RSA-512 Certificates abused in the wild

During recent weeks we have observed several interesting publications which have a direct relation to an investigation we worked on recently. On one hand there was a Certificate Authority being revoked by Mozilla, Microsoft and Google (Chrome), on the other hand there was the disclosure of a malware attack by Mikko Hypponen (FSecure) using a government issued certificate signed by the same Certificate Authority. That case however is not self-contained and a whole range of malicious software had been signed with valid certificates. The malicious software involved was used in targeted attacks focused on governments, political organizations and the defense industry. The big question is of course, what happened, and how did the attackers obtain access to these certificates? We will explain here in detail how the attackers have used known techniques to bypass the Microsoft Windows code signing security model.

Recently Mikko Hypponen wrote a blog on the F-Secure weblog (http://www.f-secure.com/weblog/archives/00002269.html) detailing the discovery of a certificate used to sign in the wild malware. Specifically this malware was embedded in a PDF exploit and shipped in August 2011. Initially Mikko also believed the certificate was stolen, as that is very common in these days, with a large amount of malware families having support, or optional support, for stealing certificates from the infected system. Apparently someone Mikko spoke to mentioned something along the lines that it had been stolen a long time ago. During the GovCert.nl symposium Mikko mentioned the certificate again, but now he mentioned that according to the people involved with investigating the case in Malaysia it likely wasn't stolen.

The reason why Mikko looked at this specific sample and this certificate was likely the recent revocation of Digisign Server ID (Enrich) by Microsoft (http://technet.microsoft.com/en-us/security/advisory/2641690) and earlier by Mozilla (http://blog.mozilla.com/security/2011/11/03/revoking-trust-in-digicert-sdn-bhd-intermediate-certificate-authority/). The interesting part in those articles is that Microsoft does not mention anything about the code signing abilities of certificates while Mozilla does. Microsoft does mention that the certificates were not fraudulently issued but were duplicated due to cryptographically weak keys. The option of stolen certificates is left completely in the middle here.

The whole commotion around Digisign was actually caused by an investigation by Fox-IT completed in mid-October, in which we recovered a number of signed executables embedded in exploits and downloaded additionally by any of the executables. While our investigation did not focus on the signing of those executables, the report was shared in the relevant community, and if you looked at the 4 certificates initially found, it was easy to determine that all were 512bit RSA and used on HTTPS websites, which were still up at the time of writing. Later during our investigation we encountered 5 more certificates which also were used to successfully sign malware throughout 2011 by the same attacker, all 512 bit RSA.

So it is rather obvious what happened, all related RSA-512 keys had been factored and also abused to sign malicious software for the purpose of infiltrating high value targets. You might ask how difficult it is to execute an attack against RSA-512, well, over 12 years ago the RSA-512 challenge was successfully factored. Also we still encounter RSA-512 in protection systems deployed even today, with relatively modern hardware in a small cluster, relatively inexpensive, it takes a couple of weeks. With the lifetime of these certificates being a couple of years, the attackers had plenty of time to do the factoring.

So the reason why Digisign Server ID (Enrich)/DigiCert Sdn. Bhd, was revoked was because their certificates had no CRL in the certificate which allowed to easily revoke the certificate. Also all those certificates were issued without a purpose, in which case the certificates can be used for anything. The certificates we found to be used in the wild recently are:

```
Subject: O=LABUAN INTERNATIONAL FINANCIAL EXCHANGE INC, CN=lfxsys.lfx.com.my
Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)

Subject: C=MY, O=JARING Communications Sdn.Bhd., OU=JARING, CN=webmail.jaring.my, L=W.Persekutuan/emailAddress=sysadmin@jaring.my, ST=Kuala Lumpur
Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)

Subject: C=MY, O=Digicert Sdn. Bhd., CN=mcrs2.digicert.com.my, L=Kuala Lumpur
Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)

Subject: C=GB, ST=Bristol, L=Bristol, O=City of Bristol College, OU=ICLT, CN=ad-idmapp.cityofbristol.ac.uk
Issuer: C=BE, O=Cybertrust, OU=Educational CA, CN=Cybertrust Educational CA

Subject: C=GB, ST=Norfolk, L=Norwich, O=City College Norwich, OU=I.T. Services, CN=stfmail.ccn.ac.uk
Issuer: C=BE, O=Cybertrust, OU=Educational CA, CN=Cybertrust Educational CA

Subject: C=GB, ST=England, L=London, O=London Metropolitan University, OU=ISS, CN=skillsforge.londonmet.ac.uk
Issuer: C=BE, O=Cybertrust, OU=Educational CA, CN=Cybertrust Educational CA

Subject: CN=agreement.syniverse.com, C=US/emailAddress=belinda.jablonski@syniverse.com, L=Tampa, O=Syniverse Technologies Inc., OU=Crossroads, ST=Florida
Issuer: O=GlobalSign Inc, CN=Cybertrust SureServer CA

Subject: C=TW, ST=Taipei, L=Taipei, O=TRADE-VAN, OU=TRADE-VAN, CN=www.esupplychain.com.tw
Issuer: C=TW, O=TAIWAN-CA.COM Inc., OU=SSL Certification Service Provider, CN=TaiCA Secure CA

Subject: C=US, ST=Indiana, L=Indianapolis, O=Anthem Insurance Company Inc, OU=EBusiness, CN=ahi.anthem.com
Issuer: C=US, O=Anthem Inc, OU=Ecommerce, CN=Anthem Inc Certificate Authority
```

