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

THREATSTREAM®

Whois Aaron

Aaron Shelmire

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

THREATSTREAM®

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

THREATSTREAM®

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

THREATSTREAM®

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

THREATSTREAM®

Our Sensor – v1

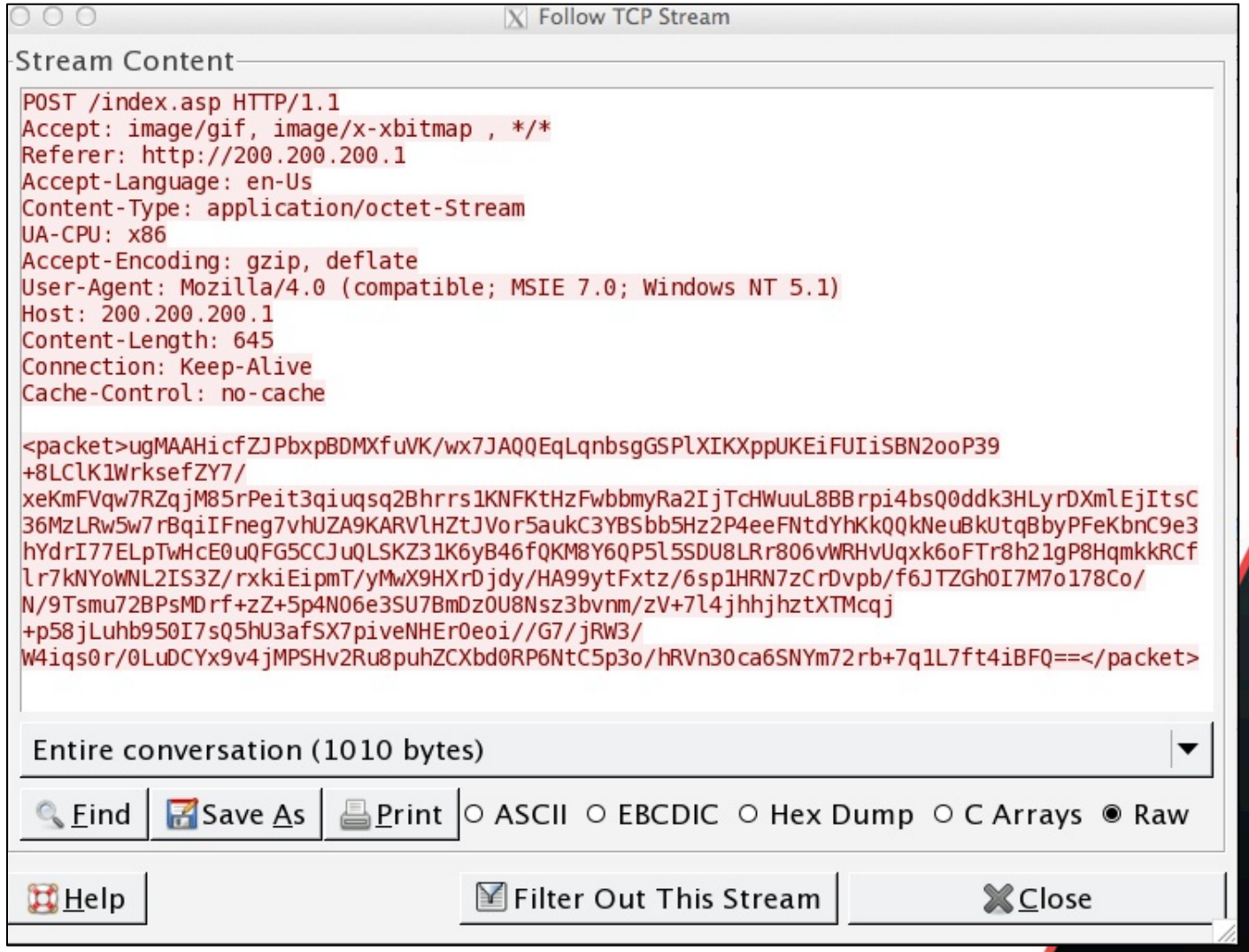

```
{
  "num_cpu": "1",
  "username": "John",
  "processes": ["winlogon.exe","services.exe","lsass.exe"],
  "ram": "1048576",
  "ip": "10.0.2.15",
  "hostname": "JOHN-PC",
  "drives": [
    {
      "drive_size": "19.99",
      "drive_type": "Fixed Disk",
      "drive_letter": "C:\\"
    }
  ],
  "bios": {
    "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

THREATSTREAM®

APT TTP OMG!



