How The Hack of DigiNotar Changed The Internet's Infrastructure

Transcript of https://www.youtube.com/watch?v=FXpTftnjqM8
&list=RDCMUCXk6whiDrWq42y9Tdv1MEhg&index=28

Rob Witcher, Destination Certification Inc, Canada
Transcript form 0:48 to 13:33, adapted by Marius Joldoș

1 Introduction

A government seemingly spying on their citizens, a respected internet security company imploding, 300 000 users affected and long lasting industry changes. All of this due to a relatively unknown Dutch company called DigiNotar.

This is the story of the biggest hack you've never heard of. This hack might have targeted a little-known company, but it had far-reaching impact the hack lasted for nearly six weeks before it was brought to the public's attention, and in that time it managed to do enough damage to shake up the online security industry and the Dutch government. It also led to some big changes in online security infrastructure.

Let's dig into what happened shall we?

On Saturday, August 27, 2011, an iranian man who went by the online name Alibo couldn't connect to his gmail account. Oddly, he discovered that if he used a vpn (a virtual private network) he could access it. Whatever was going on it seemed to be only affecting people in Iran. He asked a question about the issue in the Google help forum and, to his surprise, Google responded in a big way: they issued a public statement about the incident after Alibo's query. In the statement they attributed the problem to a hack on a Dutch company called DigiNotar.

But this hack was different than most. It wasn't that a company had failed to protect its users data. *DigiNotar was a certificate authority*, its whole job was to issue digital certificates for websites, which it did. Just not securely enough, as the security breach resulted in fraudulent certificates being issued, which in turn led to a **man-in-the-middle attack** against Google users in Iran.

Within a month of the initial discovery, the Dutch government took over DigiNotar and it didn't take long for the company to go bankrupt thereafter.

Digital Certificates. So let's back up and talk about digital certificates. Every day there are all sorts of websites and software being built and coded by all sorts of people and companies and, as we know, some of them don't have the best of intentions.

So, every time you load a web page, you go to a website, your browser checks to ensure you're connecting to the intended web server and not some phony sketchy server that an attacker is trying to trick you into, visiting to harvest your organs or something.

How can a web browser know it's talking to the intended web server?

This is where digital certificates come in.

Certificate Authorities. Trusted third parties called **certificate authorities** (CAs), vouch for websites by issuing them digital certificates and this system is basically the foundation of online security. Digital certificates and the infrastructure around them are what provides trust on the internet.

So, we can verify and trust who we are communicating with. CAs do what is known as **identity proofing** to vet website operators and software developers and sell digital certificates to the ones they deem to be legitimate.

There's different types of CAs.

A small group are *so trusted that all major browsers and operating systems around the world will automatically trust any certificates issued by these CAs*. They're called **root certificate authorities**.

Certificates enable your browser to authenticate the server and securely exchange encryption keys, so that you can have a nice and secure encrypted connection with a now trusted website. You can easily see this in your browser bar: there'll be a little lock icon beside a website address it means your browser has obtained the server certificate, inspected it, exchanged symmetric encryption keys and established a secure connection with the server.

DigiNotar was one of these few very reputable route certificate authorities trusted by all the major web browsers around the world and the Dutch government to issue digital certificates.

As you might expect CAs are a very juicy target for attackers. if an attacker could control a root CA and issue certificates, they'd have the opportunity and means for all sorts of mischief like phishing scams, malware attacks, credential harvesting etc. etc. The list is almost endless. It would be super bad adventure to say catastrophic.

Security is of utmost importance to CAs and it seems that it was taken very seriously by DigiNotar. They had segmented their network into several isolated partitions; every request for a new certificate had to be vetted and approved by two different employees; and then to issue certificates there was a whole rigamarole to go through. Certificates were only issued from a computer in a specially secured room and the description of the physical security measures in place sound like the description from a heist film.

According to report by security firm FoxIT on DigiNotar security, this room could be entered only if authorized personnel used a biometric hand recognition device and entered the correct pin code. This inner room was protected by an outer room connected by a set of doors that opened dependent on each other creating a sluice. These sluice doors had to be separately opened with an electronic door card that was operated using a separate system than any other door to gain access to the outer room from a publicly accessible zone; another electronic door had to be opened with an electronic card. I've got to say not enough hacking stories use the word sluice in them, but seriously that is some intense mission impossible style security.

2 Chronology

So how did this attack occur during the summer of 2011? It seems DigiNotar's security efforts fell short. The company was running some unpatched software on one of its web servers.

In June an intruder managed to make their way in and began to slither around in the company's partitioned networks. According to reports the intruder first gained access EXT-NET, on June 17th, 2011.

From the DMZ, the hacker managed to burrow into DigiNotar's secure net on July 1st, 2011, which contained the company's eight certificate authority servers. Specialized tools were used to create tunnels for a non-direct connection to the internet for remote access to the servers.

On July 10, 2011, the intruder issued their first *rogue certificate*: a wildcard certificate for Google.com. This certificate was posted on pastebin and was used by an unknown person in Iran to conduct a man-in-the-middle attack against Google's services, potentially allowing the attacker to decrypt and read all user traffic sent to and from what users thought was Google sites.

