

Recorded Future Alerts v1.5.1 - Anomali ThreatStream Installation Guide

- [Application Description](#)
- [Application Functionality](#)
 - [Recorded Future Classic Alerts](#)
 - [Recorded Future Playbook Alerts](#)
 - [Cyber Vulnerability](#)
 - [Affected Products](#)
 - [Data Leakage on Code Repository](#)
 - [Domain Abuse](#)
 - [Third Party Risk](#)
 - [Identity Novel Exposures](#)
 - [Malware Report \(Malware Intelligence\)](#)
 - [Updates](#)
 - [Observables](#)
 - [Confidence](#)
- [Installation](#)
 - [Configuration](#)
- [Tags](#)
- [Troubleshooting](#)
 - [Missing Observables](#)
 - [Not fetching alerts](#)
 - [Custom Alerts \(created with AQB\) not ingesting](#)
 - [IOC with 0 risk score and no Intelligence Card](#)
- [CHANGELOG](#)

Application Description

Recorded Future is continuously harvesting data from Open, Deep, and Dark Web sources in real-time including Social media, Forums, Blogs, IRC channels, Paste sites, email groups, onion sites via TOR, and more through a range of collection mechanisms. Thousands of sources are added to our index for customers each week and are currently mining and cross-correlating data from over 750,000+ sources in seven languages with a patented Temporal Analytics™ Engine.

The Recorded Future Alert Feed for Anomali ThreatStream enables:

- Delivery of Recorded Future Alert details consumed in Anomali ThreatStream (TS) as Incidents via an Anomali TS Feed.
- Triaging Recorded Future Classic Alerts and Playbook Alerts with the full alert details context directly in the Anomali TS.
- Review trending Intelligence Goals Library (IGL) data.
- Ability to document historical credential leaks.

The Recorded Future Alert Feed for Anomali TS enables better alert triaging by adding relevant and comprehensive context.

Application Functionality

Recorded Future Alerts application's functionality is underpinned by the Recorded Future API, which is the repository from which Anomali TS retrieves the Recorded Future Classic Alerts and Playbook Alerts. The Feed fetches alert details and feeds them to Anomali TS as Incidents. This makes the alert context ready for triaging within Anomali TS.

Alerts ingested by the **Recorded Future Alerts Feed** can be found in the **Thread Model** view as shown below:

The screenshot shows the 'Threat Model' interface. On the left is a 'Filter Options' sidebar with categories like 'Filter' and 'Key Filters'. The main area displays a search bar and a table of 4204 results. The table has columns for 'TYPE', 'NAME', 'DATE PUBLISHED', 'TAGS', and 'SOURCE'. The first row is expanded to show 'TAGS' including 'alert-id:task-426fb575-c8e3-4226-a7a4-0a67c3a5c546', 'organisation:Professional-Services-Development', 'owner-name:Professional-Services-Development', 'priority:High', and 'recorded-future-playbook-alert'. Other rows in the table include incidents like 'Data Leakage on Code Repository - Splunk', 'Domain Abuse - yuehln.com', and 'Data Leakage on Code Repository - Palo Alto Networks Inc.'.

Recorded Future Alerts in Threat Model View

Recorded Future Classic Alerts

The following classic alerts are supported:

- Intelligence Goal Library (IGL) Alerts
- Custom Alerts

Every Incident created from a Recorded Future Classic Alert contains:

- Tags
- Link to the [Recorded Future Platform](#) for further analysis
- Alert Trigger time
- Alert references tables

- Reason for reference inclusion in alert (Triggered by)
- Recorded Future AI Insights

Threat Models List / Incident Detail /

Potential Logo Abuse Detection: 3x4VIO

Export Actions

Recorded Future

PUBLICATION STATUS
Published

PUBLISHED DATE
27 Feb 2025 10:06

TLP
Red

Watch | 0 Star | 0 Views | 0

Share

TAGS
Visibility
My Organization

E.g., First Tag, Second Tag

alert-id:3x4VIO

organisation:Professional-Services-Development

owner-name:None recorded-future-alert

rule-name:Potential-Logo-Abuse-Detection

source:Logotype-Detection

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
Add Intelligence Initiative

FEED
Recorded Future Alerts - Test

SOURCE CREATED
27 Feb 2025 06:04

Description Associations (50) Investigations (0) Attachments (0) Notes History

Potential Logo Abuse Detection

Summary

ID: 3x4VIO
Triggered: 2025-02-27 06:04:29
Alerting Rule: Potential Logo Abuse Detection
API | Portal

AI Insights

Comment: The Recorded Future AI requires more references in order to produce a summary.

