DYNAMIC DNS: DATA EXFILTRATION

WHAT IS DATA EXFILTRATION?

One of the most common goals of malicious actors is to steal data. Data exfiltration refers to the successful sending of information out of an environment to an environment controlled by an attacker. Data exfiltration takes many different forms and is an objective of many different types of specific attacks.

WHAT IS DYNAMIC DNS?

Dynamic DNS is fundamentally a method of automatically updating name servers in public DNS (Domain Name System) in near real-time. It is used to keep a specific domain name linked to a changing IP address when a static IP address is not available or not desired. Dynamic DNS domains are typically hosted by providers for that specific purpose, where the provider owns the top level domain (tld) and a subscriber can quickly (and usually freely) register sub-domains and point them to any IP address they choose. Examples of common dynamic DNS domains/providers include:

- no-ip.com
- dyndns.org
- changeip.com
- duiadns.net
- dynamicdns.org
- many others

When a subscriber registers a subdomain, they are free to pick any name they want and map it to any IP address they want. For example, one could register **myuniquedomainname.no-ip.org** or **asnl2349qpwdan.no-ip.org** and have them both resolve to 5.6.7.8.

A Typical Attack Scenario

For nefarious purposes, dynamic DNS allows an attacker to change the actual host and IP address used as a drop zone, for "malvertizing," or as a command and control point without having to modify the behavior of the malware used on the victim's endpoint. This provides a quick and convenient mechanism for attackers to evade detection using traditional IP/domain reputation services. While dynamic DNS can be used for many stages of an attack, this scenario focuses on its use as a drop zone for data exfiltration, uncovered by noticing an anomaly in a daily report.

