Mongolian certificate authority hacked eight times, compromised with malware

therecord.media/mongolian-certificate-authority-hacked-eight-times-compromised-with-malware/

July 1, 2021

Image: Altai Baatarkhuu

Hackers have breached a server belonging to MonPass, one of Mongolia’s largest certificate authorities (CA), and have backdoored the company’s official client with a Cobalt Strike-based backdoor.

The backdoor was active inside the company’s official certificate installer app **between February 8 and March 3 this year**, security firm Avast said in a report today.

Incident has the hallmarks of a cyber-espionage campaign

The security breach came to light in late March when Avast discovered the backdoored installer and backdoor on one of its customers’ systems.

From March to June, the security firm has been working with the CERT Mongolia team and MonPass to investigate the intrusion, with MonPass providing a cloned image of the compromised server to Avast for further investigations.

> Our analysis beginning in April 2021 indicates that a public web server hosted by MonPass was breached potentially eight separate times: we found eight different webshells and backdoors on this server.
>
> *Avast research team of Luigino Camastra, Igor Morgenstern, and Jan Vojtěšek*

But despite having access to the compromised server, the Avast team said it was not able to attribute the intrusion “with an appropriate level of confidence” to any specific threat actor.

“However it’s clear that the attackers clearly intended to spread malware to users in Mongolia by compromising a trustworthy source, which in this case is a CA in Mongolia,” researchers added.

Signs point to a Chinese threat actor

But while Avast was not able to link the intrusion to a specific threat actor, previous cyber-espionage activity recorded in Mongolia and other Asian countries point the finger towards Beijing.

For example, in December 2020, security firm ESET discovered that a Chinese hacking group compromised a software company that supplied software to multiple Mongolian government agencies.

In the same month, Avast also disclosed details about a Chinese cyber-espionage campaign that targeted government agencies using spear-phishing emails, during which the threat actor tried to install backdoors and keyloggers on employee workstations.

In an incident eerily similar to the MonPass breach, a Chinese cyber-espionage group also breached and inserted malware inside the certificate installation app provided by the Vietnam Government Certification Authority (VGCA), a Vietnamese CA that provided digital certificates to local companies and government agencies.

These past campaigns and the fact that the threat actor removed the backdoor on its own, most likely after infecting the desired target, suggest this was a highly targeted attack against a high-profile Mongolian entity rather than a run-of-the-mill financially-themed malware distribution scheme.

A MonPass spokesperson was not available for comment on the Avast report, but Avast said the company appears to have cleaned up its server and notified customers who downloaded its backdoored client app earlier this year.

Tags

- APT
- certificate authority
- China

- Mongolia
- MonPass
- nation-state

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.