

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Use Anomalies to Detect Advanced Attacks Before Bad Guys Use It Against You

SESSION ID: SPO2-T09

Alexander Watson

Director of Security Research
Websense Labs





DONALD RUMSFELD...

“There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know.

But there are also unknown unknowns. There are things we don't know we don't know.”

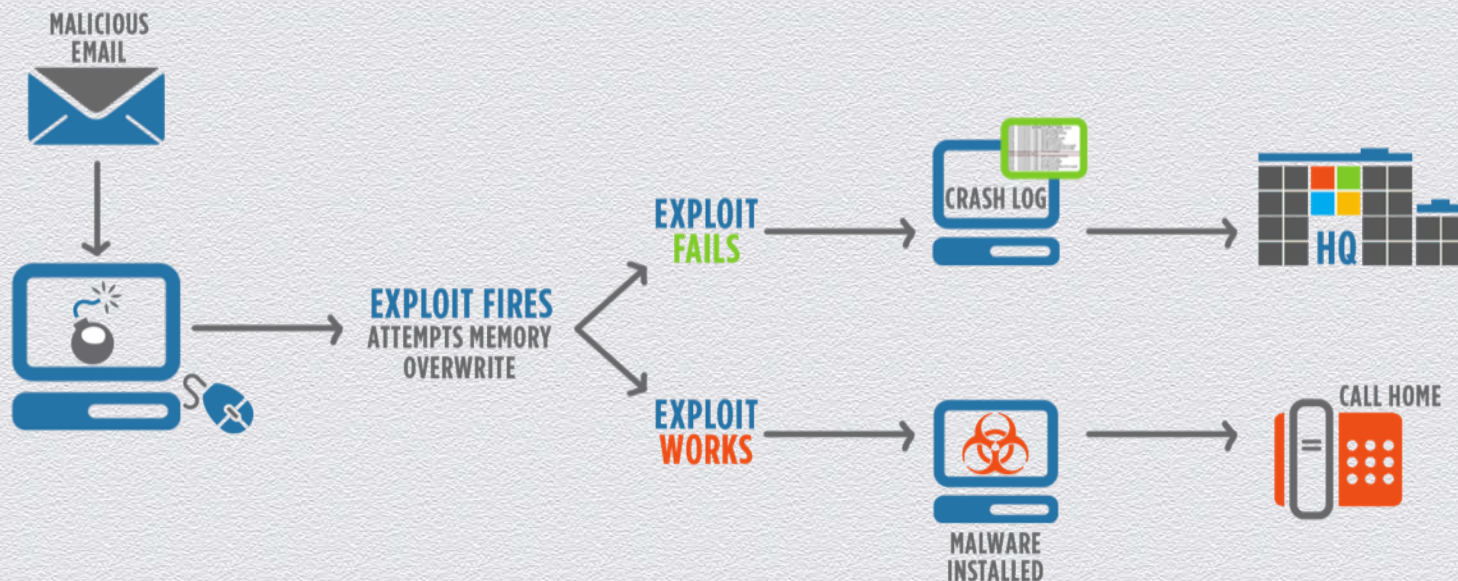


**How can we detect and provide
visibility into attacks that have made
it past organizations defenses?**

**Existing cyber security systems
are based on expert knowledge driving
analytics and signature-based defenses.
Really.**