References

- 1. From Logotype Detection**
Title: Recorded Future Logotype Detection on <https://cantho.arobistyle.com/2022/03/ao-khoac-vest-nam-can-tho.html>
The logotypes Facebook, WhatsApp have been detected in a screenshot taken on the page <https://cantho.arobistyle.com/2022/03/ao-khoac-vest-nam-can-tho.html>
Triggered By (Click to expand)
 - Facebook (Logotype) → Facebook (Company) → Brand Names Watch List (EntityList)
 - WhatsApp (Logotype) → WhatsApp Inc. (Company) → Facebook (Company) → Brand Names Watch List (EntityList)
- 2. From Logotype Detection**
Title: Recorded Future Logotype Detection on <https://liebeshop.dk/collections/hjemmet-1?page=4>
The logotypes Facebook, Instagram, YouTube, Pinterest have been detected in a screenshot taken on the page <https://liebeshop.dk/collections/hjemmet-1?page=4>
Triggered By (Click to expand)
- 3. From Logotype Detection**
Title: Recorded Future Logotype Detection on <https://dongsolar.co.ke/power-banks/57-marstek-1000w-powerstation.html>
The logotypes Facebook, Twitter, Mastercard, Visa, Bharti Airtel have been detected in a screenshot taken on the page <https://dongsolar.co.ke/power-banks/57-marstek-1000w-powerstation.html>
Triggered By (Click to expand)

Classic Alert: Potential Logo Abuse Detection

Recorded Future Playbook Alerts

The following playbook alerts are supported:

- Cyber Vulnerability
- Data Leakage on Code Repository
- Domain Abuse
- Identity Novel Exposures
- Third Party Risk
- Malware Report

Cyber Vulnerability

The Cyber Vulnerability Playbook Alerts utilise the **Vulnerability** Threat Model and can be found by selecting **Vulnerabilities** from the **Filter Options** in the **Threat Model** page.

The screenshot shows the 'Threat Model' interface. On the left is a 'Filter Options' sidebar with a 'Filter' section containing various categories like 'All', 'Actors', 'Attack Patterns', etc., and 'Vulnerabilities' is selected. The main area has a search bar and a table of 'Z1 Results'. The table has columns for 'TYPE', 'NAME', 'DATE PUBLISHED', 'TAGS', and 'SOURCE'. The first row is expanded, showing details for a 'Cyber Vulnerability' with a specific CVE ID and associated tags like 'lifecycle:Exploit-Likely' and 'risk-rule:Exploit-Likely-in-Active-Development'. The source is 'Recorded Future Alerts'.

Cyber Vulnerability Playbook Alerts as Vulnerabilities in Threat Model View

The Cyber Vulnerability Playbook Alerts contains:

- Recorded Future AI Insights for the reported vulnerability
- Summary of the vulnerability
- CVSS v2 and CVSS v3 score and additional context (if applicable)
- Insikt Notes (if applicable)
- Affected products list
- Tags:
 - **lifecycle** to indicate the exploitability of the vulnerability
 - **risk-rule** indicating which [Recorded Future Risk Rules](#) the vulnerability has matched





PUBLICATION STATUS
Published

PUBLISHED DATE
24 Oct 2025 11:22

TLP ⓘ
Red

Watch | 0 Star | 0 Views | 0

Like | 0 Comment | 0 Share

TAGS
Visibility

My Organization

E.g., First Tag, Second Tag

alert-id:task:06071981-5830-4819-a36f-029f9043f271 x

lifecycle:Exploited x

organisation:Professional-Services-Development x

priority:High x recorded-future-playbook-alert x

risk-rule:Exploited-in-the-Wild-by-Recently-Active... x

risk-rule:Recently-Reported-by-Insikt-Group x

rule-name:Cyber-Vulnerability x

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

FEED
Recorded Future Alerts - Test

SOURCE CREATED
15 Oct 2025 02:11

SOURCE MODIFIED
15 Oct 2025 02:11

<
Description
Associations (0)
Investigations (0)
Attachments (1)
Notes
Histo >

Cyber Vulnerability

Summary

ID: task:06071981-5830-4819-a36f-029f9043f271
Created: 2025-10-15 01:11:09
Updated: 2025-10-15 01:11:09
Status: New
Priority: High
[API](#) | [Portal](#)

Recorded Future AI Insights

CVE-2025-47827 is a critical vulnerability affecting IGEL OS 10 that allows a full Secure Boot bypass, potentially enabling untrusted kernels and rootkits to be executed. It has been highlighted in multiple reports across platforms like Discord and GitHub, indicating its relevance in the cybersecurity community. The vulnerability poses significant risks for Linux administrators by exposing them to exploitation due to compromised security in the shim layer signed by Microsoft, making it easier for attackers to gain unauthorized access. Given its severe implications and the presence of proof-of-concept (PoC) exploits, you should prioritize patching this vulnerability immediately to protect your company's assets from potential attacks that could exploit this flaw.

