RAPID7

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

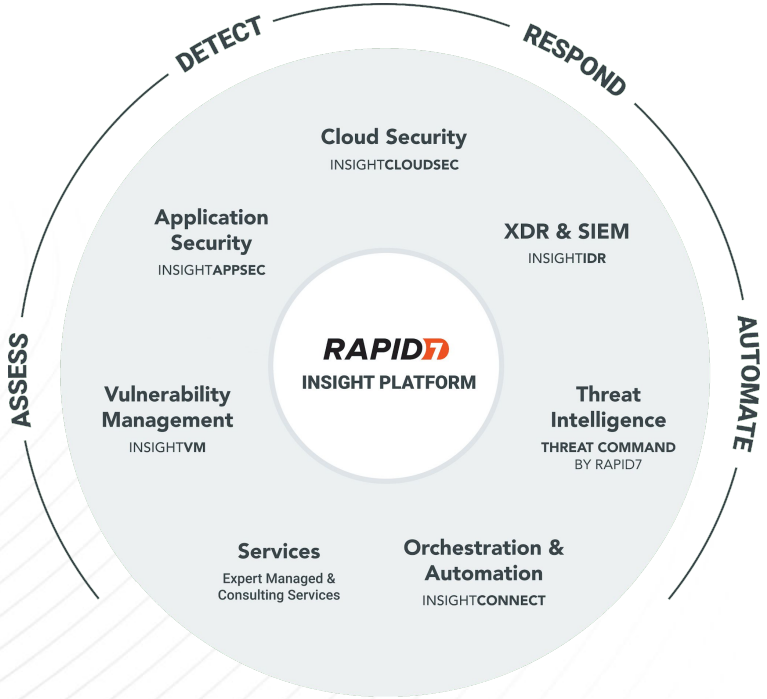
Global Footprint

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?


RAPID7
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.

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.

Threat Intelligence Platform - What does it do?

Extend Visibility

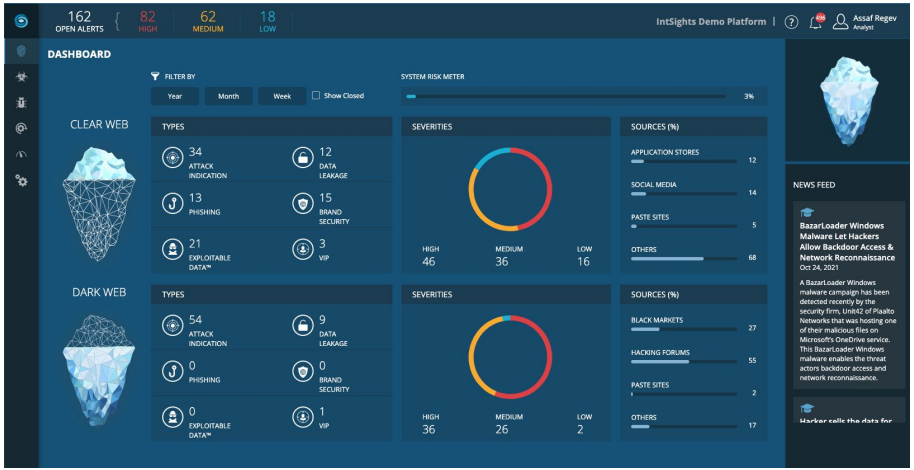
- Single-pane-of-glass visibility into external threats
- Proprietary collection & classification capabilities
- Operationalize and enrich intelligence

