Preventing Spying from Faked Security Certificates

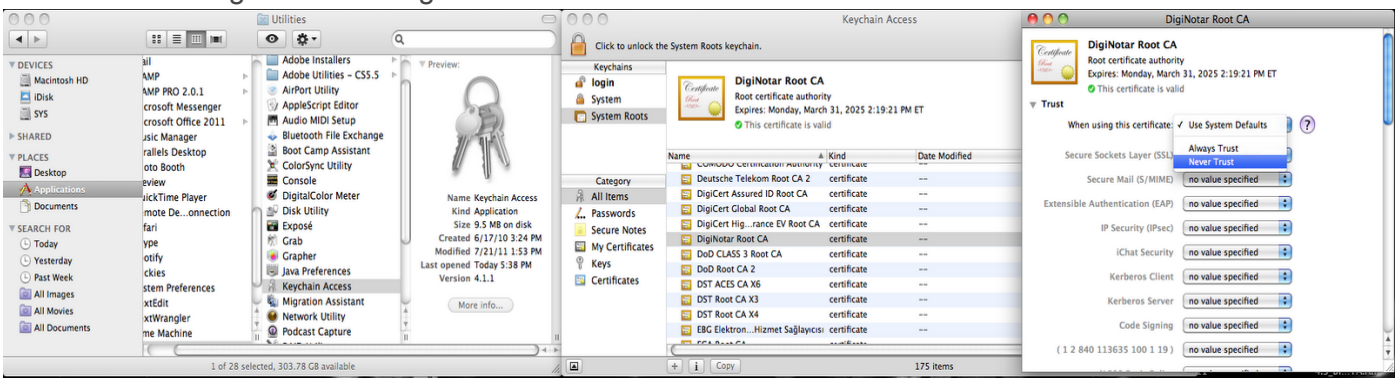
This is intended to specifically address the events happening at the end of August 2011 in Iran, where a security incident for a Dutch company has left Iranian Internet users vulnerable to spying. There has been a lot written in general about staying safe online, please consult organizations like Tactical Tech, Access Now or contact me directly at (collin@averysmallbird.com).

As written about in Mardomak[1], beginning last week, several Iranian Internet providers appeared to use security certificates stolen from a Dutch company 'DigiNotar' to impersonate other sites, including Google. This allowed individuals to spy of web browsing that is normally considered secure to eavesdropping. Using faked sites to collect passwords, government organizations may potentially have access to a large number of Iranian Google users' account. The attack was first noticed when a user in Mashhad reported the problem, however users from across the country been affected. We have confirmed this applies to at least users of ParsOnline, Pishgaman, Datak and Shatel, however it may apply to all Iranians. Additionally, it is possible other sites than Google were targeted in the attack, however, the list of who is not available yet.

Stop the Problem

1. If you do not use Google Chrome or Mozilla Firefox, switch to them. If you are already running either, keep your browser up to date. For Firefox users, the problem is only fixed by updating to a version released on Tuesday, or follow the instructions available at: http://support.mozilla.com/en-US/kb/deleting-diginotar-ca-cert
2. Make your computer not trust the company that issued the fake information.

   Mac OS X: Open the application 'Keychain Access' in the Utilities folder in 'Applications' Click 'System Roots'-> DigiNotar Root Ca -> Get Info -> Trust -> Change "When using this certificate" to 'Never Trust.'

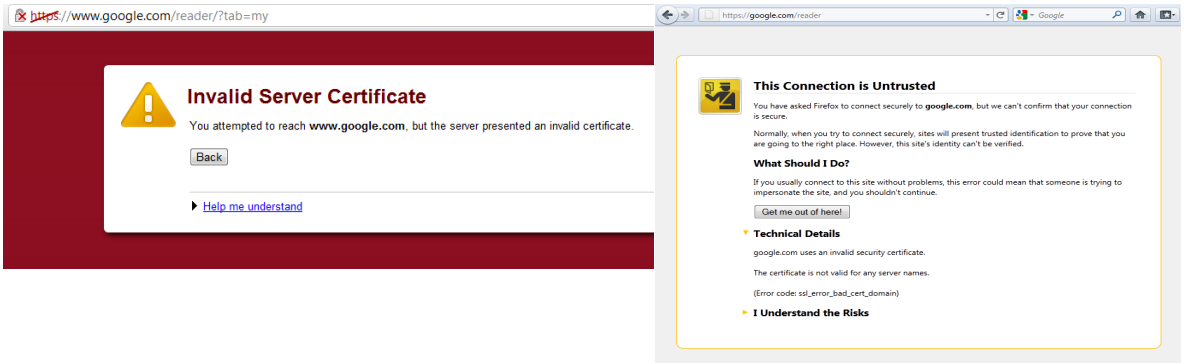


   Windows: The list of trusted companies for Internet Explorer is maintained by centrally by Microsoft and the company has been removed from that list. Internet Explorer is vulnerable to other security problems and you should take this time to switch to Chrome or Firefox. Firefox users still need to update to the latest version, or follow the instructions above.

