Threat Command, Kiberhírszerzés (CTI) platform a Rapid7-től

Foki Tamás, Clico Hungary

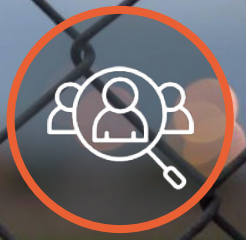
2022/10/18

No organization is immune to cyber attacks.

DIGITAL TRANSFORMATION

DELUGE OF DATA

NO PERIMETER



RESOURCE & SKILLS GAP

RAPID7

Manual IOC Creation

Multiple Departments

Phishing

Manual Monitoring

Fake Social Media

Trademark Infringement

Inefficient Remediation

Brand Impersonation

Slow Takedowns

Malicious Mobile Apps

Fraudulent Web Store

Fraudulent Rewards Accounts

Financial Fraud

Employee PII

Fraudulent Products For Sale

Attack Indication

Fraudulent Drugs

Bot Servers

Hacking Tools

Reactive Not Proactive

Third Party Ransomware

External Threats

Are Everywhere…

PII For Sale

VIP Targeting

Executive Targeting and Spoofing

Recruiting/HR scams

Open Ports

Expired SSL Certificates

Exploitable Data

Exposed Login Pages

DMARC / SPF Issues

Exposed API Keys

Credential Leakage

Confidential Documentation

Data Leakage

Leaked Customer Data

Exposed Code

Credit Card Leakage

Exposed Tokens

Clear Web

4% of Web Content
Search engine
Media, blogs, etc.

Deep Web

95% of Web content
Not searchable by most engines
Password protected content
Web mail, online banking and video on demand, corporate intranets, and subscription-based online news etc.

Dark Web

1% of Web content
Not searchable by most engines
Home to TOR, IRCs, BitTorrent, hacker forums, C2s, and more.

360° External Threat Protection

Single pane of glass for all your threat workflows

Entire threat lifecycle

Immediate time to value

Clear, deep and dark web

THREAT INTELLIGENCE

Threat Command

Minimize brand risk across the clear, deep, and dark webs.

USE CASES

- **Gain 360-degree external threat protection**
- **Automate instant responses within your environment**
- **Simplify threat workflows**
- **Save time and resources**

Get Immediate ROI

See results in as little as 24 hours.

Focus on Relevant Threats

Get alerts tailored to your unique digital properties.

Speed Response Across Your Environment

Block and automate across all security devices.

Cut Brand Exposure Time

Take advantage of best-in-class average takedown success rate of over 85% in under 24 hours.

CAPABILITIES

- External Threat Detection
- Clear, Deep and Dark Web Protection
- Alert Triage
- Investigation
- Threat Remediation
- Brand Protection

Simplify Workflows

Single, easily-accessible cloud-based platform for all threat workstreams

Built by/for security

Unlimited users

Multi-tenancy, MSSP ready

ALERTS

Rapid7 Threat Intelligence Demo | Tamas Foki Admin

Search: Search in alert title, description, URL, or ID

Status: 2 Statuses ×

Type: Phishing ×

Source Type | Flagged | Asset | More (10) | Clear Filters

Switch to Query | Export CSV

32	2	15	15
All	High	Medium	Low

- **Phishing Website Detected - 'https://rapld7.com'** — Jun 30, 2022 | 2:49 PM
- **Suspected Phishing Domain - 'rapiid7.com'** — Jun 30, 2022 | 2:49 PM — 3
- **Potential phishing email address detected - anonymoose@outlook.com** — Jun 30, 2022 | 2:42 PM — MITRE_T158... | MITRE_T159... | +2 tags
- **Suspected Phishing Domain - 'anonymooses.com'** — Apr 21, 2022 | 2:43 PM — Lowseverity... | MITRE_Buy d... | +5 tags
- **Suspected Phishing Domain - 'anonymoose.dev'** — Apr 21, 2022 | 1:49 PM — MITRE_Buy d... | Blocking Aler... | +4 tags

Phishing Website Detected - 'https://rapld7.com'

High

Alert ID: 62ac1d81ca89eed4ae9de8a5

Source URL: https://rapld7.com

Status: Open

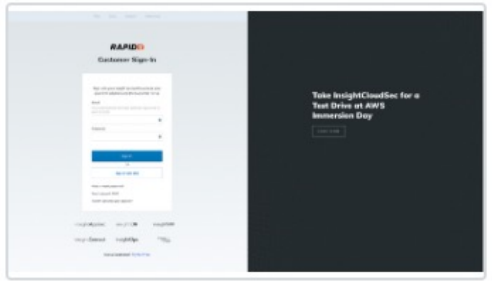
Last updated: Jun 30, 2022 | 2:49 PM

Source date: Jun 28, 2022 | 11:00 PM

unassigned | 0

Description

A phishing website was found. The site, purporting to be a company website, may be used to steal credentials from company employees or customers or distribute malware.



Recommendations

- To prevent your employees from being phished, block the website in your URL filtering system. You can do this by creating an internal remediation policy.
- To initiate the takedown process for this URL, click "Remediate".

