DNS as a Covert Channel Within Protected Networks

Author	Seth Bromberger, Co-Principal Investigator, NESCO
Document Number	WP2011-01-01
Revision	1.1
Publication Date	25 January 2011

Acknowledgement / Disclaimer
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000516.

I. Overview

Critical information relating to company operations exists within the electric sector on both control/operations and business networks. While most attempts by malicious actors to exfiltrate this data have required the ability to establish inbound or outbound connections to these networks, there are other methods of exfiltration that do not rely on direct connections that are generally blocked by perimeter security devices. Exfiltration of data via Domain Name System (DNS) queries is a method of breaching the confidentiality of company information that is commonly available, hard to detect, and can provide indirect command and control (C2) channels between an attacker and compromised hosts.

This whitepaper discusses ways to detect DNS exfiltration attempts based on current known methods, and provides recommendations for mitigation of this exposure.

To restate: The DNS exfiltration techniques described below do not require direct connectivity to any external resource from the target machine.

II. Technical Summary

- Malicious software is known to exfiltrate confidential data and establish command-and-control channels using DNS A, SRV, and TXT queries.
- The communications channel can be established on any network device whose configured DNS servers enable resolution of untrusted or external hosts. A quick check: if resolution of “exfilt-test.energysec.org” returns 10.0.0.9, establishment of a communications channel using DNS is possible from the tested host.
- Detection of this communications channel involves inspection of DNS queries and responses. Indicators are listed below.
- Mitigation methods can include isolating DNS servers on protected networks so that they do not forward queries to untrusted or less protected networks or devices.
- NESCO staff are available to provide assistance in the event you detect anomalous DNS traffic. We can help get you in touch with other organizations with nonattributable communications where appropriate.

III. Description of Issue

Exfiltration of data from control systems and business networks can put an entire organization at risk. Whether the information relates to business intelligence, operations plans, or lists of critical assets, the unauthorized disclosure of data can pose a great risk to an organization’s continuity of operations.

Most methods of remotely-initiated data exfiltration rely on two components: the compromise of a target host, and the interconnectedness of that host to the attacker’s network in order to effect the transfer of sensitive data from the target machine. In response to these requirements, many operational networks are isolated from public networks such as the Internet, and have well-defined and documented interconnections to other non-public networks (such as the organization’s business or general user network).

