



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 SOC's 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

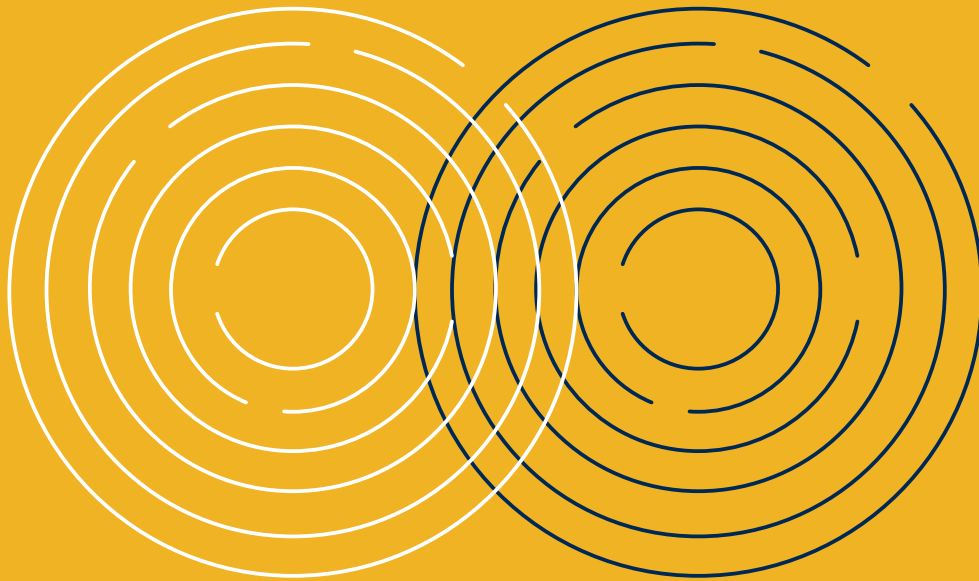
Offensive Security

- 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.



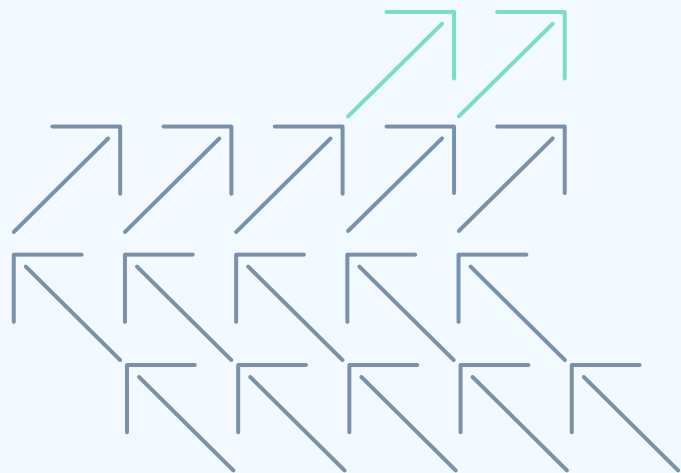
Proactive Threat Analysis

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.



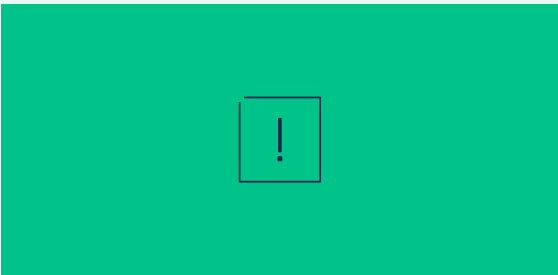
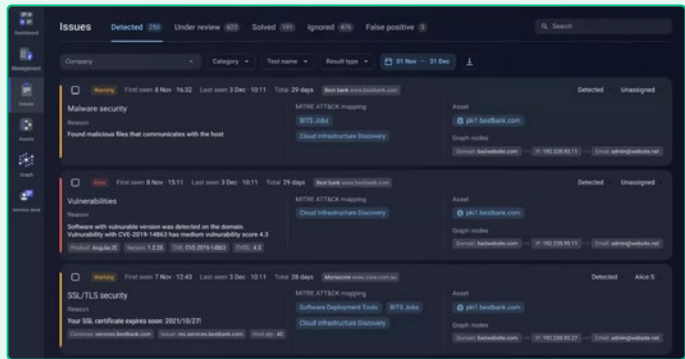
Stronger Security Posture