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

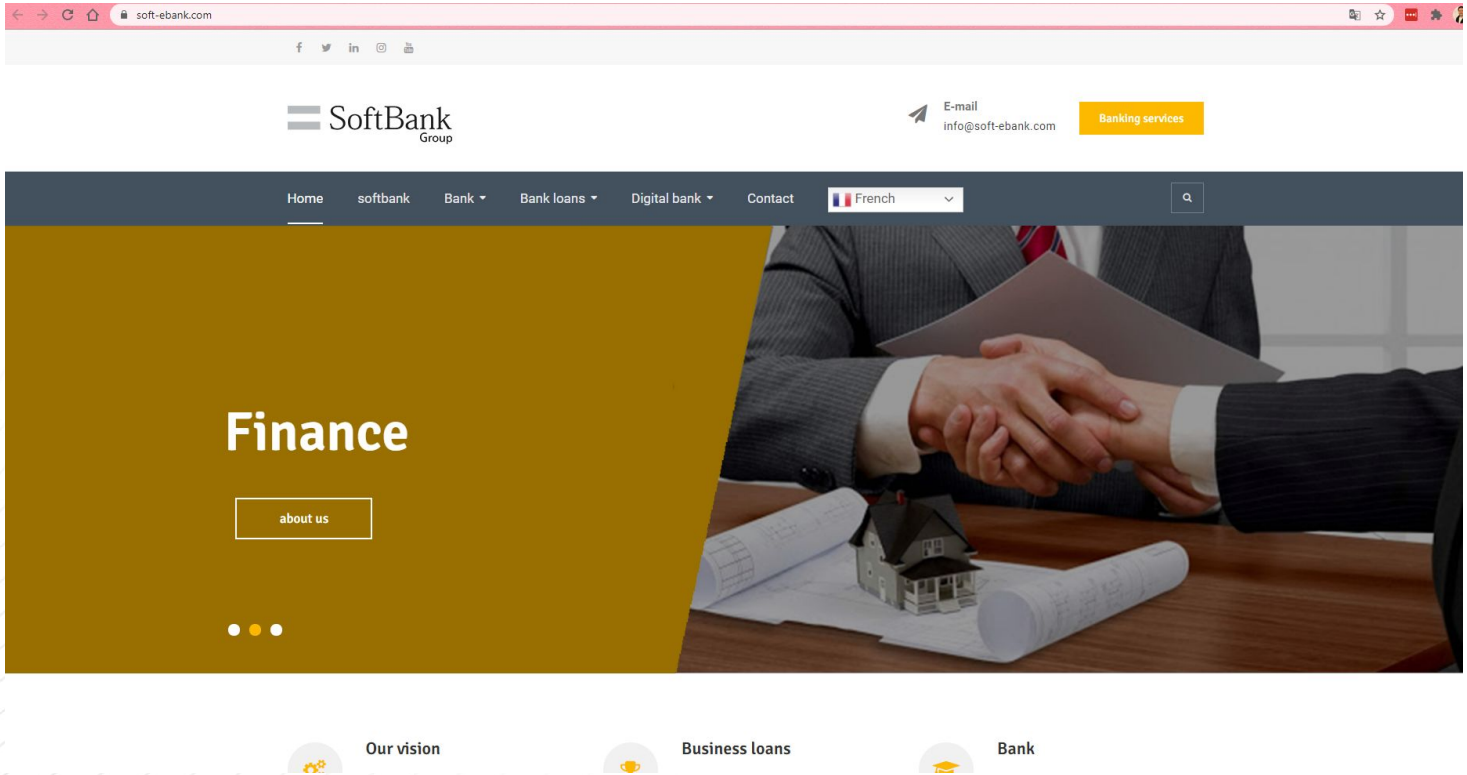
Use Cases

Where can CTI help me?

