DHS: Multiple US gov domains hit in serious DNS hijacking wave

reader comments

96 with 63 posters participating

Share this story

The Department of Homeland Security has issued an emergency directive ordering administrators of most federal agencies to protect their Internet domains against a rash of attacks that have hit executive branch websites and email servers in recent weeks.

The DHS' Cybersecurity and Infrastructure Security Agency (CISA) issued the directive on Tuesday, 12 days after security firm FireEye warned of an unprecedented wave of ongoing attacks that altered the domain name system records belonging to telecoms, ISPs, and government agencies. DNS servers act as directories that allow one computer to find other computers on the Internet. By tampering with these records, attackers can potentially intercept passwords, emails, and other sensitive communications.

"CISA is aware of multiple executive branch agency domains that were impacted by the tampering campaign and has notified the agencies that maintain them," CISA Director Christopher C. Krebs wrote in Wednesday's emergency directive. He continued:

> *Using the following techniques, attackers have redirected and intercepted web and mail traffic, and could do so for other*

networked services:

1. The attacker begins by compromising user credentials, or obtaining them through alternate means, of an account that can make changes to DNS records.

2. Next, the attacker alters DNS records, like Address (A), Mail Exchanger (MX), or Name Server (NS) records, replacing the legitimate address of a service with an address the attacker controls. This enables them to direct user traffic to their own infrastructure for manipulation or inspection before passing it on to the legitimate service, should they choose. This creates a risk that persists beyond the period of traffic redirection.

3. Because the attacker can set DNS record values, they can also obtain valid encryption certificates for an organization's domain names. This allows the redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.

To address the significant and imminent risks to agency information and information systems presented by this activity, this emergency directive requires the following near-term actions to mitigate risks from undiscovered tampering, enable agencies to prevent illegitimate DNS activity for their domains, and detect unauthorized certificates.

Krebs went on to direct administrators to take the following steps in the next 10 business days:

- audit public DNS records on all authoritative and secondary DNS servers to verify they resolve to the intended location. If any do not, report them to CISA.
- update the passwords for all accounts on systems

that can make changes to the agency’s DNS records.
- implement multi-factor authentication for all accounts on systems that can make changes to the agency’s DNS records. If MFA can’t be enabled within 10 business days, admins are to provide CISA with the names of those systems, the reasons why, and an estimate when it could be enabled.

The CISA directive made no mention of the temporary government shutdown. As Ars reported on Thursday, that situation has impacted idling US government IT workers, many of whom are responsible for securing networks. (As this post was going live, it was widely reported President Trump agreed to a deal that would reopen the government through February 15, at least.) Krebs also didn’t identify the executive branch agency domains that were hit by the hijacking attacks.

The attacks are serious because the attackers are able to obtain browser-trusted TLS certificates for the hijacked domains. That allows the interception to occur with no obvious signs that anything is amiss. For more on how the attacks work, see Ars’ previously mentioned coverage.

https://arstechnica.com/?p=1446729