Vulnerability Overview

Name: CVE-2025-47827
Risk Score: 99
Matches in Watch List (7): Microsoft Windows Server 2019, Microsoft Windows 10, Microsoft, Microsoft Windows Server 2012, Microsoft Windows Server 2016, Microsoft Windows, Microsoft Windows Server 2012 R2
Criticality: Very Critical
Lifecycle: Exploited
CVSS v3

- **Attack Complexity:** HIGH
- **Attack Vector:** LOCAL
- **Availability Impact:** LOW
- **Base Score:** 4.5
- **Base Severity:** Medium
- **Confidentiality Impact:** LOW
- **Created:** 2025-06-05 15:40:14
- **Exploitability Score:** 1.0
- **Impact Score:** 3.4
- **Integrity Impact:** LOW
- **Modified:** 2025-06-05 15:40:14
- **Privileges Required:** LOW
- **Scope:** UNCHANGED
- **User Interaction:** NONE
- **Vector String:** CVSS:3.1/AV:L/AC:H/PP:L/AU:N/S:U/C:L/AI:JAH

Playbook Alert: Cyber Vulnerability

Affected Products

A copy of **Affected Products** list can also be found in the **Attachments** tab and is available for download.





PUBLICATION STATUS
Published

PUBLISHED DATE
27 Oct 2023 09:50

TLP 
Red

Description	Associations (0)	Investigations (0)	Attachments (1)	History
1 Results				
TITLE	URL/FILENAME			
CVE-2023-35359_affected_products.csv	CVE-2023-35359_affected_products.csv			

Affected Products attachment

Data Leakage on Code Repository

The Data Leakage on Code Repository Playbook Alerts utilise the **Incident** Threat Model and can be found by selecting the **Incidents** from the **Filter Options** in the **Threat Model** page.

The Data Leakage on Code Repository Playbook Alerts contains:

- Targets related to the leaked data
- Repository where the leaked data is located
- A Recorded Future Assessment on the leaked data
- Affected products list
- Tags:
 - **assessment** indicating the type of leaked data





PUBLICATION STATUS
Published

PUBLISHED DATE
24 Oct 2025 11:20

TLP 
Red

Watch | 0 Star | 0 Views | 0

Like | 0 Comment | 0 Share

TAGS
Visibility

My Organization

E.g., First Tag, Second Tag

alert-id:task:cb92cbb2-b79e-43b7-bee7-d976f7b53... x

assessment:Possible-Key-Leak x

organisation:Professional-Services-Development x

priority:Moderate x

recorded-future-playbook-alert x

rule-name:Data-Leakage-on-Code-Repository x

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

FEED
Recorded Future Alerts - Test

SOURCE CREATED
24 Oct 2025 11:19

SOURCE MODIFIED
24 Oct 2025 11:19

< **Description** Associations (0) Investigations (0) Attachments (0) Notes Histc >

Data Leakage on Code Repository

Summary

ID: task:cb92cbb2-b79e-43b7-bee7-d976f7b53bb2
Created: 2025-10-24 10:19:30
Updated: 2025-10-24 10:19:55
Status: New
Priority: Moderate
[API](#) | [Portal](#)

Targets

example.com

Repository

Owner: damarkuncoro
URL: <https://github.com/damarkuncoro/rails8-app>

Assessments

Published: 2025-10-24 10:08:46
Assessment targets: example.com
Possible Key Leak: password
Watch List Entity Mention on GitHub: example.com
Commit: <https://github.com/damarkuncoro/rails8-app/commit/f76168d89c04da358faf1b6cc0780d355a74c3c4>
Content:

```
+ # user\<em>name: Rails.application.credentials.dig(:smtp, :user\</em>name),+ # password: Rails.application.credentials.dig(:smtp, :password),+ # address: "smtp.example.com",+ # port: 587,+ # authentication: :plain
```

Published: 2025-10-24 10:08:45
Possible Key Leak: password, token, username
Commit: <https://github.com/damarkuncoro/rails8-app/commit/f76168d89c04da358faf1b6cc0780d355a74c3c4>
Content:

```
+ # username: your-user++ # Always use an access token rather than real password when possible.+ # password:+ # - KAMAL\<em>REGISTRY\</em>PASSWORD
```

Published: 2025-10-24 10:08:45
Assessment targets: example.com
Possible Key Leak: ssl
Watch List Entity Mention on GitHub: example.com

Playbook Alert: Data Leakage on Code Repository

Domain Abuse

The Domain Abuse Playbook Alerts utilise the **Incident** Threat Model and can be found by selecting the **Incidents** from the **Filter Options** in the **Threat Model** page.

