MIRcon 2014

Did You Check the Packet?
Using Full Packet Capture to Enhance Incident Response

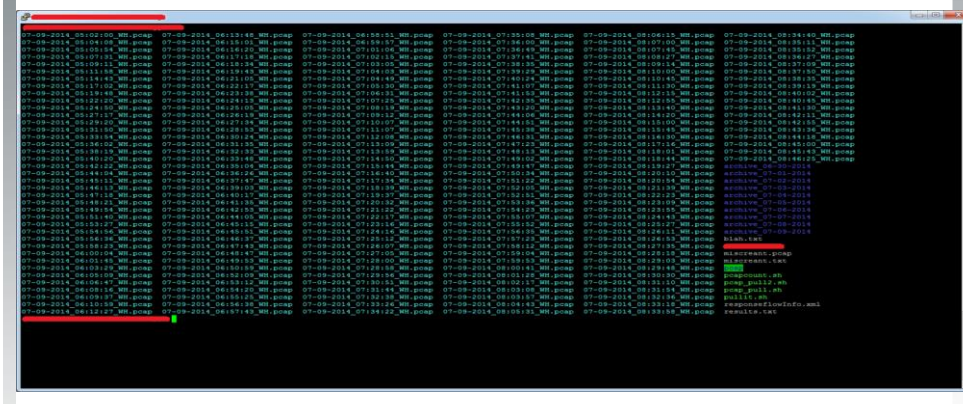
Ron Stamper
Cyber Security Engineer
Regions Bank

Table of Contents

Teach a man to fish…..

- This presentation will provide a brief crash dump on what a PCAP is and the power that can be leveraged in parsing packets at the raw ASCII text level and the tools you can create around such data.
- Quick Case Study examples will be shown how to leverage the data using nPulse, nSpector and FireEye and third party tools and SIEM solutions.
- The presentation will hopefully make sense taken as the sum of the whole.
- Please raise any questions at the end or see me in person.

PCAPs: Using daemonlogger



PCAPs: Use the proper TCPDUMP syntax

- tcpdump -r <file> -Anns0 | less
  - -r ➔ read a file
  - -A ➔ Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.
  - -nn ➔ Don't convert host addresses, protocol, or port numbers etc. to names. This can be used to avoid DNS lookups.
  - -s0 ➔ For backwards compatibility with older versions of tcpdump, sets snaplength to default of MAX
- tcpdump -r <file> -Anns0 host <ipaddress> | less
- tcpdump -r <file> -Anns0 src host <ipaddress> | less

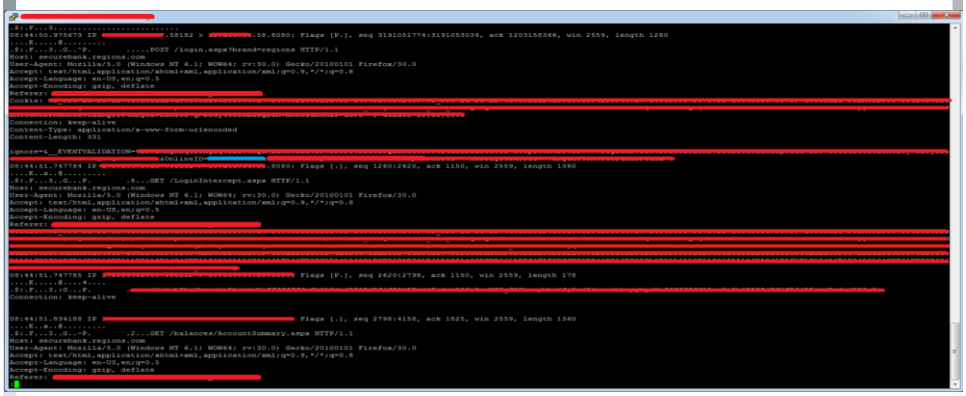
USING NPULSE TO READ RAW PCAP

```
#Enforce a minimum set of command-line arguments for success.
if [[ -z "$1" && -z "$2" ]]; then
        echo "Not enough arguments passed."
        echo 'Syntax is ./pullit.sh <HHMMSS> <IP ADDRESS> <WINDOW OPTIONAL WILL DEFAULT TO 20> or ./pullit.sh "2014-04-29 11:45:00" <IP ADDRESS> <WINDOW OPTIONAL WILL DEFAULT TO 20>'
        echo "or Syntax ./pullit.sh <IP ADDRESS> <MINUTE WINDOW/MIN OF 1>"
        echo "or Syntax ./pullit.sh <IP ADDRESS>"
        echo "or Syntax ./pullit.sh <HHMMSS> 0.0.0.0 <MINUTE WINDOW ENTER IN A 3!!> (will give you ALL traffic for the time specified! CAN GET VERY LARGE!)"
        exit 0
fi

if [[ -z "$3" ]]; then

if [[ -z "$2" ]]; then
echo "Window VALUE NOT DETECTED USING 20 MINUTE WINDOW!"
let WINDOW=20*60

if [ ${#1} -gt 6 ]; then
        echo "NO DATE ENTERED USING NOW!"
        curl -k --user packetreader:password -o /tmp/output2.txt -y 35 -Y 1 "https://X.X.X.X/api/4.0/search/stream?stime=now&window=$WINDOW&limit=0&ip_list=$1&vpf=host%20$1"
        tshark -r /tmp/output2.txt -w /tmp/converted2.pcap
        tcpdump -r /tmp/converted2.pcap -Anns0 "src host $1 or (vlan and src host $1)"
        exit 0
fi
fi
```

