



March 09, 2022

bwsecurity day 2022

# External Threat Intelligence

## Mitigate Threats from the Clear, Deep and Dark Web

**Fabian Guter**

Solution Specialist - Threat Intelligence

# About Rapid7

- .

# RAPID7

## Best-in-Class Technology



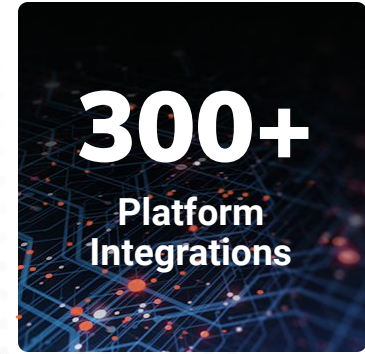
## Security Services



## Research and Community



## Global Ecosystem



## 10,200+ Customers

44% of Fortune 100  
NASDAQ: RPD

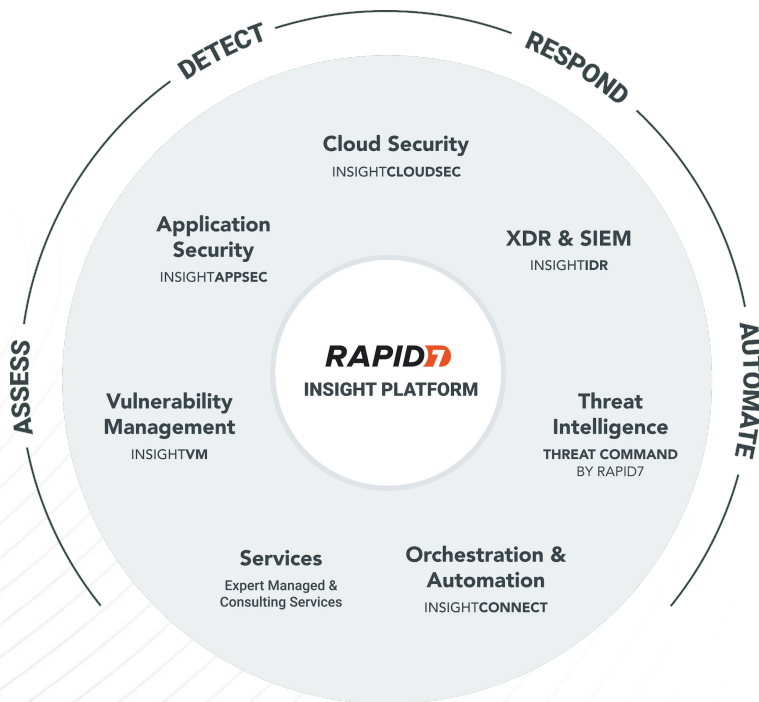
## Global Footprint

144 Countries  
21 Offices

## Leader of Innovation

56 Patents  
Open Source Communities

# Comprehensive security that powers your business.



## Technology

Best-in-Class Portfolio  
Unified Platform Services  
Plug and Play Integrations  
Intelligent Automation

## Expertise

Security Research  
Open Source Community

## Differentiators

Flexible Product and Managed  
Services Mix  
Time to Value  
Vendor Consolidation

# Cyber Threat Intelligence

What it is about?

