Poster: Malicious Service Discovery in Normal-Looking SSL/TLS Services

Security Issues by Free Domain Validated Certificates

Zigang Cao, Mingxin Cui, Zhen Li, Junzheng Shi, Gang Xiong
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
Email: {caozigang, cuimingxin, lizhen, shijunzheng, xionggang }@iie.ac.cn

***Abstract*—X.509 certificate plays a very important role in SSL/TLS services. Recently, the evolving of free certificates, especially the automatic issuing service of domain validated (DV) certificates by popular certificate authorities (CAs), has evidently aggravated security issues in SSL/TLS due to the low lost and lack of identity authentication of the corresponding physical entity [1]. In this paper, we try to illustrate the severity of this problem through a large scale measurement. Besides, some advices are given to mitigate the risk of malicious services which are related to DV certificates.**

I. Introduction

SSL/TLS is currently the most widely used encryption protocol on the Internet to ensure network communication security. Meanwhile, the encryption merit of SSL/TLS makes it convenient for attacks and malware to hide their malicious network communications from security devices. Similarly, web fraud websites using HTTPS, namely the phishing and typosquatting, are much more difficult to detect than that of HTTP if a normal-looking domain and a validated certificate are deployed. No warning will be given by browsers, and the detection methods relied on URL blacklist or web page content features become useless.

Due to the extensive usage of SSL/TLS in common encryption services, the malicious conversations can easily blend in normal SSL/TLS encrypted traffic to circumvent security devices. Fortunately, in the past attacks, self-signed certificates are usually used, so we are able to find some certificate based features to identify the suspicious behaviors. However, the widespread free certificates, especially the DV certificates, make the detection of malicious services much more difficult. An obvious change is that DV certificates is more and more used in malware command and control (C&C) servers, phishing sites, and anonymous services. There are mainly three reasons. First, DV certificate issuing process has become automatic without manual operation since for most CAs, which requires only an Email address authentication rather than complex offline identity inspection and verification. So attackers or malware makers can easily obtain a validated certificate. Second, a DV certificate is able to make the malicious sites look normal in web browser and pass certificate validation. It looks much more reliable to the victims than a self-signed one causing warnings. Thirdly, a DV certificate will help the malicious server hide it in the large scale small site servers since such certificates have similar security attributes. Therefore, the free DV certificates have become a great challenge in SSL/TLS security. The free certificate issuing in a number of well-known CAs, and the special CAs to promote Internet encryption security, i.e. Let's Encrypt [2], bring new security issues as well as the security and privacy convenience for data communications. It is time to study how to detect the malicious SSL/TLS services as early as possible to mitigate the information and property loss.

II. Measurement and Results

To study the DV certificates, we carry out a two-week X.509 certificate based measurement on SSL/TLS services in two large research networks in China, namely China Education and Research network (CERNET), and China Science and Technology Network (CSTNET), which have millions of users and tens of Gbps bandwidth. The Netflow of all SSL/TLS connections are recorded and then the certificates are obtained by active scans. Then all the certificates and user behavior data are collected and analyzed. Besides, two datasets namely the SSL Blacklist (SSLBL) [3] and PhishTank [4] are exploited to study the malicious services in SSL/TLS. The measurement results are introduced below.

A. Who Offers Free DV Certificates

In our measurement, a total of 546,493 DV certificates issued by more than 10 CAs are gathered. The name of the CAs and the scale are shown in Fig.1 below.

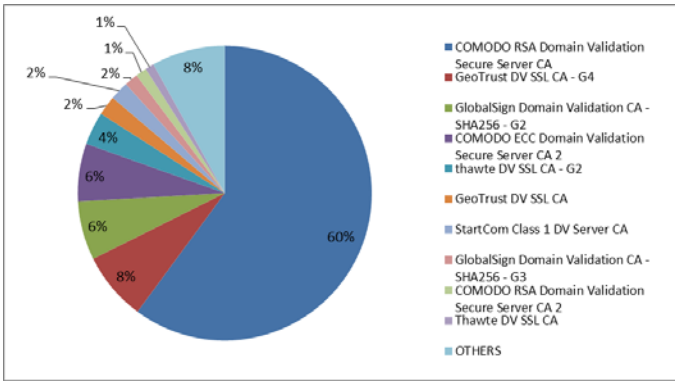

Fig. 1. CAs issuing DV certificates.