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

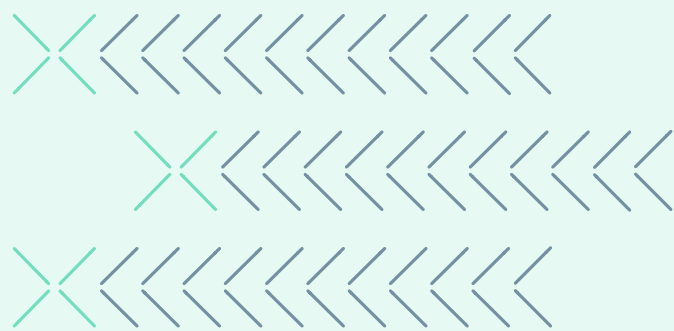


Attack Surface Management

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

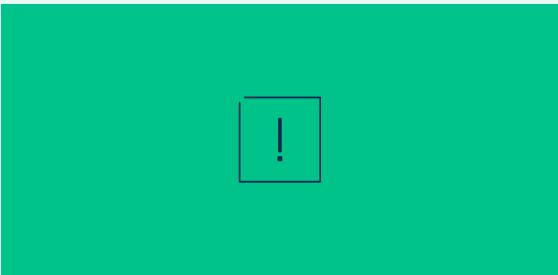
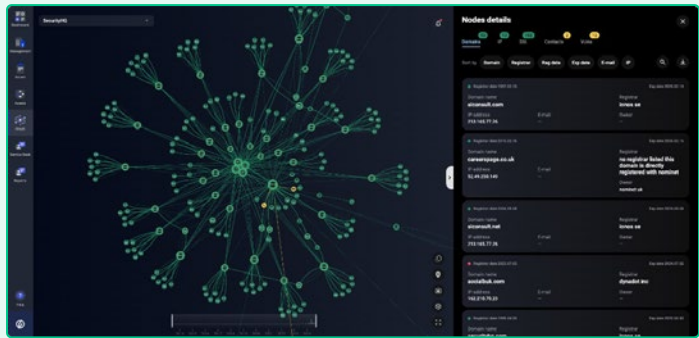


Vulnerable Services	Identify whether your organization is at risk from any vulnerabilities or incorrect configurations on your external attack surface.
Network Security	Identify open ports of remote administration services (RDP, SSH, VPN, etc), database ports, insecure service headers, open proxies or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