The Domain Abuse Playbook Alerts contains:

- Domains targeted by the typosquat
- Screenshots of the webpage (if available)
- **NS**, **A** and **MX** recorded for the involved domain

- Observables (Anomali provides additional information in regard to the Country, Organisation, ASN and Status of the IOC, if available)

Threat Models List / Incident Detail /

 Domain Abuse - Www.Anywhere.Cinderella.Co.Za: Task:9b86333e-1b12-42ed-9e0c-018c8f3ea70f Export Actions

Recorded Future

PUBLICATION STATUS
Published

PUBLISHED DATE
24 Oct 2025 11:18

TLP 
Red

[Watch](#) | 0 [Star](#) | 0 [Views](#) | 0

[Like](#) | 0 [Dislike](#) | 0 [Share](#)

TAGS
Visibility
My Organization

E.g., First Tag, Second Tag

alert-id:task-9b86333e-1b12-42ed-9e0c-018c8f3ea70f x

organisation:Professional-Services-Development x

priority:Informational x

recorded-future-playbook-alert x

rule-name:Domain-Abuse x

screenshot-present x

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

FEED
Recorded Future Alerts - Test

SOURCE CREATED
24 Oct 2025 11:08

SOURCE MODIFIED
24 Oct 2025 11:09

Description Associations (0) Investigations (0) Attachments (0) Notes Histc >

Domain Abuse

Summary

ID: task:9b86333e-1b12-42ed-9e0c-018c8f3ea70f
Created: 2025-10-24 10:08:25
Updated: 2025-10-24 10:09:35
Status: New
Priority: Informational
[API](#) | [Portal](#)

Targets

cinderella.com

DNS Records

Reason: Alert was created as a result of a triggered typosquat detection

Entity	Risk Score	Criticality	Record Type	Context
104.247.82.51	36	Medium	A	
ns1.parkingcrew.net	20	Low	NS	
mail.h-email.net	15	Low	MX	Default or Common Mail Server
ns2.parkingcrew.net	15	Low	NS	
alltheemails.com	0		MX	Default or Common Mail Server

WHOIS Details

Entity: www.anywhere.cinderella.co.za
Name servers: ns2.host-h.net, ns1.dns-h.com, ns1.host-h.net, ns2.dns-h.com
Creation Date: 2020-05-19 00:02:24
Registrar: xneelo (Pty) Ltd

Screenshots

Screenshot Count: 1
Created: 2025-10-24 10:13:32



Playbook Alert: Domain Abuse

Recorded Future
PUBLICATION STATUS
Published
PUBLISHED DATE
26 Oct 2023 13:48
TLP
Red

Watch | Star | Views | Share

Description Associations (2) Investigations (0) Attachments (0) History

OBSERVABLES (2) THREAT MODELS (0) IMPORT SESSIONS (0) SANDBOX REPORTS (0)

Type your search

2 Results

	CREATED	ITYPE	OBSERVABLES	CONFID...	COUNTRY	ORG	ASN	STATUS	VISIBILI...	TAGS	DIRECTI...	TYPE	ASSOCI...	ASSOCI...	COMME...
>	25 Oct 2...	Suspicious	102:151:181:123	1	SG	Zenlayer	21859	Falsepos	My Orga...	aler...					25 Oct 2...
>	25 Oct 2...	Suspicious	yuehin.com	6				Falsepos	My Orga...	aler...					25 Oct 2...

Playbook Alert: Domain Abuse - Observables

Third Party Risk

The Third Party Risk Playbook Alerts utilise the **Incident** Threat Model and can be found by selecting the **Incidents** from the **Filter Options** in the **Threat Model** page.

The Third Party Risk Playbook Alerts contains:

- Evidence for increased Third Party Risk
- Insikt Notes (if available)
- Observables (if available)
- Risk score of the company associated with the alert
- Tags:
 - **risk-rule** indicating which [Recorded Future Risk Rules](#) matched the third party entity



Recorded Future

PUBLICATION STATUS
Published

PUBLISHED DATE
30 Jan 2024 09:17

TLP
Red

Watch | 0 Star | 0 Views | 0

Share

TAGS

Visibility
My Organization

E.g., First Tag, Second Tag

alert-id:task:85743a62-fa26-43a4-aadf-cf3563dfa3a3 x

organisation:Professional-Services-Development x

owner-name:Professional-Services-Development x

priority:High x recorded-future-playbook-alert x

risk-rule:Hosts-Recently-Communicating-With-C&C... x

risk-rule:Recent-High-Impact-Abuse-of-Company-L... x

rule-name:Third-Party-Risk x

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
Add Intelligence Initiative

FEED

Description Associations (6) Investigations (0) Attachments (0) History

View in Recorded Future

Third Party Risk - Alibaba (99)

Priority: High
Alert Created: 2023-08-30 16:33:38
Alert Updated: 2024-01-29 16:48:16

Malicious Network

Hosts Recently Communicating With C&C Server

Added on: 2024-01-29 16:46:00
Summary: 605 sightings: Active command and control communication on uncommon ports related to malware from 8 hosts including 47.57.181.106, 47.74.17.23, 47.57.242.27. 4 related malware families including PlugX, Cobalt Strike: C2Concealer, Cobalt Strike. Last observed on Jan 28, 2024.

