SEARCHLIGHT. CYBER

YOUR PRODUCT GUIDE TO DEFEATING CRIMINALS ON THE DEEP AND DARK WEB

Searchlight Cyber is proven to defend organizations against ransomware groups, identify criminals in the pre-attack phase, and unmask high-risk threat actors in criminal investigations.

GATHER EVIDENCE ON THREAT ACTORS

Securely investigate high-risk actors to enhance your cyber posture and unmask criminals

EMPOWER YOUR TEAM WITH CUTTING-EDGE AUTOMATED TECHNOLOGY AND DATA

Empower your cybersecurity teams to securely and intuitively detect and track threat actors on the dark web – without exhausting your manpower.

SEARCH

REFINE 4 ACTIONS

- ☑ **4 Credential Actions**
  - ☑ 1 Ransomware Action
  - ☑ 3 Credentials on Markets
  - ☑ 0 Creden
  - ☑ 0 Creden
  - ☑ 0 Creden
  - ☑ 0 Creden
- ☑ 1 Traffic Actio
- ☑ 2 Network Ac
- ☑ 0 Phishing Ac

🔺 DARK WEB TRAFFIC

Apr 27   Apr 30   May 03   May 06   May 09   May 12

MING TRAFFIC   ● OUTGOING TRAFFIC

CREATE RANSOMWARE GROUP ALERT

Ransomware Group is a Ransomware-as-a-Service (RaaS) operation which targeted organizations in a number of industries and regions. Following its identification in 2020, **Ransomware Group** became one of if not the most prolific ransomware operations in history.

Last active on:
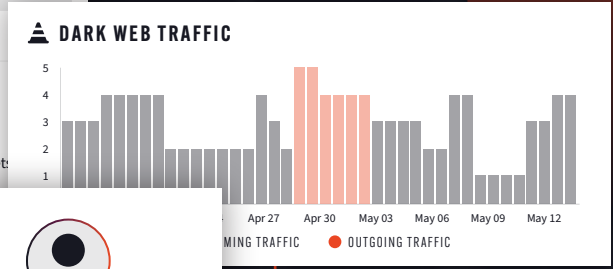20th May 2023 19:23

First active on:
29th September 2020 10:11

Actor profiles:
Actor One

VICTIMS BY GEOGRA

500

THREAT ACTOR
RANK: N/A
REPUTATION: N/A

⚠ ALERT	🔖 BOOKMARK	➕ CASE

SITE:	XSS
REGISTERED:	UNKNOWN
TOTAL POSTS:	2
PRIMARY CATAGORY:	UNKNOWN
FIRST SEEN:	MAY 11TH 2021
LAST SEEN:	MAY 12TH 2021
OSINT:	0
PGP KEYS:	0
POSSIBLE LINKED VENDORS:	N/A
POSSIBLE LINKED FORUM AUTHORS:	N/A

PASSWORD ON DARK WEB FORUM

🕐 14th June 2023   ⚠ High Priority   🗒 Exploit

We found leaked passwords from your supply chain partner XXXX on a dark we

SPOT SUSPICIOUS DARK WEB TRAFFIC TO YOUR NETWORKS

Get visibility into dark web traffic to and from your network, a key indicator of malicious activity.

INVESTIGATE CRIMINALS ON THE DARK WEB

Access previously unobtainable live and historic dark web activity.

MONITOR FOR RISKS ACROSS ALL YOUR DIGITAL ENVIRONMENTS

Be the first to know when criminals target your organization and its supply chain with automated alerts.

CRIMINALS USING THE DARK WEB THINK YOU CAN'T SEE THEM, WITH SEARCHLIGHT YOU CAN

IF YOU WERE GIVEN ADVANCE WARNING OF A CYBER ATTACK, WOULD YOU ACT ON IT?

Sadly, criminals don't send courtesy emails before they commit serious cybercrimes or breach your network. But if you know where to look, you can identify threat actors before they strike - at the beginning of the Cyber Kill Chain.

That's the power of pre-attack intelligence from the deep and dark web.