vpnlogin-ithelpdesk.com

Filenames:

anyconnect-win-4.1.04011-k9.exe

vpnagent.exe

svchost.exe

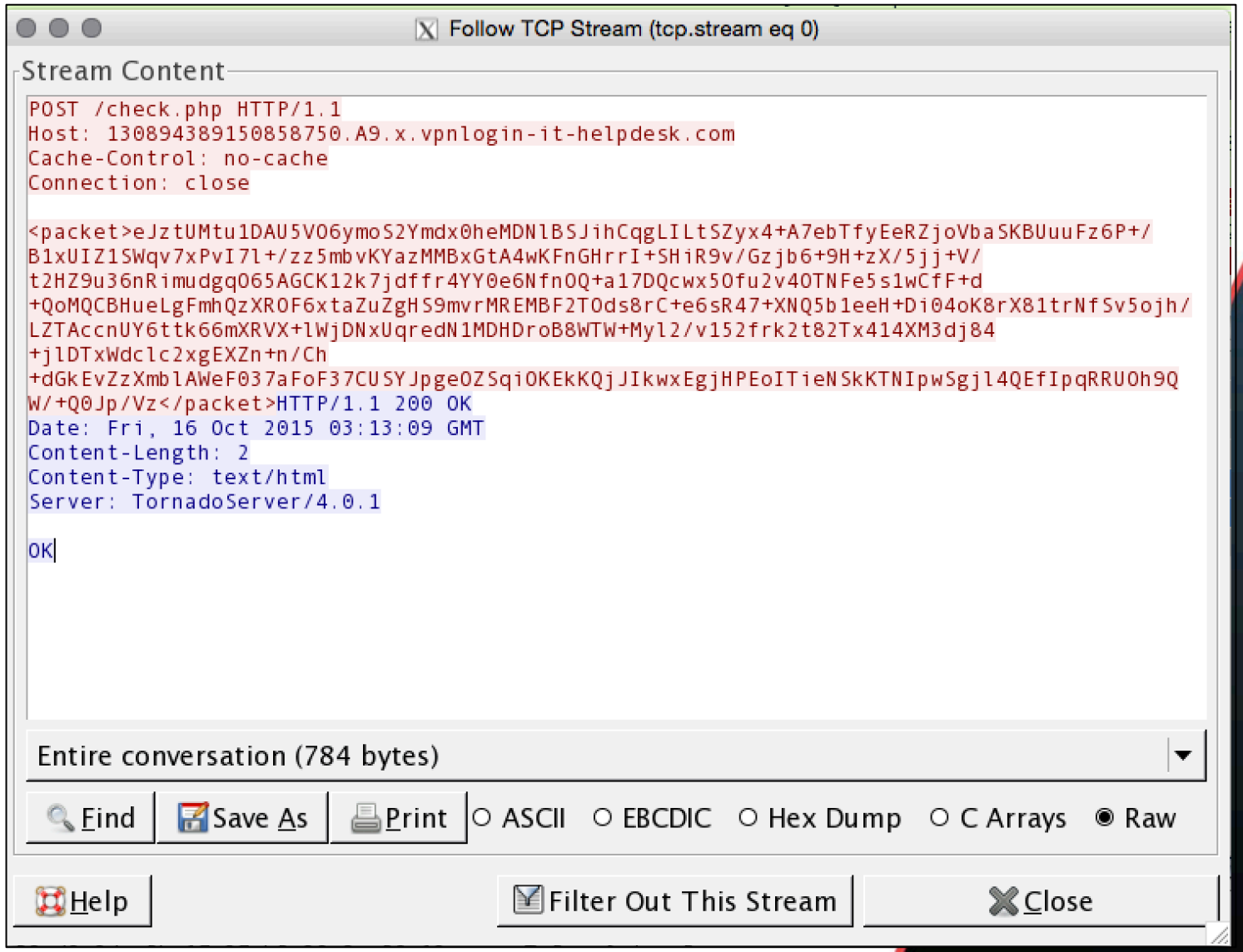
svch0st.exe

lsass.exe

...

