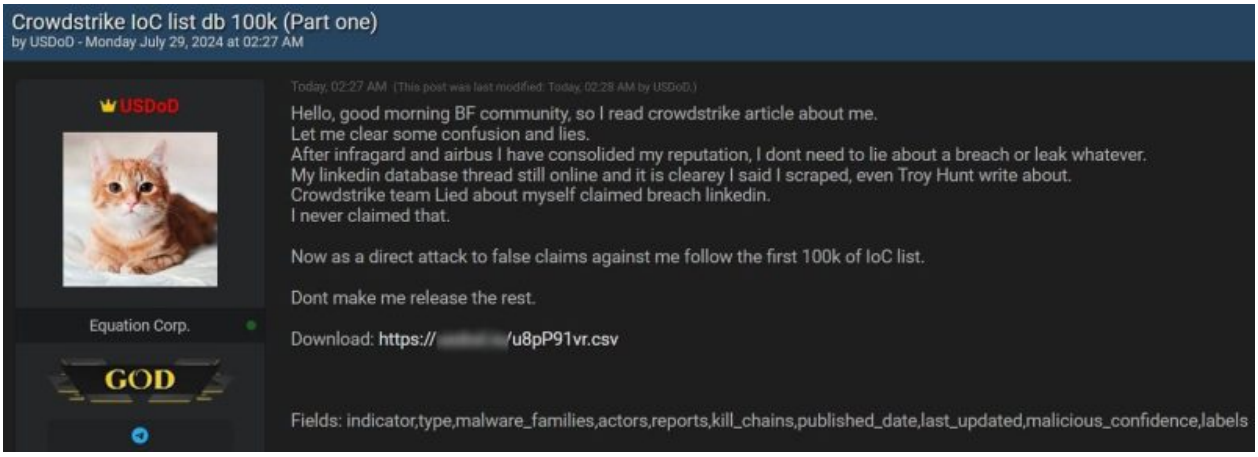
# Hacker Scrapes and Publishes 100,000-Line CrowdStrike IoC List

hackread.com/hacker-scrapes-publishes-crowdstrike-ioc-list/

July 30, 2024

USDoD hacker scrapes and leaks a 100,000-line Indicator of Compromise (IoC) list from CrowdStrike, revealing detailed threat intelligence data. The leak, posted on Breach Forums, includes critical insights into the Mispadu malware and SAMBASPIDER threat actor.

A hacker using the alias USDoD, particularly known for the data breach of FBI's Security Platform **InfraGard**, has leaked what they claim is part one of CrowdStrike's Indicator of Compromise (IoC) list. The data, a 53MB CSV file containing 103,000 lines of information, was released on Breach Forums earlier today, Monday, July 29, 2024.



USDoD hacker on Breach Forums (Screenshot credit: Hackread.com)

This leak follows an earlier claim made by USDoD on July 24, 2024, where they announced CrowdStrike's "entire threat actor list." In their post on Breach Forums, the hacker claimed "I scraped their entire IOC list tho with more than 250 million of data, I will release soon."

In **response**, CrowdStrike presented a measured reaction to USDoD's claims rather than outright dismissing them. The company acknowledged USDoD's claim of leaking their threat actor and IOC lists and analyzed the provided sample data.

However, CrowdStrike also argued that USDoD has a history of exaggerating claims to enhance their reputation, suggesting a degree of scepticism about the current allegations. They specifically mentioned the hacker's claim of leaking a **scraped LinkedIn database** with personal details of over 35 million users in November 2023.

## Contents of the Leak

The leaked sample data analysed by Hackread.com's research team provides detailed information on various Indicators of Compromise associated with the **Mispadu malware**, attributed to the notorious threat actor known as SAMBASPIDER. Here's a breakdown of the key components found in the leaked file:

1. **Hashes and Malware Information**: The CSV file includes various hash types such as MD5, SHA-1, and SHA-256, which are used to identify specific malicious files linked to the Mispadu malware.
2. **Threat Actor**: All entries in the leaked sample data seem to be associated with the threat actor SAMBASPIDER.
3. **Kill Chain Phases**: The data highlights the "Delivery" and "Installation" phases of the cyber kill chain, providing insights into the stages where the malware is delivered and installed on target systems.
4. **Confidence Levels**: Each entry is marked with a high confidence level, indicating the reliability of the threat intelligence.
5. **Threat Types**: The threats are categorized under various types including Banking, Criminal, and Modular, highlighting the multifaceted nature of the Mispadu malware.
6. **MITRE ATT&CK Techniques**: The IoCs are mapped to several MITRE ATT&CK techniques, such as:

- Execution/User Execution
- Discovery/System Checks
- Credential Access/Input Capture
- Credential Access/Credential Dumping
- Command and Control/Data Obfuscation
- Defense Evasion/Obfuscated Files or Information

It is worth mentioning that while addressing USDoD's July 24, 2024, post on BreachForums, CrowdStrike specifically referred to the timestamp of the data as the "LastActive" date, stating the following:

"The sample data contained data with "LastActive" dates until no later than June 2024; however, the Falcon portal's last active dates for some of the referenced actors are as recent as July 2024, suggesting when the actor potentially obtained the information."

The latest leak shows the timestamp as "First Seen: 2024-07-01T00:09:56Z" (indicating the IoC was first detected on July 1, 2024, at 00:09:56 UTC) and "Last Seen: 2024-07-01T01:11:27Z" (indicating the IoC was last observed on July 1, 2024, at 01:11:27 UTC).

Screenshot from the leaked data (Screenshot credit: Hackread.com)

These timestamps help in understanding the activity period of the IoC, indicating how long it has been active or relevant. This information is crucial for threat analysis and response, allowing **cybersecurity professionals** to track the lifecycle and prevalence of specific threats.

## CrowdStrike's Response

In response to our article, a CrowdStrike spokesperson stated "There is no CrowdStrike breach. This threat intel data is available to tens of thousands of customers, partners, and prospects."

To clarify, our article did not claim that a data breach occurred. We reported on the unauthorized scraping and subsequent leak of CrowdStrike's IoC list, which is indeed accessible to a wide range of their clients and partners.

## Implications of the Leak

The disclosure of this detailed Indicator of Compromise (IoC) data might negatively affect organizations that use threat intelligence from CrowdStrike to secure their networks. This information could also be exploited by malicious actors to avoid detection.

At the same time, this information can help cybersecurity researchers and experts strengthen their security mechanism against the Mispadu malware and SAMBASPIDER threat actor.

## Troublesome July for CrowdStrike

The latest security issues came just over a week after CrowdStrike experienced a major problem **due to a faulty update** to their Falcon sensor software, causing widespread system crashes on Windows devices.

Within days, threat actors began exploiting the issue by offering **fake hotfixes** for Windows devices, which in reality infected them with the notorious Remcos RAT. The situation also led Microsoft to **release a tool** to address the issues caused by the faulty CrowdStrike update.

## RELATED TOPICS

1. **World's Leading Cybersecurity Firm Kaspersky Hacked**
2. **X Account of Google Cybersecurity Firm Mandiant Hacked**
3. **Ticketmaster Data Breach: Hackers Selling 560 Million Users Data**
4. **A Minor Typo Brought the Entire Internet Network of Amazon Down**
5. **Cybersecurity Firm Hacks Itself, Finds DNS Flaw Leak AWS Credentials**