**No organization  
is immune to  
cyber attacks.**



**DIGITAL  
TRANSFORMATION**



**DELUGE  
OF DATA**



**NO  
PERIMETER**



**RESOURCE &  
SKILLS GAP**

## Clear Web

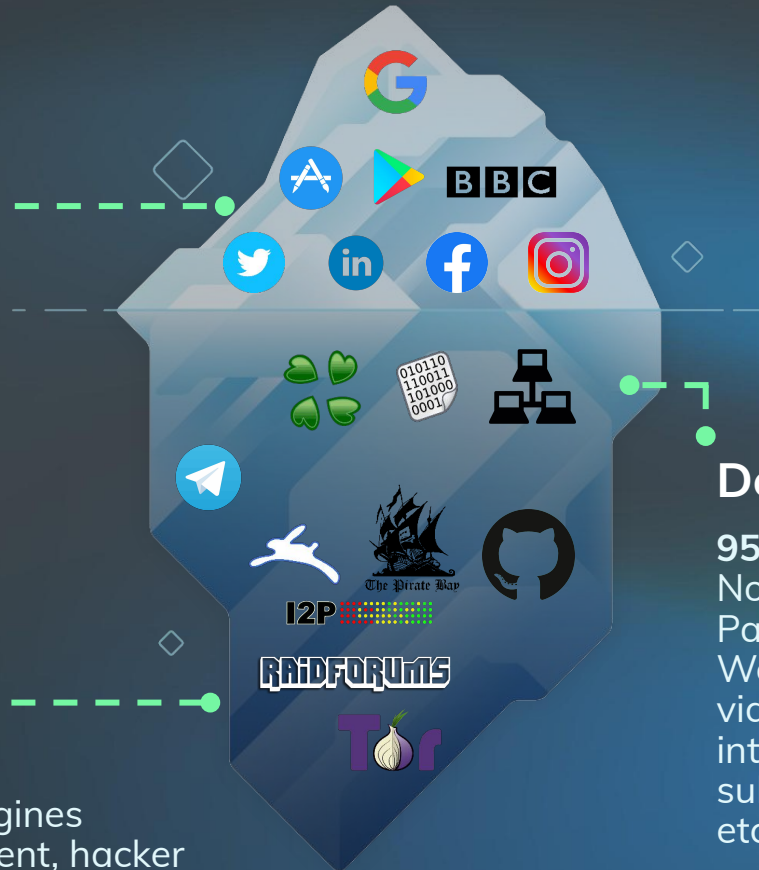
4% of Web Content

Search engine  
Media, blogs, etc.

## Dark Web

1% of Web content

Not searchable by most engines  
Home to TOR, IRCs, BitTorrent, hacker  
forums, C2s, and more.



## 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.

# Threat Intelligence Platform - What does it do?

## Extend Visibility

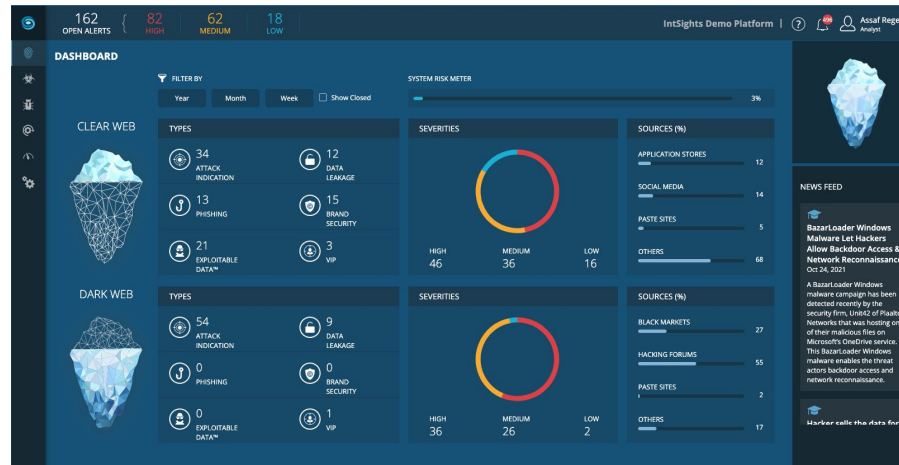
- Single-pane-of-glass visibility into external threats
- Proprietary collection & classification capabilities
- Operationalize and enrich intelligence

## Continuously Monitor

- Identify the critical threats that directly impact your business
- Intelligence data is organized and augmented with sophisticated analysis

## Automate Response

- Prioritize alerts, risk, and vulnerabilities
- Proactively mitigate/remediate threats
- Respond with confidence



