



Defining phishing attacks within the BD-BrandProtect phishing process

Phishing is the process of luring unsuspecting Internet users to a fake website by using authentic looking email and messages for fraudulent purposes. BD-BrandProtect disables these fake websites and by doing so prevents the identity theft.

BD-BrandProtect is committed to providing the best possible value to their clients for take-down services and has developed a pricing matrix which ensures that organizations with multiple attack scenarios benefit from the economies of scale without sacrificing quality of service.

For immediate action to a phishing attack BD-BrandProtect is available 24/7.

BD-BrandProtect reports all URLs involved in any type of phishing incident to Microsoft, Firefox and Google so that users can be warned of their existence and the URLs can immediately be blocked from appearing in Internet searches.

BD-BrandProtect's phishing take-down process

Each phishing incident consists of either a URL referenced in an email and/or a specific domain registered for the sole purpose of phishing. Each URL can consist of a domain or an IP address and may or may not include the "www" or the "http://" prefixes.

When is an incident considered open?

An incident is opened when a suspected phishing site is detected. This site is categorized as **active** if the site is live, and categorized as **never-active** if the site is unreachable at the time of detection.

As the incident is opened a BD-BrandProtect Incident Response Analyst monitors the site, records its properties, determines the ISP and domain owner and alerts the client of its presence.

Channels of communication are immediately opened with the ISP, domain owner and any

other relevant contacts. The Analyst vigilantly works with this group to ensure that the site is disabled in the fastest possible time frame.

As soon as the site is no longer live, cannot be reached and is not simply timing out, its status is set to **in-active** and the client is informed that the site has been disabled.

If an incident reappears within 30 days from the original take-down the incident is considered **re-active** and the take-down process is restarted. If the incident appears beyond 30 days it is considered a new incident.

When is an incident considered closed

The incident is only considered closed if the site remains in-active for 30 consecutive days. Even though the incident is now closed, monitoring remains in effect for a further 100 days to track any activity - no matter how small.

A URL is just a URL, or is it?

There are two types of URLs to be aware of:

1. The **primary** URL which is the actual phishing site
2. The **redirecting** URL which is used to redirect traffic to the phishing site

In some cases, the URL included in the spam message is not the location of the phishing site, but will redirect the user to the actual phishing site.

The fraudster develops the attack in this way so that should the primary URL be disabled, the redirecting site is still live and can be pointed to another phishing site to continue to harvest personal information.

Example:

Primary URL: www.geocities.com/badguy/pics/phish/index.htm

Redirecting URL: www.hackedwebsite.com/phish/company/update/attack.html

Incidents that include the primary and redirecting URL are grouped together; the take-down is carried out on both and is considered one take-down. When the primary URL is disabled the incident is considered **in-active**. Should the redirecting URL point to a new location after the primary URL is disabled, the new URL is then added to the same incident and it is then re-opened.

Grouping of URLs occurs when the domain and first folder path are identical to an existing incident. A common domain name does not necessarily mean two similar URLs are grouped together. In the example below, Incident # 1 and Incident # 2 are considered individual incidents due to the different folder paths:

Incident # 1: www.geocities.com/badguy/pics/phish/index.htm

Incident # 2: www.geocities.com/attack/site/index.htm

URLs are grouped together and considered the same take-down when similar URLs are found even though the wording and formatting of the phishing email might be slightly different:

URL # 1: phishingsite.co.uk/spam/banking/target/account.asp

URL # 2: phishingsite.co.uk/spam/banking/update/verify.asp

Tracking a rock phish

Tracking for rock phish domains is facilitated significantly by grouping all domains into one incident. Based on economies of scale, one take-down is levied against the client's total for every five domains included in the rock phish attack. In the event of a rock phish attack, daily reports are provided, indicating key data regarding detection and lifespan of all domains.