http://www.UKCERT.org.uk/ – **"Ten Years On" – By Paul M. Wright - June 7th 2013**

A. Introduction

http://web.archive.org/web/*/http://www.ukcert.org.uk shows that UKCERT started 10 years ago on June 23rd 2003. During the last ten years UKCERT has been CC'd on over 20,000 incident reports from a wide number of organisations including a number of regional CERT/CSIRTs outside of the UK, large ecommerce companies, online banks and information security management organisations from around the world. The majority of the incidents reported are phishing site reports asking ISPs to remove fake websites which have been used in phishing emails. This collection of incident report data represents a potential source of knowledge from which we can learn, as this short paper will illustrate in an **anonymised** fashion.

B. The questions we would like to ask of this data are:

1. What industry sectors are targeted?
2. How are they targeted?
3. What type of attacker targets them?
4. What conclusions regarding risk can be made?
5. What trends over time can be observed?

1. What industry sectors are targeted?

Taking a subset of the six months counting back from June 7th we will see that approximately 70% of reports are regarding phishing sites targeting UK based online banking organisations with the majority of the rest being US then EMEA financial services, followed by Latin American and Indian financial services with a single EU based governmental tax organisation targeted. Notably no organisations East of India have reported being targeted by IP addresses based in the UK in the last 6 months and neither have UK organisations been targeted by phishing web servers hosted in the Far East.

2. How are they targeted?

There are still a low number of cgi bin URLs being attacked but over half of the phishing web servers are "normal" web sites hosting Word Press blogs that have had malicious web pages uploaded to them. (This may be due to the popularity of Word Press rather than high vulnerability). So these phishing web sites will redirect a link from a mass email to the real web site but capture the authentication details in transit. Some examples of generic Word Press attack URLs which have been anonymised follow:

.com/wp-content/themes/newsworthy/redirect.php
.co.uk/wp/wp-admin/includes/users.php
.co.uk/wp-content/uploads/2011/www.bankx.co.uk.htm

The majority of the other incidents are caused by **dotted *nix directories** like those below:

http://lamesite.com/highslide/graphics/outlines/**www.bankx.com**/login.jsp.htm

URLs with domain names misspelt or extended were also prevalent.
The next most common phishing attack was Domain names using the correct name but with a domain suffix which has not been protected e.g. uk.com domains which had not been purchased by the authentic organisation thus leaving them open to an attacker to purchase.

3. Who targets companies with phishing sites?

UKCERT does not ask for detailed information about the phishing site hacks so the attacker's identity has not been recorded by UKCERT. There is some more information in terms of the IP addresses of the phishing sites that attackers have targeted, which may be useful.

IP logs were processed using Excel and bash regex as follows:
egrep -o '[[:digit:]]{1,3}\.[[:digit:]]{1,3}\.[[:digit:]]{1,3}\.[[:digit:]]{1,3}' 1.txt > out2.txt

And then maps generated using http://batchgeo.com/ using a random sample of 250 IP addresses reported to be hosting phishing sites related to the UK.

Figure 1 - Main Geo IP locations for phishing web sites local to UK in past 6 months

London has the highest individual proportion of locally hosted phishing sites.

Figure 2 – Zoom out - IP addresses hosting phishing web sites reported to UKCERT in past 6 months

http://batchgeo.com/map/1fa56b4889c029e83ca67f6b108ed9ba

4. **Conclusions regarding risk reduction can be made?**

The map shows that phishing web sites are clustered as the sample is 250 strong but the nodes are less numerous. A notable observation from the map is that there are IP addresses outside of the UK. These external IP addresses are either managed by UK contacts or hosting phishing web sites targeted at UK organisations or IP addresses erroneously reported. Some of this spread can be explained by IP addresses floating between geographic domains but it is likely that most of these are UK companies targeted by non-UK IP addresses. What is immediately noticeable is the lack of both Chinese, African and South American IP addresses. These geographies receive much press for Cyber Crime but the last 6 months of data to UKCERT suggest this external "foreign" Far East risk is overrated.

The organisations targeted by these phishing IP addresses are predominantly English language (UK), English (US), Spanish, Italian, Dutch, Indian with zero events effecting Chinese companies in Standard Chinese (Mandarin). Note that no other identifying information will be given by UKCERT regarding the identity of the organisations targeted as this information is private to those affected.

Incredibly Word press vulnerabilities count for half of phishing sites, and most of the rest are due to malformed and cyber-squatted domain name/URLs. It should also be noted that phishing web sites may not all have been hacked i.e. in some cases the actual owner of the web site may the phisher, though this should be exceedingly rare.

The fact is that the majority of risk to phishing attacks could be removed by everyone upgrading their Word Press blog and client users checking the validity of URLs before they click on them in their emails. This is basic User Awareness Training not advanced Cyber Technology.

5. **What trends over time can be observed?**

So far we have only analysed the last 6 months of data and we should not leap to conclusions this second. The main trend observed thus far is that there is a large and growing number of phishing web sites being reported.

C. Future Work

There is a lot more data to analyse which is growing each year, so UKCERT propose to make this an annual report on a continual basis. All results will have targeted organisation details removed and the report will be made available to submitters first for early feedback. Deeper analysis into why IP addresses outside UK are being reported and why there are no Chinese IP companies involved will also be investigated in partnership with partner organisations globally.

The primary new item of work will be the production of User Aware Training to avoid being the victim of a phishing attack using the results from the analysis of the UKCERT data and lessons learnt from real life. The usability of security guidance is seen as the major area for improvement .

If your organisation needs to ask an ISP to remove a phishing web site you are welcome to email the technical contact for the domain and CC UKCERT (paul.wright@ukcert.org.uk).

Keep Safe!

Paul M. Wright
City University London

P.S.
UKCERT was started by myself and two colleagues using the funding from an EPSRC grant gained for a research project at the University of Manchester. The idea of UKCERT came about during a discussion with Carnegie Mellon CERT research staff whilst in Lance Spitzner's Honeypot class at SANSFIRE DC, as CERT did not have a UK equivalent to contact - but the concept of maintaining high quality internet security in the UK, was initially inspired by the work of Alan Turing. UKCERT now resides in London.