1

Limit the Damage

1. Immediately change your password. Use a long combination of words and numbers that makes sense only to you, long sentences or combinations of words that you can remember are better than short passwords that you will forget. Do not use your new password anywhere else.



2. When your Internet Browser warns you that a site may not be trustworthy, do not ignore the warning. This is not normal. It means that something important has changed and that strangers are possibly watching your interactions with the site. Do not continue to use the site until the problem is addressed.

Best Practices to Avoid Future Problems

Currently, there is no way for you to directly prevent attacks like this. Keeping security in mind is the best precaution. The problem was discovered by vigilant Iranians who paid attention to browser warnings and strange behavior. However, there are ways to limit your exposure and potential damage the next time something happens.

1. Use software such as Tor or a VPN to bypass government control/censorship and avoid future attacks. Circumvention tools limit the opportunity for tampering with web browsing and provide a layer of security against spying. VPNs don't mean you are entirely safe, you should consider whether the source of the software is trustworthy before you use it.
2. Smartphone owners should add Google's 2-step authentication to their account. Enabling this feature will require you to enter in a number that your phone displays when you sign on from a new computer. This means that if someone steals your password, they will not be able to get into your email without having access to your phone as well.

   More information is available here: http://www.google.com/support/accounts/bin/static.py?page=guide.cs&guide=1056283&topic=1056284

روشهای ساده برای جلوگیری از تجسس ناخواسته توسط گواهینامه های دیجیتال جعلی

همانطور که در سایت های خبری نوشته شد، ، از آغاز هفته پیش تعدادی از سرویس های ارائه کننده اینترنت در ایران از گواهینامه های امنیتی به سرقت رفته از شرکت هلندی "دیجی نوتار" برای حمله به سایت هایی نظیر گوگل استفاده کرده اند. این حمله برای نخستین بار در شهر مشهد شناسایی شده است، با این حال این حمله بسیاری از کاربران اینترنت در سراسر کشور را در بر می گیرد. براساس تحقیقات انجام شده، بسیاری از کاربران پارس آلاین، پیشگام، داتک و شاتل هدف این حمله بوده اند. حدس و گمانها بر این است که علاوه بر گوگل، سایت های دیگری نیز هدف حمله بوده اند که هنوز نام و مشخصات آنها گزارش نشده است. مقاله زیر در تلاش است تا راههای ساده ایی را برای پیشگیری و مقابله با این نوع حملات در اختیار خوانندگان قرار دهد.

راههای ساده برای مقابله با این مشکل:

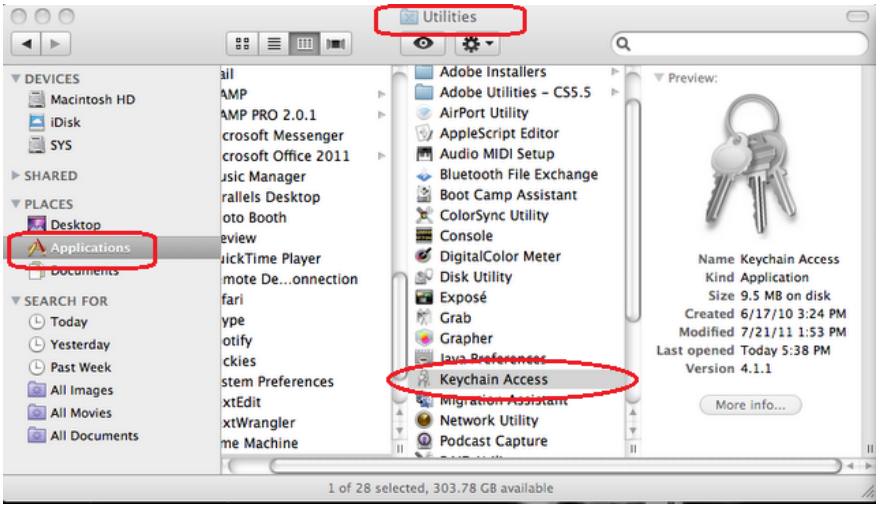
1. از یکی از دو مرورگر گوگل کروم و یا فایرفاکس استفاده کنید. اگر در حال حاضر از این دو استفاده می کنید، مرورگرخود را بروز کنید.

