Internet-based Counterintelligence

A white paper by the consultants of Matta Security Limited

http://www.trustmatta.com

info@trustmatta.com

+44 (0) 8700 77 11 00

Introduction

The Internet can be used by determined attackers as a useful tool to gather intelligence about a target organisation. Through entirely using open sources (primarily Internet search engines, WHOIS servers & DNS requests), Matta has undertaken the task of performing Internet-based counterintelligence against the Central Intelligence Agency (CIA), with some surprising results.

It should be clearly noted that, at no point did we port scan or directly probe any CIA Internet-based networks, as all of our intelligence was gathered using open sources. This counterintelligence was undertaken entirely within English and American law regarding computer misuse and control of data. If Matta had been authorised to launch a determined attack (encompassing network scanning and aggressive probing of the CIA's infrastructure) more information would have been gleaned. In the interests of Matta retaining professionalism, entirely open sources were used in-line with the law.

The Information

Our first task was to identify the CIA's points of presence globally, by using WHOIS and DNS requests to enumerate domain names and network blocks used –

Primary CIA Internet-based networks:

- cia.gov
- ucia.gov
- odci.gov

- 198.81.128.0 – 198.81.191.255

Other networks and domains identified:

- ncix.gov and nacic.gov (National Counterintelligence Executive)
- ic.gov
- istac.gov

- 162.45.0.0 – 162.45.255.255

For this task, we undertook comprehensive mapping and analysis of open source material and information relating to the CIA's primary points of presence, consisting of identifying ucia.gov, cia.gov & odci.gov hosts and networks within the 198.81.129.0 – 198.81.191.255 network space.

WHOIS Information Gleaned

Through simply using the WHOIS server at http://www.nic.gov, we were able to identify both domains used by the CIA, and individuals (by requesting information for "@ucia.gov") –

```
Central Intelligence Agency (CIA-DOM)
   Information Services Infrastructure
   Washington, DC 20505


   Domain Name: CIA.GOV
   Status: ACTIVE
   Domain Type: Federal

   Technical Contact, Administrative Contact, Billing Contact:
      Wheelock, David E.  (DEW1)
      (703) 613-9840
      DAVIDW@UCIA.GOV


   Domain servers in listed order:

   RELAY1.UCIA.GOV         198.81.129.193
   AUTH100.NS.UU.NET               198.6.1.202

   Record last updated on 31-Oct-01.


Central Intelligence Agency (ODCI-DOM)
   Information Services Infrastructure
   Washington, DC 20505


   Domain Name: ODCI.GOV
   Status: ACTIVE
   Domain Type: Federal

   Technical Contact, Administrative Contact, Billing Contact:
      Wheelock, David E.  (DEW1)
      (703) 613-9840
      DAVIDW@UCIA.GOV


   Domain servers in listed order:

   RELAY1.UCIA.GOV         198.81.129.193
   AUTH100.NS.UU.NET               198.6.1.202

   Record last updated on 31-Oct-01.
```

CIA (ISTAC-DOM)
   1820 Electric Avenue
   Vienna, VA 21076

   Domain Name: ISTAC.GOV
   Status: **ACTIVE**
   Domain Type: Federal

   Technical Contact, Administrative Contact:
      S, Dan (DS3)
      703-281-8087
      DAN@ISTAC.GOV

   Domain servers in listed order:

   MARS.ISTAC.GOV   199.99.221.33
   NS1.SPRINTLINK.NET   204.117.214.10
   NS2.SPRINTLINK.NET   199.2.252.10, 199.2.252.1
   NS3.SPRINTLINK.NET   204.97.212.10

   Record last updated on 31-Oct-97.

Central Intelligence Agency (IC-DOM)
   Information Services Infrastructure
   Washington, DC 20505

   Domain Name: IC.GOV
   Status: **ACTIVE**
   Domain Type: Federal

   Technical Contact, Administrative Contact, Billing Contact:
      Wheelock, David E. (DEW1)
      (703) 613-9840
      DAVIDW@UCIA.GOV

   Domain servers in listed order:

   RELAY1.UCIA.GOV   198.81.129.193
   AUTH100.NS.UU.NET   198.6.1.202

   Record last updated on 31-Oct-01.

Office of the Natl Counterintelligence Executive (NCIX-DOM)
   Room 3W01 NHB
   Washington, DC 20505

   Domain Name: NCIX.GOV
   Status: **ACTIVE**
   Domain Type: Federal Exception

   Technical Contact:
      Osmolskis, Tadas (TO)
      (301) 975-0103
      WCRABBS@RAMS.COM

   Administrative Contact, Billing Contact:
      Hawkey, Richard A. (RAH)
      (703) 874-4510
      RICHAAH@UCIA.GOV

   Domain servers in listed order:

   AUTH40.NS.UU.NET   198.6.1.18
   AUTH62.NS.UU.NET   198.6.1.19

   Record last updated on 23-Jul-01.

NCIX (NACIC-DOM)
   22222

   Domain Name: NACIC.GOV
   Status: **ACTIVE**
   Domain Type: Federal Exception

   Technical Contact:
      Osmolskis, Tadas (TO)
      (301) 975-0103
      WCRABBS@RAMS.COM

   Administrative Contact:
      Hawkey, Richard A. (RAH)
      (703) 874-4510
      RICHAAH@UCIA.GOV

   Domain servers in listed order:

   AUTH40.NS.UU.NET   198.6.1.18
   AUTH62.NS.UU.NET   198.6.1.19

   Record last updated on 06-Apr-01.

DNS Information Gleaned

The following types of DNS queries were used in order to enumerate CIA network address space for the 198.81.128.0.0 – 198.81.191.255 network block –

- Standard forward DNS requests
- Zone transfers
- Reverse DNS sweeps

DNS information gathering techniques are documenting in detail with working examples in a Matta white paper titled “Using DNS to Effectively Map Networks”, available from the Matta web site at http://www.trustmatta.com/services/courses.htm

Names Gleaned From Standard Forward DNS Requests

IP Address	Resolved Hostname	Notes
198.81.129.193	relay1.ucia.gov	Authoritative DNS server
198.81.129.194	relay2.ucia.gov	Mail exchanger for ucia.gov & odci.gov
198.81.129.100	www.odci.gov	ODCI web server

Names Gleaned From Zone Transfers

IP Address	Resolved Hostname	Notes
198.81.129.100	www.odci.gov	ODCI web server
198.81.129.101	www2.cia.gov	CIA second web server
192.168.64.2	ain-relay1-hme1.ucia.gov	Internal IP address for relay1
198.81.129.193	ain-relay1-hme0.ucia.gov	External IP address for relay1
192.168.64.3	ain-relay2-hme1.ucia.gov	Internal IP address for relay2
198.81.129.194	ain-relay2-hme0.ucia.gov	External IP address for relay2
198.81.129.163	ain-relay4-hme1.ucia.gov	
198.81.129.195	ain-relay4-hme0.ucia.gov	
198.81.129.222	ex-rtr-129.ucia.gov	Cisco 4000 Router, NP-1E Board
192.103.66.58	ex-rtr-191-a	ANS.NET router interface
192.103.66.62	ex-rtr-191-b	ANS.NET router interface
198.81.129.230	res.odci.gov	ODCI resource web server
198.81.129.231	comm.cia.gov	
198.81.189.3	dialbox0.net.ucia.gov	

Names Gleaned From Reverse DNS Sweeps

IP Address	Resolved Hostname	Notes
198.81.129.100	www.odci.gov	ODCI web server
198.81.129.101	www2.cia.gov	CIA web server
198.81.129.163	ain-relay4-hme1.ucia.gov	
198.81.129.193	relay1.ucia.gov	Authoritative DNS server
198.81.129.194	relay2.ucia.gov	Mail exchanger for ucia.gov & odci.gov
198.81.129.195	relay4.ucia.gov	
198.81.129.222	ex-rtr-129.ucia.gov	
198.81.129.230	res.odci.gov	ODCI resource web server
198.81.129.231	comm.cia.gov	
198.81.189.3	dialbox0.net.ucia.gov	

Sub-domains Identified

The following sub-domains of ucia.gov and odci.gov were identified, although in most cases, no hosts were found to be referenced to by the CIA's Internet-based DNS server (relay1.ucia.gov) –

- net.ucia.gov
- iron.ucia.gov
- amino.ucia.gov
- lemur.ucia.gov
- foia.ucia.gov
- tonic.ucia.gov
- iodine.ucia.gov

- nro.odci.gov
- nic.odci.gov

Analysis of Information Gathered Thus Far

From performing WHOIS querying, combined with DNS network mapping techniques, the following useful information is known –

- The relay1, relay2 & relay4 mail and DNS servers are most probably running Solaris (as 'hme' device names are used under Solaris for network interfaces).
- The relay1 and relay2 servers seem to be dual-homed, existing both on the Internet and internal 192.168.64.0 address space.
- An HINFO record exists for ex-rtr-129, telling us that the interface is an NP1E board of a Cisco 4000 series router.
- ANS.NET is (or was) used by the CIA to provide Internet connectivity.

Gathering Intelligence by Using Search Engines

Search engines provide a good way of gathering and sieving through a lot of information. It was the case that many government and military websites used to publicly present sensitive information regarding networks and operations, which was addressed by the NSA and other agencies in a joint effort to remove sensitive content from publicly accessible web servers.

In this instance, we used Google's search engine at http://www.google.com, to enumerate CIA personnel, office locations and telephone numbers –

Name	E-Mail	Telephone / Fax
Steve Argubright	stephfa@ucia.gov	703-874-4073, 703-874-5844 (fax)
Dennis Taylor	dennigt@ucia.gov	703-874-3268
Paul Vick	paulwv@ucia.gov	703-874-4078
Richard Corliss	richaac@ucia.gov	
Richard Hawkey	richaah@ucia.gov	703-874-4510
Greg Fraser	gregolf1@ucia.gov	703-874-8051
Angela Coppola	angela@ucia.gov	703-281-8015
Particia LeMay	patridl@ucia.gov	703-874-8158
John Young	johnpy@ucia.gov	703-874-2361, 703-874-0679 (fax)
David Farnham	davef@ucia.gov	703-874-2871
Bo Tumasz	henryt@ucia.gov	703-874-8521, 703-874-8165 (fax)
David Wheelock	davidw@ucia.gov	703-613-9840
Ken Stiles	kens@ucia.gov	703-874-4063
Les Davis	leslied@ucia.gov	703-874-0284, 703-874-5393 (fax)
John Dahms	johnpd@ucia.gov	703-482-8510, 703-482-8361 (fax)
Jenny Gregory	jennysg@ucia.gov	703-482-9354, 703-482-4821 (fax)
James Honeywell	jamesah@ucia.gov	703-281-8973, 703-938-4692 (fax)
Jonathan Kaplan	jonathk@ucia.gov	703-874-8212
Thomas Knoerzer	thomack@ucia.gov	703-482-0166, 703-482-9423 (fax)
Joseph Schneider	josepms1@ucia.gov	703-482-7572, 703-482-9423 (fax)
Bobby Sumner	roberas1@ucia.gov	703-482-9500, 703-482-4821 (fax)
Carol Neal		703-874-4260, 703-874-7282 (fax)
John Vasko	johnjv0@ucia.gov	703-482-1171
Tom Tamaccio	thomact@ucia.gov	703-482-7078
Jo Ann Murphy	joanm@ucia.gov	703-482-7080

Name	E-Mail	Telephone / Fax
Richard Schroeder	richaes@ucia.gov	703-605-6000
Mark MacDonald	markmz@ucia.gov	703-482-8790, 703-482-3705 (fax)
David Gordon	davidfg@ucia.gov	703-482-4128
Vanessa Ibsch	vanesli@ucia.gov	703-482-6081
Robert Sutter	robertgs@ucia.gov	703-482-3213, 703-482-8632 (fax)
Jeana Bissonnette	jbisson4@hotmail.com	703-874-4055, 703-874-4041 (fax)
Trent Wise	trentw@odci.gov	703-482-1100
Sam Herod	samueph@odci.gov	703-874-8267
Gordon Oehler	gordon@iron.ucia.gov	703-874-3030, 703-874-3076 (fax)
Huri Fraley	hurif@iron.ucia.gov	703-874-7709
Suzie Santos	suzies@iron.ucia.gov	
CIA Recruitment	recruit@lemur.ucia.gov	
John P	johnp@istac.gov	
Dan S	dan@istac.gov	703-281-8087

Main switchboard and departmental telephone numbers were also enumerated easily –

Department	Telephone Number
Personnel	800-562-7242
Office of Public Affairs	703-482-0623, 703-482-1739 (fax)
Main Switchboard	703-482-1000, 703-482-6790 (fax)
Office of the Director of the CIA	703-482-1100
Advisory Council	703-722-5970 (tty)
Employee Resource & Information	703-482-9170 (tty)
Office of EEO (Arlington)	703-351-2316 (tty)
Office of EEO (Washington)	703-874-4457 (tty)
Office of Training & Education	703-351-2338 (tty)
DO / IMS	703-482-1171, 703-482-3458 (fax)
IMS Division	703-613-1705, 703-218-8954 (fax)
Advanced Analytic Tools	703-281-8015
National Counterintelligence Executive (fax)	703-874-4122, 703-874-5844, 703-874-0271
Office of Facilities Management	703-874-4800, 703-874-4975 (fax)
Professional Services Branch	703-482-3675, 703-448-9782 (fax)
FOIA & Privacy Coordinator	703-613-1287
Office of Medical Services	703-482-3676
Crime and Narcotics Center	703-874-4610
Office of the General Counsel	703-874-3207, 703-874-3208 (fax)
Office of the Inspector General	703-874-2600
Office of Student Programs	703-281-8365
NACIC Threat Assessment Office	703-874-4119, 703-874-5844 (fax)

Telephone numbers harvested in this fashion can be used by a determined attacker to locate devices that may allow for access to internal CIA network space. 'Wardialing' is a common threat to many organisations nowadays, as Internet-based security is improved, other routes to sensitive information are followed.

Analysis of E-Mail System Errors

Internal network information can easily be gleaned and analysed by determined attackers to grasp an insight of internal network structure. In this instance, we sent bogus e-mail to non-existent users at ucia.gov and odci.gov. Below are the responses from the e-mail systems at these networks –

blahblah@ucia.gov

```
The original message was received at Fri, 1 Mar 2002 07:42:48 -0500 (EST)
from ain-relay2.net.ucia.gov [192.168.64.3]

   ----- The following addresses had permanent fatal errors -----
<blahblah@ucia.gov>

   ----- Transcript of session follows -----
... while talking to mailhub.ucia.gov:
>>> RCPT To:<blahblah@ucia.gov>
<<< 550 5.1.1 <blahblah@ucia.gov>... User unknown
550 <blahblah@ucia.gov>... User unknown

   ----- Original message follows -----

Return-Path: <info@trustmatta.com>
Received: from relay2.net.ucia.gov
        by puff.ucia.gov (8.8.8+Sun/ucia internal v1.35 (complaints to
postmaster@ucia.gov))
        with SMTP id HAA29202; Fri, 1 Mar 2002 07:42:48 -0500 (EST) sender
info@trustmatta.com for <blahblah@ucia.gov>
Received: by relay2.net.ucia.gov; id HAA26766; Fri, 1 Mar 2002 07:39:18 -0500
Received: from mail.trustmatta.com(213.239.14.106) by relay2.net.ucia.gov via
smap (4.1)
        id xma026449; Fri, 1 Mar 02 07:38:55 -0500
```

blahblah@odci.gov

```
Final-Recipient: rfc822;blahblah@odci.gov
Action: failed
Status: 5.1.1
Diagnostic-Code: X-Notes; User blahblah (blahblah@odci.gov) not listed in
public Name & Address Book
Received: from puff.ucia.gov ([198.81.128.66])
          by maryland.odci.gov (Lotus Domino Release 5.0.6a)
          with ESMTP id 2002030107465793:18563 ;
          Fri, 1 Mar 2002 07:46:57 -0500
Received: from relay2.net.ucia.gov
        by puff.ucia.gov (8.8.8+Sun/ucia internal v1.35 (complaints to
postmaster@ucia.gov))
        with SMTP id HAA29278; Fri, 1 Mar 2002 07:46:47 -0500 (EST) sender
info@trustmatta.com for <blahblah@odci.gov>
Received: by relay2.net.ucia.gov; id HAA28786; Fri, 1 Mar 2002 07:43:18 -0500
Received: from mail.trustmatta.com(213.239.14.106) by relay2.net.ucia.gov via
smap (4.1)
        id xma028643; Fri, 1 Mar 02 07:43:03 –0500
```

Analysis of Web Servers

Using Netcraft's web server analysis tools at http://www.netcraft.com, determined attackers can covertly find out the platform that a web server is running on, along with other potentially interesting information (including other web servers in the same network block).

From visiting Netcraft's site, we found that both www.odci.gov and www.cia.gov were running Netscape Enterprise 4.1 on Solaris 8 –

http://uptime.netcraft.com/up/graph?mode_u=off&mode_w=on&site=www.odci.gov
http://uptime.netcraft.com/up/graph?mode_u=on&mode_w=on&site=www.cia.gov

Bringing Everything Together

From these open sources, we are now able to build a clear network map. The information is probably not entirely correct, as we are not authorised to perform network scanning and probing to verify the existence and accessibility of specific hosts and networks, however it should certainly be an eye-opener to the open source information that can be used to map networks and perform counterintelligence.

If the map is not clearly viewable in this PDF format, you can download it as a JPEG image from http://www.trustmatta.com/services/docs/cia-map.jpg

Matta is a fiercely independent information risk management firm, specialising in true IRM through talking to clients and identifying key business drivers and information assets. Matta actively runs skills transfer and training programmes for many of it's clients, including banks and financial companies, for more information about our skills transfer services, please visit http://www.trustmatta.com/services/courses.htm, where you will also find more freely available white papers.

Alternatively, Matta consultants are available at –

Matta Security Limited
16 – 19 Southampton Place
London WC1A 2AX

+44 (0) 8700 77 11 00

info@trustmatta.com

http://www.trustmatta.com

The network map has been removed from this document to take the file size down from 500k to something a little more reasonable – due to load on our web server.

You can download the map from http://www.trustmatta.com/services/docs/cia-map.jpg

Thanks

The Matta Attack & Penetration Team