

RSAConference2021

May 17 – 20 | Virtual Experience

SESSION ID: LAB1-M14

Methodologies of Investigation Enhanced by the External Attack Surface

Benjamin Powell

Director of Technical Marketing
RiskIQ

@benjaminpowell

<https://www.linkedin.com/in/benjaminpowell>

benjamin.powell@riskiq.com

Corian (Cory) Kennedy

Principal Vulnerability Researcher
RiskIQ

@corykennedy

cory@riskiq.com



RESILIENCE

#RSAC

How will You Apply this information to your organization and career?

Complete the “equation” for attendees:

Educate + Learn = Apply

Your role as instructor

We will demonstrate and give you skills to immediately improve your overall investigations with an enhanced perspective

Attendee role as student

Your role as a student is to ask questions and verify that you can apply the knowledge you gain in your investigations

How to apply this in the office = critical to justify attendance

You will be able to demonstrate new skills, experience running freely available tools. You will be able to demonstrate smarter, faster, and more accurate investigations skills.

Provide an “Apply” Slide – Part 2

When we are complete today:

- You will be able to understand your organizations own External Attack and how you can leverage it to enhance your investigations.

Warning!!

- You will be investigating real bad things. Which include *live, real-time observations from the internet*.
- We will share online resources (e.g., IP addresses, domain names) that are dangerous and pose a clear and present danger.
- We ask our participants to use their best judgment and minimize unnecessary risk while interacting with malicious systems lab exercises.

Tools

- We will be utilizing browser-based apps except when creating and running scripts.
- Screen sharing will be used. We encourage questions to make this workshop interactive.
- Below are tools that might need to be installed on your computer for small parts of some exercises. Don't worry if you do not have the tools installed everything will be demonstrated and slides will be provided to everyone.
 - Python3 <https://www.python.org/downloads/mac-osx/>
 - Jupyter Notebook <https://jupyter.org/>
 - MISP

Tools to use in the exercises today

During the investigations we will be using the following tools.
Please bookmark the following websites.

- RiskIQ PassiveTotal <https://community.riskiq.com>
- Python3 <https://www.python.org/downloads/mac-osx/>
- RiskIQ.SunBurst.Hunter
<https://github.com/NoDataFound/RiskIQ.SunBurst.Hunter>
- Jupyter Notebook <https://jupyter.org/>
- Library for RiskIQ PassiveTotal and Illuminate API
<https://pypi.org/project/passivetotal/>
- MISP <http://rsalab.threattracking.com/>
- Lab Files <https://www.riskiq.com/threat-hunting-resources/rsalab>

Benjamin Powell

Director of Technical Marketing (CEH)



Background

- Worked in IT for over 30 years.
- Focused on Security for over 14 years.
- I have personally worked in IT in the following industries:
 - State government
 - International Airport
 - Port District
 - Education
 - Biotech
 - Financial services
 - Manufacturing
 - Software development



Fun Fact:

- Be careful when you tell people in IT your hobby is spearfishing.

Corian (Cory) Kennedy



Principal Vulnerability Researcher

Background

- Hunter for advanced threat actors at internet scale targeting critical infrastructure and across all sectors
- Contributor to intelligence sharing frameworks (code and processes) including work with the National Defense ISAC is the Information Sharing and Analysis Center for the Defense Industrial Base
- HaKCer since 87
- 19 years working with **Red**, **Blue** and **Purple** Teams
- Founder SeckC.org

```
< I love nano >
  \   ^__^
   \  (oo)\_______
      (__)\       )\/\
         ||----w |
         ||     ||
MsqSLmNvbQ==
```



Investigation Methodologies we will be using today

- Leveraging the attack surface to enhance investigations
- Attack surfaces can be your organizations, partner, and even a threat actors
- Filtering Indicators against the attack surface for relevance to take the appropriate action in your investigations.

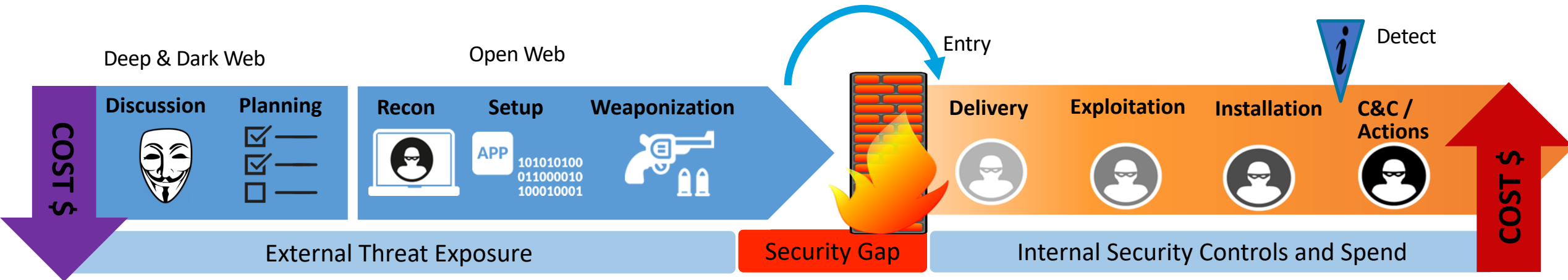
Why is Attack Surface Intelligence Important

Salesperson or Management

- I just read that there is a new Exchange Vulnerability our today.
 - Are we ok?
 - Are we patched?
 - What about our partners?
 - How bad is the attack?



Cyber Kill Chain



Proactive Security Outside the Firewall

DISCUSSION ON TARGETS

Treat Actors discuss potential targets and vectors

DOMAIN REGISTERED

Typosquatted domain purchased, but no email capability or web content associated

EMAIL CAPABLE

SPF or MX record added to the domain's DNS records

DISCUSSION ABOUT COMPROMISED HOSTS

Treat Actors discuss compromised hosts on targets network

DOMAIN PARKED

Domain resolves to a parked page. Owner generates revenue off of ads

SITE UNDER CONSTRUCTION

Un-parked, partially setup phishing page

PHISH ATTACK

Phishing page is live, email campaigns send traffic

INCIDENT RESPONSE

Phish blocked in browser blacklist, Domain name suspended; site taken down by hosting provider

Deep & Dark Web

Open Web

Entry

COST \$

Discussion



Planning



Recon



Setup



Weaponization



Delivery



Exploitation



Installation



C&C / Actions



COST \$

External Threat Exposure

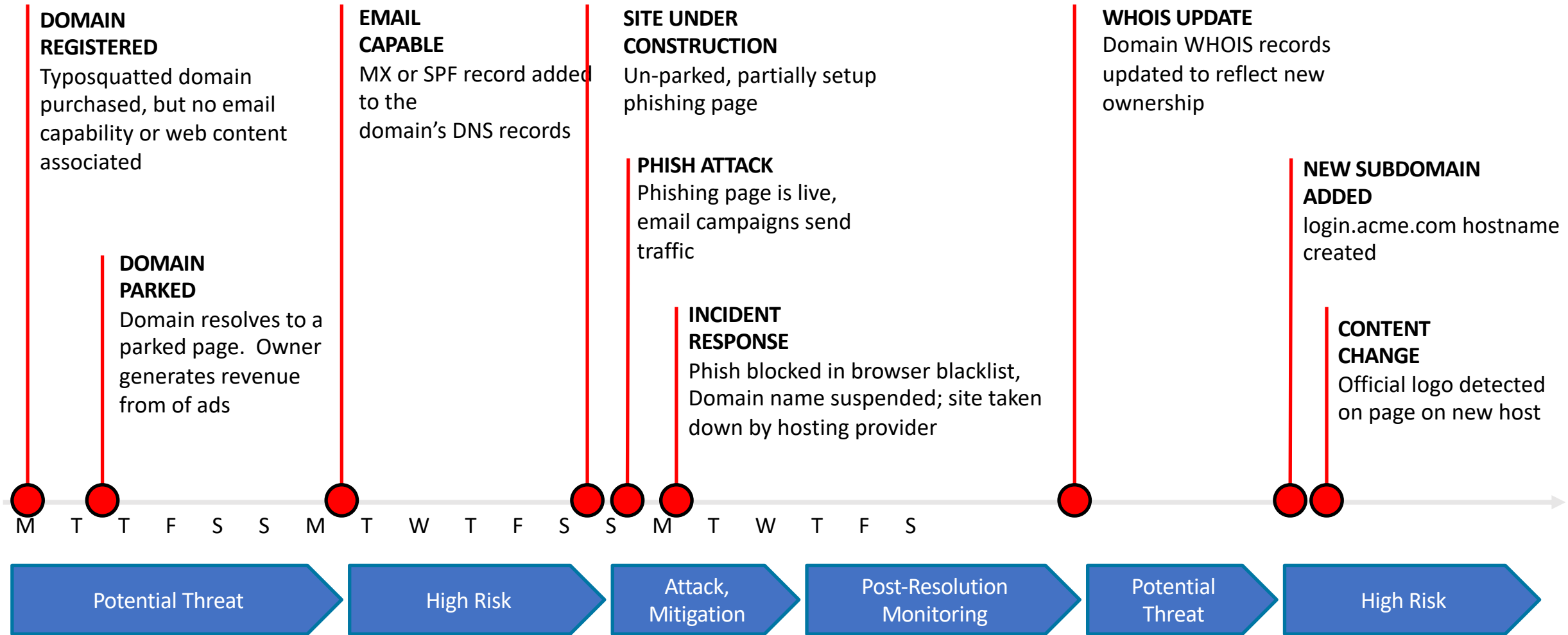
Security Gap

Internal Security Controls and Spend



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Continuously Monitoring Threats Over Time



