

An Adversarial View of SaaS Sandboxes

Jason Trost
Aaron Shelmire
Jan 16th 2016



Whois Jason

Jason Trost

- VP of Threat Research @ ThreatStream
- Previously at Sandia, DoD, Booz Allen, Endgame Inc.
- Background in Big Data Analytics, Security Research, Honeypots, and Machine Learning

Whois Aaron

Aaron Shelmire

- Senior Threat Researcher @ ThreatStream
- Previously at CERT, Secure Works CTU-SO, CMU
- Background in Incident Response, Forensics, Security Research

Motivation

- Advanced Malware Detects Sandboxes!
 - Does it?
- Threat Intelligence Feeds
- AV is Dead!
- You're going to tip off the adversary!!!
- Everyone's going to know I'm compromised

Experiment

- Created Sensors with unique CampaignIDs
- Encoded execution time and CampaignIDs in domain names
- Tornado HTTP app and Bind DNS servers
- Submitted unique samples to 29 free online Sandboxes
- Submitted unique domains to ~50 domain/URL Reputation engines
- Watched traffic roll in

Sandboxes Tested

Avira	Comodo Instant Malware Analysis	Comodo Valkyrie
F-Secure Online Analysis	Joe Sandbox – Private	File-analyzer.net
Malwr.com	NSI	Payload Security
ThreatExpert	TotalHash	ViCheck
Cloud.vmray.com	Ether.gtisc.gatech.edu	Threat track
Anubic.iseclab.com	Metascan-online	Eureka-cyber-ta.org
Microsoft portal	Online.drweb.com	uploadMalware
VirusTotal	Virusscan.jotti.org	wepawet
Virscan	ViCheck	ThreatStream's internal sandbox

Domain/URL Reputation Engines Tested

app.webinspector.com	malwaredomainlist.com	senderscore.org	trustedsource.org
avgthreatlabs.com	mxtoolbox.com/blacklists.aspx	siteadvisor.com/sites	unmaskparasites.com
Bluecoat Web Pulse	Passive Total	sitecheck.sucuri.net	URLVoid
brightcloud.com	Phishtank.com	spam404.com	urlblacklist.com
Domain tools query	Quttera	spamhaus	URLQuery
dshield.org	quttera.com	Sucuri Sitecheck	Virus Total URL query
Fortiguard iprep	reclassify.wrs.trendmicro.com	SURBL	VirusTotal URL domain/IP search
Google Safe Browsing	reputationauthority.org	Threat Log	vurl.mysteryfcm.co.uk
Hosts-file.net	safeweb.norton.com	ThreatStream	Web of Trust
isithacked.com	Scumware.org	TotalHash	wepawet.iseclab.org
isitphishing.org	senderbase.org	trafficlight.bitdefender.com	zulu.zscaler.com

Our Sensor – v1

```
{  
    "num_cpu": "1",  
    "username": "John",  
    "processes": ["winlogon.exe", "services.exe", "lsass.exe"],  
    "ram": "1048576",  
    "ip": "10.0.2.15",  
    "hostname": "JOHN-PC",  
    "drives": [  
        {  
            "drive_size": "19.99",  
            "drive_type": "Fixed Disk",  
            "drive_letter": "C:\\\"  
        }  
    ],  
    "bios": {  
        "manufacturer": "Google",  
        "vendor": "Google",  
        "bios": "Google - 1"  
    },  
    "mac_addr": "00-23-45-67-89-02"  
}
```

*Enumerate Host
Sockets Based Comms*

*Create Run Key
Delete Run Key
Exit Process*

*NO REMOTE ACCESS
CAPABILITY*

APT TTP OMG!