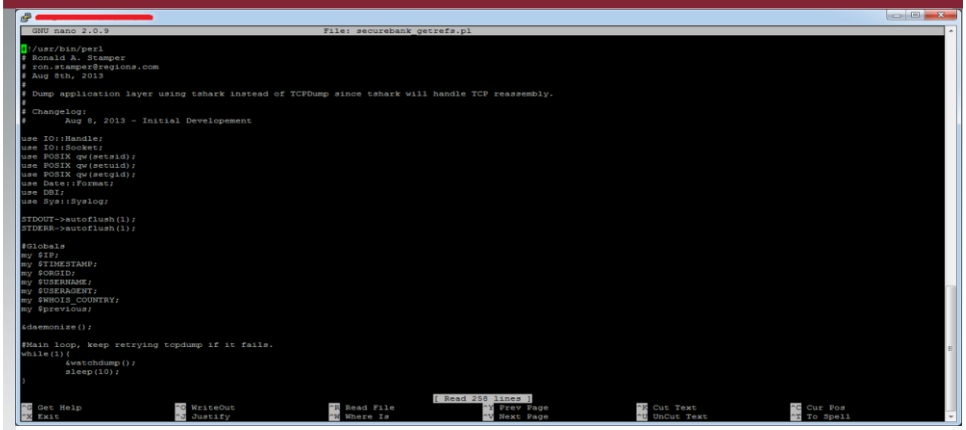
NPULSE API COMMAND ZOOMED IN

- if [${#1} -gt 6]; then
- echo "NO DATE ENTERED USING NOW!"
- curl -k --user packetreader:readthempackets -o /tmp/output2.txt -y 35 -Y 1 "https://X.X.X.X/api/4.0/search/stream?stime=now&window=$WINDOW&limit=0&ip_list=$1&xpf=host%20$1"
- tshark -r /tmp/output2.txt -w /tmp/converted2.pcap
- tcpdump -r /tmp/converted2.pcap -Anns0 "src host $1 or (vlan and src host $1)"
- exit 0
- fi

PCAPs: Lots of information can be had



PCAPs: Perl script black magic



PCAPs: Using PIPE to stdoutput

PERL ZOOMED IN <PIPE COMMAND>

- my $tcpdump = "/usr/local/bin/tshark -t ad -l -d 'tcp.port==8080,http' -i bondRef -R 'lower(http.request.uri)==\"/login.aspx\" or
- lower(http.request.uri)==\"/blahblah.url\"' -n -V 2>/dev/null";

- open(PIPE,"$tcpdump|");
- while(<PIPE>){ #START THE WHILE LOOP

- #print LOG3 "$_";
- if ($_ =~ m/\s+Arrival Time: [A-Za-z]{3}\s+\d+, \d+ (\d+:\d+:\d+)\.\d+/){ blah blah } elseif ($_ =~ blah blah){