Evidence

Observed Network Traffic - Client IP 47.57.242.27

- Recent Timestamp:** 2024-01-04 18:43:40
- Malware IP Address:** 122.254.94.69 (49)
- Malware IP Risk Description:** 18 sightings on 1 source: Recorded Future Command & Control Validation. Recorded Future analysis validated 122.254.94.69:8000 as a command and control server for PlugX on Jan 30, 2024 Mitigated by being in Multi-Domain IP Addresses (Allow List).
- Malware Family:** PlugX

Observed Network Traffic - Client IP 47.57.242.27

- Recent Timestamp:** 2024-01-07 16:53:00
- Malware IP Address:** 143.198.214.96 (99)
- Malware IP Risk Description:** 1 sighting on 1 source: Recorded Future Command & Control Validation. Recorded Future analysis validated 143.198.214.96:33434 as a command and control server for Cobalt Strike: C2Concealer on Jan 29, 2024
- Malware Family:** Cobalt Strike: C2Concealer

Observed Network Traffic - Client IP 47.74.17.23

- Recent Timestamp:** 2024-01-08 13:14:43
- Malware IP Address:** 103.145.191.118 (99)

Playbook Alert: Third Party Risk



Recorded Future

PUBLICATION STATUS
Published

PUBLISHED DATE
30 Jan 2024 09:17

TLP
Red

Watch | 0 Star | 0 Views | 0

Share

TAGS

Visibility
My Organization

E.g., First Tag, Second Tag

alert-id:task:85743a62-fa26-43a4-aadf-cf3563dfa3a3 x

organisation:Professional-Services-Development x

owner-name:Professional-Services-Development x

priority:High x recorded-future-playbook-alert x

Description Associations (6) Investigations (0) Attachments (0) History

OBSERVABLES (6) THREAT MODELS (0) IMPORT SESSIONS (0) SANDBOX REPORTS (0)

Type your search

CREATED	ITYPE	OBSERVABLES	CONFIDENCE	COUNTRY	ORG	ASN	STATUS	VISIBL	TAGS	DIRECTI	TYPE	ASSOCI	ASSOCI	COMME
> 26 Jan 2...	Suspicious IP	100.24.59.15	39	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
> 26 Jan 2...	Suspicious IP	8.130.132.92	95	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
TAGS														
alert-id:task:85743a62-fa26-43a4-aadf-cf3563dfa3a3 organisation:Professional-Services-Development owner-name:Professional-Services-Development														
> 26 Jan 2...	Suspicious IP	100.79.154.38	100	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
> 26 Jan 2...	Suspicious IP	47.309.57.38	98	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
> 26 Jan 2...	Suspicious IP	121.419.223	72	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
> 06 Oct 2...	Suspicious IP	39.104.81.101	80	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...

Playbook Alert: Third Party Risk - Observables

Identity Novel Exposures

The Identity Novel Exposures Playbook Alerts utilise the Incident Threat Model and can be found by selecting the Incidents from the Filter Options in the Threat Model page.

The Identity Novel Exposures Playbook Alerts contains:

- The identity that was exposed
- Password hint or clear text password ([Enabling cleartext passwords within Identity Intelligence](#))
- Authorization URL
- IP Address (if available)
- Dump details
- Exposed secret details
- Compromised host (if available)
- Malware family name (if available)
- Technology (if available)
- Observable of the exposed identity with **Confidence** of 20
- Tags
 - **assessment** indicating the type of exposure
 - **plain-text-password** indicating the Anomali TS incident contains a plain text password
 - **malware-family** the stealer malware family name (if available)



Recorded Future

PUBLICATION STATUS
Published

PUBLISHED DATE
24 Oct 2025 11:09

TLP
Red

Watch | 0 Star | 0 Views | 0

0 | 0 Share

TAGS

Visibility
My Organization

E.g., First Tag, Second Tag

alert-id:task:cec6659d-2125-4b7f-a460-22866e6272... x

assessment:Malware x

malware-family:XFiles-Stealer x

organisation:Professional-Services-Development x

plain-text-password x priority:Moderate x

recorded-future-playbook-alert x

rule-name:Novel-Identity-Exposure x

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

FEED
Recorded Future Alerts - Test

SOURCE CREATED
23 Oct 2025 21:05

SOURCE MODIFIED
23 Oct 2025 21:05

Description	Associations (0)	Investigations (0)	Attachments (0)	Notes	History
-------------	------------------	--------------------	-----------------	-------	---------

Novel Identity Exposure

Summary

ID: task:cec6659d-2125-4b7f-a460-22866e6272b9
Created: 2025-10-23 20:05:52
Updated: 2025-10-23 20:05:52
Status: New
Priority: Moderate
[API](#) | [Portal](#)

Exposure

Identity: atelieraplus@norsegods.online
Password: chondri#1
Assessment: Malware
Authorization URL: https://acme.com/member.php
IP Address: 72.59.17.34
Properties: Letter, Number, Symbol, LowerCase, AtLeast8Characters
Hashes:

- SHA1** ba5617274df4a5069d1e3b6b97d11b24d09cafcb
- SHA256** d73551eda68c4e2158b8c75f9a2c49b9756dbde0a18f8e9a9e712fa46db0e30c
- NTLM** c131f06bd2b1d39fc39183aca5a4a889
- MD5** ede1e91bc1665121d71b9825fc26db80

Source:

- Name:** Stealer Malware Logs 2025-10-23
- Description:** This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.

