



CYBERCRIME ANALYTICS

The New Way To **Disrupt** Cybercrime

SpyCloud

ADAPTING TO THE NEW REALITY OF CYBERCRIME



Despite increasing budgets for cybersecurity and fraud prevention and the widespread use of threat intel platforms, security monitoring tools, EDR, phishing detection, and anti-fraud signals, **90%** of organizations were affected by ransomware last year.

Criminals spread **malware** like wildfire, **identity fraud** continues its upward trajectory, and **data breaches** remain at near-record levels – and that's just what we can track.

Many security and fraud professionals believe the scale of cybercrime is much more than what's accounted for in our models today, and has the potential to **destabilize** markets and even society as a whole.

The extreme growth in cybercrime requires a new approach. It's no longer enough to gather intelligence to understand a broad threat landscape. Without relevant, actionable answers about what data criminals are using now to target a business and its customers, security and anti-fraud teams are flying blind.

Enterprises must choose a partner that can dynamically and continually surface these insights from the criminal underground with speed and actionability at the forefront.

The only answer is a partner offering Cybercrime Analytics.

This paper defines Cybercrime Analytics and why this approach is displacing traditional threat intelligence, how it is additive to anti-fraud technologies, and its use cases and benefits in detail.

When it comes to confronting the new reality of cybercrime, the optimal way to bridge the gap between cybercrime and cybersecurity is accessing the same information that criminals have – distilled into only the most actionable data for your specific enterprise.

ACTING SWIFTLY ON WHAT CRIMINALS KNOW ABOUT YOUR BUSINESS AND YOUR CUSTOMERS IS NOW THE ONLY WAY TO BEAT CRIMINALS AT THEIR OWN GAME.

Cybercrime Analytics



Automated Analytics

that Drive Action from Cybercrime Data

It's the most advantageous approach to disrupting the cycle of cybercrime because it enables faster, more confident action based on deep knowledge about user exposure in the criminal underground. It requires constant aggregation and linkage of billions of data points affecting millions of online personas, resulting in distilled insights that can be easily consumed in common security and anti-fraud tools to drive remediation.

Cybercrime Analytics can only be accomplished with a scalable engine that collects, processes, enriches, and analyzes the outputs of cybercrime. Those 'outputs' are the stolen assets from third-party data breaches, malware victim logs, and other sources that are traded and sold on the darknet – data ranging from usernames, passwords, and session cookies to sensitive PII like IP addresses, physical addresses, financial information, passport data, drivers licenses, and social security or national ID numbers. Comprising more than 200 data types, it's everything that makes up a person's digital identity that has been leaked in a breach or exfiltrated from an infostealer-infected device. The scale is massive, and as a result, linkage is required to make sense of it, and to make it useful for the teams who need it.

But the data isn't packaged in a way that's immediately useful to anyone – not even criminals. One data breach could be 100,000 files. It's spread across raw, unstructured formats that require processing and time to make it useful, so speed is an essential part of the equation. It's a race to see who can act on the data first: enterprises or attackers.

SpyCloud puts a huge emphasis on speed when it comes to recapturing these cybercrime elements from the deepest layers of the darknet (as close to where the original crime occurred) – as well as adding value at every stage. The resulting insights are relevant, correlated, and machine-readable – tying disparate breaches, malware infections, affected applications, and identity data together for individuals across their entire online identity.



WHAT
INSIGHTS DO
CYBERCRIME
ANALYTICS
REVEAL



AND WHAT
DECISIONS
CAN BE MADE
AS A RESULT?



MEET JON

Here's his high risk profile according to SpyCloud's Cybercrime Analytics.

ACROSS 8 BREACHES AND 1 MALWARE INFECTION, WE'VE LINKED JON'S EXPOSED DATA TO DETERMINE:

- He has 3 unique email addresses.
- His plaintext passwords have been exposed (and included in 2 combo lists, which put his accounts at risk of credential stuffing).
- He reuses the same password across multiple accounts, work and personal (50% reuse).
- He used a malware-infected personal/unmanaged device 1 month ago to log into critical workforce applications including a code repository, chat, and project management software – exposing both credentials and session cookies for these services.
- His sensitive PII, including his credit card number, was leaked in 1 breach.
- The last time we ingested his identity data was 24 days ago.

