proofpoint

ET Intelligence

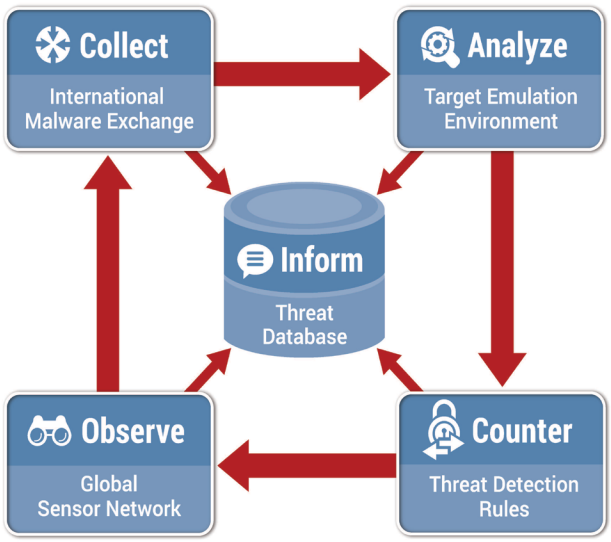
Highlights

- Keep pace with dynamic threat landscape using continuously updated intelligence.
- Block attacks and campaigns before they reach your organization.
- Increase the ROI of your existing security infrastructure with simple and easy to consume data sets.
- Adopt a proactive security posture based on real intelligence.
- Verify your prevention devices are performing as advertised by looking for the indicators of post-compromise activity.
- Enrich existing log data with global perspective on suspect IP addresses and domains.
- Enforce custom security policies based on reputation categories and score thresholds that matter to your organization.

Proofpoint ET Intelligence™ is the industry's most timely and accurate source of threat intelligence. Combining actionable up-to-the-minute IP and Domain reputation feeds with a database of globally observed threats and malware analysis, ET Intelligence gives the security professional the intelligence to proactively stop malicious attacks and provide the context needed to investigate them.

Why Proofpoint ET Intelligence?

Today, advanced cyber attack campaigns are perpetrated with increasing frequency by a variety of actors with motives ranging from profit to espionage. While the basic tools used to execute these attacks have common elements and are often derived from fewer than 20 known exploit kits, each campaign is unique in its use of bot nets, proxies, attack vectors, and command and control systems. Given the dynamic nature of these campaigns, it has become nearly impossible for enterprises to keep pace with the changing threat landscape. That's where Proofpoint comes in.



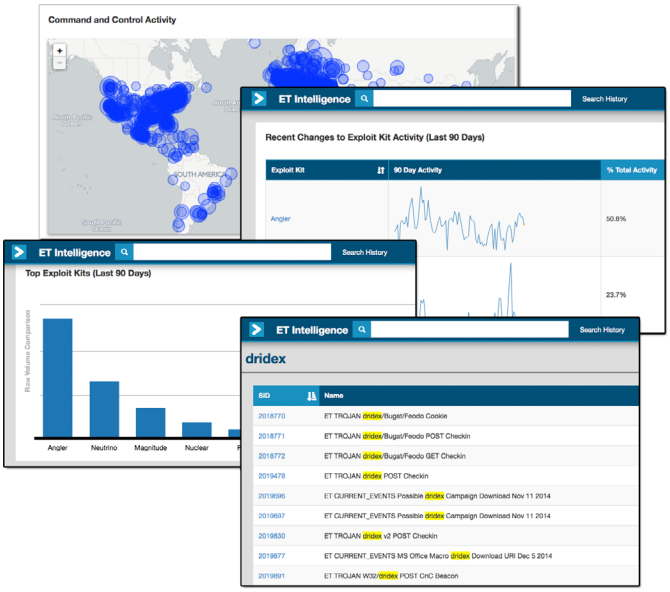
The team of dedicated threat researchers and analytics systems at Proofpoint ET Labs do the work so you don't have to. The result is 100% originally sourced threat intelligence on IP addresses, domains, malware samples and exploit kits from direct observation. Built upon a proprietary process that leverages one of the world's largest active malware exchanges, victim emulation at massive scale, original detection technology and a global sensor network, Proofpoint ET Intelligence is updated in real-time to provide organizations with the actionable intelligence to combat today's emerging threats.

Proofpoint ET Intelligence, comprised of domain and IP address reputation feeds and the global threat database, provides both actionable threat intelligence and a valuable source of context for incident investigation and threat research.

Dynamic IP and Domain Reputation

ET Intelligence provides actionable threat intelligence feeds for ingestion into firewalls, intrusion detection/protection systems (IDS/IPS), log and event management systems (SIEMs), and authentication systems. These dynamic feeds identify IPs and domains involved in suspicious and malicious activity as observed directly by Proofpoint's ET Labs. Features include:

- Separate lists for IP addresses and domains.
- IP and domains classified into over 40 different categories and assigned a confidence score (from 0 to 127) for each category.
- Scores which indicate recent activity levels and reflect aggressive aging.
- Hourly updated lists and scores that are depreciated aggressively.
- Multiple formats including TXT, CSV, JSON, and compressed.



Proofpoint ET Intelligence Global Threat Database

Global Threat Database

Organizations have learned that it is not enough to simply know what types of threats exist, but in order to prevent attacks and reduce risk, they must also understand the historical context of where they originated, who is behind them, when have they attacked, what methods they used, and why. Proofpoint ET Intelligence gives users on-demand access to current and historical metadata on IPs, domains, and other related threat intelligence to assist with incident investigation and threat research.

Features include:

- On-demand access to both current and historic threat intelligence. Searchable by IP address, domain, malware MD5, ET signature ID, and message text.
- Search results reveal related info for pivot and drill down, providing a forensic data trail for accelerating incident investigation.
- Over 5 years of observed threat activity.
- Continuously updated data.
- Dashboard with view of current global threat posture on command and control and active exploit kits.
- Available through web user interface or API

Enhance Existing Data and Tools

Today's network security infrastructure includes firewalls, next generation firewalls (NGFW), unified threat management (UTM) appliances, security incident event management (SIEM)

Proofpoint Layered Security

Individual security systems can be effective at blocking certain types of threats, but without complete coverage, compromise is inevitable.

- Get real-time, actionable intelligence and global context for detecting advanced threats with ET Intelligence.
- Investigate attacks seen in email-based attacks via Targeted Attack Protection and Proofpoint Enterprise Protection.
- Dive deeper into advanced threat forensics reported by URL Defense Service and Attachment Defense Service.
- Investigate threats blocked with Threat Response.
- Use intelligence to extend the ability to safeguard sensitive and confidential data with Proofpoint Enterprise Privacy.

platforms and authentication systems, among others. Each of these can be made more effective by timely threat intelligence.

Use Reputation Feeds to:

- Block connections to/from high-risk IP addresses in Firewall, NGFW, IPS/IDS, and UTM, increasing affectivity of these devices.
- Raise challenges for suspect IP addresses within risk-based authentication systems.
- Enrich event and log data in SIEM platforms.
- Fuel predictive analytic systems.
- Identify compromised assets and scope the extent of internal infections.

Use Global Threat Database to:

- Investigate incidents.
- Connect specific attack campaigns to billions of available individual indicators of compromise.
- Search and view attacks and actors in motion all over the world.
- Research malware with views into the network traffic produced when a malware sample executes.
- Integrate into SEIM to bring additional context to investigations.

Contact Proofpoint Today

The modern threat landscape is a lopsided battleground, where defenders must guard many fronts while attackers only need to find a single opening. Current protections, no matter how sophisticated, may not be sufficient. When applied proactively and with context, actionable threat intelligence can mean the difference between a major breach and a minor intrusion.

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com