# Plug and play with existing security solutions



# Use Cases

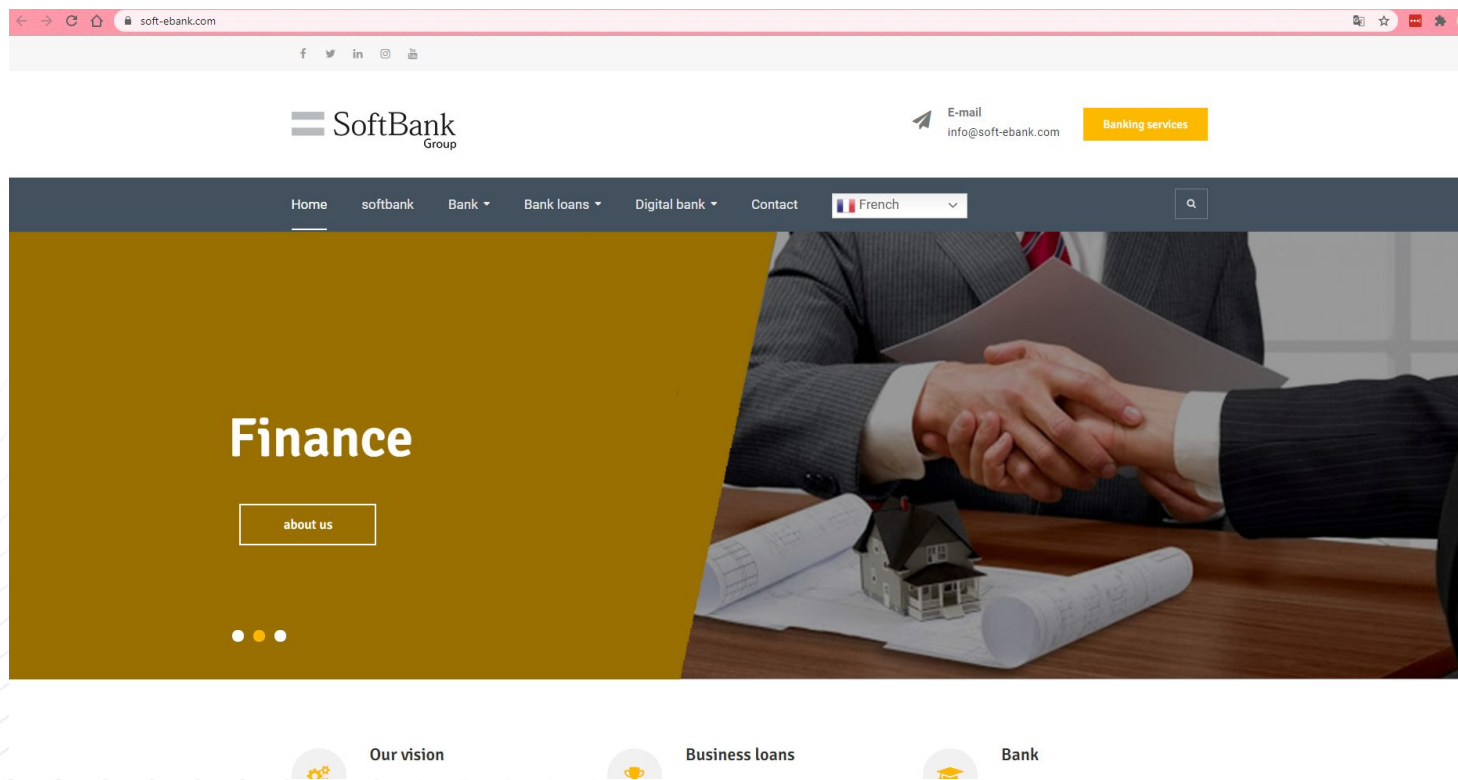
Where can CTI help me?

# Phishing Domain – Example



- A screenshot of a text message that Knab's clients received, asking them to visit 'knab-update.pro', which is a phishing domain (and website). The text says that their Knab banking app is expiring, and they need to register via this URL. This is also an example of smishing (phishing via SMS).
- This is, of course, not Knab's real website. The real one is knab.nl

# Phishing Website – Example



# Phishing Alert

**ALERTS**

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

2 Suspects x Phishing x Source Type Clear Web x Clear Filters

13 All High Medium Low

Remediation completed successfully

**Suspected Phishing Domain - 'Intsiights.com'**

Alert ID: 560bd10f9b426413232e897e  
Source URL: http://intsiights.com  
Last updated: Feb 16, 2022 | 9:54 PM Source date: Apr 07, 2019 | 6:00 AM

