WoSign and StartCom

This document contains additional information, and Mozilla's proposed conclusion for community discussion, regarding the matter of WoSign and StartCom.

For some weeks now, Mozilla has been investigating a list of potential incidents relating to the CA WoSign. Some of those turned out, in Mozilla's view, to be not WoSign's fault (e.g. Issue T, a mis-issuance for the domain alicdn.com, which got temporarily taken over by an attacker) or only minor (e.g. Issue F, a lack of proper locking); others acknowledged by WoSign are very serious, such as including arbitrary unvalidated domain names in certificates. The most serious from a trust perspective are those that WoSign has denied but where credible evidence exists of the truth of the allegation. One of these was the suggestion (Issue S) that WoSign has been intentionally back-dating certificates to avoid blocks on SHA-1 issuance in browsers, having qualified audits and/or being caught violating the CAB Forum Baseline Requirements. This document gives more information on that allegation; the involvement of StartCom will become clearer as the story unfolds.

Background: SHA-1 Deprecation

SHA-1 is a cryptographic hash algorithm which is rapidly reaching the end of its useful life. Digital certificates, such as those produced by WoSign, are "signed" by making a fixed-length "summary" of the certificate contents using a hash algorithm, and applying public key cryptography to the result in order to produce a signature. SHA-1 has historically been used for this process, but is no longer secure and is being phased out in favour of a more modern algorithm, SHA-256. This sunset process has caused difficulty for a number of companies who cannot move fast enough or who want to retain compatibility with older hardware or software which does not support SHA-256.

All CAs are required, by the policy of Mozilla and other root programs, to adhere to the Baseline Requirements of the CA/Browser Forum. This sets down minimum standards for CA operation. As of 16th October 2014, the BRs forbade the issuance of certificates whose signatures used SHA-1 ("SHA-1 certificates") on or after January 1st 2016.

Digital certificates contain (at least) two dates - a notBefore date which says when the certificate starts to be valid, and a notAfter date which says when it stops being valid. The values for these fields are chosen by the CA and there is no cryptographic requirement that they bear any relation to the actual time of certificate creation. In practice, though, it is expected that the notBefore will be around the time of certificate creation, and the notAfter will be N months later, where N is the amount of validity time agreed by the CA and the customer.

This is all relevant because browsers, including Firefox and Chrome, contain code which enforces the deprecation of SHA-1 by refusing to trust SHA-1 certificates whose (CA-chosen) notBefore date is on or after 1st January 2016, the deadline set in the Baseline Requirements. This means it is technically possible for a CA to issue a SHA-1 certificate in

2016 but attempt to avoid detection, browser blocks and any sanctions by back-dating it to some time in 2015. Mozilla, as one can imagine, frowns on this practice.

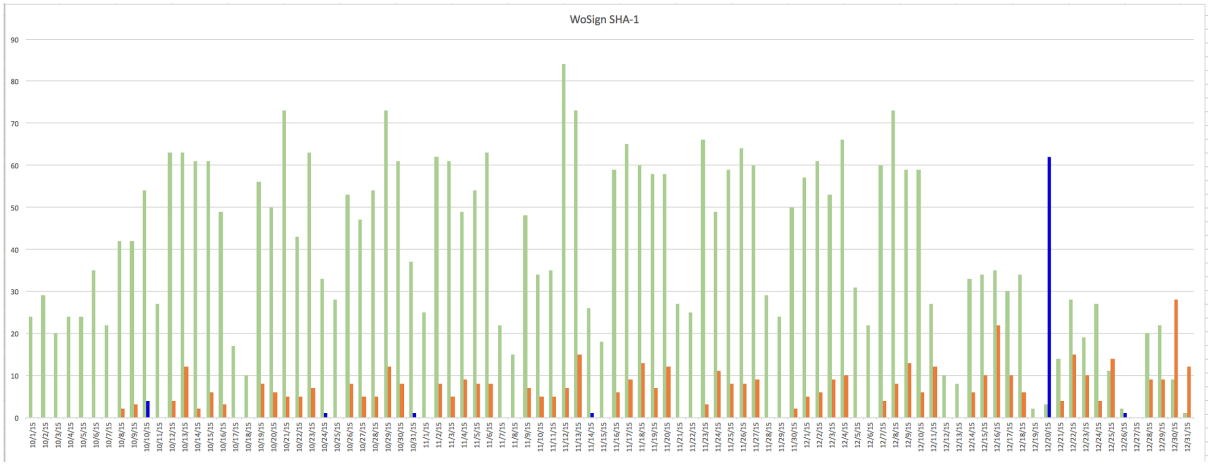
WoSign and Back-Dated SHA-1

We believe that anomalies in WoSign's patterns of issuance indicate that a collection of 62 SHA-1 certificates were issued in 2016 (or on December 31st 2015) and back-dated to indicate that they were issued in December 2015.

