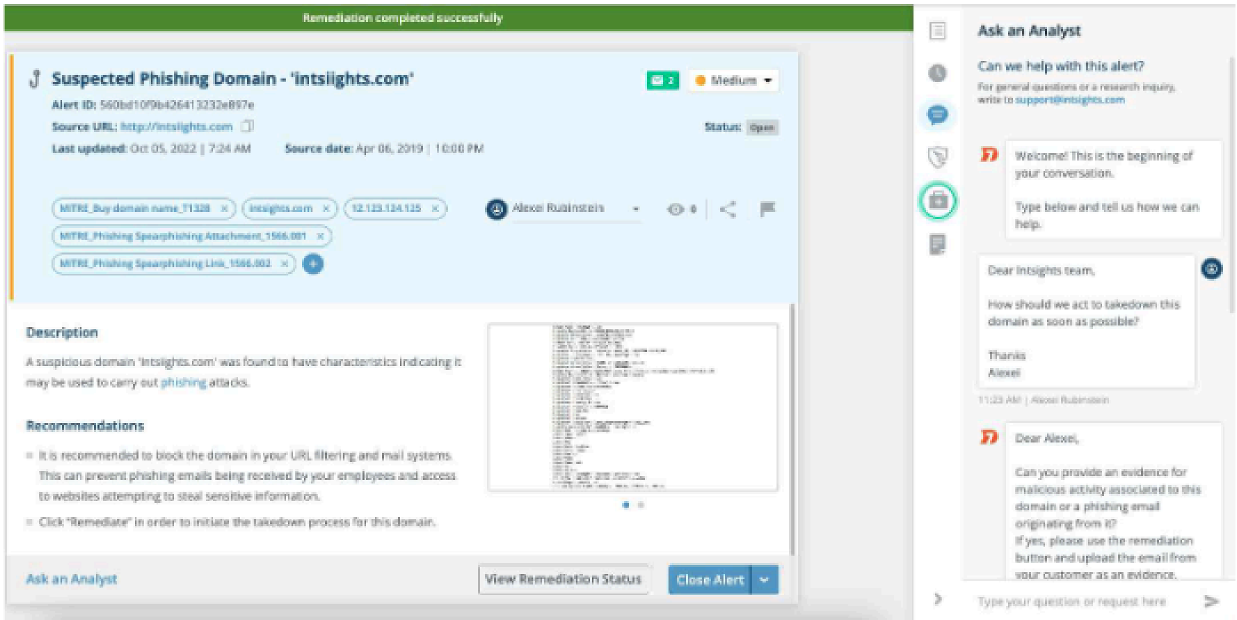
Dark Web Purchase Guide

Purchasing on the Dark Web can be tricky. Should you purchase the information being sold? Will it be posted elsewhere if it is purchased? Why does each item cost a different amount?
These are just some of the questions organizations have regarding purchasing items on the Dark Web. This document covers some best practices when making purchases on the Dark Web with a Threat Command.

How to purchase information sold on the Dark Web

- Initiate request via “Ask an Analyst”
- If bulk alerts are requested, the analyst team responds with the number of credits required to make the purchase.
- The requester is required to approve the request before the information is purchased.
- Information is purchased and sent via a secure link in the “Ask an Analyst” channel.
- The customer's account will be charged with the amount of credits according to the number of alerts purchased.



Remediation completed successfully

Suspected Phishing Domain - 'intsights.com'

Alert ID: 560bd10f9b426413232e897e
Source URL: http://intsights.com
Last updated: Oct 05, 2022 | 7:24 AM
Source date: Apr 06, 2019 | 10:00 PM
Status: Open

Description

A suspicious domain 'intsights.com' was found to have characteristics indicating it may be used to carry out phishing attacks.

Recommendations

- It is recommended to block the domain in your URL filtering and mail systems. This can prevent phishing emails being received by your employees and access to websites attempting to steal sensitive information.
- Click "Remediate" in order to initiate the takedown process for this domain.

Ask an Analyst

Can we help with this alert?

For general questions or a research inquiry, write to support@intsights.com

Welcome! This is the beginning of your conversation.

Type below and tell us how we can help.

Dear Intsights team,

How should we act to takedown this domain as soon as possible?

Thanks
Alexei

11:23 AM | Alexei Rubinstein

Dear Alexei,

Can you provide an evidence for malicious activity associated to this domain or a phishing email originating from it?
If yes, please use the remediation button and upload the email from your customer as an evidence.

2
Medium
MITRE_Buy domain name_T1328
intsights.com
12.123.124.125
MITRE_Phishing Spearphishing Attachment_1566.001
MITRE_Phishing Spearphishing Link_1566.002
Alexei Rubinstein
0
Ask an Analyst
View Remediation Status
Close Alert
Type your question or request here

DW purchases a service package:

Package credits service will include purchase items, subject to the fair use policy, directly related to an alert within the customer's account dashboard only.

The service includes the basic item cost as presented in the source, in addition to the analyst labor costs associated with the transaction fee.

Rapid7 reserves the right to deny or approve the transaction individually. In these situations, additional credits may be required to initiate the transaction.

Common Questions about Purchases on the Dark Web

1. How many credits will it cost to purchase the item being sold?

    - Each alert that the customer wants to purchase the information will cost one credit per alert but is limited according to the Fair Use Policy.

2. Will the information be posted elsewhere on the Dark Web after purchasing it?

    - Unfortunately, there is no way to know for certain if specific information purchased will be posted elsewhere in the future. What we can do is give our recommendations based on whether the information purchased typically appears elsewhere in the future. In most cases, it is beneficial to validate the information being sold prior to purchase. If found to be legitimate, the organization can take the appropriate course of action to mitigate the risk.