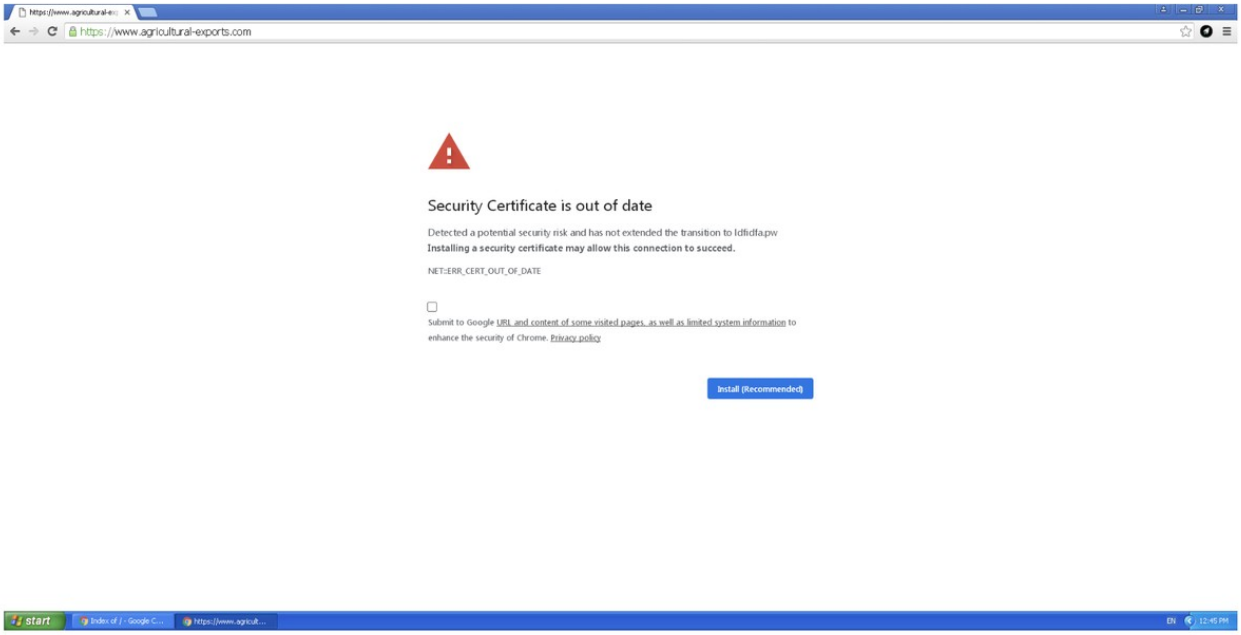
DO NOT CLICK OR ENGAGE IF YOU COME ACROSS THIS (assume it is a bad site and close your browser).



https://www.zdnet.com/article/backdoor-malware-is-being-spread-through-fake-security-certificate-alerts/

Backdoor malware is being spread through fake security certificate alerts

Victims of this new technique are invited to install a malicious "security certificate update" when they visit compromised websites.

By Charlie Osborne for Zero Day | March 5, 2020 -- 11:42 GMT (03:42 PST) | Topic: Security