TWO USE CASES, ONE MISSION:
TO PROTECT SOCIETY FROM DARK WEB THREATS

ENTERPRISE & GOVERNMENT ORGANIZATIONS

- Automatically monitor for dark web threats
- Receive tailored pre-attack threat alerts
- Mitigate threats and report on your impact

LAW ENFORCEMENT & INTELLIGENCE COMMUNITY

- Investigation tools for any skill level
- Gather dark web intelligence to build a case
- Uncover criminal activity on the dark web

STRIKE BACK AGAINST THREAT ACTORS AND CRIMINALS GROUPS

With pre-attack intelligence, you can flip the script and proactively spot the reconnaissance activity and hidden communication of cyber criminals on marketplaces, forums, and hidden chats. By shifting left in the Cyber Kill Chain, you can spot threats earlier in the MITRE ATT&CK timeline - while criminals are still in the reconnaissance phase. At the other end of the scale, Searchlight's data lake of previously unobtainable live and historic dark web data gives incident response and criminal investigation teams access to critical data you can use to defend against past, present, and future threats.

MITRE ATT&CK TIMELINE

| RECONNAISSANCE | RESOURCE DEVELOPMENT | INITIAL ACCESS | EXECUTION | PERSISTENCE | PRIVILEGE ESCALATION | DEFENSE EVASION | CREDENTIAL ACCESS | DISCOVERY | LATERAL MOVEMENT | COLLECTION | COMMAND AND CONTROL | EXFILTRATION | IMPACT |

MONITOR // **Pre-attack intelligence**
Shift left, identify threats, and take action before an attack has started.

INVESTIGATE // **Criminal investigation**
Access critical intelligence to disrupt criminals and facilitate post-breach remediation.

GAIN THE TACTICAL ADVANTAGE

LEARN MORE ABOUT OUR AWARD-WINNING DARK WEB INVESTIGATION AND MONITORING TOOLS.
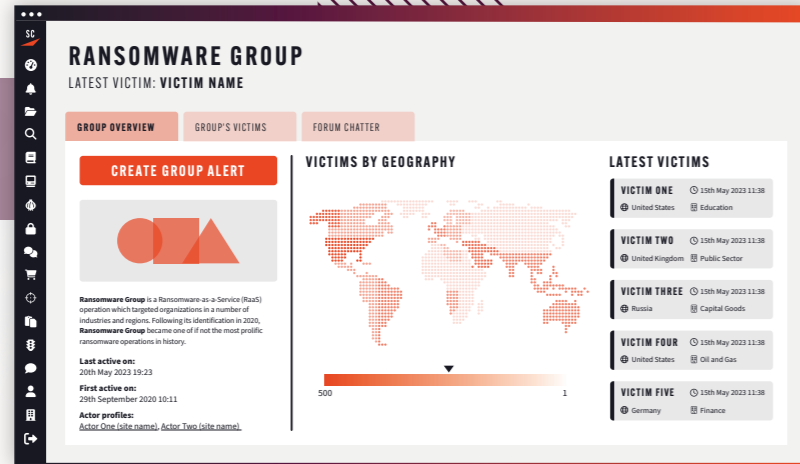
HOW IT WORKS

INVESTIGATE & PIVOT ON HIDDEN THREATS

Identify, gather, and preserve evidence on ransomware, criminal, and threat group activity.
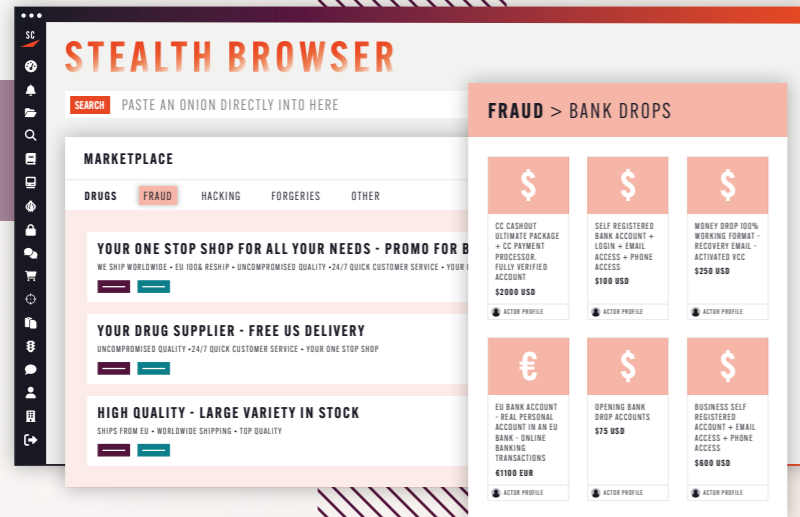
SEARCH & INVESTIGATE RANSOMWARE GROUPS

Access continuously updated intel on the latest tactics, known gang members, and victims.