**THIS APPROACH IS NOT SUFFICIENT
TO STOP TARGETED ATTACKS.**

EVEN THE MOST ADVANCED CYBER ATTACKS CREATE ANOMALIES IN NETWORK AND APPLICATION BEHAVIOR



**What if we could search
for anomalies in application
crash reports that are indicators
of attack activity?**



THERE ARE SEVERAL STAGES OF AN ATTACK
WHERE ATTACKERS ARE MORE LIKELY TO
CRASH APPLICATIONS ON THE NETWORK



Courtesy United Artists™ 1995



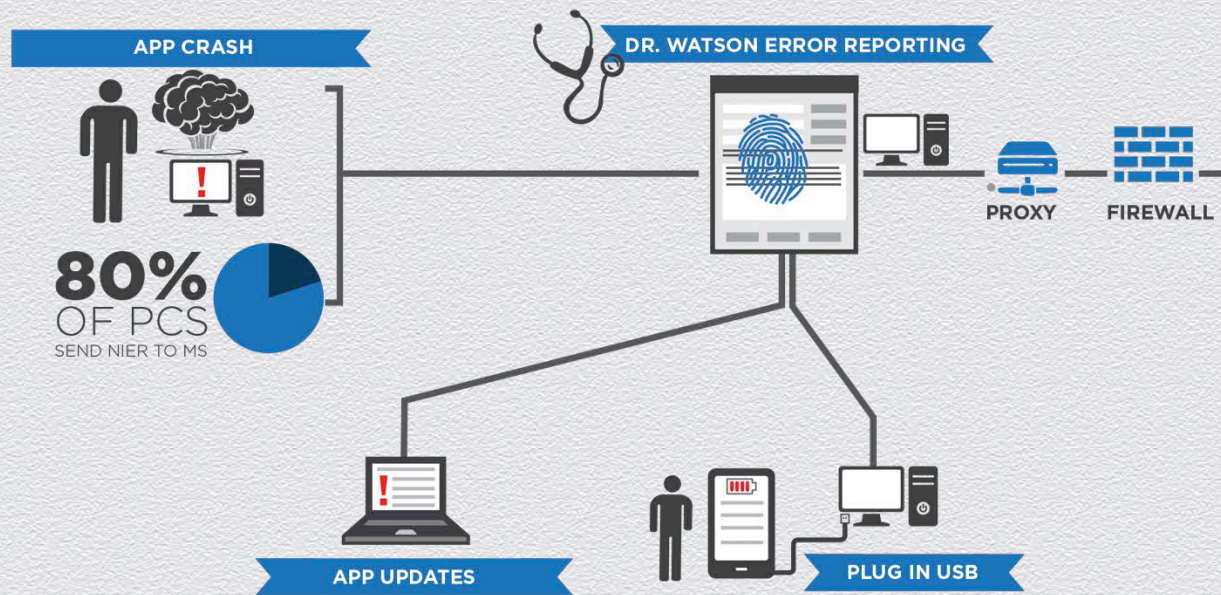
Courtesy United Artists™ 1995



Courtesy United Artists™ 1995

HOW ARE MICROSOFT WINDOWS ERROR REPORTS GENERATED?

MICROSOFT
RECEIVES BILLIONS
EACH YEAR



WHY WINDOWS ERROR REPORTING (WER)?

80 % of all network-connected PCs use WER — more than one billion endpoints worldwide.

16 million **CRASH
REPORTS**



OVER A 4 MONTH WINDOW

CRASHING APPLICATION CRASHING APPLICATION VERSION:

Chrome

27.0.1453.116

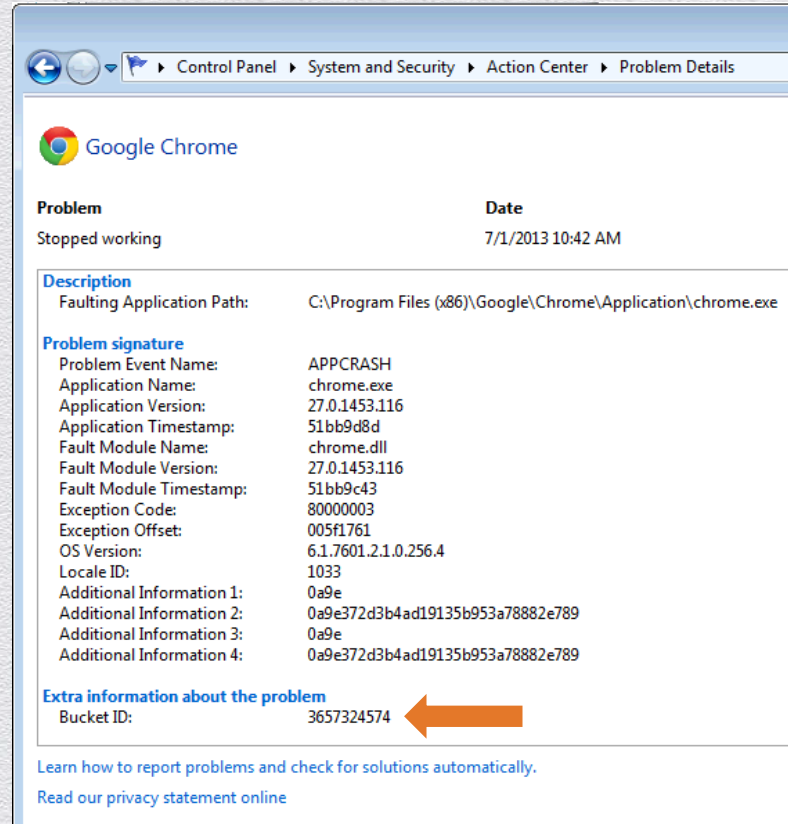
http://watson.microsoft.com/StageOne/chrome_exe/27_0_1453_116/51bb9d8d/chrome_dll/27_0_1453_116/51bb9c43/c0000005/005f1761.htm?LCID=1033&OS=6.1.7601.2.00010300.1.0.3.17514&SM=Acer&SPN=Aspire%20M3970&BV=P01-A3&MRK=1025_ACER_ACER_AM1930&MID=0513D3D-CBA4-2339-9ABC-ABCDEFABCDEF

WHAT EXACTLY IS THE “CRASH OFFSET”?