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

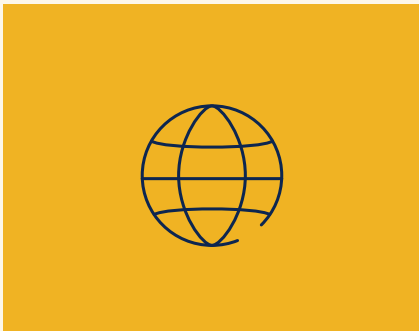
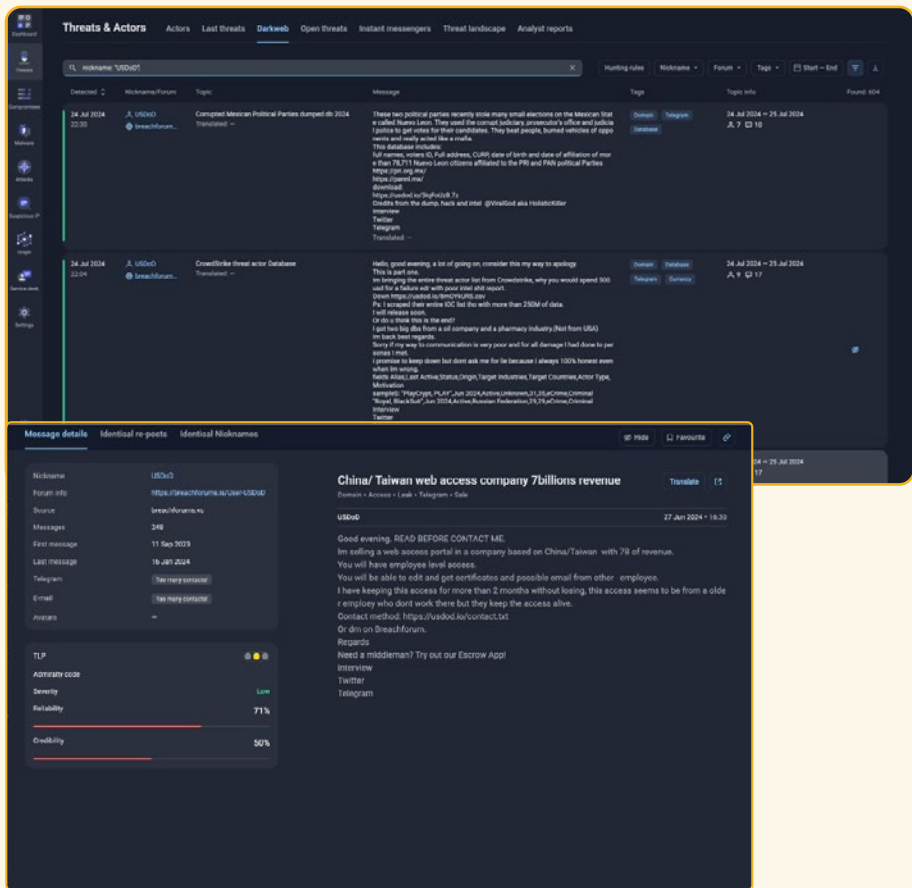
Threat Intelligence

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.

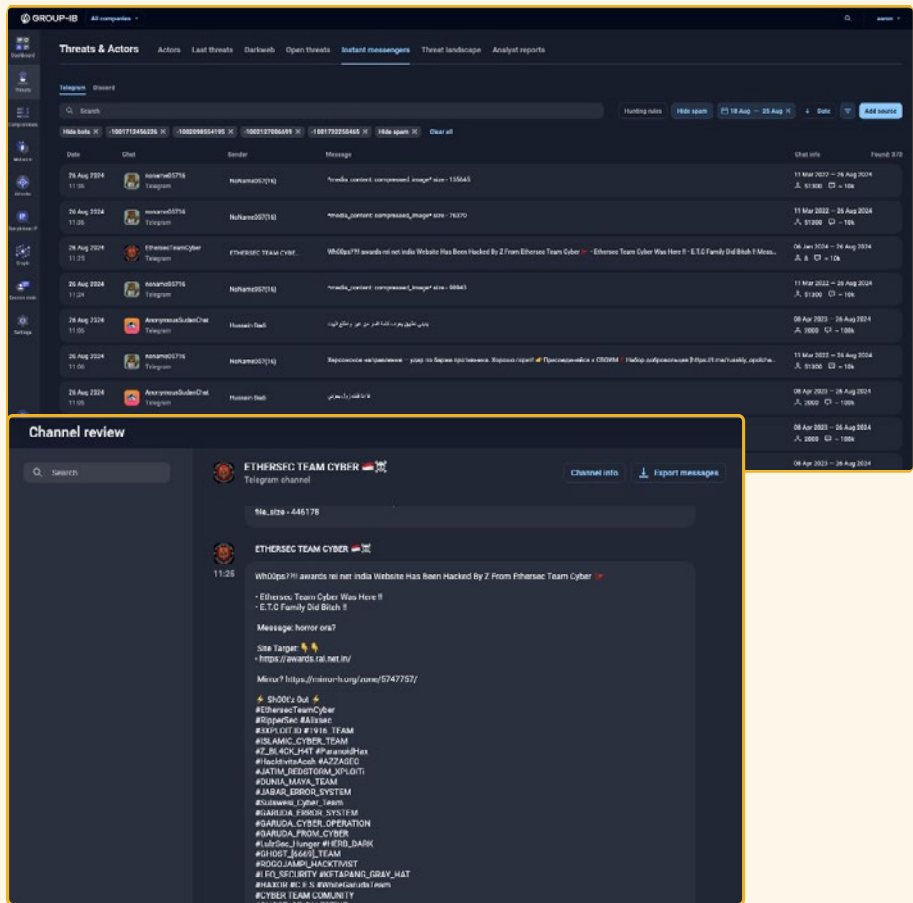


Leverage SecurityHQ’s Threat Intelligence Hunting rules to identify content posted on dark web forums.