Attackers Can't Avoid the Internet

1. Actions on the Internet emit signals
2. Signals are ephemeral and go unnoticed unless someone's listening
3. Captured signals can expose stages/elements/infrastructure of an attack
4. Exposed elements can destroy operations or render them less effective
5. Destroyed operations is money wasted

Attackers Can't Avoid the Internet



Threat Actor



Targeted User



Internet Signals Emitted

Attackers Can't Avoid the Internet

Threat Actor on the internet



Threat Actor



Internet Signals Emitted



Targeted User

- IP addresses
- Network blocks
- Autonomous systems (ASN)
- Internet service providers (ISP)



Attackers Can't Avoid the Internet

Threat Actor Creates Email



Threat Actor



Internet Signals Emitted



Targeted User

- User IP addresses
- User network blocks
- User autonomous systems (ASN)
- User internet service providers (ISP)
- Email provider
- Email subject
- Email body
- Email body
- Email attachment
- Email headers
- Email language
- Email date/timestamp

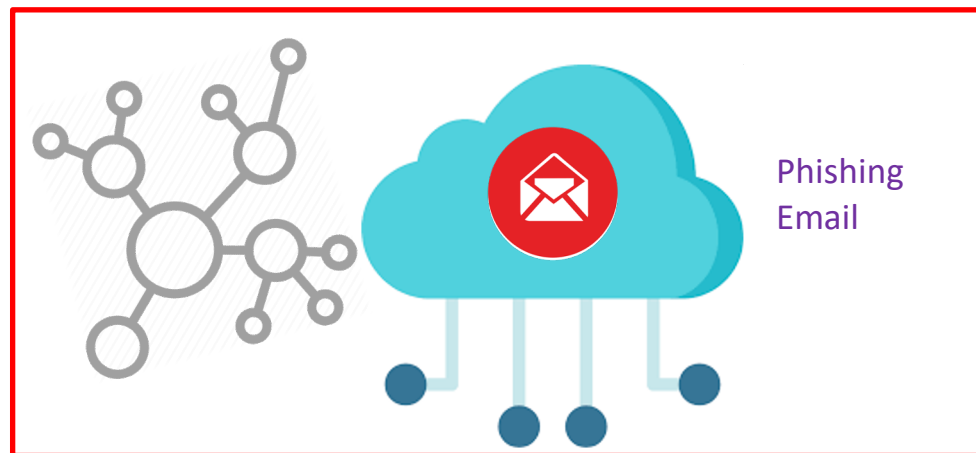


Attackers Can't Avoid the Internet

Threat actor sends phishing email message



Threat Actor



Internet Signals Emitted



Targeted User

- User IP addresses
- User network blocks
- User autonomous systems (ASN)
- User internet service providers (ISP)
- Email provider
- Email subject
- Email body
- Email body
- Email attachment
- Email headers
- Email language
- Email date/timestamp
- Transit IP addresses
- Transit network blocks
- Transit times



Attackers Can't Avoid the Internet

Targeted user receives phishing email message



Threat Actor



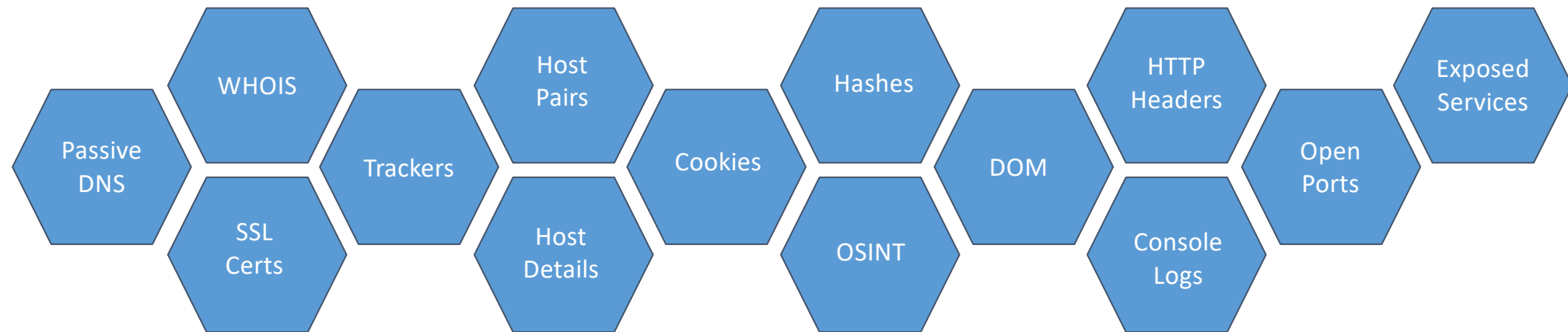
Internet Signals Emitted

- User IP addresses
- User network blocks
- User autonomous systems (ASN)
- User internet service providers (ISP)
- Email provider
- Email subject
- Email body
- Email body
- Email attachment
- Email headers
- Email language
- Email date/timestamp
- Transit IP addresses
- Transit network blocks
- Transit times
- Transit autonomous systems (ASN)
- Read date/timestamp
- Read notification
- Reader host operating system
- Reader location



Signals at your disposal to the community

- Globally-placed sensors and proxies
- Headless web crawlers performing billions of requests a day
- Regular IPv4 internet scans for ports and data
- Mined open-source intelligence and results



Caveats to Threat Infrastructure Analysis

- All data sources have a bias
 - Gaps in collection, specific processes, time zone skews, etc.
- Connection != Solid Analytical Lead (SAL)
 - Analysts must apply their experience and evaluate the results
 - SAL should be backed up with multiple points-of-proof (PoP)
- Process is not static
 - Infrastructure can change at any moment
 - Requires constant monitoring and analysis to remain accurate

Why Apply Threat Infrastructure Analysis Inside Your Organization?

- Proactively identify threats
 - Related infrastructure (reuse of unique details)
 - Uncover overlap in targeting (verticals, individual, etc.)
- Assess potential threats
 - Historical context (who did they target, when, etc.)
 - Measure capabilities -Tactics, Techniques and Procedures (TTPs)
- Identifies gaps inside your organization
 - Do you have enough to inform your own investigations?
 - Can you deploy your own sensors and collection?
 - Is there existing data not being leveraged?

How to Build an Attack Surface

- Tribal knowledge from multiple tribes
- Spreadsheets
- WHOIS information
- External DNS servers
- SSL Certificate information associated with IP addresses
- ASNs
- Port Scanning of IP addresses
- Vulnerability Scanner
- Or use a tool that can create it for you

How did we create the attack surface today

- Combination of WHOIS, PDNS, DNS Name Server Information, Web Components, SSL Certificates associated with IP addresses, Port information.
- Today we will be using the public internet accessible attack surface for Aeroflot-Russian Airlines.

Login to RiskIQ PassiveTotal

<https://community.riskiq.com/>

Username: rsalab-01@threattracking.com

Password: RSAriskiq!1-01

Aeroflot-Russian Airlines

<https://community.riskiq.com/attack-surfaces/371662>



Downloaded the Attack Surface

Home / Attack Surface Intelligence

Aeroflot-Russian Airlines

Attack Surface Priorities

High Severity

2 Observations

Found from 1 of 23 Insights

Top Observations

Microsoft Patches Four 0-Day Remote Code Execution V... 2

SUNBURST Supply Chain Attack Against SolarWinds Ori... 0

NSA Warns of Russian Actors Targeting Vulnerable Extm... 0

All 23 Insights

Medium Severity

11 Observations

Found from 5 of 43 Insights

Top Observations

Expired SSL Certificates 5

HAFNIUM targeting Exchange Servers with 0-day exploits 2

ProxyLogon - Microsoft Exchange Server Vulnerabilities (...) 2

All 43 Insights

Low Severity

14 Observations

Found from 6 of 11 Insights

Top Observations

Deprecated Tech - Nginx 3

Deprecated Tech - PHP 3

Deprecated Tech - Microsoft IIS 3

All 11 Insights

Attack Surface Composition

Assets

This dashboard provides immediate insight into the core components of your attack surface. All data shown in the interface is built from your Digital Footprint and updated in real-time. Sections are organized by common pain-points identified by our customer base.

