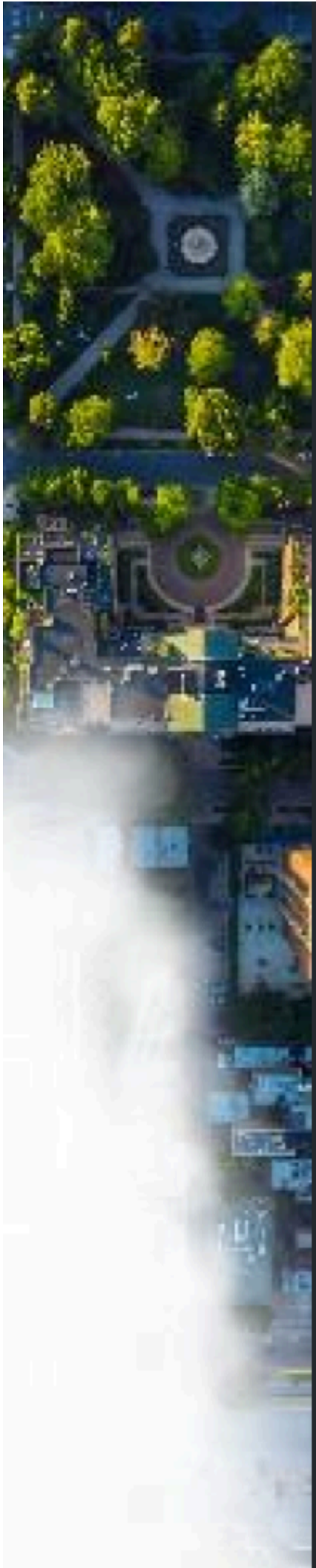


RAPID7

Threat Intelligence Research Catalog

Research Overview

Rapid7 offers deep-dive investigation services and reports into external cyber threats as an auxiliary service to Threat Command. This service includes data breach investigations and strategic trend-based research.

This catalog describes our standard menu of research offerings, general details about the research procedure, typical deliverables, and pricing information.

The Research Process

You can create a case to request a Threat Command research through the Rapid7 customer portal.
Once the request is received, the Research Team will contact you to get more information or respond with approval and its ETA.

VIP reports

VIP reports focus on the exposure of the assets and digital footprint of key people in an organization (VIP CEO, COO, CFO, HR, IT Manager). It provides an overview of the various potential threats related to the exposure of these professional and personal assets.

A VIP report includes:

- A deep investigation with a digital footprint assessment of the individual in question
- An overview of the VIP's vulnerabilities/exposure to risk
- Information about tactics cybercriminals use to attack executives and VIPs and how to identify and validate threats
- Solutions and tactics for proactively defending against executive threats

Deliverable: PDF Report

Company Landscape Research

Sector/landscape reports focus on a particular industry (For example: Finance, Telecom, Energy, Manufacturing, Automotive, Retail) and its cyber threat landscape. A sector/landscape report provides an overview of the different threats that the industry faces as well as cyber risks.

Business sector reports include:

- Recent cyber events in the sector globally and locally
- Top threat actors targeting the sector
- Top malware being used against the sector
- Active chatter regarding the sector
- Recommendations

Deliverable: PDF Report

Data Breach Reports

A data breach is an incident where information is stolen from a system without the knowledge or authorization of the system owner.

Ransomware Attacks - General Information

Rapid7 can provide you with general information about ransomware and the threat actors using it. A ransomware attack report includes an in-depth.

investigation of the attack through the analysis of:

- Email and Bitcoin addresses used by the threat actor
- Ransomware group sites/background/attacks/TTP
- Scans of underground hacking forums
- IOC & Recommendations (if available)

Requested information:

- Ransom message
- Threat actor's email address
- Threat actor's Bitcoin address
- Encrypted file extension type

Deliverable: PDF Report

Insider Threat

An insider threat typically refers to employees who use their position and access to networks to extract confidential information from their own organization. Malicious insiders often cooperate with external threat actors to provide them with initial access and confidential

information. An insider threat report includes:

- In-depth analysis of underground hacking and data breach forums to identify if the data is published or for sale
- Investigation into known threat actors that may be associated with the insider
- Analysis of internal logs (if provided)

Requested information:

- Internal logs (if possible)
- Suspicious employee contact information (name, email address, phone number)
- Any suspicious correspondence that was found on the company systems (email, phone, etc.)

