SECTIGO

Beware: phishing attacks using SSL are on the rise

By Lindsay Kent, Sectigo

An uptick in phishing websites using SSL certificates is causing concern in the industry. However, there are steps companies can take to protect their customers from being the victims of fraud.

Phishing websites using SSL certificates is not new, the first reported instances were in 2005.

The rate of phishing attacks using a valid DV SSL certificate has grown from 450 in all of 2005 to 47,500 in the first quarter of 2017. The primary cause for this increase: The price of SSL certificates has dropped to a point where it is cost effective to use a larger number of SSL certificates for phishing sites. Further encouragement has been provided by the browsers, when they collapsed the Domain Validated (DV) and Organizational Validated (OV) SSL certificate into one visual indicator in the browser, which states "secure". The consumer now believes the DV certificate means the site is legitimate, like OV, where the intended purpose of DV is to encrypt the communication.

The steps to mount a phishing attack

1. **The attacker begins by buying a domain from a registrar that is similar in name to that of their intended target.**

   For example, Paypal1.com to attack the consumers of Paypal.com.

2. **They then buy the services of a web hosting company, or content management provider, to setup a valid web site.**

3. **The next step is to purchase a SSL certificate, where the industry rules for a DV certificate require validation that the person requesting the SSL certificate has control of the domain, in this case Paypal1.com which the attacker does control.**

In rare cases, the attacker may compromise a legitimate website using an OV certificate, then install malware or add a domain with malware under a legitimate wild card OV certificate.

All SSL vendors will issue certificates to the phishing website, what will change is the number issued per SSL provider. The attacker will buy whatever is available from their web hosting company or content management provider. Therefore, the number of phishing SSL certificates issued tends to be relative to the market share of the SSL provider, but all SSL vendors are vulnerable to issuing certificates to fraudulent websites**.**

What the industry is doing?

Tools are available to registrars, SSL vendors and browsers that compare the website domain to that of their intended target, to create a risk score which either warns or prevents the consumer from reaching the malicious website. Two popular tools are "Google Safe Browsing" and "Microsoft SmartScreen". These tools also look at historical activity of the website to identify malicious intent.

The attacker uses additional methods to reduce the effectiveness of these tools:

- **The phishing website will perform legitimate activities for a long period of time before they are enabled for a phishing campaign that lasts only a few hours.**

- **Utilize non-Latin characters that look like a Latin character. For example, the letters "a" in the Cyrillic and Latin scripts are visually identical, even though they're different characters with different Unicode values used in the domain name.**

- **The phishing website will register for a wildcard certificate such as *.abc.com to avoid early detection. They then add a webserver paypal1.abc.com using the *.abc.com certificate.**

- **The phishing site will be set up and immediately used for a phishing campaign for only a few hours. They know the site will be taken down or blocked by the anti-phishing tools within 24/48 hours, however by then they will have perpetrated their fraud and moved on to the next target.**

This is a complex, industry wide problem, that while it has reduced fraud, it has not been eliminated.

Sectigo continues to evaluate the intent of requests for SSL certificates, while following the rules mandated by the CA Browser Forum, as audited annually be a 3rd party. Fraudulent website certificates are revoked daily, as identified by ourselves or as reported to ssl_abuse@Sectigo.com.

What can the legitimate website do

The usage of EV certificates will display the organization's name in compatable browsers, not simply the domain name. The validation approach for Extended Validation, is designed by the CA Browser Forum to make it tremendously difficult and expensive in time and money for the attacker to impersonate the legitimate company's legal name, Jurisdiction of Incorporation or registration and domain name.

The purchase of EV should be complemented by a campaign to your consumers to look for the company name, make sure it is the correct jurisdiction (ex. country or state), and ensure the correct domain name.

A phishing site with DV:

The legitimate site with EV:

Since April 2018 all certificates issued by all SSL Vendors are sent to the Certificate Transparency logs. Third party tools will be developed to identify high risk website names against popular targets, which can be utilized by the industry and legitimate website owners looking to protect their consumers.

Companies should inform their consumers not to click on links contained in emails. The attacker can design the link to look legitimate which will take them to a real looking phishing site to steal passwords and credit card numbers.

Consider authentication that does not utilize passwords that can be stolen by the attacker, instead use a client side SSL authentication, where the digital identity never leaves the consumer. All web servers and browsers support client side SSL authentication, where the browser proves possession of the consumer's digital identity but does not send the identity itself. This is unlike a password where the password is shared with the web server, allowing it to be stolen by the operator of the phishing web server.

