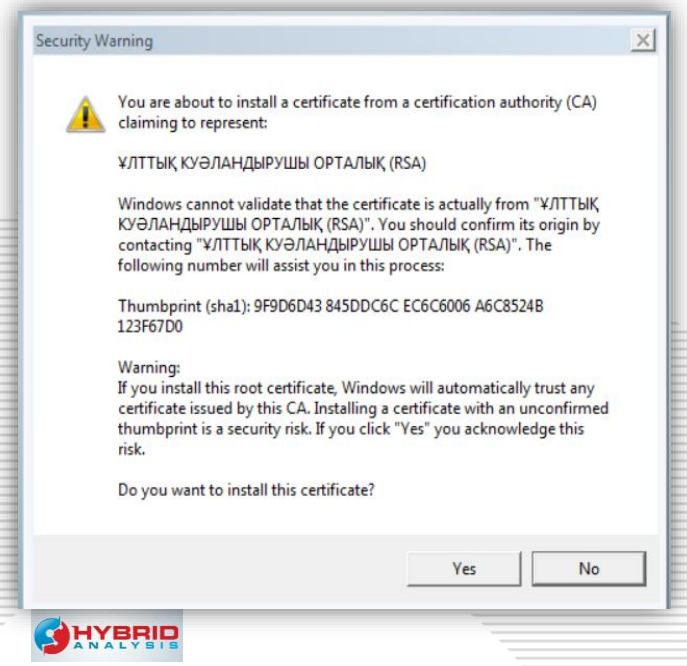
Meet the 'Creatures' Feature

This series covers the more exotic incidents observed at our client sites and how **SMARTMonitoring was able to Detect these creatures**.



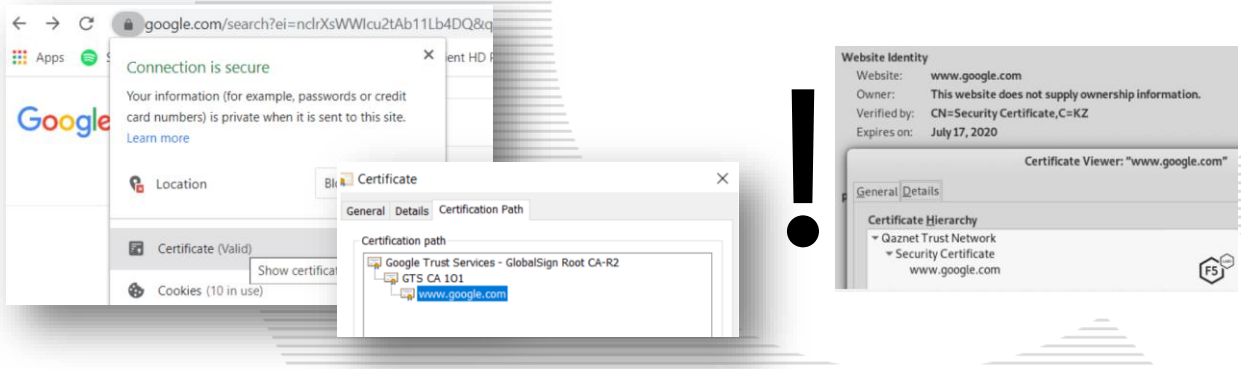
The beast: *certutil*

Not all incidents involve malware. In one instance, we detected a situation where a legitimate program had the potential to cause security problems down the line.

In some cases, programs attempt to load additional **root certificates** into the store.

By forcing the user to trust all certificates signed by this new root the programmers can insert themselves between the user and their destination web site.

For example, if a user wants to check their gmail account, the little lock icon will be locked and the website should say that it's from Google. In this case however the certificate showed the intercepted certificate which could be secretly operated by the "man-in-the- middle" (mitm) to spy on the users.



How did we catch this beast using CYDEF SMARTMonitor?

A new program, **KnpPluginSvc**, was installed which launched **certutil**. This was flagged as a deviation from the normal baseline right away because **SMARTMonitor** detects anamalous activities.

CYDEF Cyber Security Experts reviewed the logs for that observed certutil activity and could see from the command line the addition of a **new certificate** to the store.

The activity being linked with the installation of the program was very unusual. Further, the item was signed by Apache, making this software a bizarre cobbled together instance of open source software.

After more research, we confirmed that the source of the software was from the Kazakh govenrment online services website.

Regardless of whether the software was legitimate, CYDEF SMARTMonitor Analysts were immediately concerned by the installation of the certificate and the potential for a **mitm attack**.

After research and discussions with regional experts, CYDEF was further able to determine that this was likely part of a long-term campaign by the Kazakh government to perform mass surveillance on their citizens.[1]

Why AV alone couldn't help

This particular incident is not malware. It's a legitimate software introducing a significant cyber risk to the organization which pushes it out of scope for most AV products.

Need more info? Let's talk

[1] https://www.f5.com/labs/articles/threat-intelligence/kazakhstan-attempts-to-mitm-itscitizens