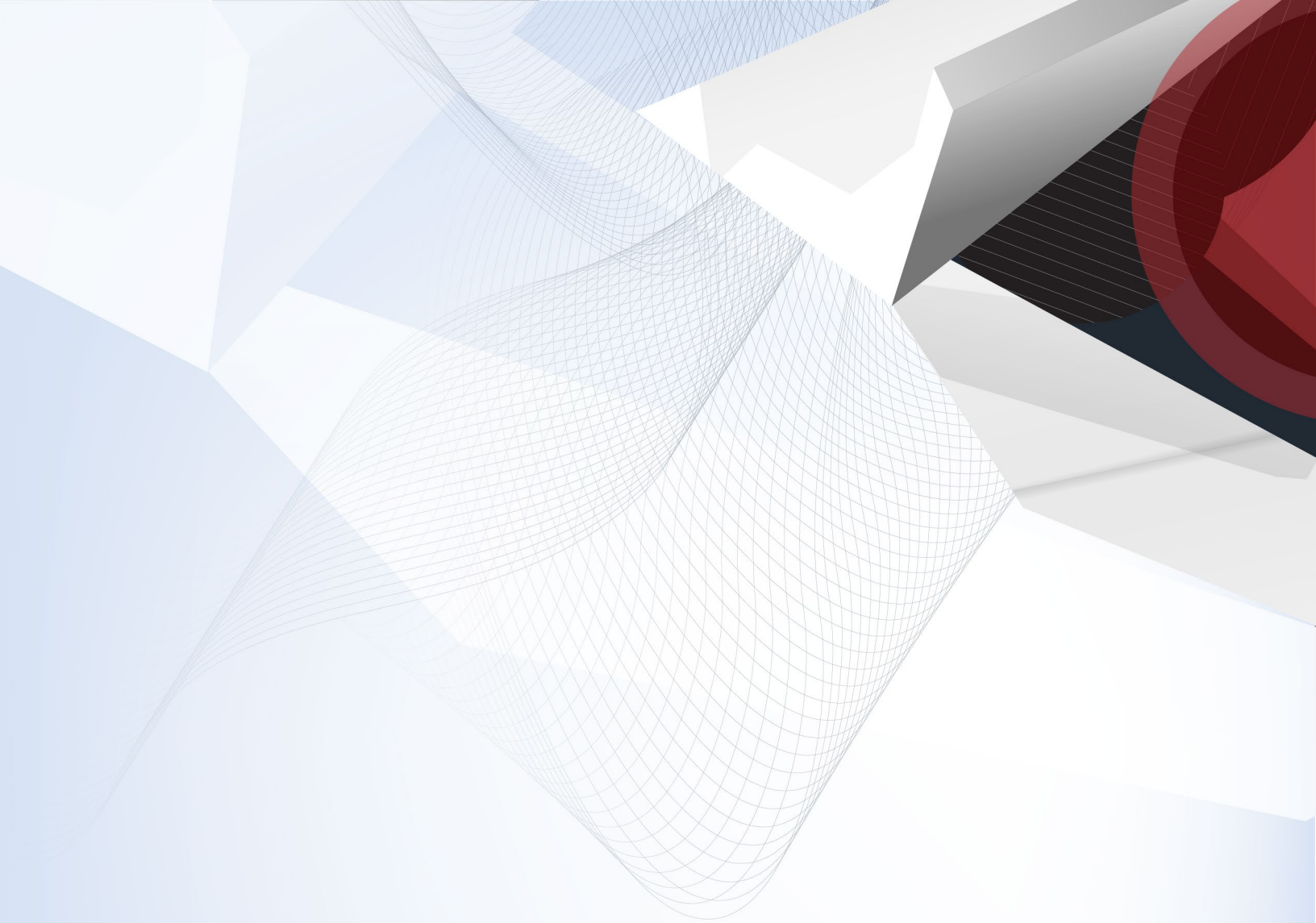

Redline Release Notes

FireEye

March 11th 2020

CONTENTS

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

Redline Release Notes

Release 2.0

Revision 1

FireEye Contact Information:

Website: www.fireeye.com

Support Email: redline@fireeye.com

Support Website for FireEye customers: csportal.fireeye.com

Phone:

United States: 1.877.FIREEYE (1.877.347.3393)

United Kingdom: 44.203.106.4828

Other: 1.408.321.6300

Announcements

Redline 2.0 is now able to collect investigative artifacts available from OS X and Linux environments. Redline will also import and analyze triages and acquisitions from the FireEye Endpoint Security audit viewer.

Data collection is supported in the following OS environments:

Windows	OS X	Linux
Windows 8	OS 10.9 (Mavericks)	RHEL 6.8-6.10, 7.1-7.6, 8
Windows 8.1 Update 1	OS 10.10 (Yosemite)	CentOS 6.8-6.10, 7.1-7.6
Windows 10	OS 10.11 (El Capitan)	
Server 2008 R2	OS 10.12 (Sierra)	
Server 2012, 2012 R2	OS 10.13 (High Sierra)	
Server 2016	OS 10.14 (Mojave)	
Server 2019		

Results can be viewed in Redline only on a Windows OS.

What's New

The following sections describes the features that are new in the 2.0 release.

- Redline collector now supports audit collection on OS X and Linux platforms. Results can be viewed on Windows only.

- Redline collector in v. 2.0 no longer supports Windows XP and Windows 2003 Server environments. For these older systems, please continue to use Redline 1.20.

Issues Fixed

The following section describes the issues that were fixed in the 2.0 release.

- Invalid timestamps showing 0001-01-01 00:00:00Z in Tasks and Timeline columns were resolved. **(RED-629)**
- Redline can now display IPv6 where it is appropriate. **(RED-648)**
- Fixed issue with Redline adding its startup directory to File audit files with unknown path. **(RED-520)**
- Improved navigation performance in Process and File audits. Improved tagging performance in all audits. **(RED-645)**
- Out of memory exceptions were resolved. Redline now supports up to 4 GB of RAM on 64-bit Windows. **(RED-628)**
- Port information is now correctly shown in Process details. (**RED-617**)
- Correctly processing file audits where files have an invalid timestamp in PE header (**RED-623**)
- Resolved issue with showing audit as "Not Collected" even though it is present in imported data (**RED-624**)
- No longer showing two "File System" audits in audit list. (**RED-627**)

- Removed thousands separator for EID values in Event Log audit. (**RED-634**)
- Now Redline collector for Windows can be run from folder with space in full path. (**RED-646**)