LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

DNS Tunneling

03/04/2021

TLP: WHITE, ID# ***202103041030***

Agenda

- DNS Overview
- Example: DNS Tunneling Technique
- DNS Tunneling Threats
- Detection
- Mitigation Strategies

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

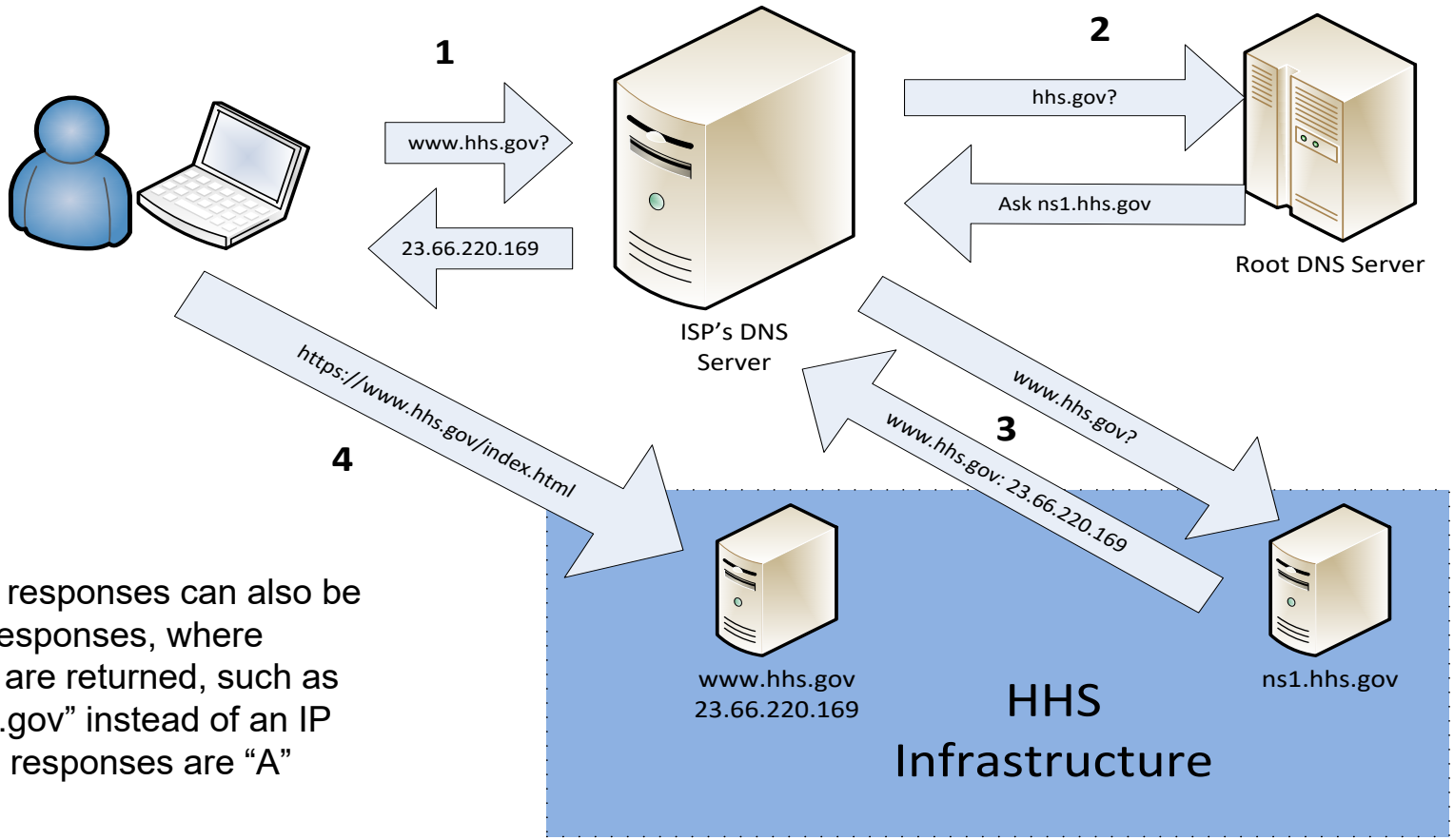
Early Internet (ARPA Internet)

- To access a host across the network, users had to reference its numeric IP address; for example: 192.168.161.45.
- Hosts were registered (listed) in a global table available as a text file.
- This file mapped host names to host addresses.

