Maltego In The Enterprise

J. David Bressler

Senior Security Consultant

About Me

- Senior Security Consultant, GuidePoint Security
- I like to Make Things
- I like to Break Things
- My Alphabet Soup: OSCP, MCSA, ABCDEFG… (You know the rest)

Contact Me

- Twitter: @bostonlink (Say Hello!)
- Github: https://github.com/bostonlink

GuidePoint SECURITY

What is Maltego?

- Created by Paterva www.paterva.com
- Reconnaissance and Information Gathering
- Visualize Gathered Information
- Customizable!

GuidePoint SECURITY

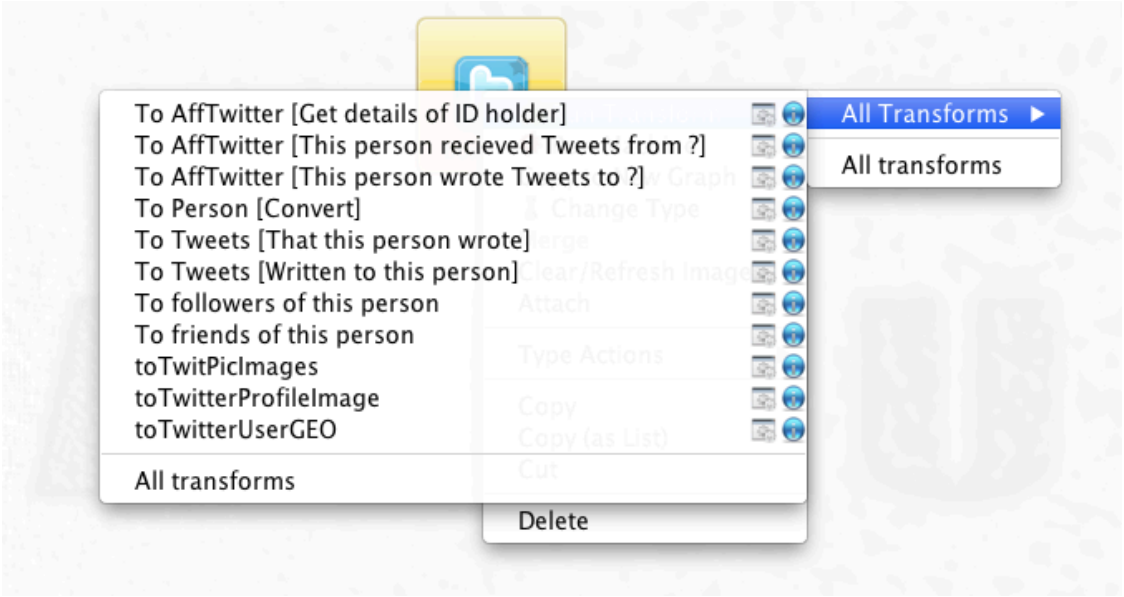
Why Maltego In the Enterprise?

- Single tool for Information Gathering and Analysis
- Integrate internal tools/APIs with custom transforms
- And More! Think outside the box!

GuidePoint SECURITY

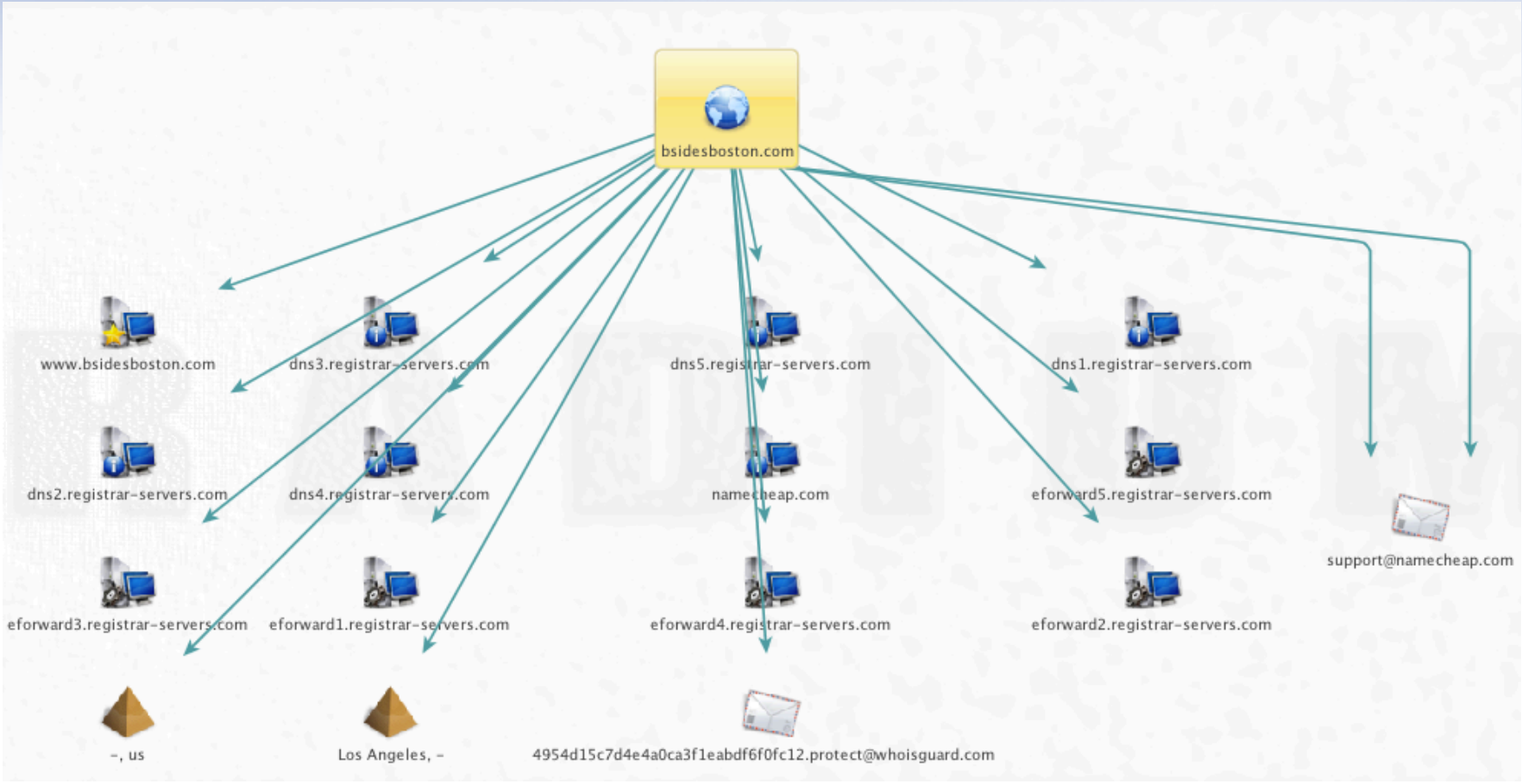
Maltego Transforms

backend or remote scripts/programs that pull information from specific sources and creates entities



GuidePoint SECURITY

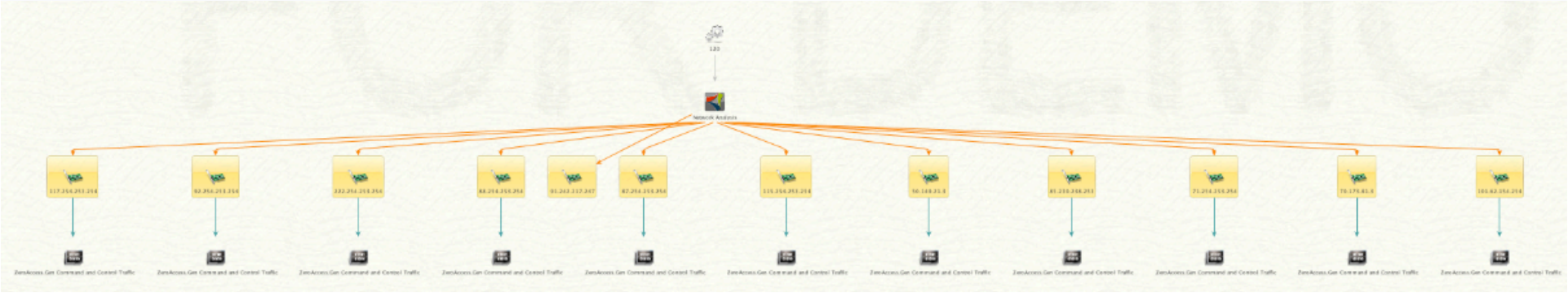
Built-in/Remote Transforms



GuidePoint SECURITY

Local Transforms

Example of CuckooForCanari and PAMalt Canari Framework transform packs



GuidePoint SECURITY

Which Transform Should I Use?

- Depends on your overall goal & architecture
- Internal systems and tools
  - Local Transforms or Internal TDS Server
- External data sources
  - Local or Remote Transforms

The Canari Framework

- Created by Nadeem Douba (Sploitego)
- Maltego Local Transform Development framework
- www.canariproject.com
- forums.canariproject.com (Community)

GuidePoint SECURITY

The Canari Framework

- No need to focus on the XML output formatting
- Focus on the data gathering and parsing logic
- Gives you the easy ability to install transforms packs, and a lot more!

```
bostonlink:~ $ canari
usage: canari help <command>

Shows help related to various canari commands

positional arguments:
  <command>   The canari command you want help for (csv2sheets, list-commands,
              shell, help, rename-transform, run-server, debug-transform,
              delete-transform, create-transform, uninstall-package, run-
              transform, generate-entities, version, mtgx2csv, install-
              package, banner, create-package)

optional arguments:
  -h, --help  show this help message and exit
bostonlink:~ $
```


GuidePoint SECURITY

Why Integrate Other Tools?

1. Because It's AWESOME!
2. Value of data
3. To visualize internal enterprise data
4. Ability to easily pivot from internal data to external data

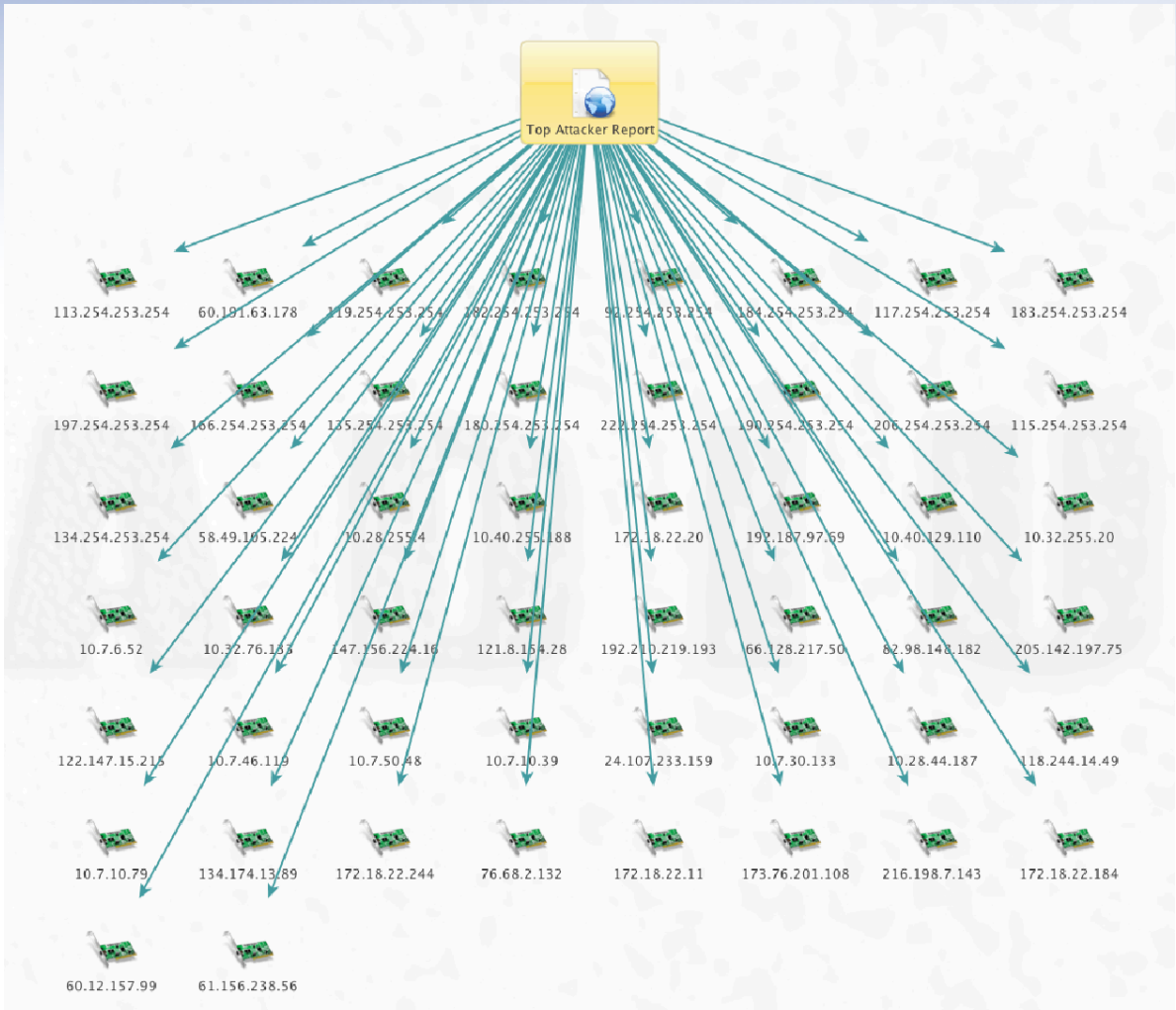
GuidePoint SECURITY

PAmalt Overview

- Palo Alto Networks Firewall Transform Pack
- Used to quickly visualize detected top attacks, threats, malware, etc.

https://github.com/bostonlink/pamalt_canari

PAmalt Example



GuidePoint SECURITY

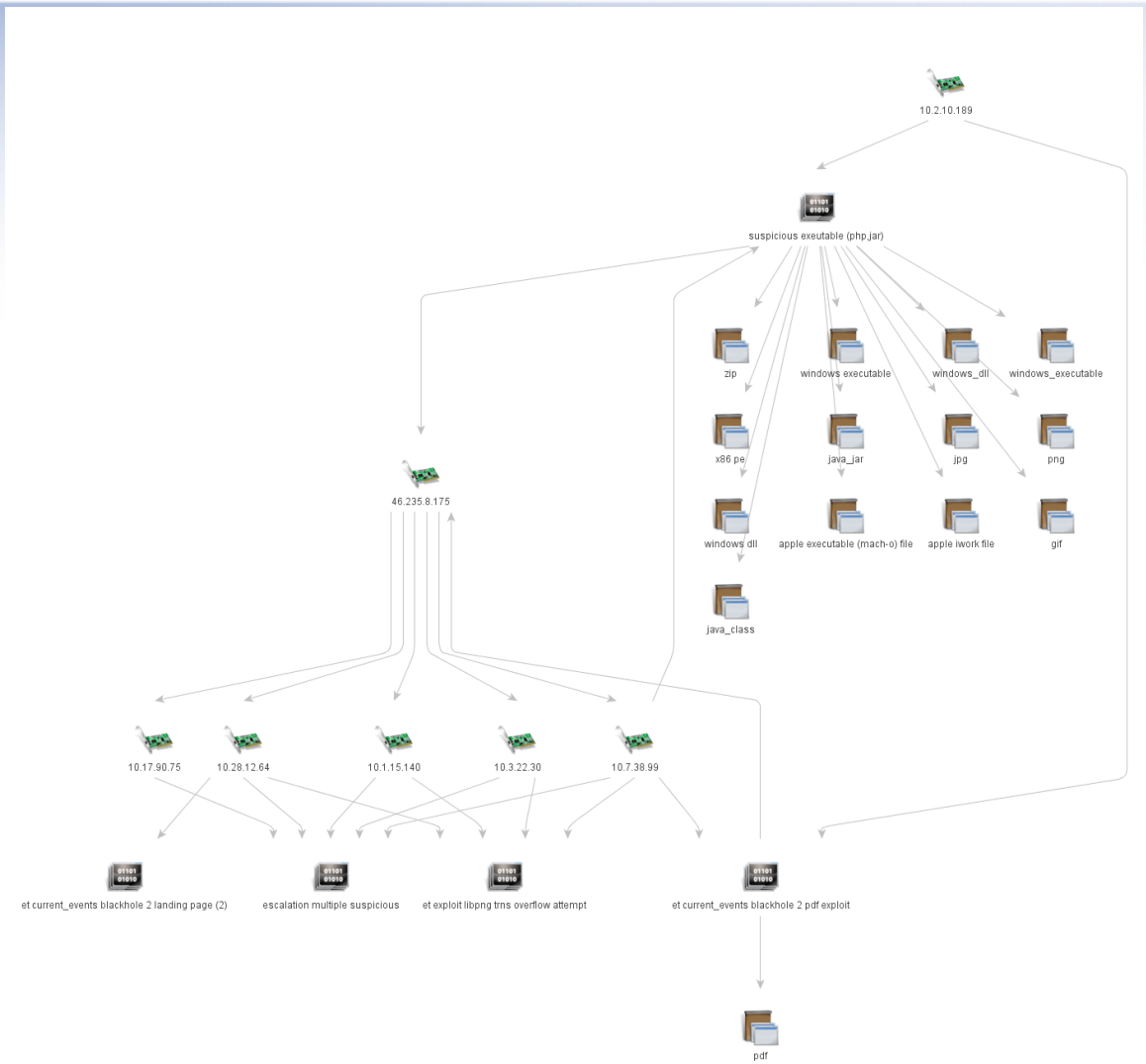
NWmaltego Overview

- RSA Netwitness NSM/Packet Capture Transform Pack
- Used to quickly query Netwitness for metadata parsed from network sessions

https://github.com/bostonlink/nwmaltego_canari

GuidePoint SECURITY

NWmaltego Example



GuidePoint SECURITY

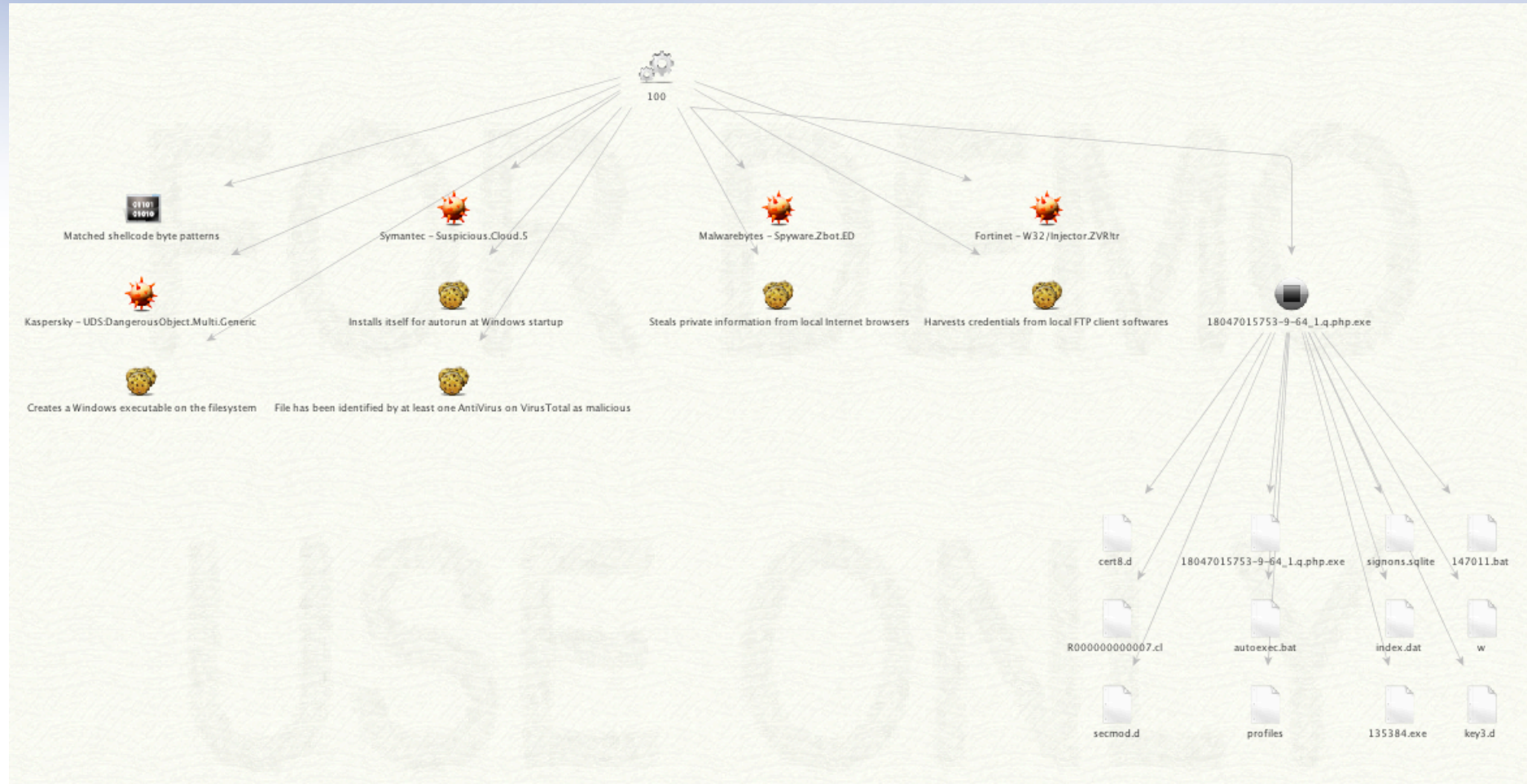
CuckooForCanari Overview

- Cuckoo Sandbox Transform Pack
- Used to visually display dynamic malware analysis

https://github.com/bostonlink/cuckooforcanari

GuidePoint SECURITY

CuckooForCanari Example



GuidePoint SECURITY

Nextego

- Rapid7's Nexpose Maltego Transforms
- Launch a Nexpose Vulnerability Scan on a Host within Maltego
- Display Ports, Services, Service Versions / Fingerprints
- Display Vulnerabilities, Metasploit Modules, exploit-db Exploits available
- Version 1.0 Released Today!

GuidePoint SECURITY

Nextego Demo

Demo Time!

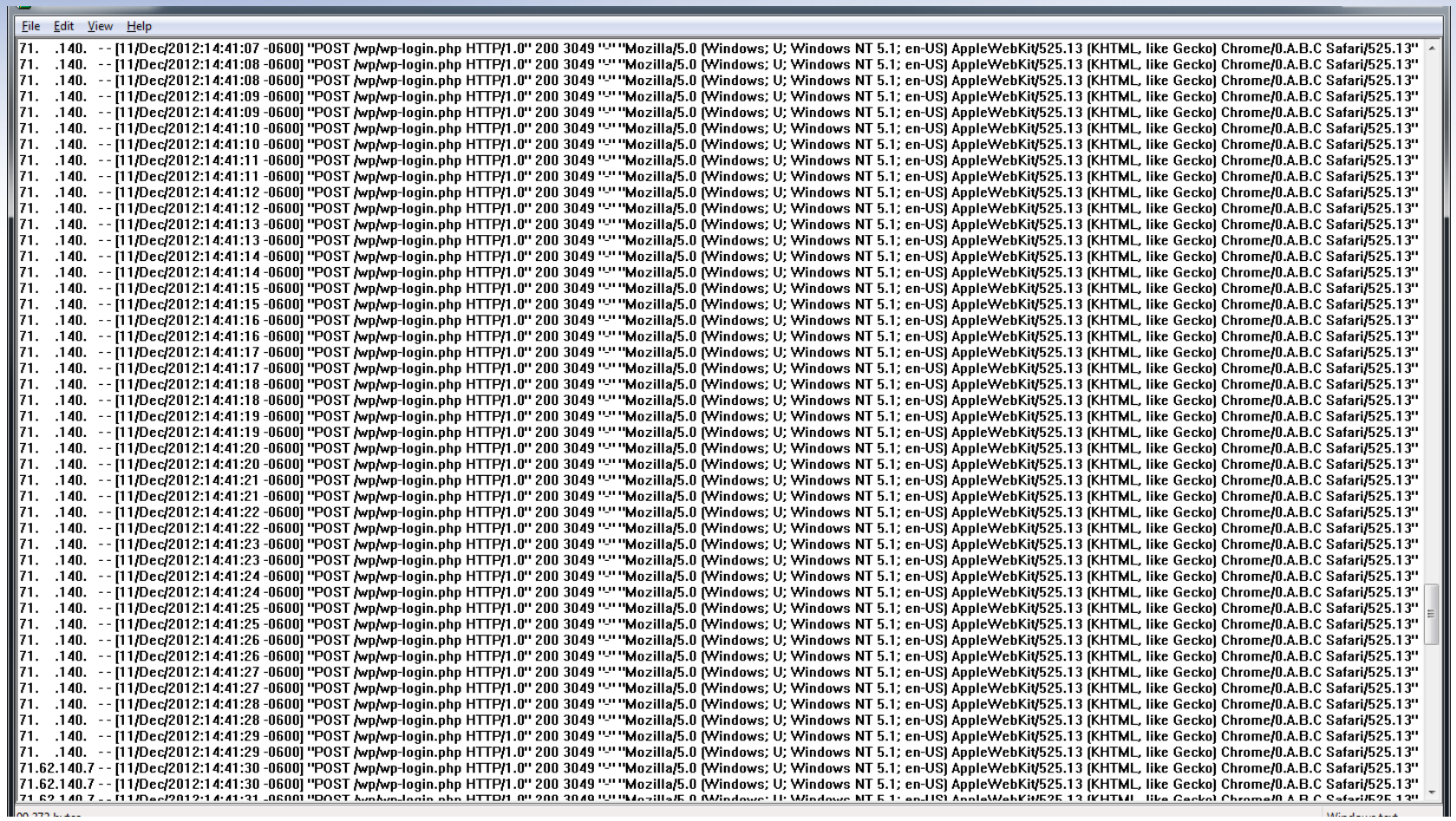
GuidePoint SECURITY

Putting It All Together

- Integration with multiple tools can paint a better picture for security teams
- Having the ability to visualize data from multiple sources in one window is VALUABLE
- Ability to do high-level analysis on visualized data to come to a quicker conclusion

