TLP: WHITE
MS-ISAC CYBER ALERT

TO: **All MS-ISAC Members and Intel Partners**

DATE ISSUED: **January 24, 2019**

SUBJECT: **DHS Issues Emergency Directive on DNS Infrastructure Tampering**

On January 22, 2019, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released Emergency Directive 19-01 (ED19-01): *Mitigate DNS Infrastructure Tampering*. Per Jeanette Manfra, Assistant Director, Cybersecurity Division, CISA, this directive was issued to address significant risks to federal information systems based on observed activity related to the Domain Name System (DNS) infrastructure tampering campaign. Emergency Directives are a type of DHS cybersecurity directive – like BODs – intended to drive specific, immediate action to mitigate urgent issues and imminent risks. ED19-01 requires all federal agencies to mitigate risks from undiscovered tampering, enable agencies to prevent illegitimate DNS activity for their domains, and detect unauthorized certificates.

According to ED19-01, Address (A), Name Server (NS) and Mail Exchanger (MX) records for a select number of websites were tampered with by malicious cyber actors. *A Records* point a domain to a specific Internet Protocol (IP) address, *NS Records* specify the servers that are providing DNS records for a domain, and *MX Records* specify the mail server responsible for accepting messages on behalf of the domain.

Within 10 business days (February 5, 2019), ED19-01 requires all federal civilian agencies to take the following actions:

- Audit DNS Records
- Change DNS Account Passwords
- Add Multi-Factor Authentication (MFA) on DNS Accounts
- Monitor Certificate Transparency Logs to ensure authenticity of certificate requests

RECOMMENDATIONS:
The MS-ISAC is currently working with DHS to determine any potential concerns for SLTT governments and, as appropriate, will conduct notifications on the actionable results. The MS-ISAC recommends members follow the federal guidance in the ED19-01 and:

- Implement multifactor authentication on domain registrar accounts, or on other systems used to modify DNS records.
- Verify that DNS infrastructure (second-level domains, sub-domains, and related resource records) points to the correct Internet Protocol addresses or hostnames.
- Search for encryption certificates related to the identified domains and revoke any fraudulently requested certificates.

SLTT governments are encouraged to report suspicious findings to the MS-ISAC for further analysis and assistance.

REFERENCES:

DHS Statement on ED19-01:
https://cyber.dhs.gov/ed/19-01/

US-CERT:
https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

FireEye:
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

Cisco Talos:
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722