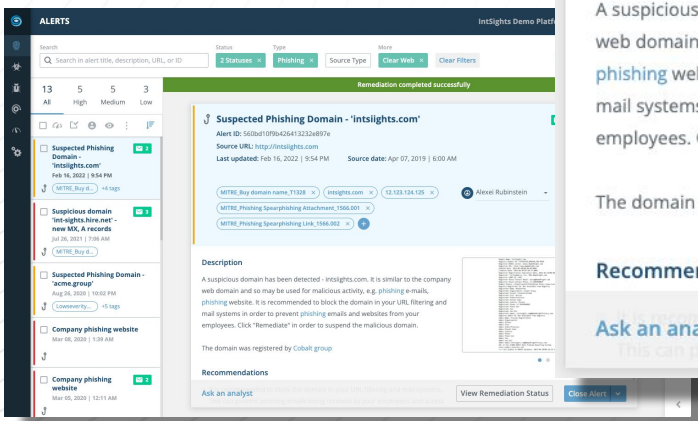
Phishing Domain – Example

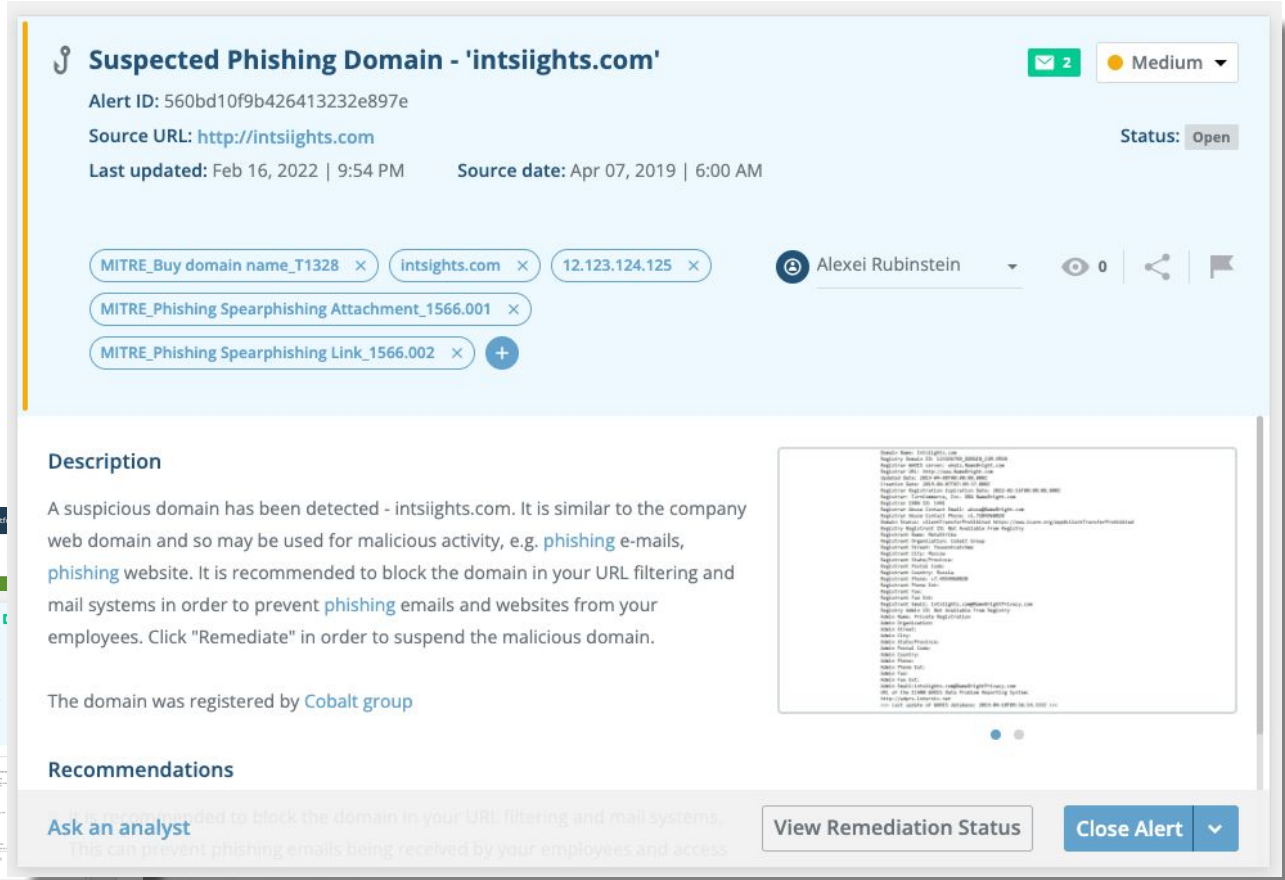
- A screenshot of a text message that Knab's clients received, asking them to visit 'knab-update.pro', which is a phishing domain (and website). The text says that their Knab banking app is expiring, and they need to register via this URL. This is also an example of smishing (phishing via SMS).
- This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

Phishing Website – Example



Phishing Alert





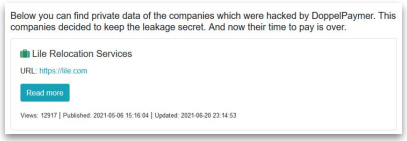
Use Case – Phishing

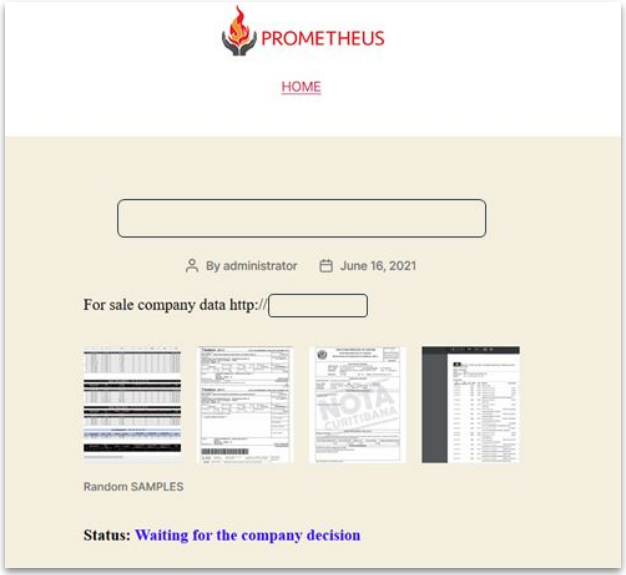
- Identification of Phishing domains and websites
- Research on dark web about planned phishing campaigns

Countermeasures

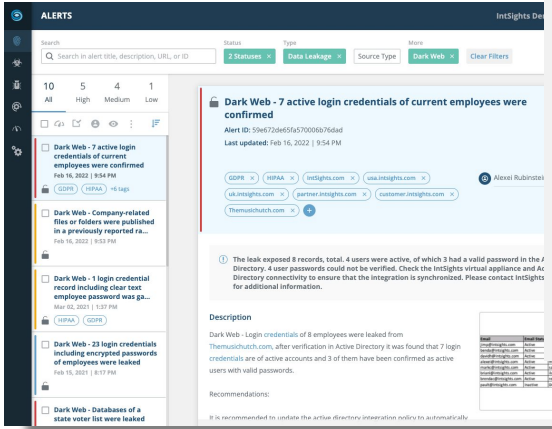
- Takedown of domain and websites (Remediation)
- Reporting to Phishing Trackers and lists
- Automation: block websites and domains in your firewall/gateway/proxy

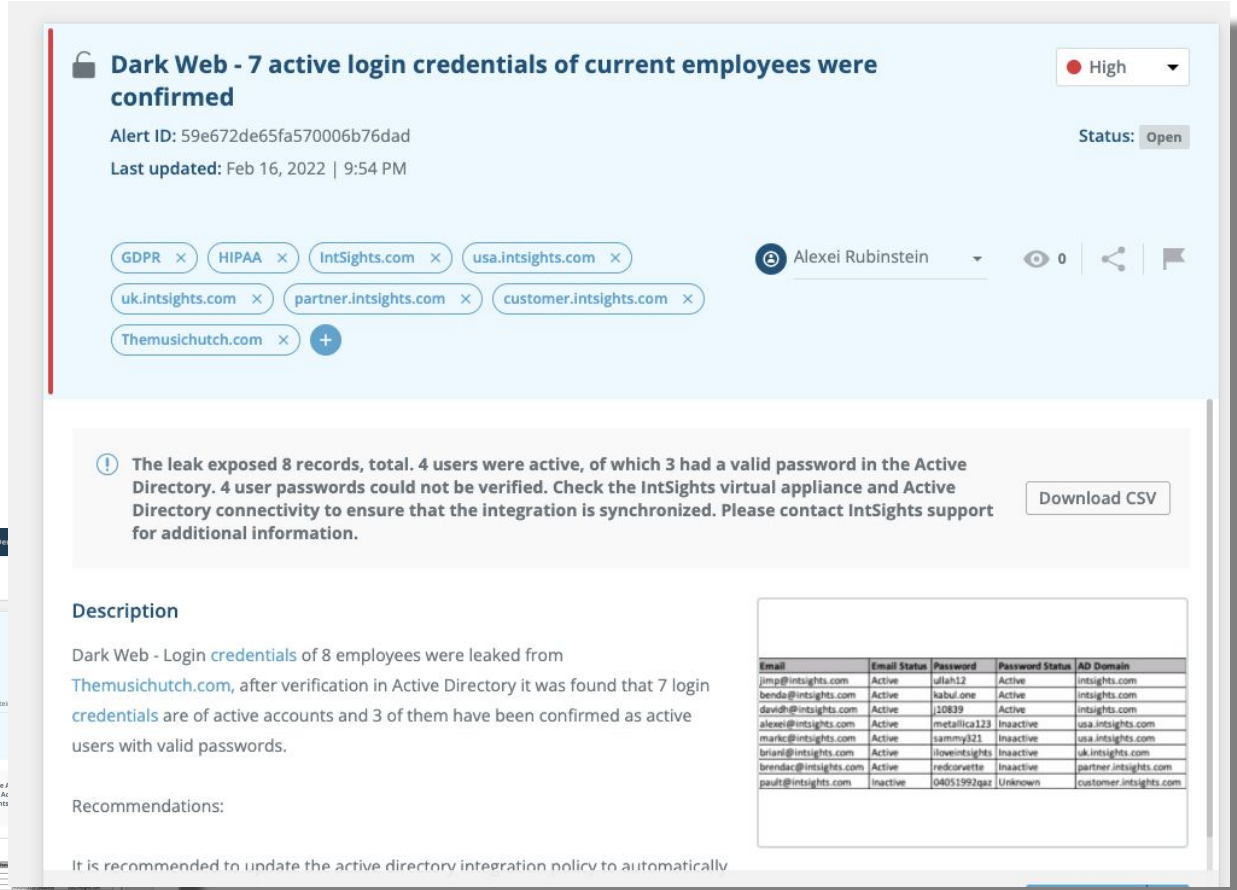
Ransomware - Double Extortion





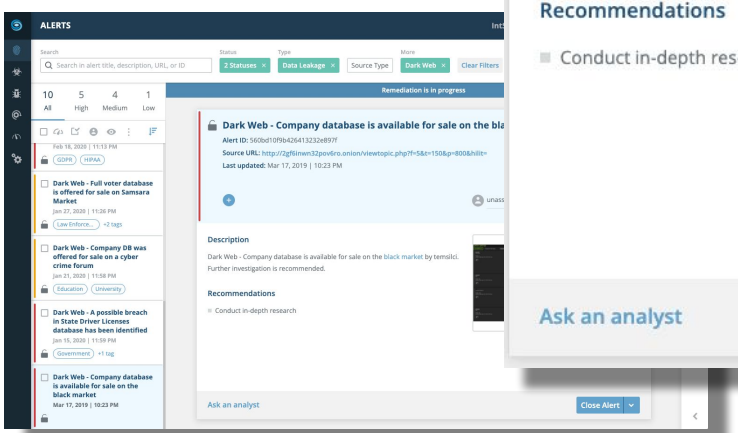