RFC 882 (November 1983):

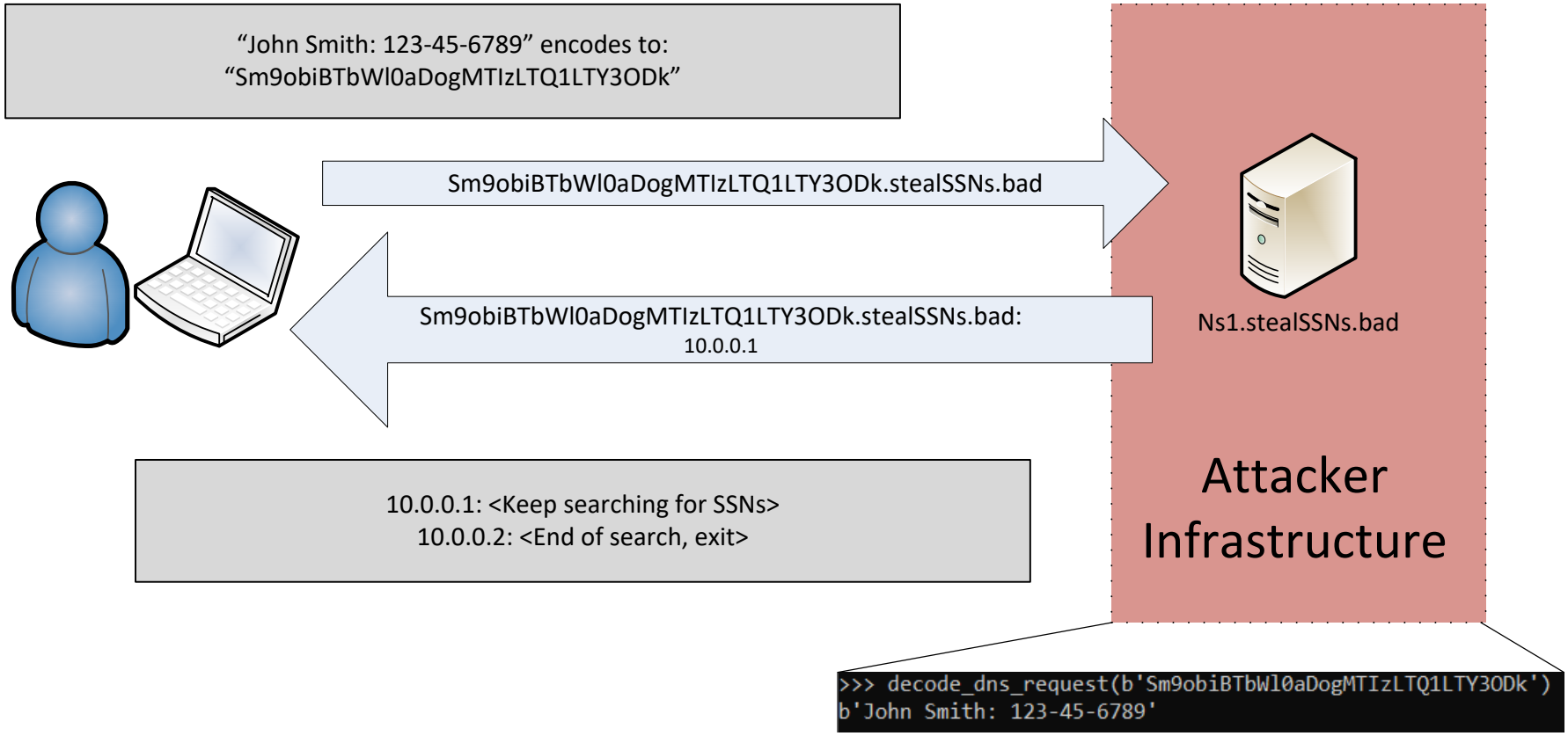
- "The size of this table, and especially the frequency of updates to the table, are near the limit of manageability. What is needed is a distributed database that performs the same function, and hence avoids the problems caused by a centralized database." – Paul Mockapetris, inventor of DNS
- "The problem for computer mail is more severe."
- This RFC outlines the basics of the Domain Name System (DNS)

Normal Operation of DNS Infrastructure and Information Flow



Note: DNS responses can also be "CNAME" responses, where hostnames are returned, such as "www1.hhs.gov" instead of an IP address. IP responses are "A" responses.

