



TALES FROM THE DARK WEB

FOLLOWING THREAT ACTOR BREAD CRUMBS:

How to Monitor Access Brokers
to Help Prevent Full Breach Incidents

**FOLLOWING THREAT ACTOR BREAD CRUMBS:
HOW TO MONITOR ACCESS BROKERS TO HELP
PREVENT FULL BREACH INCIDENTS**

EXECUTIVE SUMMARY

Cybercrime is a lucrative business fueled by high rewards and often with low consequences for the adversary. The thriving criminal underground ecosystem of services, distribution and monetization makes it easy for criminal operators to “set up shop,” join the cybercrime scene, and profit at the expense of their victims. This evolution in “cybercrime-as-a-service” generates an inflow of highly motivated threat operators, and creates a formidable opponent for modern security defenders. Continuous monitoring of the underground ecosystem enables early warning and can help prevent data leak incidents and ransomware attacks.

In this white paper, we focus on one specific use case of monitoring access brokers, following the bread crumbs they left behind, and identifying critical threat activity in a high-noise, fast-moving criminal ecosystem.

ACCESS BROKERS HAVE KEYS TO YOUR FRONT DOOR

Behind every cyberattack is a human actor looking to identify new victims with stealthy attack methods. Many are motivated by easy financial gains, but some are willing to put in hard work to get big payoffs. Some may also have more than one motivation. These criminal operators don't often work in isolation. Instead they collaborate and often leverage a mix of criminal services, distribution capabilities and monetization methods to stage attacks and get their prize from the victim.

Access brokers are often at the start of the eCrime value chain. These intruders gain access insights into victim infrastructure and sell the illegitimately obtained credentials or access methods on underground communities. Malware operators can purchase this access information, thereby eliminating the need to identify targets or gain initial access, ultimately resulting in faster and more targeted weaponization. Some access brokers even include details on escalated privileges to the domain administrator level (often advertised as “full access”), while other access brokers just provide the credentials and endpoints necessary to gain access.






Over the past years, the use of access brokers has become common among big game hunting (BGH) actors and aspiring ransomware operators. So how can security teams reveal these stealthy actors and help protect themselves against imminent ransomware attacks or data breaches?

In this white paper, we focus on one specific use case of monitoring access brokers and identifying critical threat activity in a high-noise, fast-moving criminal ecosystem.

**FOLLOWING THREAT ACTOR BREAD CRUMBS:
HOW TO MONITOR ACCESS BROKERS TO HELP
PREVENT FULL BREACH INCIDENTS**

THE PRICE IS RIGHT

Access brokers stay afloat by selling a broad array of access types. Here are some recently discovered examples ready to be picked up by BGH or other malicious operators.

<p>Financial Account Login</p>  <p>1% to 5% of account value</p>	<p>Business Account with Email Credential</p>  <p>Starting at \$1.2K USD</p>	<p>Code Signing Certificate</p>  <p>Negotiable from \$35K USD</p>
<p>Remote Access to Network Asset</p>  <p>Between \$5 & \$100 USD</p>	<p>Custom Exploit to IT Infrastructure</p>  <p>Starting at \$30K USD</p>	

BREAD CRUMBS LEFT BEHIND

To sell and advertise their illegitimate merchandise on underground communities, access brokers often use specific keywords and specialized marketplaces. Via these descriptions and posts, unique “bread crumbs” are often left behind.

Here are some attributes surrounding the typical access broker post:

- Company details (company size, revenue, vertical, country)
- Domain
- IT Infrastructure exploit details: hardware vendor and model for uniquely crafted exploits kit (e.g., exploit script for Network Attached Storage or Network Access product)
- Tool (unique malware) used to gather steal credentials(e.g. Redline Stealer)
- The name of the tool, or malware, used (e.g. xss, Russian Market, 2EASY)
- Access broker alias name used on the forum

Of course, these details offer defenders an opportunity to detect compromised accounts or imminent threat risks to prevent a full ransomware incident scenario or data theft. By continuously scanning underground markets and forums for certain keywords or bread crumbs, threat analysts can get proactively alerted on infrastructure access that’s brokered to malware operators.