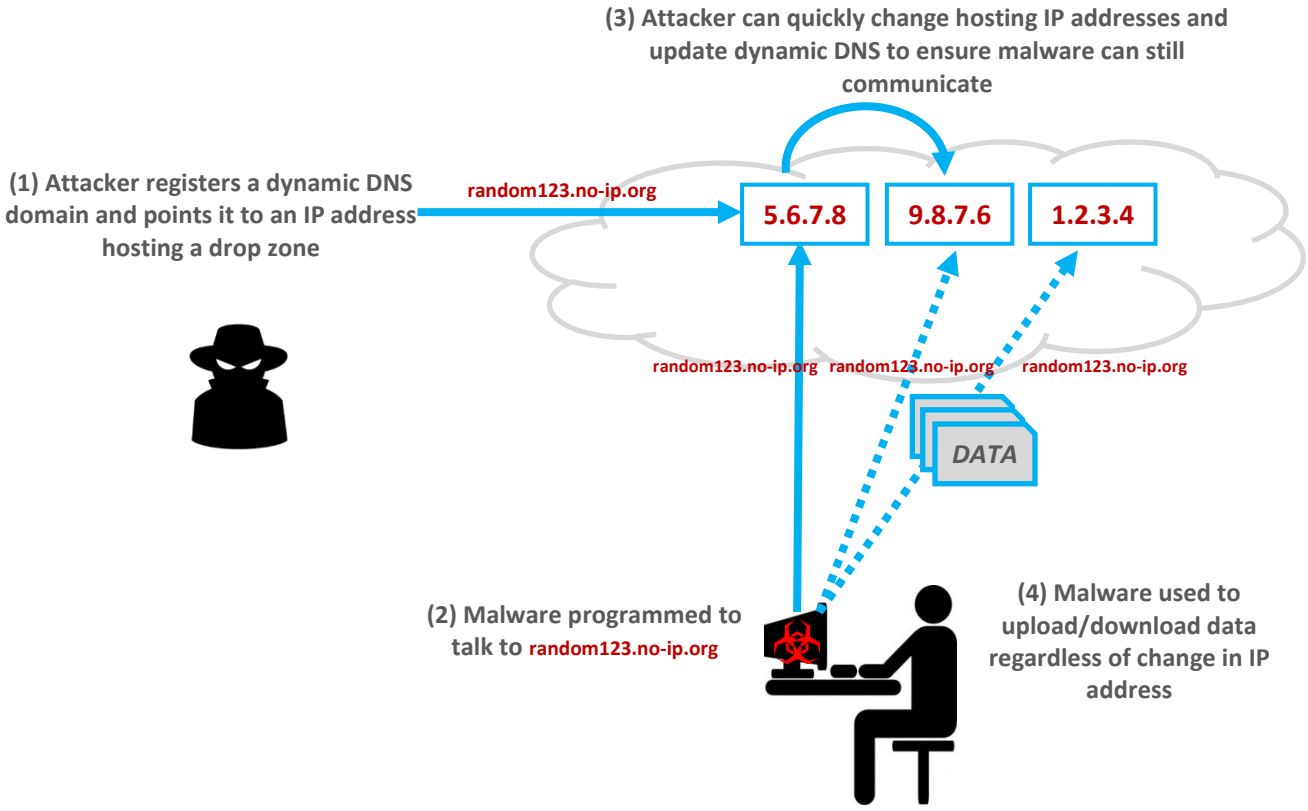


Figure 1 – Attacker Use of Dynamic DNS Domain

Detection and Response

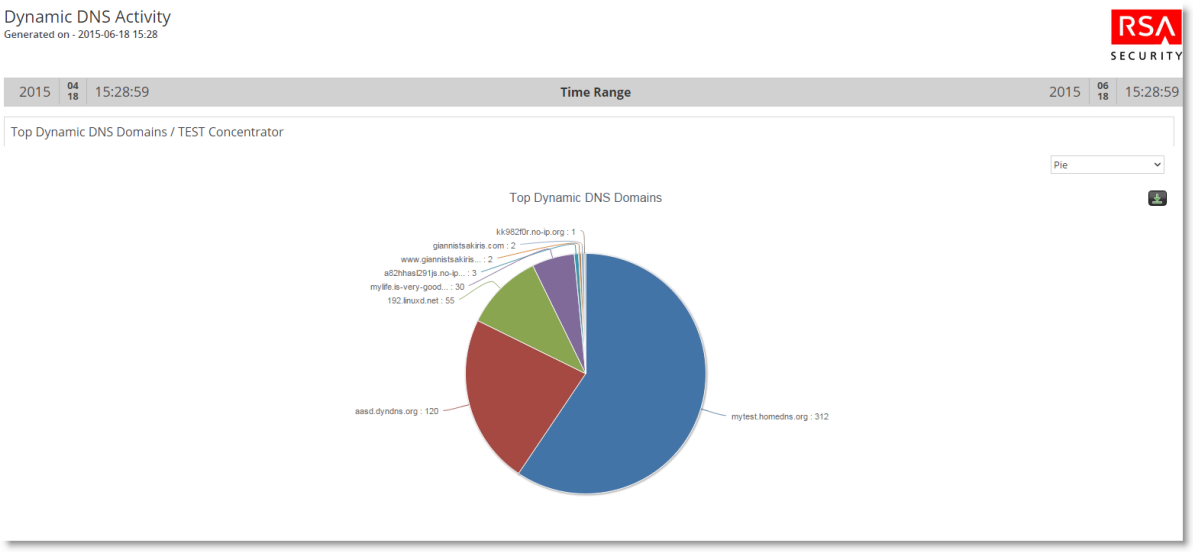
Detection of traffic or logs containing access to and from dynamic DNS domains can be done by traditional tools such as IDS/IPS, Firewalls, and SIEM, however depending on the nature of the attack none of those tools can provide full visibility into the associated network traffic, particularly in the case of data exfiltration.