Type	Count
IP Blocks	18
IPs	2,182
Domains	25
Cloud Hosts	5
SSL Certificates	51
Whois Contacts	18
ASNs	1
Hosts	1,762

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE		
1	Asset Name	UUID	Status	Keystone	Description	Created	Updated	First Seen	Last Seen	Tags	Priority	Brands	Primary Co	Secondary	Organizational	External ID	Additional	Domain	Cname	Cname Dns	IP Address	Web Comp	Web Comp	Web Comp	Web Comp	Web Comp	Header	Header	Header	Header	Header		
2	*andrey.s.296b3a1e-6	Approved				2021-05-01	2021-05-01	2021-05-01	2021-05-01									aeroflot.ru			185.69.82.												
3	*aeroflot.14755104-6	Approved				2021-05-01	2021-05-01	2021-05-01	2021-05-01									aeroflot.ru			185.69.80. Apache						Server	Server	Content-En	gip, Apache	185.69.80.		
4	*aeroflot.c80158be-6	Approved				2021-05-01	2021-05-01	2021-05-01	2021-05-01									aeroflot-ca			185.69.80. Apache												
5	test-groups.c2f5c748-6	Approved				2021-04-21	2021-05-01	2021-04-21	2021-05-01									aeroflot.co			178.154.2.												
6	*.tcp.vc.a.e68bf0e9-6	Approved				2021-04-01	2021-04-01	2021-04-01	2021-04-01									aeroflot.tw			185.69.80.												
7	*.tcp.vc.a.4bdc2b23-6	Approved				2021-04-01	2021-04-01	2021-04-01	2021-04-01									aeroflot-jag			185.69.80.												
8	m-aff-stagi.1daa0aea-6	Approved				2021-03-21	2021-04-01	2021-03-21	2021-04-01									aeroflot.ru			185.69.83.												
9	myapps.aer.1a0cfc19-6	Approved				2021-03-11	2021-05-01	2021-03-11	2021-05-01									aeroflot.ru	myapps.mi	microsoft.c	20.190.151												
10	*.www.aer.1e023834-6	Approved				2021-03-01	2021-04-01	2021-03-01	2021-04-01									aeroflot-ca			185.69.80.												
11	*.m.aeroflot.69d94f0f-6	Approved				2021-03-01	2021-03-01	2021-03-01	2021-03-01									aeroflot-ca			185.69.80.												
12	*.aeroflot.1075a050-6	Approved				2021-03-01	2021-03-01	2021-03-01	2021-03-01									aeroflot-va			185.69.80.												
13	*.aeroflot.046c2b71-6	Approved				2021-03-01	2021-03-01	2021-03-01	2021-03-01									aeroflotcar			185.69.80.												
14	*.aeroflot.4086c2a4-6	Approved				2021-03-01	2021-03-01	2021-03-01	2021-03-01									aeroflot-ca			185.69.80.												
15	*.aeroflot.71607eaf-6	Approved				2021-03-01	2021-03-01	2021-03-01	2021-03-01									aeroflot-en			185.69.80.												
16	dpp.f5.aer.f6c1006-f	Approved				2021-02-01	2021-05-01	2021-02-01	2021-05-01									aeroflot.ru			80.92.37.9												
17	aff-sfb-wco.57868f5d-6	Approved				2021-01-31	2021-05-01	2021-01-31	2021-05-01									aeroflot.ru			80.92.39.1												
18	aff-sfb-sip.c.e7590e35-6	Approved				2021-01-31	2021-05-01	2021-01-31	2021-05-01									aeroflot.ru			80.92.39.1												
19	*.aeroflot.eca335d2-6	Approved				2021-01-31	2021-04-01	2021-01-31	2021-04-01									aeroflot.ac			185.69.80.												
20	aff-sfb-sip.c.8fab98d6-6	Approved				2021-01-21	2021-05-01	2021-01-21	2021-05-01									aeroflot.ru			80.92.36.7												
21	aff-sfb-av.d.2c851767-6	Approved				2021-01-31	2021-05-01	2021-01-31	2021-05-01									aeroflot.ru			80.92.36.7												
22	aff-sfb-wco.680dcd1a-6	Approved				2021-01-31	2021-05-01	2021-01-31	2021-05-01									aeroflot.ru			80.92.36.7												
23	stage.flight.61514773-6	Approved				2021-01-21	2021-05-01	2021-01-21	2021-05-01									aeroflot.ru	aeroflot-ij	azurewebs													
24	flights.aero.244b0a30-6	Approved				2021-01-21	2021-05-01	2021-01-21	2021-05-01									aeroflot.ru	aeroflot-ij	azurewebs													
25	www.test.j.b1a97d9c-6	Approved				2021-01-21	2021-05-01	2021-01-21	2021-05-01									test-jul20i			37.140.159.	Reg.ru											
26	test-jul20i.c5ca0f0e-6	Approved				2021-01-21	2021-05-01	2021-01-21	2021-05-01									test-jul20i			37.140.159.	Reg.ru											
27	*.aeroflot.j.681da216-6	Approved				2021-01-21	2021-05-01	2021-01-21	2021-05-01									aeroflot-jax			185.69.80.												
28	gw-origin.f.1cd33ec4-6	Approved				2021-01-31	2021-05-01	2021-01-31	2021-05-01									aeroflot.ru			185.69.80.												
29	*.georgk.a.447c66e9-6	Approved				2021-01-11	2021-05-01	2021-01-11	2021-05-01									aeroflot.ru			185.69.82.												
30	gw-origin.k.2202d478-6	Approved				2021-01-11	2021-05-01	2021-01-11	2021-05-01									aeroflot.ru			185.69.81.												
31	ivo-ssc-aw.56133aa5-6	Approved				2021-01-11	2021-05-01	2021-01-11	2021-05-01									aeroflot.ru			80.92.39.1												
32	*.serguy.a.ae27cdac-6	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.82.												
33	*.romank.a.0ba5eef8-6	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.82.												
34	*.kirillh.aff.f6478b0-6	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.82.												
35	*.dev.aff.te.12aa33ae-6	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.82.												
36	*.aleks.aff.957b5d3c-6	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.82.												
37	*.aff-stagin.afcbbad8-6	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.83.												
38	*.aff-dev20.bafcfb7-d	Approved				2021-01-01	2021-05-01	2021-01-01	2021-05-01									aeroflot.ru			185.69.82.												
39	netstorage.9ad22051-6	Approved				2020-12-21	2021-05-01	2020-12-21	2021-05-01									aeroflot.ru	netstorage	edgekey.ne													
40	rim.aeroflot.58ab0956-6	Approved				2020-12-21	2021-05-01	2020-12-21	2021-05-01									aeroflot.ru			80.92.37.1												
41	mlk-ssc-aw.dd5c75a9-6	Approved				2020-12-21	2021-05-01	2020-12-21	2021-05-01									aeroflot.ru			80.92.36.8												
42	gw.aeroflot.d502f95-6	Approved				2020-12-01	2021-05-01	2020-12-01	2021-05-01									aeroflot.ru	gw.aeroflot	edgekey.ne													
43	travel-safe.4a67a059-6	Approved				2020-11-11	2021-05-01	2020-11-11	2021-05-01									aeroflot.ru			54.169.13.	Amazon Wi											
44	aac-aff-test.509a0e0b-6	Approved				2020-11-11	2021-05-01	2020-11-11	2021-05-01									aeroflot.ru	aff-test	edgekey.ne													
45	jenkins-m3.d84b08f4-6	Approved				2020-11-11	2021-05-01	2020-11-11	2021-05-01									aeroflot.ru			10.254.82.												
46	id-git.aff.te.6318bd40-6	Approved				2020-11-11	2021-05-01	2020-11-11	2021-05-01									aeroflot.ru			185.69.82.												
47	id-email.aff.74a3fa10-6	Approved				2020-11-11	2021-05-01	2020-11-11	2021-05-01									aeroflot.ru			185.69.82.												
48	dockerid.aff.d9d36e4c-6	Approved				2020-11-11	2021-05-01	2020-11-11	2021-05-01									aeroflot.ru			185.69.82.	Apache, Go											
49	aff-sfb-wco.57868f5d-6	Approved				2021-01-31	2021-05-01	2021-01-31	2021-05-01									aeroflot.ru			185.69.83.												

Preparing the data for MISP

- Importing the individual sheets of data (AS, Domain, IP_Block, IP_Address, Host, SSL_Cert, Contact)
- Enriching the attack surface inside of MISP
- Enriching the attack surface via API Calls to RiskIQ PassiveTotal

Sunburst Hunter Commands to enrich data

Usage

```
$ python RiskIQ.Sunburst.Hunter.py
```

All menu selections provide additional instruction.

File uploads require full path, unless file for upload resides in the running directory.