TAKING ACTION ON CYBERCRIME ANALYTICS

Armed with the same insights about Jon's exposure, security operations and fraud prevention teams can enhance their decisioning in the following ways:

THE **SECOPS** TEAM AT JON'S EMPLOYER



Consider Jon an unwitting insider threat, exposing the business to risk of account takeover or worse – ransomware.

Reach out to coordinate **Post-Infection Remediation** of Jon's malware-infected personal device, recommending an anti-virus solution, then resetting his passwords and invalidating active sessions where his credentials and cookies were exfiltrated by malware.

Require that he reset exposed passwords across all of his work accounts.

THE **CYBERCRIME PREVENTION TEAM** AT JON'S ONLINE BANK



Lock his account until he resets his password because his exact, in-use credentials are in criminals' hands.

Optionally, contact Jon to explain the extra steps required, and offer educational resources about better protecting himself online.

Clear active web sessions on all devices Jon has recently logged into.

Send his credit applications through manual review for extra verification.

Flag his account for additional scrutiny when modifications are made, such as address changes, backup email changes, or ordering checks.

THE **FRAUD PREVENTION TEAM** AT AN ECOMMERCE MERCHANT JON IS PURCHASING FROM



Clear active web sessions on all devices Jon has recently logged into, and require Jon to re-login.

Require MFA when he logs into an existing account.

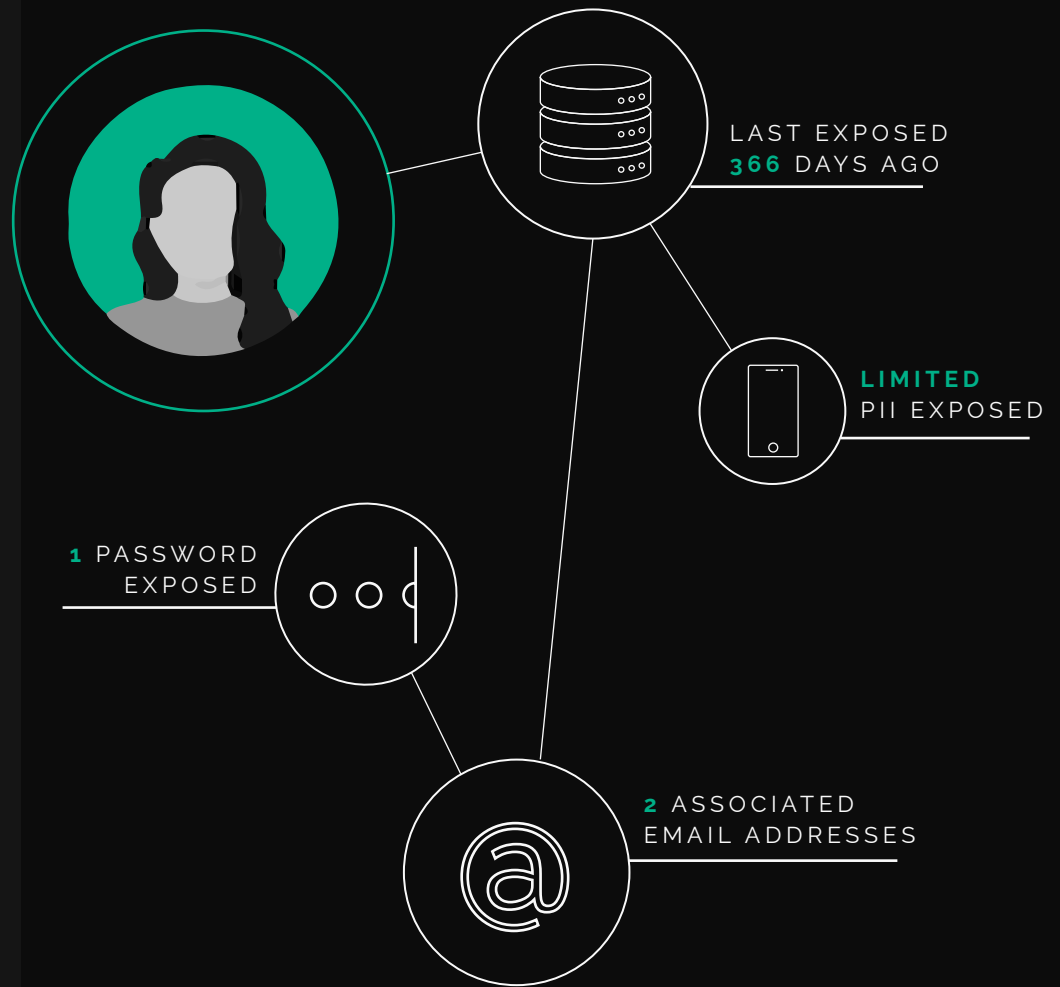
Remove stored payment information; if a criminal logs into his account using stolen credentials, they'll face a barrier to making a fraudulent purchase.