Stream Content

X Follow TCP Stream

```
POST /index.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap , */
Referer: http://200.200.200.1
Accept-Language: en-US
Content-Type: application/octet-Stream
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: 200.200.200.1
Content-Length: 645
Connection: Keep-Alive
Cache-Control: no-cache

<packet>ugMAAHicfZJPbxpBDMXfuVK/wx7JAQQEqLqnbsgGSPlXIKXppUKEiFUIiSBN2ooP39
+8LcLK1WrksefZY7/
xeKmFVqw7RZqjM85rPeit3qiuqsq2Bhrrs1KNFKtHzFwbbmyRa2IjTchWuuL8BBrpI4bsQ0ddk3HLyrdXmLEjItsc
36MzLRw5w7rBqiIFneg7vhUZA9KARVlH7tJVor5aukC3YBSbb5Hz2P4eeFNTdYhKkQ0kNeuBkUtqBbyPFeKbnC9e3
hYdrI77ELpTwHcE0uQFG5CCJuQLSKZ31K6yB46fQKM8Y6QP515SDU8Lrr806vWRHvUqxk6oFTTr8h21gP8HqmkkRCf
lr7kNYoWNL2IS3Z/rxkiEipmT/yMwX9HXrDjdy/HA99ytFxtz/6sp1HRN7zCrDvpb/f6JTZGh0I7M7o178Co/
N/9Tsmu72BPsMDrf+zZ+5p4N06e3SU7BmDz0U8Ns3bvnM/zV+7l4jhhjhztXTMcqj
+p58jLuhb950I7sQ5hu3afSX7piveNHEr0eo1//G7/jRW3/
W4iqs0r/0LuDCYx9v4jMPSHv2Ru8puhZCXbd0RP6NtC5p3o/hRVn30ca6SNYm72rb+7q1L7ft4iBFQ==</packet>
```

Entire conversation (1010 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

vpnlogin-ithelpdesk.com

Filenames:
anyconnect-win-4.1.04011-k9.exe
vpnagent.exe
svchost.exe
svchost.exe
lsass.exe
...

THREATSTREAM®

© 2015 ThreatStream Confidential

Sensor C2 – HTTP POST

X Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
POST /check.php HTTP/1.1
Host: 130894389150858750.A9.x.vpnlogin-it-helpdesk.com
Cache-Control: no-cache
Connection: close

<packet>eJztUMtu1DAU5V06ymoS2Ymdx0heMDN1BSJihCqgLIltS7yx4+A7ebTfyEeRZjoVbaSKBUuuFz6P+/
B1xUIZ1SWqv7xPvI7l+/zz5mbvKYazMMBxGtA4wKFnGHrrI+SHiR9v/Gzjb6+9H+zX/5jj+V/
t2HZ9u36nRimudgq065AGCK12k7jdffr4YY0e6Nfn0Q+a17DQcwx50fu2v40TNFe5s1wCff+d
+QoMQCBHueLgFmhQzXROF6xtaZuZgHS9mvrmREMBF2T0ds8rC+e6sR47+XNQ5b1eeH+Di04oK8rX81trNfSv5ojh/
LZTAccnUY6ttk66mXRVX+lWjDNxUqredN1MDHDroB8WTW+My12/v152frk2t82Tx414XM3dj84
+j1DTxWdclc2xgEXZn+n/Ch
+dGkEvZzXmb1AWeF037aFoF37CUSYJpge0Z5qi0KEkKQjJIkwxEgjHPEoITieNSkKTNIpwSgjl4QEfiIpqRRUOh9Q
W/+Q0Jp/Vz</packet>HTTP/1.1 200 OK
Date: Fri, 16 Oct 2015 03:13:09 GMT
Content-Length: 2
Content-Type: text/html
Server: TornadoServer/4.0.1