Leaked Credentials

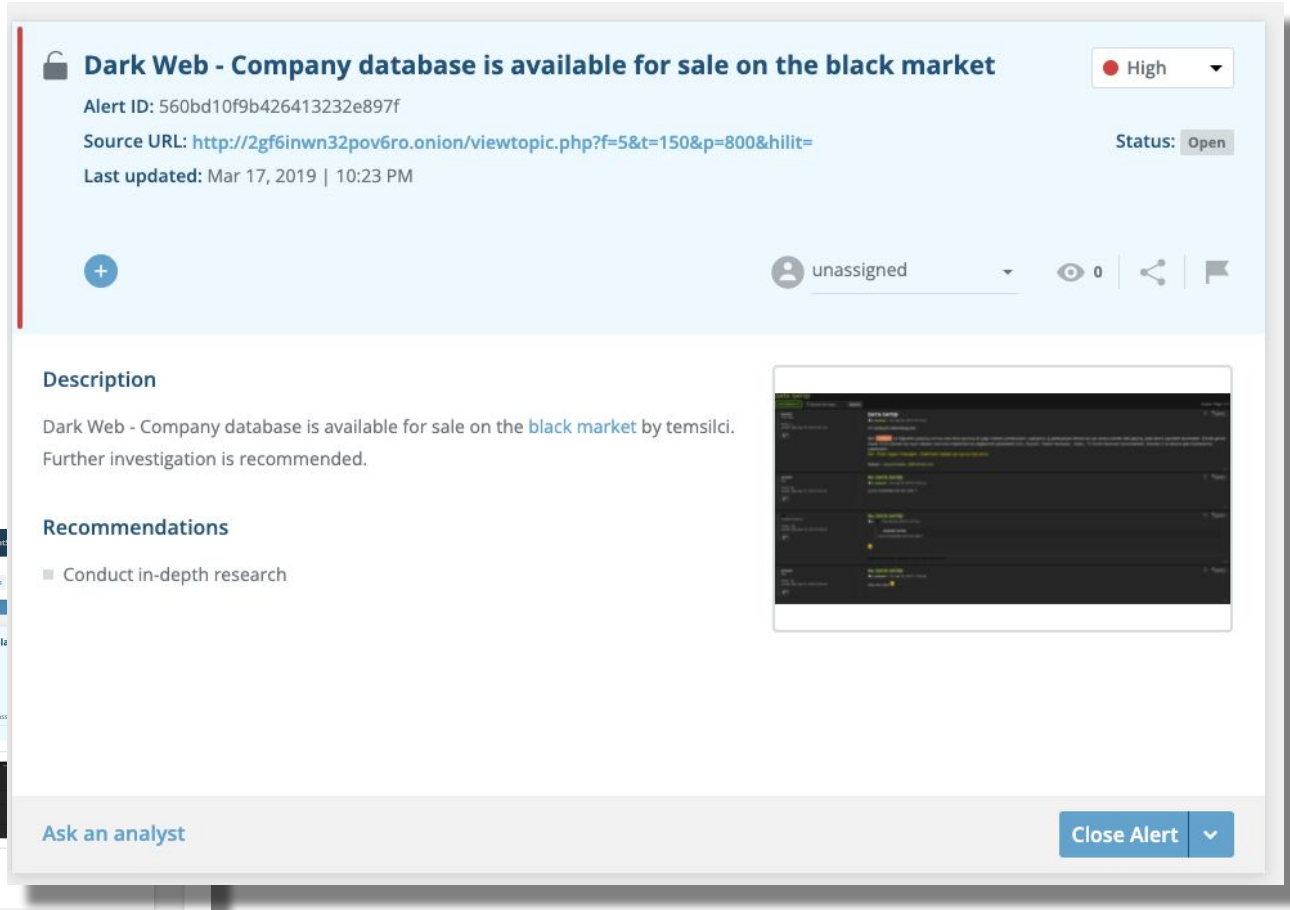




RAPID7

Leaked Data


ALERTS
Dark Web - Company database is available for sale on the bla
Description
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=
Status: Open
Last updated: Mar 17, 2019 | 10:23 PM
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

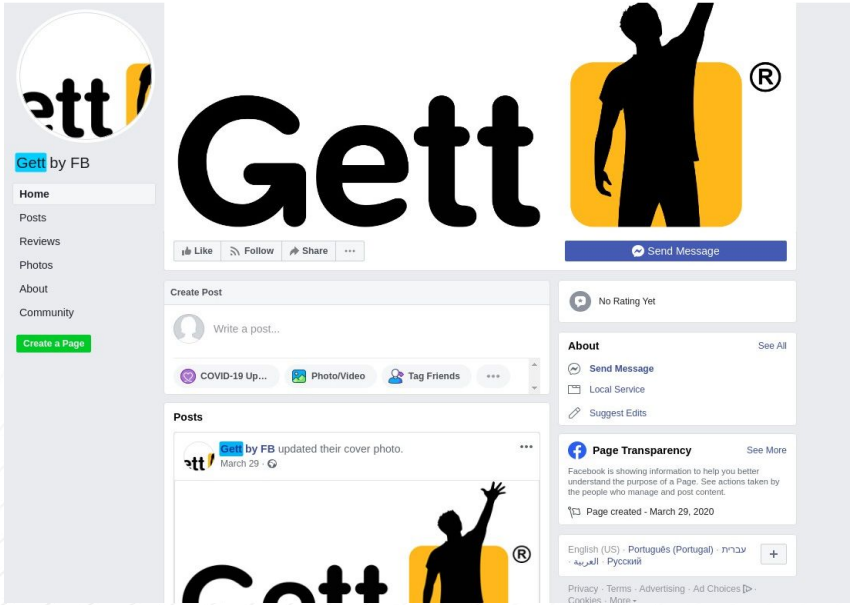
Countermeasures

- 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

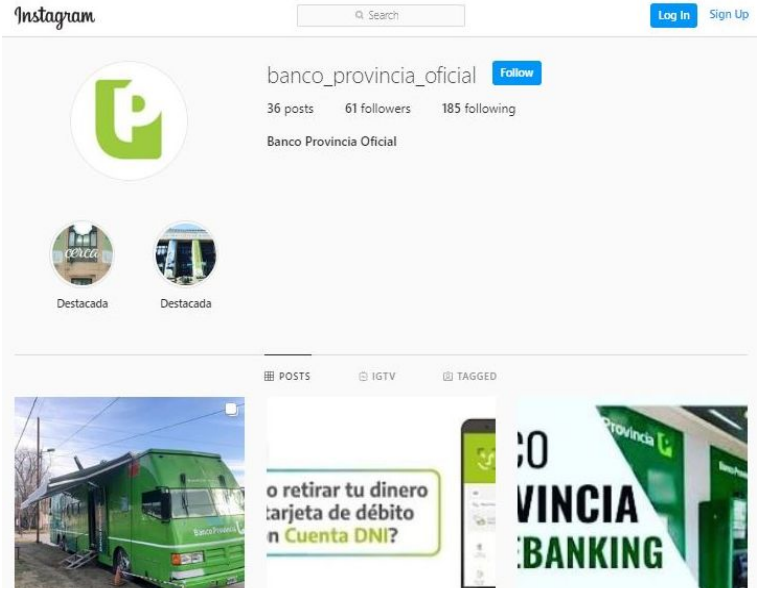
VIP Impersonations on Social Media

Masayoshi Son, SoftBank's CEO