By continuously scanning underground markets and forums for certain keywords or bread crumbs, threat analysts can get proactively alerted on infrastructure access brokered to malware operators.

FOLLOWING THREAT ACTOR BREAD CRUMBS: HOW TO MONITOR ACCESS BROKERS TO HELP PREVENT FULL BREACH INCIDENTS

This use case is an example of how the digital risk protection solution, CrowdStrike Falcon X Recon™, comes to the rescue. Falcon X Recon not only informs security teams of imminent threat activity, it creates an opportunity to mitigate access exploitation as well.

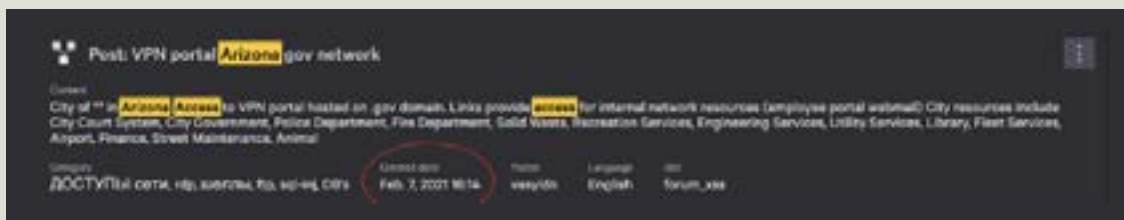
EXAMPLE VICTIM FOR SALE ON CRIMINAL FORUM XSS

STATE GOVERNMENT COMPUTER SYSTEM HIT BY CYBERATTACK

In February 2021, several news sites reported a ransomware attack on a major city in the United States. Negative consequences included a costly incident response, system downtime for over a month, and exposure of personal and sensitive information.

Six weeks prior to the incident going public, the access broker “vasylrn” posted on a popular Russian hacker forum “xss” an offer to sell VPN portal access to this city’s IT network.

The post included details on accessing departmental infrastructure including the city court system, police department, fire department and utility services.



A month after the ransomware attack, the threat actor WIZARD SPIDER published critical city documents, which were accessed via the city’s VPN portal, to a dedicated leak site.

While the city likely did not pay any ransom, the aftermath was still discussed on public news sites into August 2021.

EARLY WARNING VIA KEYWORDS

In this example, threat analysts using CrowdStrike Falcon X Recon could have created a monitoring rule to identify the access broker information in advance of the ransomware attack and mitigate VPN access gaps.

Falcon X Recon’s search and monitoring rules for simple keywords such as:

- “state name” AND
- “city name” OR
- “government” OR
- “government” or “gov”
- AND “access”

would have proactively alerted the team that an incident had occurred, allowing time to prepare for an imminent cyberattack if the vulnerability could not be addressed quickly enough.

**FOLLOWING THREAT ACTOR BREAD CRUMBS:
HOW TO MONITOR ACCESS BROKERS TO HELP
PREVENT FULL BREACH INCIDENTS**

FORMING A MONITORING STRATEGY TO FOLLOW THE BREAD CRUMBS

Though creating monitoring rules can be relatively simple, the amount of data or chatter on underground forums remains enormous. Additionally, access broker posts contain a mix of structured and unstructured data that may leave defenders confused on where and what to look for. Some actors do not advertise at all and prefer to use marketplaces.

To maximize monitoring efforts and actionable outputs, threat analysts need a repeatable methodology to fine-tune keywords when searching underground forums.

Security teams often have limited time or expertise to reliably and consistently monitor the online underground for threats to their business. To help security teams create a monitoring strategy, CrowdStrike's managed service, Falcon X Recon+, enables security teams to offload some of these efforts by providing experts to monitor and triage threats found in these communities on your behalf. Not only can Falcon X Recon+ reduce time, skills and effort required to mitigate your digital underground risk, it can increase the effectiveness of your overall security team.