OK
```

Entire conversation (784 bytes)

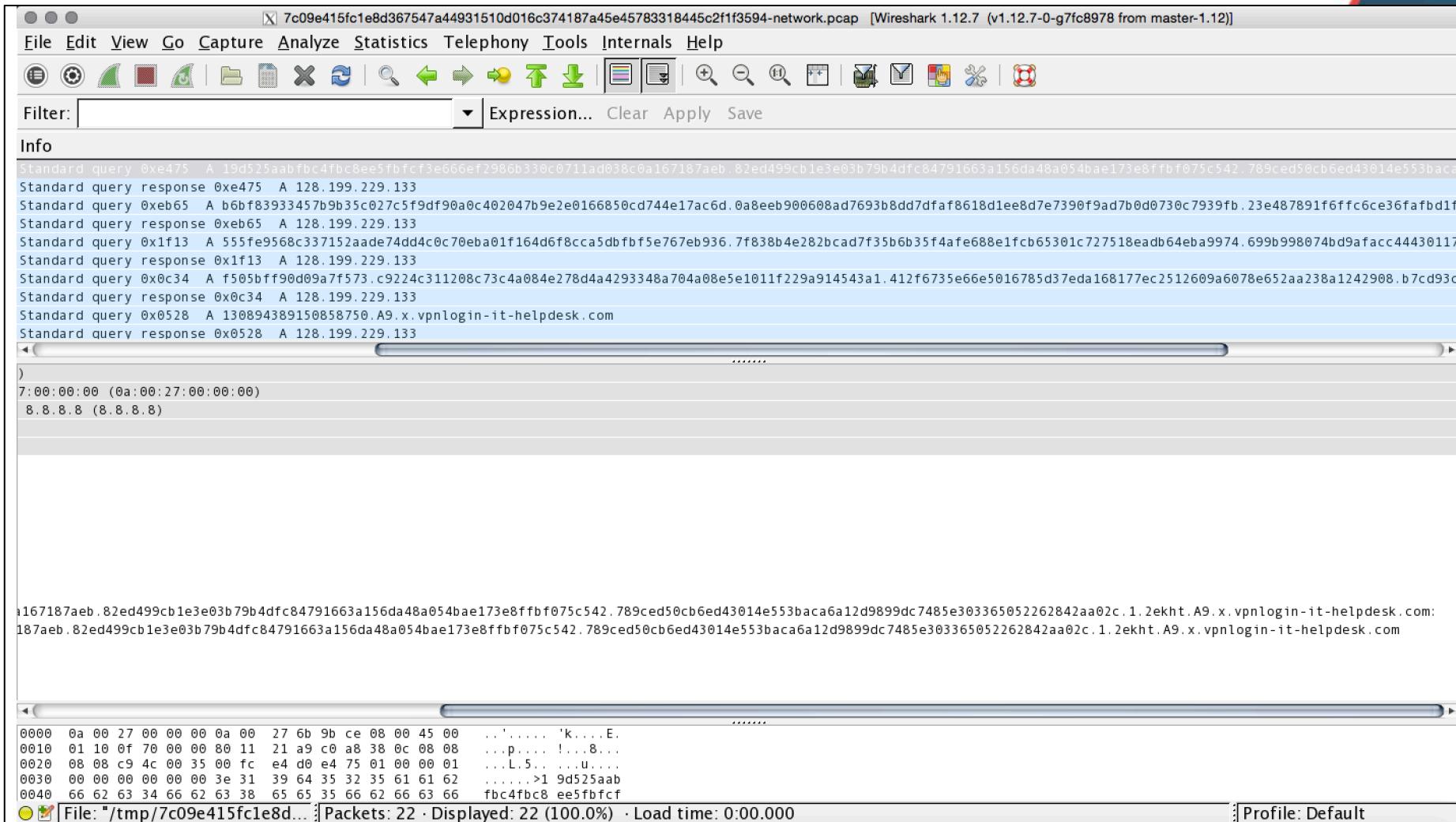
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

*Exfil HTTP POST
 zlib compression
 base64 encoded*

Worked pretty well, but...

Sensor – v2 DNS Covert Channel C2



Some Sandboxes block TCP conn
Most allow DNS unmodified

zlib compression
hex encode
split data into chunks
multiple DNS A requests

Malware Detects Sandboxes



Complimentary White Paper

Debunking the Myth of Sandbox Security

Organizations are under assault by a new generation of cyber attacks that easily evade traditional signature-based defenses. These coordinated campaigns are targeted. They are stealthy. And they are persistent.

HOT KNIVES THROUGH BUTTER:

Evading File-based Sandboxes

Authors: Abhishek Singh
and Zheng Bu

Sandbox detection features ver. 1

- System Services Lists
 - Processes – VBoxService(1), vmtools (8)
- MAC address
 - VMware, Inc. (55), Cadmus Computer Systems (40), ASUSTek COMPUTER INC. (23)
- Bios
 - VMware (50), Bochs(34), ASUS(23), Google(8), Qemu(8)
- Disk Size
 - 19.99GB (52), 25GB (37), 120GB (28), 50GB (20), 39GB (20)
- RAM
 - 1GB (92), 1.5GB (18), 512MB (10)
- Was the EXE renamed?
 - sample.exe, malware.exe, \${md5}.exe

Really Detecting Virtual Machines

- System Services Lists
 - Processes – **VBoxService(1), vmtools (8)**
- MAC address
 - **VMware, Inc. (55), Cadmus Computer Systems (40), ASUSTek COMPUTER INC. (23)**
- Bios
 - **VMware (50), Bochs(34), ASUS(23), Google(8), Qemu(8)**
- Disk Size
 - **19.99GB (52), 25GB (37), 120GB (28), 50GB (20), 39GB (20)**
- *RAM*
 - **1GB (92), 1.5GB (18), 512MB (10)**
- *Was the EXE renamed?*
 - *sample.exe, malware.exe, \${md5}.exe*

Sandbox Detection Techniques – Not Implemented

- User Engagement
 - Dialog box, Double Click. Doc Scroll
 - Slow Mouse, Fast Sandbox
- Execution after reboot
- Pretty sure these would work
- Require User engagement / Suspicion

Sandbox detection features ver. 3

- Wanted to try some new checks...
- Uptime – Malware checks for over 12 minutes?
- Is Sleep patched?
- Is the Security Information Descriptor valid ?
 - Really checking if AV is emulating the process
- What Group is the user in?

Sandbox detection features ver. 3

38 hosts w/ HTTP check in, only 4 valid check ins

Uptime	Is Sleep Patched?	ValidSid	Group
~60 minutes	No	Yes	Administrators
~5 minutes	No	Yes	Administrators
~2 minutes	No	Yes	Administrators
~20 minutes	No	Yes	Administrators

Sandbox Detection Techniques -- Way too Advanced!!!!

- Many companies, but only a few virtual machines used!
 - Same usernames
 - Same hostnames
 - Same disk size
 - Same CPU count
-
- And then...

...just check the process name

- artifact.exe
- wbOxyeRLI6z7Jiq.exe
- sampel.exe
- 905DFEBA7A75DE9C6BF261CD5A076A5C5CB5FC1F.exe
- samp1e_9ac36e185072270b0745ea0d68085dd9.exe

