Malware Analysis and Intelligence aka Identifying Threats On Your Network

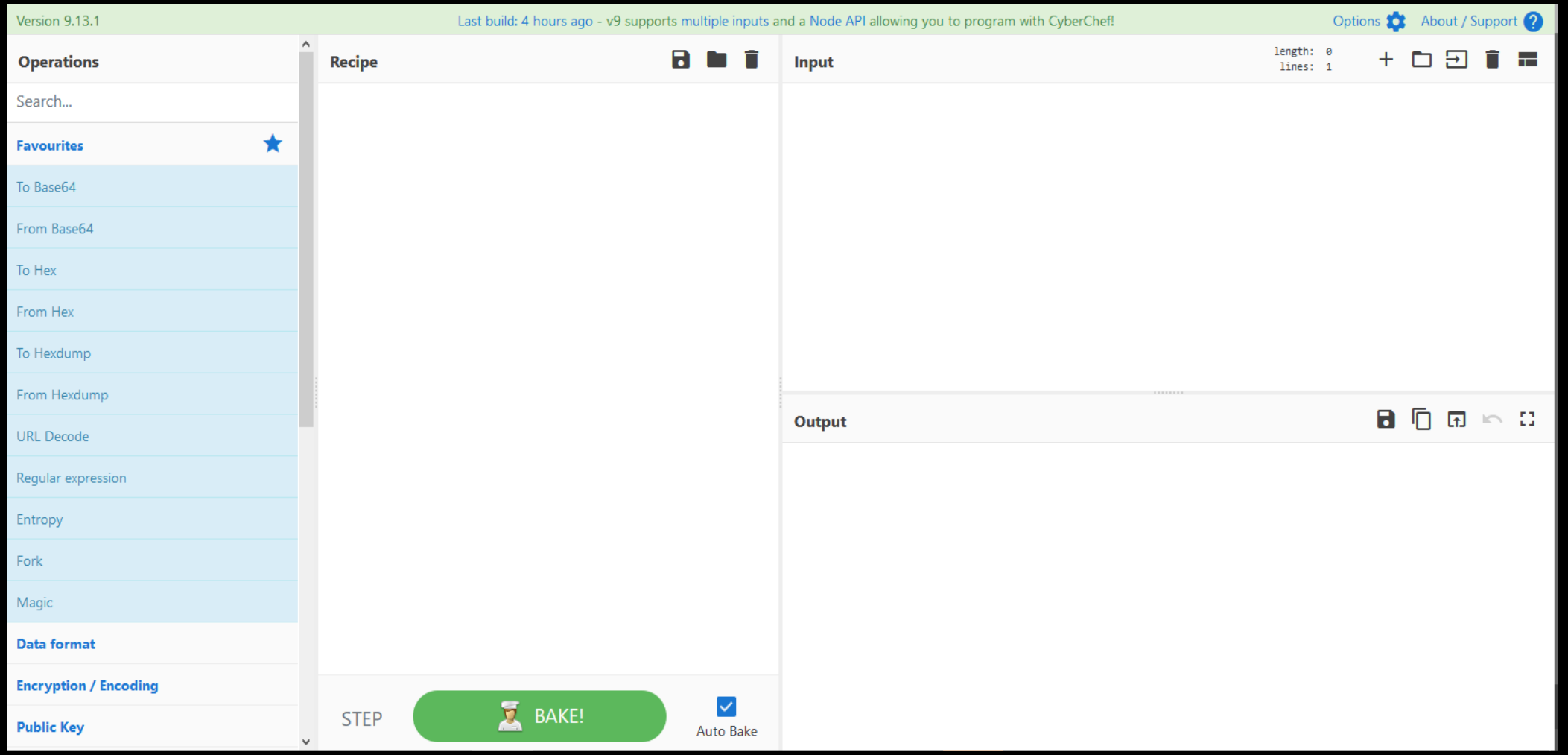
Andrew Plassmeyer
State of Missouri Office of Cyber Security
andrew.plassmeyer@oa.mo.gov

Malware Analysis

- joesandbox.com
  - Requires login
  - https://www.joesandbox.com/analysis/317549 --vbs
  - https://www.joesandbox.com/analysis/317539 --docm
  - https://www.joesandbox.com/analysis/317528 --exe
  - hybrid-analysis.com
  - Login not required, but useful for finding your submissions
  - https://www.hybrid-analysis.com/sample/50e128b4c4defb8a9de0993cf64a90c323611d58cf2aba3fa352f736848733bb/5e2f5729697152759e7d800d --vbs
  - https://www.hybrid-analysis.com/sample/f35eb6d8db1c14dcc6cbf5d7f23c012fb31a51b822d7568d73d0d09a9b6d4cb2?environmentId=120 –docm
  - https://www.hybrid-analysis.com/sample/df3e2bbc127429a987085c4ceece445118ab5c8c0d79417fc5cfc0603db07cfa?environmentId=120 --exe

CyberChef

- Web app for encryption, encoding, data analysis, etc.
- gchq.github.io/CyberChef/



Research tools

- ipvoid.com
  - Lookup various records associated with IP Addresses
  - ipvoid.com/ip-blacklist-check
- virustotal.com
  - Can scan files and websites for malicious content
    - Sometimes results take a while after submission to show bad
  - Search IP addresses to see what is on them
  - Search for file hashes
- infobyip.com/ipbulklookup.php
  - Bulk IP address and URL tool

Research tools Continued

- sitecheck.sucuri.net
  - Site Checker for malware
- urlvoid.com
  - Website reputation checker
- threatcrowd.org
  - Visual IP address and URL information
- threatminer.org
  - Intelligence portal for searching

Research Tools

- urlscan.io
  - View webpages without actually going to them
- otx.alienvault.com
  - Threat intelligence community
- mxtoolbox.com
  - Lookup MX records for mail servers

Research Tools

- Missouri Office of Cyber Security IP Blacklist
  - portal.cybersecurity.mo.gov/util/ip_blacklist.txt
- Missouri Office of Cyber Security URL Blacklist
  - portal.cybersecurity.mo.gov/util/url_blacklist.txt

Blogs

- portal.cybersecurity.mo.gov
  - Cyber security articles worth mentioning
  - Articles about malware that the State of Missouri receives.
- krebsonsecurity.com
- isc.sans.edu
- blog.talosintelligence.com
- bleepingcomputer.com
- nakedsecurity.sophos.com
- blog.malwarebytes.org
- grahamcluley.com
- securelist.com

Questions?