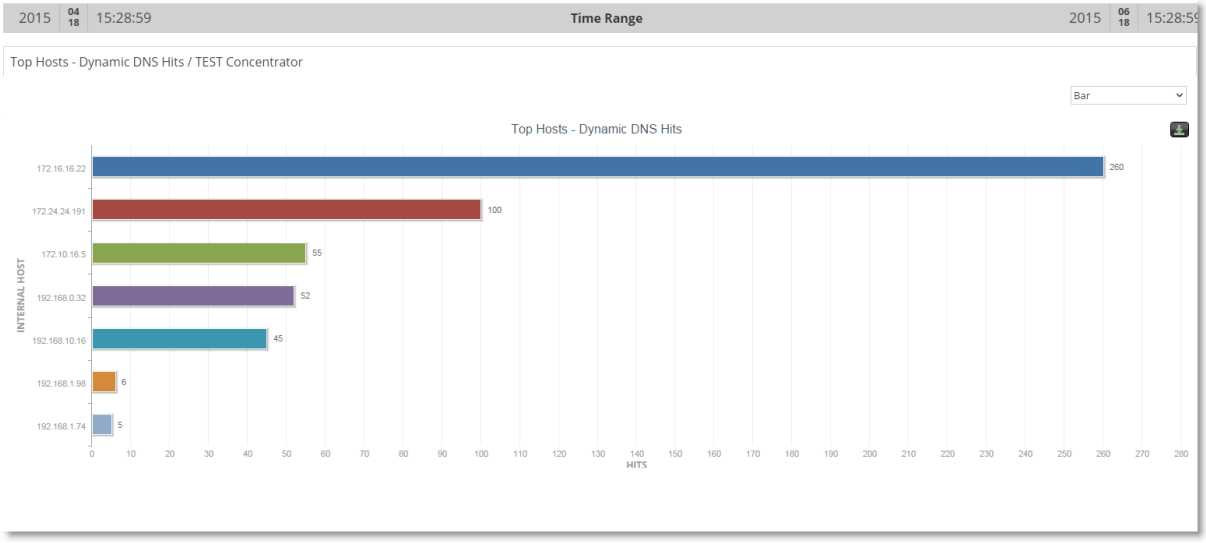
	Delivery Varies	**Exploit/Installation** Varies	**C2** Traffic to Dynamic DNS Domains	**Action** Data Exfiltration
AV/FW/IDS/IPS:				
Traditional SIEM:				
RSA Security Analytics:				

No visibility	Partial Visibility/Signature	Full Visibility

DYNAMIC DNS/DATA EXFILTRATION VISIBILITY WITH RSA SECURITY ANALYTICS FOR PACKETS AND LOGS

RSA Security Analytics allows for the reporting of all network, log, net flow and endpoint data from a single interface. By leveraging a feed of known dynamic DNS top level domains, RSA Security Analytics can produce a rich report summarizing all activity that has been seen both on the wire (packets) or from various devices in the network such as proxies and firewalls (logs). In addition to just tagging traffic to and from dynamic DNS domains, RSA Security Analytics can add valuable business and asset context to help an analyst sift through the noise. In this case, the analyst can see the dynamic DNS traffic split by asset criticality and function:





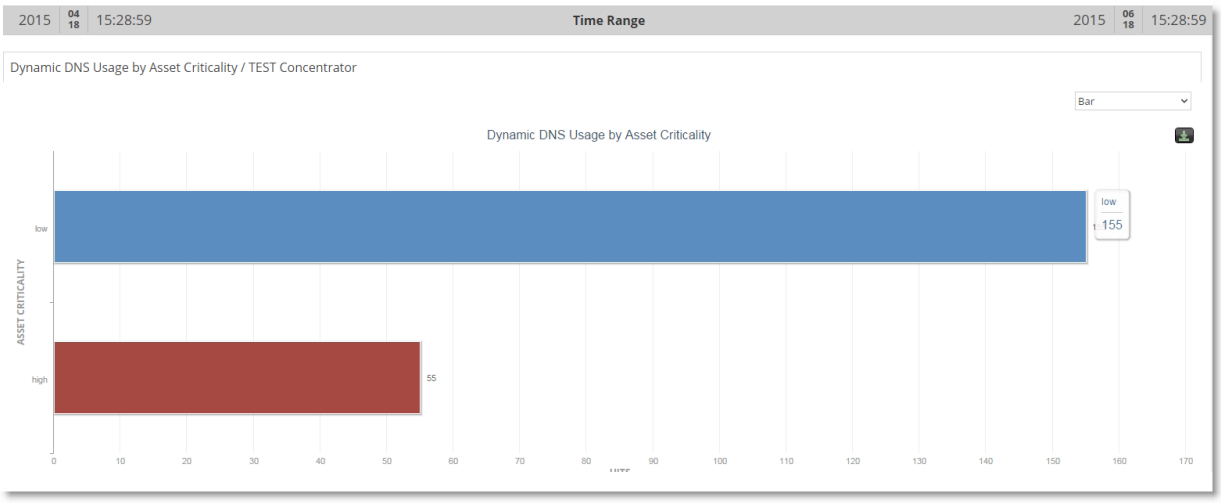


Figure 2 – Sample Dynamic DNS Report

From this report, the analyst can prioritize and drill in to the most interesting data points to investigate further. In this particular report, the analyst focuses in on data uploads to dynamic DNS domains from critical servers (which should never happen in this environment):

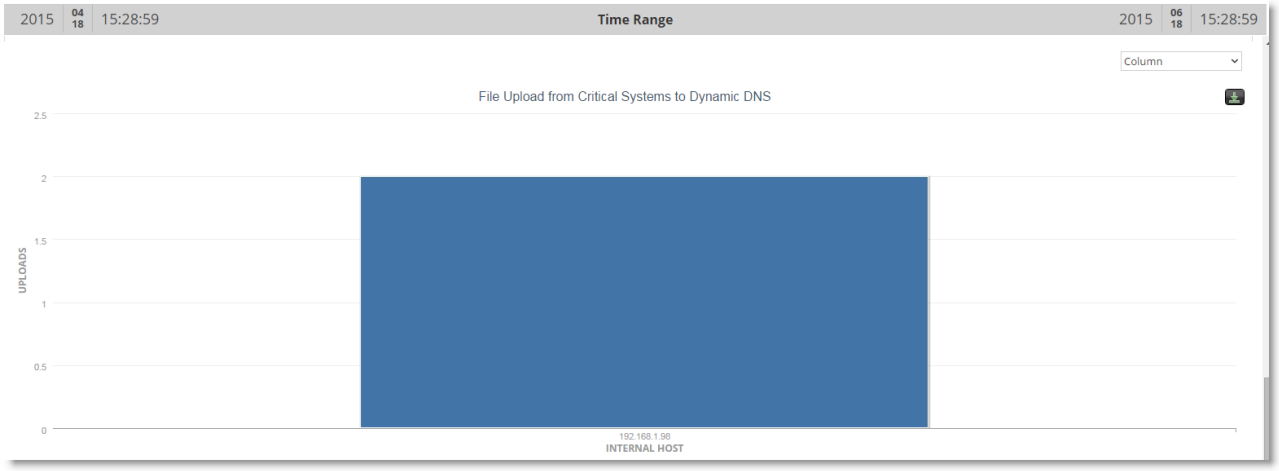


Figure 3 – Dynamic DNS Session from a File Server

Directly from the report, the analyst can drill down to gain insight into the specific sessions:

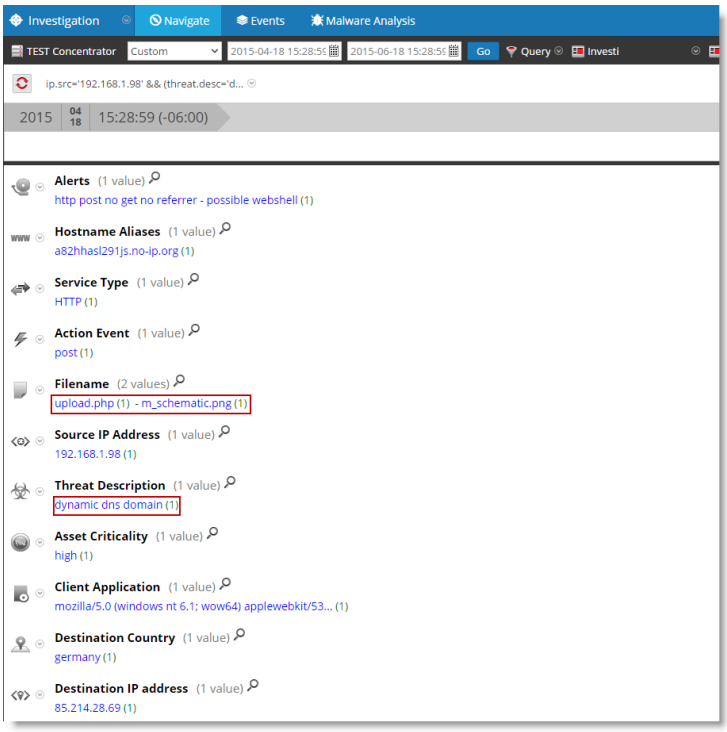


Figure 4 – Drill from Dynamic DNS Report into Sessions from a File Server

This looks suspicious enough on its own, but by drilling once more, the analyst can see the reconstructed network session, and in turn extract any files that had left the environment:

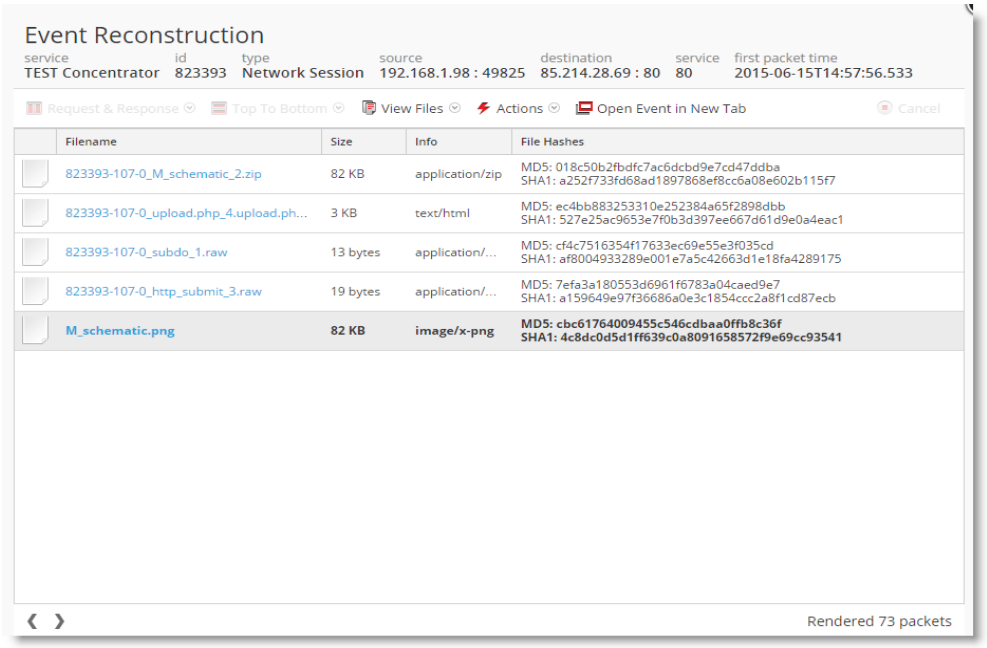


Figure 5 – HTTP Upload of Files to a Dynamic DNS Host from a Critical Server

Going one step further, the analyst can download and extract the archive and see the actual company information that has left the environment. By understanding the business impact, proper steps can now be taken to handle the incident further:

823393-107-0_subdo_1.raw	13 bytes	application/...	MD5: cf4c7516354f17633ec69e55e3f035cd SHA1: af8004933289e001e7a5c42663d1e18fa4289175
823393-107-0_http_submit_3.raw	19 bytes	application/...	MD5: 7efa3a180553d6961f6783a04caed9e7 SHA1: a159649e97f36686a0e3c1854ccc2a8f1cd87ecb
M_schematic.png	**82 KB**	**image/x-png**	**MD5: cbc61764009455c546cdbaa0ffb8c36f SHA1: 4c8dc0d5d1ff639c0a8091658572f9e69cc93541**