کاربران فایرفاکس تنها لازم است که آخرین نسخه ایی که در روز سه شنبه 30 آگوست منتشر شده را دانلود کنند. برای اطلاعات بیشتر می توانید به تارنمای زیر مراجعه کنید:
http://support.mozilla.com/en-US/kb/deleting-diginotar-ca-cert

2. در تنظیمات کامپیوتر خود، نام کمپانی تولید کننده این گواهینامه جعلی را وارد کنید:

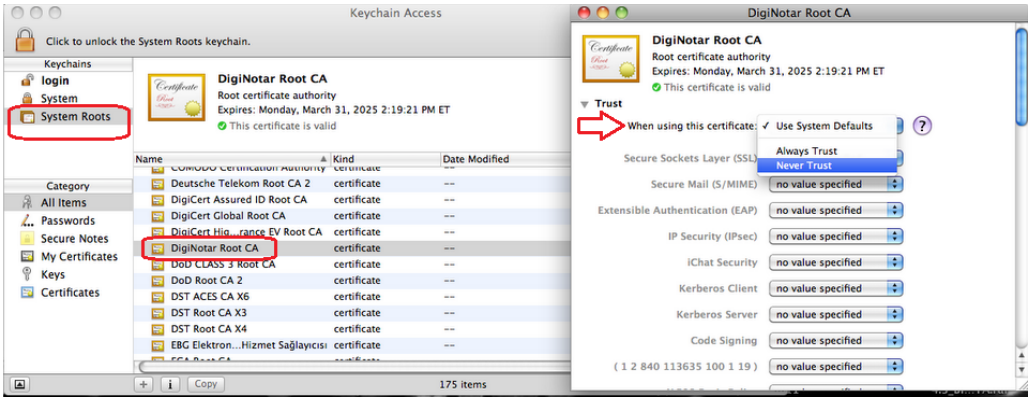
برای کاربران سیستم عامل مک:

به بخش Applications بروید. بر روی فولدر Utilities کلیک کنید و برنامه Keychain Access را باز کنید:



سپس مراحل زیر را انجام دهید:

در برنامه "Keychain Access" بر روی "System Roots" کلیک کنید و از میان گزینه ها، بر روی گزینه " DigiNotar Root Ca" کلیک سمت راست کنید و گزینه "Get info" را انتخاب کنید:



سپس گزینه "Never Trust" را با توجه به تصویر بالا انتخاب کنید.

برای کاربران سیستم عامل ویندوز:

نام این شرکت از لیست شرکت های قابل اعتماد در اینترنت اکسپلورر حذف شده است. با این وجود توجه داشته باشید که مرورگر اینترنت اکسپلورر از سایر جهات امنیتی قابل اعتماد نیست و توصیه اکید این است که ازمرورگر فایرفاکس و یا گوگل کروم استفاده کنید.

میزان خسارت را به حداقل برسانید:

1. حتما رمز عبور خود را عوض کنید. استفاده از ترکیب عبارتها و ارقام طولانی و یا جملات طولانی که فقط برای شما معنی می دهد استفاده کنید. رمز عبور خود را در جای دیگری به جز برای ایمیل استفاده نکنید.

2. زمانی که مرورگر اینترنت به شما این هشدار را می دهد که سایتی که میخواهید وارد شوید قابل اعتماد نیست، این اخطار را نادیده نگیرید. این نوع اخطارها طبیعی نیست. این هشدارها به این معناست که چیز مهمی در سیستم امنیتی شما بهم ریخته و افراد دیگری احتمالا به سیستم شما رخنه کرده اند. تا زمانی که این اخطار را دریافت می کنید از ورود به سایت خودداری کنید.

جلوگیری از این نوع مشکلات در آینده:

در حال حاضر راهی برای مقابله مستقیم با این نوع حملات وجود ندارد. بهترین راه پیشگیری، حفظ امنیت و مشاهده دقیق تغییرات جزئی در سیستم است. با این حال برای محدود کردن این نوع حملات راهکارهای زیر را پیشنهاد می کنیم:

1. برای دور زدن سانسور از ابزارهای مانند "Tor" و یا وی پی ان استفاده کنید. <u>استفاده از وی پی ان به معنی این نیست که سیستم شما کاملا در امان است. پیش از استفاده از وی پی ان، مطمئن شوید که منبع آن قابل اعتماد است.</u>
2. به دارندگان گوشیهای هوشمند توصیه می کنیم تا از گزینه دو مرحله ایی احراز هویت در گوگل برای دسترسی به ایمیل خود استفاده کنند. با این روش برای دسترسی به حساب کاربری خود توسط یک کامپیوتر جدید، باید در ابتدا ارقامی که توسط گوگل به تلفن شما فرستاده می شود را وارد کنید تا بتوانید به حساب کاربری خود دسترسی داشته باشید. با این روش، اگر فردی به غیر از شما بخواهد به این ایمیل دسترسی داشته باشد باید تلفن شما را هم در اختیار داشته باشد.

برای اطلاعات بیشتر می توانید به تارنمای زیر مراجعه کنید:

http://www.google.com/support/accounts/bin/static.py?page=guide.cs&guide=1056283&topic=1056284

برای اطلاعات بیشتر در این زمینه می توانید با نویسنده این مقاله از طریق آدرس ایمیل زیر در ارتباط باشید:

Collin Anderson, collin@averysmallbird.com