

Haute école du paysage, d'ingénierie et d'architecture de Genève



MISE A JOUR DES CERTIFICATS ROOT PAR MICROSOFT

Stéphane Küng

19 juin 2014

Mise en évidence de l'installation automatique de certificats Root par Microsoft sur un ordinateur Windows 7 (toutes versions) de manière invisible pour l'utilisateur et sans son consentement explicite. Une option existe pour bloquer ce dispositif, mais n'est par défaut pas activée.

Haute école du paysage, d'ingénierie et d'architecture de Genève



Table Des matières

INTRODUCTION	3
DEMONSTRATION	3
FONCTIONNEMENT	<u> </u>
CONCLUSION	11
DEVELOPPEMENT ULTERIEUR DU SUJET	11





Introduction

Lors d'un test en entreprise, j'ai constaté que malgré l'absence d'un certificat **Root** dans le gestionnaire de certificats Windows pour un domaine nouvellement acheté, un site web pouvait quand même s'afficher avec un certificat valide et conforme. Après vérification, le certificat **Root** de l'autorité de certification (CA) avait magiquement apparu dans mon gestionnaire de certificats Windows, et ce sans en avoir été informé ou avoir donné mon aval sur son installation.

Le certificat du site web visité n'aurait tout simplement pas dû être validé, car mon ordinateur n'accordait aucune confiance à l'autorité de certification de ce domaine.

Démonstration

La démonstration est ici effectuée sur ordinateur Windows 7 en version professionnelle équipé d'un Internet Explorer 8. Le site web utilisé ici est celui de la Bank of America <u>https://www.bankofamerica.com</u> en **HTTPS** (Figure 1). A noter que toutes les versions de Windows 7 (de Home à Ultimate) sont concernées.

🖉 Bank of Am	erica — Banking, Credit Cards, Mortgages and Investi	ng - Wind	ows Internet Expl	orer				
OO - 	https://www.bankofamerica.com/			_	Bank of Americ	a Corporation	n [US]	47 🗙
🔆 Favorites	✤ Bank of America — Banking, Credit Cards, Mortgages …							Č
			Personal	Small Business	Wealth Man	agement	Busi	inesses 8
	Bank of America 🧇			Locati	ons Contact	Us Help	En es	spañol
	Enter your Online ID Sign In		Bank	Borr	ow	Inv	vest	
	Save this Online ID							

Figure 1 - Site sécurisé de la Bank of America

Haute école du paysage, d'ingénierie et d'architecture de Genève



Figure 2 - Certificat EV de la banque



Figure 4 – Certificat Root de VeriSign

Nous commençons par constater que le certificat de ce site web est valide (Figure 2) et nous apercevons également son chemin de certification émanant de VeriSign (Figure 3). Il s'agit d'un certificat EV¹ qui n'est normalement délivré qu'après vérification de l'identité de l'organisme acquéreur

l'identité de l'organisme acquéreur.

Ce certificat **Root** (Figure 4) se trouve bien dans le gestionnaire de certificats Windows (Figure 5) de notre ordinateur. Ces certificats sont installés par défaut avec le d'exploitation. système Le gestionnaire de certificats Windows permet un aperçu global des certificats (du système et des utilisateurs) ce que l'outil d'aperçu certificats **Root** d'Internet des

Explorer ne permet pas. Il permet également de créer des CSR ainsi que des certificats autosignés.

Nous sélectionnons ensuite tous les certificats Root se trouvant dans le dossier Trusted Root

Certification Authorities et les supprimons (Figure 6).