```
GetModuleFileNameEx(hProcess, 0, lpBuff, MAX_PATH);  
if (lpBuff != lpszMyName) ExitProcess();
```

So we had some other questions...

- AV?
- Tipping off the adversary?
- Threat Intel Feeds?

AV is Dead!

- Is it?

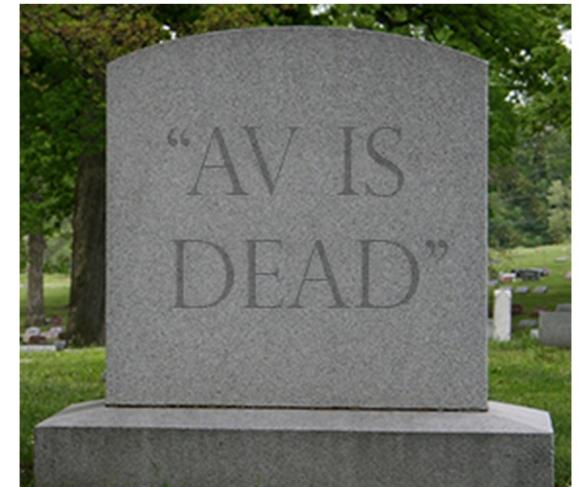
With 'AV Dead,' It's Time for an Operational Revolution

DATE: MAY 8, 2014 | BY: JEFFREY GUY | SR DIRECTOR PRODUCT MANAGEMENT | FOLLOW @JJGUY

CATEGORY: ADVANCED THREAT PROTECTION

Symantec made waves this week by declaring "[AV is dead](#)." I'm delighted to see an industry pioneer finally catch up to what the rest of us have [known for years](#).

Traditional antivirus does one thing very well: it limits the damage from widespread, well-known threats. Once a given malware passes the threshold of detection, usually measured by how widespread the malware is deployed, our antivirus ecosystems provide infrastructure to rapidly deploy signatures—across the enterprises of you and your peers.



What did AV think of our sensor?

- At first...

Jotti

Jotti's malware scan Scan file Search hash Language FAQ Privacy Contact

qtttask.exe

Name:	qtttask.exe	Status:	Scan finished. 0/21 scanners reported malware.
Size:	85.5kB (87,552 bytes)	Scan taken on:	August 20, 2015 at 10:13:37 PM GMT+2
Type:	PE32 executable (console) Intel 80386, for MS Windows		
First seen:	August 20, 2015 at 10:13:34 PM GMT+2		