DNS Tunneling Example: Exfiltrating Social Security Numbers



- **DGAs = Domain Generation Algorithms**
  - The technique of dynamically generating hostname queries based on certain criteria
- Frequently used for generating C2 (Command and Control) domains for malware
  - It is common for them to change based on time
  - Technique is better than a static list of C2 IP addresses
- As seen in the previous example, DGAs can be used to encode data
  - Information which may be blocked by email gateways or web proxies can be tunneled via DNS
  - The combination of DNS requests and DNS responses provides two-way communication

Notable use of DGA / DNS tunneling by malware families:

Malware Family	DGA / DNS Tunneling Use
CHOPSTICK	CHOPSTICK can use a DGA for Fallback Channels, and domains are generated by concatenating words from lists.
MiniDuke	MiniDuke can use DGA to generate new Twitter URLs for C2 (Command and Control).
Ngrok	Ngrok can provide DGA for C2 servers through the use of random URL strings that change every 12 hours.
OilRig	OilRig has used DNS for C2.
PlugX	PlugX can be configured to use DNS for C2.
TEXTMATE	TEXTMATE uses DNS TXT records for C2.

Source: MITRE ATT&CK Framework

Notable use of DGA / DNS tunneling by malware families:

Malware Family	DGA / DNS Tunneling Use
CHOPSTICK	CHOPSTICK can use a DGA for Fallback Channels, domains are generated by concatenating words from lists.
MiniDuke	MiniDuke can use DGA to generate new Twitter URLs for C2 (Command and Control).
Ngrok	Ngrok can provide DGA for C2 servers through the use of random URL strings that change every 12 hours.
OilRig	OilRig has used DNS for C2
PlugX	PlugX can be configured to use DNS for command and control
TEXTMATE	TEXTMATE uses DNS TXT records for C2.
SunBurst	***SunBurst used DNS for C2 traffic designed to mimic normal SolarWinds API communications.***

Source: MITRE ATT&CK Framework

SunBurst

- A digitally-signed component of SolarWinds was compromised with backdoor code and distributed via the vendor's standard distribution channels.
- C2 (Command and Control) communication takes place over HTTP to third party servers.
- SunBurst (mis)uses DNS in the following ways:
  - It encodes information, including the machine domain name of the server it is installed on, using a DGA.
  - A DNS request is made for a DGA-determined hostname under "avsvmcloud[.]com".
  - DNS "CNAME" responses point Sunburst to the C2 servers to use.
  - DNS "A" responses control the malware behavior based on the returned IP address block.

CISA Alert AA20-302 (October 28, 2020):

Ransomware Activity Targeting the Healthcare and Public Health Sector

- Joint alert by CISA, HHS, and the FBI
- "CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services."
- The FBI observed TrickBot modules named "Anchor" being used.
- "As part of the new Anchor toolset, TrickBot developers created anchor_dns, a tool for sending and receiving data from victim machines using Domain Name System (DNS) tunneling."

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- **While detecting DNS tunneling and use of DGAs can be challenging, here are some strategies which may be leveraged:**
  - Size of request and response
  - Entropy of hostnames
  - Volume of requests per domain or IP address
  - DNS requests without follow-up traffic
  - DNS requests from clients directly to third party DNS servers, not to internal or ISP resolvers

Apart from detection, there are some proactive strategies which may be leveraged:

- Filter Network Traffic
  - Consider filtering DNS requests to unknown, untrusted, or known bad domains and resources.
  - Resolving DNS requests with on-premises/proxy servers may also disrupt adversary attempts to conceal data within DNS packets.

- Network Intrusion Prevention
  - Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.

Source: MITRE ATT&CK Framework

Reference Materials

References

Background:

- https://tools.ietf.org/html/rfc810
- https://tools.ietf.org/html/rfc882

DNS Tunneling Threat:

- https://attack.mitre.org/techniques/T1568/002/
- https://attack.mitre.org/techniques/T1071/004/
- https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Sunburst:

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Detection:

- https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152

Mitigation:

- https://attack.mitre.org/techniques/T1071/004/

Questions

Upcoming Briefs

- 2021 Forecast: the Next Year of Healthcare Cybersecurity
- HPH Supply Chain Risk Management

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday–Friday, between 9am–5pm (EST), at **(202) 691-2110.**

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday–Friday, between 9am–5pm (EST), at **(202) 691-2110.**

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV