PRODUCT BRIEF

Malware Module

A Powerful Addition to the Augury™ Platform

Apply network forensics at Internet scale in a proactive way. Optimize security operations, accelerate incident response, monitor your supply chain for compromised third-party vendors, and even identify attacks underway against peers in your industry. With the visibility the Augury platform provides, our clients and partners regularly see new malicious infrastructure being stood up and are able to block attacks before they are even launched.

Adding the Malware Module to this solution expands this already unparalleled visibility.

The Malware Module is an integrated malware sandbox and correlation engine that expands Augury insight to include the malware associated with the infrastructures and activity being investigated. It not only provides the results of our own dynamic and static analysis, but cross references with leading antivirus vendors to provide a detection rate.

Expand understanding and visibility into APTs and threat group infrastructures.

1. Determine campaign scope by correlating malware with Internet signal to see the size and locations of the infection base.
2. Expand your understanding and visibility into APT and threat group infrastructures.
3. Accelerate identification of additional infrastructure and potential victims.
4. Ensure comprehensive prevention and/or remediation by identifying additional malware associated with a campaign and additional campaigns associated with your malware samples.
5. Tie together malicious campaign components correlating attributes, such as DNSRR, URL, MUTEX, and registry modification.

Correlate

Correlate Augury results against our malware samples. Just left click and go.

Search

Search our malware library.

Upload

Detonate your samples in our sandbox environments.

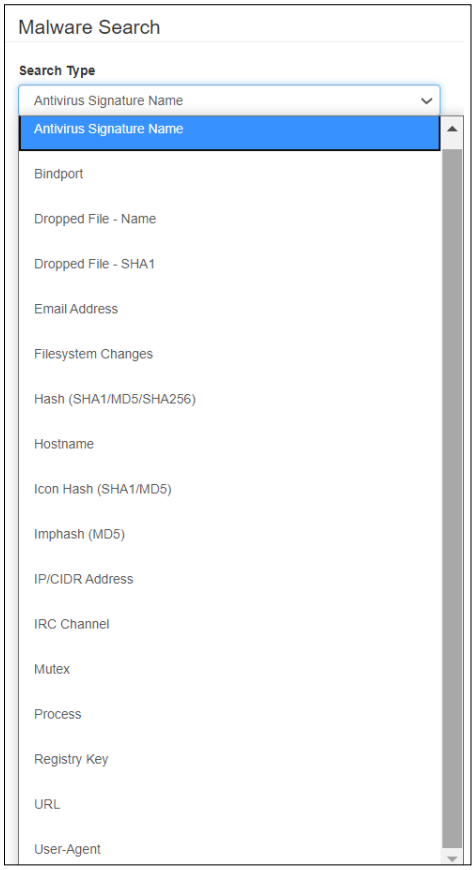
sales@cymru.com

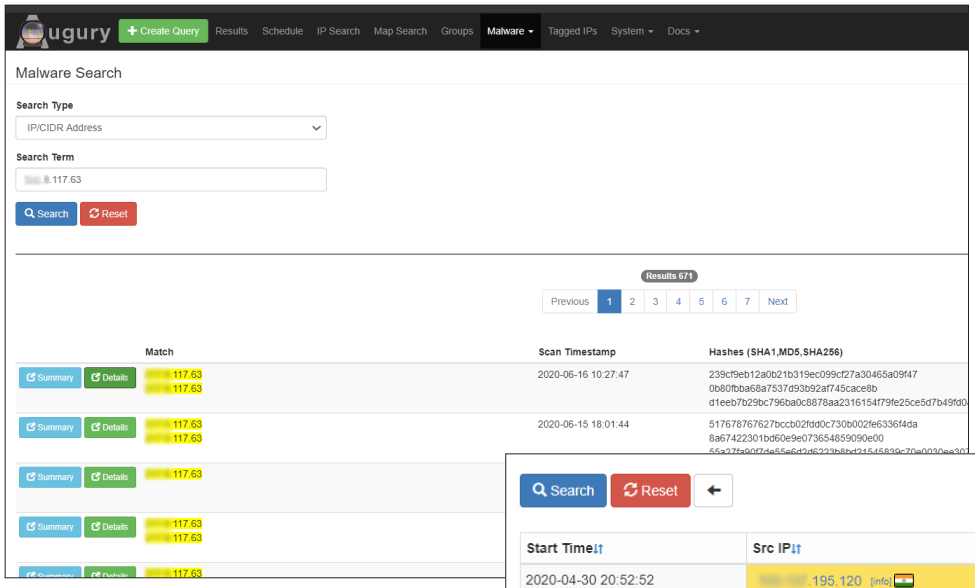
Pure Signal™ + Malware Correlation = Unprecedented Visibility

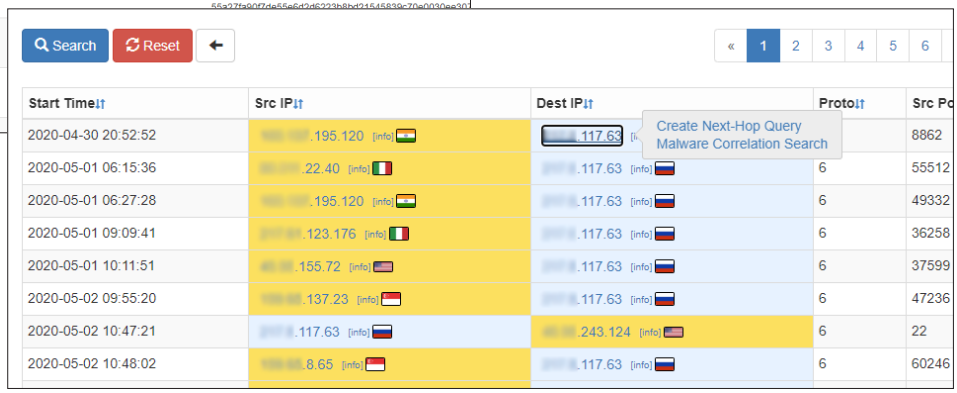
Key Features

- Use IOCs discovered in the Augury™ Malware Module to pivot across other Augury datasets.
- Evaluate malware samples against multiple AV engines for detection rate.
- Dynamic analysis in both virtualized and bare-metal sandbox identifies and mitigates evasion behavior.
- Keep track of searches and pivots, and easily return to any sample previously viewed.
- Sample upload supports the most common compression file types, and samples can be up to 100 MB and 25 files
- Export results in JSON and XML formats.

Search against 15+ attributes.







Left-click access to malware correlation.

CONTACT US
tel: +1 847-378-3300
fax: +1 407-878-7833
sales@cymru.com

EMERGENCY CONTACT
+1 847-378-3301
support@cymru.com

TEAM CYMRU™