Figure 3 - Chemin de certification

Menu : Démarrer Exécuter : certmgr.msc

Figure 5 – Gestionnaire de certificat Windows

🚟 Console1 - [Console Root\Certif	ficates (Local Computer)\Trusted R	oot Certification Authorities\Certific	ates]			_ 🗆 🗡
🚠 File Action View Favorites	Window Help					_8×
🗢 🔿 🙍 📅 🔯 🖉						
Console Root	Issued To 👻	Issued By	Expiration Date	Intended	Actions	
Certificates (Local Computer) Personal	The	ere are no items to show in this view.			Certificates	-
🖃 🧮 Trusted Root Certification #					More Actions	•
Certificates						
Enterprise Trust						
Trusted Publishers						
Untrusted Certificates						
🕀 📔 Third-Party Root Certificatio						
Image: Trusted People		. 6				
E Smart Card Trusted Roots						
Trusted Devices						
					1	

Figure 6 - Dossier nettoyé des certificats Root (Thrusted Root Certification Authorities)

¹ Extended Validation (Vérification de l'identité de l'acquéreur)







Nettoyons ensuite le cache SSL du navigateur Internet Explorer (Figure 7 et 8). Le but ici est de forcer le navigateur à revérifier le chemin de certification pour chaque site visité.

Internet Options	
General Security Privacy Content Connections Programs Advanced Parental Controls Image: Content that can Image: Parental Controls Image: Content Advisor Content Advisor Image: Control the Internet content that can be viewed on this computer. Image: Content that can be viewed on this computer.	Menu : Outils Options : Internet Onglet : Contenu Bouton : Vider le cache SSL
Certificates Use certificates for encrypted connections and identitivation. Use certificates for encrypted connections and identitivation. Publishers AutoComplete Publishers AutoComplete stores previous entries Settings Feeds and Web Sices Settings read in Internet Explorer and other programs. Settings CK Cancel Apply	Figure 8 - Procédure pour vider le cache SSL d'Internet Explorer 8

Actualisons ensuite la page d'accueil du site <u>https://www.bankofamerica.com</u>. Nous constatons déjà qu'aucune erreur n'est apparue, que la barre d'adresse est verte (certificat EV valide) et que son certificat est validé. Rafraichissons le dossier **Trusted Root Certification Authorities** dans le gestionnaire de certificats Windows. Nous constatons immédiatement l'apparition de quatre nouveaux certificats **Root** : deux VeriSign, un Equifax et un DigiCert (Figure 9).

Mann Farraitas	MGa davis - Utala				
view Favorites	window Help				
1 0 0					
	Issued To 🔻	Issued By	Expiration Date	Intended A	Actic
s (Local Computer)	🔄 VeriSign Class 3 Public Primary Cer	VeriSign Class 3 Public Primary Certifi	17.07.2036	Server Al	Certi
al	Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	22.08.2018	Secure Er	
d Root Certification /	DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	10.11.2031	Server AL	
rtificates	Class 3 Public Primary Certification	Class 3 Public Primary Certification A	03.08.2028	Server AL	
rise Trust					
ediate Certification A					
d Publishers					
ted Certificates					
s i a ca ca c	l n				
	Figure 9 - Les qua	atre nouveaux certificats Root			





Fonctionnement

Lançons maintenant Wireshark pour analyser les paquets d'une requête HTTPS vers le site <u>https://www.bankofamerica.com</u>. Nous remarquons assez rapidement que notre ordinateur, lors de la requête, se connecte sur le site de VeriSign et reçoit un paquet (Paquet N° 50 sur la Figure 10) contenant 3 certificats de manière non chiffrée.

Capturing from Local Area Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]	
<u>Ele Edit View Go Capture Analyze Statistics Telephony</u> Tools Internals <u>H</u> elp	
● ● ∡ ■ ፈ ⊟ ≞ ≭ ₴ ♀ ⇔ ⇒ ₮ ⊈ 🗏 🖶 Q Q 🖭 i	📓 🖻 🎭 📜
Filter: Expression Clear Apply Save	
No. J Time Source Source Destination	Protocol Length Info
41 12.2827890 10.2.2.5 www-ilg.verisign.net	TCP 66 49930 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_F
42 12.3801830 www-ilg.verisign.net 10.2.2.5	TCP 66 https > 49930 [SYN, ACK] Seq=0 ACK=1 Win=5840 Len=0 MSS=1380
44 12.3822040 10.2.2.5 www-ilg.verisign.net	TLSV1 178 Client Hello
45 12.4795230 www-ilg.verisign.net 10.2.2.5	TCP 60 https > 49930 [ACK] Seq=1 Ack=125 Win=5888 Len=0
46 12.4802770 www-ilg.verisign.net 10.2.2.5	TLSV1 1434 Server Hello
4/ 12.4803/50 WWW-11g.Ver151gn.net 10.2.2.5	TCP 1434 LICP segment of a reassembled PDUJ
49 12.5779660 www-ila.verisian.net 10.2.2.5	TCP 1434 [TCP segment of a reassembled PDU]
50 12.5779930 www-ilg.verisign.net 10.2.2.5	TLSV1 575 Certificate
51 12.5780130 10.2.2.5 www-ilg.verisign.net	TCP 54 49930 > https [ACK] Seq=125 Ack=4662 Win=66240 Len=0
52 12.5789440 10.2.2.5 www-11g.ver1sign.net	TLSV1 380 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
53 12.060/010 www-rig.verisign.net 10.2.2.5	ARP 60 who has 10.2.2.202 Tell 10.2.1.1
55 12.7190800 10.2.2.5 255.255.255	DHCP 342 DHCP Inform - Transaction ID 0x83dbbeef
56 12.7194220 pfsense. localdomain 10.2.2.5	DHCP 342 DHCP ACK - Transaction ID 0x83dbbeef
57 10 701500010 0 0 5 10 0 055 055	
Certificates Length: 4555 □ Certificates (4555 bytes) Certificate Length: 1750 ■ Certificate Length: 1750 ■ Certificate Length: 1570 © Certificate Length: 1226 □ Secure Sockets Layer □ Tsit Secure Layer: Handbake Protocol: Server Hello Done	Name-Infrastructure Operations
OO90 13 25 54 56 72 67 73 65 20 61 .2 terms of use a OO000 74 20 67 67 77 27 65 20 61 .2 terms of use a OOb00 74 20 68 74 77 77 27 65 20 28 risign.c cm/rpa (OOb0C 63 29 30 36 31 33 30 06 03 55 40 31 21 56 C)O61806 .0	

Figure 10 - Réception des certificats Root

Les paquets suivants étant chiffrés, nous supposons que le dernier certificat est récupéré ici.

Si aucun élément récupéré ici ne permet de montrer comment VeriSign est intervenu ici, nous pouvons penser qu'un lien vers le site de VeriSign est codé en dur dans la machine.

Deux points nous permettent d'affirmer ceci :

- 1. Il serait beaucoup trop facile d'autosigner un certificat pour un site web et d'inclure un lien qui forcerait Windows 7 à installer ce certificat **Root** dans son gestionnaire de certificats de manière transparente.
- 2. Si le CA n'est pas VeriSign, la procédure passe par un téléchargement du certificat au travers de Windows Update et non pas directement sur le site du CA.

h e p i a

Haute école du paysage, d'ingénierie et d'architecture de Genève



En effet, après divers essais, nous avons constaté que si le certificat **Root** d'un domaine n'est pas VeriSign, mais par exemple GoDaddy², et que ce dernier n'existe pas dans le gestionnaire de certificats Windows ou qu'il a été supprimé par manque de confiance. Une connexion est directement établie vers le serveur <u>www.download.windowsupdate.com</u> pour récupérer le certificat **Root** manquant. Ce dernier est automatiquement installé dans le gestionnaire de certificats (Figure 11), et la page web s'ouvre ensuite sur le site web. Cette récupération du certificat se fait également au travers d'une connexion non chiffrée comme le laisse apercevoir la capture Wireshark (Packet N° 53 sur la Figure 12) sur lequel le lien de téléchargement est clairement visible et exploitable (Figure 14)

Go Daddy Root Certificate Authori... Go Daddy Root Certificate Authority... 01.01.2038