PCAPs: TShark command

```
      #Non-PCRE URI match, faster than PCRE by about 15% CPU utilization.
      my $tcpdump = "/usr/local/bin/tshark -t ad -l -d 'tcp.port==8080,http' -i bondRef -R 'lower(http.request.uri)==\"/login.aspx\"
or http.request.uri==\"/\"
or lower(http.request.uri)==\"/login.aspx?brand=regions\" or http.request.uri==\"/\" or lower(http.request.uri)==\"[redacted]"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]"
or lower(http.request.uri)==\"/customerlogin.aspx\" or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"/[redacted]"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"/[redacted]"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"/wcmfd/wcmpw/customerlogin\"
or lower(http.request.uri)==\"[redacted]" or lower(http.request.uri)==\"[redacted]\"' -n -V 2>/dev/null";
```

PCAPs: Regex match the text

- }elsif($_ =~ m/Internet Protocol Version 4, Src: (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}) /){
- $IP = "$1";
- }elsif($_ =~ m/\s+POST \s?(.*)HTTP/){
- $URL = "$1"; $METHOD = "2";
- }elsif($_ =~ m/\s+GET \s?(.*)HTTP/){
- $URL = "$1"; $METHOD = “1";
- }elsif($_ =~ m/\s+User-Agent:\s?(.*)/i){
- $USERAGENT = "$1";

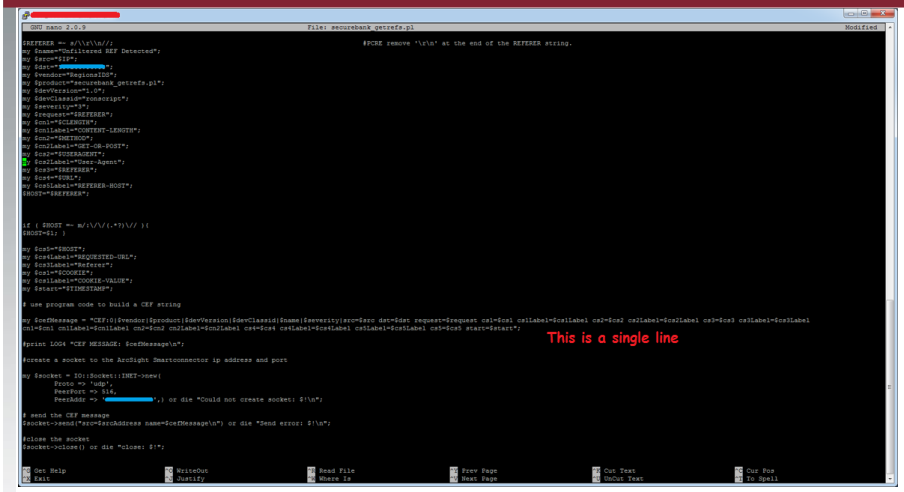
URL: What can I do with the URL?

- Use Script to check URL against 4 letter word list when URL is above 15 characters. Ie like www.microsoft.com
- Use Script to check age of Domain name using WHOIS. Less than 30 days old its bad.
- Check URL against intel lists.
- Generate CEF Message to Arcsight (or SIEM) or have script issue a direct BAN.

PCAPs: Populating a database

```
#DBI Handler for MySQL
    my $dbh = DBI->connect("dbi:mysql:DBNAME:IP:3306", "username", "password") or die "Cannot connect to the MySQL Database";
    $dbh->{mysql_auto_reconnect} = 1;
    $dbh->{'AutoCommit'} = 1;

#SQL INSERT into MySQL DB, using $dbh->quote() to escape strings for potential SQL-injection.
    my $SQL = "INSERT HIGH_PRIORITY INTO PAGE_REFS(TIMESTAMP,IP,CLENGTH,COOKIE,COUNTRY,USERAGENT,REFERER,URL,METHOD) VALUES (" . $dbh->quote($TIMESTAMP) . "," .$dbh->quote($IP) . "," . $db$blah blah blah

                #Logging FPs
                open LOG4, ">>", "/tmp/securebank_getrefs" . strftime("%Y-%m-%d",@lt) . ".mysql_output4";

                #Commit and log the changes to the DB
                #print LOG4 "$SQL\n";

                my $sth = $dbh->prepare($SQL) or print LOG4 "\t*** ERROR: " . $dbh->errstr . " ***\n";

                if ( $sth->execute() ){
                    #print LOG4 "\t*** Insert OK ***\n";
                } else {
                    print LOG4 "\t*** ERROR: " . $sth->errstr . " ***\n";
                }

                $sth->finish();
```

