The FDIC's Actions to Mitigate the Risk of Domain Name System Infrastructure Tampering

September 2019 **AUD-19-006**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

September 24, 2019

Subject ***The FDIC's Actions to Mitigate the Risk of Domain Name System Infrastructure Tampering***

On January 22, 2019, the U.S. Department of Homeland Security (DHS) issued Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*, (Emergency Directive 19-01 or Directive) to all Federal Executive Branch Departments and Agencies (Agencies).[1] DHS issued Emergency Directive 19-01 following a series of computer security incidents referred to as "Domain Name System (DNS) infrastructure tampering" that targeted multiple Agencies. DNS infrastructure tampering occurs when an attacker intercepts or redirects an organization's web or email traffic to a separate information technology (IT) infrastructure that the attacker controls. This allows the attacker to inspect and manipulate the traffic, thereby exposing the organization's sensitive information and allowing the attacker to disrupt critical IT operations or perpetrate other malicious activity. According to Emergency Directive 19-01, DNS infrastructure tampering presents a "significant and imminent" risk to Federal information and information systems.

Emergency Directive 19-01 required Agencies, including the FDIC, to take four specific actions to mitigate the risk of DNS infrastructure tampering. Agencies were to complete these actions within 10 business days of the issuance of the Directive. We conducted an audit, the objective of which was to determine whether the FDIC took responsive actions to address the requirements of Emergency Directive 19-01 to mitigate DNS infrastructure tampering. Details regarding our audit objective, scope, and methodology are contained in the Appendix of this report.

BACKGROUND

DNS is a critical IT service that translates website names (domain names), such as www.fdic.gov, into Internet Protocol (IP) addresses, such as 167.176.6.69. Every IT device connected to the Internet, including servers, routers, and personal computers, has a unique IP address. IP addresses function much like postal addresses that allow IT devices to communicate with each other. DNS allows a user to access a

[1] DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering* (January 2019). Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of DHS to issue an Emergency Directive to the head of an Agency in response to "a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency." These Emergency Directives do not apply to national security systems or to systems operated by the U.S. Department of Defense or the Intelligence Community. 44 U.S.C. § 3553 (d), (e), and (h). The Federal Deposit Insurance Corporation's (FDIC) Legal Division has determined that Emergency Directive 19-01 is legally applicable to the FDIC.

website through the use of an easily recognizable domain name, rather than through the use of an IP address.

According to Emergency Directive 19-01, the attackers that perpetrated the DNS infrastructure tampering used the following techniques to intercept and redirect the web and email traffic of Agencies:

- The attacker began by compromising a user's credentials (User ID and password), or obtaining them through alternate means, for system accounts that could make changes to the Agency's DNS records.[2]

- The attacker then accessed and altered the Agency's DNS records, replacing legitimate IP addresses with IP addresses that the attacker controlled. This enabled the attacker to redirect network traffic to their own IT infrastructure for inspection or manipulation before passing the traffic on to the legitimate IP address (should the attacker have chosen to do so).

- Using the compromised user credentials, the attacker obtained valid encryption certificates[3] and used them to decrypt the redirected traffic, exposing user-submitted data.

A successful attack on the FDIC's DNS infrastructure could allow an attacker to view sensitive FDIC email communications exchanged between employees and outside parties. Such an attack could also direct FDIC network users to a fake website when surfing the Internet, allowing the attacker to steal sensitive information, such as the user's passwords and personally identifiable information.

To mitigate the risks of DNS infrastructure tampering, Emergency Directive 19-01 required Agencies to take the following four actions within 10 business days of the issuance of the Directive (or February 5, 2019):

1. **Audit DNS Records.** Agencies must audit their public DNS[4] records on all authoritative and secondary DNS servers[5] for all .gov or other Agency-managed domains. The purpose of this action is to verify that the Agency's domain names

[2] A DNS record is a database record that maps a domain name to its IP address.
[3] According to the National Institute of Standards and Technology (NIST) Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure* (February 2001), an encryption certificate is a digital document containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes.
[4] DNS records may be public (accessible externally) or private (accessible only through an internal network). Emergency Directive 19-01 specifically refers to public DNS records.
[5] An authoritative DNS server is a server that creates and manages DNS records. A secondary DNS server often serves as a mirror for the authoritative server in order to provide effective distribution of network traffic or redundancy, should the authoritative server fail to operate.

resolve to their intended IP addresses. Agencies must report any identified exceptions to DHS's Cybersecurity and Infrastructure Security Agency (CISA).

2. **Change DNS Account Passwords.** Agencies must change the passwords for all accounts on systems that can make changes to DNS records. By changing the passwords, Agencies can deny an attacker's access to accounts that may have been compromised.

3. **Implement Multi-Factor Authentication.** Agencies must implement multi-factor authentication (MFA)[6] for all accounts on systems that can make changes to DNS records. According to NIST, MFA makes it more difficult for an attacker to gain unauthorized access to an information system than single factor authentication.[7] This is because the attacker must compromise two factors—not just one—to gain access. Agencies that cannot enable MFA for accounts or systems with access to DNS records must report detailed information about the exceptions to CISA.

4. **Monitor Certificate Transparency (CT) Logs.** A certificate is a digital document used to achieve security assurance in an electronic transaction. In the context of DNS, organizations use certificates to enable users to verify the authenticity of a domain with which they are attempting to communicate and establish a secure connection. A CT log is a listing of all certificates issued for an Agency's domains. Following the issuance of Emergency Directive 19-01, CISA began regular delivery of newly added certificates to CT logs for the FDIC's domains via the Cyber Hygiene service.[8] Agencies were directed to monitor these CT logs for certificates issued on their behalf that they did not request. If an Agency confirms that a certificate was not authorized, the Agency must report the certificate to the issuing certificate authority and to CISA.