Additionally an external party found several other samples which contained 512 bit RSA certificates signed by Digicert Sdn. Bhd:

```
Subject: C=MY, O=BANK NEGARA MALAYSIA, OU=BANK NEGARA MALAYSIA, CN=payments.bnm.gov.my
Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)

Subject: O=FUNDAMENTAL BUSINESS CONCEPTS (M) S/B, CN=www.fbcm.com.my
Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)
```

One of those samples was found in August 2010, and possibly used back in March 2010, indicating how long this issue has been going on without any clear action from the industry. Microsoft whose platform has been targeted by this is the victim of this, and I think that Microsoft should not have relied on weak security properties for a security solution that can apparently be bypassed by parties far outside of the control of Microsoft. Microsoft could simply deny verification of executables which have been signed with a 512bit RSA key after a certain date, as 512 bit RSA has been considered weak for a long time. From the article at TechNet it is clear that Microsoft understand the problem and that they have acted on this accordingly, but the question is if it was not a bit late. Also interesting is that none of the samples have an actual timestamp, we think this is another design decision made that makes these executables pass verification, but it might cause the executables to no longer pass verification after the certificate has expired, we were unable to test this however.

Also one certificate that was used, ahi.anthem.com, did not have the "Digital Signature" property in "Key Usage", thus it should not have passed verification. But we wonder if that indeed is true, as why would the attackers go through great lengths of factoring the RSA key and using it to sign their executables, if it did not pass verification? Either the attackers overlooked something here, or the digital signature verification system in Windows is at fault. We are however unable to verify this as the relevant certificate has expired in April 2011.

So the problem will solve itself eventually with CAs no longer signing 512 bit and more attention is given on the subject. The model of code signing certificates is however not very good as even the expensive code signing certificates can be stolen, and this can be done by simple off-the-shelf malware, such as ZeuS and SpyEye. But let's focus on the issue at hand, how could we go about finding other certificates that might have been abused or could be abused, but that we do not have the executables from to prove it? Well someone already did all the work for us, that would be Peter Eckersly (EFF), Jesse Burns (iSec Partners) and Chris Palmer (EFF) who have worked in 2010 on EFF SSL Observatory (http://eff.org/observatory) that has indexed certificates used on port 443 (HTTPS). They have done presentations on this various times and we want to explicitly thank these guys for their hard work.
So we have used the database from mid-2010 which might be more close to the data the attackers had. So let's see, if we check the 9 certificates we have found being abused in the wild

```
mysql> select distinct `ext:X509v3 Key Usage` as `Key Usage`,`ext:X509v3 Extended Key Usage` as `Ext. Key Usage`,RSA_Modulus_bits as `RSA bits`,name as `CN` from all_names,all_certs where certid=nid and name in
('ahi.anthem.com','lfxsys.lfx.com.my', 'webmail.jaring.my','ad-idmapp.cityofbristol.ac.uk','stfmail.ccn.ac.uk','skillsforge.londonmet.ac.uk','agreement.syniverse.com',
'www.esupplychain.com.tw','mcrs2.digicert.com.my','payments.bnm.gov.my','www.fbcm.com.my');
```