IP Claims: Trademark/Copyright Infringements



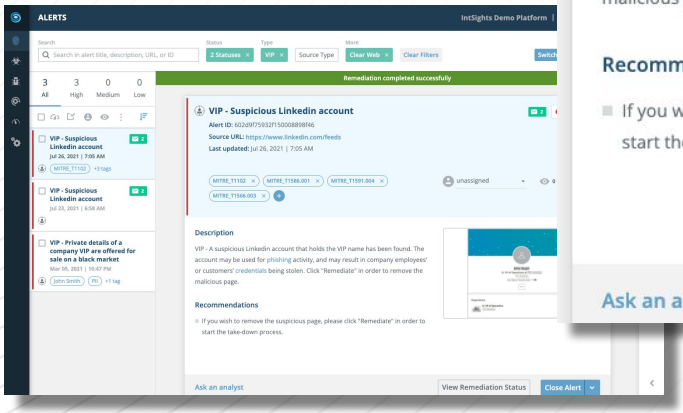
A Facebook page using Gett's logo

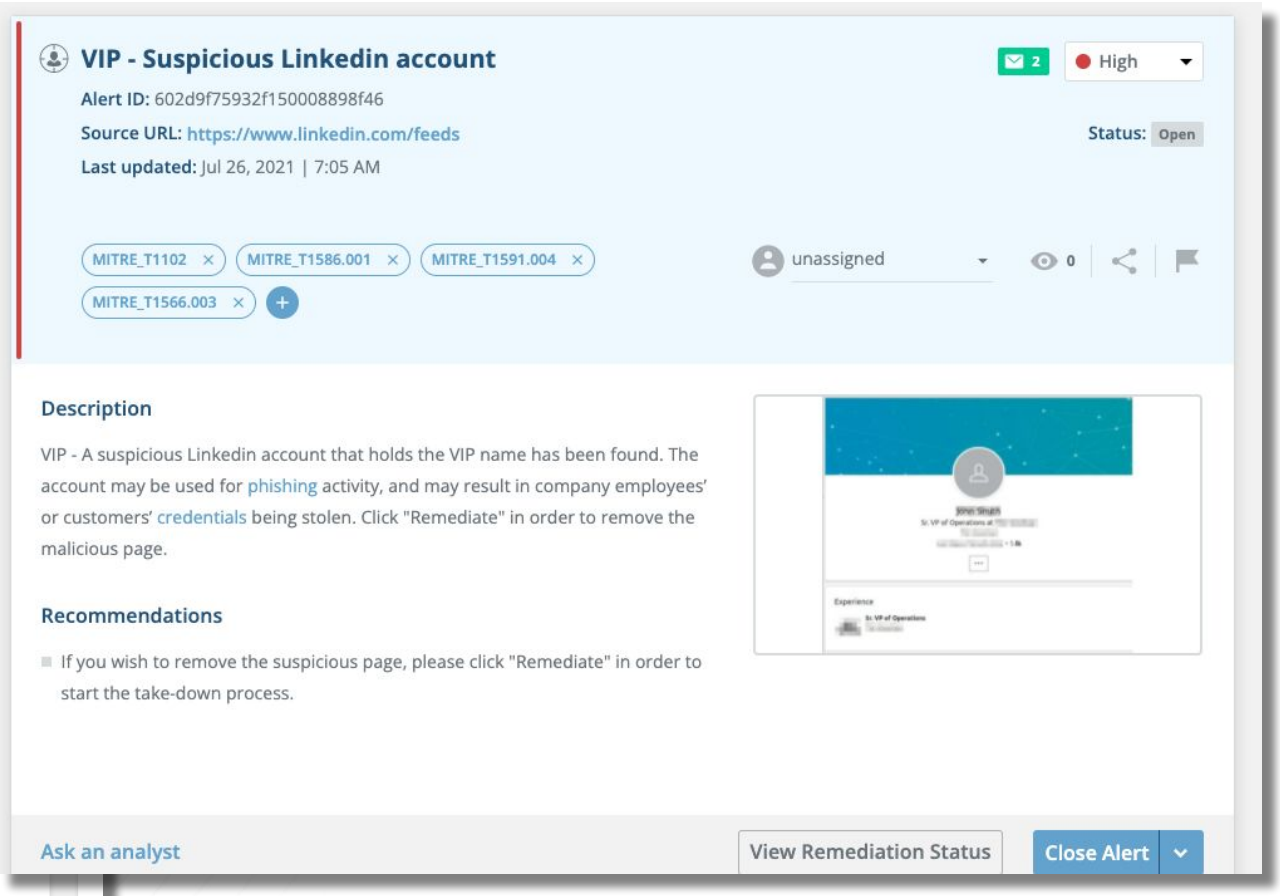


An Instagram account using Banco Provincia's name and logo and publishes fake posts.