THREATSTREAM®

Sensor C2 – HTTP POST

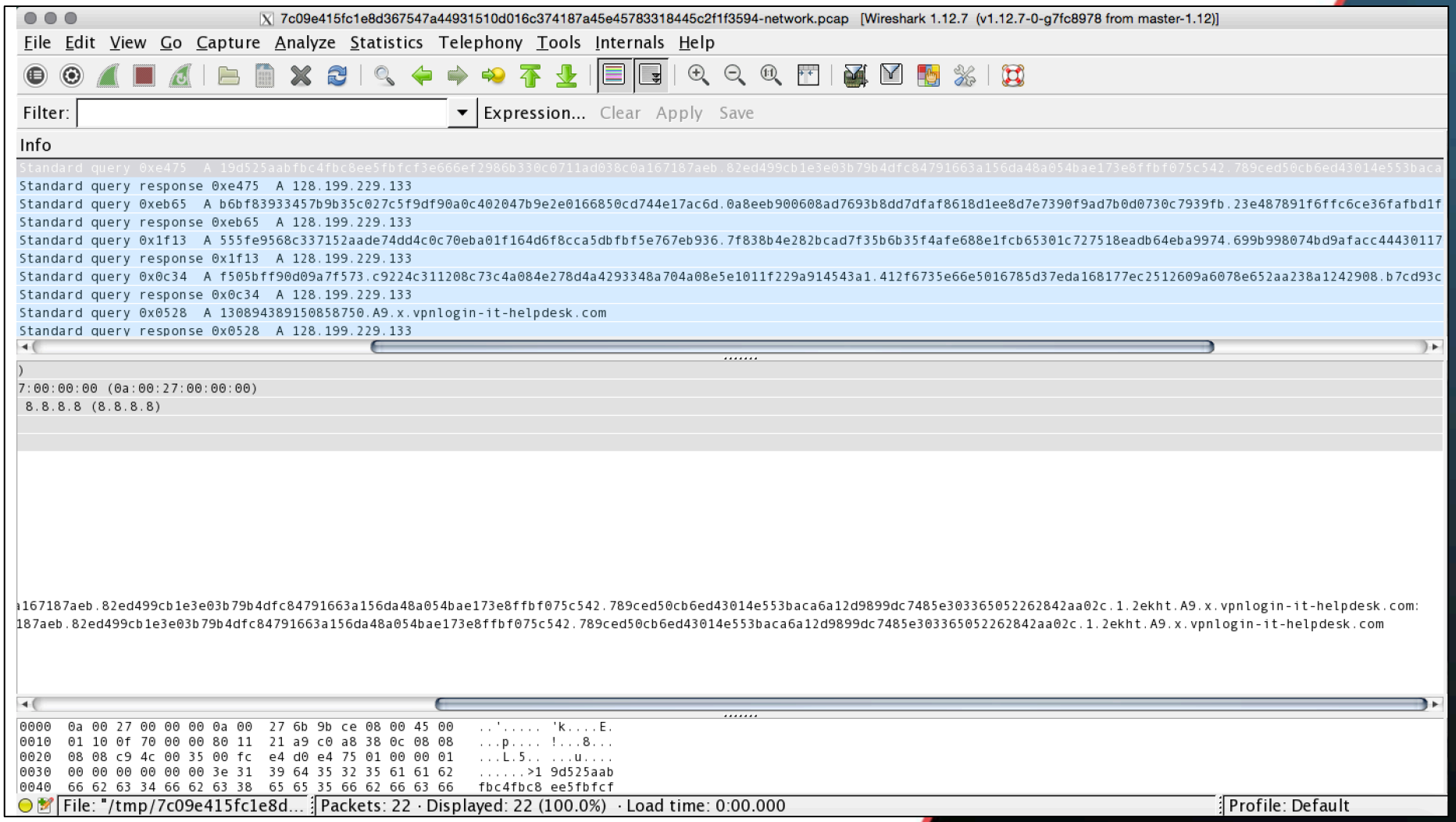


Exfil HTTP POST
zlib compression
base64 encoded

Worked pretty well, but…

THREATSTREAM®

Sensor – v2 DNS Covert Channel C2



Some Sandboxes block TCP conns
Most allow DNS unmodified

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

THREATSTREAM®

Malware Detects Sandboxes

THREATSTREAM®

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*

THREATSTREAM®

*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*

THREATSTREAM®

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

THREATSTREAM®

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
- wbOxyeRLl6z7Jiq.exe
- sampel.exe
- 905DFEBA7A75DE9C6BF261CD5A076A5C5CB5FC1F.exe
- samp1e_9ac36e185072270b0745ea0d68085dd9.exe

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

THREATSTREAM®

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.

THREATSTREAM®

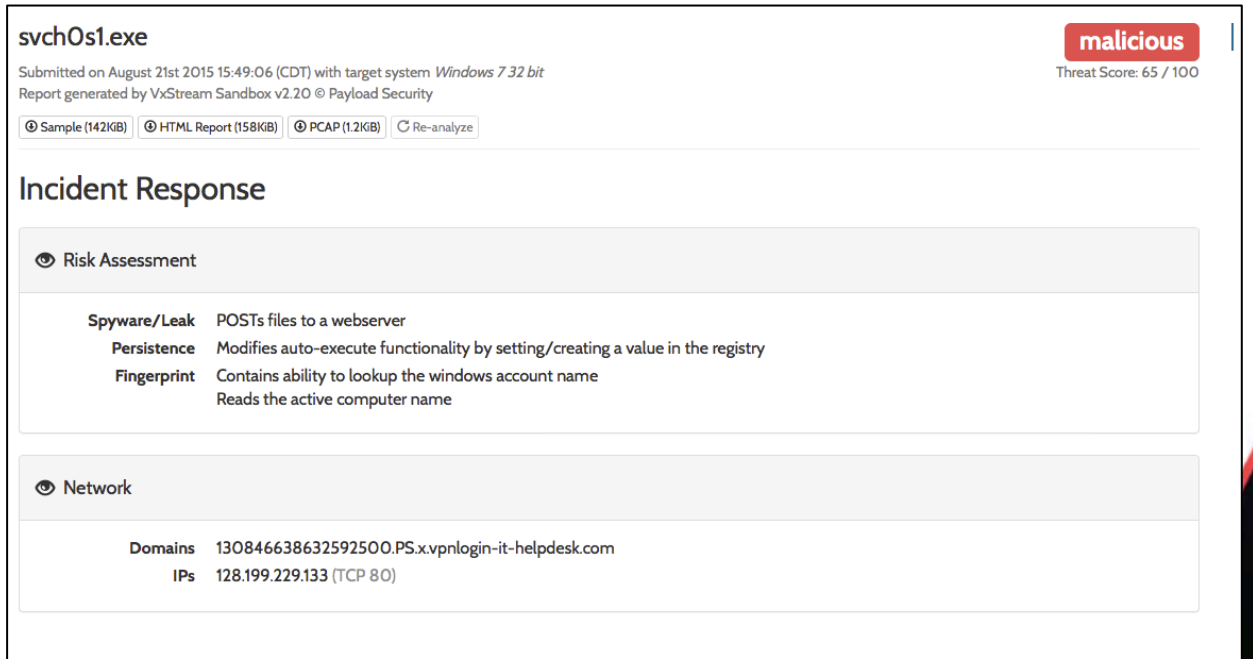
What did AV think of our sensor?

- At first…

THREATSTREAM®

Eventually…

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


svch0s1.exe

malicious

Threat Score: 65 / 100

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 (142KiB) | HTML Report (158KiB) | PCAP (1.2KiB) | Re-analyze

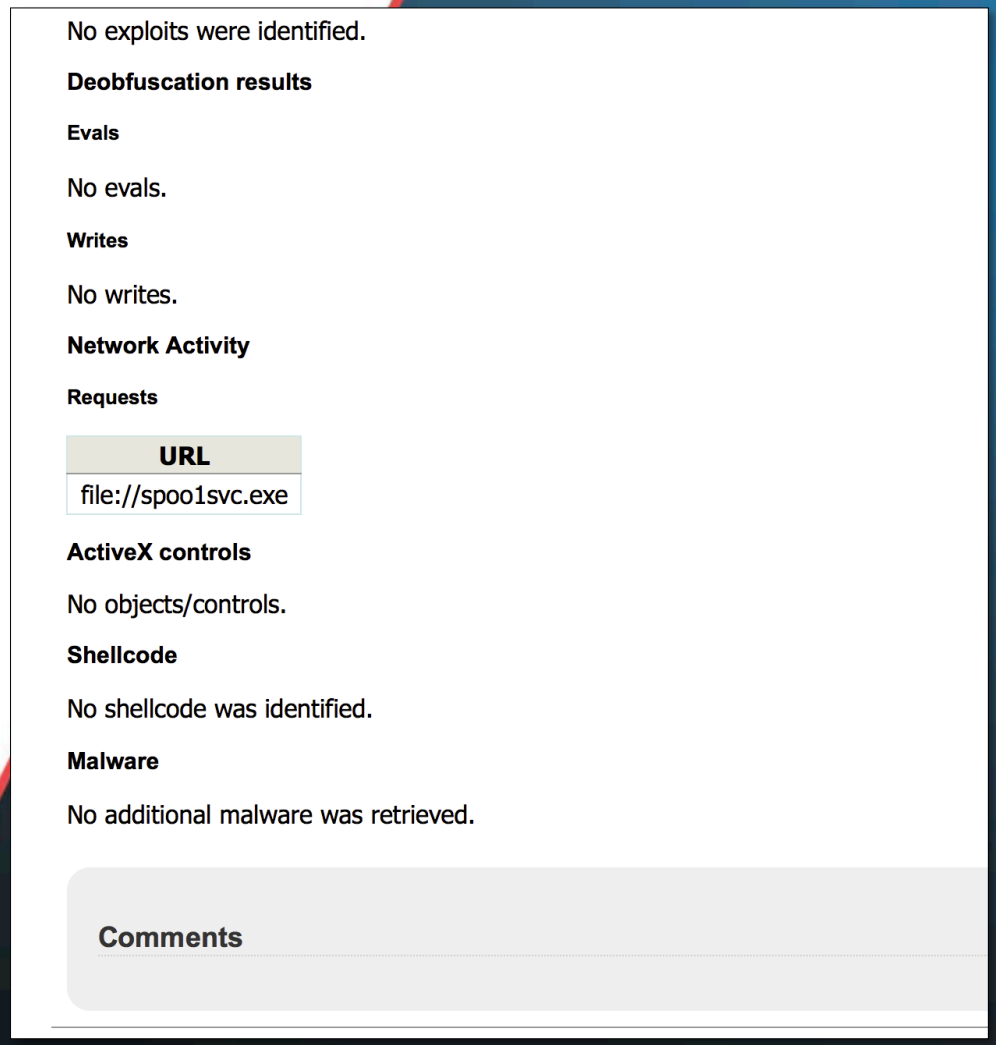
Incident Response

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.

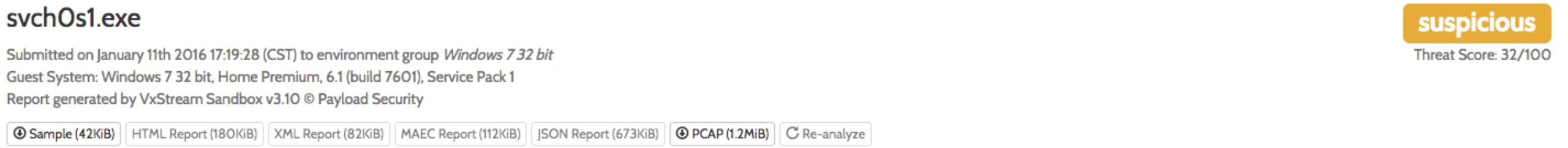
Malware

No additional malware was retrieved.