The screenshot displays a multi-windowed environment for crash analysis:


- Wireshark:** Shows a packet capture of an HTTP GET request. The packet list pane highlights a packet with a red box around the offset `00079A22` in the stream content.
- WinDbg:** The "Exception" window shows a crash with the exception code `0xC0000005` (AccessViolation). The "Exception Address" field is highlighted with a red box and labeled with a red '1', showing the value `7DCA9A22`.
- Calculator:** The "Hex" view shows the address `7DCA9A22` entered into the input field, labeled with a red '4'.
- Module List:** The "Module List" window shows the loaded modules. The module `C:\WINDOWS\system32\mshtml.dll` is highlighted with a red box and labeled with a red '2'. The "Image base" for this module is `7DCA0000`.
- Stream Content:** The "Follow TCP Stream" window shows the raw data of the HTTP request, with the offset `00079A22` highlighted by a red box and labeled with a red '3'.

EXAMPLE: GOOGLE CHROME CRASH REPORT TO WATSON



The screenshot shows a Windows Control Panel window titled "Control Panel > System and Security > Action Center > Problem Details". The window displays a Google Chrome problem report. The problem is titled "Google Chrome" and is described as "Stopped working" on "7/1/2013 10:42 AM". The "Description" section shows the "Faulting Application Path" as "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe". The "Problem signature" section lists various details: Problem Event Name (APPCRASH), Application Name (chrome.exe), Application Version (27.0.1453.116), Application Timestamp (51bb9d8d), Fault Module Name (chrome.dll), Fault Module Version (27.0.1453.116), Fault Module Timestamp (51bb9c43), Exception Code (80000003), Exception Offset (005f1761), OS Version (6.1.7601.2.1.0.256.4), Locale ID (1033), and four additional information items (0a9e, 0a9e372d3b4ad19135b953a78882e789, 0a9e, 0a9e372d3b4ad19135b953a78882e789). The "Extra information about the problem" section shows the "Bucket ID" as "3657324574", which is highlighted by an orange arrow. At the bottom, there are links to "Learn how to report problems and check for solutions automatically" and "Read our privacy statement online".

Control Panel > System and Security > Action Center > Problem Details

 Google Chrome

Problem	Date
Stopped working	7/1/2013 10:42 AM

Description

Faulting Application Path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Problem signature

Problem Event Name: APPCRASH
Application Name: chrome.exe
Application Version: 27.0.1453.116
Application Timestamp: 51bb9d8d
Fault Module Name: chrome.dll
Fault Module Version: 27.0.1453.116
Fault Module Timestamp: 51bb9c43
Exception Code: 80000003
Exception Offset: 005f1761
OS Version: 6.1.7601.2.1.0.256.4
Locale ID: 1033
Additional Information 1: 0a9e
Additional Information 2: 0a9e372d3b4ad19135b953a78882e789
Additional Information 3: 0a9e
Additional Information 4: 0a9e372d3b4ad19135b953a78882e789

Extra information about the problem

Bucket ID: 3657324574

[Learn how to report problems and check for solutions automatically.](#)
[Read our privacy statement online](#)

The background of the slide is light blue with a pattern of white and light blue circuit-like lines. These lines are more prominent in the corners, forming a border around the central text area.

**WE CAN USE THESE CRASH REPORTS
TO DETECT MALICIOUS ACTIVITY
SUCH AS EXPLOITS AND CODE INJECTION.**

RISK INDICATORS IN CRASH REPORTS

- ◆ Crashes in key applications for businesses at high risk of attack
 - ◆ SCADA, Point of Sale, Telecom, Research, etc.
- ◆ “Fingerprints” for known exploits that detect application crashes according to application version, DLL version, and crash offset locations of known CVEs.
- ◆ Temporal anomalies, or clusters of crashes isolated to a company, industry or region
- ◆ Indicators of code injection or ROP-based exploits
- ◆ Microsoft’s Bucketing Algorithm
- ◆ Unusual faulting libraries
- ◆ Crashes in widely deployed, commonly exploited applications





RSACONFERENCE**2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

PROVING IT

Creating a MSIE 0-Day
Fingerprint for CVE-2013-3893

QUESTION: WHO ELSE HAS USED THIS ZERO-DAY?

[illegible]

cap001.pcap [Wireshark 1.8.1 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply Save

