# Registry Cyber Threat Mitigation/Intelligence Service

## Problem:

It is estimated by McAfee that $140 billion in cash and lost time was tied to online malicious activity (Malware/Phishing/Scams) in the last 12 months in the US alone. Ensuring a safe haven against this activity while providing end users a streamlined and threat free experience is crucial to the success of Top Level Domains (TLDs). Registries are uniquely positioned to lead the fight against these threats because of their ability to control activities within their name space. Savvy registry operators will leverage this positioning to protect TLD brands, minimize economic damage and differentiate themselves.

## Solution:

Neustar's Registry Threat Mitigation Service will provide registry owners the ability to identify, detect, catalog, and disrupt malicious activity within their registries. This service will enable registries to combat the brand damaging effects of phishing, malware distribution, exploit hosting, and botnets within their TLDs. If warranted, Neustar may take down any domains verified to be harboring and/or supporting online threats. This action shuts down all activities associated with the domain name, including all websites and email. Therefore, resorting to such a measure is not taken lightly; however, Neustar's position has always been that removing threats from the consumer outweighs any potential damage to the registrar/registrant relationship. Neustar will also enable its registry partners to keep both registrars and registrants updated of any malicious activity within the TLD.

Deliverables include:

- Monitoring and detection of malicious activity within the TLD;
- Take down of domains verified to be malicious;
- Weekly and monthly reporting;
- Access to both legal and technical subject matter experts.

Registry partners will also have the ability to leverage Neustar's existing relationships with international law enforcement agencies if necessary.

Benefits of Neustar's Registry Threat Mitigation Service are:

- Minimizing the threat of spam, malware and phishing to TLD registrants/registrars on the domain name platform;
- Ability to quickly mitigate malicious activities that negatively impact the TLD;
- Brand protection for the TLD;
- Public representation within the private international security community;
- Experienced and friendly customer support and technical staff to manage security related concerns.

## Reporting Includes:

- Number of domain takedowns and appropriate attributes of those takedowns where available
- Malicious domains and malicious files
- Phishing feeds
- Analysis reports of a domain, its infrastructure, and its content based on available data

## Other provided services include:

- Analyses of third party data feeds
- Secure handling of outside complaints and requests for actions against domains
- Registrar/registrant communications and outreach

Neustar is at the forefront of the prevention of abusive practices on the Internet, and is a leader in developing and implementing an active domain takedown policy.

This service is provided for a charge to customers. Fees are based on number of domains under management according to the following schedule:

| Number of Domains | Annual Fee |
|---|---|
| 1 to 50k Domains | $ 16,500 |
| 50k +1 to 100k Domains | $ 24,200 |
| 100k +1 to 150k Domains | $ 27,500 |
| 150k +1 to 200k Domains | $ 30,250 |
| 200k +1 to 250k Domains | $ 33,000 |
| 250k +1 to 500k Domains | $ 49,500 |
| 500k +1 to 1M Domains | $ 93,500 |
| 1M+1 to 2.5M Domains | $ 110,000 |
| 2.5M+1 to 5M Domains | $ 137,500 |
| More than 5M Domains | $ 165,000 |

For more than one TLD, there is an additional per TLD annual handling fee of $1,000.

Note that for a closed TLD, the service is provided for up to 5k domains for annual fee of $2,000. Above 5k domains, the schedule provided above should be used.