Figure 11 - Le certificat Root GoDaddy est installé dans le gestionnaire de certificats Windows

certificateQualintra.pcapng [Wireshark 1.1]	0.6 (v1.10.6 from master-1.10)]		_ @ ×
<u>Elle E</u> dit <u>Vi</u> ew <u>Go</u> <u>Capture Analyze Stati</u>	tics Telephony Tools Internals Help		
e 💿 🖌 🔳 🔬 🗁 🛗 💥 🔁	🔍 🗢 🔿 🐨 👱 🗐 📑 Q. Q.	0, 🖭 🖼 🗹 畅 💥 📜	
Filter:	Expression Clear Appl	y Save	
No. Time Source	Destination	Protocol Length Info	
44 9.98136000 10.2.1.1	Broadcast	ARP 60 who has 10.2	2.21: Tell 10.2.1.1
45 10.9092690 10.2.2.5	10.2.255.255	NBNS 92 Name guery N	3 WPAD<00>
46 11.6652390 10.2.2.5	10.2.255.255	NBNS 92 Name query N	3 WPAD<00>
47 12.4296050 10.2.2.5	10.2.255.255	NBNS 92 Name query N	3 WPAD<00>
48 13.2108350 10.2.2.5	10.2.255.255	NBN5 92 Name query N	3 WPAD<00>
49 13.3032130 10.2.1.1	Broadcast 10 2 255 255	ARP 60 WHO Has 10.2	2.21? TETT 10.2.1.1
51 14, 5652090 10, 2, 1, 1	Broadcast	ARP 60 who has 10.2	2.217 Tell 10.2.1.1
52 14.7383660 10.2.2.5	10.2.255.255	NBNS 92 Name query N	3 WPAD<00>
53 15.5032690 10.2.2.5	a95-101-0-113.deploy.akamaitechnolog	ies.com HTTP 268 GET /msdown]	pad/update/v3/static/trustedr/en/47BEABC922EAE80E78
54 15.5039130 a95-101-0-113.d	eplo10.2.2.5	TCP 60 http > 49932	[ACK] Seq=1 Ack=215 Win=5840 Len=0
55 15. 5373210 a95-101-0-113. d	ep1010.2.2.5	TCP 1078 [TCP segment	of a reassembled PDU]
50 15.5373530 a95-101-0-113.0	epioiu.2.2.5	HITP 308 HITP/1.1 200	OK (application/x-x509-ca-cert)
58 15 5651150 10 2 1 1	Broadcast	APP 60 who has 10 2	2 212 Tell 10 2 1 1
59 15, 9787820 10, 2, 2, 5	pfsense.localdomain	DNS 85 Standard que	v 0x7878 PTR 113.0.101.95.in-addr.arpa
60 15.9797590 pfsense.localdo	main10.2.2.5	DNS 142 Standard que	y response 0x7878 PTR a95-101-0-113.deploy.akamai
4			
Frame 53: 268 bytes on wire (2)	44 bits), 268 bytes captured (2144 bits)	on interface 0	
Ethernet II, Src: AsustekC_91:1	8:3f (90:e6:ba:91:f8:3f), Dst: IntelCor_	9f:ba:ae (00:15:17:9f:ba:ae)	
Internet Protocol Version 4, S	<pre>c: 10.2.2.5 (10.2.2.5), Dst: a95-101-0-1</pre>	13.deploy.akamaitechnologies.com (95.101.0.113)
Transmission Control Protocol,	Src Port: 49932 (49932), Dst Port: http	(80), Seq: 1, Ack: 1, Len: 214	
GET /msdownload/undate/v3/st:	tic/trustedr/en/478EA8C022EAE80E78783465	0470645C254EDE688 crt HTTP/1 1\r\n	
Connection: Keep-Alive\r\n			
Accept: */*\r\n			
User-Agent: Microsoft-Crypto/	API/6.1\r\n		
Host: www.download.windowsup	late.com\r\n		
(Full request URT: http://www	w download windowsundate com/msdownload/u	indate /v2/static/trustedr/en/4785AB	C022EAE80E78782462A70E45C254EDE688_crt]
[HTTP request 1/1]	1. downroad, wrndowsupdate, com/ insdownroad/ d	puace/v5/scacic/cluscedi/ell/4/beAb	<u>C922EAE60E76763462A79F43C234F0E668.CfC1</u>
[Response in frame: 56]			
		-	
0020 00 71 c3 0c 00 50 52 ff 73	42 0a 02 02 05 5T 656.@ WB	_e	<u> </u>
0030 f6 ba f9 97 00 00 47 45 54	20 2f 6d 73 64 6f 77GE T /msdo	w	
0040 6e 6c 6t 61 64 2t 75 70 64 0050 73 74 61 74 69 63 2f 74 73	61 74 65 21 76 33 21 nload/up date/v3		
0060 65 6e 2f 34 37 42 45 41 42	2 43 39 32 32 45 41 45 en/47BEA BC922EA	/ E	
	36 32 41 37 39 46 34 80E78783 462A79F	4	
0090 48 54 54 50 2f 31 2e 31 00	38 42 20 63 72 74 20 SC254FDE 68B.CFC 1 0a 43 6f 6e 6e 65 63 HTTP/1.1Conne		
00a0 74 69 6f 6e 3a 20 4b 65 6	70 2d 41 6c 69 76 65 tion: Ke ep-Aliv	/e	
0000 00 0a 41 63 63 65 70 74 3a	20 2a 2f 2a 0d 0a 55Accept : */* 3a 20 4d 69 63 72 6f ser-agen t: Micr	0	
00d0 73 6f 66 74 2d 43 72 79 70) 74 6f 41 50 49 2f 36 soft-Cry ptoAPI/	6	
00e0 2e 31 0d 0a 48 6f 73 74 3a	1 20 77 77 77 2e 64 6f .1Host : www.d		
0100 64 61 74 65 2e 63 6f 6d 00	I Oa Od Oa date.com	Υ.	_
The full requested URL (including host name) (htt Packets: 60 * Displayed: 60 (100.0%) * Dronned: 0 (0.0%)		Profile: Default
			21:11
🔽 Start 💋 🧭 🔚	📸 💻		* 🔊 📜 _{08.05.2014} 💻
Figur	e 12 - Récention du certifi	cat Root au travers de	Windows Undate