Send large purchases through manual review for extra verification.

Lock his account until he resets his password because his exact, in-use credentials are in criminals' hands.

MEET MARIE

Here's her low risk profile according to SpyCloud's Cybercrime Analytics.



ACROSS 4 BREACHES, WE'VE LINKED MARIE'S EXPOSED DATA TO DETERMINE:

- She has 2 unique email addresses.
- She has only 1 plaintext password exposed (not included in any combo lists, which would put her accounts at risk of credential stuffing).
- She has some sensitive PII exposed, including a physical address and a phone number.
- The last time we ingested any data about her was 366 days ago.

TAKING ACTION ON CYBERCRIME ANALYTICS

Armed with the same insights about Marie's exposure, security operations and fraud prevention teams can enhance their decisioning in the following ways:



THE **SECOPS** TEAM AT MARIE'S EMPLOYER

Consider Marie a low-risk employee who is subject to standard security checks and password policies – requiring intervention only in the case of a future exposure.

Spend their time remediating risk introduced by other employees.




THE **CYBERCRIME PREVENTION TEAM** AT MARIE'S ONLINE BANK

Ensure Marie meets standard online security requirements, including a strong password and MFA.

Intervene in the event of suspicious or anomalous behavior.

Spend their time remediating risk introduced by other consumers.



THE **FRAUD PREVENTION TEAM** AT AN ECOMMERCE MERCHANT MARIE IS PURCHASING FROM

Ensure Marie meets standard online security requirements, including a strong password and MFA.

Intervene in the event of suspicious or anomalous behavior.

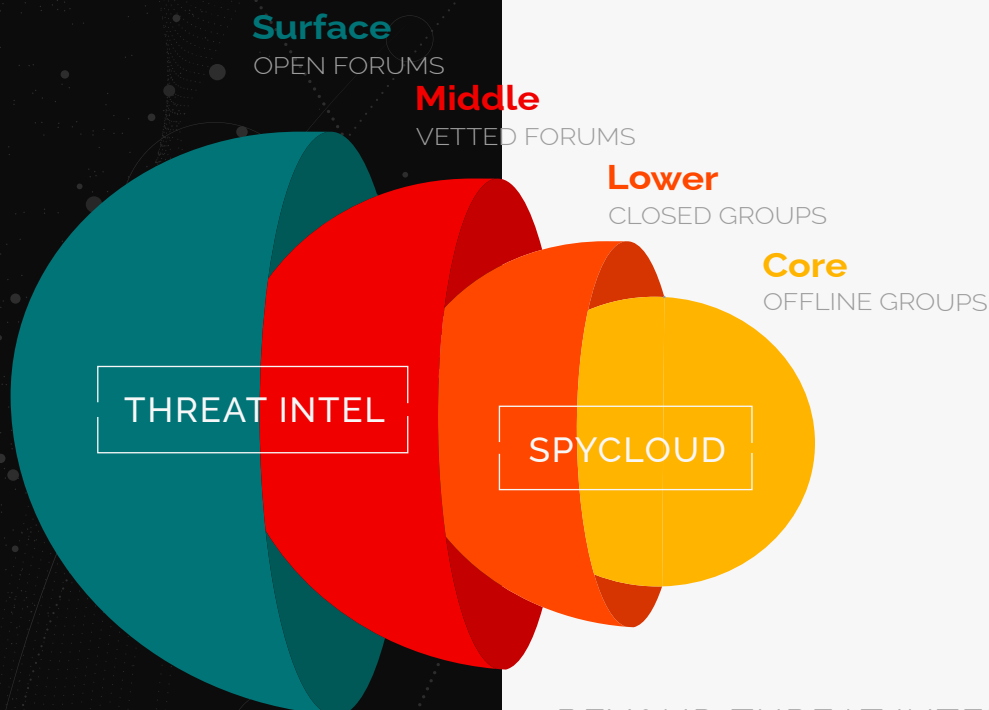
Spend their time remediating risk introduced by other consumers.