Ask an Analyst | Remediate | Close Alert

Alert details

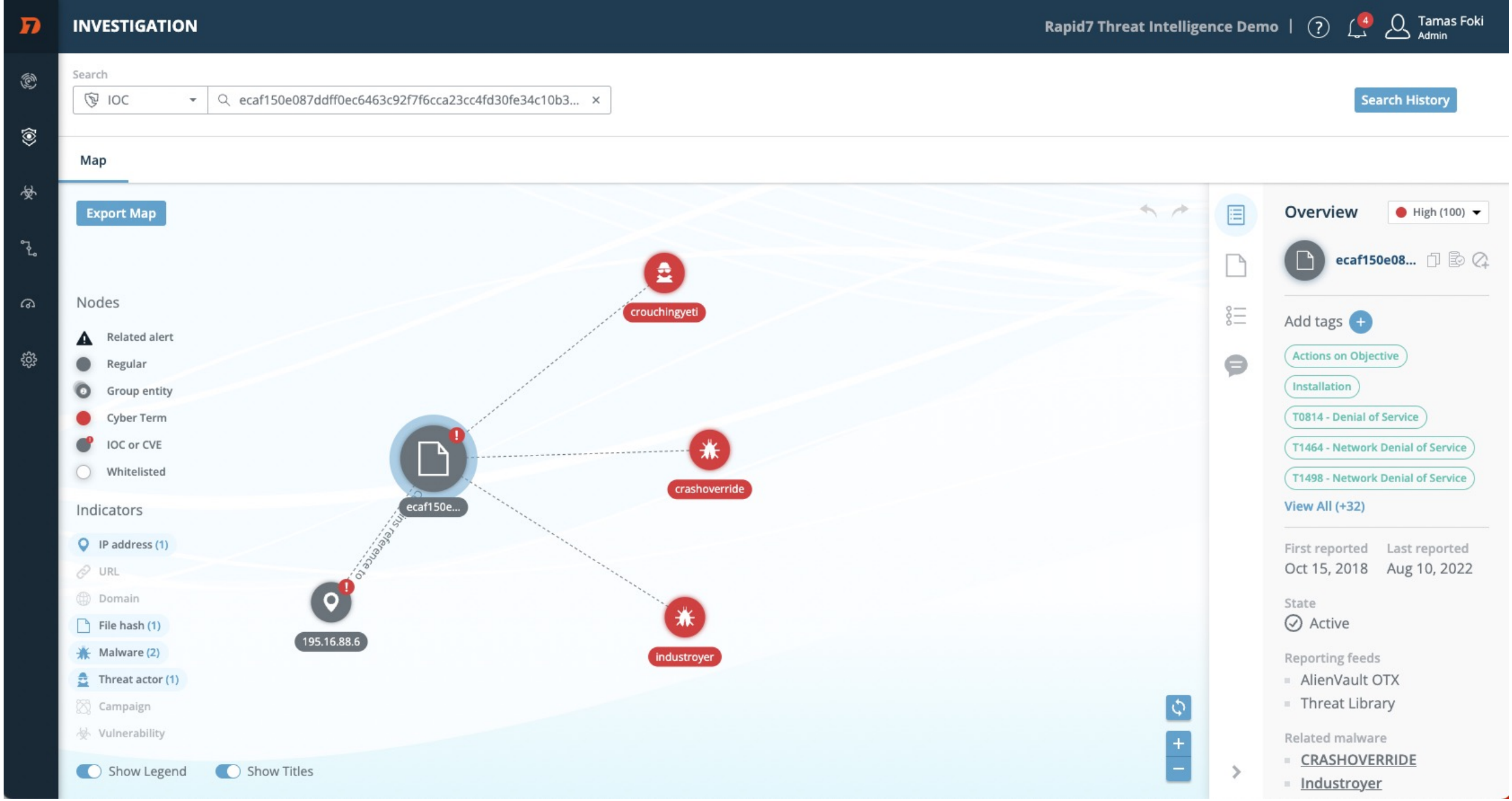
Source type
WHOIS servers

Network type
Clear Web

Report date
Jun 30, 2022 | 1:49 PM

Matched assets
- rapid7.com
- rapid7

Copy alert ID


INVESTIGATION
Rapid7 Threat Intelligence Demo |
Tamas Foki
Admin
Search
IOC
ecaf150e087ddff0ec6463c92f7f6cca23cc4fd30fe34c10b3...
Search History
Map
Export Map
Nodes
Related alert
Regular
Group entity
Cyber Term
IOC or CVE
Whitelisted
Indicators
IP address (1)
URL
Domain
File hash (1)
Malware (2)
Threat actor (1)
Campaign
Vulnerability
Show Legend
Show Titles
crouchingyeti
ecaf150e...
crashoverride
195.16.88.6
industroyer
Overview
High (100)
ecaf150e08...
Add tags
Actions on Objective
Installation
T0814 - Denial of Service
T1464 - Network Denial of Service
T1498 - Network Denial of Service
View All (+32)
First reported
Oct 15, 2018
Last reported
Aug 10, 2022
State
Active
Reporting feeds
AlienVault OTX
Threat Library
Related malware
CRASHOVERRIDE
Industroyer

Accelerate Response

Plug and play with existing security devices

Threat Command takes the complexity out of threat intelligence delivering instant value

REDUCE NOISE; PRIORITIZE RELEVANT THREATS

SPEED RESPONSE ACROSS ENVIRONMENT

DO MORE WITH LESS INVESTMENT

SIMPLIFY SECOPS WORKFLOWS

Köszönöm a figyelmet!

Email rapid7@clico.hu vagy tamas.foki@clico.hu