PRODUCT BRIEF

Malware Module

A Powerful Addition to the PureSignal™ Platform

TEAM CYMRU™

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 **PureSignal™ RECON** 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 your 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 RECON results against our malware samples. Just left click and go.

Search

Search our malware library.

Upload

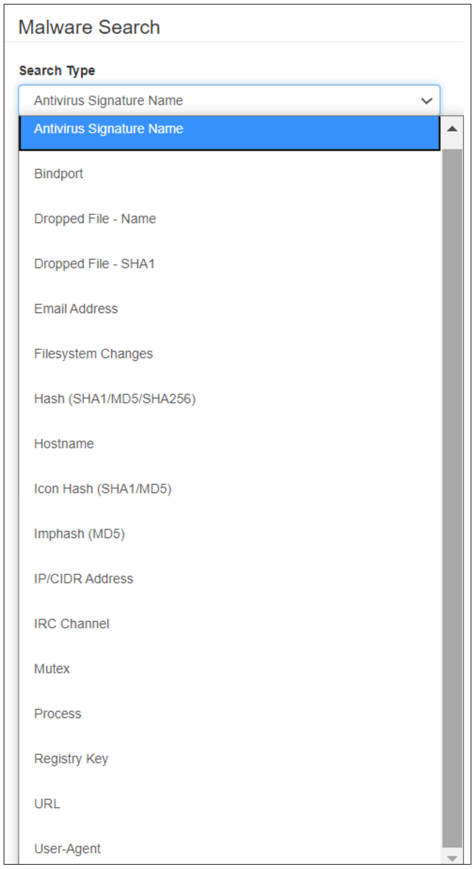
Detonate your samples in our sandbox environments.

Pure Signal™ + Malware Correlation = Unprecedented Visibility

Key Features

- Use IOCs discovered in the PureSignal™ Malware Module to pivot across other RECON 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.

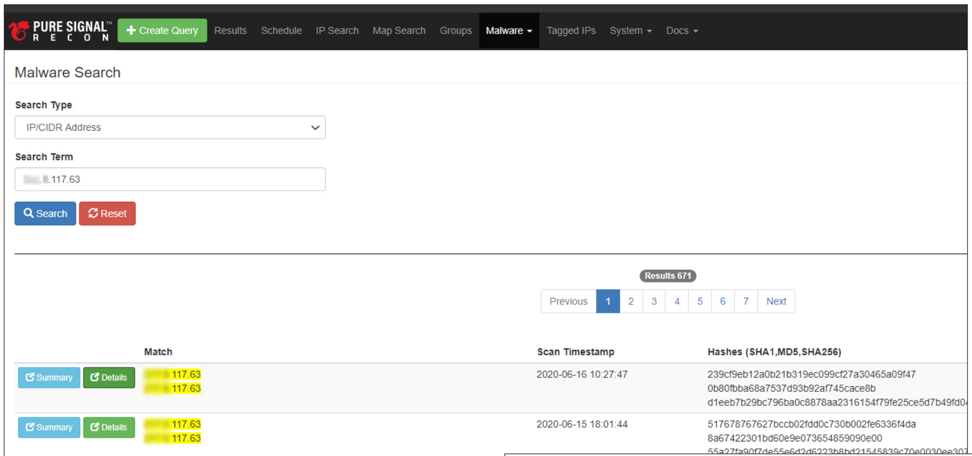
Search against 15+ attributes.


Malware Search

Search Type

Antivirus Signature Name

- Antivirus Signature Name
- Bindport
- Dropped File - Name
- Dropped File - SHA1
- Email Address
- Filesystem Changes
- Hash (SHA1/MD5/SHA256)
- Hostname
- Icon Hash (SHA1/MD5)
- Imphash (MD5)
- IP/CIDR Address
- IRC Channel
- Mutex
- Process
- Registry Key
- URL
- User-Agent

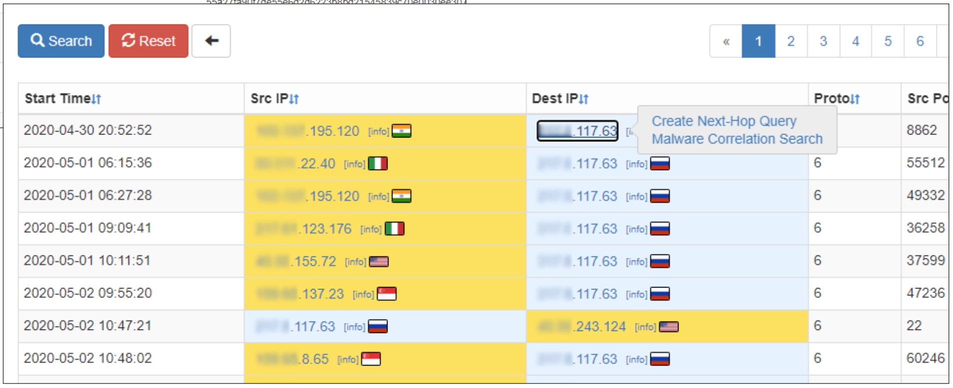


Malware Search

Search Type: IP/CIDR Address

Search Term: [redacted].117.63

	Match	Scan Timestamp	Hashes (SHA1,MD5,SHA256)
Summary Details	[redacted]117.63 [redacted]117.63	2020-06-16 10:27:47	239cf9eb12a0b21b319ec099cf27a30465a09f47 0b80fbba68a7537d93b92af745cace8b d1eeb7b29bc796ba0c8878aa2316154f79fe25ce5d7b49fd0
Summary Details	[redacted]117.63 [redacted]117.63	2020-06-15 18:01:44	517678767627bccb02fdd0c730b002fe6336f4da 8a67422301bd60e9e073654859090e00 55a27fa90f7de55e6d2d6223b8bd21545839c70e0030ee307
Summary Details	[redacted]117.63		
Summary Details	[redacted]117.63 [redacted]117.63		
Summary Details	[redacted]117.63		



Start Time	Src IP	Dest IP	Proto	Src Po
2020-04-30 20:52:52	[redacted].195.120 [info]	[redacted].117.63		8862
2020-05-01 06:15:36	[redacted].22.40 [info]	[redacted].117.63 [info]	6	55512
2020-05-01 06:27:28	[redacted].195.120 [info]	[redacted].117.63 [info]	6	49332
2020-05-01 09:09:41	[redacted].123.176 [info]	[redacted].117.63 [info]	6	36258
2020-05-01 10:11:51	[redacted].155.72 [info]	[redacted].117.63 [info]	6	37599
2020-05-02 09:55:20	[redacted].137.23 [info]	[redacted].117.63 [info]	6	47236
2020-05-02 10:47:21	[redacted].117.63 [info]	[redacted].243.124 [info]	6	22
2020-05-02 10:48:02	[redacted].8.65 [info]	[redacted].117.63 [info]	6	60246

Left-click access to malware correlation.