Compromised Host:

- Operating System:** Windows 11
- OS Username:** aiban
- Machine Name:** Russia 34

Malware Family: XFiles Stealer

Actions to Consider

- [Check Incident Report](#)
- Enforce Password Reset
- Initiate MFA Challenge
- Request Compromised Host Incident Response
- Review Malware Hunting Packages

Playbook Alert: Novel Identity Exposures



Description **Associations (1)** Investigations (0) Attachments (0) History

OBSERVABLES (1) THREAT MODELS (0) IMPORT SESSIONS (0) SANDBOX REPORTS (0)

Type your search

1 Results

<input type="checkbox"/>	CREATED	ITYPE	OBSERVABLES	CONFIDENCE	STATUS	TAGS	ASSOCI...
<input checked="" type="checkbox"/>	29 Jan 2024 12:02	Compromised Account Email	y.babakr.ncbs@norsegods.online	20	Active	alert-id:task:e21726... >	09 Feb 2...

TAGS

alert-id:task:e217266a-a84b-4d3c-a971-da6d8f66a21b assessment:Malware assessment:Technology malware-family:Vidar plain-text-password

Playbook Alert: Novel Identity Exposures: Observables

Malware Report (Malware Intelligence)

The Malware Report Playbook Alerts utilise the **Incident** Threat Model and can be found by selecting the **Incidents** from the **Filter Options** in the **Threat Model** page.

The Malware Report Playbook Alerts contains:

- Matched hashes
- Observables of the matches hashes with **Confidence** equivalent to Recorded Future Risk Score + 1
- Sandbox Reports
 - Score
 - Tags
- Tags
 - **malware-family** identified malware family name (if available)





PUBLICATION STATUS
Published

PUBLISHED DATE
23 Jul 2025 11:29

TLP 
Red

Watch | 0 Star | 0 Views | 0

Share

TAGS
Visibility

My Organization

E.g., First Tag, Second Tag

alert-id:task:0647fd1f-38bc-451d-a49f-43a5ef071891 ×

organisation:Professional-Services-Development ×

priority:Informational ×

recorded-future-playbook-alert ×

rule-name:Ransomware-with-no-family ×

VISIBILITY
My Organization

Description	Associations (994)	Investigations (0)	Attachments (0)	Notes	History
<h2>Ransomware with no family</h2>					
<h3>Summary</h3>					
ID: task:0647fd1f-38bc-451d-a49f-43a5ef071891					
Created: 2025-07-21 05:00:13					
Updated: 2025-07-21 05:00:13					
Status: New					
Priority: Informational					
API Portal					
<h3>Matched Hashes (994)</h3>					
02f6f3af20b1ffbaa53a8c5a4c13289b34e38c1bfecfdb851b4f26327fd5c9a3 (70)					
Sandbox Reports (Click to expand)					
250720-e8vq4aszhh-behavioral1					
Sandbox Score: 9					
Tags: X86, WINDOWS, WINDOWS:4, DISCOVERY, ARCH:X86, RANSOMWARE					
0553a1eb7bd9de85bcb7a17707174a25c3d1f5ba05e94b02dc11e08126d90903 (70)					
Sandbox Reports (Click to expand)					
0754b0d040e404fca43e25ac6f4867e380ef692248fde808d6f7b9cf0e536c86 (70)					
Sandbox Reports (Click to expand)					

Updates

One of the unique aspects of Recorded Future Playbook Alerts is that these alerts will receive updates and these updates will also propagate to Anomali TS by updating the **Description** tab and other relevant data inside the appropriate **Threat Model**.

Observables

Not all Recorded Future Alerts are equal meaning not every **Incident** will have **Observables** available in the **Associations** tab. The list below summarises which alerts will produce **Observables** when available.

Recorded Future Classic Alerts

- Leaked Credential Monitoring
- Leaked Email Monitoring

Recorded Future Playbook Alerts

- Domain Abuse
- Third Party Risk

- Identify Similar Domains
- IP Address Mentions
- Increased IP Address Risk Score
- Increased Domain Risk Score
- Potential Logo Abuse Detection
- Novel Identity Exposures
- Malware Report

✓ New in v1.3.0:

- Select more Classic Alerts (IGL or Custom) to create Observables with the desired iType
- Disable Observable creation for the predefined Classic Alerts (listed above)
- Override the Observable iType for the predefined Classic alerts (listed above)

For more information please contact support at support@recordedfuture.com.