Otherwise just enter filename 'file.txt'

<https://www.riskiq.com/threat-hunting-resources/>

Under Other Resources

Download the RSALab zip file

<https://github.com/NoDataFound/RiskIQ.SunBurst.Hunter>



Account: rsalab-01@threattracking.com Password: RSARiskIQ1-01

What is MISP

MISP - Open-Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

- <https://www.misp-project.org/>
- We have created an instance that we will use in the labs
 - <https://rsalab.threattracking.com/>

<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Hosted MISP <https://rsalab.threattracking.com/>

- We have created accounts for everyone to use. An attack surface has already been loaded for you to use in the labs.
- Account information will be
 - **Account:** rsalab-01@threattracking.com
 - **Password:** RSAriskiq!1-01

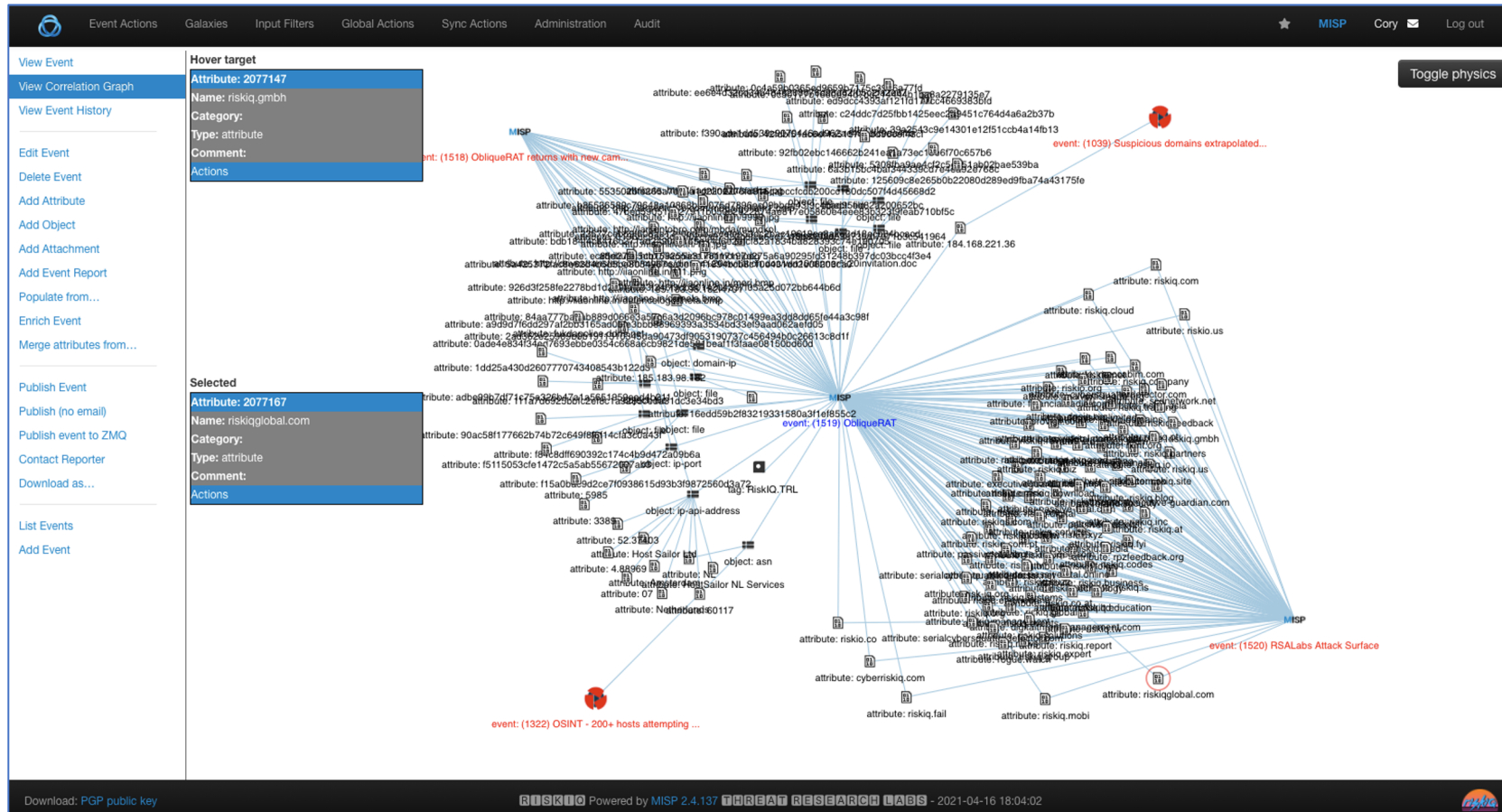
<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Hosted MISP <http://rsalab.threattracking.com>

- View Correlation Relationship Map to see your attack surface



<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSARiskiq11-01

29
Cory

RSAC Conference 2021

What Can I Do With My Attack Surface

(Red / Blue / Purple Teams)

- Is an OSINT article relevant to my organization?
- Do we have the vulnerability that was published OSINT article?

What Can I Do With My Attack Surface

(Red / Blue / Purple Teams)

Hands-on LAB

- Is an OSINT article relevant to my organization?
- Do we have the vulnerability that was published OSINT article?
- Tasks
 - Import 2 OSINT Articles
 - View Correlation Relationship Map

<https://www.fireeye.com/blog/threat-research/2020/05/analyzing-dark-crystal-rat-backdoor.html>

<https://community.riskiq.com/article/f990eb3b>

<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01



OSINT -> Attack Surface -> MISP -> Impact -> Action

RISKIQ Illuminate + Add Ons Profile

Threat Intel Portal / Exchange servers under siege from at least 10 APT groups

- Created about 1 month ago

Exchange servers under siege from at least 10 APT groups

Malware Microsoft ESET hafnium

Description Public Indicators (55)

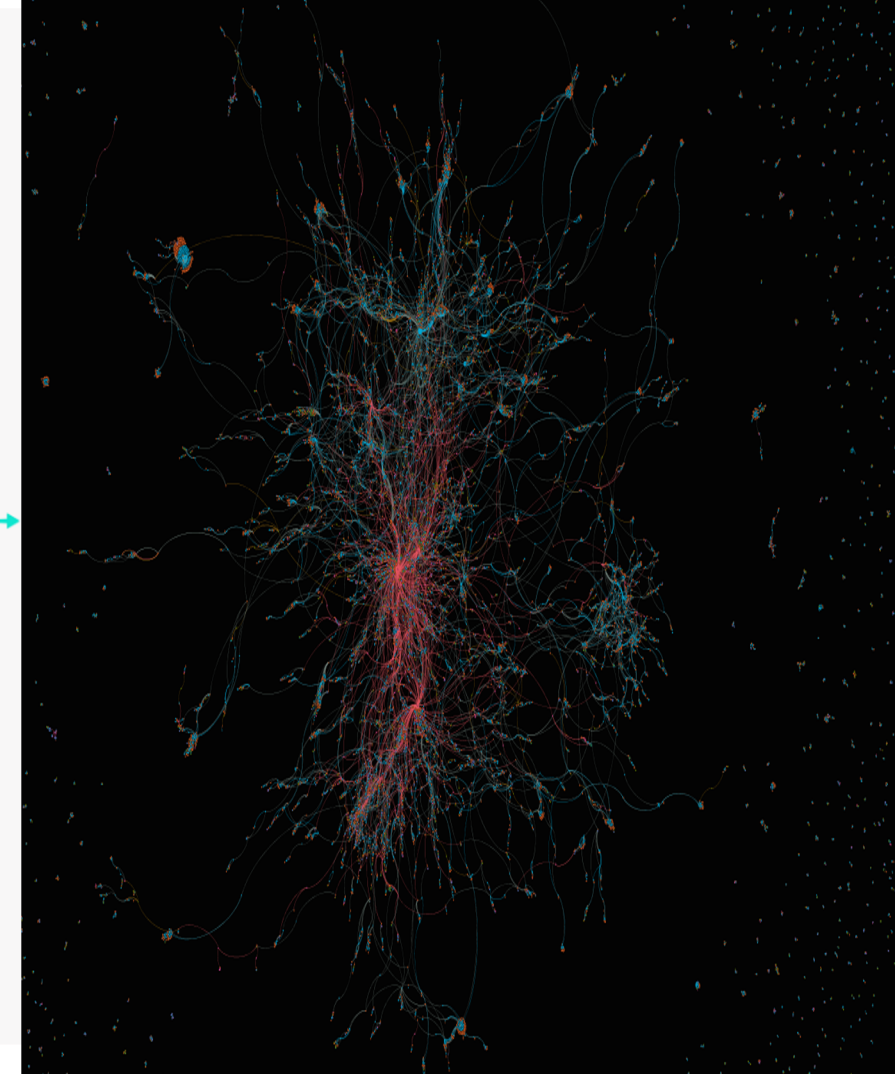
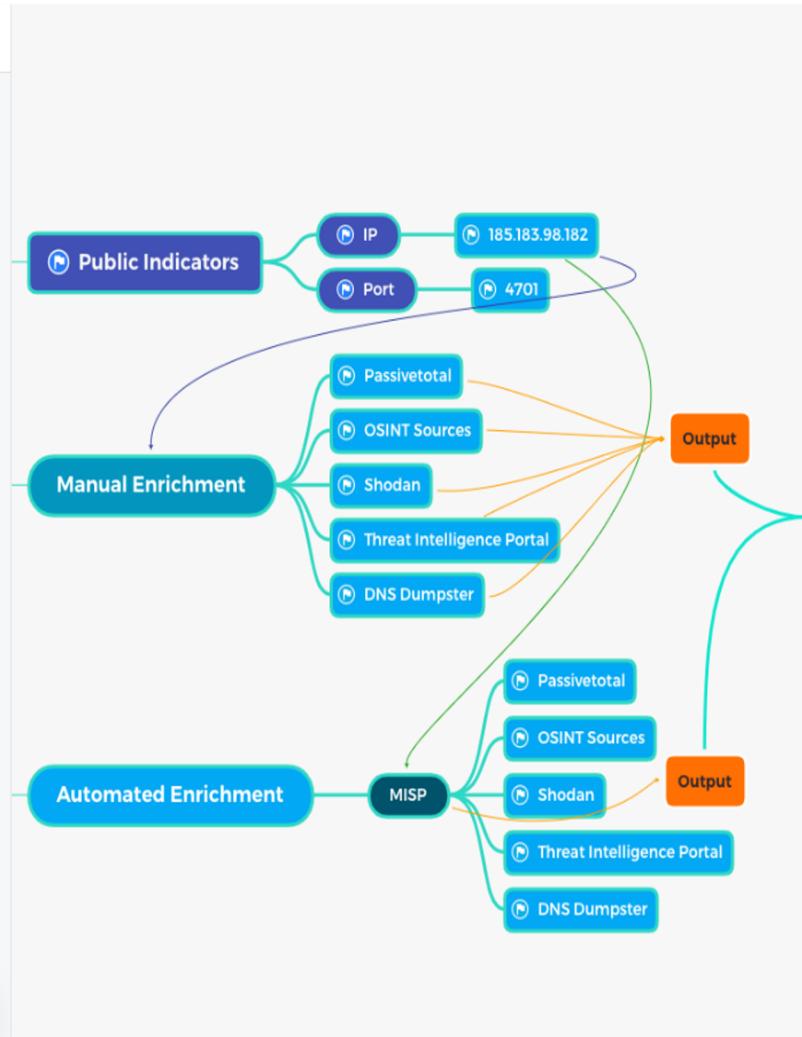
Description

