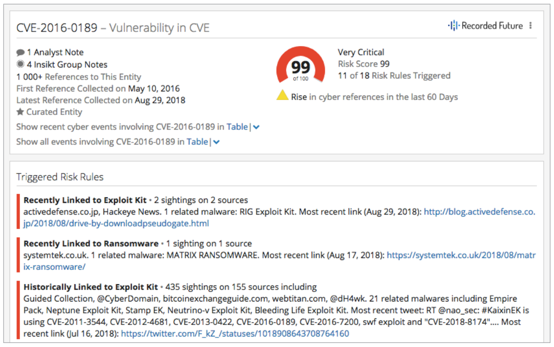

CVE-2016-0189 – Vulnerability in CVE

1 Analyst Note
4 Insikt Group Notes
1 000+ References to This Entity
First Reference Collected on May 10, 2016
Latest Reference Collected on Aug 29, 2018
Curated Entity
Show recent cyber events involving CVE-2016-0189 in Table |
Show all events involving CVE-2016-0189 in Table |

Very Critical
Risk Score 99
11 of 18 Risk Rules Triggered
Rise in cyber references in the last 60 Days

Triggered Risk Rules

Recently Linked to Exploit Kit • 2 sightings on 2 sources
activedefense.co.jp, Hackeye News. 1 related malware: RIG Exploit Kit. Most recent link (Aug 29, 2018): http://blog.activedefense.co.jp/2018/08/drive-by-downloadpseudogate.html

Recently Linked to Ransomware • 1 sighting on 1 source
systemtek.co.uk. 1 related malware: MATRIX RANSOMWARE. Most recent link (Aug 17, 2018): https://systemtek.co.uk/2018/08/matrix-ransomware/

Historically Linked to Exploit Kit • 435 sightings on 155 sources including
Guided Collection, @CyberDomain, bitcoinexchangeguide.com, webtitan.com, @dH4wk. 21 related malwares including Empire Pack, Neptune Exploit Kit, Stamp EK, Neutrino-v Exploit Kit, Bleeding Life Exploit Kit. Most recent tweet: RT @nao_sec: #KaixinEK is using CVE-2011-3544, CVE-2012-4681, CVE-2013-0422, CVE-2016-0189, CVE-2016-7200, swf exploit and "CVE-2018-8174".... Most recent link (Jul 16, 2018): https://twitter.com/F_kZ_/statuses/1018908643708764160

DETAILS

Vendor: Recorded Future

Solution: Recorded Future

Price: Starting at $65,000.

Contact: recordedfuture.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths: A strong collection of feeds and reports to empower any intelligence program. The browser plugin is a great addition to an already strong solution.

Weaknesses: None that we found.

Verdict: This product is one of the best we looked at this month. We can really see why most other solutions in this space integrate with Recorded Future. This is a must-have in your organization and why this is the SC Lab Approved solution.

Recorded Future

**363 Highland Avenue
Somerville, MA 02144**

1-617-553-6400

info@recordedfuture.com

www.recordedfuture.com

Recorded Future

Recorded Future

Recorded Future should be a familiar name to any security professional who has researched multiple products in this technology space. Recorded Future has been providing data and intelligence for more than nine years and many vendors incorporate Recorded Future's feed into their own platforms. The fact that so many trust and refer to this company's data and research speaks volumes to the benefits of integrating Recorded Future into a threat intelligence program.

Recorded Future data is a unique combination of 65 integrated feeds and reports aimed at threat intelligence platforms. By using patented machine learning, the solution can handle the same volume of data, received in real-time, that it would take 8,000 humans working full-time for an entire year to review. The focus of the analysis is on trends, patterns and risk scoring. Once the data is analyzed, a security analyst can use an intuitive web application or API to gain access to threat intelligence results.

To enhance analysts' efforts, Recorded Future scours and analyzes structured and unstructured intelligence globally from technical, open and dark web sources and aggregates customer-proprietary data. The goal is to deliver enriched intelligence, rather than isolated and unintelligible threat feeds. Data is updated in real time so the intelligence in context stays current. The centralized information is then processed through a combination of machine learning, natural language translation and review by researchers. Only then is the output ready for human analysis and collaboration.

Upon first logging in, we found the landing page to contain primary data points relevant to the user. The layout is simple, not overwhelming. This makes the solution's Intel Cards easy to locate and review. Intel Cards are dossier-like intelligence summaries that focus on two dimensions of the threat space. The first is IP-based, highlighting the substantiated information gleaned from various sources on the web and numerous feeds, all of which culminate in a Dynamic Risk Score. The second Intel Card indicates vulnerability per potential exploit, which is determined by the NVD's CVSS risk score. In both cases, a higher score indicates a more serious threat.

More recently, Recorded Future expanded its mission, aiming to develop an all-in-one threat intelligence solution for its customers so they would not necessarily need other platforms to make direct use of the company's data. The belief is that all threat intelligence organizations should move toward having one spot to house all of their threat intelligence feeds. An example of this movement toward holistic efficiency is a tailored browser plugin that can directly scan webpage content for indicators of compromise (IOCs).

Otherwise, Recorded Future's intelligence can be tailored and customized for specific use cases before integrating with security technologies such as SIEM, ticketing, incident response, SOAR and more. As a result, customers can share reports with other analysts; export to csv, json, docx, and STIX; or make use of an API for even greater flexibility.

The standard starting package is $65,000, although there are some less expensive alternatives, and support is available 24/7.

*– Dan Cure;
reviewed by: Matthew Hreben & Michael Diehl*