OpenText Threat Intelligence Real-Time Anti-Phishing Service

Effective, real-time protection against zero-hour phishing attacks

Benefits

- Dynamic and real-time 'latest' classification of potential phishing sites
- Minimized risk of compromise due to accidental interaction with phishing site
- Simple and flexible integration for policy-based compliance

Overview

- The most dangerous phishing sites are short-lived, living minutes or hours, not days
- Static phishing lists are too slow to keep up with the pace of today's attacks
- The OpenText™ Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service provides technology partners with the ability to leverage time-of-need site scans to prevent users from visiting malicious sites

The number of phishing attacks continues to grow. Phishing sites are designed to evade detection by block lists, crawling engines and law enforcement. Additionally, because the majority of today's phishing sites are active for hours, not days, static phishing lists are too slow to keep up. By the time blocklists are published, many of the sites they contain are no longer active. You need answers in milliseconds, not days.

The OpenText Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service is the only truly effective live protection against zero-hour phishing attacks. We apply advanced machine learning using thousands of feature vectors. For nearly a decade, these feature vectors have been trained to consistently monitor for the latest phishing trends. We determine whether the site is phishing at the precise moment it is encountered, meaning our analysis and determinations are never stale. This approach allows for a highly effective phishing determination engine with a false positive rate consistently below 1%.

Real-time URL validation is the only truly effective protection against zero-hour attacks, disguised redirection and recently hijacked websites. The OpenText Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service catches advanced phishing attacks by providing time-of need protection through real-time scans immediately before sites are visited.

Phishing and spear phishing attacks are now aimed at organizations of all sizes and are a preferred method cybercriminals use to breach networks.

Phishing analysis by F5 Labs found scans of phishing sites from OpenText Threat Intelligence (BrightCloud) showed that 72% used HTTPS. Phishers are playing on the trust users have of the green lock as another way to make their URLs seem legitimate.[1] Phishing attacks are so sophisticated, they often fool IT security professionals.

Stopping Phishing Attacks in Their Tracks

The OpenText Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service crawls potential phishing links and determines their risk level in real-time, helping prevent security breaches and data loss by leveraging advanced machine learning and content classification to automate phishing detection. The service crawls and evaluates requested URLs in milliseconds using

1 2020 Phishing and Fraud Report, F5 Labs

There was a 770% increase in phishing during the month of May compared to the average for the previous months. November was by far the most active month for phishing, with 34.3% of all activity for the year.[2]

hundreds of site attributes as well as external factors associated with the site. This includes correlated intelligence from the contextual analysis engine, such as the reputation of embedded links, the geolocation of the hosting IPs, the length of time the site has existed and the history of threats on that domain. The service returns a risk score for each requested URL.

Add-on OpenText Threat Intelligence (BrightCloud) Threat Insights for the Real-Time AntiPhishing Service for supplementary information on phishing URLs. This includes:

- Identifying the target of the phishing site so users can identify patterns in attacks and focus their analysis
- A snapshot of the phishing site when it was live to enable customers to see what the site looked like
- Additional data on the URL used for the phishing attack
- Searching for phishing URLs that attempt to imitate a specific brand or website

OpenText Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service in Action

Whenever users access the internet, the OpenText Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service can protect them from accidentally compromising their accounts or picking up malware or ransomware from malicious sites.

Additionally, this service can be integrated to:

- Improve web security for network appliances
- Identify new zero-hour threats for anti-fraud services
- Provide safe web browsers and plugins
- Enhance email filtering software and endpoint security products
- Filter user generated content in social networks, blogs and messaging apps

Integration Options

OpenText Threat Intelligence (BrightCloud) provides a RESTful web service, as well as an SDK, allowing technology partners to incorporate the OpenText Threat Intelligence (BrightCloud) Real-Time Anti-Phishing Service into their own solutions with ease. Additionally, this service combines with existing security solutions through the same SDK as other OpenText Threat Intelligence (BrightCloud) services, making integration as simple and straightforward as possible.