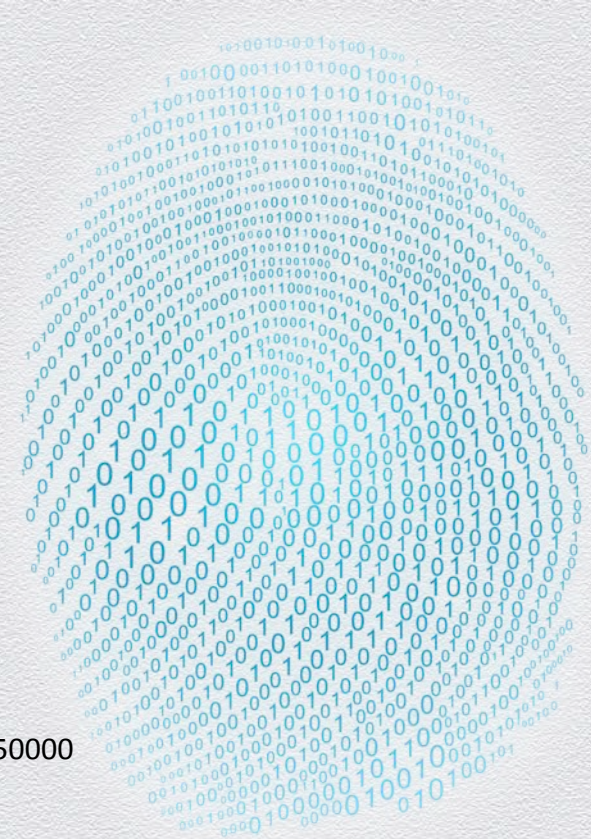
No.	Time	Source	Destination	Protocol	Length	Info
141	33.359720	192.168.179.188	192.168.179.2	DNS	78	Standard query 0xd695 A login.monoshop.org
142	33.472828	192.168.179.2	192.168.179.188	DNS	94	Standard query response 0xd695 A 210.17.236.29
151	43.544609	192.168.179.188	192.168.179.2	DNS	77	Standard query 0x4379 A crl.microsoft.com
152	43.544920	192.168.179.188	192.168.179.2	DNS	77	Standard query 0x3717 A crl.microsoft.com
153	43.556573	192.168.179.2	192.168.179.188	DNS	173	Standard query response 0x3717 CNAME crl.www.ms.akadns.net CNAME a1363.g.akamai.net A 23.62.99.122 A 23.62.99.107
155	43.561324	192.168.179.2	192.168.179.188	DNS	173	Standard query response 0x4379 CNAME crl.www.ms.akadns.net CNAME a1363.g.akamai.net A 23.62.99.107 A 23.62.99.122

REVERSING THE EXPLOIT

CREATING A CRASH FINGERPRINT

Analyze CVE-2013-3893 and searching for the location that a failed exploit would crash

```
ModLoad: 71a50000 71a8f000 C:\WINDOWS\system32\mswsock.dll
ModLoad: 662b0000 66308000 C:\WINDOWS\system32\hnetcfg.dll
ModLoad: 71a90000 71a98000 C:\WINDOWS\System32\wshtcpip.dll
Heap corruption detected at 12320000
Heap corruption detected at 12120018
Heap corruption detected at 11F20000
(228.10c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=11f20000 ebx=00000000 ecx=11420000 edx=11920000 esi=11920000 edi=00150000
eip=7c929f09 esp=015dd090 ebp=015dd14c iopl=0 nv up ei pl nz ac pe cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000eefl=00010217
ntdll!towlower+0x517:
7c929f09 3b5004c mpedx,dword ptr [eax+4] ds:0023:11f20004=????????
```



REVERSING THE EXPLOIT

CREATING A CRASH FINGERPRINT

We can find all of the information that would be included in a WER report:

THIS IS OUR FINGERPRINT!

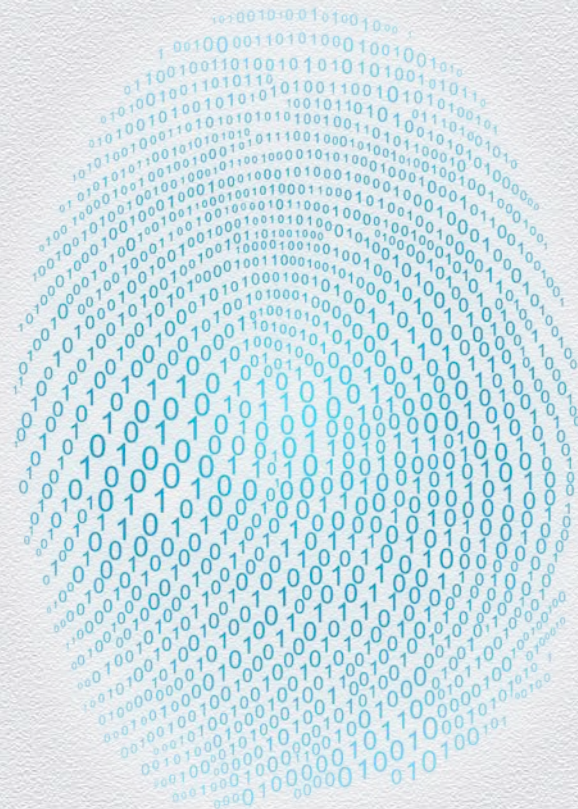
```
!analyze -v
```

```
...
```

```
PROCESS_NAME: iexplore.exe
```

```
WATSON_STAGEONE_URL:
```

```
http://watson.microsoft.com/StageOne/iexplore\_exe/8\_0\_6001\_18702/49b3ad2e/ntdll\_dll/5\_1\_2600\_6055/4d00f27d/c0000005/00029f09.htm?Retriage=1
```



OUT OF 16 MILLION REPORTS, 5 MATCHED OUR FINGERPRINT

Tier-1 Mobile Network Operator

Industry: Telecommunications

Date: 12-16-2013

Crash 12-10-2013 URL:

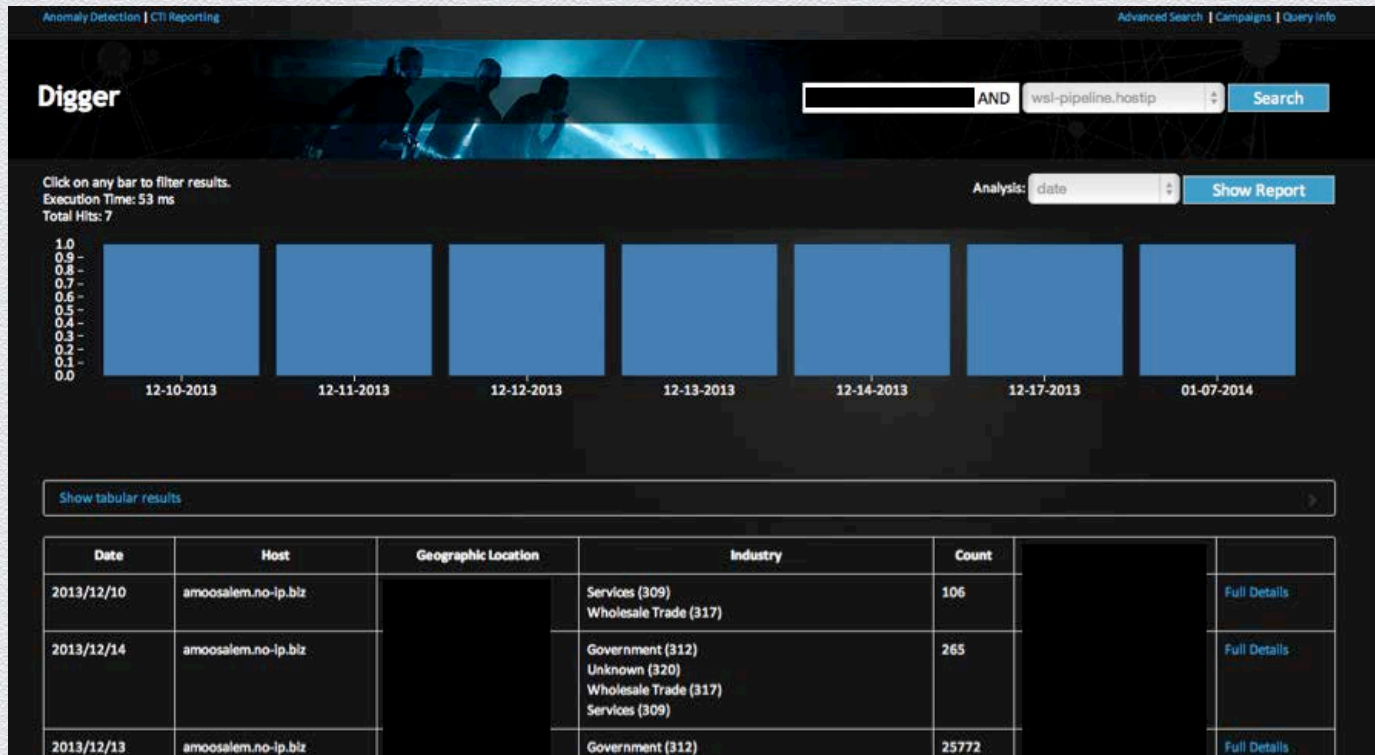
http://watson.microsoft.com/StageOne/iexplore_exe/8_0_6001_18702/ntdll_dll/5_1_2600_6055/00029f09.htm?

Crash 12-16-2013 URL:

http://watson.microsoft.com/StageOne/iexplore_exe/8_0_6001_18702/ntdll_dll/5_1_2600_6055/00029f09.htm?



AUGMENTING THE ANOMALY WITH SECURITY INTEL: SUSPICIOUS OUTBOUND CONNECTIONS FROM MNO



CONFIRMED H-WORM RAT BEACONING

Pipeline Detail Report

Host	amooalem.no-ip.biz
Server IPs	79.124.66.209 79.124.66.163
Path	/is-ready
MIME	None

Statistics

Urls with non-security categories:	0
Urls with risk categories:	0
Urls with security categories:	0

Details

Dynamic DNS	(212) (6)
Analytic Flag	(199) (6)

Campaigns

Generic	(18309)
---------	---------

Threatnames

Generic.Call_Home.Backchannel_Traffic.RTSS	
--	--

Stages

Call_Home	
-----------	--

Reasons

Backchannel_Traffic	
---------------------	--

Industries

Services	(309)
Wholesale Trade	(317)