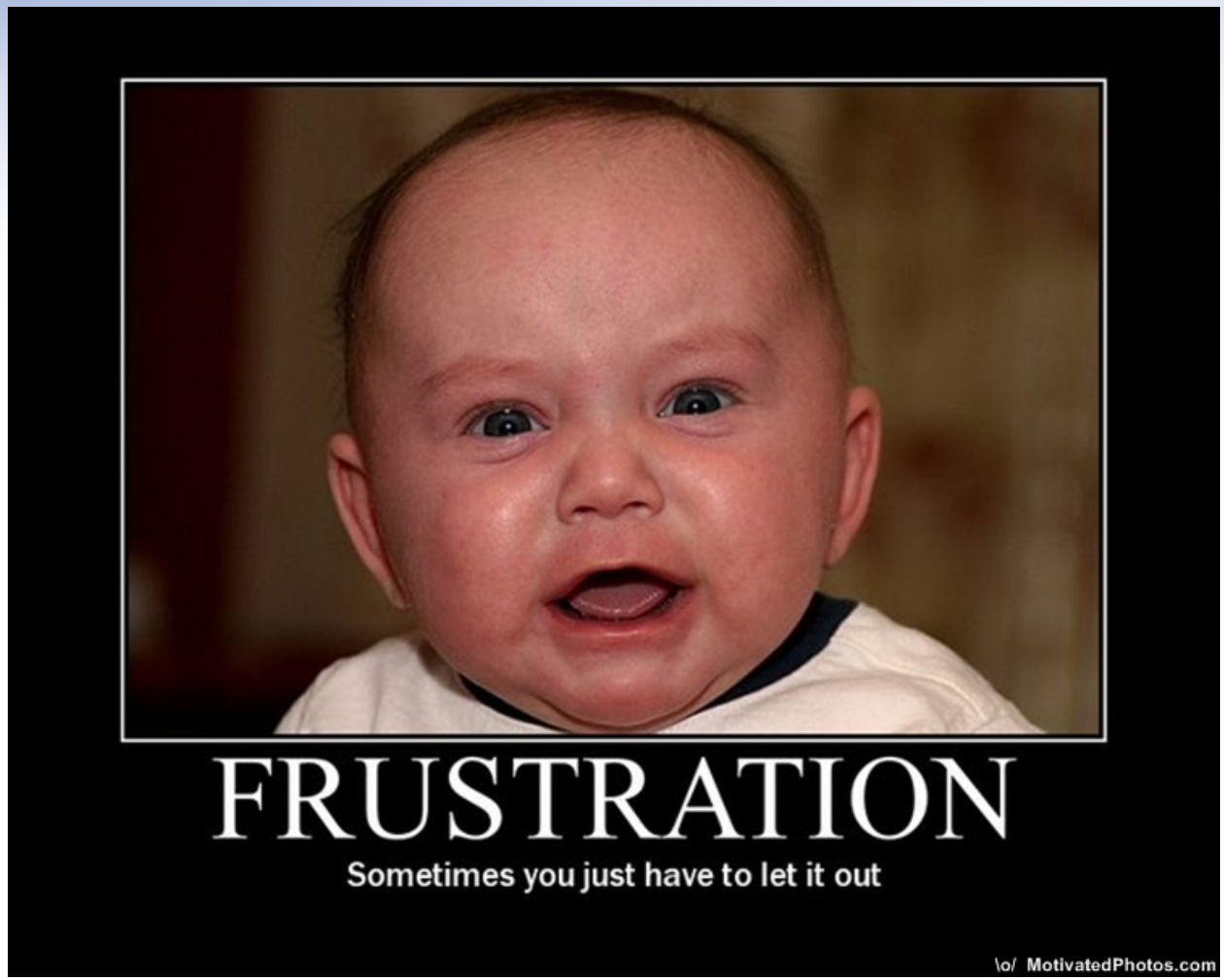
GuidePoint SECURITY

No One Likes Looking At This



GuidePoint SECURITY

Drives You To Look Like This



GuidePoint SECURITY

Special Thanks!

- GuidePoint Security (@GuidePointSec)
- Paterva (@Paterva)
- Nadeem Dooba (@ndooba)
- Rich Popson (@Rastafari0726)
- The Canari Framework (@canariframework) and community behind it

GuidePoint SECURITY

Questions or Feedback?

GuidePoint SECURITY