BLACKBIRD.AI NARRATIVE INTELLIGENCE BRIEF

CROWDSTRIKE OUTAGE - REPORT 1

July 19, 2024

BLACKBIRD.AI

METHODOLOGY

NARRATIVE DISCOVERY

Blackbird's AI-powered narrative detection capability automatically surfaces conversations of interest within a dataset which are captured by the Constellation Dashboard for further analyst exploration.

NARRATIVE SELECTION & RISK SIGNALS

Blackbird considers a wide range of Risk Signals and other relevant contextual factors and conversation drivers in order to select narratives for inclusion in a report, which may provide qualitative or quantitative indications of potential risk or interest. This may include, but is not limited to:

- The presence of **bot-like activity** indicating synthetic automated social media accounts
- **Anomalous activity** that may indicate unusual content propagation patterns that deviate from the expected behavior of regular online platform users.
- Levels of **negative sentiment or toxic speech** that denotes emotive messaging deemed to be pejorative or critical, or otherwise offensive.
- The narrative's perceived **relevance to stated client interests**.
- Notable presence of **cohorts** of interest
- Partisan sentiment or user affiliation indicating the potential **politicization** of a topic.
- Involvement of **influential or high-profile users** in shaping conversations.
- A narrative's relative **volume of posts and engagements**

NETWORK GRAPH VISUALIZATIONS

Network graph images visual representations of relationships between users, and/or hashtags, URLs, or other concepts captured within a narrative. Graph images are selected based their ability to communicate insights around networked activity, narrative crossovers, audience and influencer identification, or distribution of Blackbird Risk Signals or other classifiers.

Volume & Velocity
Post Volume, Engagements, Reach

INVESTIGATE FOR INCREASED RISK

- CrowdStrike Falcon agent causes blue screen of death

ESCALATE & MITIGATE

MONITOR

- Affected users should switch to Linux

INVESTIGATE FOR INCREASED VOLUME

Assorted fringe narratives, including:

- The outage was a result of state-sponsored cyber attacks
- Rival tech companies or disgruntled employees orchestrated the outage
- The outage was a cover for government agencies to implement or test mass surveillance technologies
- The outage is a prelude to larger, coordinated cyber events
- CrowdStrike was paid to fraudulently link the 2016 DNC hack to Russia

Risk Factors
Bot-like, Anomalous, Cohorts

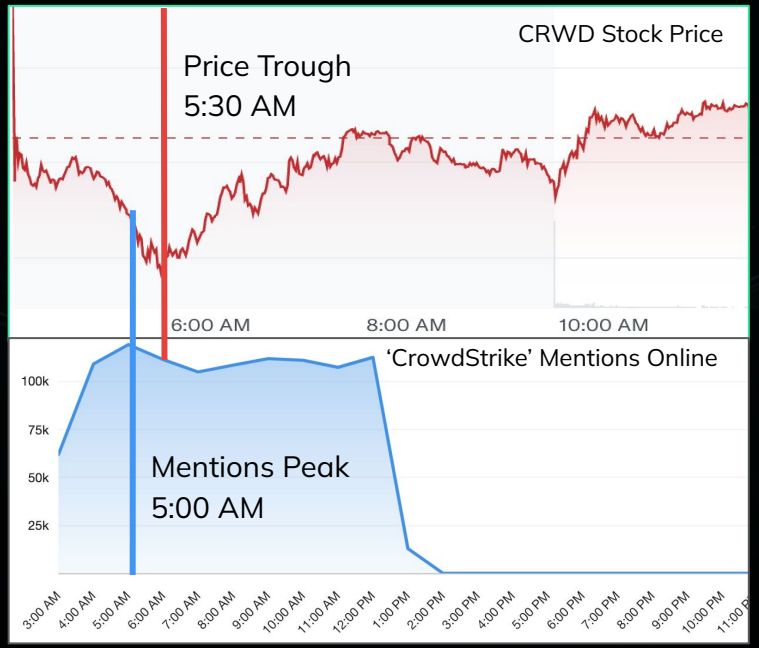
EXECUTIVE SUMMARY

- At the time of this report early July 19, the majority of social media discussion around the CrowdStrike outage displayed no direct agenda or additional angle. Many users made light of the incident and specifically at Microsoft, dampening reputational damage aimed at CrowdStrike. These posts, seen in the form of **memes** and **parodies**, generated high engagement from users who do not otherwise participate in relevant discourse.

- The number of fringe narratives surrounding the outage was high, although associated post volumes remained low and propagation patterns showed signs of manipulation. As a result, these fringe narratives posed low risk to CrowdStrike's reputation at the time of reporting, so long as they did not receive engagement from major influencers and agenda-driven communities who have the power to push these narratives towards the mainstream.

