FireEye™

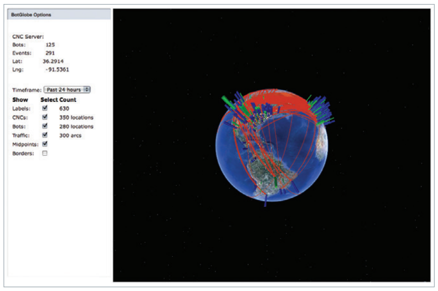
Datasheet

Dynamic Threat Intelligence Cloud

Real-Time Global Exchange of Threat Data to Identify and Block Zero-Day Attacks

Highlights

- Global sharing of anonymized intelligence on emerging Web-, email-, and file-based threats
- Organizations can subscribe to data feeds on zero-day malware and advanced targeted attacks to complement real-time identification and blocking of new cyber attacks
- Ongoing callback destination updates to block recently identified malware communications to supplement real-time blocking of newly identified malware communications
- Subscription to and publishing of threat intelligence is optional allowing users the flexibility to decide how much to share



BotGlobe Options

CNC Server:
Bots: 125
Events: 291
Lat: 36.2914
Lng: -91.5361

Timeframe: Past 24 hours

Show	Select	Count
Labels:	☑	630
CNCs:	☑	350 locations
Bots:	☑	280 locations
Traffic:	☑	300 arcs
Midpoints:	☑	
Borders:	□	

The FireEye Dynamic Threat Intelligence cloud shares malware intelligence between FireEye researchers and platforms

The FireEye® Dynamic Threat Intelligence™ (DTI) cloud is a global network that connects FireEye threat prevention platforms to provide a real-time exchange of threat data on today's cyber attacks.

The FireEye DTI cloud provides subscriber platforms with the latest intelligence on advanced cyber attacks and malware callback destinations, enabling the FireEye deployment to proactively recognize new threats and block attacks.

Real-time sharing of global threat intelligence

The FireEye DTI cloud interconnects FireEye platforms deployed within customer networks, technology partner networks, and service providers around the world. The FireEye DTI cloud serves as a global distribution hub to efficiently share auto-generated threat intelligence such as new malware profiles, vulnerability exploits, and obfuscation tactics, as well as new threat findings from the FireEye APT Discovery Center and verified third-party security feeds. By leveraging the FireEye DTI cloud, the FireEye Threat Prevention Platform is more efficient at detecting both unknown zero-day, highly targeted attacks used in cybercrime, cyber espionage, and cyber reconnaissance as well as known malware.

How it works: stopping today's new breed of cyber attacks

The FireEye Threat Prevention Platform, which includes the FireEye NX, EX, FX, CM, and AX platforms offers integrated, multi-vector threat prevention by utilizing stateful attack analysis to stop all stages of an advanced attack. Within the platform, the FireEye Multi-Vector Virtual Execution™ (MVX) engine creates dynamic threat intelligence based on the analysis of suspicious Web traffic, email attachments, and files. The FireEye DTI cloud infrastructure collects locally-generated, anonymized

> **"Within seconds of a potential compromise the FireEye appliance tells us exactly what we need to know, and it allows us to focus our resources on what is important. The benefits, not only to my own organization but to all the scientists and engineers, have been invaluable."**
>
> *— Lead Analyst, Cyber Defense, Government Agency*

malware intelligence from the FireEye MVX engine analysis and makes it available to the global FireEye community. The FireEye CM platform is then used to distribute the dynamic threat intelligence to each platform in order to provide real-time threat prevention throughout the entire FireEye deployment.

Organizations that subscribe to the FireEye DTI cloud receive threat data from, and can opt-in to send anonymized threat data to, the global subscriber base. Individual sites can decide how much or how little information to share. For example, an enterprise can choose not to send cyber attack information enacted against its company but will still receive threat intelligence from the FireEye DTI cloud in real time.

Dynamic analysis protects against unknown, zero-day attacks

The FireEye MVX engine captures, replays, and confirms zero-day malware and targeted attacks by executing suspicious binaries and Web objects against a range of browsers, plug-ins, applications, and operating environments. The FireEye MVX engine confirms an attack is underway by tracking vulnerability exploitation, memory corruption that facilitates arbitrary code execution, and other definitive malicious actions. As the virtual attack plays out, it captures dynamic callback channels used by the zero-day attack and then creates blocking rules for that channel. By integrating the FireEye platform activity across multiple threat vectors, customers get comprehensive attack analysis of the OS, Web, email, and other application threats. This integrated approach enables the most comprehensive protection against zero-day malware used in advanced targeted attacks as well as known threats.

Detailed intelligence on emerging threats

Threat intelligence includes:

- Malware attack profiles (MD5s of malware code, network behaviors, obfuscation tactics) that identify confirmed and now-known attacks
- Analysis of file share objects, email attachments, and URLs
- Fully qualified malware callback destinations (destination IP address, protocols, ports) used to exfiltrate data and deliver cybercriminal commands
- Malware communication protocol characteristics, such as custom commands used to instantiate transmission sessions

Blocks based on facts to avoid false positives and negatives

Unlike reputation- and risk-based threat intelligence networks, which make false assumptions about potentially risky code and broadcast signatures, the FireEye platform confirms malicious activity before blocking or allowing identified traffic. The assessments captured by the FireEye platform are conclusive because suspicious code is fully tested in the patented FireEye MVX engine. An example demonstrates the value of real-time intelligence updates:

1. A FireEye platform identifies a malicious IP address serving as a command and control (CnC) server and begins to block outbound calls to that address
2. The platform automatically notifies the FireEye DTI cloud of the destination IP address, port, and malware protocol used in the attempted connection
3. The FireEye platforms subscribed to the FireEye DTI cloud receive regular updates and block connections to that IP address that uses the same port and malware protocol
4. Compromised systems at all FireEye DTI cloud subscriber sites are blocked from contacting the botnet CnC server