Gone Phishin’

Posted on February 5, 2019

Too many people seem to think that some nebulous security force, perhaps, even a form of law enforcement, is engaged in taking down phishing sites. They may not even think about this subject at all. The security force thing is something that couldn't be farther from the truth. In reality, the security community is a literal community that depends on practitioners finding malicious sources of information and acting on them. It's a bit like the awareness see-something-say-something mantra. It is difficult to assess how many acts of violence and threats across the internet are revealed through a goodwill party that speaks up. But it happens, all the time. Most of us would prefer a nicer, gentler internet but there are always going to be outliers that see the internet as an opportunity to bait victims into giving up sensitive information and thus being exploited financially.

Reacting to Events

It terms of how organizations report, phishing is interesting because a typical organization will not discover or report these incidents until it is too late and they have been phished, ostensibly taking on some kind of damage. Organization gets attacked, reports to its ISP (and, perhaps, authorities), the ISP analyzes the information, and if the site in question still exists, they will notify the hosting ISP that unfavorable activity is coming from their network from the site in question. If all works out well, the ISP takes the site down, meaning further incidents from the site are not a concern.

When it comes to pests, there's a saying that goes, "Where there's one, there's more." Phishing sites are more or the less the same. Take down one site, and ten more are ready to replace it. In some ways, it might even seem futile to take down just one phishing site.

The WHOIS solution

One of the most valuable tools in detecting and removing offending sites is the WHOIS database of domain registration information. There is a lot of interesting stuff that goes into these records, including registrants, contact info, dates of registration, and many more. Whois data can be an important part of any anti-phishing email security solution.

Even when those who apply phishing schemes use false information, it is possible to find broad behavior patterns throughout falsified and incomplete registrations. Specific repetitive info, common dates, countries of origin, and a variety of data points may indicate that there is something suspicious or worth going into regarding a target domain.

Why WHOIS works

Security principles drive the industry, and it is common for ISPs, hosting companies, cloud providers, and other technology platforms to have very little tolerance for criminal behavior. Registrars can be quick to terminate the accounts and assets of a criminal organization based on fake registration information or otherwise dubious registrations possibly linked to phishing schemes. With both the technical community at large and this show of force at the registrar and hosting level, criminals learned that realistic information is critical to pass muster and to give the feel of an authentic domain.

That's where things start to get interesting. It is where emails see reuse across domain registrations. It is where dates and other corroborating information become apparent. Those bits of information may be the breadcrumbs that raise red flags and suspicion.

WHOIS unleashed

The WHOISXML API is a powerful base of information in these efforts. The information held within includes correlated data, source information, dates, and just about every sort of search field for information a researcher could want. If it's in WHOIS, it's in the API. That's valuable information for modern environments that use dynamic infrastructure, cloud elements, hybrid configurations, and cutting-edge virtualization technologies. The internet is just too fraught with elements to not have a powerful information tool that can help stop phishing and other fraudulent attacks before they occur.

Airbnb phishing: a study

Recently, WHOISXML API published a deep dive at a very simple yet actual phishing outbreak in the wake of incidents at Airbnb.

Ultimately, it is important to recognize how WHOIS information and phishing intelligence can be used to mitigate the risks of phishing attacks against an organization.