What is DNS Abuse?

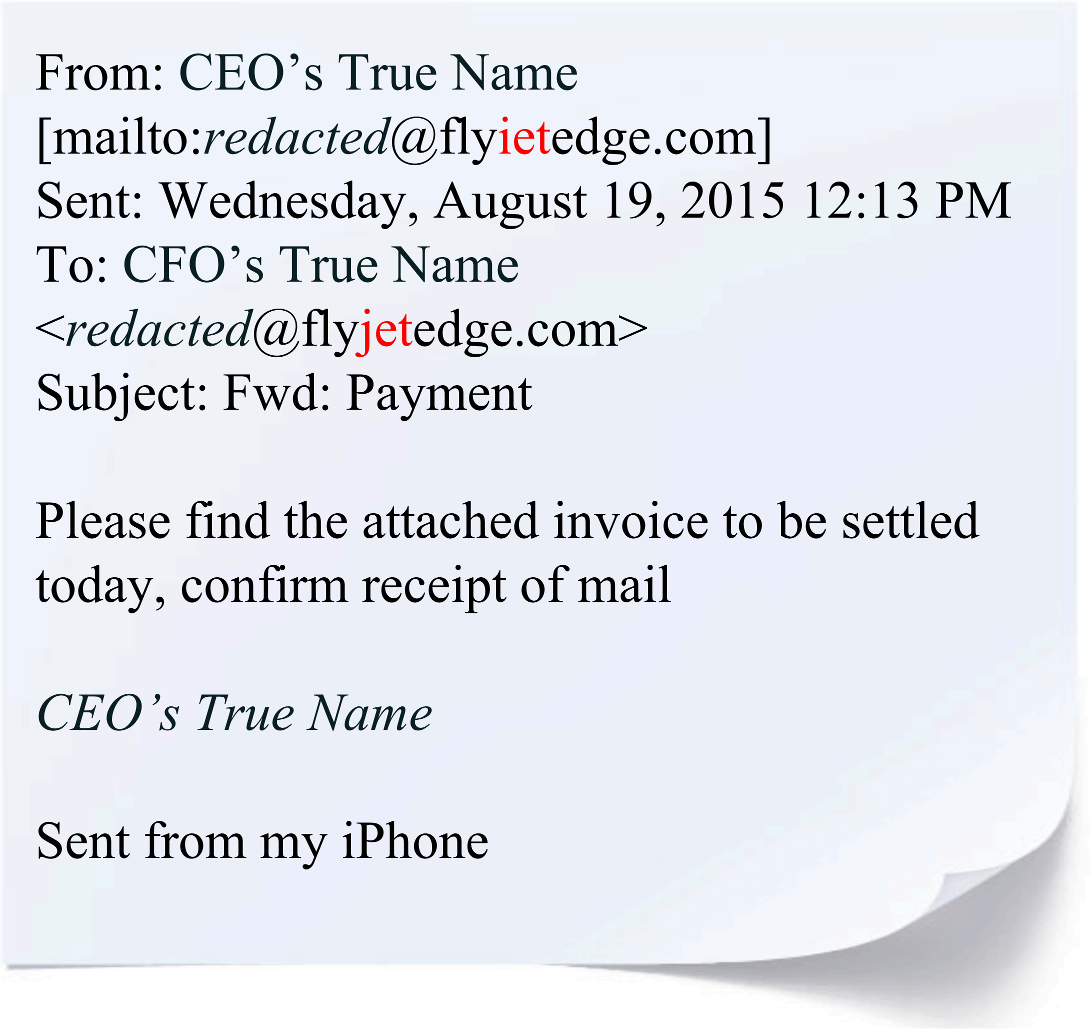
- **Government Advisory Committee (GAC) Beijing Advice (11 April 2013)**
  - *3. Security checks— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate **security threats, such as pharming, phishing, malware, and botnets.** If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.*

- **Specification 11 3b (Per NGPC Proposal for Implementation of 25 June 2013)**
  - *Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate **security threats, such as pharming, phishing, malware, and botnets.** Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. [...]*

- **ICANN's Domain Abuse Activity Reporting (DAAR)**
  - DAAR identifies and tracks reported domain names associated with four kinds of security threats: ***Phishing, Malware, Botnet command-and-control, Spam***

- **Competition, Consumer Trust and Consumer Choice (CCT) Review Definitions (8 September 2018)**
  - **DNS Abuse** as "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names."
  - **DNS Security Abuse** to refer to more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse.