Confidence

The confidence of each observable is set as follows:

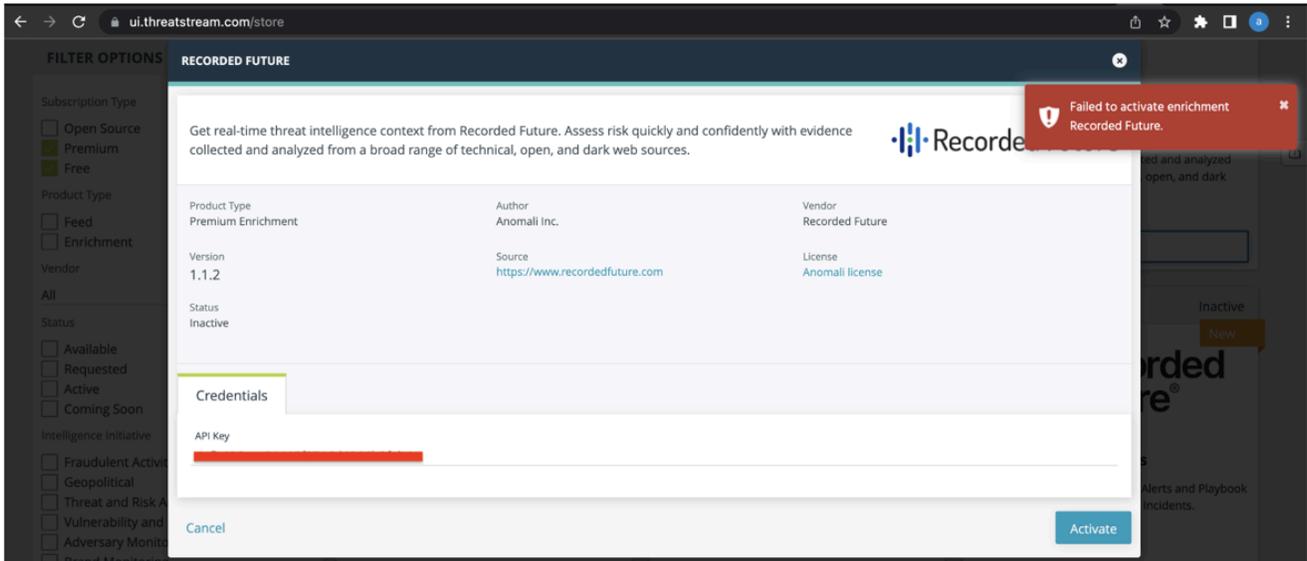
- For Playbook Alerts: this will be equal to the Recorded Future risk score of the observable plus 1, as shown in the screenshot above. The addition of 1 is to match the Anomali scale which goes up to 100 instead of 99.
- For classic alerts: the default confidence is **16** for all ITypes except for **Compromised Emails** ITypes which will be **20**.

Installation

The preferred installation method for the Recorded Future Alert Feed is through the Anomali TS App Store.

Configuration

Once the application is installed please set the Recorded Future token and click **Activate**.



Tags

Recorded Future Alert Feed uses a set of common tags that are added to Observable and Incidents. These tags help to quickly and easily search and build dashboards from the Recorded Future alert data. Note that tags are limited to 50 per alert.

Tag	Observable	Threat Model	Example	Description
alert-id	✓	✓	<i>alert-id:wyf7g0</i>	Recorded Future Alert ID
assessment		✓	<i>assessment:Possible-Key-Leak</i>	Indicates the assessment made by Recorded Future
author	✓	✓	<i>author:Bot</i>	Author of the data
lifecycle		✓	<i>lifecycle:Exploited</i>	Indicates the lifecycle stage of a vulnerability
malware-family	✓	✓	<i>malware-family:Lumma</i>	Indicates stealer malware name
organisation	✓	✓	<i>organisation:PS-Development</i>	The organisation of the alert
owner-name	✓	✓	<i>owner-name:Moise</i>	The owner of the alert

plain-text-password		✓	<i>plain-text-password</i>	Indicates that the Incident contains a plain text password
priority		✓	<i>priority:High</i>	Indicates the priority of a Recorded Future Playbook Alert
recorded-future-alert		✓	<i>recorded-future-alert</i>	Indicates that this is a Recorded Future Alert
recorded-future-playbook-alert		✓	<i>recorded-future-playbook-alert</i>	Indicates that this is a Recorded Future Playbook Alert
risk-rule		✓	<i>risk-rule:Recent-Validated-Cyber-Attack</i>	Name of the matched Recorded Future Risk Rule
rule-name	✓	✓	<i>rule-name:Leaked-Credential-Monitoring</i>	Recorded Future Alert rule name
screenshot-present		✓	<i>screenshot-present</i>	Indicates that the Incident contains a screenshot
source	✓	✓	<i>source:Genesis-Store</i>	Source of the data

Troubleshooting

Missing Observables

In some cases an **Incident** might display a certain amount of observables in the **Description** tab and yet contain less in the **Associations** tab, this is due to the fact that Anomali TS has a whitelisting mechanism that prevents certain **Observables** from being ingested. For more information please contact the Anomali Support team.