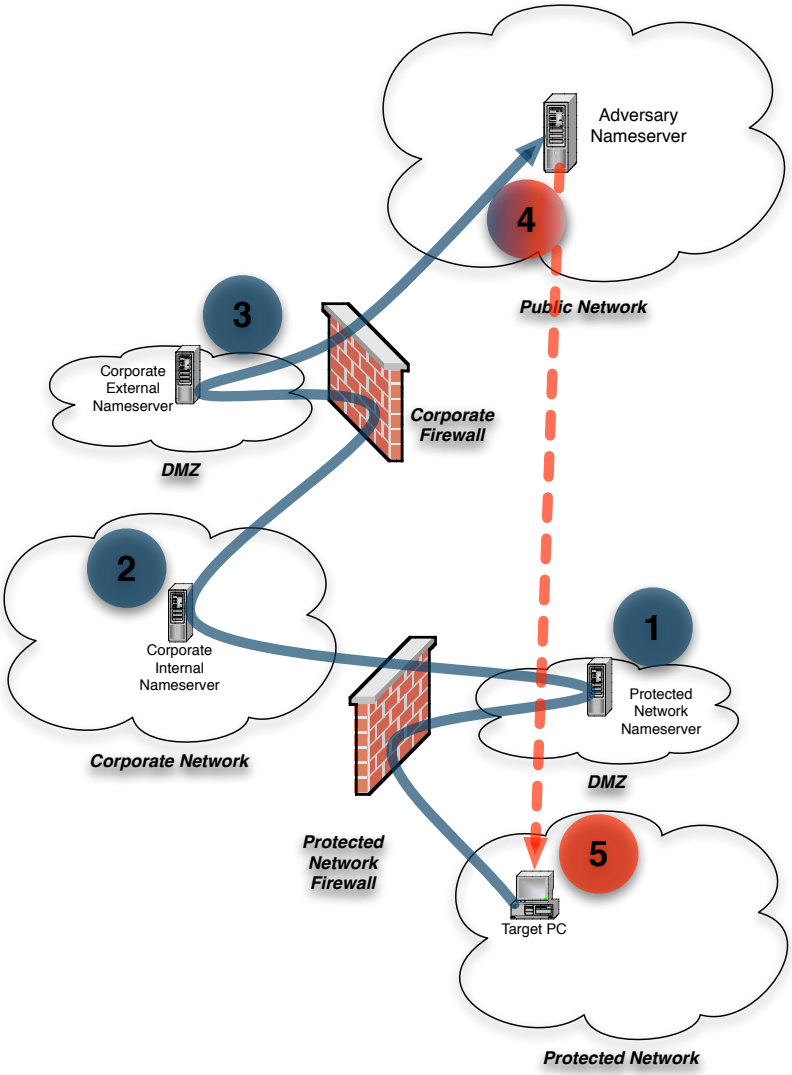
Even with a well-defined set of interfaces to other networks, all networks require some set of common infrastructure services in order to function normally. Among those services is network name resolution, commonly implemented using the Domain Name System (DNS). It is via DNS that common names of servers and other network devices are associated with the Internet Protocol (IP) network addresses that are used to establish connectivity among communicating

hosts. Without this service, IP-based communications are often restricted to using numeric IP addresses to establish connectivity. Using IP addresses in this manner has impacts on network and service availability, and makes network reconfiguration and maintenance more difficult.

The process by which most DNS resolution occurs is via query forwarding: that is, if a DNS nameserver is not authoritative for the underlying domain, it will relay the query to other nameservers that either are authoritative for the domain or can further relay the query. In this way, the IP addresses for internet hosts such as www.google.com can be resolved by hosts within a protected network: the local DNS servers are queried first; since they are not authoritative for google.com, they will relay the query to a set of servers that can either query the authoritative nameservers or can pass the query to a server that can further relay the query. This allows arbitrary name resolution by hosts without requiring a direct connection to the set of nameservers that might hold the data for the destinations being queried.

A full description of DNS forwarding is outside the scope of this paper. Please see the appendix for further references.

The act of relaying DNS queries from secure systems to arbitrary internet-based nameservers forms the basis of this uncontrolled data channel. Consider a target host that meets condition 1: it has been compromised by some malicious software. Even if we assume that connections to public networks are not allowed, if the target host is able to resolve arbitrary domain names, data exfiltration is possible via forwarded DNS queries, as shown in the following example.



Setup: A malicious application on the target host is designed to transfer the contents of a specific file ("confidential.doc") to an adversary who controls a public internet server and has control of a domain name ("badguy.com"). The malicious application takes the contents of the confidential.doc ("ultra-secret stuff") and prepends it to the "badguy.com" domain ("ultra-secret.stuff.badguy.com") and then requests name resolution for this domain name. (In most cases, the data are typically encoded or encrypted prior to prepending to the adversary's domain.)

Steps 1 - 3: The target host's primary nameserver receives this request, determines that it is not authoritative for "badguy.com", and forwards the request through a series of internal and external nameservers where it eventually reaches "nameserver.badguy.com", the nameserver that is authoritative for "badguy.com" and is under the adversary's control.

Steps 4 - 5: "nameserver.badguy.com" receives and logs the "ultra-secret.stuff.badguy.com" request. The adversary now has the target's confidential data. In addition, the adversary now has the opportunity to return command and control data to the target via the expected response: an IP address. The malicious application could interpret specific IP address responses as instructions to perform other activity, such as erasing or modifying data, interfering with computer operation, or exfiltrating other data.