MD5:	8f8a0980657f9038454be844d79f8e44		
SHA1:	8f2fc20b52eb42e65e84577844cd60bc45cc3e9e		

Start Download > ✖

File size: 487KB. OS: MacOSX. Get PDF Pronto 100% Full Version!

● ○

Ad-Aware Aug 20, 2015 Found nothing	agnitum Aug 20, 2015 Found nothing	Arcabit Aug 20, 2015 Found nothing
avast! free Aug 20, 2015 Found nothing	AVG Aug 20, 2015 Found nothing	AVIRA Aug 20, 2015 Found nothing
Bitdefender Aug 20, 2015 Found nothing	ClamAV Aug 20, 2015 Found nothing	Dr.WEB Aug 20, 2015 Found nothing
'eScan Aug 20, 2015 Found nothing	eset Aug 20, 2015 Found nothing	FORTINET Aug 20, 2015 Found nothing
F-PROT Aug 20, 2015 Found nothing	F-Secure Aug 20, 2015 Found nothing	GDATA Aug 20, 2015 Found nothing
IKARUS Aug 20, 2015 Found nothing	KASPERSKY Aug 20, 2015 Found nothing	Quick Heal Aug 19, 2015 Found nothing
SOPHOS Aug 20, 2015 Found nothing	TREND MICRO Aug 19, 2015 Found nothing	VBA32 Aug 20, 2015 Found nothing

Download Now ✖

Yeti media player ✖

Eventually...

- VirusTotal: 6 Samples
 - Detection ranges from 8/57 to 30/57
 - A lot of Trojan Zsusy and Trojan Graftor
- More malicious as time went on

svch0s1.exe

Submitted on August 21st 2015 15:49:06 (CDT) with target system Windows 7 32 bit
Report generated by VxStream Sandbox v2.20 © Payload Security

[@ Sample \(142KB\)](#) [@ HTML Report \(158KB\)](#) [@ PCAP \(1.2KB\)](#) [Re-analyze](#)

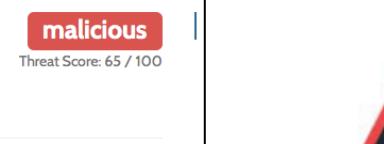