Certificate authorities often use a system of templates and automation to cut down on the manual work of issuing certificates, and reduce errors. A template sets many of the fields in a certificate to a known value or one of a set of known values. A CA's issuance automation may also determine how certain fields are calculated automatically from other fields, or from environmental data such as the current time. These templates and systems can have "fingerprints", such as particular extensions, fixed fields, ways of doing things or even encoding errors, which allow you to work out which template was in use.

In the latter part of 2015, when SHA-1 issuance was still permitted, data from online archives of issued certificates indicate two distinct types of SHA-1 certificate being issued by WoSign. In the first, which we will call Type X, certificates have the same hours, minutes and seconds values in the notBefore and the notAfter fields. The dates, of course, would generally be one year apart. Here is an example of a Type X certificate. In the second, which we will call Type Y, the notAfter field (i.e. the expiry date) is fixed at Dec 29th 2016 16:00 UTC, which is midnight on Dec 29th/30th 2016, China time. Here is an example of a Type Y certificate. This fixing of the notAfter date in this style of certificate may have been a sensible move to avoid accidentally issuing SHA-1 certificates whose validity extends into 2017, which would go against a SHOULD NOT in the BRs. (WoSign was in fact doing that for several months early in 2015 before they fixed it - Issue D.)

This graph shows the number of SHA-1 certificates issued by WoSign with a notBefore date in the last three months of 2015, as we approach the SHA-1 issuance cut-off date. (Note that the certificates have been grouped by day in China Standard Time, not UTC.)

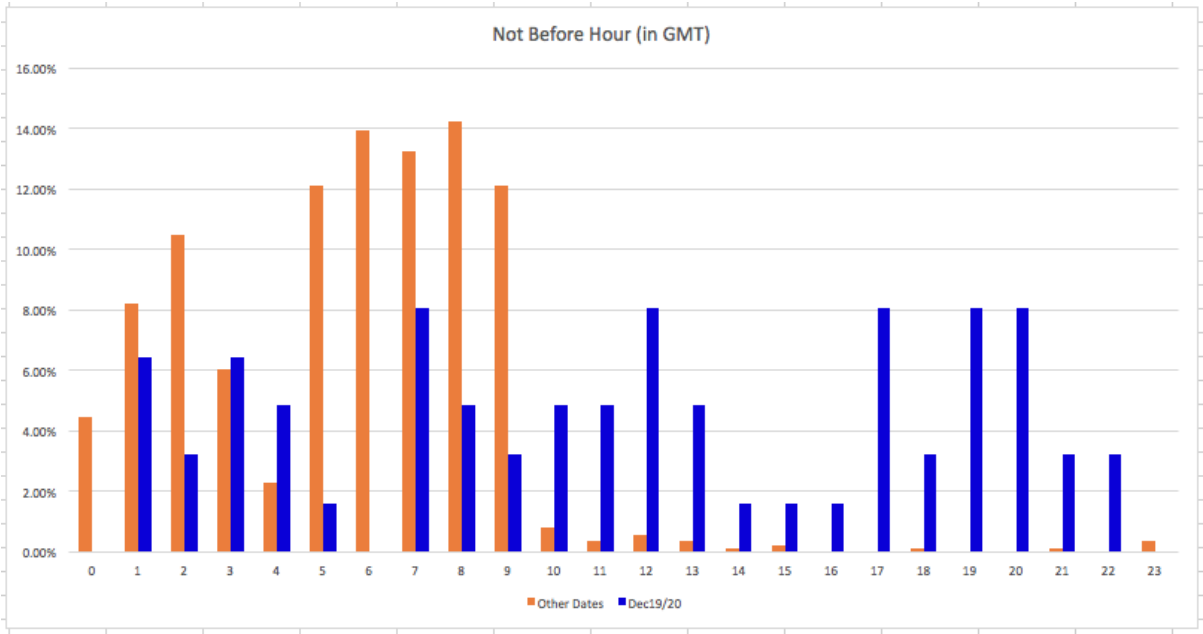


The green bars are Type X issuances, and the orange and blue bars are Type Y issuances. For Type Y, the orange colour represents issuances on a working day in China, and the blue colour represents issuances on a non-working day (these are normally Saturday and Sunday, but there are occasional exceptions).