IV. Indicators

Testing to determine whether such an attack is feasible is very straightforward. Both UNIX and Windows systems have a command called "nslookup" which can be used to test DNS resolution. NESCO has set up a test domain name that can be used to determine whether DNS forwarding is enabled for a given device/network. At a command prompt, if "nslookup exfilt-test.energysec.org" returns an IP address of 10.0.0.10, then externally-forwarded name resolution is enabled from that system and, if the system were to be infected by malicious

software that uses the techniques described above, exfiltration and C2 access would be successful.

Determining whether any systems are actually exfiltrating data via nameserver queries is a bit more difficult and requires access to the corporate nameservers' query logs (which may not be enabled by default). Note that in many cases, encryption or encoding of the query data makes it difficult to analyze the queries themselves for the presence of confidential or control information.

Current known attacks utilizing DNS exfiltration include one or more of the following characteristics:

- DNS name lookups that have multiple levels (a.b.c....n.domain.com) where a,b,c...n are composed of hexadecimal strings (*e.g.*, e04fdbe587a1.f6c7.example.com)
- DNS name lookups as described above, where the cumulative length of the third and higher-level names (a.b.c....n) exceeds 40 bytes
- Multiple DNS name lookups to non-obvious or foreign domains (e.g., 4c7a.obscure.com, 1a6d.some.site.cn)
- Multiple DNS name lookups to several non-obvious or foreign domains within a short timespan
- DNS TXT or SRV record queries to non-obvious or foreign domains
- DNS responses that include loopback or RFC1918 address space (e.g., a response to an external DNS query of any address in the 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, or 192.168/16 netblocks) - these can indicate C2 activity as described above.
- Multiple DNS queries to non-obvious or foreign domains occurring outside of normal business hours, including weekends
- DNS queries to Dynamic DNS service providers (*e.g.*, dyndns and xname)
- DNS queries that are not followed by a proxied request for connection (such as HTTP, FTP, or other expected data transfer)

V. Mitigation

To prevent DNS exfiltration from a protected network, ensure that DNS queries are not relayed outside the trusted perimeter. This will prevent any information being leaked via DNS to untrusted hosts.

To detect DNS exfiltration, evaluation of namequery network traffic is required. The easiest way to accomplish this is to enable query logging on nameservers; however, the servers can quickly become overloaded with logging data if they are not sufficiently provisioned to handle this extra load. Network sensors that can capture DNS traffic could also be used. Implementation of network sensors is more difficult, but can yield better results as analysis of inbound and outbound DNS traffic is generally easier.

Correlation of DNS queries to other proxy logs to determine whether the queries were the result of legitimate service access is also very important. Outbound connection logs, including firewall and other perimeter control devices, should be monitored in conjunction with DNS queries, and any DNS query that does not result in a proxied outbound connection request should be investigated.

VI. What to do if you detect this activity

If you detect suspicious DNS traffic on your networks, your company's computer incident response and forensics plans should be activated. NESCO is here to help: if your organization

needs assistance in interpreting logs or in contacting other incident response organizations, please reach out to us. Our contact information is listed below.

VII. Conclusion

Exfiltration of sensitive information and command and control of critical systems using DNS as a covert communications channel is no longer relegated to the class of theoretical attacks. However, while attacks against utility systems using DNS exfiltration have been reported, the extent to which the compromises resulted in disclosure of confidential data is unknown due to encryption of the payloads. It is therefore important to assume that any evidence of DNS exfiltration in a sensitive environment has targeted confidential information and has resulted in full command and control of the affected devices.

VIII. Appendix and Further Reading

- Microsoft TechNet guide to DNS: http://technet.microsoft.com/en-us/library/cc779489(WS.10).aspx
- RFC1035, “Domain Names: Implementation and Specification”: http://www.faqs.org/rfcs/rfc1035.html