Date

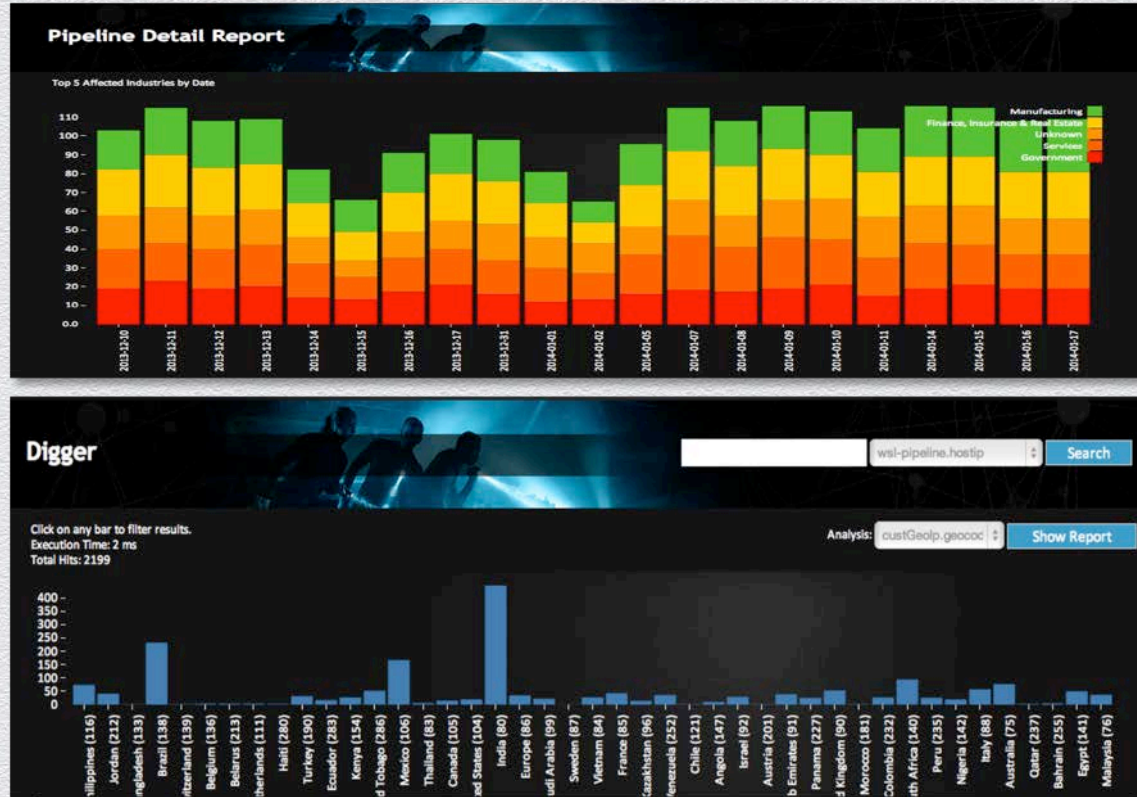
2013/12/10	
------------	--

Total Hits

106	
-----	--

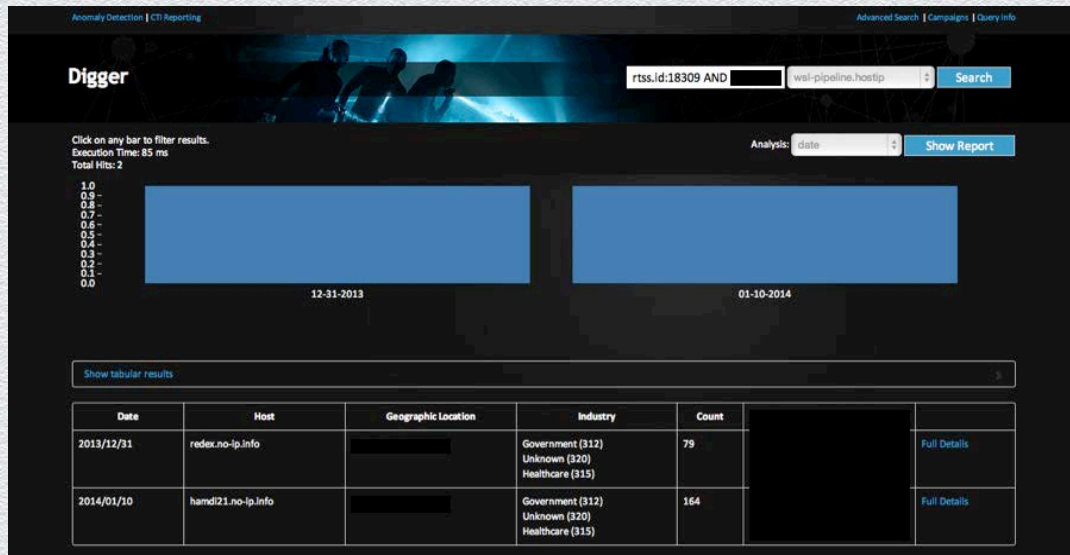
HOUDINI H-WORM RAT

ADDITIONAL RISK INDICATORS



A SECOND TARGET—

Government Agency also infected with H-Worm RAT



CRASH LOGS CAN IDENTIFY ADVANCED THREATS

- ◆ When crash telemetry identifies anomalous behavior...
- ◆ ... and we validate those anomalies with additional security context...
- ◆ These items validate that crash reports can be an indicator of advanced attacks and can be used to identify threats that **have made it past existing security measures undetected.**