First, you can see that Type X is issued more often than Type Y - the peaks are much higher. But also, with one big exception, Type Y issuances almost always occur on working days in China. This suggests that the process for issuing Type Y certificates is only triggered by direct WoSign employee action - it is not used for automated issuance.

The one big exception, the long blue bar, is the 20th of December 2015, which was a Sunday. There are 62 WoSign certificates whose notBefore dates are at some point on that Sunday, China time. These are the only ones on a Sunday - the other small number of "non-working-day" Type Y issuances are all on Saturdays. For want of a better name, we will call these 62 certificates "Macau certificates".[1]

Additional evidence that the Macau certificates are unusual can be seen by graphing the time portion of all Type Y issuances, in two buckets:



For all other Type Y issuances (orange), the notBefore time is almost always during the working day, China time (UTC +0800) - you can even detect the presence of a lunch break. This is further proof that these certificates are manually issued. By contrast, for the Macau certificates (blue), the times are distributed, perhaps randomly, throughout the entire 24 hour period.

[1] 20th December is "Macau Special Administrative Region Establishment Day" in China, the day Macau was transferred from Portugal to China in 1999.

We think it is highly unlikely that WoSign employees decided to go to work on that particular Sunday for a marathon 24-hour period and approve an unprecedented number of Type Y certificate requests. We think it is more plausible that for those certificates, the notBefore date does not reflect the actual date of certificate creation, and that these certificates were created in 2016 (or, for a handful, on the last day of 2015) and back-dated.

There is actual cryptographic evidence of back-dating in six Macau certificates, which have embedded Certificate Transparency SCTs from either very late December 2015 or January 2016, up to a month after the notBefore date in the certificate (20th December 2015). Certificate Transparency is a system invented by Google which, among other things, issues accurate timestamps, called SCTs, which can be embedded in certificates as part of the issuance process, thereby helping to determine when they were created. Here are links to those six: yffsc.com, congfubao.com, my.xbniao.com, passport.huayingjuhe.com, puxbao.com, modai.cc. These six are all EV certificates and so needed embedded SCTs in order to produce the EV UI in Google Chrome.

The difference between the notBefore date and the embedded SCT date for these six certificates ranges from 10 days to 28 days. By contrast, over its entire lifetime of operations WoSign has issued 898 EV certificates with embedded SCTs and there are no others with a difference of more than 51 hours. Most have a difference of less than 3 hours; the other outliers have notBefore dates on 27th July 2016, when (according to WoSign) there was a connection problem between their infrastructure and the Google CT servers. In other words, it is normal practice in WoSign EV issuance for SCT dates and notBefore dates to differ by around 3 hours - but for the six EV Macau certificates, the difference is no less than 10 days.

Many of the rest of the Macau certificates, which do not have an embedded SCT to show when they were issued, have “matching” SHA-256 versions issued at some point in 2016 for the same domains. This hints at the possibility (and it’s only a possibility) that the two certificates were actually issued at the same time, and the date in the SHA-256 version is the correct issue date for both. If this is true, it shows misissuance continued until at least June 2016 (*.zlbaba.com SHA-1, SHA-256).

Additional circumstantial evidence that WoSign’s certificate issuance machinery had a notBefore of 20th December 2015 hard-coded somewhere for SHA-1 issuance is found in the events of Issue V, where in July 2016 a researcher tinkered with the StartEncrypt API published by StartCom and managed, to his surprise, to get it to produce two SHA-1 WoSign certs back-dated to this date. (These two are included in the figure of 62 given above, so the number intentionally issued by WoSign is 60.)

All of this demonstrates that the “Macau certificates” are notable and unusual in a number of ways.