- 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.

Threats & Actors									
Threats									
35628	Nation-State	2778	Cybercriminals	1588	Ransomware (SL)	21461	Match hunting rules		
Search									
Published 30 Jul 2024									
Clear all									
Anonymouse_KSA posted message containing data about possible attack targeting									
30 Jul 2024 - 30 Jul 2024	Anonymouse_KSA	Published 30 Jul 2024	Cybercriminals	General					
Cicada3301 Ransomware attack on Leach Lake Gaming Div									
30 Jul 2024 - 30 Jul 2024	Cicada3301	Published 30 Jul 2024	Cybercriminals	General					
Cicada3301 Ransomware attack on Leach Lake Gaming Div									
30 Jul 2024 - 30 Jul 2024	Cicada3301	Published 30 Jul 2024	Cybercriminals	General					
Cicada3301 Ransomware attack on Leach Lake Gaming Div									
30 Jul 2024 - 30 Jul 2024	Cicada3301	Published 30 Jul 2024	Cybercriminals	General					
Lululemon posted message containing data about possible attack targeting									
30 Jul 2024 - 30 Jul 2024	Lululemon	Published 30 Jul 2024	Cybercriminals	General					
Anonymouse_KSA posted message containing data about possible attack targeting									
30 Jul 2024 - 30 Jul 2024	Anonymouse_KSA	Published 30 Jul 2024	Cybercriminals	General					
Hunters International Ransomware attack on Texas Health And Human Services									
30 Jul 2024 - 30 Jul 2024	Hunters International	Published 30 Jul 2024	Cybercriminals	General					
Moroccan Black Cyber Army posted message containing data about possible attack targeting									
30 Jul 2024 - 30 Jul 2024	Moroccan Black Cyber Army	Published 30 Jul 2024	Cybercriminals	General					

APT41									
Info									
86	MITRE ATT&CK	267	Indicators	2886	Tools	72	Contacts	143	
Actor details									
Name APT41									
Alias BARIUM · Winnti · LEAD · WICKED SPIDER · WICKED PANDA · Blackfly · Suckfly +4									
First seen 27 Nov 2009									
Last seen 28 Feb 2023									
Attribution China									
Spoken languages Chinese									
Expertise tags Backdoor · Cobalt Strike · Windows +19									
Description									
A China-sponsored criminal group with dual attack goal (cyber espionage and financial benefit) that has been active since at least 2007.									
Area of interest									
APT41 specializes in stealing digital certificates for use in operations involving user data theft (cyber espionage), as well as placing cryptominers and ransomware on devices. Previously, the group's goals were also currency manipulation in online games and theft of intellectual property.									
Alternative names									
The network penetration operations are called WICKEDPANDA, while those related to financial gain are called WICKED SPIDER. In the Microsoft classification, attacks on the video game and technology industry are usually called BARIUM, and cyber espionage operations are called LEAD.									
C2 servers special character									
The second-level domains consonant with the name of the legitimate company were used with no routed localhost IP-address in the A-record when inactive. After that, a third-level domain was created, which resolved to the IP address of the attackers' server. At the same time, the address of the legitimate site of the company was used for the second-level domain, as the attackers were mimicking.									
Victims									
Geography Taiwan · South Korea · United States · India · Japan · China +48									