CRASH ANOMALIES TO FIND PREVIOUSLY UNKNOWN ATTACKS AGAINST BUSINESS APPLICATIONS

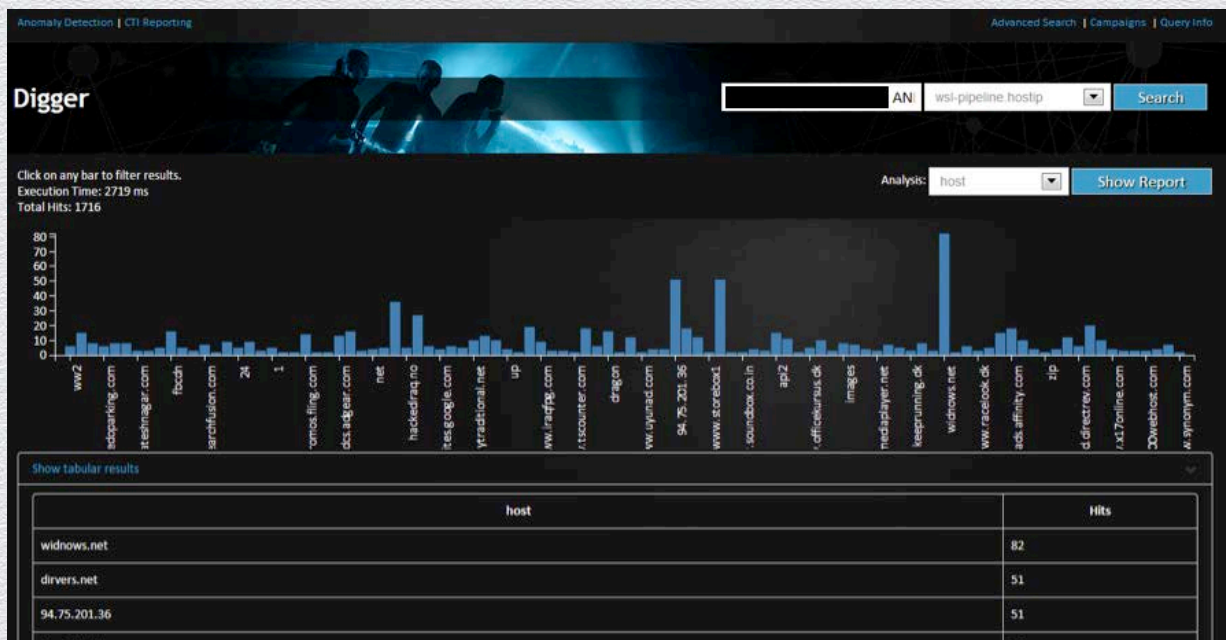
AN ANOMALY-BASED PERSPECTIVE ON POS MALWARE

- ◆ Data breaches of retail organizations have dominated the news.

AN ANOMALY-BASED PERSPECTIVE ON POS MALWARE

```
"2013/09/19","http://watson.microsoft.com/StageOne/pos_exe/2_8_60_0/517144a4/ntdll_dll/5_1_2600_6055/4d00f27d/0/0000100b.htm?",  
"2013/11/25","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/pos_exe/2_8_64_0/000fc44a.htm?",  
"2013/11/25","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/pos_exe/2_8_64_0/000fc44a.htm?",  
"2013/11/25","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/524179b1/pos_exe/2_8_64_0/524179b1/40000015/00103dd3.htm?",  
"2013/11/25","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/524179b1/pos_exe/2_8_64_0/524179b1/40000015/00103dd3.htm?",  
"2013/11/25","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/524179b1/pos_exe/2_8_64_0/524179b1/c0000005/000397f2.htm?",  
"2013/11/25","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/524179b1/pos_exe/2_8_64_0/524179b1/c0000005/000397f2.htm?",  
"2013/11/26","http://watson.microsoft.com/StageOne/pos_exe/2_8_51_0/504ef82e/ole32_dll/6_1_7601_17514/4ce7b96f/c0000005/000db901.htm?",  
"2013/11/26","http://watson.microsoft.com/StageOne/pos_exe/2_8_51_0/504ef82e/pos_exe/2_8_51_0/504ef82e/c0000005/000d7991.htm?",  
"2013/11/26","http://watson.microsoft.com/StageOne/pos_exe/2_8_51_0/504ef82e/pos_exe/2_8_51_0/504ef82e/c0000005/000d7991.htm?",  
"2013/11/26","http://watson.microsoft.com/StageOne/Generic/AppHangB1/pos_exe/2_8_51_0/504ef82e/5f39/2304.htm?",  
"2013/11/28","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/524179b1/mscorwks_dll/2_0_50727_5472/5174dd69/c0000005/0013726a.htm?",  
"2013/11/29","http://watson.microsoft.com/StageOne/pos_exe/2_8_64_0/524179b1/ntdll_dll/5_1_2600_6055/4d00f27d/0/0000100b.htm?",  
"2013/12/02","http://watson.microsoft.com/StageOne/Generic/AppHangB1/pos_exe/2_8_64_0/524179b1/479f/262400.htm?",  
"2013/12/03","http://watson.microsoft.com/StageOne/Generic/AppHangB1/pos_exe/2_8_60_0/517144a4/0000/256.htm?",  
"2013/12/03","http://watson.microsoft.com/StageOne/pos_exe/2_8_60_0/517144a4/mscorwks_dll/2_0_50727_5472/5174dd69/c0000005/0013726a.htm?"
```