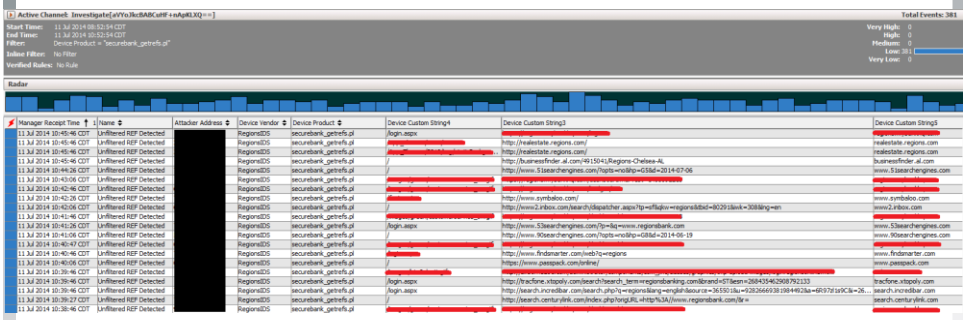

PCAPs: Create a CEF message



Use Case: Phishing

- Send referrer URLs to SmartConnector
  - Send the requested URL in addition to referrer URL
  - Use customString, not requestUrl
  - Extract at least FQDN to customString, can be done by pre-processing to send CEF or implementing a FlexConnector
  - Extracting second-level domain into the ArcSight event is better for whitelisting than FQDN
- Note any files being requested from your site by external referrers
- Build rule to notify your internal/external phishing team based on external requests to these resources
- Adding new phish to an ActiveList can allow a simple way to know both the first and most recent time a phish was seen
- Advanced Mode: use additional heuristics, such as content retrieval or automated processing by external partner

Use Case: Phishing

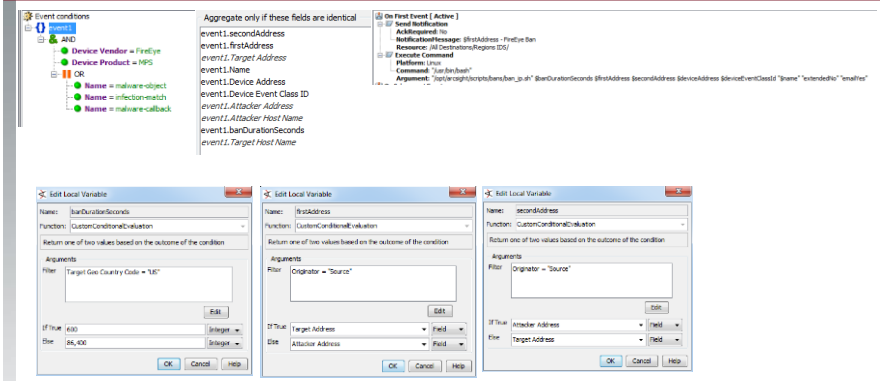


Use Case: Auto Incident Creation using PCAP Data and rules.

- First-stage rule triggers on IDS event, calls an external bash script
- Bash script uses lynx to POST data to external system for processing
- External system performs actions
  - Lookup in local database
  - Retrieve information from raw PCAP
- Returns CEF event with most or all of first_stage event, plus enrichment data in customString and customNumber fields
- Second-stage rules handle this second_stage event. Could be multiple rules or just one depending on Use Case
- What if the second_stage event never arrives?
  - In first_stage event, add eventId to a fields-based ActiveList with a low TTL (5 minutes)
  - Pass eventId to external system
  - External system returns first_stage's eventId as part of second_stage event as customNumber
  - In any rule that handles second_stage events, remove the eventId from the above ActiveList
  - If any event expires from ActiveList (deviceEventClassId=activelist:104), send a notification

Use Case: Fraud Detection with PCAPs

Use Case: FireEye Malware Response



Bonus Ideas: Populate Pcap Login Userid's into a database

Ignore logins originating from the United States (US)

Search for idstest in UserID since Today ordering by Date/Time DESC and group by Do Not Group

Search Clear Results

A arbitrary hard-limit of 1000 max records has been imposed, no more than 1000 records will be returned

Notes Regarding Object USERNAME for 'idstest' last updated never

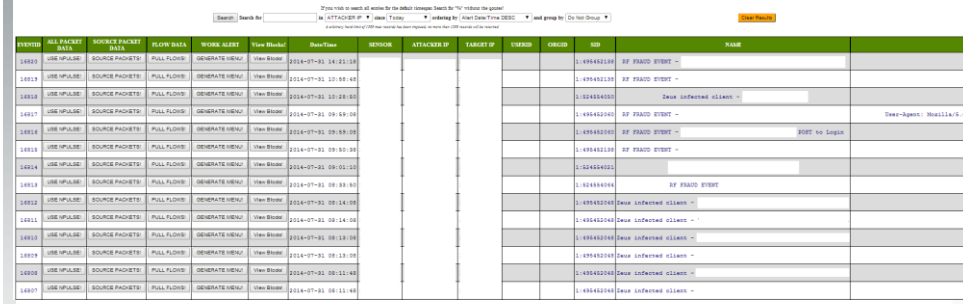
8 Jul 2014 13:48:50 CDT USER: idstest MALWARE INFECTION AUTO GENERATION IP: 205.255.224.99 USING UA: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0

Update Notes

NPULSE TXT	SOURCE PACKETS	Date/Time	IP Address	Country	User ID	CLENGTH	User-Agent Expand All UAs AND REFERER	REFERER
USE NPULSE	SOURCE PACKET	2014-07-10 17:20:12	205.255.224.99	United States (US)	idstest	171	686; rv:10.0.11) Gecko/2012112	https://securebank.regions.com

1 total records found matching the specified search criteria

Bonus Ideas: Populate incident database use nPulse API to pull packets at a button click.



PHP Code for pull pcap function (page 1/3)

```
elseif ($ACTIONTODO=="npulsepull")
{
$window=$window*60;


$command="https://X.X.X.X/api/4.0/search/stream?stime=$newetime0&window=$window&limit=0&ip_list=$AIP&xpf=host%20$AIP";

if ($searchon=="attandtar")
{
    if (isset($_GET["PTIME"]))
    {
        $ptime=trim($_GET["PTIME"]);
        $command="https://X.X.X.X/api/4.0/search/stream?stime=$ptime&window=$window&limit=0&ip_list=$AIP&xpf=host%20$AIP%20and%20host%20$TIP";
    }
                else
                {
                $command="https://X.X.X.X/api/4.0/search/stream?stime=$newetime0&window=$window&limit=0&ip_list=$AIP&xpf=host%20$AIP%20and%20host%20$TIP";
    }
}

$getfile=`curl -k --user username:password -o /var/www/html/itres/convert/"$random".data.txt -y 45 -Y 1 "$command"`;
$writeoutpcap=`tshark -r /var/www/html/itres/convert/"$random".data.txt -w /var/www/html/itres/convert/"$random".data.pcap`;

$storepcap="/var/www/html/itres/convert/$random.data.pcap.txt";
#file_put_contents($storepcap, utf8_encode($data));
```

PHP Code for pull pcap function (page 2/3)

```
#New write out pcap data

if (isset($_GET["FSOURCE"]))
{
$writepcaptxt=`tcpdump -r /var/www/html/itres/convert/"$random".data.pcap -Anns0 "src host $AIP or (vlan and src host $AIP)" > "$storepcap"`;
}
else
{
$writepcaptxt=`tcpdump -r /var/www/html/itres/convert/"$random".data.pcap -Anns0 > "$storepcap"`;
}

echo "<br>";
echo "Download PCAP: <a href=https://X.X.X.X/itres/convert/$random.data.pcap>Click to download PCAP!</a>";
echo "<br>View PCAP via HTTPS: <a href=https://X.X.X.X/itres/convert/$random.data.pcap.txt>Click to view PCAP as TXT</a>";
echo "<br><br>";

if ((!($_GET['BB']=="1"))&&(!($_GET['BB']=="2")))
{
?>
<br>
<iframe src="http://X.X.X.X:8000/itres/convert/<?php echo "$random.data.pcap.txt"?>" width="100%" height="600px"></iframe>
<?php
}
elseif ($_GET['BB']=="1")
{
?>
```


PHP Code for pull pcap function (page 3/3)

```
<script>
function Redirect(url)
{
 location.href = url;
}

Redirect ("<?php echo "http://X.X.X.X:8000/itres/convert/$random.data.pcap.txt"; ?>");
</script>
<?php
}
elseif ($_GET['BB']=="2")
{
?>
<script>
function Redirect(url)
{
 location.href = url;
}

Redirect ("<?php echo "https://X.X.X.X/itres/convert/$random.data.pcap.txt"; ?>");
</script>
<?php
}

}
```

Bonus Ideas: nPulse PHP function result

Leverage FireEye and MD5 feeds for nSpector to crush malware.

- nSpector can generate an MD5 feed that can be incorporated into a SIEM solution such as ArcSight that can be used to populate an Active List of all files propagating the network.
- Bad MD5 hash can be further read into the SIEM using third party tools and intel feeds such as FireEye Malware detection events.
- All instances of flagged files can be found in nSpector or using the data provided by nSpector in your SIEM.
- Correlate third party host tools to provide seen on host MD5 feeds into SIEM, auto detonate past finds!!

Using nSpector to farm on flagged MD5's

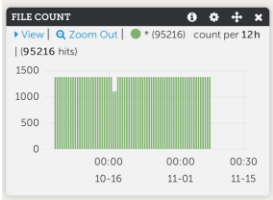
FLOW DATA

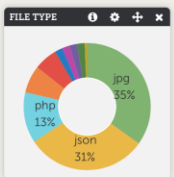
0 to 100 of 500 available for paging

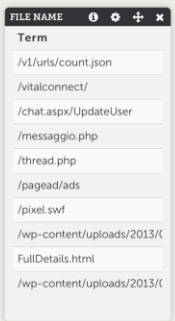
@timestamp	destinationIPAddress	sourceIPAddress	filename	fileMD5	fileMagic	appType	destinationTransportP
2013-10-04T00:03:36.000Z	208.76.12.4	69.164.223.203	/wp-content/uploads/2013/07...		PNG image data, 550 x 87, 8...	80	36148
2013-10-04T00:03:39.000Z	208.76.12.4	69.164.223.203	/share_facebook.png	d494707823bf19afaa3bc392c50...	PNG image data, 50 x 17, 8-...	80	36149
2013-10-04T00:04:35.000Z	208.76.12.4	69.164.223.203	/wp-content/uploads/2013/07...	255284300ad8944d53bc03d9880...	JPEG image data, JFIF stand...	80	36150
2013-10-04T00:04:51.000Z	208.76.12.4	69.164.223.203	/wp-content/uploads/2013/07...	987ef1cd438e3747b509d454e56...	JPEG image data, JFIF stand...	80	36151
2013-10-04T00:05:00.000Z	208.76.12.4	69.164.223.203	/wp-content/uploads/2013/07...	9dbc1aeca8f5e3bf084b5e50408...	JPEG image data, JFIF stand...	80	36152
2013-10-04T00:06:20.000Z	208.76.12.4	199.189.107.150	/chat.aspx/UpdateUser	76220e838f77a2d0f46d288fa80...	ASCII text, with no line te...	80	52018

Using nSpector find all files matching MD5

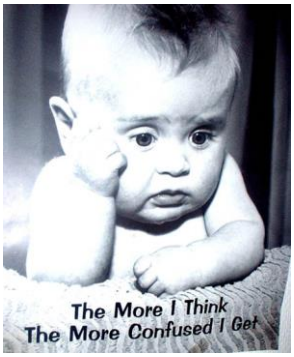
- Search all instances of files identified as malware by FireEye on your network if you feed nSpector full core VLAN switch traffic







Questions????



- Ron Stamper – ron.stamper@regions.com (Engineer – aka the real worker)
- Don Turrentine – don.turrentine@regions.com (VP of IDS – aka meeting monkey)