Example 1: Business Email Compromise



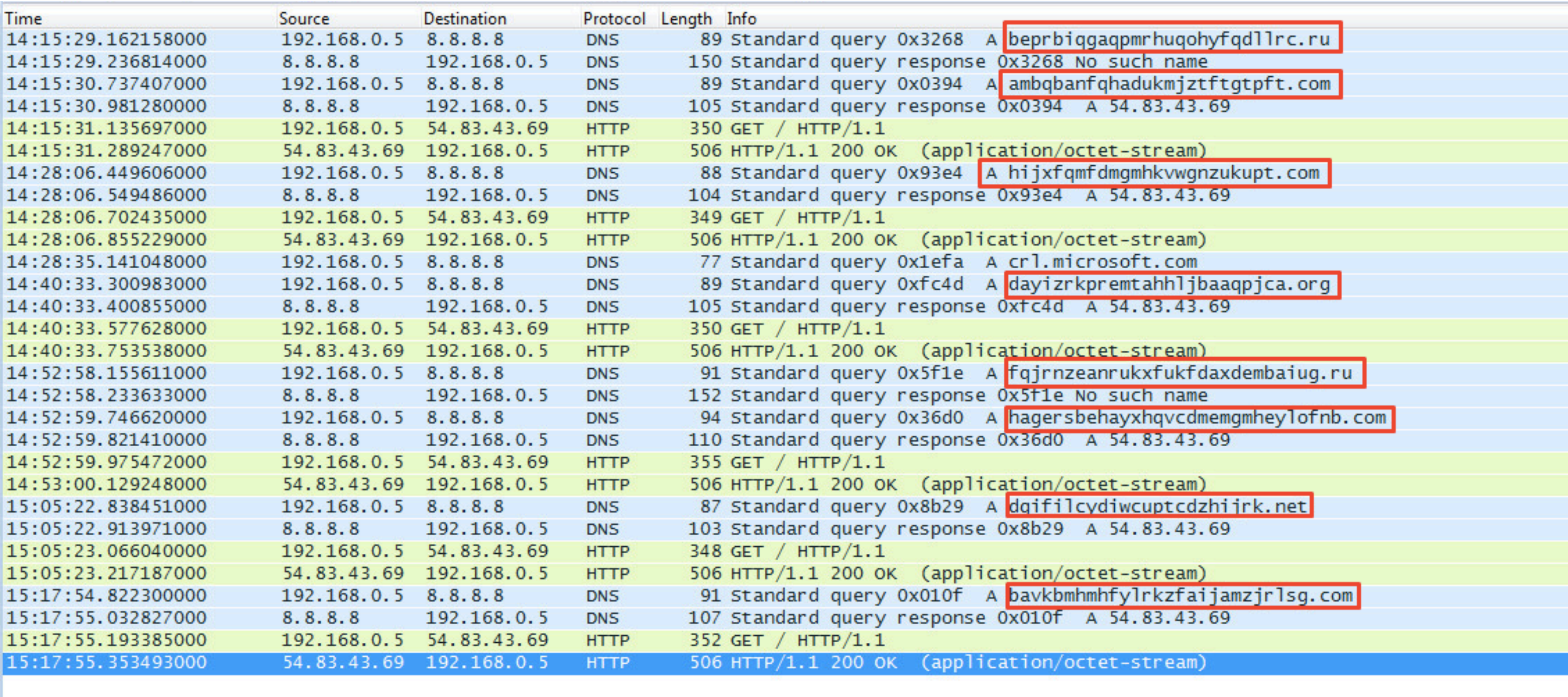
From: CEO’s True Name
[mailto:*redacted*@flyietedge.com]
Sent: Wednesday, August 19, 2015 12:13 PM
To: CFO’s True Name
<*redacted*@flyjetedge.com>
Subject: Fwd: Payment

Please find the attached invoice to be settled today, confirm receipt of mail

CEO’s True Name

Sent from my iPhone

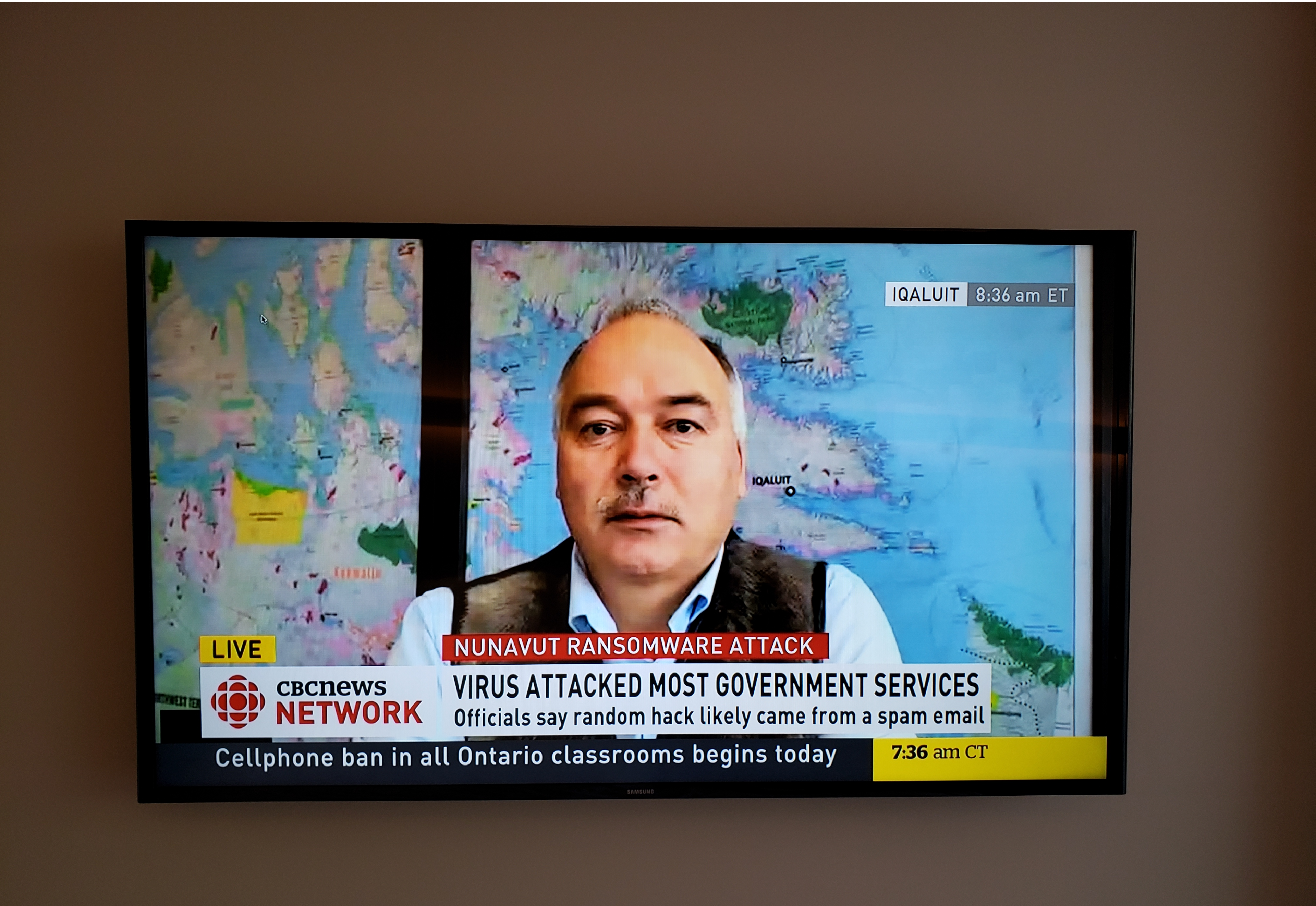
2. Botnets run by "Domain Generation Algorithms"



Time	Source	Destination	Protocol	Length	Info
14:15:29.162158000	192.168.0.5	8.8.8.8	DNS	89	Standard query 0x3268 A beprbiqgaqpmrhuqohyfqdllrc.ru
14:15:29.236814000	8.8.8.8	192.168.0.5	DNS	150	Standard query response 0x3268 No such name
14:15:30.737407000	192.168.0.5	8.8.8.8	DNS	89	Standard query 0x0394 A ambqbanfqhadukmjztftgtpft.com
14:15:30.981280000	8.8.8.8	192.168.0.5	DNS	105	Standard query response 0x0394 A 54.83.43.69
14:15:31.135697000	192.168.0.5	54.83.43.69	HTTP	350	GET / HTTP/1.1
14:15:31.289247000	54.83.43.69	192.168.0.5	HTTP	506	HTTP/1.1 200 OK (application/octet-stream)
14:28:06.449606000	192.168.0.5	8.8.8.8	DNS	88	Standard query 0x93e4 A hijxfqmfdmgmhkvwgnzukupt.com
14:28:06.549486000	8.8.8.8	192.168.0.5	DNS	104	Standard query response 0x93e4 A 54.83.43.69
14:28:06.702435000	192.168.0.5	54.83.43.69	HTTP	349	GET / HTTP/1.1
14:28:06.855229000	54.83.43.69	192.168.0.5	HTTP	506	HTTP/1.1 200 OK (application/octet-stream)
14:28:35.141048000	192.168.0.5	8.8.8.8	DNS	77	Standard query 0x1efa A crl.microsoft.com
14:40:33.300983000	192.168.0.5	8.8.8.8	DNS	89	Standard query 0xfc4d A dayizrkpremtahhljbaaqpjca.org
14:40:33.400855000	8.8.8.8	192.168.0.5	DNS	105	Standard query response 0xfc4d A 54.83.43.69
14:40:33.577628000	192.168.0.5	54.83.43.69	HTTP	350	GET / HTTP/1.1
14:40:33.753538000	54.83.43.69	192.168.0.5	HTTP	506	HTTP/1.1 200 OK (application/octet-stream)
14:52:58.155611000	192.168.0.5	8.8.8.8	DNS	91	Standard query 0x5f1e A fqjrnzeanrukxfukfdaxdembaiug.ru
14:52:58.233633000	8.8.8.8	192.168.0.5	DNS	152	Standard query response 0x5f1e No such name
14:52:59.746620000	192.168.0.5	8.8.8.8	DNS	94	Standard query 0x36d0 A hagersbehayxhqvcdmemgmheylofnb.com
14:52:59.821410000	8.8.8.8	192.168.0.5	DNS	110	Standard query response 0x36d0 A 54.83.43.69
14:52:59.975472000	192.168.0.5	54.83.43.69	HTTP	355	GET / HTTP/1.1
14:53:00.129248000	54.83.43.69	192.168.0.5	HTTP	506	HTTP/1.1 200 OK (application/octet-stream)
15:05:22.838451000	192.168.0.5	8.8.8.8	DNS	87	Standard query 0x8b29 A dqifilcydiwcuptcdzhijrk.net
15:05:22.913971000	8.8.8.8	192.168.0.5	DNS	103	Standard query response 0x8b29 A 54.83.43.69
15:05:23.066040000	192.168.0.5	54.83.43.69	HTTP	348	GET / HTTP/1.1
15:05:23.217187000	54.83.43.69	192.168.0.5	HTTP	506	HTTP/1.1 200 OK (application/octet-stream)
15:17:54.822300000	192.168.0.5	8.8.8.8	DNS	91	Standard query 0x010f A bavkbmhmhfylrkzfaijamzjrlsg.com
15:17:55.032827000	8.8.8.8	192.168.0.5	DNS	107	Standard query response 0x010f A 54.83.43.69
15:17:55.193385000	192.168.0.5	54.83.43.69	HTTP	352	GET / HTTP/1.1
15:17:55.353493000	54.83.43.69	192.168.0.5	HTTP	506	HTTP/1.1 200 OK (application/octet-stream)

Source = CyberReason
(http://www.cybereason.com/the-fbi-vs-gameover-zeus-why-the-dga-based-botnet-wins/)

3. Spam as malware delivery



NUNAVUT RANSOMWARE ATTACK

VIRUS ATTACKED MOST GOVERNMENT SERVICES

Officials say random hack likely came from a spam email

Cellphone ban in all Ontario classrooms begins today