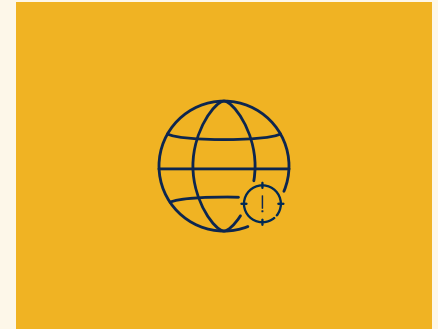
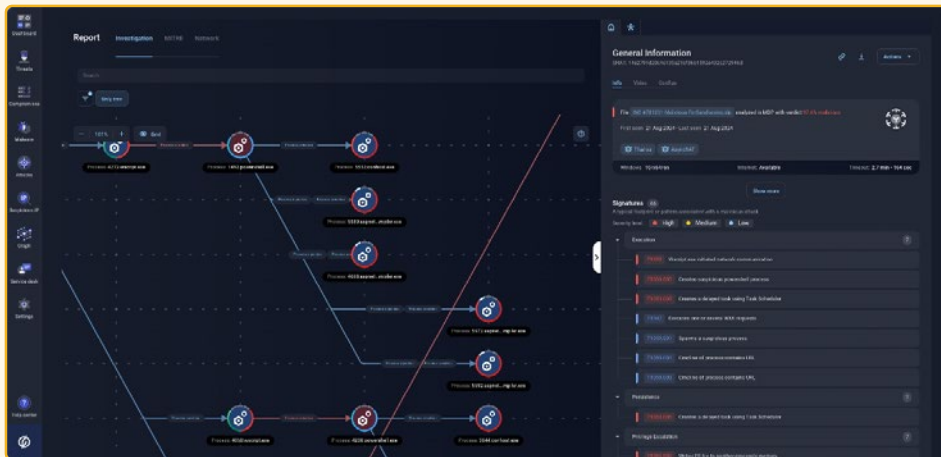
Leverage SecurityHQ's Threat Intelligence Hunting rules that concentrate on primary threats to your organization, utilizing a variety of attributes that include:

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



Malware Sandbox

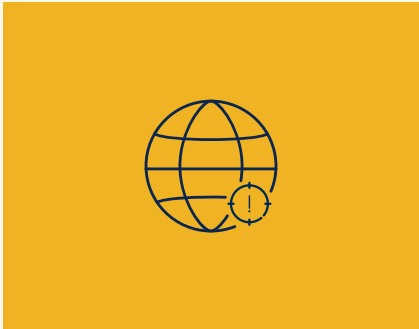
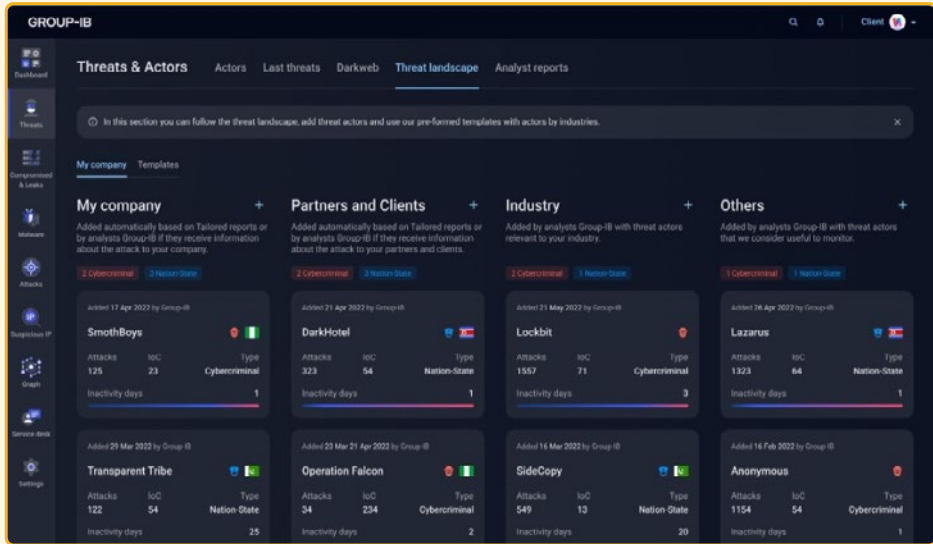
Gain access to a malware detonation sandbox to **analyze malicious code** in a controlled, isolated environment, offering comprehensive detection of various malware types. Generate detailed reports, **understand malware TTPs** and behavior in your environment.