² GoDaddy : Prestataire de service internet ayant commencé la vente de certificats SSL après le lancement de Windows 7



Haute école du paysage, d'ingénierie et d'architecture de Genève



Ouvrons ensuite ce certificat pour constater qu'il s'agit bien du certificat **Root** de GoDaddy (Figure 13).

Centrificate
Certificate Information
This certificate is intended for the following purpose(s):
Ensures the identity of a remote computer Proves your identity to a remote computer Ensures software came from software publisher Protects software from alteration after publication Protects enail messages Allows data to be signed with the current time
Issued to: Go Daddy Root Certificate Authority - G2
Issued by: Go Daddy Root Certificate Authority - G2
Valid from 01. 09. 2009 to 01. 01. 2038
Install Certificate Issuer Statement Learn more about certificates
ОК

Figure 13 - Le certificat Root GoDaddy Récupéré via Windows Update

	Untitled	×	
~	\rightarrow C	🗅 www.download.windowsupdate.com/msdownload	l/update/v3/static/trustedr/en ☆ 🗧
			\searrow
	This type of want to kee	file can harm your computer. Do you p 47BEABC922EAE80E78crt anyway? Keep Discard	Show all downloads ×

Figure 14 - Téléchargement en HTTP du certificat Root GoDaddy

Après quelques recherches, il semble bien que Microsoft utilise cette méthode pour mettre à jour les certificats périmés, supprimés, mais semble également l'utiliser pour enlever et supprimer des certificats **Root** révoqués ou qui sont jugés dangereux par Microsoft sur notre

Haute école du paysage, d'ingénierie et d'architecture de Genève



Désactivation

Si l'on ne désire pas, pour des raisons de sécurité, que des certificats **Root** sur notre ordinateur soient manipulés à notre insu. Par exemple dans le secteur bancaire, ou seul certains sites sensibles (souvent même internes) sont accessibles ou si simplement nous décidons de ne pas accorder notre confiance au gouvernement chinois (CNNIC Root Certificate) ou américain (Government Root Certification Authority). Il est possible de modifier ce comportement dans les GPO de Windows (Figure 15, 16 et 17).