On 2021-03-02, Microsoft released out-of-band patches for Microsoft Exchange Server 2013, 2016 and 2019. These security updates fixed a pre-authentication remote code execution (RCE) vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) that allows an attacker to take over any reachable Exchange server, without even knowing any valid account credentials. ESET has already detected webshells on more than 5,000 email servers as of the time of writing, and according to public sources, several important organizations, such as the European Banking Authority, suffered from this attack.

On 2021-02-28, ESET noticed that the vulnerabilities were used by other threat actors, starting with Tick and quickly joined by LuckyMouse, Calypso and the Winni Group. This suggests that multiple threat actors gained access to the details of the vulnerabilities before the release of the patch, which means we can discard the possibility that they built an exploit by reverse engineering Microsoft updates.

Reference URL(s)

- <https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/>
- <https://community.riskiq.com/article/6d6dc10b>



How Can Threat Hunters Leverage the Attack Surface

Hands-on Lab

<https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html>

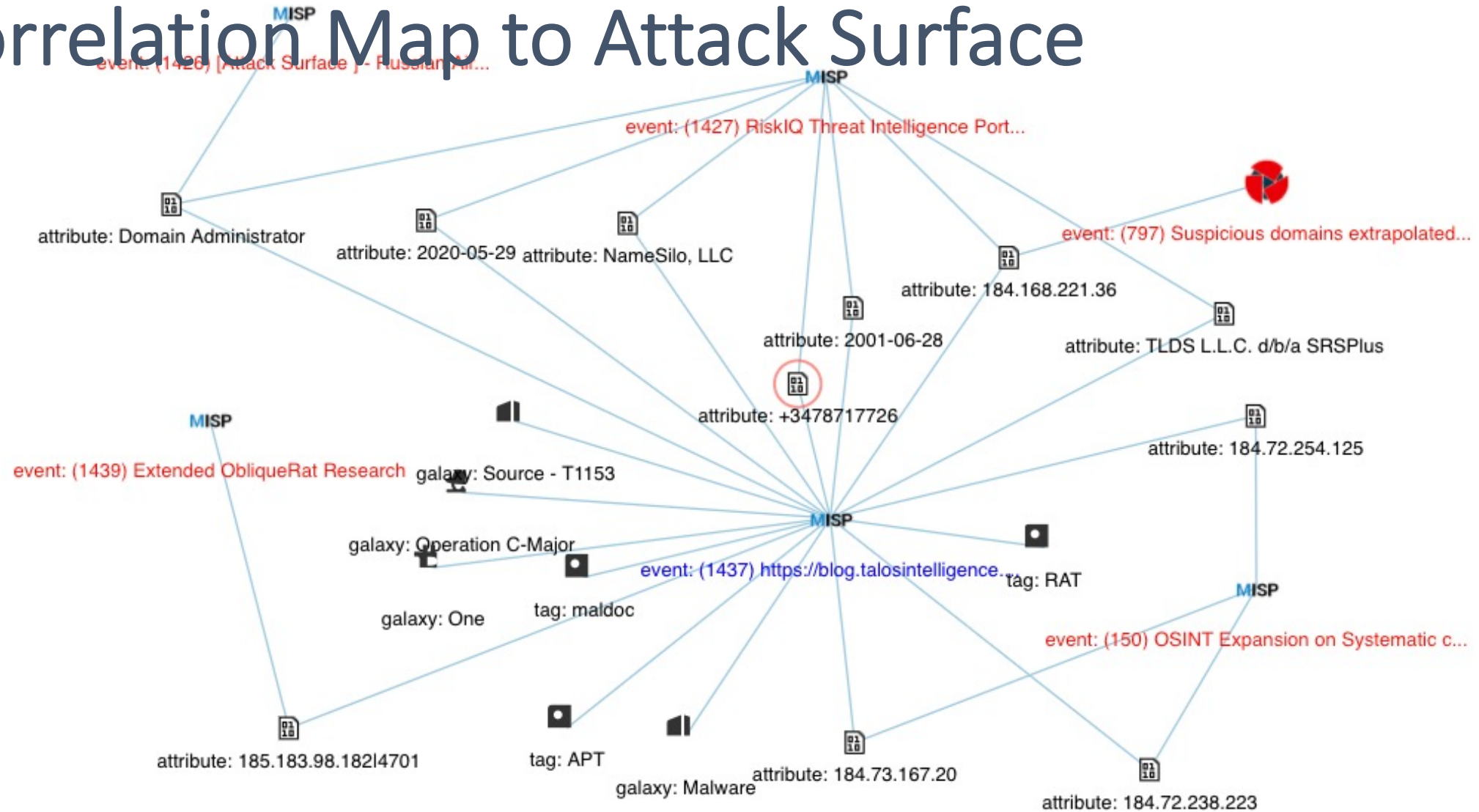
- Tasks
 - Import OSINT article indicators
 - View Correlation Relationship Map

<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Correlation Map to Attack Surface