Key Usage	Ext. Key Usage	RSA bits	CN
(critical) Digital Signature, Key Encipherment	NULL	512	ad-idmapp.cityofbristol.ac.uk
(critical) Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	512	agreement.syniverse.com
(critical) Key Encipherment	NULL	512	ahi.anthem.com
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	512	lfxsys.lfx.com.my
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	512	mcrs2.digicert.com.my
NULL	NULL	512	payments.bnm.gov.my
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	512	payments.bnm.gov.my
(critical) Digital Signature, Key Encipherment	NULL	512	skillsforge.londonmet.ac.uk
(critical) Digital Signature, Key Encipherment	NULL	512	stfmail.ccn.ac.uk
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	512	webmail.jaring.my
NULL	NULL	512	www.esupplychain.com.tw
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	512	www.fbcm.com.my

Bingo, they are all there, this is a good indication the people who found these certificates used a similar method to find these certificates, scanning port 443 (HTTPS) for valid 512 bit RSA certificates with no Extended Key Usage property defined and being usable. Note again that the ahi.anthem.com has no Digital Signature Key Usage property.

Okay, so now let's see what other certificates there are in the database from mid-2010 which match similar search criteria, that were valid according the the certificates from Microsoft at the time and have not expired yet.

```
mysql> select name,RSA_Modulus_bits as `RSA bits`,`ext:X509v3 Key Usage` as `Key Usage`,`ext:X509v3 Extended Key Usage` as `Ext. Key Usage`,issuer from all_names,all_certs where certid=nid and enddate>now() and RSA_Modulus_bits='512'
and `ext:X509v3 Extended Key Usage` is NULL and ms_valid='Yes' and (`ext:X509v3 Key Usage` LIKE '%Digital Signature%' or `ext:X509v3 Key Usage` is NULL);
```

name	RSA bits	Key Usage	Ext. Key Usage	issuer
www.altinokburo.com.tr	512	(critical) Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	C=BE, O=GlobalSign nv-sa, OU=ServerSign CA, CN=GlobalSign ServerSign CA
mijn.trust-id.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
applicaties-preprod1.digid.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
as-preprod1.digid.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
was-preprod1.digid.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
applicaties-preprod2.digid.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
as-preprod2.digid.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
was-preprod2.digid.nl	512	(critical) Digital Signature, Key Encipherment, Key Agreement	NULL	C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
supplier.sappi.com	512	(critical) Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	C=BE, O=GlobalSign nv-sa, OU=ServerSign CA, CN=GlobalSign ServerSign CA
suppliertest.sappi.com	512	(critical) Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	C=BE, O=GlobalSign nv-sa, OU=ServerSign CA, CN=GlobalSign ServerSign CA
mcrs2.digicert.com.my	512	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)
mcrs.digicert.com.my	512	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment	NULL	C=MY, O=Digicert Sdn. Bhd., OU=457608-K, CN=Digisign Server ID (Enrich)
skillsforge.londonmet.ac.uk	512	(critical) Digital Signature, Key Encipherment	NULL	C=BE, O=Cybertrust, OU=Educational CA, CN=Cybertrust Educational CA

Okay, we can find two certificates in there which we know that have been abused, specifically skillsforge.londonmet.ac.uk and mcrs2.digicert.com.my, those have 512 bit RSA keys that have been factored. All other certificates seem to have been either revoked directly or indirectly, these are the ones related to DigiNotar and Digicert Sdn. Bhd/Digisign Server ID (Enrich). Others have been individually revoked after they have been replaced in the past. So, it looks like indeed the problem has been solved by revoking trust in Digicert Sdn. Bhd. and DigiNotar B.V. (unrelated) and revoking those specific certificates. We have not observed in the wild usage of other certificates such as the ones signed by DigiNotar, possibly there are other constraints which make it unusable for Code Signing. We will leave it as an exercise to the reader to inspect the other databases which the EFF SSL Observatory has created to find other certificates.

Concluding we can say that definitely there has been a lot of attention on Certificate Authorities and their procedures and also with several incidents such as the forging of data to match an md5 signature and the more recent DigiNotar incident. But this specific issue, while factoring is widely known, had not been addressed and has been used over a year for targeted break-ins of high value targets. While it has not been used for signing of drivers as far as we know, as was done with the stolen certificates used in the Stuxnet and Duqu attacks, it did play a part in the attacks we have observed and as such we think that letting the issue unaddressed for such a long time might have helped the attackers. It was trivial to find these certificates using published data by EFF and luckily it appears that all known certificates have now been revoked, but the question is if there are more certificates which have not been recorded in a database and have been, for example, used on other ports than HTTPS. The fact remains that the code signing mechanism is relying on trust in many parties which are not necessarily trusted, as human error and intentional or unintentional bypassing of procedures can break the entire security model.

Michael Sandee, sandee@fox-it.com
Principal Security Expert at Fox-IT