On July 19th, DigiNotar performed one of their routine checks. It was discovered that there were some digital certificates that had been issued, that DigiNotar had no record of whatsoever. An internal investigation was launched and the rogue certificates revoked immediately.

By the end of July, DigiNotar believed they'd effectively dealt with a problem and it was business as usual. Little did they know the issues were only the beginning of the end for the company: when the iranian user Alibo brought to light the unauthorized Google certificate and Google pointed the finger at DigiNotar, it became clear that their internal investigation had only scratched the surface of the problem.

Users from 298,140 unique IP addresses, trying to access Google websites, were redirected to sites that looked like Google, smelled like Google and were certified to belong to Google, based on the fake digital certificate.

But, of course, they weren't Google sites. 95% of the users who were affected were from Iran. To this day, no one really knows if or how the intruder managed to get past the physical security protecting the inner room for certificate issuing. Did they dangle from the air conditioning vents in the ceiling? Surely that's how Tom Cruise would have done it. The investigator's best guess is that some of the electronic key cards for the doors were left permanently in place, largely defeating the whole purpose of all the other security measures. Less exciting but probably more plausible in the end.

The intruder managed to issue a total of 531 rogue certificates.

One thing stood between these impostor sites and unsuspecting users: the Google chrome browser. Although Chrome had DigiNotar as a trusted root CA, it would have accepted any of DigiNotar's certificates for any other domains, the browser had something special in place for Google domains. Google knew exactly which certificates it had purchased and had **pinned** these certificates to its Chrome browser. So when the redirects occurred, although the impostor site seemed to have a valid certificate belonging to, Google chrome knew better this wasn't one of Google's legitimate certificates and that's why Google chrome users such as Alibo couldn't access gmail accounts.

In august Google chrome was blocking their access because the browser knew it was an *invalid certificate*.

3 Investigations

The incident was so serious that the Dutch government felt the need to step in they took control of DigiNotar and commissioned the security firm FoxIT to investigate the breach. The Dutch government themselves had put a lot of trust in DigiNotar, relying on them for their own digital certificates: all tax returns filed in the Netherlands had relied on certificates issued by DigiNotar. For example, the Dutch government's IT infrastructure suffered significant damage from this attack.

Roel Schowemberg, senior antivirus researcher for Kaspersky said at the time that the hack truly crippled part of the Dutch infrastructure, including some hospitals, financial services and law firms. But what was the purpose behind the fake Google web pages and rogue certificates? Probably to gain access to view users emails. The Iranian government was strongly suspected to be involved, but no one was ever charged for anything related to the incident. In typical cyber attack fashion, the only hint as to the identity of the perpetrator who issued the fraudulent certificates was a poorly written comical message left behind on a server which read: "I know you are shocked of my skills how I get access to your network. There is no any hardware or software in this world exist, which would stop my heavy attacks, my brain or my skills or my will, my expertise". Why do cyber criminals always tend to sound like megalomaniacs?

It's amazing, but there's a serious side note to the redirection of Iranian gmail users. **Hans Hoogstraaten** of FoxIT, who led the investigation, said in an email: "what really shocked me was when i realized the impact it had for the people of Iran. In those days people got killed for having a different opinion.

The hackers, presumably the state, had access to over 300 000 gmail accounts. The realization that the security of a small company in Holland may have played a part in the killing or torture of people really shocked me"

This breach had enormous implications and really left the internet security realm reeling and it was the catalyst for some tangible lasting changes to the world of online security infrastructure.

So what were the major lessons learned from this breach?

4 Lessons Learned

Five years later, in 2016, leading CAs and Microsoft introduced new minimum security requirements to help protect consumers online. These were the first ever standardized guidelines related to **code signing** which is *a method of verifying an author's identity and ensuring the code has not been changed or corrupted*.

As the beginning of 2017, Microsoft announced that they would require all CAs to adhere to these minimum security standards, which really forced CAs to comply, since Microsoft is, well, Microsoft.

The thing which led to the initial discovery of the DigiNotar debacle was Google's system for **pinning** its own certificates in its own Chrome browser. This allowed Google to recognize the fraudulent certificate, which uncovered the truth the DigiNotar hack, gave rise to greater use of certificate pinning.

Issues with certificate pinning have subsequently been identified and most browsers have now *deprecated* pinning and switched to **certificate transparency**. The certificate transparency initiative aimed to *make sure that all certificates issued by CAs are logged and these logs are made publicly available*. In the past the public wasn't really aware about the behind-the-scenes going-ons of the CAs and the certificates they issued. But this knowledge makes it far easier for individual domain owners to monitor whether any certificates have been issued for their domains without their knowledge. More awareness and transparency can help to keep people vigilant and help to catch fraudulent certificates more quickly.

As an incentive to encourage CAs to log their certificates, in 2015 Google began only displaying the green address bar in chrome for companies whose certificates had been logged.

The internet security research group established a **CA**, called **Let's encrypt**, in 2016, advocating for widespread online encryption. **Let's encrypt** (`https://letsencrypt.org/`) *offers free certificates to anyone who wants one more certificates*, means more encryption. This hack set in motion a series of events that may have mostly gone unnoticed by the broader public, but that really changed the online certificate landscape.

CAs are still prime targets for attackers, but hopefully another incident like this one won't occur anytime soon.