<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq1-01

35
Cory

RSA®Conference2021

How Can Threat Hunters Leverage the Attack Surface

Hands-on Lab

<https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html>

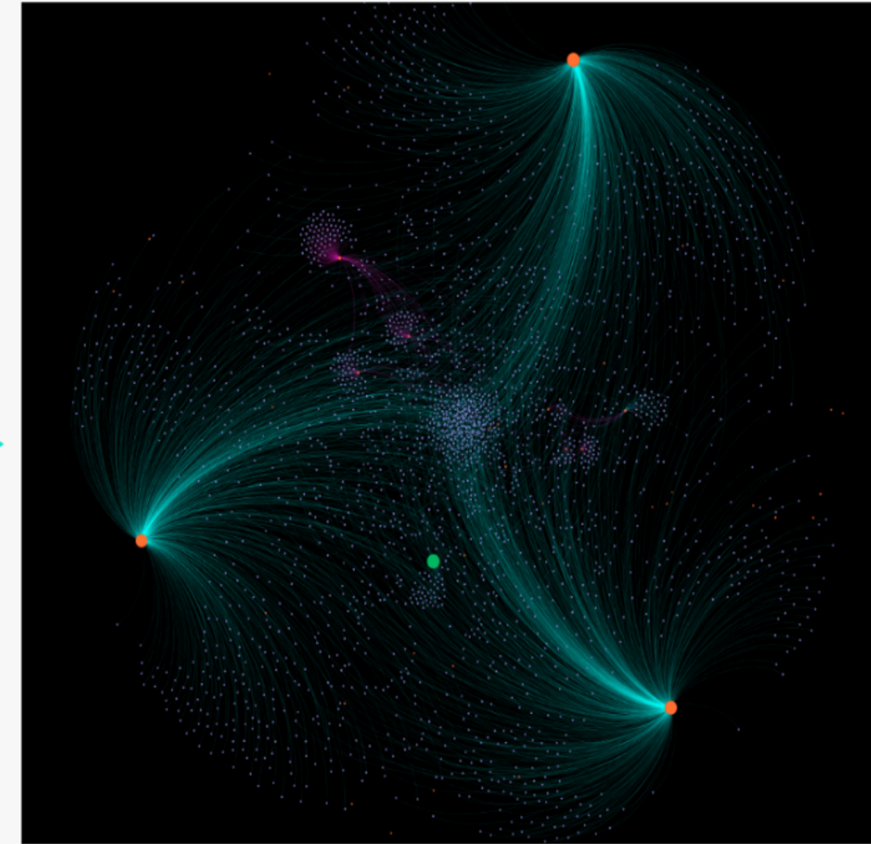
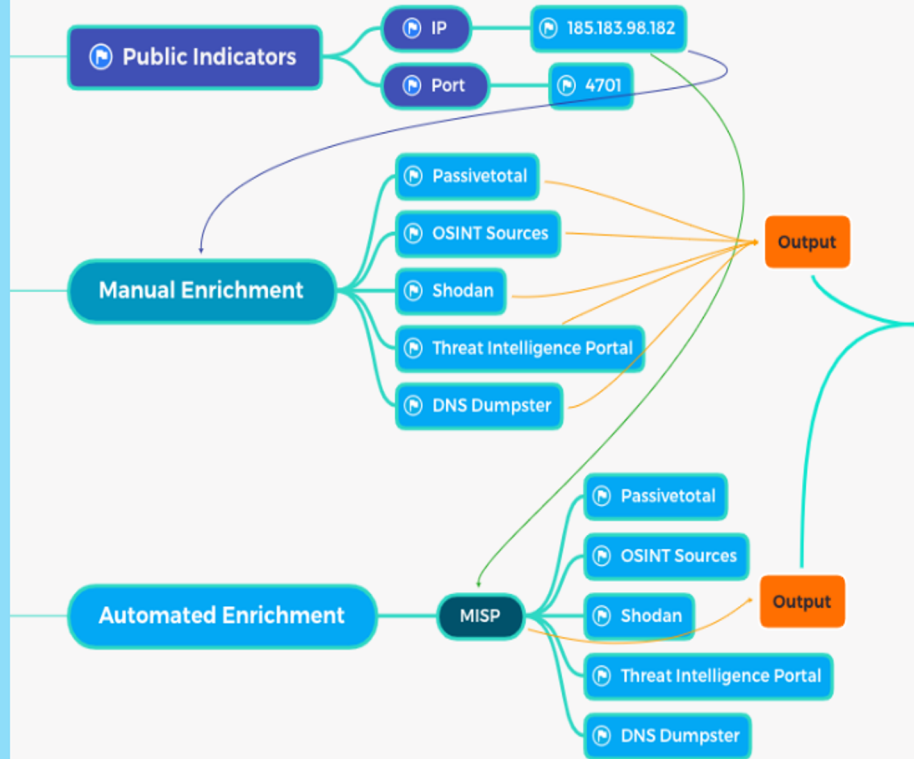
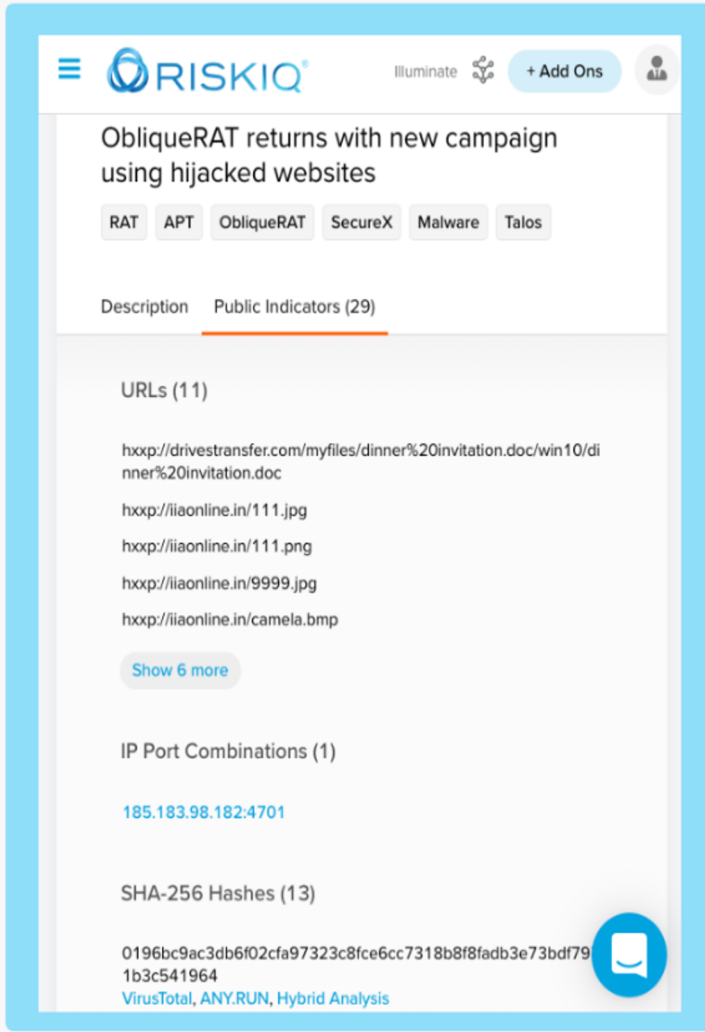
- Check Indicators in MISP
 - microsoft[.]ddns.net
 - yepp[.]ddns.net:4315
 - 185[.]183.98.182:4701
- Any hits on those indicators?

<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

How Can Threat Hunters Leverage the Attack Surface



Infrastructure Enumeration

<https://rsalab.threattracking.com/>

How Can Threat Hunters Leverage the Attack Surface

- Is that all?
- What is your next step as a Threat Hunter?
 - Find related infrastructure

<https://community.riskiq.com/search/185.183.98.182>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

PassiveTotal Investigation

- Hands-on Lab
- <https://community.riskiq.com>
 - Account: rsalab-01@threattracking.com
 - Password: RSAriskiq!1-01

Initial Search ObliqueRAT

<https://community.riskiq.com/article/f6ee031b/description>

<https://community.riskiq.com>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Search for IP address 185[.]183.98.182

The screenshot shows the RiskIQ search interface. At the top, the search bar contains the IP address 185.183.98.182. Below the search bar, there is a navigation bar with various filters and tabs. The main content area displays the search results, which are currently empty, showing a message "No Results Matching Your Query". The interface includes a sidebar with "ANALYST INSIGHTS" and "HEATMAP" sections. The bottom of the page features a "DATA" section with various filters and a "NEW" badge.

<https://community.riskiq.com/search/185.183.98.182>



Account: rsalab-01@threattracking.com Password: RSAriskiq1-01

40
Benjamin

RSA®Conference2021

Search for IP address 185[.]183.98.182

The screenshot shows the RiskIQ search interface. At the top, the search bar contains the IP address 185.183.98.182. Below the search bar, there are tabs for 'Query Results', 'ANALYST INSIGHTS', and 'HEATMAP'. The 'Query Results' tab is active, showing a table with columns for 'First Seen', 'Last Seen', 'ASN', 'Organization', 'Netblock', 'Country', 'Hosting Provider', 'Operating System', 'Routable', 'Host-Sailor', and 'Categorize'. The table shows one result for the IP address 185.183.98.182, which is associated with ASN AS60117 - HS, Organization Host Sailor Ltd, Netblock 185.183.98.0/24, Country NL, Hosting Provider, Operating System Windows, and is marked as 'Routable' and 'Host-Sailor'. Below the table, there is a section for 'DATA' with various filters like 'Resolutions', 'Whois', 'Certificates', 'Trackers', 'Components', 'Host Pairs', 'OSINT', 'Hashes', 'Reverse DNS', 'Projects', 'Cookies', 'CrowdStrike', 'Services', and 'Microsoft'. The 'DATA' section shows 'No Results Matching Your Query'.

Is the investigation over?

