

Comodo CA Security in 2011

Why PKI still works

2011 is fast becoming an “annus horribilis” for the CA Industry. Producers and consumers of SSL certificates have been affected by multiple security breaches of varying severity.

CA Security in 2011

And why PKI still works.

Comodo CA's certificate issuing infrastructure was not compromised in any way.

Comodo CA's HSM modules and private keys were not compromised.

REVIEW

There have been four service-affecting breaches of security of systems or processes in or around commercial CAs this year – and the year isn't over yet.

Comodo had the unfortunate distinction of being the first target of the year.

We released information about the fraudulent certificates that were issued from our CA back in March. As we said at the time – “.. with regard to your inquiry concerning the [then] recent events involving the fraudulent access and use of a Comodo RA's user account. This RA account was then used fraudulently to issue 9 SSL certificates in 7 domains. The fraud was detected within hours, as Comodo revoked the certificates, alerted browsers, domain owners and relevant law enforcement authorities in the USA and UK.”

- Comodo CA's certificate issuing infrastructure was not compromised in any way.
- Comodo CA's HSM modules and private keys were not compromised.

Although our own computer systems resist a regular onslaught of attacks, we were made aware that our RAs (in layman's terms we really mean a subset of our largest and most trusted customers such as WebHosts, Registrars, and Enterprise Service Providers) had become proxy targets.

COMODO CA SECURE

- A Comodo RA (not Comodo itself) was compromised in March.
- 9 Certificates were fraudulently issued on 15th March. The event was detected immediately.
- The browsers and the targeted site-owners were informed the next day and reacted immediately.
- Details were published 8 days after the attack in March.
- Comodo and its resellers and its competitor CAs have continued to be the target of frequent attacks.
- Comodo has suffered no breach and its systems and services remain secure.

CA Security in 2011

And why PKI still works.

Comodo CA's certificate issuing infrastructure was not compromised in any way.

Comodo CA's HSM modules and private keys were not compromised.

REVIEW

As a result of the events of March, and meeting (and exceeding) new requirements on CAs put out by Microsoft in the wake of those events, we took steps to protect the issuance of certificates even when the usual, trusted, legitimate source of certificate requests (such as the RAs) was under attack or had already been compromised.

If you are a non-retail customer of ours you will have seen our processes changing since March, and our requirements for information about the certificates you require becoming more onerous. These are just the visible effects of the process changes we have made. There are many more going on behind the scenes.

The measures we put in place after the March event have been tested by a number of subsequent attacks and, as we expected, there has been no further fraudulent or unauthorized issuance of certificates. The attacks have not succeeded. We have always been a target for attacks and we always will be. As long as the attacks remain unsuccessful then we are achieving our goal of providing you with a secure CA platform.

Sadly there have been attacks on other CAs too and the attack on DigiNotar (a Dutch CA providing CA services to commerce and the Dutch government) appears to have resulted in a thorough breach of their systems. Many certificates were mis-issued – perhaps no-one knows how many. The browsers and platforms which had trusted DigiNotar to issue SSL (and other) certificates have stopped trusting them and their certificates are now useless.

Comodo did not have any business dealings with DigiNotar and there is no trust relationship between our certificates and theirs. Their success or failure does not affect any Comodo-issued certificates in any way.

There have been recent claims of an attack on another competitor, GlobalSign, and they are dealing responsibly with the issue and, at the time of writing, have ceased issuing certificates but are planning to recommence.

The Timeline of events in 2011

Comodo CAs Issuing infrastructure, HSM modules and private keys were not compromised.

Comodo (Through a Reseller)

15th March - Attack

- Incident - A server on the site of an Italian reseller was compromised
- Outcome - 9 Certificates for high-profile sites were issued without validation being carried out (i.e. were issued to the attacker)
- Internal Actions - Detection, revocation

16th March - Disclosure to affected site owners & to major browser producers (Microsoft, Mozilla, Google, Apple, Opera)

- External Actions - Browsers blacklist the 9 certificates.

23rd March - Coordinated public disclosure.

Startcom

15th June - Attack, Detection & Ceases issuing certificates.

- Incident - An application server at the CA was compromised.
- Outcome - Some system(s) breached, but no certificates issued.
- External actions - none/unknown

18th June - Disclosure of event to closed audience.

- Recommence issuing certificates.

21st June - Public disclosure of event.

DigiNotar

17th June - Attack

- Incident - Multiple CA systems compromised
- Outcome - Systems breached, 531(+?) certificates issued

19th July - Detection

29th August - Public detection (google.com)

30th August - Public disclosure (turned out to be partial)

1st Sep - Further disclosure

- External Actions - browsers blacklist 531 certificates & all known DigiNotar intermediates & roots.
- External Actions - dutch government swoop to close DigiNotar

5th Sep - Publication of 3rd party cyber security report

GlobalSign

5th Sept - Hacker publishes unsubstantiated claims of multiple CAs compromised, names GlobalSign.

6th Sept - GlobalSign begins concerted investigation and "temporarily cease[s] issuance of all Certificates"

7th Sept - GlobalSign announces appointment of 3rd party cyber security group to assist with investigations.

8th Sept - GlobalSign publishes timetable for recommencement of issuing.

9th Sept - GlobalSign discover webserver breach.

10th Sept - GlobalSign announce they are working with 'Cyber Defense Institute Japan'

13th Sept - GlobalSign address a specific claim related to the issuance of untrusted "demo" certificates.

The Future & Conclusion

Comodo CA's certificate issuing infrastructure was not compromised in any way.

Comodo CA's HSM modules and private keys were not compromised.

Future Review

There will continue to be attacks on CAs, on their resellers, and on their customers.

The CAs are here to help the certificate users to provide secure and authenticated ways for them to interact with their website users.

The hierarchical trusted PKI security model is not perfect. It requires that there be a number of trusted 3rd party CAs. There are other models which involve trusting no-one, or trusting every-one, or trusting majority votes and these models may yet be developed to provide a working alternative but they too will not provide perfect security. A vigilant, competent, well-policed, trusted CA remains a core part of today's security model.

The CAs must remain secure to retain their position as trusted 3rd parties. Comodo's CA is secure

Conclusion

- Comodo's CA certificate issuing infrastructure, HSM modules and private keys were not compromised in any way.
- Comodo's Root CAs are still included within the trusted root stores of all major Web browsers.
- Comodo is an active participant in the Certificate Authority and Browser Forum, and fully supports the CAB Forum's standards and recommendations.
- Comodo has audited and will continue to audit on an ongoing basis all of its operations to ensure that it is in full compliance with all applicable industry standards.
- Comodo has implemented additional authentication measures for all partners and enforced Domain Control Verification across all certificate products.
- As the second largest provider of high assurance certificates worldwide, Comodo takes its responsibilities to all of its customers and all those who rely on its certificates extremely seriously, and we know that we continually need to remain worthy of your trust. We appreciate and value our partnerships with each and every one of our customers.