Comments

THREATSTREAM®

3rd gen sensor…



- *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!*

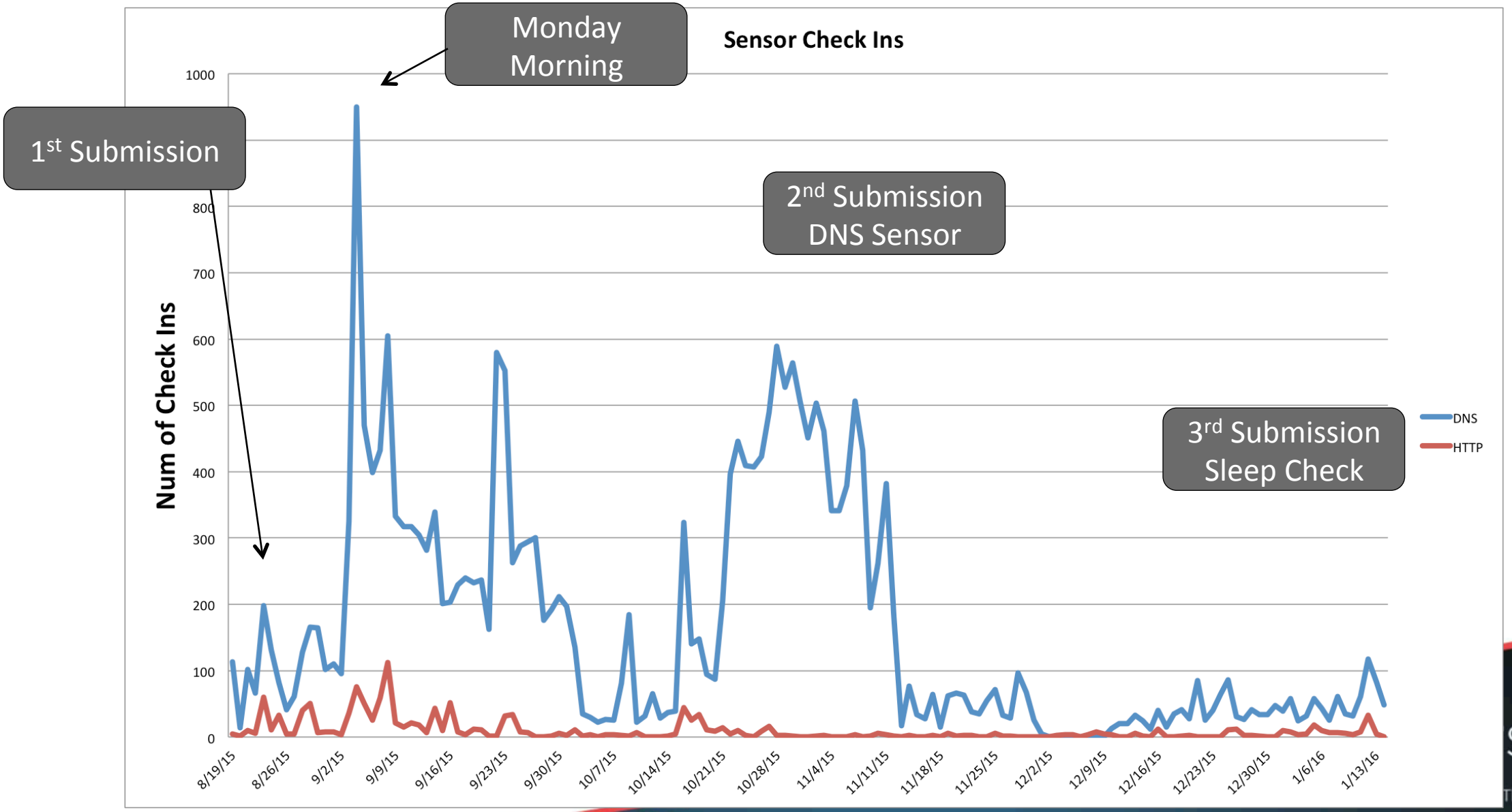
THREATSTREAM®

Sharing?