WoSign responded to this issue, denoted Issue S, in their final report. They concede that the six EV certificates (those for which cryptographic evidence is available) were mis-issued. WoSign says that this discrepancy is due to delays between application and issuance, combined with a bug in their systems when the system tried to replace the certs with

SHA-256 ones partway through the process. They also concede that the two certificates from Issue V were mis-issued. They assert that all of the remaining Macau certificates were validly issued in 2015, and the “matching” SHA-256 ones issued in 2016 were due to the customer returning and asking for a new cert some months later.

WoSign’s Ownership of StartCom

As documented in Mozilla’s investigation and as confirmed by a Hebrew-speaking lawyer who has examined the documents for us, as of November 1st 2015, WoSign took 100% ownership of the Israel-based CA “StartCom”, through intermediary companies in the UK and Hong Kong. Issue R in the original list of issues covers this. While purchasing another CA is by no means illegal, Mozilla’s program requirements say that a change of CA ownership must be disclosed. In this case, that was not done - and in fact, the change was directly denied a few months after it happened. More recently, even after the evidence of total control was public, WoSign referred to their interest in StartCom in a press release as “an equity investment”, and maintain that the two businesses continue to be separate even today. They say “the original system ... of StartCom remains unchanged”.

However, there is technical evidence that around a month and a half after the acquisition, StartCom issuances switched to using WoSign’s infrastructure - either the same instance of it, or their own instance.

Since as far back as 2013, WoSign certificates have contained 128-bit serial numbers. However, these numbers have an interesting quirk. The top 4 bits of the number are currently always between 0x1 and 0x6 - never 0x0 or 0x7 or above. (Historically, 0x0 and 0x7 appeared between January and November 2014 and 0x00, 0x7-0x9 appeared in April 2015, but none of these values have appeared recently. 0xA-0xF have never appeared.)

Mozilla asked WoSign how they generated their serial numbers, and was told that they used the Java package java.security.SecureRandom. They supplied the following code snippet:

```
        public static String createSerialNumber() {
                String serialString = "";

                while(true) {
                        BigInteger serialNumber = new BigInteger(128, new SecureRandom());
                        serialString = serialNumber.toString(16);
                        if (serialString.length() == 32) {
                                break;
                        }
                }
                logger.debug(" Generating 32 bits certificate sequence number: "+
serialString +
                                "  len=" + serialString.length());
                return serialString.toUpperCase();
        }
```

However, as can be seen from this simple test harness, this code snippet does not produce serial numbers matching WoSign’s idiosyncratic pattern. The requirement for a full-length number explains the lack of 0x0, but not the other missing digits. Mozilla has been unable to

determine the significance of this discrepancy between WoSign's provided code and reality. However, this quirk suggests that when such a serial number appears in a certificate, it was issued by WoSign-authored infrastructure.

On 18th December 2015, StartCom's website StartSSL.com closed down operations for a system upgrade, reopening on 22nd December 2015. As part of this transition, which took place a month and a half after they were acquired by WoSign, StartCom issuances switched to using 128-bit serial numbers, which have the same numerical quirk as the serial numbers in certificates explicitly issued by WoSign. Also, at the same time, StartCom started issuing from a new set of intermediate certificates whose naming conventions matched those used by WoSign. StartCom's intermediate list shows the old intermediates (CN contains "Intermediate") at the top, and the new ones (CN contains "DV", "IV", "OV" or "EV") lower down. Also, if you look at the day of issuance of their certificates as a whole, before this date StartCom had reduced issuance on Friday and Saturday (the weekend in Israel) and afterwards they had reduced issuance on Saturday and Sunday (the weekend in other parts of the world, e.g. US, China and the UK).

Lastly, whilst otherwise being closed, at around 3-4.30pm UTC on 18th December 2015 StartCom issued 3 EV certificates (1, 2, 3) using the new serial number format. One was from the old intermediates and two were from the new intermediates. The O field of these certificates says "WoSign CA Limited", and the domain name was www.wgh.cn. This site identifies itself as "Richard Wang Personal Blog". One might infer that these were testing certificates issued during the transition - they seem not to have been intended for use because that site today still uses an IV cert issued from WoSign's hierarchy back in April 2015. Given that it was late in the night in China, and given the requirements of the EV process to validate companies (EV does not have a process for validating individuals), it seems that the most likely way these could have been issued with anything like the right amount of checks and obtained permissions would be if Richard Wang, CEO of WoSign and owner of the site in question, was present at StartCom's offices at the time.

We believe that, taken together, all this shows that StartCom's certificates are now being issued using either WoSign's existing infrastructure or a clone of it, and that WoSign's operational control of StartCom began straight after the November 1st 2015 sale date. This evidence should be compared against WoSign's recent assertion that "Even now, it still independent in the system, in the validation team and management team, we share the CRL/OCSP distribution resource only."

SHA-1 Exceptions Process

Since the banning of SHA-1 issuance on January 1st 2016, it has emerged that companies in certain sectors have been unable to move their operations to SHA-256 in time for the deadline, and did not have enough forethought to stockpile the necessary certificates so they could have an extra year to move. This became clear in February of 2016, where a payment processor called WorldPay applied to the CAB Forum for an exception so they could acquire 8 SHA-1 certificates to keep SSL working for their legacy payment terminals. Their CA was unable to help them because of the ban in the CAB Forum Baseline Requirements, and to

issue in violation of the ban would lead to a “qualified” (not clean) audit, which might lead to browsers no longer accepting their audit as valid to keep them trusted.

This issue was discussed at length in the CAB Forum face-to-face meeting from 16th-18th February 2016 in Scottsdale, Arizona (where Richard Wang of WoSign was present). Mozilla then had a public discussion about it in our policy forum starting on 23rd of February. In the end, the browsers reluctantly agreed to let Symantec issue these certificates for Worldpay - or rather, they agreed to accept that Symantec’s next audit would be qualified in this way.

Even at this point, in February 2016, it was (or should have been) clear to all CAs, including WoSign, that issuing SHA-1 certificates in violation of the ban was a Very Big Deal, and that permission had to be sought from the browsers in order for the CA not to face difficulty.

On 3rd of June, Andrew Whalley of Google posted a draft document proposing a more formal process for acquiring exceptions. This document was discussed during June, agreed by the browser vendors, and used for the application of another payment processor, TSYS, in July and August. So this was very much a live issue in early June.

Tyro

So what’s the connection between all of these different pieces of information?

Tyro is an Australian payments processor, who have historically been customers of GeoTrust (owned by Symantec) and Comodo. You will recall from earlier that the payment processing industry is one of those industries which is having particular difficulty with the SHA-1 transition.

If we look in crt.sh, we can see a number of certificates issued for the DNS name “*.tyro.com” by different CAs. These are wildcard certs, able to be used by any number of hosts inside the tyro.com domain. Ordering them by age, we can construct a picture which looks like this:

Feb 3rd 2010	GeoTrust issues a SHA-1 certificate for *.tyro.com from their Equifax root, valid until May 6th 2013.
Apr 6th 2013	A month before their old cert expires, GeoTrust issues a replacement SHA-1 certificate for *.tyro.com from a GeoTrust root, valid until June 7th 2016. A simple roll-over replacement.
Jan 1st 2016	SHA-1 issuance ban comes into effect.
May 24th 2016	A month before their old cert expires, GeoTrust issues a **SHA-256** certificate for *.tyro.com from a GeoTrust root, valid until June 23rd 2019.

But the strong evidence is that this SHA-256 certificate did not meet Tyro's needs. We can see a **SHA-1** certificate for *.tyro.com which was logged in CT on June 8th 2016, a day after their previous SHA-1 certificate expired. This certificate is not issued by GeoTrust (who still provide the cert for their main website) or Comodo, tyro.com's usual providers, but by StartCom. And the notBefore date is that magic date of 20th December, 2015 - a date on which, as noted above, StartSSL.com was closed for upgrading, and on which we have seen many Macau certificates issued by WoSign, which we believe are back-dated.

This certificate, and a very similar one for *.test.tyro.com, are together unusual in StartCom's corpus of issued certificates. We can see this by again thinking about the concept of certificate template "fingerprints". Starting on 29th December 2014, StartCom used 56-bit serial numbers, with the top 24 bits being a sequential counter that increased periodically and the remaining 32 bits being random. The time portions of notBefore and notAfter were also randomized. (Together, the randomization of the times and of the end of the serial number meet a Microsoft requirement for 64 bits of entropy in certificates.) As noted above, a year later, starting on 18th December 2015, they switched to using 128-bit WoSign-style serial numbers and with the times of the notBefore and notAfter matching to the second. Additionally, at the same time, Startcom switches to a new set of issuing CAs which include the terms "DV", "OV" and "EV" in the common names.