Cybercrime Analytics deliver **actionable insights** that go further to protect the enterprise and its users than has *ever* been possible before.

A GLOBAL COMPUTER RETAILER USED SPYCLOUD'S CYBERCRIME ANALYTICS TO SEGMENT THEIR WEBSITE INTERACTIONS INTO **LOW-RISK USERS (82%), MEDIUM- AND HIGH-RISK USERS (14%), AND CRITICAL-RISK USERS (4%),** WHO WERE USING A MALWARE-INFECTED DEVICE.



THIS DEEPLY-ENHANCED CONTEXT ENABLED THE CYBER FRAUD PREVENTION AND INVESTIGATIONS TEAMS TO FOCUS THEIR LIMITED RESOURCES ON THE RISKIEST USERS AND REDUCE POST-TRANSACTION INVESTIGATION TIME BY 30%.



BEYOND THREAT INTELLIGENCE: FROM RAW DATA TO MEANINGFUL ACTION

With the shift to support remote work, the increased amount of online transactions taking place, and more accounts managed by everyone in a post-pandemic world, the amount of criminal activity has increased dramatically. The explosive growth in cybercrime has led to a darknet so large – and with so much of the world’s information in it – that it impacts every business in some way.

Many cyber teams turn to traditional solutions like threat intelligence to solve this problem. However:

- There is **no sign** that broad indicators of compromise based on surface-level data and dark web forum chatter is putting a stop to cybercrime, as evidenced by its relentless growth.
- IOCs are **not specifically relevant** to most businesses. After scoping the relevance to existing systems, writing rules, testing and deploying them, the exploit has likely made the news and security tools have already accounted for the vulnerability.
- Threat intel feeds **do not tell** security or anti-fraud teams what authentication data and PII criminals are using right now to target their business or customers.
- Raw data is **not actionable** without significant analyst intervention, and it’s incredibly time-consuming to get critical insights without a scalable process.
- Threat intel vendors’ approach to data collection – scanning open forums and pastebin sites – is **reactive**, while proactive infiltration of underground cybercriminal communities is the only way to obtain still-valid data from recent breaches and malware campaigns.
- Threat intel platforms cause **alert fatigue** from old exposures or worse: they **miss high-severity compromises** that are known only to small circles of initial access brokers.

Relying on traditional solutions makes it impossible to react quickly enough to stop cyberattacks. Security teams need more than a news feed with the broad context of darknet activity. Simply put, they need definitive evidence of the stolen data tied to their organization so they can invalidate it – making that data worthless.

BOOSTING FRAUD PREVENTION EFFECTIVENESS WITH MORE CONTEXT

As for fraud prevention solutions, most are missing important context about user risk entirely. Every step in a consumers' digital journey – from new account setup to login to modification and payment – requires signals about user risk including identity verification, account history, device and location data, and patterns of behavior. But fraud decisioning can be greatly enhanced with signals from the criminal underground. Much of what passes for this type of data these days is noisy, so the key is integrating analytics that are pre-calculated and simple for your decision engine to ingest and easy to build rules around.

As fraud prevention teams begin adopting a security mindset, one of the greatest leaps they can make is to leverage knowledge about consumers' exposures in data breaches and malware infections to make informed decisions that deem interactions safe or suspicious – resulting in a higher degree of confidence that users interacting with the application are legitimate and not criminals using stolen data.

