Announcement of “London Protocol” among participating CAs

Chris Bailey, Entrust Datacard

Entrust Datacard™

INCIDENCE OF ENCRYPTED PHISHING BY CERT TYPE

- It's known that identity-based certificates like OV and EV are *safer* than DV
- This table shows breakdown of encrypted phishing sites by certificate type – most phishing uses anonymous DV certificates (no identity). DV sites are more dangerous on a proportionate basis than OV and EV sites.

Certificate Type	Phishbank Dataset		The Internet	
	Phishing Sites in Sample (1)	Percent of Total Phishing Sites in Our Sample	Total Internet Certificate Population (1)	Percent of Total Cert Population
EV	0	0.0%	195,409	0.7%
OV	29	0.9%	1,480,294	5.0%
DV	3189	99.1%	27,822,384	94.3%
Total	3218	100.0%	29,498,087	100.00%

(1) Source: Phishbank.org – Based on 30 days of phishing sites in Apr 2018 with SSL / TLS
(2) Based on Netcraft valid certificate population by certificate type as of April 2018.

WHERE DOES PHISHING COME FROM - OV AND EV SITES?

Three sources:

1. *Compromised websites* – e.g., hosting companies that don't do patches and upgrades, leaving website customer at risk – phishers post content at website pages the owner can't see at directory level

2. Shared *certificates* – multiple independent SANs, one of which posts **phishing** content (hosting companies, etc. using OV or EV certs for their customers) – bad practice.

   Subject: C=US, ST=Delaware, L=Dover, O=**Incapsula Inc**, CN=incapsula.com

   X509v3 Subject Alternative Name:

   DNS:incapsula.com, DNS:*.aidatraconis.com, DNS:*.aisfl.com, DNS:*.alltoosimple.com, DNS:*.awakenthroughmindfulness.com, DNS:***.bontrade.com**, ***

3. Shared *content* sites – blog sites where independent parties control separate pages, one blog page posts **phishing** content. Blog site uses OV or EV certificate – bad practice.

   1. DNS:blogspot.com.mt, DNS:blogspot.com.ng, DNS:**blogspot.com.tr**, DNS:blogspot.com.uy, ***

OBJECTIVE OF LONDON PROTOCOL

- OV and EV sites are already more secure for users than DV sites.
- **Objective of London Protocol**: To improve identity assurance and minimize the possibility of phishing activity on websites encrypted by OV (organization validated) and EV (extended validation) certificates (together referred to as “Identity Websites”).
- Reinforces the distinction between *Identity Websites* (OV and EV) by making them *even more secure* for users than websites encrypted by DV (domain validated) certificates.
- That extra security feature can then be *utilized by others* for their own security purposes, including
  - *Informing users* as to the type of website they are visiting, and
  - Use by *antiphishing engines and browser filters* in their security algorithms (otherwise, they just have DV certs – no identity data to follow).

HOW THE PROTOCOL WILL BE IMPLEMENTED

The London Protocol will be implemented through voluntary action by public Certification Authorities (CAs) working jointly to take the following steps:

- Actively monitor phishing reports for websites encrypted by the CA's own OV and EV certificates;
- Notify the affected website owner that phishing content was found and provide remediation instructions as well as prevention methods;
- Each CA will contribute to a common database to help reduce future phishing content. This data will be available to other participating CAs so that each CA can conduct additional due diligence before issuing new OV or EV certificates to the website.

SOURCES OF DATA / PUBLIC REPORTS

- **Sources of Phishing Data for Encrypted Websites:** The CAs who are voluntary members of the London Protocol will collaborate to find the most reliable sources of anti-phishing data useful in implementing the protocol.

- **Public Reports:** Data and results will be shared among participating CAs. Those who find the information useful will be encouraged to utilize it in their own security processes. Additionally, those who use this data will be encouraged to provide feedback on how this data can be improved to better serve the ecosystem.

- From time to time the participating CAs will compile statistics and other information collected during implementation and publish the results to the CA/Browser Forum and to the media.

PROTOCOL PHASES

The London Protocol will be implemented in four phases:

Phase 1 ***(June - August 2018):*** Official announcement of Protocol and participating CAs. Participating CAs further develop Protocol details and research feasibility of implementation and may begin to implement some basic procedures.

Phase 2 ***(September - November 2018):*** Participating CAs apply Protocol concepts to their own customers' Identity Websites according to their own policies and procedures, share feedback with other participating CAs, refine Protocol as warranted by experience.

Phase 3 ***(December 2018 - February 2019):*** Participating CAs update Protocol policies and procedures and approve plan for uniform policies and procedures to be applied by all participating CAs on a voluntary basis.

Phase 4 ***(March 2019)*** Participating CAs forward report and recommendations to CA/Browser Forum for possible changes to Baseline Requirements.

OTHER PRINCIPLES

Antitrust Laws; Withdrawal by CAs: The participating CAs will comply with all applicable antitrust laws, including the limitations specified by the Antitrust Notification read aloud prior to CA/Browser Forum meetings.

Participating CAs may withdraw from this Protocol at any time upon notice to the other participating CAs.

This voluntary Protocol is open to all CAs who want to make OV and EV websites that are secured by their certificates as *free from phishing* as possible. ***Join us!***

Founding Participants in the London Protocols:

COMODO

GlobalSign GMO INTERNET GROUP

Entrust Datacard™

GoDaddy™

Trustwave®

Thank you!
Questions?

Entrust Datacard™