DARK WEB VIRTUAL MACHINE

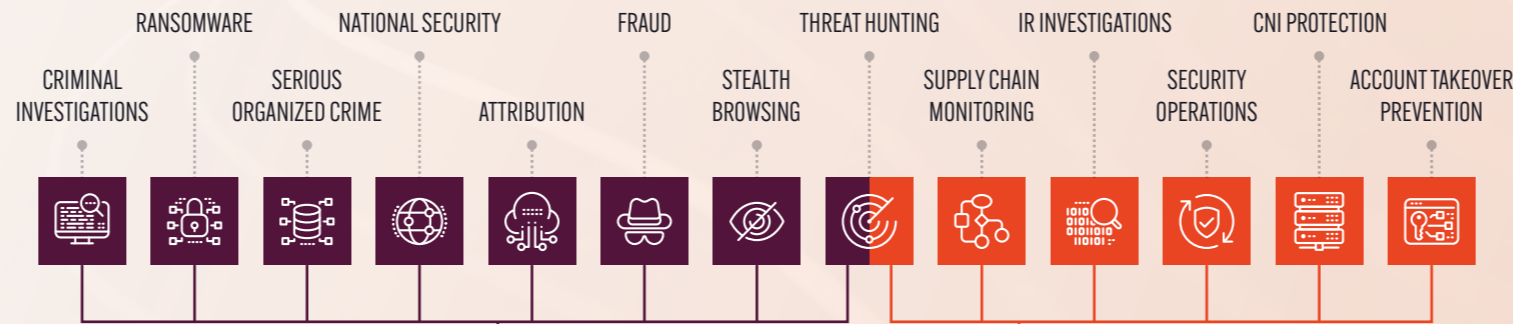Explore Tor and I2P onions knowing your identity and network are protected.

CERBERUS

The world's most powerful dark web search and investigation platform. Give your cyber teams access to previously unobtainable live activity and over 15 years of archived dark web data.

DARKIQ

Automatically monitor for dark web risks across all your digital environments, so you can spot threats earlier and prevent attacks.
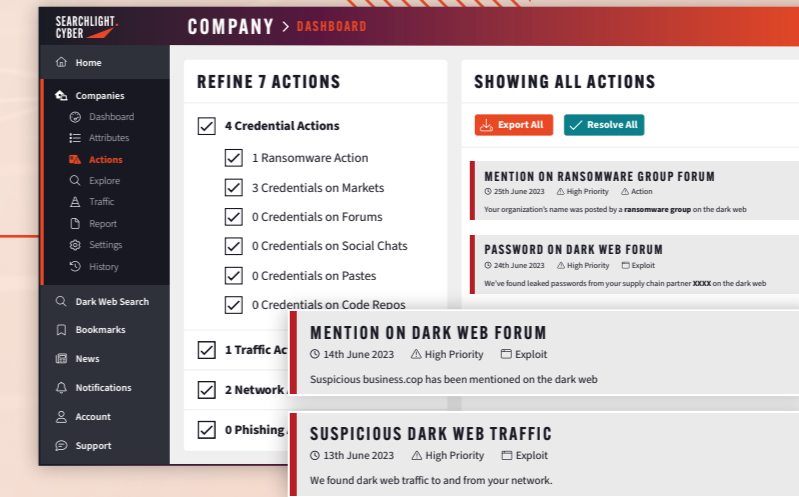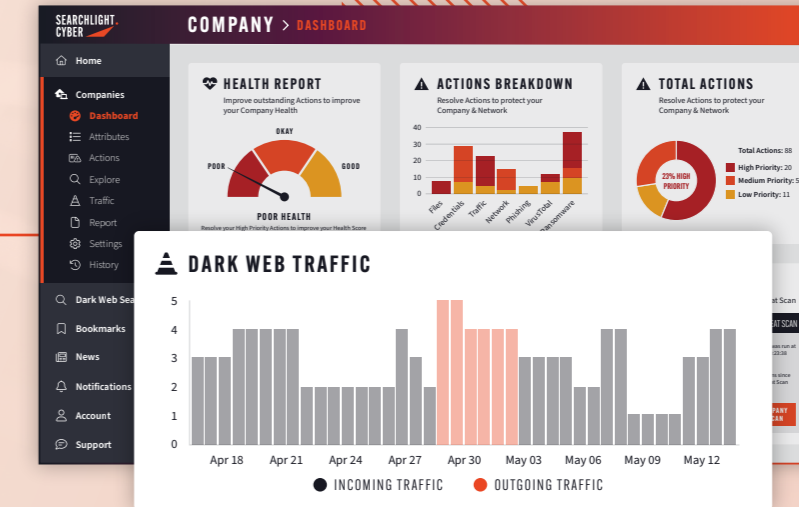
MONITOR CLOSED SOURCES