Incident Response

[Risk Assessment](#)

Spyware/Leak POSTs files to a webserver
Persistence Modifies auto-execute functionality by setting/creating a value in the registry
Fingerprint Contains ability to lookup the windows account name
Reads the active computer name

Network

Domains 130846638632592500.PS.x.vpnlogin-it-helpdesk.com
IPs 128.199.229.133 (TCP 80)



No exploits were identified.

Deobfuscation results

Evals

No evals.

Writes

No writes.

Network Activity

Requests

URL
file:///spoo1svc.exe

ActiveX controls

No objects/controls.

Shellcode

No shellcode was identified.

Malware

No additional malware was retrieved.

Comments

3rd gen sensor...

svchOs1.exe

suspicious

Threat Score: 32/100

Submitted on January 11th 2016 17:19:28 (CST) to environment group *Windows 7 32 bit*

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

Report generated by VxStream Sandbox v3.10 © Payload Security

[⊕ Sample \(42KiB\)](#) [HTML Report \(180KiB\)](#) [XML Report \(82KiB\)](#) [MAEC Report \(112KiB\)](#) [JSON Report \(673KiB\)](#) [⊕ PCAP \(1.2MiB\)](#) [↻ Re-analyze](#)

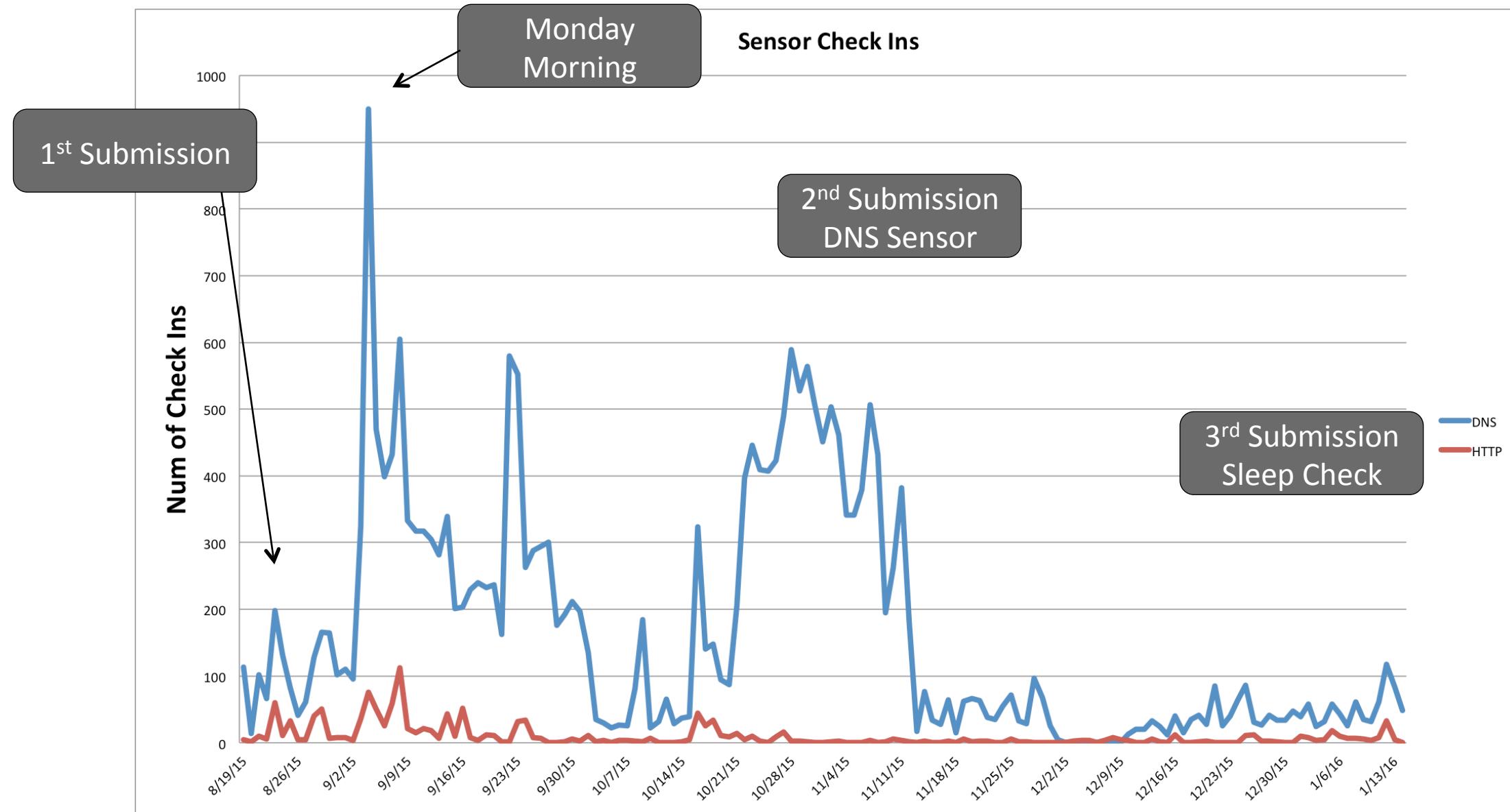
- *Removed Sandbox accuracy checks*
 - *Run key that was added, then removed*
 - *Touch and Delete a file*
 - *Large amount of host profiling*
- *Much more reasonable scoring*
 - *Accuracy is worse than before!*

Sharing?