Using Cybercrime Analytics, these teams can make decisions using context about consumers' risk of account takeover, synthetic identity, and fraud tied to malware without exposing passwords or sensitive PII. Instead, analytics can reveal key risk indicators including recency of exposure in a breach or malware infection, prevalence of password reuse, and exposure of PII and financial information, including credit card numbers, that can be leveraged immediately for unauthorized credit card purchases. This metadata alone (essentially the answers without the sensitive details) is enough. And it's seamless, adding no additional friction for low-risk consumers.

HIGH RISK

MALWARE
DETECTED

SSN & DOB
EXPOSED

EXPOSED 55
DAYS AGO



LOW RISK

NO MALWARE
DETECTED

LIMITED
PII EXPOSED

LOW
PASSWORD REUSE



COLLECT



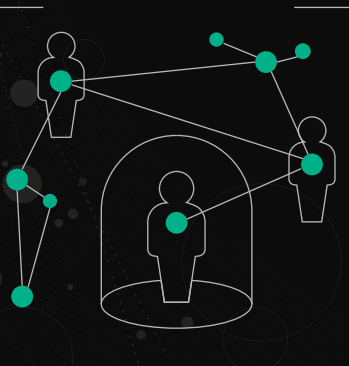
CURATE



ENRICH



ANALYZE



HOW DOES SPYCLOUD UNIQUELY ENABLE CYBERCRIME ANALYTICS?

▼

SpyCloud is able to perform advanced analytics with our proprietary Cyber Analytics Engine. This engine was built to make raw data actually actionable at a massive scale. It takes recaptured data from all layers of the darknet, curates it, enriches and analyzes it to drive our products that automate protecting businesses. It augments our database by 12B+ assets per month, and identifies and tosses erroneous data that would cause alert fatigue. Its focus is delivering only the most relevant and actionable information to our customers.

The process begins with data collection from the deepest layers of the darknet, led by a prolific security research team who socially engineers it directly from bad actors. This data is in messy, unstructured data formats obtained in a variety of broken databases and data structures, often in binary or mixed formats – amounting to thousands of files at a time. The next step is figuring out what that raw data is, and parsing and curating it so that it can be ingested into our dataset.

Over the last 6+ years, we have invested heavily in cracking and analyzing passwords, resulting in 90% of passwords being provided in plaintext in our products. Access to plaintext passwords alongside hundreds of other elements allows us to perform analysis and create relational links about individual identities, producing actionable insights that help businesses fend off cyberattacks



SPOTLIGHT ON MALWARE ANALYTICS: IDENTIFYING THE HIGHEST RISK EMPLOYEES & CONSUMERS


▼

Criminals have begun emphasizing malware with an infostealer component as a means to steal valid, in-use authentication data and PII to enable the most damaging attacks. Infostealers are relatively cheap for criminal actors to buy – as low as \$200-\$300 – and easy to deploy. Many are designed to not only avoid detection by anti-malware solutions, but also leave no trace of infection. This “dissolvable malware” means security teams may have no knowledge of an infection having occurred and cannot take proper remediation steps.

What makes infostealers especially attractive for cybercriminals – and boosts their ROI – is their success rate and effectiveness. The siphoned credentials are accurate and valid since they are fresh, while the stolen session cookies and tokens allow threat actors to bypass multi-factor authentication (MFA) so they can assume the user identity without any friction – sometimes long after the initial infection takes place – making the stolen data far more harmful as it can lead to additional attacks such as ransomware.

The popularity of infostealers (and the damage that can be inflicted by the data they steal) necessitates that cybercrime prevention solutions incorporate the same data.