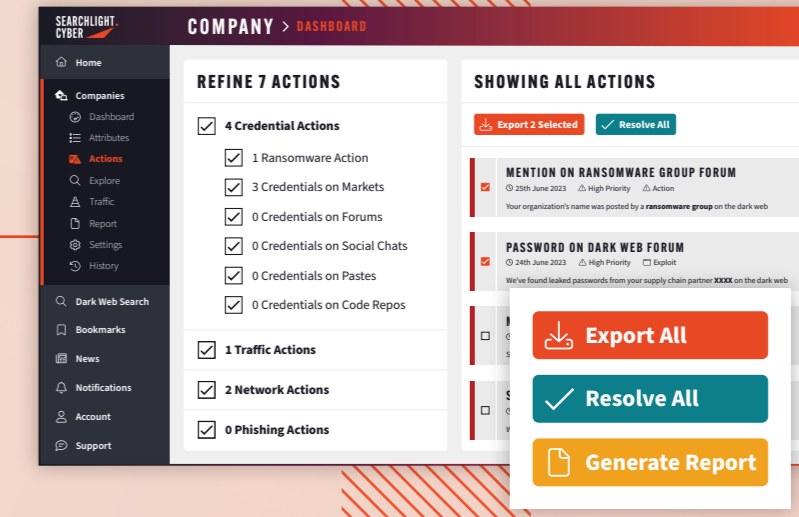Receive actionable alerts about specific threats to your organization and its supply chain.

ENRICH YOUR THREAT INTEL

Monitor dark web traffic to and from your network and integrate our API with your SIEM.

TAKE ACTION AND REPORT

Focus on imminent threats and create one-click reports to prove your team's impact.

RANSOMWARE · NATIONAL SECURITY · FRAUD · THREAT HUNTING · IR INVESTIGATIONS · CNI PROTECTION

CRIMINAL INVESTIGATIONS · SERIOUS ORGANIZED CRIME · ATTRIBUTION · STEALTH BROWSING · SUPPLY CHAIN MONITORING · SECURITY OPERATIONS · ACCOUNT TAKEOVER PREVENTION

CERBERUS: INVESTIGATIONS

DARKIQ: MONITORING & INTELLIGENCE

SEARCHLIGHT PLATFORM

THE DARK WEB

FORUMS · PASTE SITES · TRAFFIC · MARKET PLACES · CHATS · ONION SITES · LEAKS

ACCESS PREVIOUSLY UNOBTAINABLE DEEP AND DARK WEB DATA.

RAPID DEPLOYMENT, RAPID DARK WEB INSIGHTS

Give your cybersecurity team secure access to the most cutting-edge technology and data, enabling them to detect and track threat actors on the dark web.

PROPRIETARY DARK WEB TECHNOLOGY	**INTUITIVE USER INTERFACE**	**INVESTIGATE LIVE AND HISTORIC DARK WEB DATA**
SAFEGUARD ALL YOUR DIGITAL ASSETS	**DRILL INTO A CRIMINAL'S ACTIVITY AND MODUS OPERANDI**	**COMPLY WITH SECURITY STANDARDS, INCL. ISO 27001 & PCI DSS 4.0**

TRUSTED BY THE WORLD'S MOST FORWARD-THINKING ENTERPRISES, MSSPS, AND CYBER INVESTIGATION TEAMS

★ ★ ★ ★ ★

THIS DARKWEB SCANNER IS THE ONE TO HAVE! THIS WORKS WONDERS FOR OUR INVESTIGATIONS EFFORTS AND CROSS-SITE REFERENCING OF USERS AND SITES.

SENIOR CYBER SECURITY ENGINEER

SOURCE: GARTNER PEER INSIGHTS (INDEPENDENTLY VERIFIED REVIEWS)

YOUR ORGANIZATION'S BEST DEFENSE AGAINST THREATS ON THE DARK WEB

By partnering with Searchlight Cyber, you'll unlock access to 15+ years of expertise and research in internet anonymity and previously unobtainable dark web sources, including;

LIVE AND HISTORIC DATA FROM

850K+
dark web sites

INTEL ON BUYERS, SELLERS, AND GOODS FROM

100+
dark web marketplaces

AND CHATTER ON

70+
dark web forums

SEARCHLIGHT. CYBER

Founded in 2017, Searchlight Cyber is a company that specializes in dark web threat intelligence. We assist US Government and Law Enforcement agencies, commercial enterprises, and managed security services providers around the world in identifying criminal activity on the dark web and preventing potential threats.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service Supplier