MarkMonitor®
PART OF THOMSON REUTERS

PROTECTING BRANDS IN THE DIGITAL WORLD™

Case Study of A Recent Incident

Janelle McAlister
Manager, Global Relationship MarkMonitor

Objectives

- Who is a target?
- Our role during an incident
- Review the timeline from a recent incident

Everyone is a target

Registries

Registrars

Registrants

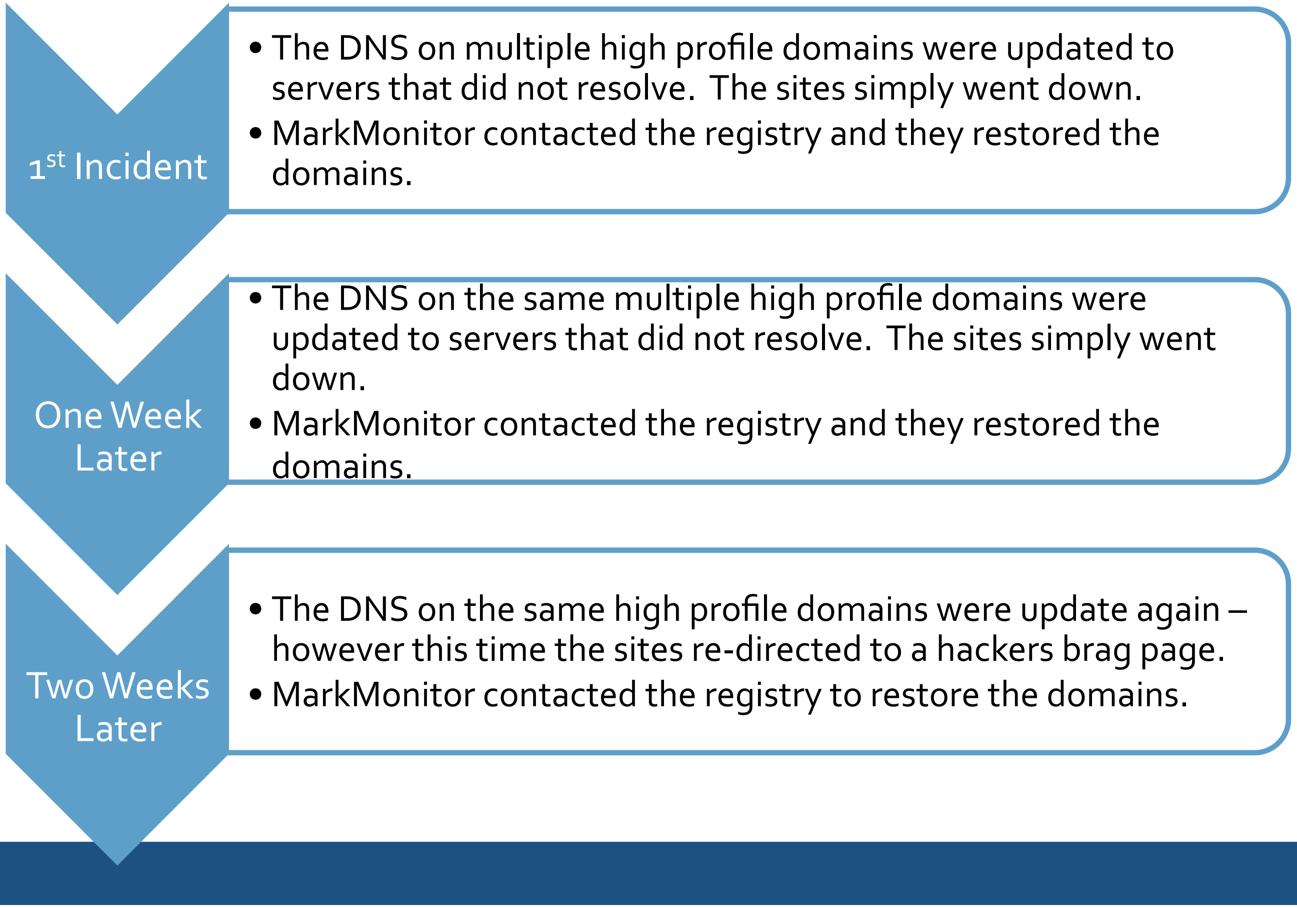
Why is MarkMonitor so concerned about ccTLD security?