AUGMENTING OUR ANOMALIES WITH SECURITY INTEL



SPIKES IN ACTIVITY ON THE SAME DAYS AS THE CRASHES

2013/11/24	94.75.201.36	308	11	Full Details
2013/08/29	94.75.201.36	13	17	Full Details
2013/10/03	94.75.201.36	281	19	Full Details
2013/08/03	94.75.201.36	16	20	Full Details
2013/09/24	94.75.201.36	16	25	Full Details

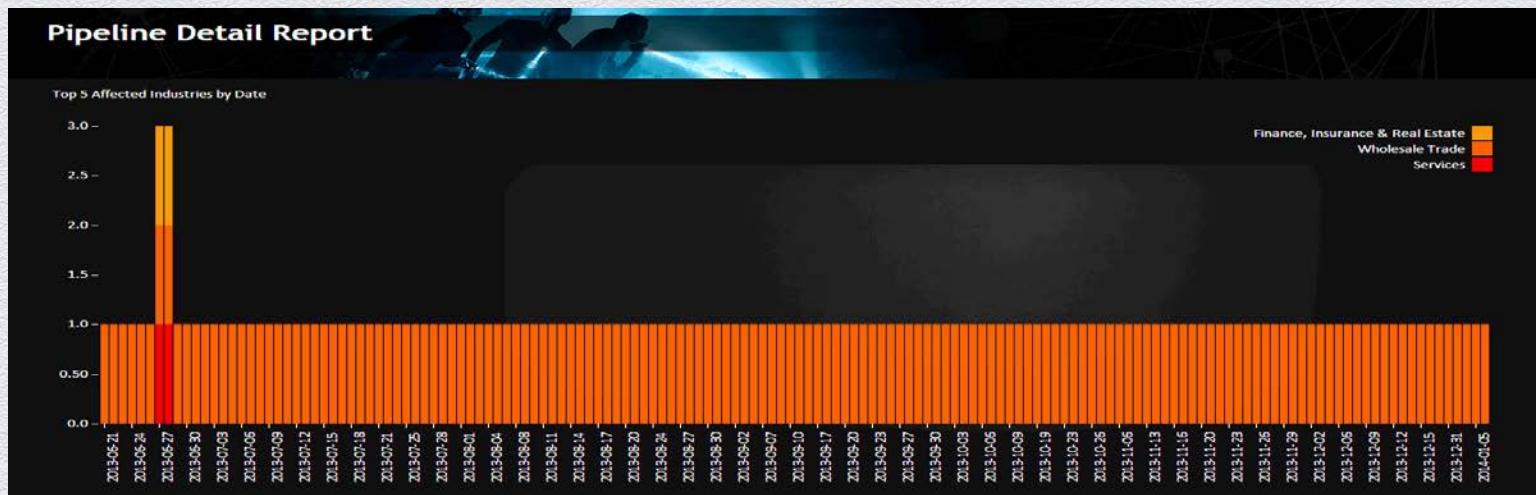
UMMM, YOU FOUND ZEUS? NAP TIME...



LOOKS LIKE TYPICAL ZEUS C&C TRAFFIC

- /sadcxvbv/vdfbffddf.php
- /sadcxvbv/fgfvsada.php

ALMOST...



ANOMALY DETECTION CAN FIND THE UNKNOWN THREAT

- ◆ Gathering crash data for a process specific to an industry...
- ◆ Again applying security context to the data...
- ◆ We were able to identify anomalous crashes occurring outside of memory space...
- ◆ Which lead us to identify a previously unreported, targeted attack against a retailer...
- ◆ ... and identify a new variant of Zeus, presumably targeting POS systems



NEXT STEPS...

- ◆ Research anomalies in other critical and high risk business applications
 - ◆ SCADA systems
 - ◆ Cellular core networks
 - ◆ Banking systems
 - ◆ ...

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



**HOW CAN YOU APPLY
THESE FINDINGS?**

INFORMATION SHARING IS THE KEY

- ◆ Think about anomaly detection as part of your security strategy
- ◆ Download lookup tables and example SIEM queries to examine crash reports yourself
 - ◆ <http://www.websense.com/DrWatsonGITHUB>

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



THANK YOU