Recorded Future

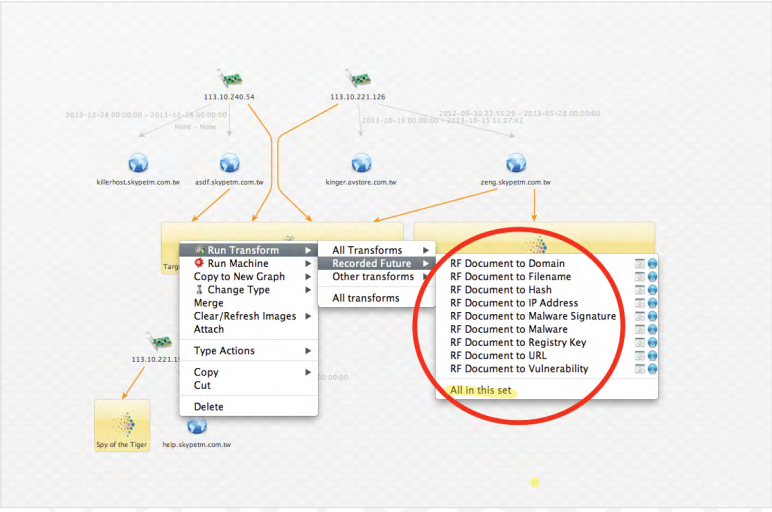
DATA SHEET

Recorded Future for Maltego

Recorded Future transforms for Maltego make it simple and fast to fuse real-time threat intelligence into Maltego investigations. The transforms help you easily enrich and add context to the threat indicators you are investigating — and enable you to move smoothly between enrichment with real-time threat intelligence from the entire web and other open or confidential data sources.

Discovering and validating known IOCs (indicators of compromise) can be a daunting task for any cyber security operation. Building out a comprehensive set of quality IOCs to enhance your detection and attribution capabilities is key to your success. Security analysts need the ability to quickly determine if a digital artifact contained in a SIEM (security incident event management) alert from the IDS or proxy firewall is malicious or benign in real time. Doing so could make the difference between an undetected system-wide breach that causes irreparable damage to your organization's public reputation and successfully short circuiting a multi-stage attack or, better yet, preventing the adversary from gaining access to your network in the first place.

The Recorded Future transforms for Maltego make it easy for security analysts to discover and validate known IOCs in the vast expanse of the open, deep, and dark web while simultaneously giving a unified view and streamlined workflow between Recorded Future and Maltego. Recorded Future uses the core Maltego entities (IPv4, Domain, URL, etc.) and the malware entities defined by the Malformity project (hash, filename, registry entry, etc.) — no need to reinvent the wheel.



Why Recorded Future

Quickly discover and validate IOCs with threat intelligence enrichment from the entire web.

Gain instant context around an IOC with Recorded Future Intel Cards that summarize all related threat indicators including threat actors, malware, and vulnerabilities.

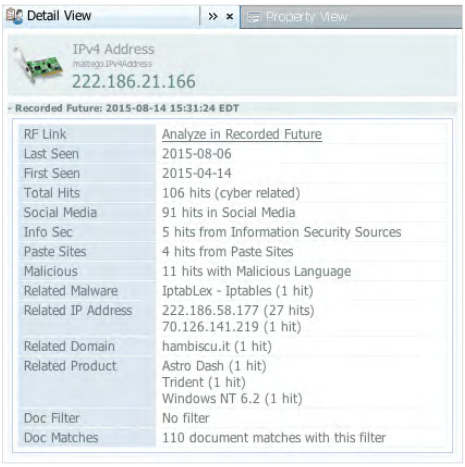
Make analysis easier with a unified view and streamlined workflow between Recorded Future and Maltego.

MALFORMITYLABS

Recorded Future for Maltego transforms have been developed through our partnership with Malformity Labs.

More Intelligence

Recorded Future packs a lot of intelligence into the entities returned by our Maltego transforms. An intelligence summary is returned for IP addresses, domains, and hashes and appears in the Detail View. The summary lists related infrastructure, malware, or CVE vulnerabilities. The summary below, for example, shows an IP address recently linked to the IpTabLex botnet.

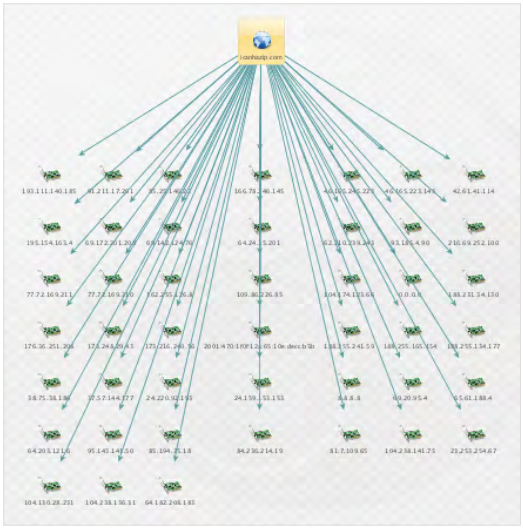


Recorded Future also provides intelligence on document entities. Below is the summary for a recent blog post about CVE-2015-3113, which shows how the included source link can be used to read the original source. This improved summary gives you a clear "information scent" for what's available in that document.

More Efficiency

Building on the above intelligence summaries, Recorded Future offers additional transforms for IP addresses, domains, and hashes that retrieve those top related entities directly — without drilling down into detailed document-level intel. This makes it faster to pull related entities into investigations, vet them for hits in your other technical intel sources, and focus investigations on those interesting multi-source hits.

Below is a graph snippet with the top 12 hits for a specific domain — one that is not malicious per se, but is reportedly exploited as secondary infrastructure. After checking off these IPs against other internal logs and other intel sources, one can zero in on the interesting ones.



More Drilldown

For some entities, these summaries cover a lot of information — more than can readily be pushed back into Maltego. The full summary is available through a drilldown link back to Recorded Future. The Recorded Future Intel Card is the beginning of the summary for that same domain. We've also added deep links into Recorded Future for documents so you can slice and dice all of the events reported in the document, and access any cached content.

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA | © Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners. | 09/16

Recorded Future

REQUEST A DEMO

@RecordedFuture | www.recordedfuture.com