Emergency Directive 19-01 also required Agencies to provide CISA with status and completion reports covering the four actions described above.

AUDIT RESULTS

The FDIC took responsive actions to address the requirements in Emergency Directive 19-01. The FDIC completed these actions within 10 business days, as

[6] MFA is a method of verifying the identity of an individual seeking access to an information system. MFA uses a combination of factors, such as passwords, Personal Identity Verification cards, or tokens, to verify an individual's identity.
[7] NIST Cybersecurity White Paper, *Best Practices for Privileged User PIV Authentication* (April 2016).
[8] CISA offers Agencies a free vulnerability scanning service called Cyber Hygiene. As part of the service, CISA conducts weekly scans of public-facing Agency systems to identify weak configurations and known vulnerabilities. CISA provides the scan results to Agencies to encourage the adoption of modern security best practices.

prescribed in the Directive. In addition, the FDIC provided CISA with timely status and completion reports. A summary of the FDIC's actions to address the requirements of Emergency Directive 19-01 follows.

Requirement	Actions Taken
1. Audit DNS Records	The FDIC identified and reviewed all public DNS records to ensure that domain names resolved to their intended IP address.
2. Change DNS Account Passwords	The FDIC changed the passwords for all accounts capable of making changes to DNS records. However, the FDIC inadvertently omitted one such account from its completion report submitted to CISA on February 5, 2019. Because the FDIC had changed the password for this account prior to submitting its completion report, we concluded that the FDIC complied with Emergency Directive 19-01.
3. Add Multi-Factor Authentication	The FDIC implemented MFA for all accounts capable of making changes to DNS records.
4. Monitor CT Logs	The FDIC began reviewing weekly CT logs provided by CISA for potential unauthorized certificates. Although not required by Emergency Directive 19-01, the Chief Information Officer (CIO) Organization staff stated that the FDIC's cyber threat detection solution monitors the IT environment for new certificates. If a new certificate is identified, an email alert is sent to appropriate FDIC personnel to determine whether the certificate is authorized. Further, based on our inquiries during the audit, FDIC staff developed a new Standard Operating Procedure, *Monitor Certificate Transparency Logs*, Release 0.2 (June 17, 2019), that defines the FDIC's processes for monitoring CT logs.

FDIC COMMENTS AND OIG EVALUATION

Our report contains no recommendations, and the CIO and Director, Division of Information Technology, elected not to provide a written response.

Objective

The audit objective was to determine whether the FDIC took responsive actions to address the requirements of Emergency Directive 19-01 to mitigate DNS infrastructure tampering.

We conducted this performance audit from May 2019 to August 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Scope and Methodology

The scope of the audit covered the actions taken by the FDIC to address the requirements of Emergency Directive 19-01. To accomplish our objective, we gained an understanding of the requirements in Emergency Directive 19-01 by interviewing FDIC staff and managers in the CIO Organization; reviewing key documents, such as the FDIC's status and completion reports submitted to CISA on January 25, 2019, and February 5, 2019, respectively; and contacting DHS to clarify aspects of Emergency Directive 19-01. To assess the responsiveness of the FDIC's actions to address the requirements of Emergency Directive 19-01, we performed detailed audit procedures as described below.

Audit DNS Records

We obtained and reviewed the listing of all 178 public DNS records on authoritative and secondary DNS servers for the FDIC's .gov or other Agency-managed domains that the CIO Organization generated in response to Emergency Directive 19-01. We determined that this listing was reliable for purposes of our analysis by speaking with CIO Organization staff and observing the process they used to generate the listing. We also interviewed CIO Organization staff about the procedures they used to verify that all FDIC domain names resolved to their intended IP addresses. Further, we observed CIO Organization staff re-perform these procedures for 2 of the 178 DNS records to ensure our understanding of how the procedures were implemented.

Change DNS Account Passwords

We obtained and reviewed a listing of 37 DNS accounts that the CIO Organization identified as having the ability to make changes to DNS records as of February 5, 2019. We determined that this listing was reliable for purposes of our analysis by

discussing it with CIO Organization staff and observing the tools and processes used to generate the listing. During our audit, we learned that CIO Organization staff had inadvertently omitted one account capable of making changes to DNS records from the FDIC's completion report submitted to CISA on February 5, 2019. We reviewed documentation confirming that the FDIC had changed the password for this and the remaining 37 accounts prior to submitting the report.

Implement Multi-Factor Authentication

We reviewed documentation confirming that the CIO Organization had implemented MFA for all accounts that could make changes to DNS records as of February 5, 2019. We also observed CIO Organization staff log into two accounts to confirm that MFA was enabled and working as intended.

Monitor Certificate Transparency Logs

We interviewed CIO Organization staff to gain an understanding of the process they used to monitor CT logs. In addition, we obtained and reviewed the following documents:

- The DHS's Cyber Hygiene report, dated February 5, 2019, that included the FDIC's CT logs.
- The FDIC's Standard Operating Procedure, *Monitor Certificate Transparency Logs*, Release 0.2 (June 17, 2019).
- An example email alert generated by the FDIC's cyber threat detection solution that identified a new certificate in the IT environment.

We assessed the risk of fraud and abuse related to our audit objective in the course of evaluating audit evidence. We performed our work at the FDIC's Virginia Square offices in Arlington, Virginia.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.