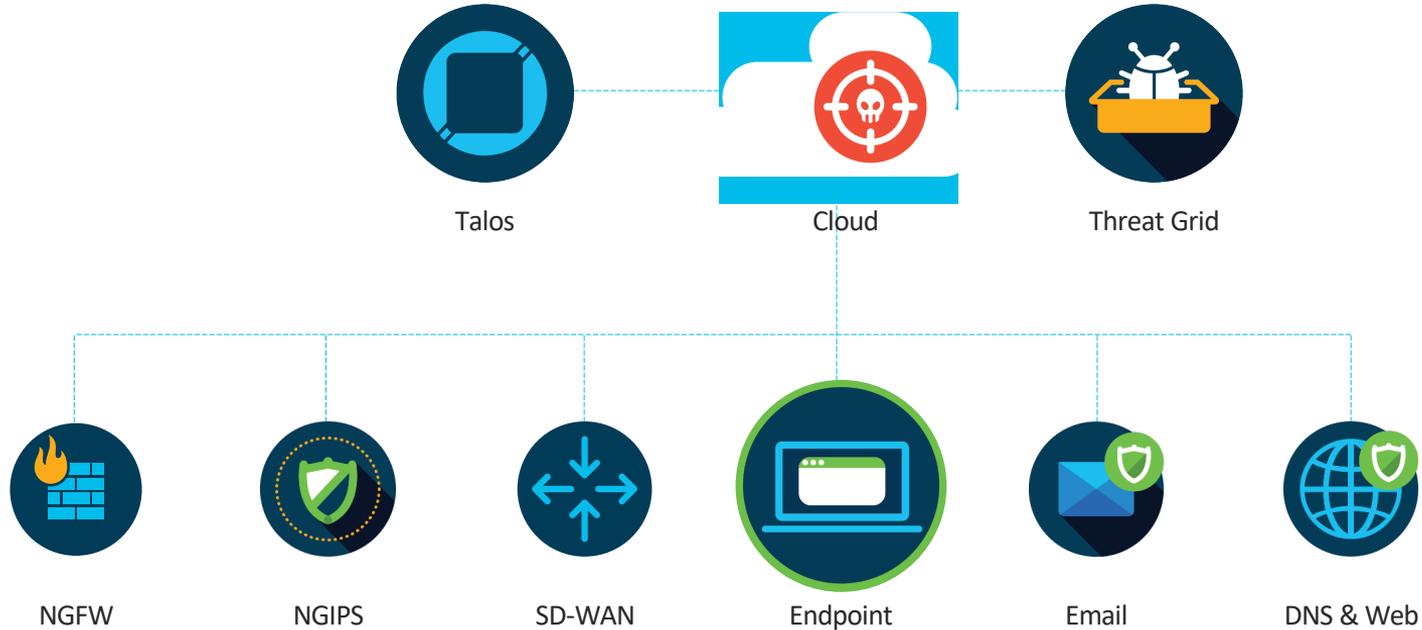
Relations Graph Showing 30 nodes



Na záver...

# Cisco Integrated Threat Defense

Share intelligence across network, cloud, web, email, and endpoints to see once & block everywhere.





TALOSINTELLIGENCE.COM



[blog.talosintelligence.com](https://blog.talosintelligence.com)



[@talossecurity](https://twitter.com/talossecurity)