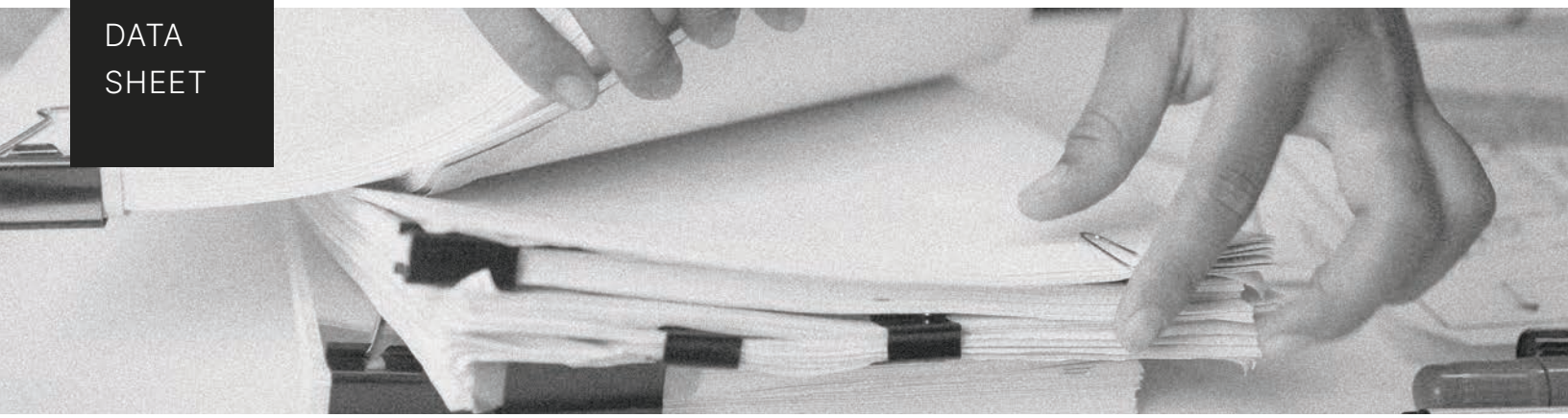
Recorded Future®

DATA SHEET



Identity Intelligence from Malware Logs

Catching Infostealers in the Act to Prevent Identity Fraud

With real-time access to malware log information, Recorded Future Identity Intelligence offers organizations an unmatched, novel source of truth for identity authenticity, empowering organizations to proactively prevent identity fraud and account takeovers resulting from infostealer malware.

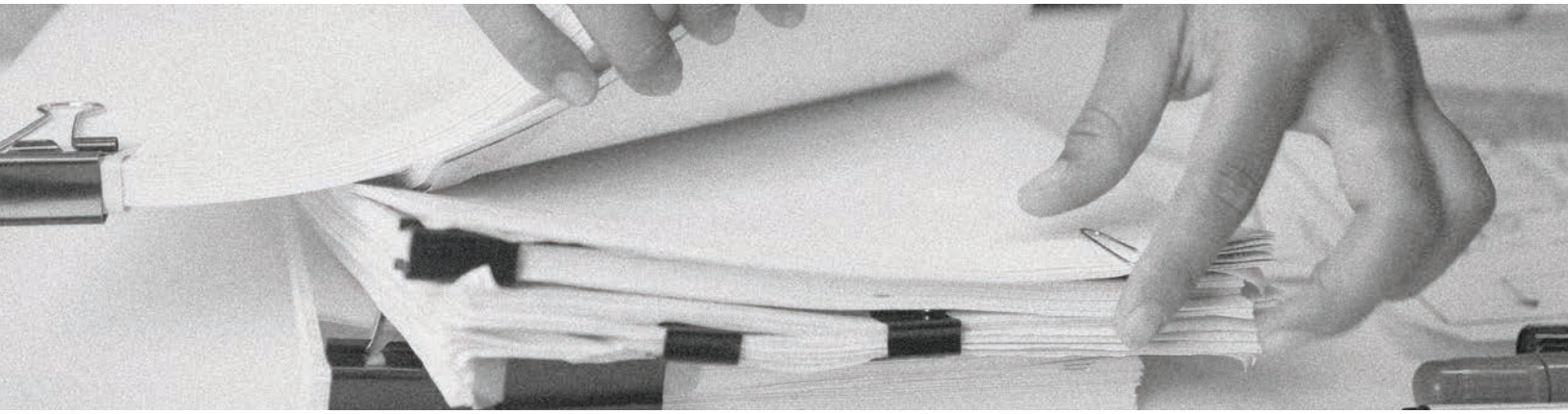
Stolen corporate data such as user credentials regularly ends up on paste sites and dark web channels, allowing cybercriminals to purchase the data, and potentially use it to gain access to an organization's network or systems. Since users often re-use credentials on multiple sites, a threat actor can then launch a credential stuffing (MITRE T1110) attack against any other application that the user may be using.

These recycled credentials also cause issues for organizations trying to monitor for identity compromises, as time can be wasted investigating old credentials that have already been remediated. Unable to keep up with the growing onslaught of alerts and potential attacks on their own, organizations are not able to be proactive and are left exposed to financial, legal, and reputational consequences. And the problem is not limited to the sheer volume of attacks, but the sophistication of attacks is also growing, with advanced evasive tactics making detection much more difficult.

Historically, threat actors would attack application backends to steal credentials. A rise in infostealers like RedLine Stealer, where threat actors leverage malware installed on an endpoint or server to capture and steal information directly from the end user, has been on the rise. This is providing real-time, live credentials stolen directly from the user. With this information, a threat actor can create a synthetic identity of the user and impersonate them online, commit fraudulent activities, exfiltrate information, or escalate privileges to gain additional access to systems.

BENEFITS

- Automate fraud prevention
- Confidently prioritize threats
- Eliminate false positives
- Disrupt attacks before they begin



Recorded Future's Identity Intelligence module provides access into this freshly stolen information, related to both employee and customer identities, allowing organizations to prevent breaches before damage is widely spread. Organizations can then confidently take action and block access to corporate systems before the compromised identities of employees are exploited, and access greater visibility that ensures customer credentials are secure when accessing any portals or information. This ultimately empowers organizations to be more proactive in preventing identity fraud, and dramatically reduces the amount of time it takes to prioritize and respond to real risks to the business.

What Makes Malware Logs Different from Credential Data Dumps Found on the Dark Web?

- **High-Fidelity Intelligence** vs. information that requires checking validity against internal or customer identity databases
- **Unaltered, New Compromises** vs. recycled credentials filtered by cybercriminals
- **Intelligence Collected Today** vs. breaches that were potentially collected months ago