Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

By Dennis Fisher

Published: 2012-10-31 · Archived: 2026-04-06 01:56:14 UTC

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a security company commissioned to investigate the DigiNotar attack shows that the compromise of the now-bankrupt certificate authority was much deeper than previously thought.

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a security company commissioned to investigate the DigiNotar attack shows that the compromise of the now-bankrupt certificate authority was much deeper than previously thought.

In August 2011 indications began to emerge of a major compromise at a certificate authority in the Netherlands, previously unknown to most of the Internet's citizens, and the details quickly revealed that the attack would have serious ramifications. The first public acknowledgement of the attack was the discovery of a large-scale man-in-the-middle attack against Gmail users in Iran. Researchers investigating that attack discovered that the operation was using a valid wildcard certificate, issued by DigiNotar, for *.google.com, giving the attacker the ability to impersonate Google to any browser that trusted the certificate.

It quickly emerged that the attacker also had obtained valid certificates for a number of other high-value domains, including Yahoo, Mozilla and others. The browser manufacturers scrambled to revoke trust in the compromised certificates and reassure users that the Internet was not broken. Now, the final report from Fox-IT, the Dutch company brought in at the time of the attack in 2011 to find the root cause and determine the extent of the damage, says in its final report that the attack was a wide-ranging one that likely started more than a month before the CA discovered it.

"The investigation by Fox-IT showed that all eight servers that managed Certificate Authorities had been compromised by the intruder. The log files were generally stored on the same servers that had been compromised and evidence was found that they had been tampered with. Consequently, while these log files could be used to make inconclusive observations regarding unauthorized actions that took place, the absence of suspicious entries could not be used to conclude that no unauthorized actions took place," the report, which was just made public this week, says.

One of the most worrisome aspects of the DigiNotar breach at the time it leaked out was that the company not only was a commercial CA, but it also issued government certificates, calling into question the legitimacy of those certificates, as well. The Fox-IT report says there are some indications in their investigation that the attacker may have issued some rogue certificates that have not been identified yet, a troubling prospect.

“Serial numbers for certificates that did not match the official records of DigiNotar were recovered on multiple CA servers, including the Qualified-CA server which was used to issue both accredited qualified and government certificates, indicating that these servers may have been used to issue additional and currently unknown rogue certificates,” the report says.

An anonymous hacker who earlier had claimed responsibility for the attack on Comodo, another certificate authority, said he also had executed the DigiNotar hack. In its report, Fox-IT said that there were some signs that the same person who compromised Comodo had indeed penetrated DigiNotar, as well.

“A fingerprint that was left by the intruder was recovered on a Certificate Authority server, which was also identified after the breach of the Certificate Service Provider Comodo in March of 2011. Over the course of the intrusion at DigiNotar, the intruder used multiple systems as proxies in order to obscure his true identity. However, several traces were recovered during the investigation by Fox-IT that independently point to a perpetrator located in the Islamic Republic of Iran,” the report says.

DigiNotar had its network highly segmented and had a number of those segments separated from the public Internet. However, the company did not have strict enforcement of the rules on its network, something that may have enabled the attacker to move from the Web server he initially compromised over to the servers that house the certificate authorities.

“The investigation showed that web servers in DigiNotar’s external Demilitarized Zone (DMZ-ext-net) were the first point of entry for the intruder on June 17, 2011. During the intrusion, these servers were used to exchange files between internal and external systems, with scripts that were placed on these systems serving as rudimentary file managers,” the Fox-IT report says.

“From the web servers in DMZ-ext-net, the intruder first compromised systems in the Office-net network segment between the 17th and 29th of June 2011. Subsequently, the Secure-net network segment that contained the CA servers was compromised on July 1, 2011. Specialized tools were recovered on systems in these segments, which were used to create tunnels that allowed the intruder to make an Internet connection to DigiNotar’s systems that were not directly connected to the Internet. The intruder was able to tunnel Remote Desktop Protocol connections in this way, which provided a graphical user interface on the compromised systems, including the compromised CA servers.”

The attack on DigiNotar lasted for nearly six weeks, from start to finish, according to the report, and the attacker was using multiple systems outside and inside the network during the operation.

“The investigation by Fox-IT showed that all servers that managed Certificate Authorities had been compromised by the intruder, including the Qualified-CA server, which was used to issue both accredited qualified and government certificates. In total, a non-exhaustive list of 531 rogue certificates with 140 unique distinguished names (DNs) and 53 unique common names (CNs) could be identified. The last known date for traffic that was

initiated from within DigiNotar's network to an IP address that was presumably (ab)used by the intruder was on July 22, 2011. Traces of activity by the intruder in DMZ-extnet were found up to July 24, 2011," the report says.

The attacker had complete control of the CA servers during the attack and had the ability to alter log files, which were kept on the same servers as the CAs, and to make changes to the database. An interesting detail from the report is that DigiNotar could not produce any records showing whether a smart card had been used to activate the private keys in the hardware security module that correspond to the compromised CAs. The attacker would not have been able to issue the rogue certificates without the private keys, so he also needed to find a way to activate them.

"The private keys were activated in the netHSM using smartcards. No records could be provided by DigiNotar regarding if and when smartcards were used to activate private keys, except that the smartcard for the Certificate Authorities managed on the CCV-CA server, which is used to issue certificates used for electronic payment in the retail business, had reportedly been in a vault for the entire intrusion period," Fox-IT's report says.
