MANDIANT®

Mandiant Redline™

Black Hat USA 2013 | Arsenal

PRESENTED BY: Ted Wilson

AUGUST 1, 2013

What is Mandiant Redline?

- Redline provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis, and the development of a threat assessment profile.

- Download the latest version at https://www.mandiant.com/freeware

Redline Answers the Question

Are You Compromised?

MANDIANT®

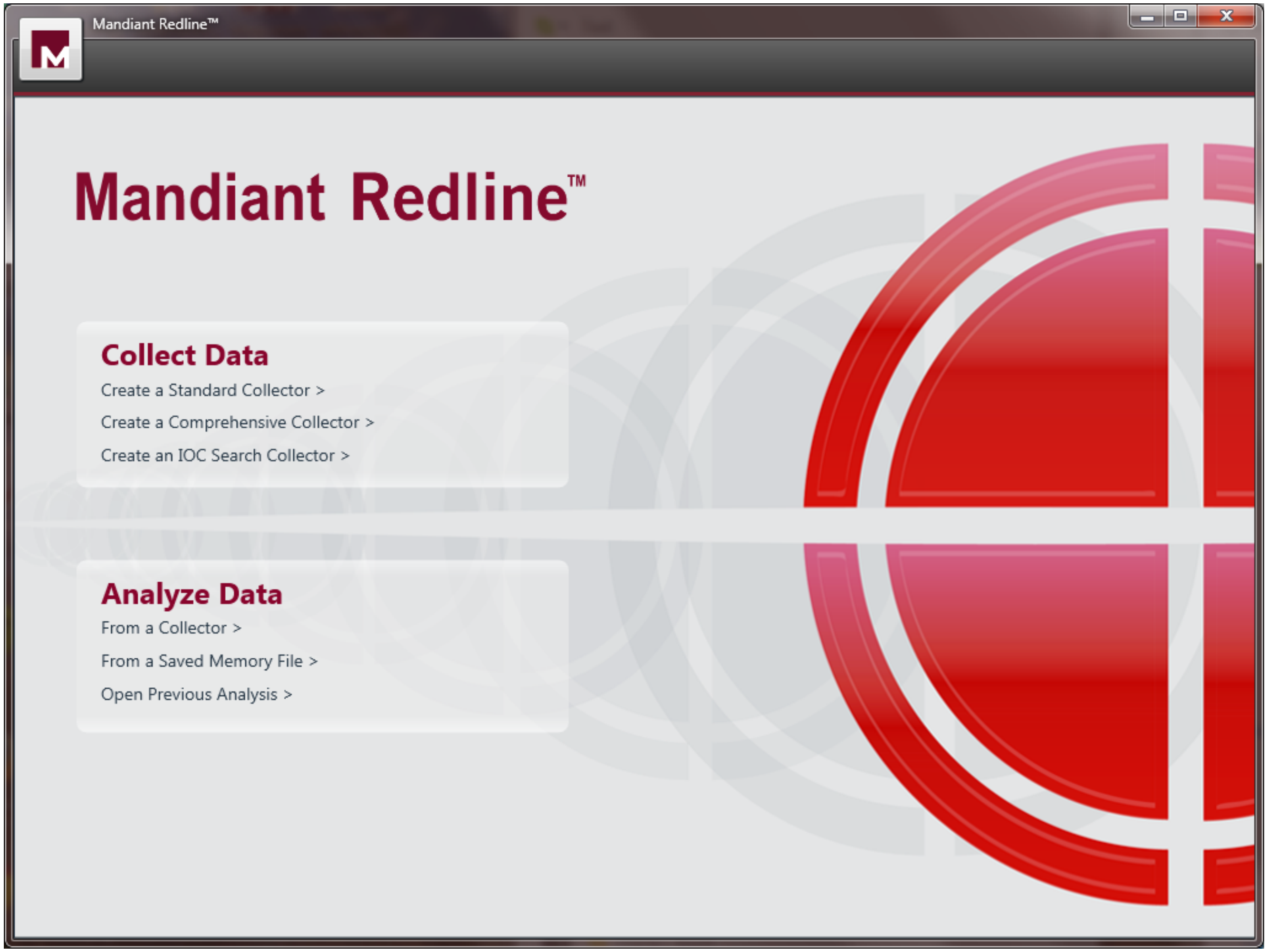
Redline’s Key Capabilities

- Thoroughly audit and collect all run processes, audit data, and memory images.
- Analyze and view imported audit data.
- Streamline memory analysis.
- Identify processes more likely worth investigating based on the Redline Malware Risk Index (MRI) score.
- Perform Indicator of Compromise (IOC) analysis.

Demo Scenario

- **You:** IT specialist at a small company.
- **Situation:** A user has just called you stating that they have accidently clicked on a “strange” link in an email and that ever since their computer has been running “slow”.
- **Question:** Is this user’s computer compromised?
- **Answer:** Mandiant Redline…

Demo



Mandiant Redline™

Mandiant Redline™

Collect Data

Create a Standard Collector >

Create a Comprehensive Collector >

Create an IOC Search Collector >

Analyze Data

From a Collector >

From a Saved Memory File >

Open Previous Analysis >

Works with Memoryze™ 3.0 Collections

- Adds support for:
  - Windows 8 x86 and x64
  - Windows Server 2012 x64
  - IPv6
  - And, forensic reporting of all 12 TCP states

- Download at https://www.mandiant.com/freeware

Questions

- Arsenal Station 7 from 12:45 through 15:15
- Email at redline@mandiant.com
- Discuss on the Mandiant forums at https://forums.mandiant.com/