<https://community.riskiq.com/search/185.183.98.182>



Account: rsalab-01@threattracking.com Password: RSAriskiq1-01

41
Benjamin

RSA®Conference2021

Search for IP address 185[.]183.98.182

The screenshot shows the RiskIQ search interface for the IP address 185.183.98.182. The top navigation bar includes the RiskIQ logo, a search bar with the IP address, and various filters like 'First Seen', 'Last Seen', 'ASN', 'Organization', 'Netblock', 'Hosting Provider', 'Operating System', 'Routable', 'Host-Sailor', and 'Categorize'. The main content area is divided into sections: 'Query Results', 'ANALYST INSIGHTS' (with filters like 'Not Blocklisted', 'Not a Tor Exit Node', 'Open Port Last Detected 6 days ago', 'Not a Proxy', 'Infrastructure Routable', 'Hosts a Web Server'), 'HEATMAP' (with a message 'No Heatmap Data Available'), and 'DATA' (with a table of results). The 'DATA' section shows a table with columns for various categories and their counts. The bottom of the interface has a large text area with the question 'What is the paths forward in this investigation?' and a blue circular icon in the bottom right corner.

Query Results

ANALYST INSIGHTS

HEATMAP

DATA

What is the paths forward in this investigation?

<https://community.riskiq.com/search/185.183.98.182>



Account: rsalab-01@threattracking.com Password: RSAriskiq1-01

42
Benjamin

RSA®Conference2021

Search for IP address 185[.]183.98.182

RISKIQ Search: 185.183.98.182

First Seen: AS60117 - HS Netblock: 185.183.98.0/24 Host: 185.183.98.182 NL

Host: AS60117 - HS Host: AS60117 - HS Host: AS60117 - HS

Query Results

ANALYST INSIGHTS

Not Blocked Not a Tor Exit Node Open Port Last Detected 6 days ago Not a Proxy Infrastructure Routable Hosts a Web Server

HEATMAP

No Heatmap Data Available

DATA

Resolutions Whois Certificates Trackers Components Host Pairs OSINT Hashes Reverse DNS Projects Cookies CrowdStrike

CHANGE HISTORY

Current Record

2020-11-16

2020-11-11

2020-06-12

2020-06-01

2020-04-15

2019-06-14

CERTIFICATE

Current Record

SHA-1

Serial Number

Issued

Expires

Common Name

Alternative Names

Organization Name

SSL Version

Organization Unit

Street Address

Locality

State/Province

Country

Other Service

21 | TCP | Open

Response

Seen 42 Times | 2021-03-07 → 2021-04-14 | Last Scanned 2021-04-14

220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/

Windows Remote Desktop

3389 : Remote Access | TCP | Filtered

Response

Seen 826 Times | 2017-01-14 → 2021-04-14 | Last Scanned 2021-04-14



SYN / ACK HANDSHAKE ONLY

Services & SSL Certificates

<https://community.riskiq.com/search/185.183.98.182>



Account: rsalab-01@threattracking.com Password: RSAriskiq1-01

43
Benjamin

RSAC Conference 2021

Search for IP address 185[.]183.98.182

- What are the steps used to find related infrastructure?
 - SSL Certificates common issuer name
 - Historical IP address overlap
 - PDNS records on IP addresses that were found
- How can you speed up your investigation?
- How can you make the investigation easily repeatable?

<https://community.riskiq.com/search/185.183.98.182>



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Scaling Investigations with Scripts using APIs

Open your browser and visit the following URL

<https://www.riskiq.com/threat-hunting-resources/>

Under Other Resources

Download the RSALab zip file

Scaling Investigations with Scripts using APIs

Start Jupyter Notebook

Open Notebook file RSA-ObliqueRat

Credentials have been preloaded to make it easier for you to use.

These credential can be changed to use your own PassiveTotal API credentials once the class is over.

Scaling Investigations with Scripts using APIs

Now have a list of indicators with reputation scores
good, neutral, suspicious, and malicious

import all indicators that are suspicious and malicious back into MISP

How Can Threat Hunters Leverage the Attack Surface

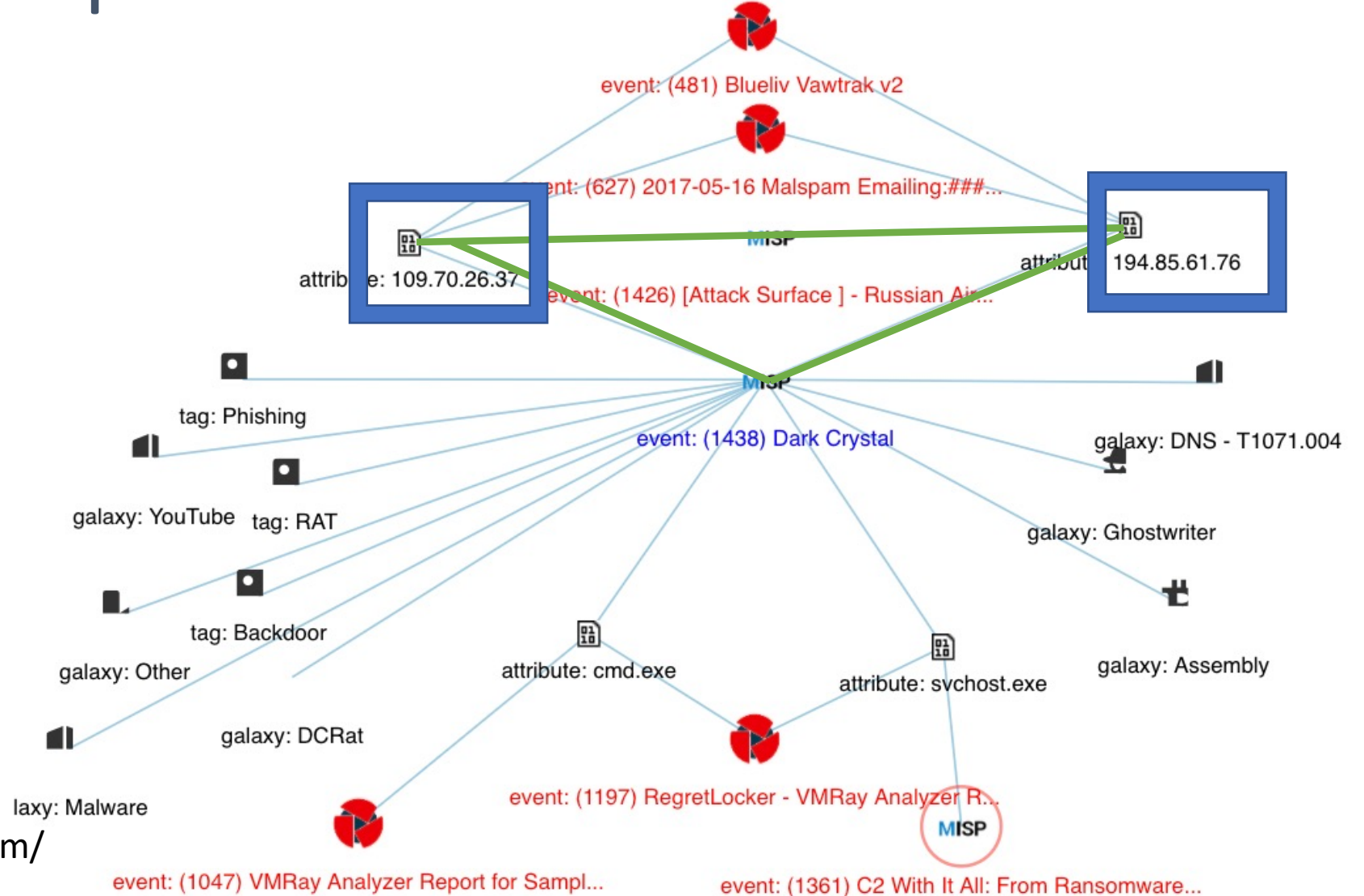
- Tasks
 - Import API suspicious and malicious indicators
 - View Correlation Relationship Map

Hosted MISP <http://rsalab.threattracking.com>. Account: rsalab-XX Password: RSAriskiq!1



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

Correlation Map to Attack Surface



<https://rsalab.threattracking.com/>



Account: rsalab-01@threattracking.com Password: RSAriskiq11-01

49
Cory

RSA®Conference2021

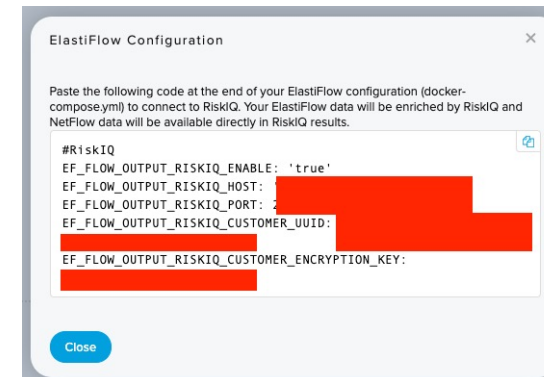
Improving Visibility in the Attack Surface Capabilities

