Security Incident Report

We didn't find any evidence of

- Rogue Certificates issued.
- Customer data exposed.
- Compromised GlobalSign Root Certificate keys and associated Hardware Security Modules (HSM).
- Compromised GlobalSign Certificate Authority (CA) infrastructure.
- Compromised GlobalSign Issuing Authorities and associated HSMs.
- Compromised GlobalSign Registration Authority (RA) services.

What did happen

- Peripheral web server, not part of the Certificate issuance infrastructure, hosting a public facing web property was breached.
- What could have been exposed? Publicly available HTML pages, publicly available PDFs, the SSL Certificate and key issued to www.globalsign.com.
- SSL Certificate and key for www.globalsign.com were deemed compromised and revoked.

Impact to Customers

GlobalSign adopted a high threat response to the claims that unfortunately resulted in 9 days of service disruption, specifically:

- New Certificate issuance temporarily halted between 6th and 15th September.
- During outage:
    - GlobalSign contracted Fox-IT to provide third party analysis of the GlobalSign infrastructure. Fox-IT were also retained by the Dutch Government as part of the ongoing Comodohacker criminal investigation.
    - GlobalSign contracted Cyber Security Japan to oversee the rebuild of a newly hardened Certificate issuance infrastructure, on the now disproven assumption that previous infrastructure had been breached.

Timeline

This timeline covers events from 5th September to 15th September 2011.

- The self-titled attacker "Comodohacker" has been assumed to be a credible threat to security providers, in particular Certificate Authorities, since the attack made by the Comodohacker on a Comodo RA Partner resulted in the issuance of rogue Certificates by Comodo in March 2011.
- A post was made on 5th September by the Comodohacker via the Pastebin service claiming responsibility for the DigiNotar hack.
- The same post also stated that several other CAs had been compromised, including a reference to GlobalSign.
- GlobalSign deemed the threat credible and immediately began a thorough network analysis, assuming a highly sophisticated attack had been executed on, or was in process against, multiple Certificate Authorities.

- On 6th September, even though the non-specific Comodohacker claims were yet to be substantiated, GlobalSign deemed the most responsible reaction was to halt issuance of new Certificates in order to:
    - Accelerate the investigation.
    - Protect against issuance of rogue Certificates should the claims be true.
- On 9th September, the investigative team found evidence of a breach to the web server hosting the www.globalsign.com website. The breached web server (located in a hosting facility in North America) was a peripheral web server located externally (both logically and geographically seperate) from the GlobalSign Certificate issuance infrastructure. GlobalSign immediately assumed the contents of the web server were compromised, including:
    - All public facing HTML files.
    - All public facing documents and PDF files.
    - The www.globalsign.com SSL Certificate and key.
- The www.globalsign.com domain is used only for the externally facing North American web sites and runs no web applications capable of requesting or issuing Certificates nor does it hold any customer data.
- The SSL Certificate for www.globalsign.com was revoked.
- The breached web server was immediately locked down and subsequently rebuilt with a new disk and hardened system image.
- In parallel additional security precautions were taken, including:
    - GlobalSign Certificate infrastructure was rebuilt with new hardware and hardened images for all services.
    - Additional IDS (Intrusion Detection Services) were deployed to certificate related services.
    - Enhanced internal controls have been placed around logical access to issuance systems.
    - Operational environment for Internet facing systems has been hardened further.
- On September 15th services were brought back online. All customer account passwords were reset as part of bringing the service back online.

Controls – mitigating against future attacks

GlobalSign, with the help of Fox-IT, found no evidence that the GlobalSign Certificate issuance infrastructure was compromised. However, GlobalSign has implemented additional controls around infrastructure, customer data protection and access to all systems. It is our view that this attack is one phase of an advanced persistent threat against all security solution providers. Because the threat landscape has evolved, GlobalSign believes greater controls are necessary across the industry and echos the calls covered in WebTrust 2.0 and the recent updates to the Mozilla Root CA acceptance program. In response to such requirements, GlobalSign specifically confirms:

- GlobalSign maintains an offline root, and has done since 1996.
    - An offline root means that the GlobalSign Root Certificate key material is not connected to any network of any type. Root key material is physically (geographically) separate from any networked systems and is only ever exercised in controlled, and physically sealed offline ceremonies.
- GlobalSign has never directly issued end entity Certificates using the Root Certificate, instead only ever issuing off Subordinate Certificates (also referred to as the Issuing Authority). In the event of a compromise this would not require the revocation of the entire PKI but only the compromised Subordinate Certificate.
- Fox-IT has been contracted to provide ongoing security consultancy.
- All issuance and Internet facing infrastructure is now monitored 24/7 through a managed IDS service.

Additionally, GlobalSign wishes to restate to customers and partners that physically geographic and logical separation is maintained between critical infrastructure applications, including web servers, order processing applications, CRM, RA applications, Certificate issuance applications and Root Certificates.

GlobalSign Executive Team Response

As one of the longest operating Certification Authorities, the worldwide GlobalSign team is aware of the impact to customers and partners of halting Certificate issuance for any period of time. The executive team apologizes sincerely for the inconvenience caused when undertaking such an important decision. However the organization stands by the decision and maintain that the ultimate duty of care for GlobalSign, like all responsible CAs, is to avoid issuance of rogue Certificates.

We are truly thankful for the positive reaction to our chosen response to the incident, including the press covering this and other incidents, our peers, and ultimately from our valued customers and partners.

GlobalSign has learned much from this incident. More than ever, we appreciate that the threat has evolved, and we are committed to ensuring no such outages occur again from future claims or attacks. In the period since the claims, we have invested significantly in additional security measures and monitoring and suggest other CAs and security providers align to self-regulate to ensure that:

1. Infrastructure is designed and managed in such a way that it is resilient to attack.
2. In the event of a successful attack, swift and appropriate measures are put into place to mitigate the impact.
3. Incident responses are open and transparent allowing Relying Parties the visibility into the risks they may be exposed to.

As an active participant in the CA/B Forum, GlobalSign is a strong supporter of the industry's continued definition and adoption of:

- Transparent incident response and issuance practices.
- Continuous auditing of network and security infrastructure.
- Standards for operational and vetting practices.
- Technology and processes for speedy response to such security incidents.
- Formal collaboration between global authorities and security providers.

Such efforts include the CA/B Forum's minimum guidelines, Mozilla's CA security controls and any future industry initiatives that serve in the best interest of PKI and Internet security in general.

Finally, we also support ongoing co-operation between the security providers, CAs and the various global authorities in sharing threat information promptly and accurately.

Ongoing Authority Involvement

- Many international authorities maintain detailed profiles of the Comodohacker and other actors, and continue to build a more accurate picture with evidence gathered and volunteered by many industry members.
- GlobalSign, like other security providers, continues to share threat information and collaborate closely with all appropriate authorities.

Definitions

As defined in the CA/B Forum Baseline Guidelines – www.cabforum.org

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.