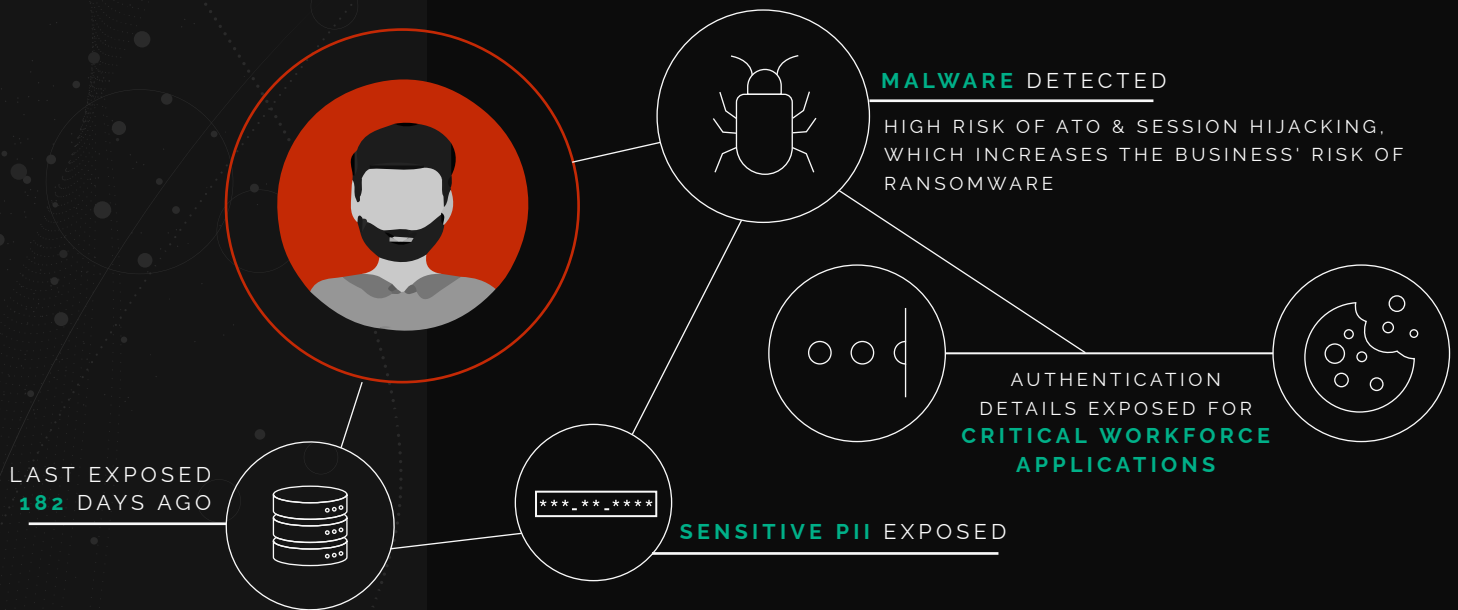
What makes the Cybercrime Analytics approach that much more valuable is the ability to correlate a user’s exposures from malware infections on corporate and personal devices. The linkage SpyCloud uniquely provides reliably ties who a user is in their personal life to who the user is at work, enabling the business to make decisions based on the individual’s entire identity, with or without accessing their private details.



Below, you’ll meet Chris.

He’s a contractor for Sparefactor, a global financial institution. He was issued a corporate device when his engagement began, but on a recent trip to visit family, he used his aunt’s home computer to log into his workplace’s SSO, and from there, a company wiki, chat program, and work email.

▼



MEET CHRIS

Here's his high risk profile according to SpyCloud's Cybercrime Analytics.

HOW SPYCLOUD HELPS

SpyCloud researchers socially engineer a dump of malware victim logs containing Chris' authentication details – target URLs, credentials, and session cookies (among other data) – from a bad actor within 2-3 days of infection. SpyCloud's Cyber Analytics Engine ingests, parses, and analyzes the data, identifying Chris' credentials and session cookies from his SSO instance, along with those three other exposed workforce applications, to his other exposures in third-party data breaches and combo lists to add to the full picture of his risk.

While Chris has become a target for initial access brokers looking for an entry point into Sparefactor, SpyCloud has equipped Sparefactor (as a SpyCloud customer) with Chris' data so they can properly remediate. **Post-Infection Remediation** steps include:

- Prioritizing remediation of his SSO account, which could open the door to **211 applications**, on average, for large organizations.
- Resetting the compromised credentials for his accounts.
- Invalidating his active sessions across all devices.
- Reviewing application logs to confirm that activity is coming from expected IP address ranges and geographies.