- Yup, Lots
- Samples shared
 - Evidence of new executions seen from different origins
- Domain names shared (or scraped)
 - Previous execution's domains resolved later by other orgs, different nameservers
 - Some domains appear on threat intel lists
- Many orgs are trivially identified as security companies
 - Every major AV company is represented in our DNS logs
 - Several Security Product Companies

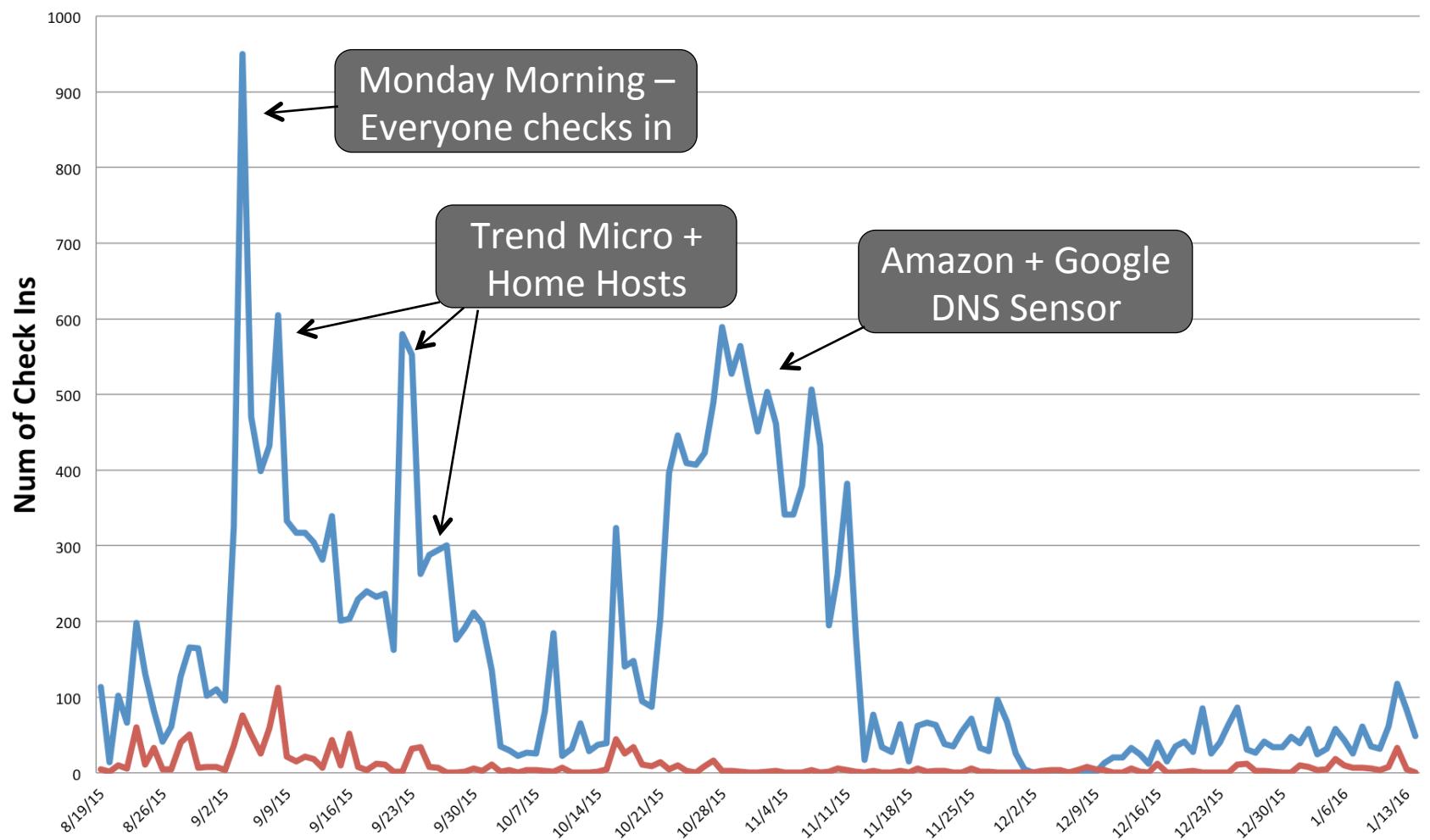


Tipping off the Adversary

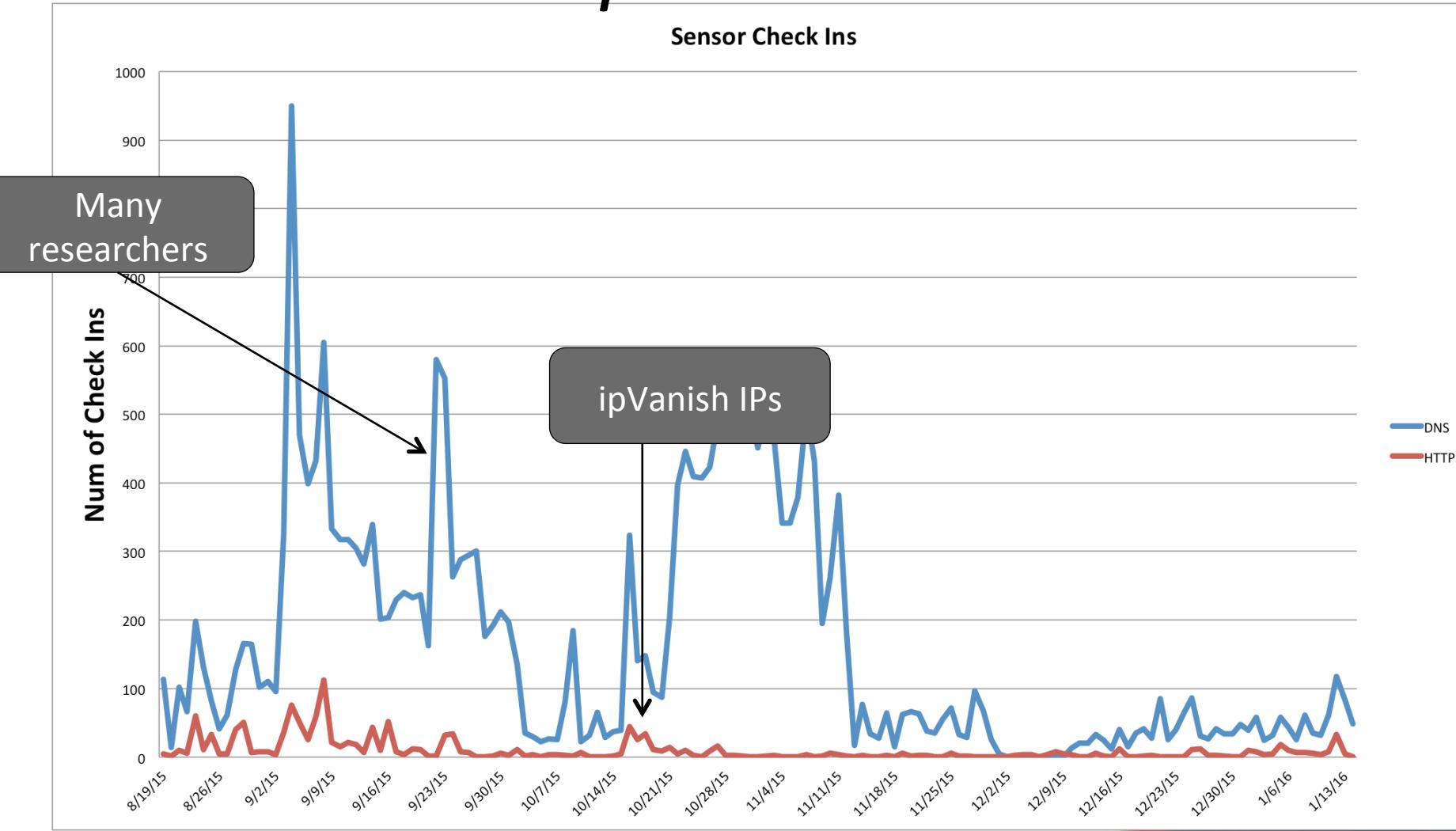


Check In Activity

Sensor Check Ins



Anomalous Spikes



Sharing? – then something happened

	1st Gen	3rd Gen
HTTP unique IPs	~400	38
HTTP unique IP for source	~130	38
Valid HTTP Post	4	4
VT detections	~8/57 +	1/57

- Sharing based upon VT detections + new_file?
- Takes ~4 days for files to reach VT from most sandbox sources.

Sharing: Threat Intelligence Feeds?

Campaign	First DNS	First HTTP	Threatfeed
UM	2015-08-29 22:47	2015-08-29 23:41	2015-08-30 06:33
AV	2015-08-30 17:08	2015-08-30 19:45	2015-08-30 18:43
A9	2015-09-03 20:33	2015-09-03 20:33	2015-10-24 08:55
A12	2015-09-03 20:45	2015-09-03 20:46	2015-10-27 18:47
AN	2015-09-08 07:10	2015-09-08 10:23	2015-09-08 17:55
C21	2015-10-22 00:28	-	2015-10-22 00:29
PS-Y	2016-01-11 23:21	2016-01-11 23:15	2016-01-13 04:14

Sharing: URL Reputation Services

- Crafted unique campaign IDs and timestamp domains