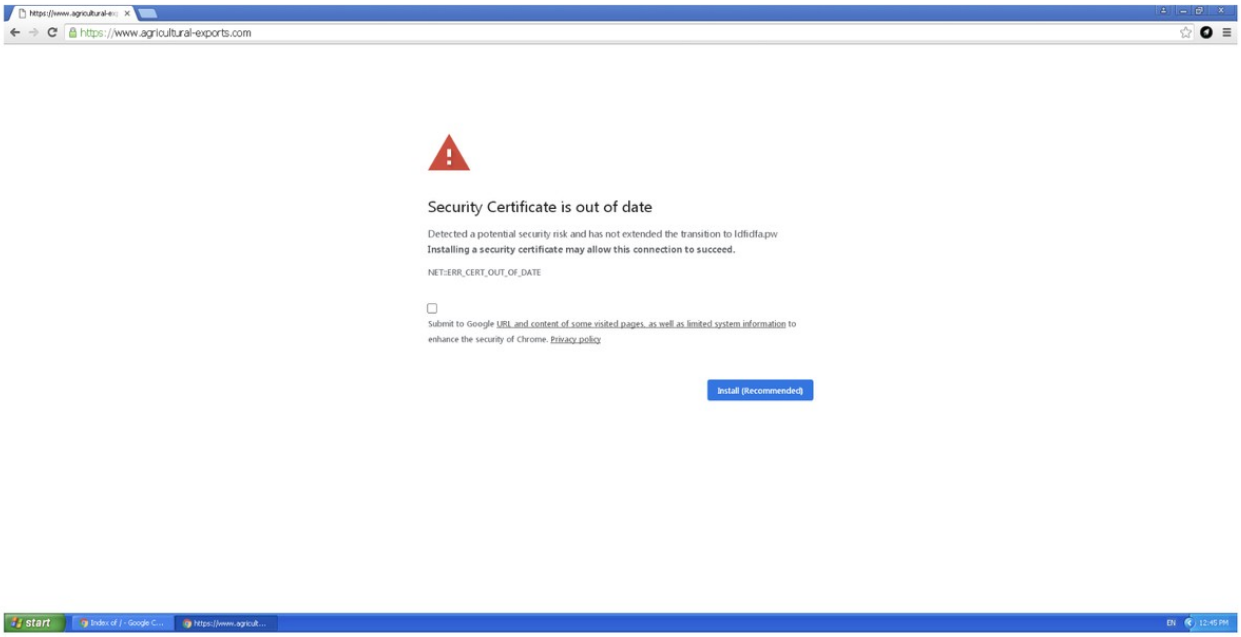
Backdoor and Trojan malware variants are being distributed through a new phishing technique that attempts to lure victims into accepting an "update" to website security certificates.

Certificate Authorities (CAs) distribute SSL/TLS security certificates for improved security online by providing encryption for communication channels between a browser and server

-- especially important for domains providing e-commerce services -- as well as identity validation, which is intended to instill trust in a domain.

While there are cases of certificate misuse, fraud, and even cybercriminals posing as executives to obtain security certificates to sign off fraudulent domains or malware payloads, a new phishing approach is now abusing the certificate trust mechanism. On Thursday, cybersecurity researchers from Kaspersky reported that the new technique has been spotted on a variety of websites, ranging from a zoo to an e-commerce store selling vehicle parts. The earliest infections date back to January 16, 2020.

Visitors to a domain compromised by the campaign are met with the following screen:



The alert claims the website's security certificate is out of date, but rather than this being the domain owner's problem, victims are urged to install a "security certificate update" to proceed.

The message is contained within an iframe and content is loaded via a jquery.js script from a third-party command-and-control (C2) server, while the URL bar still keeps the legitimate domain's address, adding to the ploy's legitimacy.

"The jquery.js script overlays an iframe that is exactly the same size as the page," the researchers say. "As a result, instead of the original page, the user sees a seemingly genuine banner urgently prompting to install a certificate update."

If the victim chooses to click the update button, the download of a file, Certificate_Update_v02.2020.exe, is initiated.

When unpacked and installed, the executable will deliver one of two malware variants to the victim, either Mokes or Buerak.

Mokes is a macOS/Windows backdoor, deemed "sophisticated" by the cybersecurity firm, which is able to execute code, take screenshots, steal PC information including files, audio, and video captures; install a backdoor for persistence, and use AES-256 encryption to disguise its activities.

In comparison, Buerak is a Windows-based Trojan able to execute code, tamper with running processes, steal content, maintain persistence through registry keys, and detect various analysis and sandboxing techniques.

In related news this week, CA Let's Encrypt announced plans to revoke over three million certificates due to a bug in backend code that caused verification systems to ignore some CAA field checks. The programming error has now been fixed. Impacted domain owners will have to request new certificates.