OFFICIAL

Problem Profile Bulletin: **Domain Slamming**

November 2015

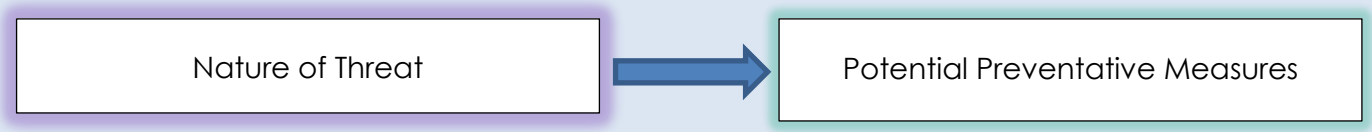
Domain Slamming is an attempt by third parties to obtain money by pressurising individuals or companies into paying for domain name renewals or similarly named domains.

This type of fraud can be split into two types, both of which can affect any individual or company. When contacting a victim company the fraudster will claim either one of the following:

(A) they are the only domain renewal service available for that individual's or company's domain

or

(B) they own the rights to similar domain names to that owned by the victim company



Nature of Threat

1. The main culprits behind these frauds have been noted as fraudulent Asian and/or Chinese domain name vendors. Using publically available websites such as *Who Is* they identify domains that are close to expiry or have already recently expired, to create a list of potential target companies.
2. In scenario A, the victim company is contacted by a fraudster who claims to be from a domain registrar or web host, who pressures the individual or company into renewing their domain name through the fraudster within a very short time frame and at a larger price. Consequently, the domain name is transferred to a new provider, putting it (and the victim's website) at risk.
3. Once a website domain has been transferred to another provider this can result in; unnecessarily large subscription fees, long-term unbreakable contracts, the termination of the once fully-functional website and email account and finally possibly the loss of the domain altogether.
4. In scenario B, the victim company is contacted by a fraudster again claiming to be from a domain registrar or web host, who pressures the individual or company into purchasing similar domain names from the fraudster in order to protect their 'brand identity'. Companies are often told that their domain or similar domain names will be sold to another company that has expressed an interest in purchasing them if they don't purchase it within a short time period. Consequently, the victim company purchases similarly named domains at extortionate prices – it is not clear whether the fraudster even provides the domain names purchased by the victim company.
5. Some domain vendors claim to be working as a subsidiary of a legitimate and reputable vendor; this does not mean that they themselves are legitimate.

Potential Preventative Measures

1. Call your domain registrar / web hosting company to check whether they have sent out this information to you, or whether they are aware of it. Be aware and make note of the genuine channels your provider will use to contact you, and be cautious of new or different ones.
2. Always renew domain ownership via the website from which it was purchased, and not a third party.
3. Research the company or individual who has signed the letter or email online – do they exist? Are they mentioned online as a previous scammer, reported by a previous victim? Do not always assume that corporate-looking headers, signatures and logos mean legitimacy.
4. If you receive a renewal notice, check the company owns the domains in the first instance via, for example, *Who Is*.
5. Observe cyber safety measures, such as placing the cursor over the 'sending' email address in order to determine its origin, and not clicking on links embedded in emails. More online safety advice can be found at https://www.cifas.org.uk/stayunique.

Appendix

- **Domain name** – the part of a website address that identifies it as belonging to a particular domain
- **Domain registrar** – an organisation that manages the reservation of Internet domain names
- ***Who Is*** – a website that stores database content regarding internet sources
- **Web Host** – hosting service that allows website owners to make them accessible on the World Wide Web

--- END OF BULLETIN --

Problem Profile Bulletins are researched, prepared and distributed Cifas – The UK's Fraud Prevention Service. If you want to find out more about Cifas and how we can work with your organisation, contact Scott Reeve (scott.reeve@cifas.org.uk) or Wayne Bath (wayne.bath@cifas.org.uk).