Figure 6 – Extract Files to See what has Left the Organization

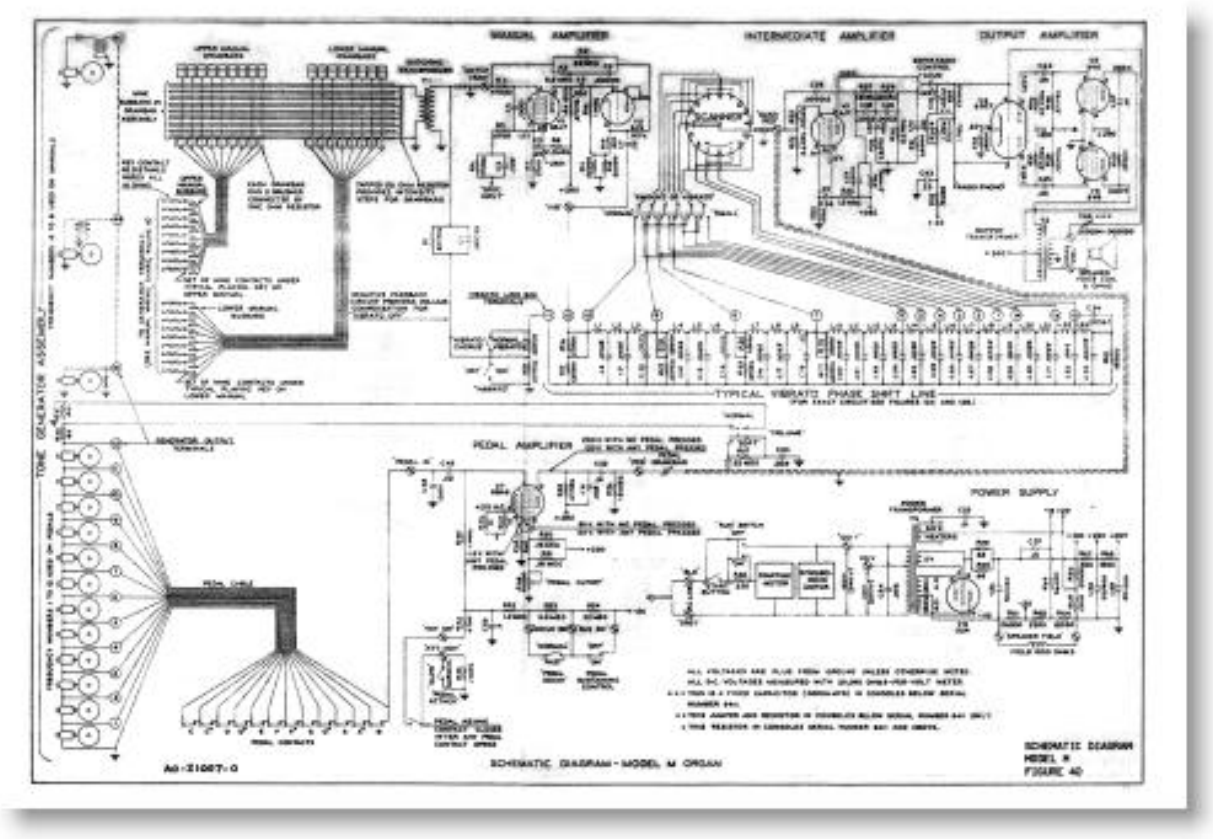


Figure 7 – Extracted Schematic Diagram

REFERENCES

Dynamic DNS: http://en.wikipedia.org/wiki/Dynamic_DNS
List of common dynamic DNS domains: http://mirror1.malwaredomains.com/files/dynamic_dns.txt
C2 using Dynamic DNS: http://info.opendns.com/rs/opendns/images/OpenDNS_SecurityWhitepaper-DNSRoleInBotnets.pdf
Cyber Kill Chain: http://www.lockheedmartin.ca/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html