- We are the domain registrar for some of the worlds most well known brands

- Historically, when a registry or registrar is targeted by hackers they attempt to update high profile domains.

What does MarkMonitor do during an incident?

- We have an internal monitoring system which checks domains under our management for unauthorized DNS updates.
- Once we have been alerted to an unauthorized update we have a detailed incident response plan
- We can provide the affected registry some technical expertise



1st Incident

- The DNS on multiple high profile domains were updated to servers that did not resolve. The sites simply went down.
- MarkMonitor contacted the registry and they restored the domains.

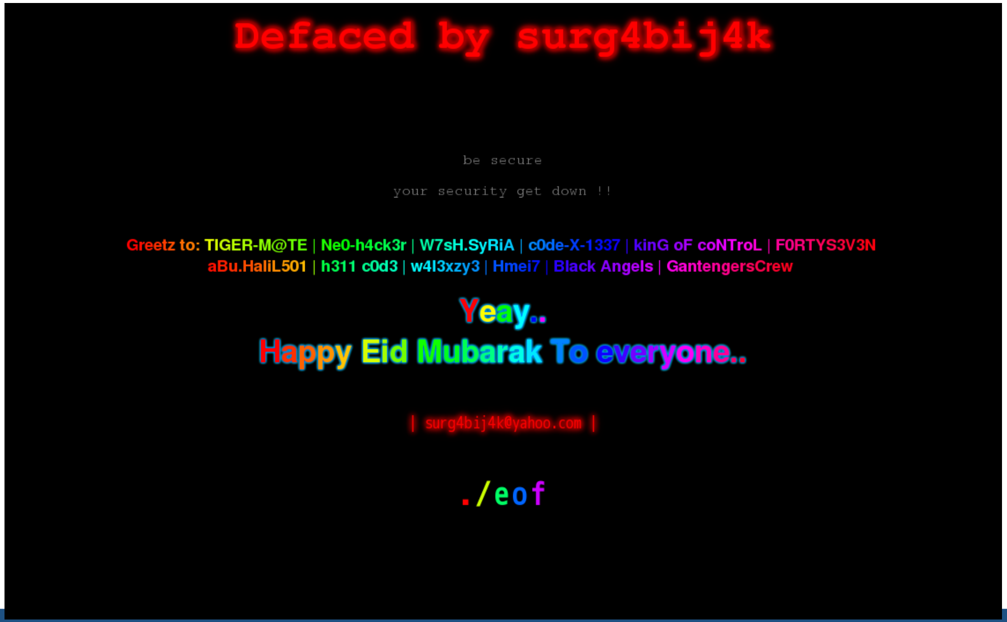
One Week Later

- The DNS on the same multiple high profile domains were updated to servers that did not resolve. The sites simply went down.
- MarkMonitor contacted the registry and they restored the domains.

Two Weeks Later

- The DNS on the same high profile domains were update again – however this time the sites re-directed to a hackers brag page.
- MarkMonitor contacted the registry to restore the domains.

After the 3rd update the sites were re-directed to a hackers brag page



Defaced by surg4bij4k

be secure

your security get down !!

Greetz to: TIGER-M@TE | Ne0-h4ck3r | W7sH.SyRiA | c0de-X-1337 | kinG oF coNTroL | F0RTYS3V3N
aBu.HaliL501 | h311 c0d3 | w4l3xzy3 | Hmei7 | Black Angels | GantengersCrew

Yeay..

Happy Eid Mubarak To everyone..

| surg4bij4k@yahoo.com |

./eof

With the Registries permission, we reached out to ICANN and the NSRC to offer assistance in analyzing the attack.