- 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

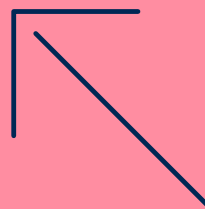


Sensor Network

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

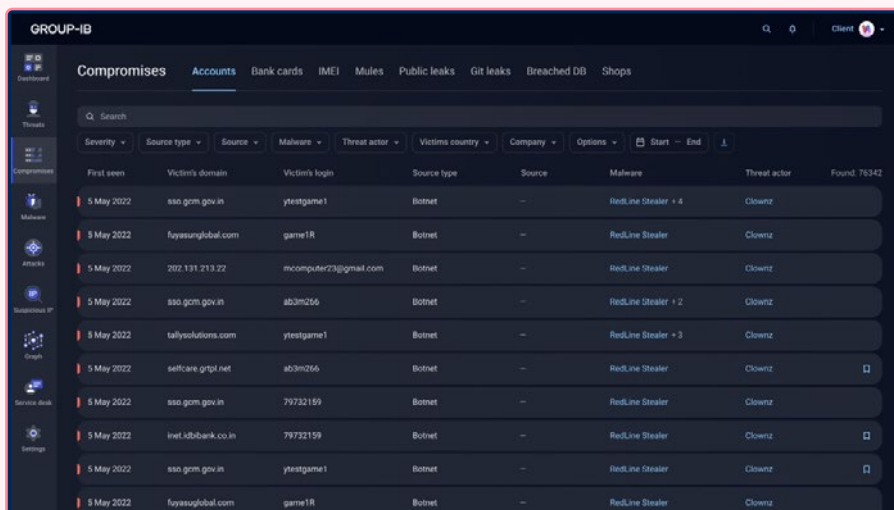
Digital Risk Protection

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 displays the Group-IB Threat Intelligence dashboard. The 'Compromises' tab is active, showing a table of compromised accounts. The table has columns for Severity, Source type, Source, Malware, Threat actor, Victims country, Company, Options, Start, End, and Found. The data shows several entries for compromised accounts, including victims like 'Victim's domain', 'Victim's login', and 'Source type', with threat actors like 'Botnet' and 'RedLine Stealer'.

Severity	Source type	Source	Malware	Threat actor	Victims country	Company	Options	Start	End	Found
First seen	Victim's domain	Victim's login	Source type	Source	Malware	Threat actor	Found	75342		
5 May 2022	aso.gom.gov.in	ytstgame1	Botnet	RedLine Stealer + 4	Clorenz					
5 May 2022	huyesunglobal.com	game1R	Botnet	RedLine Stealer	Clorenz					
5 May 2022	202.131.213.22	mcomputer23@gmail.com	Botnet	RedLine Stealer	Clorenz					
5 May 2022	aso.gom.gov.in	ab3m266	Botnet	RedLine Stealer + 2	Clorenz					
5 May 2022	tallysolutions.com	ytstgame1	Botnet	RedLine Stealer + 3	Clorenz					
5 May 2022	selfcare.grip.net	ab3m266	Botnet	RedLine Stealer	Clorenz					
5 May 2022	aso.gom.gov.in	79732159	Botnet	RedLine Stealer	Clorenz					
5 May 2022	inet.kdbibank.co.in	79732159	Botnet	RedLine Stealer	Clorenz					
5 May 2022	aso.gom.gov.in	ytstgame1	Botnet	RedLine Stealer	Clorenz					
5 May 2022	huyesunglobal.com	game1R	Botnet	RedLine Stealer	Clorenz					



- 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.

GROUP-IB

Compromises

Accounts

Bank cards

IMEI

Mules

Public leaks

Git leaks

Breached DB

Shops

Q Search

Severity Source type Source Malware Threat actor Victims country Company Options Start End

First seen	Victim's domain	Victim's login	Source type	Source	Malware	Threat actor	Found
5 May 2022	aso.gom.gov.in	ytestgame1	Botnet	—	RedLine Stealer + 4	Clowitz	79342
5 May 2022	huyesunghub.com	game1R	Botnet	—	RedLine Stealer	Clowitz	
5 May 2022	202.131.213.22	mcomputer23@gmail.com	Botnet	—	RedLine Stealer	Clowitz	
5 May 2022	aso.gom.gov.in	ab3m266	Botnet	—	RedLine Stealer + 2	Clowitz	
5 May 2022	tallysolutions.com	ytestgame1	Botnet	—	RedLine Stealer + 3	Clowitz	
5 May 2022	selfcare.grpt.net	ab3m266	Botnet	—	RedLine Stealer	Clowitz	
5 May 2022	aso.gom.gov.in	79732159	Botnet	—	RedLine Stealer	Clowitz	
5 May 2022	inet.kdbank.co.in	79732159	Botnet	—	RedLine Stealer	Clowitz	
5 May 2022	aso.gom.gov.in	ytestgame1	Botnet	—	RedLine Stealer	Clowitz	

Victim's domain: login.microsoftonline.com

TLP: AZ

Adversity code: High

Severity: 100%

Reliability: 80%

Source list (3)

Compromised: 27 Feb 2024 11:52

Detected: 06 Mar 2024 14:38

Source type: Stealer logs cloud

Source: @grapefruitcloud

Source link: -1307160756a815

Malware: RedLine Stealer

Compromised: 27 Feb 2024 11:52

Detected: 06 Mar 2024 21:05

Source type: Stealer logs cloud

Source: eazacoultopack0

Source link: -1307160756a814

Malware: RedLine Stealer

Compromised: 27 Feb 2024 11:52

Detected: 09 Aug 2024 15:01

Source type: Yu Net (stealer logs)

First seen: 18 Jan 2024 12:01

Last seen: 14 Aug 2024 20:08

Login: rsejncbaagroup.com

Password: Kuttin@2023

Login URL: https://login.microsoftonline.com/common/oauth2/v2.0/authz

Host information structured

Username: Francis Profile

Hardware ID: EYLWFKAAJZ1ETNN11EAKBHKUMJES

OS Details: Windows 10 Enterprise x64

OS Family: Windows 10

Country: KE

ZIP Code: UNKNOWN

Screen Resolution: 1366x768

Time Zone: UTC+03:00

System Locale: English (United States)

Malware Location: C:\Windows\Microsoft.NET\Framework\v4.0.30319\jav.exe

Stealer Build: @GOODELESS

Host information unstructured

IP: 41.88.512.550

OS: Windows 10

Process ID: 1116

Process Name: explorer.exe

Log date: 02/27/2024 11:52:33

Host: Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 2 Core

Mem: 1 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 2 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 3 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 4 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 5 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 6 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 7 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 8 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 9 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 10 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 11 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 12 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 13 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 14 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 15 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 16 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 17 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 18 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 19 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 20 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 21 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 22 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 23 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 24 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 25 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 26 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 27 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 28 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 29 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 30 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 31 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 32 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 33 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 34 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 35 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 36 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 37 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 38 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 39 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 40 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 41 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 42 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 43 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 44 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 45 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 46 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 47 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 48 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 49 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 50 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 51 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 52 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 53 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 54 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 55 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 56 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 57 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 58 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 59 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 60 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 61 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 62 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 63 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 64 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 65 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 66 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 67 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 68 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 69 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 70 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 71 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 72 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 73 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 74 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 75 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 76 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 77 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 78 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 79 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 80 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 81 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 82 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 83 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 84 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 85 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 86 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 87 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 88 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 89 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 90 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 91 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 92 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 93 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 94 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 95 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 96 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 97 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 98 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 99 - Intel(R) HD Graphics 620, 163746328 bytes

Mem: 100 - Intel(R) HD Graphics 620, 163746328 bytes

- 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.