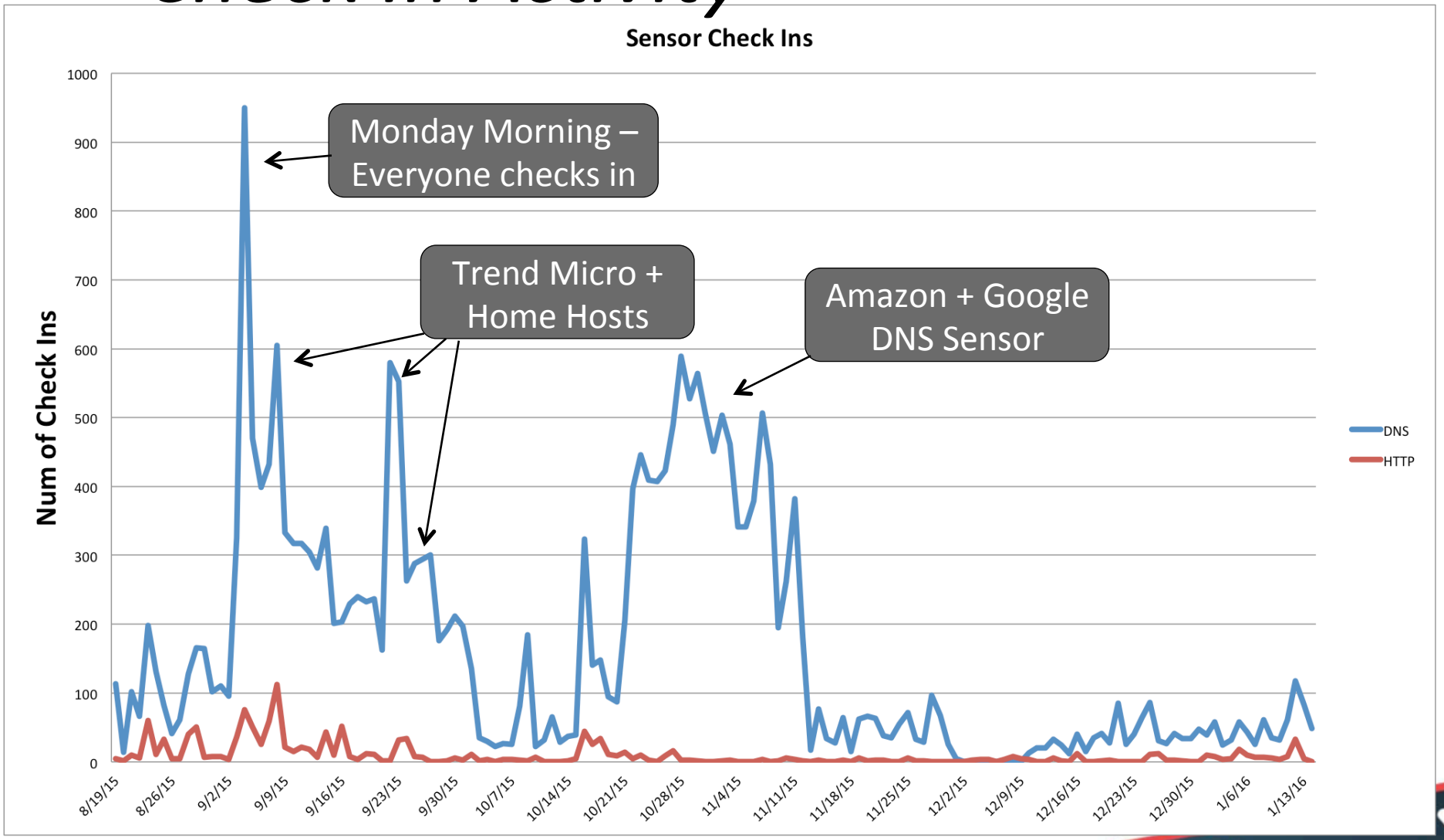
- Yup, Lots
- Samples shared
  - Evidence of new executions seen from different origins
- Domain names shared (or scraped)
  - Previous execution's domains resolved later by other orgs, different nameservers
  - Some domains appear on threat intel lists