- This activity should be continuously monitored in order to prevent and/or prepare for a secondary spike in conversation if this engagement occurs.

CRWD Stock vs. Online Mentions



CrowdStrike's online mentions, reputational risk, and share price are inextricably linked during the spread of 'supernode' narratives.

- Mentions of CrowdStrike online peaked just before stock price reached its lowest trough. The speed and scale of social media make it an effective tool in measuring the spread of adverse narratives.
- When combined with risk metrics sourced in the Constellation dashboard, users can effectively evaluate whether or not rapid increases in conversation pose a risk to reputation, shareholder confidence, or stock price.

BLACKBIRD.AI

NARRATIVE 1

CrowdStrike Falcon agent causes blue screen of death

Narrative 1

CrowdStrike Falcon agent linked to blue screen of death

Posts	Engagements	Authors
34,901	583,433	28,419

Bot-Like Activity
LOW RISK
7.2% of authors

Anomalous Activity
HIGH RISK
27.3% of posts

Negative Sentiment
MODERATE RISK
14.1% of posts

Mis, Dis, & Malinformation
MODERATE RISK

Cohorts
POLITICAL IDEOLOGY AFFILIATION COHORT

INDIAN STATE SUPPORTER

POLITICAL PARTY SUPPORTERS

This was among the highest volume conversations following initial reports of CrowdStrike's software outage. Many users propagated anecdotes, jokes, and memes surrounding the infamous 'blue screen of death' or 'BSOD' reportedly caused by CrowdStrike software deployed to Microsoft systems. Some emphasized that the issue lies with CrowdStrike's Falcon agent, which they speculated failed to prevent widespread attacks.

This narrative originated in Indian social media communities as evidenced by user cohort participation, very likely due to the time zone difference. As the day progressed, European and North American users joined the conversation. Top users engaging in anomalous activity used hashtags such as #crowdstrike and #bsod in viral posts that showed the Las Vegas Sphere experiencing a blue screen of death.

Anomalous activity was extremely high in this narrative, indicating a high level of coordination between users. This is commonly observed amid the spread of 'supernode' narratives - characterized by fast viral spread, damaging material, and frequently used information sharing patterns.

Bot-like activity in this narrative was relatively low, reflecting organic methods of content propagation - nearly all posts and interactions in this narrative originated from authentic users. In the case of a 'supernode' narrative, this dynamic tends to be more damaging and present more staying power than conversation that originates with or is spread by bots.

NETWORK ANALYSIS

ANOMALOUS ACTIVITY

The graph visualizes networked interactions between users, hashtags, and URLs with a red filter representing the distribution of anomalous activity in this narrative.

- High levels of anomalous activity are present in this narrative. A network of highly interconnected users leveraged hashtags such as #Microsoft and #crowdstrike flagged for anomalous propagation.
- This is a typical pattern of propagation in the immediate aftermath of a 'supernode' narrative. Swaths of users unite around a small subset of phrases, hashtags, and URLs which generates a strong amplification effect around a small cluster of content. As this narrative evolves over the coming days, more subversive threat actors are likely to inject damaging rhetoric into the larger pool of conversation via bot-like and cohort activity.

NARRATIVE 2

Affected users should switch to Linux

Narrative 2

Affected users should switch to Linux

Posts	Engagements	Authors
3,448	121,717	2,927

Bot-Like Activity
MODERATE RISK
10.8% of authors

Anomalous Activity
HIGH RISK
50.3% of posts

Negative Sentiment
LOW RISK
1.5% of posts

Mis, Dis, & Malinformation
MODERATE RISK

Cohorts
INDIAN STATE SUPPORTER

POLITICAL IDEOLOGY AFFILIATION COHORT

RUSSIAN STATE SUPPORTERS

Linux users entered the conversation as more posts linked outages to the combination of Microsoft systems and CrowdStrike's Falcon agent. These users boasted that they had not experienced outages and suggested to others that they switch away from Microsoft to Linux. Many Linux users bragged via memes and sarcastic posts that Linux was a superior system to Microsoft after George Kurtz, CrowdStrike's CEO, confirmed that Mac and Linux users were unaffected by the event.

In this narrative, we again observed very high levels of anomalous activity. This is consistent with the theme of this narrative, where disparate users clustered together to spread adverse narratives about CrowdStrike in a coordinated manner. This is a commonly observed pattern of propagation in the immediate aftermath of a highly damaging viral event. Common hashtags (i.e. #Microsoft, #Windows, #CrowdStrike) and widely shared images also contributed to high levels of anomalous activity.