For more details visit: www.securityhq.com
Contact us: www.securityhq.com/contact
Email: sales@securityhq.com

Social Media:

[in](#) [X](#) [v](#) [f](#)

Threat & Risk Intelligence: 24/7 Managed Service

©2024 Copyright SecurityHQ

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.**

Compromises									
Accounts Bank cards IMEI Mules Public leaks Git leaks Breached DB Shells									
Search									
My own filters Type Data found Keywords Start - End									
aws_access_key_id password api_key api_key High									
First seen	Source	Data found	Rules	Contributors	Email	File	Found		
01 Jun 2024	https://github.com/Department-for-Transport/Transport-for-London...	aws_access_key_id +1	Go North West	Alana Jaffer +7	#123787@transportforlondon... +7	81			
01 May 2024	https://github.com/real-ty-data/info	aws_access_key_id +1	Littlebury	antidragon +17	anthonyvalent@gmail.co... +17	77			
21 Apr 2024	https://github.com/gigadownload/ghosties.org	aws_access_key_id +1	Go North West	AngryBurntweed +1	ang@passio.net +1	30			
27 Jan 2024	https://github.com/veryangpaleon/consort	api_key +1	Leidrebus	Jack-Jack Strigel	antonyng@gmail.com	154			
22 Feb 2023	https://github.com/rodrigo19/Windows-8.1-BitLocker-Fix	begin rsa private +1	Marek Tarnowski	Begin13	begin13@gmail.com	235			
23 Dec 2022	https://github.com/3602/cutemask	begin rsa private +1	Marek Tarnowski	Boltemark +1540	Boltemark@gmail.com +1540	222			
02 Nov 2022	https://github.com/T3R45T3R32/keccak-ask	begin rsa private +1	Marek Tarnowski	dergipen	139229592@qq.com	166			
30 Aug 2022	https://github.com/gigadownload/ask	begin rsa private +1	Marek Tarnowski	Boltemark +1511	Boltemark@gmail.com +1511	228			
28 Jul 2022	https://github.com/Phap-Lu/faceidgit	password +1	Marek Tarnowski	big +3	94009929+773222@users.n... +3	39			
09 Aug 2021	https://github.com/leleup/leleupask.git	begin rsa private +1	Marek Tarnowski	Alexandre Piquere +11	alexandre.leleup@leleup... +11	168			
04 Aug 2021	https://github.com/leleup/leleupask.git	begin rsa private +7	Marek Tarnowski	Boltemark +184	Boltemark@gmail.com +184	181			
04 Aug 2021	https://github.com/gigadownload/ask	password +1	Marek Tarnowski	elguyte +16	elguyte@5134074388... +16	163			
30 Jul 2021	https://github.com/leleup/leleupask	secretkey +7	Marek Tarnowski	Boltemark +111	Boltemark@gmail.com +111	163			



- 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.

Compromises

Accounts

Bank cards

IMEs

Mobex

Public leaks

Git leaks

Breached DB

Shops

Search

Source

Match hunting rules

AI

First seen	Last seen	Source	Title	Data found	Risk	Found 12
29 Aug 2023	29 Aug 2023	https://pastebin.com/5qcdy9s	Anonymous #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
28 Feb 2022	20 Feb 2022	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
19 Feb 2022	19 Feb 2022	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
19 Feb 2022	19 Feb 2022	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
21 Jan 2022	21 Jan 2022	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
11 Nov 2021	11 Nov 2021	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
30 May 2021	30 May 2021	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
31 Mar 2020	31 Mar 2020	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
28 Mar 2020	28 Mar 2020	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	
29 Feb 2020	29 Feb 2020	https://pastebin.com/5qcdy9s	Anonymous JTSEC #OpKiluminati JTSEC Full Recon #9	[REDACTED]	High	

Source: https://x2F/pastebin.com/5qcdy9s

TLP

Admiralty code

Severity

Reliability

Credibility

High

50%

50%

Code preview

Hostname glquebec.org ISP iWeb Technologies Inc. Continent North America Flag CA Country Canada Country Code CA Region Quebec Local time 25 Sep 2019 14:53 EDT City Montreal Postal Code H0S IP Address 174.142.35.172 Latitude 45.459 Longitude -73.55

Source list

Title

Anonymous #OpKiluminati JTSEC Full Recon #9

URL

https://pastebin.com/5qcdy9s

Author

JTSEC1333

Published

25 Sep 2019



- 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 Databased	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