- Flow Data – NetFlow, sFlow, IPFIX

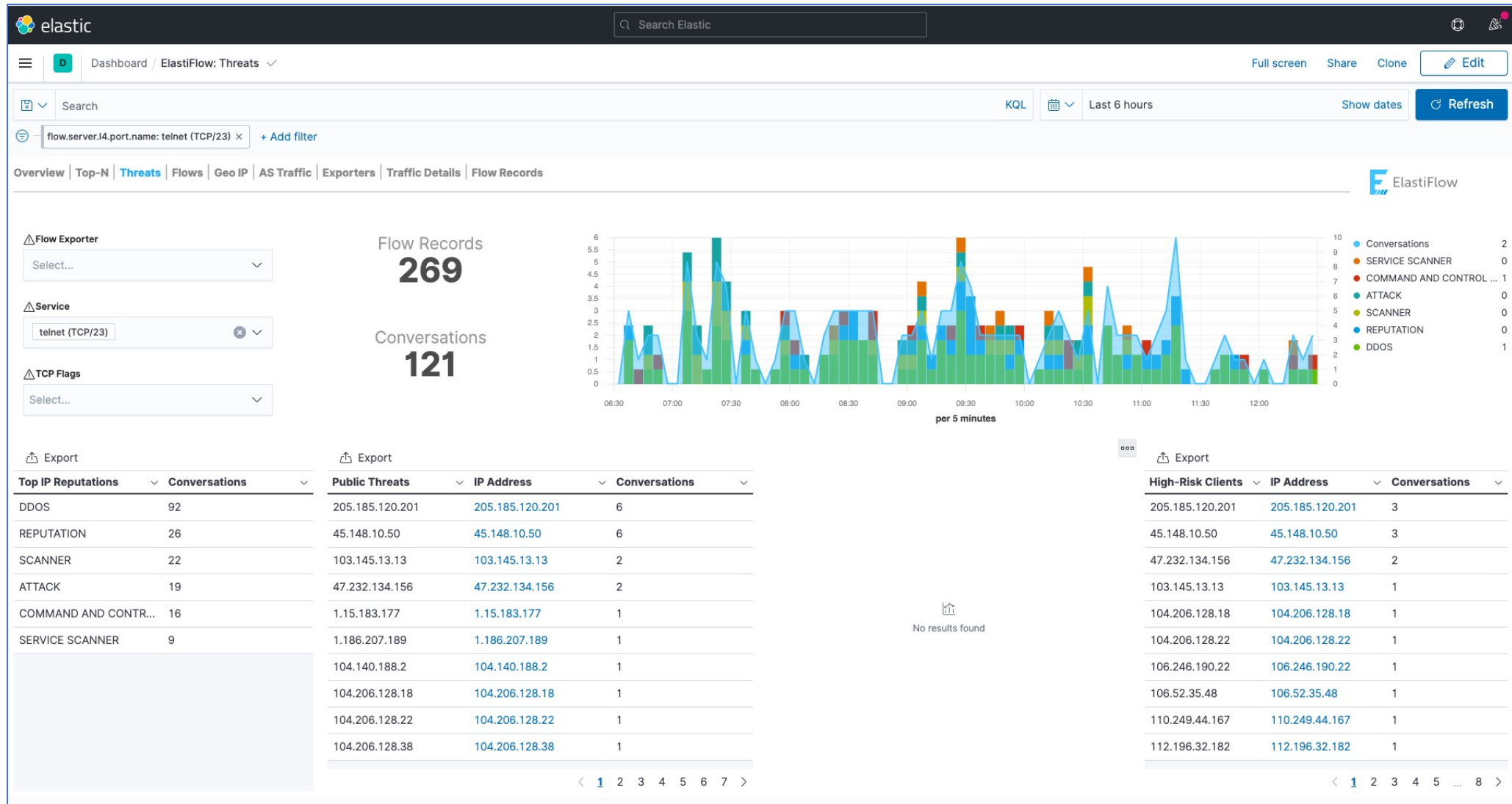
Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2010-09-01 00:00:00.459	0.000	UDP	127.0.0.1:24920	->	192.168.0.1:22126	1	46	1
2010-09-01 00:00:00.363	0.000	UDP	192.168.0.1:22126	->	127.0.0.1:24920	1	80	1

ElastiFlow – free and paid options available

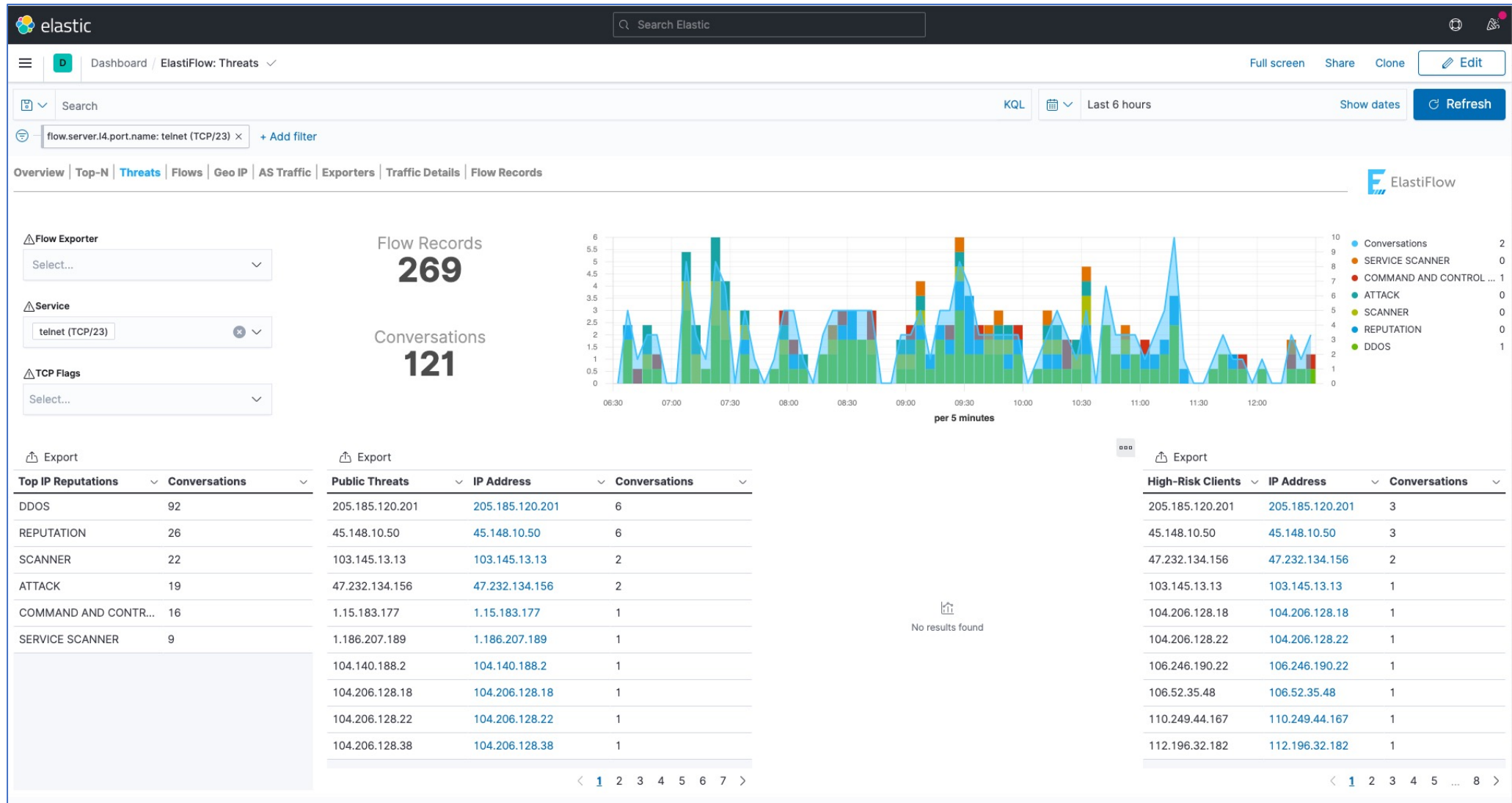
- Network Performance and Security Analytics for
 - <https://www.elastiflow.com>



Improving Attack Surface Capabilities



Elastiflow Quick Demo



Improving Attack Surface Capabilities

- We have already loaded flow data into MISP for you.
- Tasks
 - Do you see any traffic to or from the ObliqueRAT indicators?
 - View Correlation Relationship Map

Hosted MISP <http://rsalab.threattracking.com>. Account: rsalab-XX Password: RSAriskiq!1



Account: rsalab-01@threattracking.com Password: RSAriskiq!1-01

How can we leverage the external attack surface to enhance your investigations?

- Bridging the inside events and investigations with external sources and attack surfaces.
- Filtering OSINT with your own External Attack Surface to determine priorities and risks from exposures
- Filtering OSINT with your partners External Attack Surface to determine their risk and your potential exposures
- Leveraging threat actor's attack surfaces based upon TTPs and threat actor finger printing.
- Determining the overlap in Threat Actor's Attack Surfaces and your own attack surface.
- Overlaying the map of the internet with the traffic of the internet to determine targets, victims, and attackers.

Thank You