



Vertex

Synapse Bootcamp

Module 21

More Fun with Spotlight

v0.4 - May 2024



Objectives

- Describe additional Spotlight Tool features
- Understand use cases for the Table Extractor
- Know what a Spotlight Extractor is
- Create and use helpful Extractors
- Leverage the Spotlight Tool and Threat Intel Workflow together
- Describe some considerations when processing reports



Spotlight Table Extractor



Spotlight Table Extractor

- Spotlight makes a "best effort" to capture arbitrary HTML
- Cannot account for every website layout
 - o Pop-ups, banners, scrolling...
 - o Save as PDF does not fix everything
- Spotlight recognizes HTML **tables**
- Captures and displays for review
- Useful for:
 - o Table-based data not captured cleanly
 - o Creating additional nodes

IP Address	Target Port	Domain(s)
165.232.186[.]197	80, 443, 4433	api.infinitycloud[.]info connect.infinitycloud[.]info ns.infinitycloud[.]info
167.71.226[.]171	80, 81, 82, 443, 769, 4433, 8086, 8089	file.wonderbackup[.]com connect.infinitybackup[.]net share.infinitybackup[.]net sync.wonderbackup[.]com
104.248.153[.]204	82, 443	update.wonderbackup[.]com login.wonderbackup[.]com ns1.infinitybackup[.]net
143.110.189[.]141	443	mfi.teleryanhart[.]com ads.teleryanhart[.]com
172.105.34[.]34	8081, 8087, 8443, 8888	jlp.ammopak[.]site kwe.ammopak[.]site lxo.ammopak[.]site dfg.ammopak[.]site fwg.ammopak[.]site
194.195.114[.]199	8080, 8443, 9200	connect.clinkvl[.]com



Spotlight Table Extractor Demo



Spotlight Extractors



Spotlight Quick Forms

- Highlight text
- Tell Spotlight what node to create
- Automatically link important references:
 - o Threat names
 - o Malware names
 - o CVE numbers
 - o Industry names
 - o Country / region names
 - o More!

Executive Summary
Talos continuously monitors malicious emails camp...
one specific spear phishing campaign launched aga...
Palestine, and specifically against Palestinian law en...
This ca selected: Palestine 7, using a spear p...
deliver... order to remotely...
system...
techniq...

create node > geo:name
extractors > ou:industryname
document details > ou:name



Quick Forms Limitations

- Text must be the **primary property** of the node you create
- Cannot create a guid node from text

This campaign started in April 2017, using a spear phishing technique to deliver the MICROPSIA payload in order to remotely access target systems. Although this is a well-known technique for attackers, the malware itself was developed in-house.

selected: MICROPSIA

it:dev:regkey

it:prod:softname

create node > other

Add Node

risk:tool:software

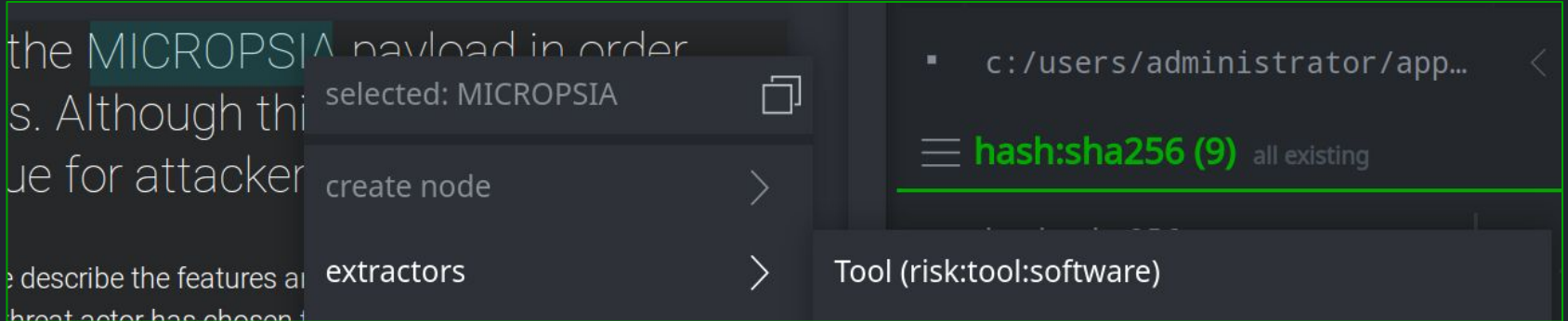
risk:tool:software:taxonomy

A red arrow points from the 'other' option in the context menu above to the 'Add Node' dialog box.



Extractors

- **Extractors** use Storm to tell Spotlight what to create
- Highlight any text > create any node!
- Saved in your Spotlight **Preferences**
- Available from **right-click** menu





Extractors Demo



Spotlight and the Threat Intel Workflow



Spotlight and Threat Intel

- Spotlight allows us to extract more than IOCs
 - Quick Forms: threat names, industry names, victim / target organization names...
 - Extractors: threats, vulnerabilities...
- Use Spotlight with the Threat Intel Workflow
 - Add detail on threats, malware...
 - Easily link relevant nodes



Spotlight and Threat Intel - Demo



Spotlight Wrap Up



Considerations

- How much is enough?
 - Do what works for you!
 - New vs. experienced users
 - Activity we care about vs. activity we don't
- Set guidelines / expectations
 - When / what to process
 - Minimum level of data extraction
 - Agreement on tags / tag structures to use
 - Any review / approval process



Summary

- Spotlight's **table extractor** can process HTML tables
 - Similar to the Ingest Tool
- Spotlight **extractors** can create nodes from selected text
 - Specify how Spotlight should handle the data
- Both use Storm to simplify / automate tasks
- **Spotlight** and the **Threat Intel Workflow** together:
 - Help create and capture operational and strategic threat data