From the results, we can see that "COMODO RSA Domain Validation Secure Server CA" issues 60% of the total active DV certificates, and COMODO is currently the most popular CAs in DV certificate issuing.

B. How Popular Are the DV Certificates in The Real World

There are totally 68,885,481,789 SSL/TLS connections related to 5,310,455 distinct servers, of which 6.35% servers and 4.81% connections use DV certificates. While the result was 2.21% and 0.11% respectively in October 2015. So actually the DV certificate is becoming quite popular now.

C. How Does A Normal DV Certificate Look Like

We find out that the subject of most DV certificate only has CommonName (CN) and OrganizationUnit (OU) fields, and generally one OU field contains the phase "Domain Control Validated". An example is shown in Fig. 2 below.

Fig. 2. A DV certificate used by a phishing site.

D. How often are DV certificates used in malicious services

SSLBL is a well-known project offering SHA1 fingerprints of known malicious certificates and IP addresses associated with malware activities. While PhishTank offers a real-time updating phishing URLs dataset. We analyze the evolution of DV certificates' usage in the two datasets. Table I shows the statistics of all the certificates in SSLBL from 2014 to now.

TABLE I. DV CERTIFICATES IN SSLBL

Certificate Type	Counts	Percentage
DV	158	4.14%
Self-Signed	3626	94.95%
Others	35	0.92%

The result obtained from SSLBL reveals that more attackers are using DV certificates to encrypt their SSL connections as time goes. In 2014, only 60 DV certificate cases were found In SSLBL, while the number came up to 123 in 2015, which is twice as much as that in 2014.

We employ an analysis of the latest PhishTank dataset on April 8th, 2016. 439 URLs are extracted using HTTPS out of the total 31,373 ones and finally are classified into 240 domains. After an active scanning we obtain 240 certificates and 85 of them were DV types, with a percentage of 35.4%.

III. ANALYSIS AND CONCLUSION

A. Possible Trends

CAs use different ways for verifying the identities of the organization or individual purchasing certificates. Domain Validated certificates are typically verified and issued through automated and loose processes, so they are more and more frequently used in malicious services. From two typical public datasets we have confirmed the trend. Therefore, the problem should be paid enough attention to from now on.

B. Challenges and Future Work

To the best of our knowledge, no solution to SSL/TLS malicious service detection is satisfying in practice. Signature-based methods fail due to the data encryption. Certificate fingerprints based method is incomplete and delayed. Certificate feature based machine learning is usually limited to small sample datasets [5, 6, 7], and is usually tested against phishing problem which has apparent domain or CN inconsistency. As for other malicious services, such as banking Trojan, ransomware, and botnet, there are not good solutions.

In our opinion, threat intelligence sharing should be enhanced among different research groups, security companies, and governments to improve malicious SSL/TLS service discovery. Besides, the authentication of entry identity in applying DV certificate should be reinforced. Meanwhile, small sites should be helped to improve their security level against attacks and hijacking.

ACKNOWLEDGMENT *(HEADING 5)*

This work is supported by the National Science and Technology Support Program (No. 2012BAH46B02) and the Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDA06030200).

REFERENCES

[1] Dangers of Domain-Validated SSL Certificates. http://www.symantec.com/connect/blogs/dangers-domain-validated-ssl-certificates

[2] Let's Encrypt - Free SSL/TLS Certificates. https://letsencrypt.org/

[3] The Swiss Security Blog. SSL Blacklist. HTTPS://sslbl.abuse.ch/.

[4] PhishTank | Join the fight against phishing. https://www.phishtank.com/index.php

[5] Z. Dong, A. Kapadia, J. Blythe and L. Jean Camp, "Beyond the Lock Icon: Real-time Detection of Phishing Websites Using Public Key Certificates," the tenth Symposium on Electronic Crime Research (eCrime 15), Barcelona, Spain, 2015.

[6] M. Almishari, E. De Cristofaro, K. El Defrawy, G. Tsudik, "Harvesting SSL certificate data to identify web-fraud", International Journal of Network Security , 2012, 14 (6) , pp. 324-338

[7] R. Bortolameotti, "C&C Botnet Detection over SSL", University of Twente, 2014.