NARRATIVE 3

Fringe theories around the origin and motive of the CrowdStrike outage

Narrative 3

Fringe theories

Posts	Engagements	Authors
1,271	19,276	957

Bot-Like Activity
HIGH RISK
20.1%% of authors

Anomalous Activity
HIGH RISK
44.4% of posts

Negative Sentiment
MODERATE RISK
18.3% of posts

Mis, Dis, & Malinformation
HIGH RISK

Cohorts
POLITICAL IDEOLOGY AFFILIATION COHORT

RUSSIAN STATE SUPPORTER

INDIAN STATE SUPPORTER

ANTI VAXXER

As chatter surrounding CrowdStrike and the global outages evolved, it became plagued with a wide spectrum of fringe narratives, often stemming from politically-motivated groups and pro-Russian cohorts. The most common theories included:

1. **The outage was planned by the deep state and foreign adversaries to disrupt Trump's bid for reelection - CrowdStrike is funded and owned by the deep state**
2. **CrowdStrike was paid to fraudulently link the 2016 DNC hack to Russia**
3. **Russian critical infrastructure is perfectly functional while Western systems have collapsed**

Variations on the above claims were widespread and present across different online platforms. Furthermore, each of these narratives featured far higher levels of bot-like activity than any other conversation in the dataset. This further emphasizes the idea that damaging narratives are more likely to be spread in an inauthentic manner via threat actors after the initial frenzy of news coverage. This is also evident in the cohort distribution of these narratives - Russian State Supporters were **six times** more prevalent in these conversations than in the aggregate data.

The third narrative originally spread via a **news segment** from RT India, the Indian bureau of Russia's main state-owned news network and a strong vector of pro-Russian propaganda. Various chat channels shared this story, as RT India **propelled it to** social media sites, and eventually **mainstream news coverage on Reuters**. On more niche chat platforms, the primary conversations were fringe theories, as opposed to main social media networks, where most conversation was dominated by anecdotes describing blue screens and simple outage reports. Alternative chat platforms are key to monitor, as they tend to function as a proving ground for more fringe narratives that subsequently migrate to front-of-house social media sites.

APPENDIX: DATA PROCESSED & METHODOLOGY

DATA PROCESSED

DATASET: CrowdStrike Mentions

- **Date range** July 19, 2024
- **Total documents** 263,992
- **Total authors** 157,854
- **Total engagements** 15,445,168

DATA METHODOLOGY

Blackbird.AI offers clarity in the social media landscape with our proprietary Constellation Dashboard. Our AI analytics provide comprehensive situational awareness by leveraging four pillars of intelligence. This empowers industry stakeholders to protect their message, mission, and future from rapid and widespread informational attacks on human perception.

NARRATIVE INTELLIGENCE

Blackbird's AI-powered narrative detection capability automatically surfaces social media conversations at their point of emergence, cutting through the noise of online chatter to the topics that matter. Narratives are monitored as they develop and grow across social media platforms, giving insight into how discourse is influenced and shaped over time.

THREAT INTELLIGENCE

Blackbird.AI identifies and prioritizes potential threats based on proprietary risk metrics. These metrics include toxic content, partisan sentiment, and narrative manipulation. Manipulation encompasses various online activities that aim to influence public opinion, such as spreading disinformation and artificially amplifying stories to subvert audience perception.

ACTOR INTELLIGENCE

Blackbird.AI identifies and maps online actors and communities to understand their impact on social media messaging. Cohort classifications group users based on affiliations, providing insights into behaviors and motives. Network analysis reveals significant relationships between users and the content they share, considering audience influence.

IMPACT INTELLIGENCE

Blackbird's impact intelligence enables understanding of online information operations, including harmful activity and the effectiveness of countermeasures. It analyzes network connectivity, actor characteristics, and content trends to gain insight into outcomes and future trajectories.

DATA METHODOLOGY

Blackbird.AI's RAV3N analysts assign each metric a risk level based on the criteria listed below.

HIGH

30% of the data analyzed or more for negative sentiment
20% or more for anomalous activity / bot-like activity
Narrative is focused on Mis-, Dis-, or Malinformation (MDM)
10,000 or more posts

MODERATE

15% to 29.9% of the data analyzed for negative sentiment
10% - 19.9% for anomalous activity / bot-like activity
Some MDM content identified within the narrative
Between 1,001 and 9,999 posts

LOW

Under 15% of the data analyzed for negative sentiment
Under 10% for anomalous activity / bot-like activity
No significant presence of MDM content
Less than 1,000 posts

BLACKBIRD.AI

THANK YOU

To find out more about how Blackbird.AI can support your narrative intelligence efforts, reach out to dferris@blackbird.ai