



www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1 800.652.4020

Fidelis Threat Advisory #1003

SSL CHALLENGES IN 2011

September 15, 2011

Document Status: FINAL
Last Revised: 2011-09-27

Executive Summary

Certificate authorities Comodo and DigiNotar were breached in March and August of 2011 respectively, resulting in the creation of large numbers of fraudulent SSL certificates. Many of these stolen certificates were used in subsequent attacks against prominent websites. These events call into question the ability of SSL and TLS to provide trustworthy authenticity, upon which rests the global “web of trust” model they were designed to deliver. Enterprises are urged to monitor SSL activity and take steps to prevent their devices from participating in sessions involving fraudulently signed certificates.

Threat Overview

SSL and TLS are ubiquitous protocols that are intended to create a “web of trust” for securing web and e-mail traffic along with a wide variety of other communication on the Internet. Two incidents have called the authenticity—and hence the overall security—of SSL into question. In March 2011, certificate authority Comodo was breached by attackers who then created fraudulent SSL certificates for prominent websites. In August 2011, an attack against DigiNotar produced similar results. SSL certificates generated by attackers were subsequently used to impersonate those websites in campaigns to deceive and/or defraud their users.

Risk Assessment

An attacker in possession of a fraudulent SSL certificate has the ability to digitally impersonate the entity named in the certificate, establishing a trusted relationship where none should exist. Execution of such an attack requires more than the theft or generation of a false certificate: an attacker must also divert victim traffic to a fraudulent server via DNS manipulation or other means, or gain direct access to the stream as a man-in-the-middle (MITM). This is a nontrivial exercise, but advanced, purpose-driven adversaries have clearly shown that they are up to the task.

Users are granted permission to copy and/or distribute this document in its original electronic form and print copies for personal use. This document cannot be modified or converted to any other electronic or machine-readable form in whole or in part without prior written approval of Fidelis Security Systems, Inc.

While we have done our best to ensure that the material found in this document is accurate, Fidelis Security Systems, Inc. makes no guarantee that the information contained herein is error free.



www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1 800.652.4020

Indicators & Mitigation Strategies

Four parallel approaches are available to mitigate concerns about SSL authenticity.

1. Ensure that root certificates issued by breached root CA's are no longer trusted by devices in your enterprise.
2. Monitor for servers on the Internet presenting SSL certificates to your devices that are signed by invalid root certificates.
3. Inspect the history of SSL activity on enterprise networks after a CA breach is announced, to see whether fraudulent certificates were presented to enterprise hosts in the past.
4. Consider a transition of business critical communication to alternate protocols, such as SSH or IPSEC. Ensure that such a transition does not introduce more risk than it mitigates. Such protocols are suitable for point-to-point security, but neither is viable for implementing the global web of trust for which SSL was designed.

The Fidelis Take

Monitoring for fraudulent SSL certificates can be accomplished with ease using Fidelis SSL Inspector, or less efficiently by using network content inspection technologies like Fidelis XPS to search for these certificates in network traffic streams. Fidelis' SSL Inspector can also be used to identify suspect certificates in hindsight.

Further Reading

- Threat Geek, "Curses! Is SSL Broken Forever?" Will Irace, 9/1/11. <http://goo.gl/KPUEq>
- Black Hat 2011, "SSL And The Future Of Authenticity" [Video], Moxie Marlinspike, Aug 2011. <http://goo.gl/3v3CQ>
- ThreatPost, "Phony SSL Certificates issued for Google, Yahoo, Skype, Others." Paul Roberts, 3/23/2011. <http://goo.gl/Mk4ce>
- The Tech Herald, "Questions remain as DigiNotar suspends SSL offerings after breach." Steve Ragan, 8/31/2011. <http://goo.gl/gY4q1>