DEX portal introduction and Frequently Asked Questions

Infoblox DEX portal

Introduction:

The infoblox DEX portal, accessible at https://dex.infoblox.com/, is a suite of sales tools designed to demonstrate how DNS can be used as communications channel, as opposed to its intended and original use of providing information about a given domain name.

The DEX portal is capable not only of showing how data can be exfiltrated, it does so by actually exfiltrating data. The tools in the portal replicate the traffic most commonly used by malware such as botnets and ransomware.

DNS can be used to transport other protocols for bi-directional communication, including the transport of data or instructions from compromised hosts to specifically programmed servers which pose as public external DNS servers.

DNS can be used to exfiltrate virtually any kind of information of data, but the most common examples are:

- Customer proprietary data, manufacturing data, designs, test results
- Personal Identifiable Data (PII) (your name, phone, address and more)
- passwords
- Financial data, account numbers, userid's, passwords, balances

DNS can also be used to transport this data in any format and by consequence, the DEX portal can also be used to transport any file format, including:

- binaries
- text files
- executables
- zip files
- pictures

DEX Portal Tools:

The DEX portal offers different tools that can be used to explain how DNS can be used to transport data, as well as actually transport the data. These tools are of different categories: Data Exfiltration, Data Infiltration, Fast Flux, Domain Generation Algorithms (DGA).

IMPORTANT: You MUST obtain explicit permission from the appropriate contact at the customer. Depending on the customer organization, the appropriate contact might be in the network team, the network security, or the information security, however this may vary. DO NOT USE THE DEX PORTAL WITHOUT THE APPROPRIATE KNOWLEDGE AND/OR PERMISSION.

Data Exfiltration:

- DNS Text Decoder: This is a real-time tool demonstrating exfiltration of a text message over encoded DNS. It uses single and very short DNS requests to send data to an external server.
- DNS Script Decoder: Similar to DNS Text Decoder, except it will output the commands to exfiltrate a file using Perl, Unix Shell, or PowerShell
- Hexify: This tool (an HTML page), will call a graphic from a webserver. The catch is that the web browser MUST first do a DNS lookup to get the file. Hence, the user’s browser is exfiltrating data over DNS. If there is a Web Proxy in place, then the Web Proxy is exfiltrating data over DNS.

Data Infiltration:

- DNS Plain Text: This is a real-time tool demonstrating infiltration of a text message over encoded DNS. It uses single and very short DNS requests to retrieve data to an external server. Non-english symbols and special characters are not supported.
- DNS Encoded Text: This is a real-time tool demonstrating infiltration of a encoded text message over DNS. It uses very short DNS requests to retrieve data from an external server. Non-english symbols and special characters are supported.
- DNS Static Files: This tool demonstrates infiltration of three different data types (Graphic image, Windows executable file, and a shell script). All three data types are transferred to the user workstation by using DNS queries to retrieve and reassemble data held on a remote DNS server. This emulates one possible vector in which malicious code could be introduced into a network using a protocol and message types that would not be detected by traditional security measures.
- DNSMessenger: DNSMessenger uses DNS queries to carry out malicious PowerShell commands on compromised computers, a method that researchers said makes it difficult to detect that a remote access Trojan is being dropped onto targeted systems. The tool emulates DNSMessenger behavior.

DEX portal tips and hints:

- Some customers may insist on running DEX demo on their own. SEs can provision access to their customers in the “End Customer’s Access” section. From there, they can invite customers using their email address and some other customer information.
- Infoblox Partners should also receive access to the portal automatically, when they are provisioned for a Security Assessment portal account.
- In the upper right corner of the DEX webpage, one can access the Profile page by clicking on the User’s Name. This profile page offers the option to change the user’s Full Name, but also offers the option to change the DNS Domain Name used for exfiltration.
- While DNS can transport information of any type and size, it does so relatively slowly, which is why it is recommended to use files smaller than 1MB.

Frequently Asked Questions

- Which DNS record type(s) can be specified for data exfiltration in the DEX tool?
  A: MX, TXT, A, SRV, DNSKEY
- DEX exfiltration or infiltration attempts seem to be blocked, what should I do next?
  A: If these are attempts are being blocked due to the Exfiltration Domain being blacklisted, this domain can be changed in the Profile section as explained in the tips and hints section. If using a different domain does not work, please contact the Security SME team and copy your SE Manager.
- Who should I contact if I need assistance with DEX?
  A: Please contact the Security SME team group address and copy your SE Manager.