MITRE\_Buy domain name\_T1328 x intsiights.com x 12.123.124.125 x Alexei Rubinstein

MITRE\_Phishing Spearphishing Attachment\_1566.001 x

MITRE\_Phishing Spearphishing Link\_1566.002 x +

**Description**

A suspicious domain has been detected - intsiights.com. It is similar to the company web domain and so may be used for malicious activity, e.g. phishing e-mails, phishing website. It is recommended to block the domain in your URL filtering and mail systems in order to prevent phishing emails and websites from your employees. Click "Remediate" in order to suspend the malicious domain.

The domain was registered by Cobalt group

**Recommendations**

Ask an analyst

View Remediation Status

Close Alert

## Suspected Phishing Domain - 'intsiights.com'

Alert ID: 560bd10f9b426413232e897e

Source URL: <http://intsiights.com>

Last updated: Feb 16, 2022 | 9:54 PM

Source date: Apr 07, 2019 | 6:00 AM



Medium

Status: Open

MITRE\_Buy domain name\_T1328 x

intsiights.com x

12.123.124.125 x

Alexei Rubinstein

0



MITRE\_Phishing Spearphishing Attachment\_1566.001 x

MITRE\_Phishing Spearphishing Link\_1566.002 x



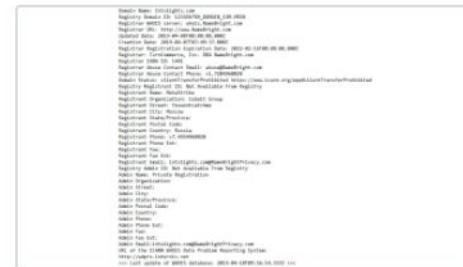
## Description

A suspicious domain has been detected - intsiights.com. It is similar to the company web domain and so may be used for malicious activity, e.g. **phishing** e-mails, **phishing** website. It is recommended to block the domain in your URL filtering and mail systems in order to prevent **phishing** emails and websites from your employees. Click "Remediate" in order to suspend the malicious domain.

The domain was registered by **Cobalt group**

## Recommendations

Ask an analyst to block the domain in your URL filtering and mail systems. This can prevent phishing emails being received by your employees and access



View Remediation Status

Close Alert

## Use Case – Phishing

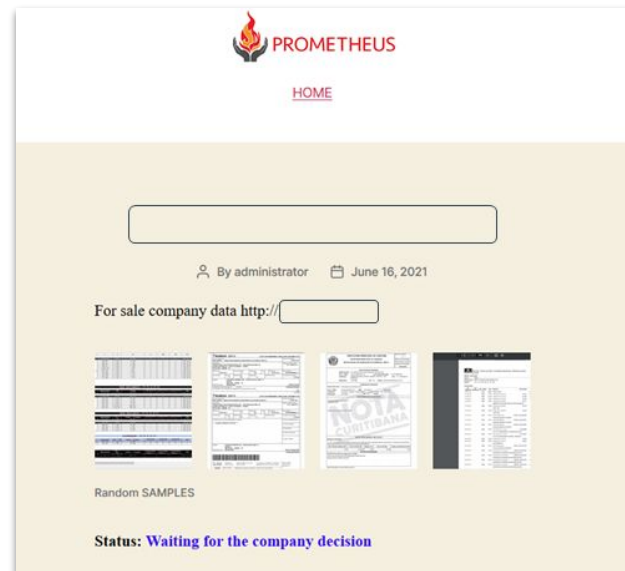
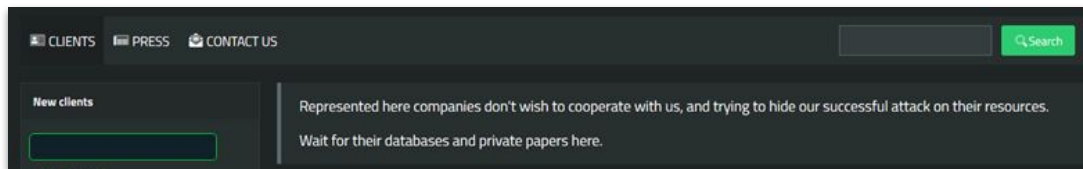
---

- Identification of Phishing domains and websites
- Research on dark web about planned phishing campaigns

### Countermeasures

- Takedown of domain and websites (Remediation)
- Reporting to Phishing Trackers and lists
- Automation: block websites and domains in your firewall/gateway/proxy

# Ransomware - Double Extortion



## Ransomware as a Service - Himalaya

We offer ransomware for free!

We take a commission of 30% of all ransoms paid

We send the part of your ransom maximum 24 hours after confirmation of the transaction

We manage communication with victims

VERY IMPORTANT WARNING :

PROHIBITION OF ATTACKING HEALTH FACILITIES

PROHIBITION OF ATTACKING ANY PUBLIC ORGANIZATION OR NON-PROFIT ASSOCIATION

ONLY ATTACK PRIVATE COMPANIES OR INDIVIDUALS

# Leaked Credentials

## Dark Web - 7 active login credentials of current employees were confirmed

Alert ID: 59e672de65fa570006b76dad

Last updated: Feb 16, 2022 | 9:54 PM

High

Status: Open

GDPR x HIPAA x IntSights.com x usa.intsights.com x  
uk.intsights.com x partner.intsights.com x customer.intsights.com x  
Themuschutch.com x +

Alexei Rubinstein

0

Share

Flag

The leak exposed 8 records, total. 4 users were active, of which 3 had a valid password in the Active Directory. 4 user passwords could not be verified. Check the IntSights virtual appliance and Active Directory connectivity to ensure that the integration is synchronized. Please contact IntSights support for additional information.

Download CSV

### Description

Dark Web - Login credentials of 8 employees were leaked from Themuschutch.com, after verification in Active Directory it was found that 7 login credentials are of active accounts and 3 of them have been confirmed as active users with valid passwords.

### Recommendations:

It is recommended to update the active directory integration policy to automatically

Email	Email Status	Password	Password Status	AD Domain
jimp@intsights.com	Active	slah12	Active	intsights.com
benda@intsights.com	Active	kabul one	Active	intsights.com
david@intsights.com	Active	10839	Active	intsights.com
alexei@intsights.com	Active	metallica123	Inactive	usa.intsights.com
mark@intsights.com	Active	sammy321	Inactive	usa.intsights.com
brian@intsights.com	Active	slowintsights	Inactive	uk.intsights.com
brendac@intsights.com	Active	redcorvette	Inactive	partner.intsights.com
pault@intsights.com	Inactive	04051992qar	Unknown	customer.intsights.com

**ALERTS**

IntSights Desktop

Search

Status

Type

More

2 statuses

Data Leakage

Source Type

Dark Web

Clear Filters

10

5

4

1

All

High

Medium

Low

Dark Web - 7 active login credentials of current employees were confirmed

Feb 16, 2022 | 9:54 PM

GDPR

HIPAA

4 tags

Dark Web - Company-related files or folders were published in a previously reported n...

Feb 16, 2022 | 9:53 PM

Dark Web - 1 login credential record including clear text employee password was pu...

Mar 02, 2021 | 1:37 PM

HIPAA

GDPR

Dark Web - 23 login credentials including encrypted passwords of employees were leaked

Feb 16, 2022 | 8:37 PM

Dark Web - Databases of a state voter list were leaked

Dark Web - 7 active login credentials of current employees were confirmed

Alert ID: 59e672de65fa570006b76dad

Last updated: Feb 16, 2022 | 9:54 PM

GDPR

HIPAA

IntSights.com

usa.intsights.com

uk.intsights.com

partner.intsights.com

customer.intsights.com

Themuschutch.com

Alexei Rubinstein

The leak exposed 8 records, total. 4 users were active, of which 3 had a valid password in the Active Directory. 4 user passwords could not be verified. Check the IntSights virtual appliance and Active Directory connectivity to ensure that the integration is synchronized. Please contact IntSights for additional information.

Description

Dark Web - Login credentials of 8 employees were leaked from Themuschutch.com, after verification in Active Directory it was found that 7 login credentials are of active accounts and 3 of them have been confirmed as active users with valid passwords.

Recommendations:

It is recommended to update the active directory integration policy to automatically

# Leaked Data

**ALERTS**

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

Status: 2 Stages -> Type: Data Leakage -> Source Type: Dark Web -> Clear Filters

10 5 4 1  
All High Medium Low

Remediation is in progress

- ☐ Dark Web - Full voter database is offered for sale on Samsara Market  
Feb 16, 2020 | 11:13 PM  
[Copy] [Share]
- ☐ Dark Web - Company DB was offered for sale on a cyber crime forum  
Jan 21, 2020 | 11:58 PM  
[Education] [University]
- ☐ Dark Web - A possible breach in State Driver Licenses database has been identified  
Jan 16, 2020 | 11:59 PM  
[Government] +1 tag
- ☐ Dark Web - Company database is available for sale on the black market  
Mar 17, 2019 | 10:23 PM

**Dark Web - Company database is available for sale on the black market**  
Alert ID: 560bd10f9b426413232e897f  
Source URL: <http://2gf6inwn32pov6ro.onion/viewtopic.php?f=5&t=150&p=800&hilit=>  
Last updated: Mar 17, 2019 | 10:23 PM

Description

Dark Web - Company database is available for sale on the black market by temsilci. Further investigation is recommended.

Recommendations

- Conduct in-depth research

Ask an analyst

Close Alert

**Dark Web - Company database is available for sale on the black market** High

Alert ID: 560bd10f9b426413232e897f

Source URL: <http://2gf6inwn32pov6ro.onion/viewtopic.php?f=5&t=150&p=800&hilit=>

Last updated: Mar 17, 2019 | 10:23 PM

Status: Open

+ unassigned 0

**Description**

Dark Web - Company database is available for sale on the **black market** by temsilci. Further investigation is recommended.

**Recommendations**

- Conduct in-depth research

Ask an analyst

Close Alert

## Use Case – Ransomware Protection

---

- Leaked credentials or data in databases, on paste sites/repositories, on dark web
- Identification of information in exfiltrated data from 3rd parties
- Misconfigurations/vulnerabilities of the digital perimeter

### Countermeasures

- Takedown of Paste Sites, malicious web sites (Remediation)
- Acquisition of leaked credentials and databases
- Automation: Block compromised accounts by Active Directory Integration
- Fix configuration issues

# VIP Impersonations on Social Media



**Stephen schwarzman**  
@Stephen42835559

Stephen schwarzman from United States as a philanthropist, Am American businessman. chairman and CEO the founder of Blackstone Group,.

Joined December 2019

11 Following 2 Followers

Not followed by anyone you're following



**toddmullinsprayerline** Follow ...

15 posts 22 followers 260 following

**Todd Mullins**  
Husband to my 7th grade sweetheart, Dad to the best son, Pastor of the greatest church ..... S LF

This Account is Private



**Masayoshi Son**

Home

Posts

Reviews

Photos

About

Community

Create a Page



Like Follow Share ... Send Message

Write a post...

Photo/Video Tag Friends Check in ...

**Posts**

Masayoshi Son updated their cover photo.  
January 8 at 11:02 PM · 🌐

About See All

Send Message

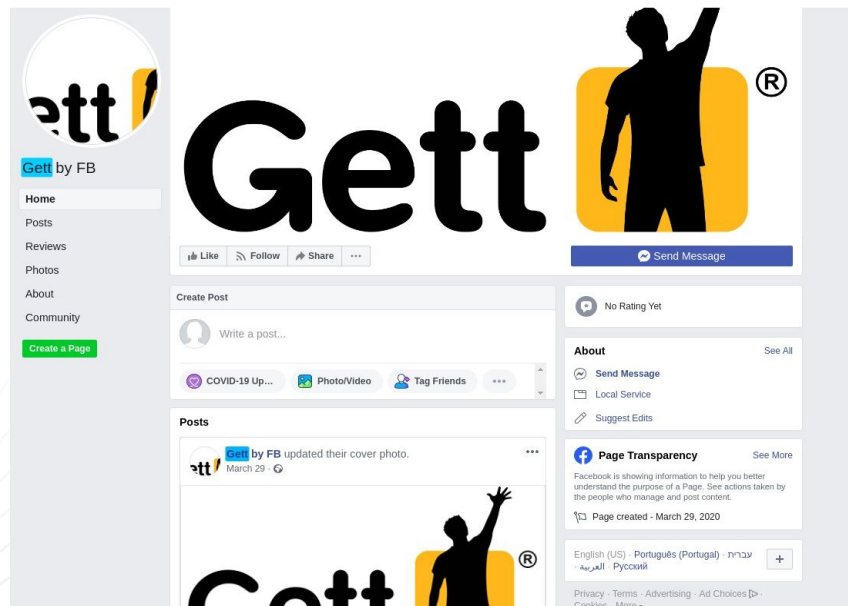
Public Figure

Page Transparency See More

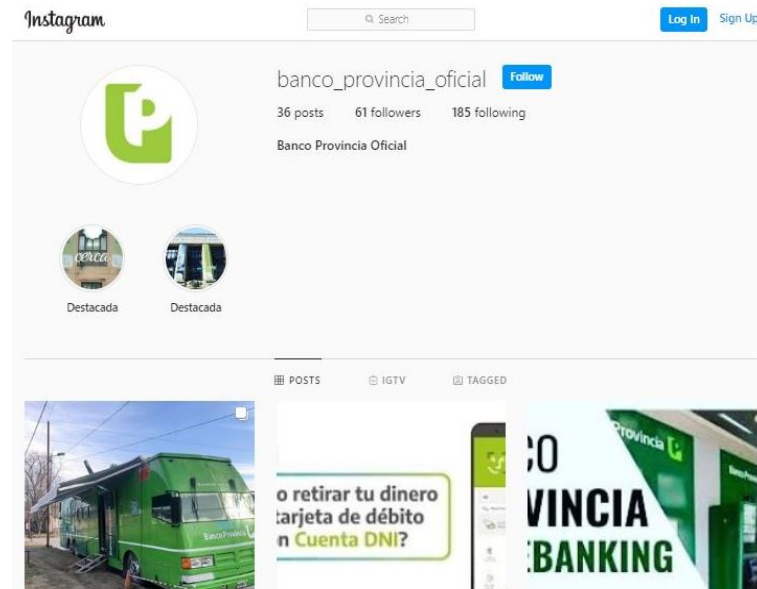
Facebook is showing information to help you better

Masayoshi Son, SoftBank's CEO

# IP Claims: Trademark/Copyright Infringements

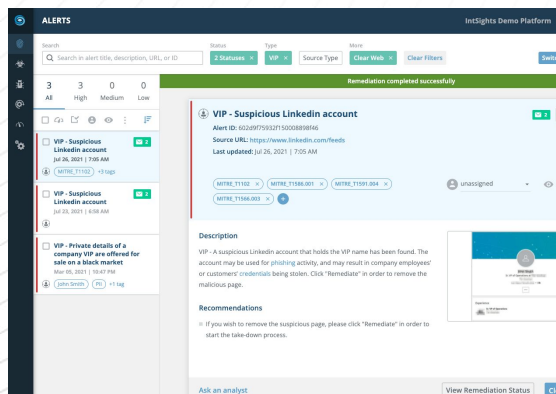


A Facebook page using Gett's logo



An Instagram account using Banco Provincia's name and logo and publishes fake posts.

# Fake Profile



**VIP - Suspicious LinkedIn account**

 2
 ● High

Alert ID: 602d9f75932f150008898f46

Source URL: <https://www.linkedin.com/feeds>

Last updated: Jul 26, 2021 | 7:05 AM

Status: Open

MITRE\_T1102 ×
MITRE\_T1586.001 ×
MITRE\_T1591.004 ×

MITRE\_T1566.003 ×
+

unassigned
 0

### Description

VIP - A suspicious LinkedIn account that holds the VIP name has been found. The account may be used for phishing activity, and may result in company employees' or customers' credentials being stolen. Click "Remediate" in order to remove the malicious page.