CrowdStrike's Falcon X Recon+ experts identify data exposure and threats to your business by monitoring restricted forums, marketplaces, messaging platforms, social media posts, data leak sites and much more to provide relevant, real-time warnings, mitigation recommendations, and rapid takedowns if necessary.



FIVE STEPS TO KICK OFF YOUR MONITORING STRATEGY AND ACHIEVE ACTIONABLE RESULTS:

1. Know what to protect. Identify your digital assets or key attributes that describe you as a target. Examples include domains, email address extensions and externally facing asset details. Also include your country or industry.

2. Identify the attributes of actors that would harm or access your assets or target your industry. List known access broker author aliases, how they advertise on underground communities and what they sell. CrowdStrike Intelligence actor profiles, alerts and tippers will give you a head start to identify author names.

3. Make a short list of known underground markets used by criminal actor and malware or malware tools. For instance, you can review Falcon X Intelligence infostealer malware reports and extract product names like "redline" or "mystery" stealers.

4. Codify the rules using keywords gathered in steps 1-3 to prioritize alerts and **build dashboards** providing an overview of triggered rules.

5. Assign alerts to various owners and **review** on a regular basis. **Tune out false positives** by sharpening keywords or using watchlists. Be sure to reassess rules and update regularly with new information from finished intelligence reports.

**FOLLOWING THREAT ACTOR BREAD CRUMBS:
HOW TO MONITOR ACCESS BROKERS TO HELP
PREVENT FULL BREACH INCIDENTS**

INFORMING STAKEHOLDERS WITH ACTIONABLE DATA

The return on investment of this process depends on how quickly internal stakeholders can be informed with actionable data to neutralize imminent threats before they interrupt the business or how quickly they can eradicate incidents by eliminating external attack vectors.

Here are ways that security team members use alerts to take action against underground access brokers.

- **Intelligence Teams** can use the information from Falcon X Recon as an additional data source for their analysis, tying incidents to activity to better understand longer term organizational threats.
- **Identity and access managers** can mitigate enterprise accounts based on details discovered on underground markets, interrupting weaponization or exploitation by malware operators.
- **Vulnerability risk managers** can mitigate custom asset exploits advertised by specialized actors to reduce the attack surface.
- **SOC analysts** can use underground access broker alerts to prioritize related incidents and investigate surrounding events.
- **Incident responders** can eradicate incidents (e.g., endpoint infections) in depth by understanding the root cause behind the infection.

DISRUPTING ATTACKERS ON THEIR VALUE CHAIN

Cybercrime is a dynamic ecosystem consisting of threat actors, a broad array of services and a thriving underground marketplace. Access brokers, a known malicious entity, form the beginning of an attack value chain by selling access details stolen from their victims.

For modern defenders, it is not if but when these known attackers will advertise about an organization. Following threat actor bread crumbs by monitoring underground marketplaces on a continuous basis not only informs stakeholders, it allows them to take immediate action to protect the organization from costly incident escalations

Access brokers, a known malicious entity, form the beginning of an attack value chain by selling access details stolen from their victims.

**FOLLOWING THREAT ACTOR BREAD CRUMBS:
HOW TO MONITOR ACCESS BROKERS TO HELP
PREVENT FULL BREACH INCIDENTS**

and ransomware scenarios to better protect their brand and critical assets.

Additionally, when access brokers learn that their illegitimately obtained credentials or access methods are being monitored or pose low value to ransomware operators, their business model will break and eventually they will stop advertising.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform. There's only one thing to remember about CrowdStrike: **We stop breaches.**

Speak to a representative to learn more about how CrowdStrike can help you protect your environment:

Phone: 1.888.512.8906

Email: sales@crowdstrike.com

Web: www.crowdstrike.com

ACCESS BROKERS DON'T
STAND A CHANCE WITH
FALCON X RECON

Learn More

Learn more at **www.crowdstrike.com**

© 2021 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