Menu : Démarrer Executer : gpedit.msc Chemin : /Computer Configuration/Administrative Template /System/Internet Communication Management/ Dossier : Internet Communication settings GPO : Mettre Turn off Automatic Root Certificates Update à Enabled

Figure 15 - Désactiver la mise à jour de certificats







Aucun redémarrage de l'ordinateur n'est nécessaire, une fois cette modification effectuée, il suffit de vider le cache SSL du navigateur, supprimer les certificats Root du gestionnaire de certificats Windows et de rafraichir la page de Bank of America pour constater que le certificat n'est pas valable (Figure 18). En effet, aucun certificat Root n'est disponible pour ce domaine, la relation de confiance n'a donc pas lieu d'exister.

🙆 Certificate	Error. Navigation Blocked - Windows Internet Explorer	
G - [https://www.bankofamerica.com/	• •
🔆 Favorites	Certificate Error: Navigation Blocked	
×	There is a problem with this website's security certificate.	
	The security certificate presented by this website was not issued by a trusted certificate authority.	
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.	
	We recommend that you close this webpage and do not continue to this website.	
	Vick here to close this webpage.	
	Sontinue to this website (not recommended).	
	⊗ More information	

Figure 18 - Certificat invalide pour la banque sans le certificat Root et avec modification du GPO adéquat

A noter que la modification de cette règle GPO dans Windows 7 a pour effet d'ajouter un certificat Root de Microsoft dans le gestionnaire de certificats Windows (Figure 19). La raison n'est pas connue.

Issued To 🔺	Issued By	Expiration Date	Intended
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	10.05.2021	<all></all>

Figure 19 - Certificat Root Microsoft

A noter également que chrome utilise le même gestionnaire de certificats, à savoir celui de l'OS. Cette modification affectera donc également chrome, qui, de la même manière affichera un message d'erreur mentionnant qu'aucune confiance n'est attribuée à ce domaine. Firefox à l'inverse, utilise son propre gestionnaire de certificats et n'est pas conséquent pas affecté par cette manipulation. Il convient néanmoins de vérifier dans son gestionnaire de certificats en quel CA l'on place sa confiance.

Haute école du paysage, d'ingénierie et d'architecture de Genève



Conclusion

Nous constatons que cette fonctionnalité de mise à jour de certificats Root par Microsoft sur Windows 7 n'est absolument pas documentée ni expliquée. Le choix par défaut du GPO n'est également pas justifié par Microsoft.

On peut évidemment le comprendre pour des versions comme Home de Windows 7 où l'utilisateur ignorant du fonctionnement des Autorités de certification ne veut pas qu'on le dérange avec des messages incompréhensibles pour lui. Il donne donc toute sa confiance à la société Microsoft qui lui a vendu une licence d'utilisation de son OS.

Inversement ce choix se justifie difficilement pour des versions Professionnelles de Windows 7 utilisées en entreprise, ou la sécurité informatique est un point vital (exemple : une banque, un état) et où l'on peut se demander de la pertinence de la présence d'un certificat Root pour le gouvernement chinois et surtout sa réapparition après suppression. La simplification de l'utilisation se fait ici au détriment de la sécurité, ce qui n'est du gout de l'auteur pas tolérable.

Après un test le 19 juin, J'ai constaté que la version serveur Windows Server 2012 R2, sortit en octobre dernier est également impacté.

Après un deuxième test effectué ce même jour, l'utilisation de Google Chrome comme navigateur impacte également la machine. Chrome utilisant également le gestionnaire de certificat Windows. Je pense que c'est peut-être cet élément de Windows qui effectue les mises à jours (A vérifier).

Développement ultérieur du sujet

Le temps à disposition pour ce travail n'étant que de dix heures, certains points n'ont pas pu être développés ici.

Il est néanmoins possible avec plus de temps, dans le cadre un travail d'approfondissement d'utiliser les points proposés ici comme direction :

- Mettre en place un proxy pour faire une attaque de type Man-in-the-Middle et remplacer le certificat téléchargé en HTTP par un autre.
- Expliquer pourquoi lorsque le CA est VeriSign, la procédure ne passe pas par Windows Update, mais télécharge directement le certificat sur le site de VeriSign.
- Ce système permettrait également la suppression de certificats si ce dernier n'est pas ou plus proposé par Microsoft.