- Made queries for unique domains to ~50 reputation engines
- Three sites resulted in daily DNS lookups spanning > 5 days
- Two resulted in daily DNS lookups spanning nearly 2 months
 - Most major AV/security companies networks represented
- **YOUR QUERIES ARE SHARED (implicitly?/explicitly?)**
- **When you query these sites, you lose control of the domain/URL**

Threat Intel vs the Sandbox IPs?

- Of all the Sandbox IPs that made valid POST requests to our server 15 were also identified in some threat intelligence feeds as malicious
- 6 were TOR IPs
- 1 was an Anonymous proxy
- All others were characterized:
 - Bot IPs
 - Spammer IPs
 - Brute Force IPs
 - Scanning IPs
 - Compromised IPs (Hawkeye Keylogger, Dyre)
- Interesting, but not surprising

Lessons

- Most people use the same Sandbox Images
- Most sandboxes don't change the environment settings across executions
- AV thinks your file is malicious
- You will tip off the adversary
- Everyone will hit their network touch points ... forever ...
- Reputation services can result in noisy traffic to the NS
- Malware sandboxes can be fingerprinted with very simple techniques
- **You get what you pay for**

Contact

Jason Trost

- @jason_trost
- jason [dot] trost [AT] threatstream [dot] com
- <https://github.com/jt6211>

Aaron Shelmire

- @Ashelmire
- aaron[dot] shelmire [AT] threatstream [dot] com