However, these two tyro.com certificates are outliers. They have the new 128-bit WoSign-style serial numbers but are issued from the older intermediates. They also do not have the time-match between notBefore and notAfter. Instead the notAfter field contains 2016-12-29T16:00:00Z for each. They are the only certificates StartCom has ever issued (that we know of) which mix styles in this exact way, making them very notable.

Consider two possible ways these certificates could have come to exist:

Possibility 1: In December 2015, in the period leading up to Christmas when they and most companies in their industry are in a change freeze, Tyro decided to change CAs for one part of their infrastructure from the market-leading CAs they had traditionally used to a smaller CA they had never previously used. They decided to renew their main and test wildcard certificates six months in advance of needing them rather than the usual month, and their new CA hand-issued them, using a unique set of identifying marks, during a period of major change and downtime, when they were otherwise closed to the public - despite the fact that the request was not urgent. Then, tyro.com didn't deploy these certificates until very near the moment their existing certs ran out, contrary to their normal practice of allowing a month's overlap. These certificates were then spotted and logged in CT by someone other than StartCom.

Possibility 2: In May 2016, Tyro came to renew their certificates, found they couldn't get SHA-1 certificates from GeoTrust without going through the browser exception process that Worldpay went through, and (desperate and very short of time) went knocking on StartCom's door. StartCom used the WoSign back-dating system to issue them a pair of SHA-1 certificates which were back-dated. These certificates were either logged in CT by StartCom themselves (they committed to logging all their certs to CT from 23rd March 2016, and may

have left this feature turned on) or were logged by e.g. Google's crawler as soon as Tyro started using them.

We believe that the second scenario is the more plausible one, and that StartCom agreed to issue a SHA-1 cert for Tyro without going through the public exception process, and they backdated it to avoid being seen to violate the SHA-1 ban, getting a qualified audit and possibly facing browser sanction.

At the time this document was written, the SHA-1 certificate in question was still in use on https://iclient.tyro.com/.

Conclusions

From the above observations about the Tyro certificates, we believe we can draw the following conclusions:

- StartCom are using WoSign's infrastructure (the same or a clone);
- Certificates on this infrastructure with a notBefore of 2015-12-20 (China time) are indeed back-dated - this further confirms our suspicions about the Macau certificates we saw issued by WoSign; and
- StartCom's hierarchy has been directed by management to mis-issue "WoSign-style".

This last point is important; the practices at WoSign are now being seen at StartCom. Therefore, we conclude that all of ownership, infrastructure and control are sufficiently common between the two companies that it would therefore be reasonable for any action Mozilla chooses to take against WoSign to also be taken against StartCom and vice versa.

We can then add those conclusions to the wider issues regarding WoSign noted in the original list:

- Back-dating SHA-1 certs was a relatively common practice at WoSign, and they have consistently denied doing so. (Issue S, and the evidence given above)
- WoSign built a system where applicants could add extra arbitrary domains to their certificates before issuance. Even when mis-issuances happened they did not determine the root cause, and eliminated the flaw only in an unrelated system upgrade. (Issue N)
- WoSign has an "issue first, validate later" process where it is acceptable to detect mis-issued certificates during validation the next working day, and revoke them at that point. (Issue N)
- WoSign's team do not seem to think a misissuance is worth investigating further than simply revoking the certificate. (Issue N)

- WoSign's approach to their CPS is backwards - instead of following it and changing it first when necessary, they change their practice and then update the documentation when reminded. (Issue J)

- If the experience with their website ownership validation mechanism is anything to go by, It seems doubtful that WoSign keep appropriately detailed and unalterable logs of their issuances. (Issue L)

- The level of understanding of the certificate system by their engineers, and the level of quality control and testing exercised over changes to their systems, leaves a great deal to be desired. It does not seem they have the appropriate cultural practices to develop secure and robust software. (Issue V, Issue L)

- It does not appear that WoSign learns from the experience of other CAs, e.g. Symantec's test certificate issue, or the SHA-1 exceptions process. (Issue P, Issue S)

- For reasons which still remain unclear, WoSign appeared determined to hide the fact that they had purchased StartCom, actively misleading Mozilla and the public about the situation. (Issue R)

- WoSign's auditors, Ernst & Young (Hong Kong), have failed to detect multiple issues they should have detected. (Issue J, Issue X)

Proposed Action

The above information, along with the list of WoSign issues, makes up the current state of our investigation. We are open to accepting further evidence, including whether there are any significant errors in the above which would affect the narrative, whether there have been any other problems with WoSign or StartCom's certificate issuance, and also any data relevant to our current view that it is appropriate to treat these two CAs together. However, we also feel it is necessary at this point to take some steps towards a conclusion.