The result is immediate risk reduction for targeted attacks, including ransomware.

The ability to draw connections that include exposures on infected non-corporate-issued devices is a value-add not found with existing threat intelligence or anti-fraud approaches.

“ **S** PYCLOUD IDENTIFIED A MALWARE INFECTION ON A DEVICE USED BY A CONTRACTOR WORKING REMOTELY OVERSEAS. [THE CONTRACTOR'S] ENDPOINT PROTECTION (EPP) WAS NOT UPDATED, AND EVEN AFTER UPDATING THE EPP, THEY DID NOT FIND THE MALWARE.



THIS CONFIRMS THE RISK MOST COMPANIES HAVE WITH THIRD-PARTY VENDORS SINCE WE TRULY CANNOT MEASURE THE EFFICACY OF THE CONTROLS OF SUCH VENDORS WHO ACCESS OUR SYSTEMS. ”

-CISO, FINANCIAL INSTITUTION

USE CASES FOR CYBERCRIME ANALYTICS

ENTERPRISE PROTECTION

Act on previously invisible exposures to stop cyberattacks, reducing risk while improving speed of detection & remediation

Stop ransomware attacks leveraging entry points created by infostealer malware infections on managed and unmanaged devices • Protect your company from ATO, data breaches, and BEC resulting from third-party breach exposures • Prevent unauthorized access of critical workforce services including corporate SSO instances • Monitor the ATO risk of supply chain vendors and partners accessing corporate systems • Empower VIPs to secure their personal identities, without compromising their privacy

FRAUD PREVENTION

Act on the full picture consumers' risk to substantially reduce fraudulent activity

Make more confident decisions based on consumers' risk of ATO, synthetic identities, and fraud tied to malware • Thwart fraud caused by account takeover by resetting compromised credentials • Reduce new account enrollment and guest checkout fraud • Prevent fraud from session hijacking with stolen cookies • Reduce post-transaction investigation cycle time with immediate insights about user risk

INVESTIGATIONS

Act on connected data to streamline investigations and identify threats efficiently

Attribute specific threat actors and their alternate personas to crimes • Research criminal campaigns and their infrastructure • Analyze and build profiles of potential insider threats

PRODUCT ENHANCEMENTS

Act on refined insights from over 200+ data types to build innovative services & solutions

Enhance existing consumer protection products, including identity monitoring and password managers • Create new revenue streams with novel services leveraging Cybercrime Analytics • Improve retention with value-added services that drive customer satisfaction • Increase customer acquisition with higher conversion to paid services that use darknet insights

CONCLUSION



The threat landscape is constantly changing, and yet organizations are still applying the same tools to solve the rapidly growing problem of cybercrime in its many forms. Stopping account takeover requires resetting stolen passwords. Stopping session hijacking requires invalidating stolen cookies. Stopping ransomware requires thwarting these precursor attacks and shutting down entry points into your network. Stopping transaction and payment fraud requires confidence that a user is legitimate and not a bad actor using stolen information. Stopping account enrollment fraud requires knowing whether the users' information is constructed from stolen identity data. **Stopping criminals requires a new approach.**

The answers are not readily found in threat intel feeds. They require extreme processing and analysis to deliver prioritized, actionable information. When getting ahead means taking swift action, distilled answers are essential – and that is the promise of Cybercrime Analytics:

- Real evidence of compromise without unnecessary alerts or false positives
- Deep context about user risk
- Knowledge of the severity of employee and consumer exposure
- Identification of previously unknown risks to the business
- Improvement in the metrics that matter to you

And ultimately: **the ability to prevent more cybercrime.**

**CHECK YOUR
EXPOSURE TODAY**
and reveal details about your
company, customer, and
personal risk.

Knowing what's out there is the
first step to protecting yourself
and your organization from
identity exposure that can lead
to account takeover,
ransomware, and online fraud.

[CHECK YOUR EXPOSURE](#)

We **Disrupt** Cybercrime

SpyCloud