Not fetching alerts

The integration only fetches alerts with a status of **no-action** or as shown in the portal **New** . Verify that the alerts you wish to fetch have this status set.

Custom Alerts (created with AQB) not ingesting

By default Recorded Future Custom Alerts created using the Advanced Query Builder (AQB) are private to the user and are not visible to the Anomali integration. To share a custom Alert with your Anomali ThreatStream (TS) instance please follow [this support article](#).

IOC with 0 risk score and no Intelligence Card

There might be playbook alerts (specifically Domain Abuse, Third Party Risk and Cyber Vulnerability) where an IOC might have a risk score of 0 but no information in the intelligence card associated with it in the Recorded Future Portal. That is expected, we decided to still show those IOCs related to an alert for completeness of information. The occurrences of such IOC is expected to be very low.

CHANGELOG

[1.5.1] - 2026-03-05

Added

- User set Playbook Alert rule names are now used in the Anomali Threat Model title field, as well as the `alert-rule` tag, instead of the default rule name.

[1.5.0] - 2026-02-03

Added

- Support for `Malware Report` Playbook Alert

Changed

- Updated Incident layout for the following Playbook Alerts
 - `Domain Abuse`
 - `Code Repo Leakage`
 - `Cyber Vulnerability`
 - `Third Party Risk`
 - `Identity Novel Exposures`
- Optimised ingestion of `Domain Abuse` Playbook Alerts which results in much faster ingestion times
- `PSEngine` upgraded to v2.4.2
- `Anomali Feeds SDK` upgraded to v2.6.0

[1.4.3] - 2026-01-05

Added

- Classic Alerts entity tags optimisation.

[1.4.2] - 2025-09-15

Changed

- Alert ingestion optimisations

[1.4.1] - 2025-05-07

Fixed

- Classic Alerts
 - Missing reference fragment sometimes prevented alert ingestion.
- Playbook Alerts
 - Domain Abuse MX records sometimes caused alert fetch to fail.

Changed

- PSEngine upgraded to v2.0.5

[1.4.0] - 2025-03-24

Added

- Classic Alerts
 - Source Created time is now set using the alert created time
 - Triggered by now tells the user why a specific reference has matched and is part of the alert
 - Observables are now created from alert rule Malicious Infrastructure on Monitored IP Addresses
- Playbook Alerts
 - Source Created time is now set using the alert created time
 - Source Modified time is not using the alert updated time

Changed

- Classic Alerts
 - New enhanced layout
- Playbook Alerts
 - Source Created time is now set using the alert created time
 - Source Modified time is not using the alert updated time

Fixed

- Classic Alerts
 - Hashes from sandbox analysis references are now created as Observables

Removed

- Playbook Alerts

- Alert Created / Updated removed from the description in favour of **Source Created** and **Source Modified**

[1.3.1] - 2024-08-14

Fixed

- Playbook Alerts
 - Novel Identity Exposure
 - An incorrectly formatted password hint no longer stops ingestion of playbook alerts.
 - Cyber Vulnerability
 - Unusual vulnerability names such as '0.0.0.0 day' no longer stop ingestion of playbook alerts.

[1.3.0] - 2024-07-01

Added

- Classic Alerts
 - Support for custom Observables mapping
- **rule-name** tag added to Observables

Changed

- Classic Alerts
 - New layout

Fixed

- Classic Alerts
 - Some Observables from URLs were not being enriched correctly

[1.2.0] - 2024-03-14

Added

- Support for **Identity Novel Exposures** Playbook Alert
- New Tags (see install guide for complete list)

Changed

- **PSEngine** upgraded to v1.12.0
- **Anomali Feeds SDK** upgraded to v2.5.17

- `Anomali Feeds SDK` upgraded to v2.5.17

[1.1.0] - 2023-11-03

Added

- Classic Alerts now support `Recorded Future AI Insights`
- Classic Alerts contain the full Insikt Analyst Note text instead of a fragment
- Playbook Alert `Domain Abuse` now displays the `Targets` of a typosquat
- Support for `Code Repository Leakage`, `Cyber Vulnerability` and `Third-Party Risk` Playbook Alert
- Generic Incident for not yet fully supported Playbook Alerts - New Tags (see install guide for complete list)

Changed

- Classic Alerts IOC enrichment is now enabled by default for all clients
- `Anomali Feeds SDK` upgraded to v2.5.16
- `PSEngine` upgraded to v1.10.2

Fixed

- Removed reference count from the `Incident Name`
- `PSEngine` upgraded which fixed the `limit` parameter issue when paginating through results

Removed

- Removed `enrich_alerts` parameter from `[anomali_ts]` stanza
-

[1.0.0 GA] - 2023-03-08

Added

- Official package release

