



## Takedown and Incident Definition

### Identity Theft Attacks

Whether your customers are being targeted by a Phishing, Vishing, SMSing, email-based, or malware attack, BrandProtect can handle it and you can track our progress in our secure Portal.

#### Phishing

Phishing Incidents can consist of either a URL referenced in distributed email (spam), and/or a domain registered for the purposes of phishing. URLs can consist of domain or IP addresses. The presence or lack of http:// or www. in subsequent URLs does not warrant creation of a new incident.

BrandProtect's method of grouping phishing URLs is unique. Although our per attack cost may differ from our competitors, our method of grouping attacks ensures that in a multiple attack scenario our customers pay less for BrandProtect's services than they would with a competitor without sacrificing quality of service.

All URLs - be they individual URLs, grouped URLs, Redirecting URLs, Primary URLs, or Rock Phish domains – get reported to Microsoft for blocking in IE7/8 and Mozilla for blocking in Firefox and Google Toolbar.

#### Vishing/SMSing

Vishing attacks are similar to phishing attacks, however a phone number is used in place of a URL. BrandProtect is able to detect vishing if the number is sent in an email, however some iterations of vishing attacks use an auto-dialler to cold-call your customers or an SMS (text) message is sent out (also known as SMSing), instructing the recipient to call the fraudulent number. Regardless of the method used by the perpetrators, each unique number is considered one takedown. Each unique number is considered one takedown.

#### Email-based attack

In some attacks, emails are sent out which instruct the recipient to reply to the email directly with their personal information. If the fraudulent email message is available, BrandProtect is able to get the email address used to collect people's information disabled. In some cases, the reply-to address in the email is different from the address the user is instructed to send their information to – in those cases, both the reply-to address and the address included in the message are considered one takedown.



## Malware

Malware incidents can come in one of two forms – either the user is instructed to click a link in the email message, which then takes them to the malware; or the malware comes as an attachment to the email message.

In cases where there is a URL that is hosting the malware, BrandProtect is able to perform takedown on the malicious URL. Each unique URL is considered one takedown.

## The Response Process

To help you better understand what is considered an incident and what is considered a takedown, you first need to understand our process. Below is a summary of the response process.

When a suspected attack is detected – regardless of the detection method – a new Suspect incident is created. A member of the Incident Response Team reviews the suspected attack, and if it is live, sets its state to Active. If the suspect appears to be an attack, but the site/phone number/email address is unreachable, the incident state is set to Never Active. Never Active incidents are not considered takedowns.

At this point, monitoring of the URL (if phishing or malware) is established, regardless of it being Active or Never Active.

If the attack is Active, the team member immediately notifies the client of the presence of a new incident via email. Properties are then set – we make a note of what the attack is asking for (username/password/SSN/malware, etc) and determination of the ISP or carrier. Emails are immediately sent to the ISP/carrier informing them of the presence of the malicious content, and any ticket numbers which may be assigned to the incident are noted. For phishing attacks, emails are also sent to the Domain Owner and any website contacts we may be able to find. Phone calls are made to all appropriate parties and emails resent on a regular basis until the URL/number is disabled.

Once the site/number is unreachable, the team member sets the incident state to In-active, and notifies the client.

In some cases, a URL may be timing out, as opposed to being removed. Should this occur, we do not consider the incident In-active until all URLs are unreachable for 2 hours.

If the URL remains In-active for 30 consecutive days, the incident status (not state) is considered Closed. Up until this point, the status of the incident is considered Open.

Monitoring remains in effect for 100 days after the last activity, in order to alert us to any possible changes. Activity can consist of log entries being added, or something as simple as the “404 - Not Found” page being modified.



For information about incidents that were once In-active but are now Active again, see the Re-active incidents section of this document.

## Incident Basics

An email message was found with the following domain-based URL as the target:

xyzsasw.com/badguy/attack.htm

This is considered a Suspect incident.

Another spam message was found with identical text as the example above, however the following IP-based URL was the target:

127.0.0.1/phishingsite/ver.php

This is considered a separate Suspect incident, despite the similarity of the spam email.

## Grouping

A common domain name does not necessarily mean two similar URLs are grouped together.

Incident 1 - [www.geocities.com/badguy/pics/phish/index.htm](http://www.geocities.com/badguy/pics/phish/index.htm)

Incident 2 - [www.geocities.com/attack/site/index.htm](http://www.geocities.com/attack/site/index.htm)

These are considered individual incidents due to the different folder paths.

Grouping occurs when the domain and first folder path are identical to an existing incident.

Example:

A spam message is found with the following URL as the target:

[phishingsite.co.uk/spam/banking/target/account.asp](http://phishingsite.co.uk/spam/banking/target/account.asp)

A subsequent email is discovered, with different wording and formatting, and uses the following URL as the target:

[phishingsite.co.uk/spam/banking/update/verify.asp](http://phishingsite.co.uk/spam/banking/update/verify.asp)

These URLs would be grouped together, and would be considered the same takedown.

## Rock Phish



Rock Phish domains are also grouped into one incident, however they are considered multiple takedowns based on the number of domains included. For every 5 domains included in the Rock Phish attack, 1 takedown is levied against the client's total. Tracking for Rock Phish domains is facilitated significantly by grouping all domains into one incident, and the amount of effort required to get one URL disabled is approximately 1/5th that of a standard phishing attack.

## **Redirecting URLs**

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 content. This is beneficial for the perpetrator, in that should the phishing content be disabled, the URL included in the original spam message can be modified to point to a live phishing site to continue to harvest personal information. BrandProtect refers to the original URL as a Redirecting URL, and the actual phishing page as the Primary URL.

Incidents which contain a Redirecting URL are grouped together with the Primary URL, takedown is performed on both URLs, and each Redirecting/Primary URL combination is considered a takedown.

Example:

[www.geocities.com/badguy/pics/phish/index.htm](http://www.geocities.com/badguy/pics/phish/index.htm) (URL included in spam, "Redirecting URL") redirects the user to [www.hackedwebsite.com/phish/company/update/attack.html](http://www.hackedwebsite.com/phish/company/update/attack.html) (not included in spam, "Primary URL")

These types of incidents are considered In-active when the Primary URL is disabled. Should the Redirecting URL point to a new location after the Primary URL is disabled, the new URL is added to the same incident and it is then re-opened and takedown resumed.

We only consider the incident inactive when there is no longer a live phishing site.

## **Re-active incidents**

In some cases, the phishing URL is removed by the ISP/domain owner/webmaster, only to be replaced by the perpetrator.

If this occurs within 30 days of being disabled, the incident is re-opened, and takedown resumed. This is considered the same takedown. If this occurs beyond the 30 day mark, it is considered a new incident and therefore a new takedown.