### Recommendations

- If you wish to remove the suspicious page, please click "Remediate" in order to start the take-down process.

View Remediation Status
Close Alert
▼

# VIP Data for sale

The screenshot shows the IntSights Demo Platform interface. At the top, there's a search bar and filters for Status (2), Type (VIP), Source Type (Dark Web), and Clear Filters. Below this, a table lists alerts with columns for ID, Status, Type, and Source. The first alert is highlighted: 'Dark Web - Private details of John Smith are posted on a black market' with a status of 'High' and a source of 'John Smith'. The main content area shows the details of this alert, including the alert ID, last updated time, source date, and status. A description section explains that the alert contains private details of John Smith, including Social Security Number (SSN), Date Of Birth (DOB), Bank account details, Credit Card details, and address, which are offered for sale on an identities black market. A screenshot of the black market listing is shown, displaying various personal details like first name, last name, address, city, state, zip code, phone number, SSN, driver's license, MVA, DOB, card type, card number, expiry date, CVV2, ATM pin, routing number, and account number. A recommendation is provided to purchase the record to cross-check the SSN for sale with the VIP's actual SSN and verify whether the information is valid. If this is the case, the recommendation is to notify the targeted employee so they can take the necessary steps, including acquiring a copy of their credit report from nationwide credit bureaus to check for unauthorized activity, and if such activity is found, consider posting a fraud alert on their credit report or placing a credit freeze.



## Dark Web - Private details of John Smith are posted on a black market

High

Alert ID: Scaba46fd9c2d1000795e616

Last updated: Feb 17, 2021 | 11:59 PM

Source date: Feb 15, 2021 | 8:08 PM

Status: Open

John Smith



unassigned



0



### Description

Dark Web - Private details of John Smith, including Social Security Number (SSN) Date Of Birth (DOB), Bank account details, Credit Card details and address are offered for sale on an identities black market. In the attached screenshot these details are hidden and will be visible only after purchasing the record. Threat actors may buy and use this information to carry out identity theft, assuming the VIP's identity for credit, benefits or services.

First name: F	
Lastname: F	
Address: 14	
City: C	
State: TX	
Zipcode: 7	
Phone: 817	
SSN: 44	
Driver's license: MVA	
DOB: 3	
Cardtype: Debit	
Cardnumber: 402	
Expiry Date: 6	
CVV2: 2	
ATM Pin: 6	
Routing Number: 60	
Account Number: 60	

We recommend purchasing the record in order to cross-check the SSN for sale with the VIP's actual SSN and verify whether the information is valid. If this is the case we recommend notifying the targeted employee so they can take the necessary steps, including acquiring a copy of their credit report from nationwide credit bureaus to check for unauthorized activity, and if such activity is found, consider posting a fraud alert on their credit report or placing a credit freeze.

Ask an analyst

Close Alert

## Use Case – Social Media, VIP and Brand Protection

---

- Faked personal profiles on social media are used for phishing and scam
- Non-approved user groups and company sites increase risk additionally
- Activity on social media can impact brand and company reputation

### Countermeasures

- Takedown of fake profiles and illegit company profiles (Remediation)
- Automation: Block access to illegit pages on firewall/gateway/proxy
- Collect proof for non-security related brand protection activities

# **Any Questions so far?**

# How to continue from here?

Potential next steps

# Next steps

## Demo with Specialist?

Contact us to book a dedicated demo and technical deep dive with our solution specialist.

Learn about use cases you are specifically interested in.



## Proof of Concept?

Test our service and solution against your own digital footprint and digital exposure. Includes free remediations and analyst time for one week.

With the POC, you can assess the value of CTI in your business context.



## Contact us!

Get in touch with us anytime to answer any questions you might have and align on the next steps.



# **What do you think?**

...and thanks for listening!

# Thank You!



**Fabian Guter**

Account Executive -  
Threat Intelligence

fabian\_guter@rapid7.com



Visit: <https://www.rapid7.com/products/threat-command/>