- Many orgs are trivially identified as security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

THREATSTREAM®

Tipping off the Adversary

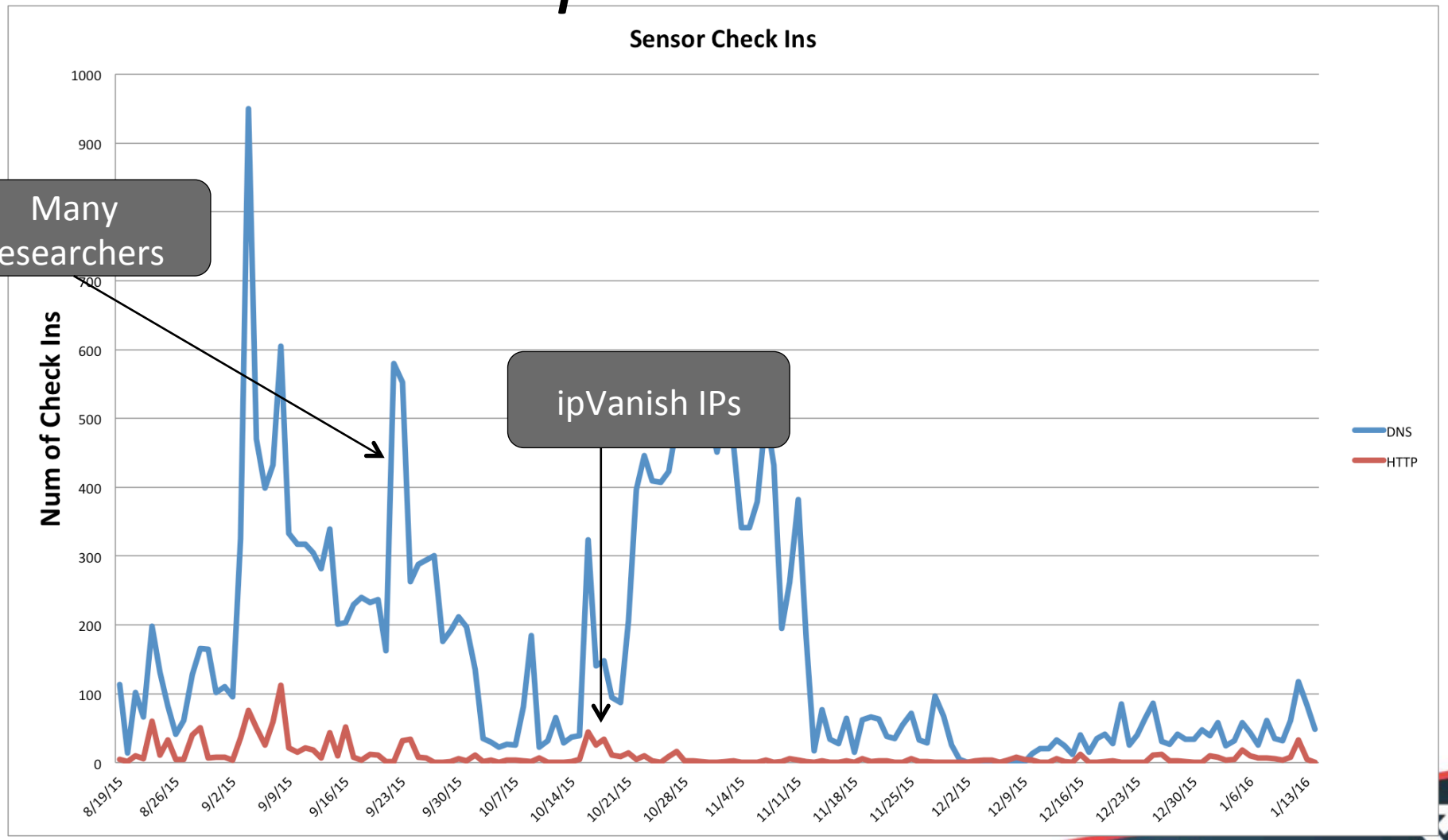


Check In Activity



THREATSTREAM®

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**

THREATSTREAM®

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

THREATSTREAM®