In our policy newsgroup, WoSign proposed that an appropriate response to this list of issues (or the subset of them known at the time they made their proposal, which did not include any of the SHA-1 backdating information) would be to constrain them to issuing in the China market only in future. However, we don't feel that Mozilla's users in China have lower requirements for CA trustworthiness than Mozilla's users elsewhere.

Taking into account all the issues listed above, Mozilla's CA team has lost confidence in the ability of WoSign/StartCom to faithfully and competently discharge the functions of a CA. Therefore we propose that, starting on a date to be determined in the near future, Mozilla products will no longer trust newly-issued certificates issued by either of these two CA brands.

We plan to distrust only newly-issued certificates to try and reduce the impact on web users, as both of these CA brands have substantial outstanding certificate corpuses. Our proposal is that we determine “newly issued” by examining the notBefore date in the certificates. It is true that this date is chosen by the CA and therefore WoSign/StartCom could back-date certificates to get around this restriction. And there is, as we have explained, evidence that they have done this in the past. However, many eyes are on the Web PKI and if such additional back-dating is discovered (by any means), Mozilla will immediately and permanently revoke trust in all WoSign and StartCom roots.

This distrust would remain for a minimum of 1 year. After that time, WoSign/StartCom may be readmitted to the Mozilla trust program, under the following conditions:

- A Point-In-Time Readiness Audit (PITRA) from a Mozilla-agreed WebTrust auditor;
- A full code security audit of their issuing infrastructure from a Mozilla-chosen security auditor;
- 100% embedded CT for all issued certificates, logged to at least one Google and one non-Google log not controlled by WoSign/StartCom;
- Going through the normal Mozilla inclusion process.

Only certificates issued after the above audits were complete would be trusted. In addition, Mozilla will:

- add all of the Macau certificates, plus the two Tyro ones, to OneCRL immediately; and
- no longer accept audits carried out by Ernst & Young (Hong Kong).

Open questions include:

- How much lead time does the ecosystem need before we take this action?
- Should StartCom/WoSign be permitted to re-apply using the same roots, or would they need new roots?

The above steps are a proposal for discussion, as is our practice, and we invite public comment on them from interested parties, including those who currently purchase or rely on WoSign/StartCom certificates. If the timeline would be a problem for some large users of these certificates, we might consider building a list of domains which are exempt from the dis-trusting for a further period. The final decision on action to take remains with the CA Certificates Module owner.

Mozilla believes that continued public trust in the correct working of the CA certificate system is vital to the health of the Internet, and we will not hesitate to take steps such as those outlined above to maintain that public trust. We believe that the behaviour documented here would be unacceptable in any CA, whatever their nationality, business model or position in the market. While other browser vendors and root store operators will need to make their own decisions, we have laid out the information in this document so that they will understand the basis on which we have made our decision and can make their own decisions

accordingly. We also hope the public can see that when there are allegations of CA wrongdoing, Mozilla is committed to a fair, transparent and thorough investigation of the facts of each case.

Gervase Markham (CA Certificates Module peer and lead investigator)
Ryan Sleevi (CA Certificates Module peer)
Richard Barnes (CA Certificates Module peer)
Kathleen Wilson (CA Certificates Module owner)

Acknowledgements

Mozilla would like to thank:

- Ben Laurie and his team at Google for creating Certificate Transparency
- Rob Stradling of Comodo for creating crt.sh and for other help
- Thijs Alkemade of Computest for his research on Issue S
- Paul Pearce for his research on Issue X
- Other helpful community members who choose to remain anonymous

Appendix A: WoSign and StartCom Roots

The following WoSign and StartCom roots are currently in the Mozilla root program. We also have a list of known cross-signatures.

WoSign

- CA 沃通根证书
- Certification Authority of WoSign
- Certification Authority of WoSign G2
- CA WoSign ECC Root

StartCom

- StartCom Certification Authority
- StartCom Certification Authority G2