Proofpoint Targeted Attack Protection

Defense Against Targeted Attacks

Targeted threats have become one of the top concerns of security officers of all organizations. Outside threats have shifted from broad-based phishing attacks to highly targeted spear-phishing campaigns. Proofpoint Targeted Attack Protection™ models normal email behavior in order to highlight anomalies that require additional scrutinizing, effectively neutralizing and responding to targeted attacks, because when it comes to malicious phishing attacks – every message matters.

Complete protection against the most malicious threats today: Spear-phishing attacks

There is an epidemic of targeted attacks. The majority of the large organizations have reported seeing these attacks; and email is the primary vector for them. These attacks are not random, but focused and coordinated efforts based on research through sources such as social media sites. Furthermore, once attacked, it can take weeks or even months before an organization may realize that they have been penetrated and possibly breached.

Proofpoint Targeted Attack Protection provides the tools to keep an organization safe from the malicious nature of targeted spear-phishing attacks and is a natural complement to any existing email security gateway.

proofpoint™

Targeted Attack Protection Benefits

- Comprehensive solution that covers multiple attack vectors
- Provides visibility into attacks in real-time – for threat management as well as incident response
- Leverages big data techniques to immediately identify when you are under attack and neutralize threats even if they have been delivered

Complete Protection

- Works together with Proofpoint Enterprise Protection to provide complete protection against all email threats.
- Protect sensitive and confidential data with Proofpoint Enterprise Privacy to accurately detect both structured and unstructured data to be secured with an integrated email encryption solution.

Big Data

Big data refers to compilations of data that are so large that traditional database tools are unable to manipulate the data as a whole in short time frames. Innovative big data techniques enable the efficient processing of large quantities time frames. Proofpoint leverages big data techniques in order to capture, store, and process immense amounts of data in order to provide insights on targeted threats. Big data has enabled Proofpoint to perform analyses that can actually stop a targeted attack the very first time it appears.

Full Lifecycle Approach

Simply detecting threats is no longer sufficient in today's world. A complete solution against targeted threats needs to be able to address messages even after they have been delivered to an end user. In addition, administrators need the visibility in order to clearly ascertain if they were able to block specific attacks or if remediation actions need to be taken. To address this, Targeted Attack Protection defends against threats with a full lifecycle strategy – Detect, Protect, Block, and Respond.

Detect

Anomalytics Service

One of the largest challenges in defending against targeted spear-phishing attacks is detecting the threats. Given the low-volume of these targeted spear-phishing messages, traditional solutions may not detect the presence of the attacks for some time, if at all. And because each and every phishing message has the potential to become the beachhead for attackers, every missed message represents a true and real threat to the security of an organization.

Proofpoint has taken a different approach to threat detection. Proofpoint's Anomalytics Service leverages big data systems to identify targeted spear-phishing campaigns by modeling an organizations normal email patterns in order to spot emails that deviate from the norm – i.e., an anomaly.

Protect

URL Clicktime Defense Service

While malware may be delivered directly as an attachment to a phishing message, a more frequent tactic has been to drive recipients to click on a link where the resulting web page either automatically initiates a download or tricks the user to enter sensitive or private information. Users who click on these links may be doing so at home, the airport or a hotel, and not behind the corporate firewall, making standard web gateway solutions useless.

To counter these attacks, the URL Clicktime Defense Service ensures that each time a user clicks on a link, the URL request is redirected to analysis by Proofpoint's cloud – and that URL is analyzed in real-time before the user is allowed to proceed. Working in conjunction with Proofpoint's Anomalytics Service, only suspicious URLs are redirected for the Clicktime Defense Service, giving organizations the ability to defend against targeted attacks even after an email has been delivered to the recipients inbox.

Block

Malware Analysis Service

Legacy approaches to malware analysis relied heavily on a list of known signatures or by dynamically examining the file within an isolated virtual machine, commonly referred to as "sandboxing". Unfortunately, polymorphic malware continuously changes its signature, easily defeating signature-based techniques. Remote and mobile users were generally bypassing these solutions as well.

Proofpoint's Malware Analysis Service utilizes anomalytics to identify suspicious files and immediately begins the process of analyzing the files in a sandbox for the hallmarks of a malware attack – all in the cloud – to ensure that when a user takes an action to download a file, it has already been inspected.

Respond

Threat Insight Service

Visibility into current threats is critical in mounting an effective response. Proofpoint's Threat Insight Service dashboard enables organizations to answer a few critical questions:

Proofpoint Targeted Attack Protection	
Feature	**Benefit**
Anomalytics Service	Easily *detect* targeted attacks the very first time they appear.
URL Clicktime Defense Service	*Protect* users, even when they are not behind the corporate firewall, with analysis of URLs at the time a user clicks on a link.
Malware Analysis Service	*Block* polymorphic malware that would be missed by traditional signature–based detection.
Threat Insight Service	*Respond* to threats quickly with a real–time view of attacks, who is being targeted and the status of each threat.

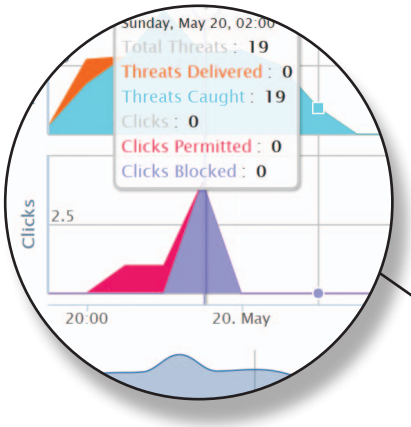
Respond (Continued)

1. Is our organization under attack?
2. Who is being targeted and what threats have been received?
3. What is the status of each threat? Have we blocked it? Or, have they been neutralized? Or, are they still valid threats?

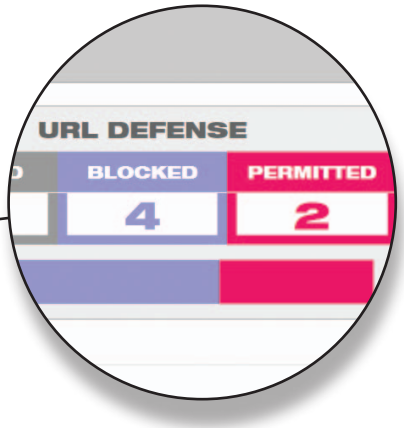
The Threat Insight Service dashboard provides a real–time view to see how many and what types of threats are currently being received. The dashboard measures the attacks on your organization against the current industry benchmark, so organizations can quickly see if they are being targeted.

When an organization is under attack, the Threat Insight Service provides details to identify which users are being targeted and if any messages have actually been delivered. The status of delivered emails can immediately be identified: emails that have been neutralized via the URL Clicktime Defense Service or emails that still pose a threat and need to be manually remediated.

The Threat Insight Service gives administrators the information to easily understand the current effectiveness of each aspect of their threat solution.

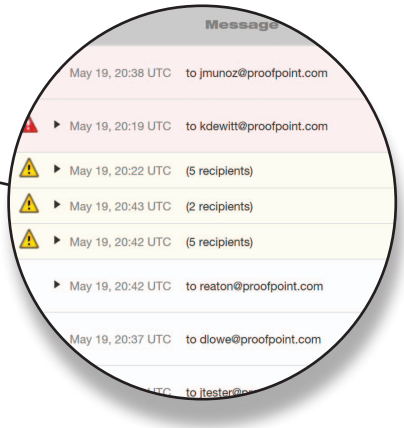


Find out exactly ***when*** the threat hit your system..



Know ***what*** went through your system.

Get more details about ***what*** made it through.



Find out specifically ***who*** was hit by the threat.

proofpoint

Proofpoint, Inc. (US Headquarters)
892 Ross Drive, Sunnyvale, CA 94089 USA
Tel: +1 408 517 4710 Fax: +1 408 517 4711
www.proofpoint.com