Deliverable: PDF Report

Malware Enrichment

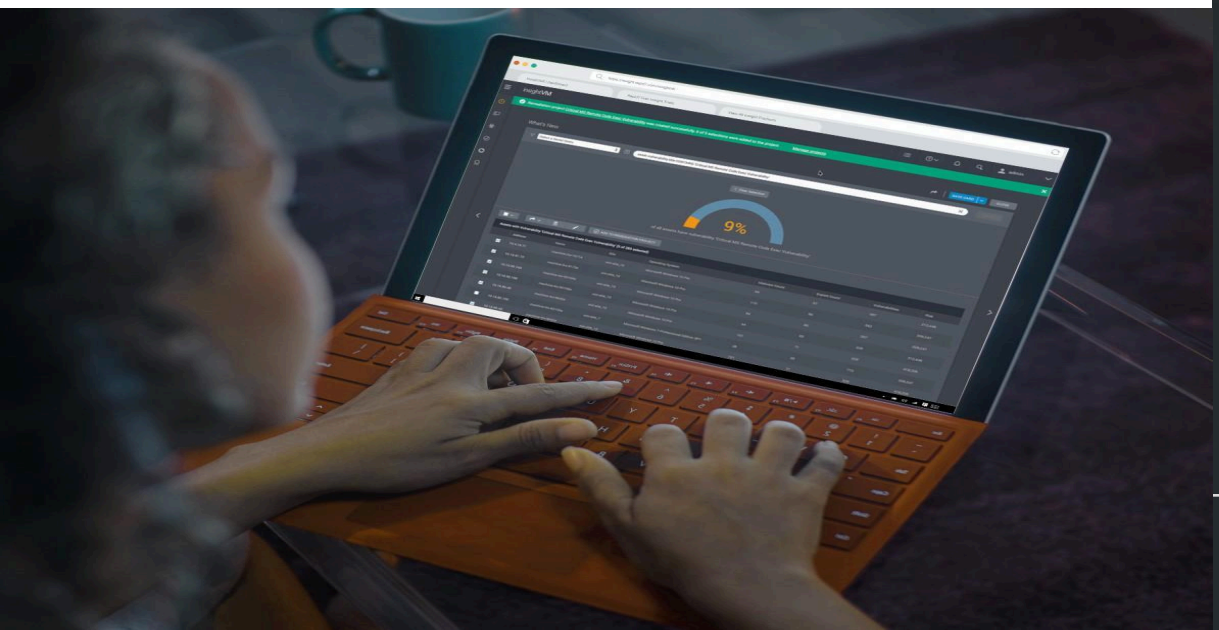
A malware enrichment report related to a data breach includes an in-depth investigation into:

- The type of malware used for the attack (remote access Trojan, log stealer, etc.)
- The modus operandi of the malware and its indicators of compromise (IOC)
- The threat actors operating, using, or selling the malware on the dark web

Requested information:

- Attack vector information (email, download link)
- IOC (IP, hash, email)

Deliverable: PDF Report



Phishing Reports

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

Phishing Investigation - Email/Smishing/Vishing

An investigation of the email addresses/phone numbers/SMS used to perform the phishing attack, including:

- Email/SMS message content analysis
- A deep scan of the email address and phone number on the dark web and on
- Rapid7's internal databases
- Analysis of IP addresses/servers related to the phishing email address/phone number and whether it was used for specific campaigns

Requested information:

- Email addresses and header used by the threat actor
- Suspicious phone numbers
- IP addresses
- URL of the phishing and screenshots

Deliverable: PDF Report

Domain/URL Phishing Investigation

An investigation of up to 5 domains/URL addresses used to perform the phishing attack, including:

- Research on the dark web and Rapid7's internal databases
- A deep check of the hosting service and IP addresses related to the domains/URL (C&C and drop servers, etc.)
- Research on related domains that link to the same campaign
- The phishing infrastructure

Requested information:

- Email addresses and header used by the threat actor
- IP addresses
- URL of the phishing and screenshots

Deliverable: PDF Report

Business Email Compromise (BEC)

A business email compromise (BEC) is a type of scam in which an attacker obtains access to a business email account and impersonates its owner. Typically, the goal of a BEC is to defraud the company and its employees, customers, or partners.
A BEC investigation
includes:

- Analysis of messages and the included artifacts for any anomalies and insights
- Analysis of the IP address related to the email address to identify if it is part of blocklists from previous incidents and determine the geolocation of attackers
- Examples of similar campaigns that were observed in the past

Requested information:

- Email addresses and header used by the threat actor
- Content of messages
- IP addresses

Deliverable: PDF Report

Employment Scams

An employment scam is an attack aimed at deceiving job seekers by giving them false hopes of obtaining a better position. In this type of attack, threat actors aim to get as much information as possible about the victim. In some cases, they might also attempt to extort money from victims.
An employment scam investigation includes:

- An analysis and profiling of the threat actor and the campaign launched against the company
- Deep research on forums, messaging applications, etc., to identify whether other organizations were targeted by the same method/threat actor/campaign
- Remediation advice/process (if available)

Requested information:

- Content of the message
- Email addresses and header used by the threat actor

Deliverable: PDF Report

Impersonation Fraud

Impersonation fraud is a type of attack that involves stealing the identity of a CEO or high-level executive to extort money from a victim (for example, a supplier or customer).
An impersonation fraud investigation includes:

- Investigating the email message/profile that impersonates the VIP, and its content
- Investigating the origin of the sender/creator of the profile and trying to understand their motives
- Deep research on the deep and dark web to find any chatter regarding the impersonation of the company VIPs

Requested information:

- Email addresses and header used by the threat actor
- Name of the VIP

Deliverable: PDF Report

OSINT/HUMINT Reports

OSINT:

Open-source intelligence is a passive process of intelligence gathering.
This includes collecting and analyzing data obtained from open and publicly available sources to produce actionable intelligence.

HUMINT:

Virtual Human Intelligence is an active part of the intelligence collection process.
HUMINT allows users to interact directly and privately with different types of threat actors through the use of avatars and various social networks, forums, marketplaces, and messaging platforms. HUMINT provides valuable information about the threat actors' malicious activities and TTP.

Threat Actor Research

Threat Actor research includes the following:

- Investigation of online presence (forums, social networks, messaging platforms, etc.)
- Profile investigation (nicknames used on the different platforms, reputation, geolocation/country of origin, technical skills, and communication assets)
- Tactics, Techniques, and Procedures (TTP) research (attack vectors and commonly Used tools)

Requested information (might not apply for known threat actors):

- Threat actor nickname
- Threat actor's email address or any communication

Deliverable: PDF Report

Deep and Dark Web Threat Hunting Research

Dark and deep web hunting is a general investigation that includes the collection and analysis of data from public open sources to produce actionable intelligence. A deep and dark web threat hunting report includes:

- A deep check on sources, including forums, marketplaces, and messaging applications within the deep and dark web to identify potential threats targeting your organization based on specific demands

Deliverable: PDF Report

Pricing

Report Type	Report	Price
Executive Exposure	VIP	1
Company Landscape	Threat Landscape	2
Data Breach	Ransomware Attack General Information	1
	Insider Threat	1
	Malware Enrichment	1
Phishing	Phishing Investigation - Email/Smishing/Vishing	1
	Domain/URL Phishing Investigation	1
	Business Email Compromise (BEC)	1
	Employment Scams	1
	Impersonation Fraud	1
OSINT/ HUMINT	Threat Actor Research	1
	Deep and Dark Web Threat Hunting Research	1

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attack methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security XDR & SIEM

Threat Intelligence Vulnerability Risk Management

Application Security Orchestration & Automation Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/