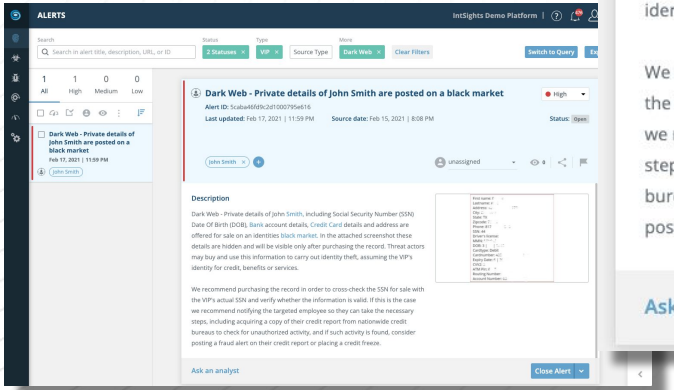
Find trademarks on WIPO

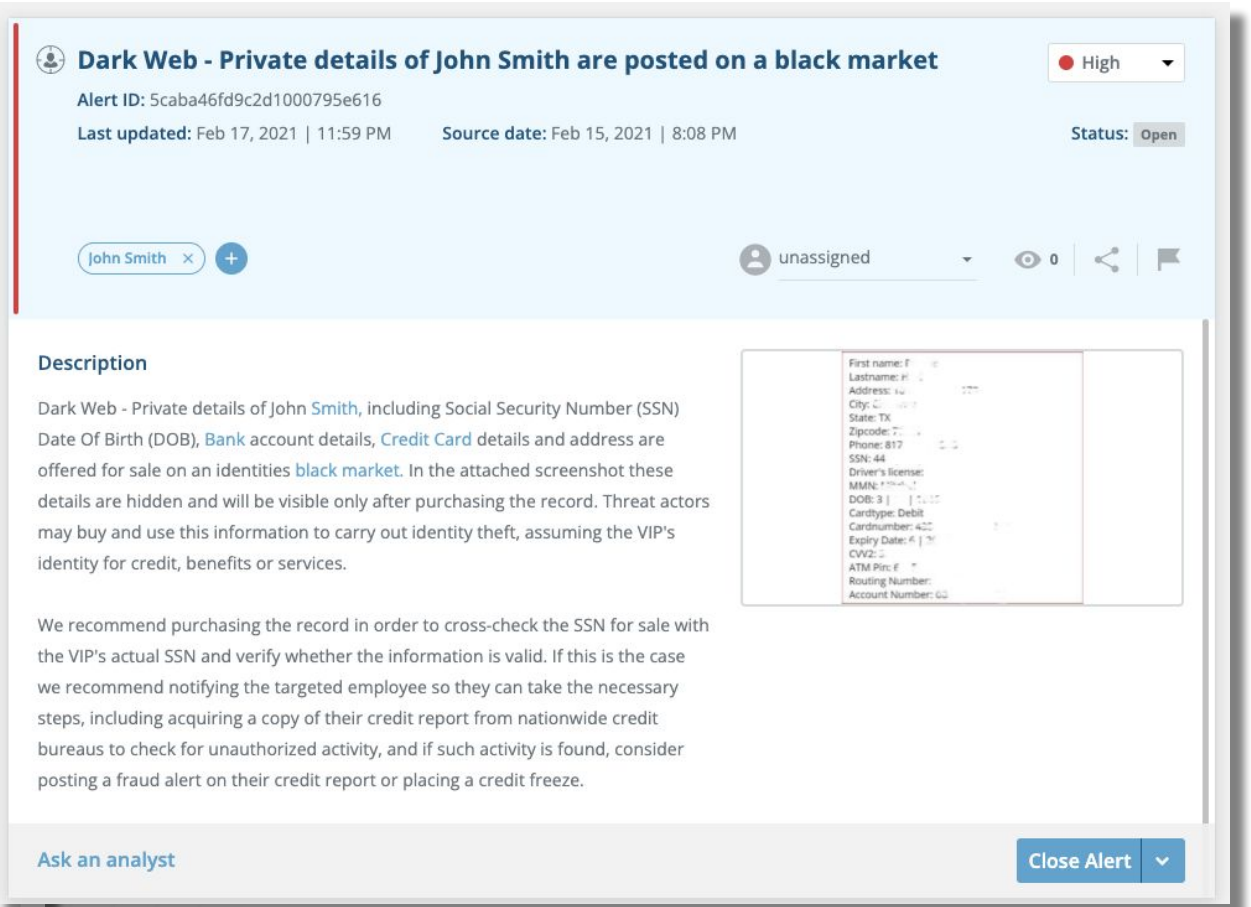
Fake Profile





VIP Data for sale





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/