Malware Command and Control Channels
- a journey into Darkness -

By Brad Woodberg

- Emerging Threats Product Manager / Proofpoint
- @bradmatic517
- bradmatic@gmail.com

Agenda

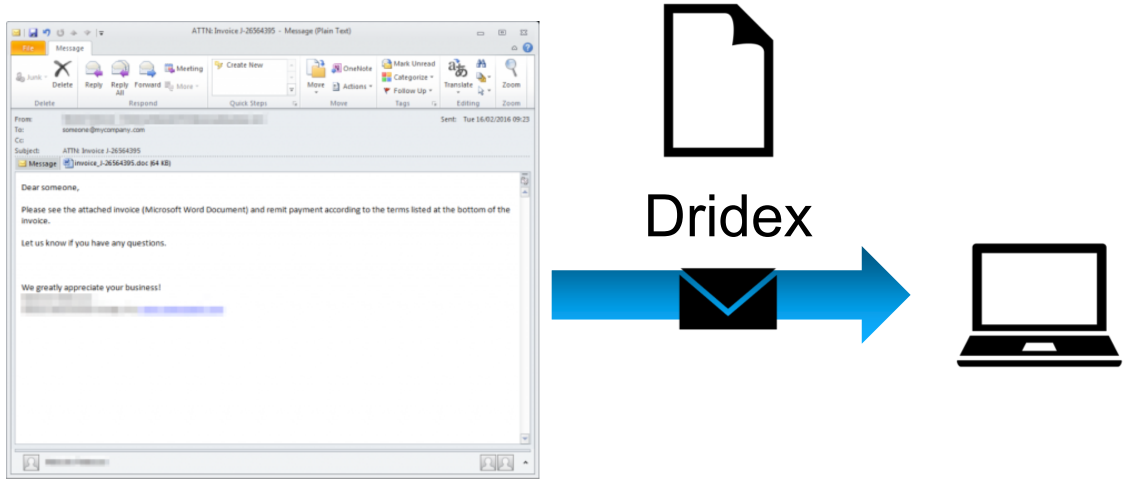
- C2 Intro and Background (7 mins)
- Modern C2 Techniques (6 mins)
- Case Studies (15 mins)
- Predictions for C2 (5 mins)
- Defense (10 mins)
- Wrap Up (2 mins)

Why Command & Control?

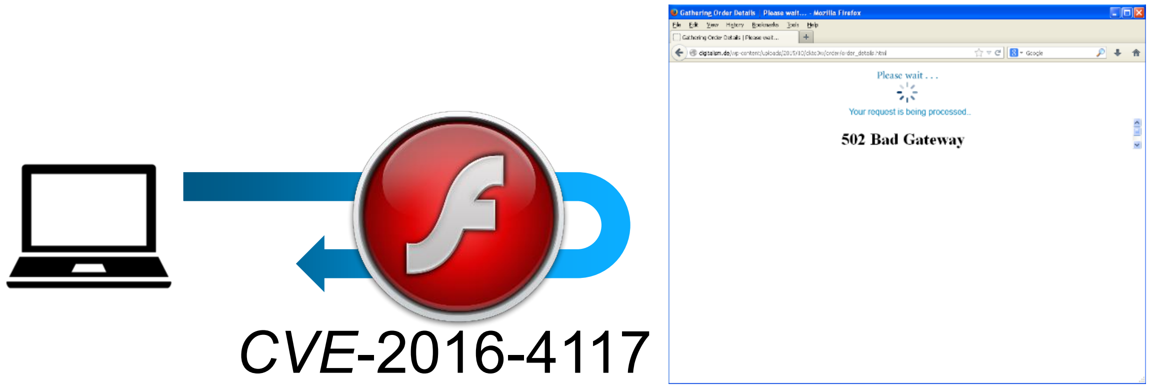
- Vulnerabilities, Exploits, and Malware grab the headlines and analyst focus
- While very interesting, it is also very noisy, many exploits fail, very FP prone.
- If you can effectively detect C2 activity, you have a high fidelity indicator that an asset is actually compromised.
- With C2, the tables are turned on attackers, they go on defense, and we go on offense.

Primary Breach Vectors

- Modern malware is delivered in one of two ways:
  - Executable Content: Binary executables, embedded executable content like macros typically through web or email channels on the network.
  - Exploit Driven: An exploit against a software vulnerability such as those against Flash, PDF, Java, Office Docs, Browsers, and other network enabled applications.



- Regardless of how modern malware compromises a system, it is rarely autonomous.



Angler EK

Why malware needs C2?

Initial malware execution may occur under non-ideal scenarios:

- Malware may land on a non-target asset
- Malware may not have sufficient privileges when it executes
- Malware may be delivered in pieces to evade detection / fit into buffers
- Malware may require payload before it is malicious (e.g. TinyLoader)
- Malware may require coordination with C2 for operating instructions before it takes action (e.g. Crypto Ransomware waiting to receive a key)

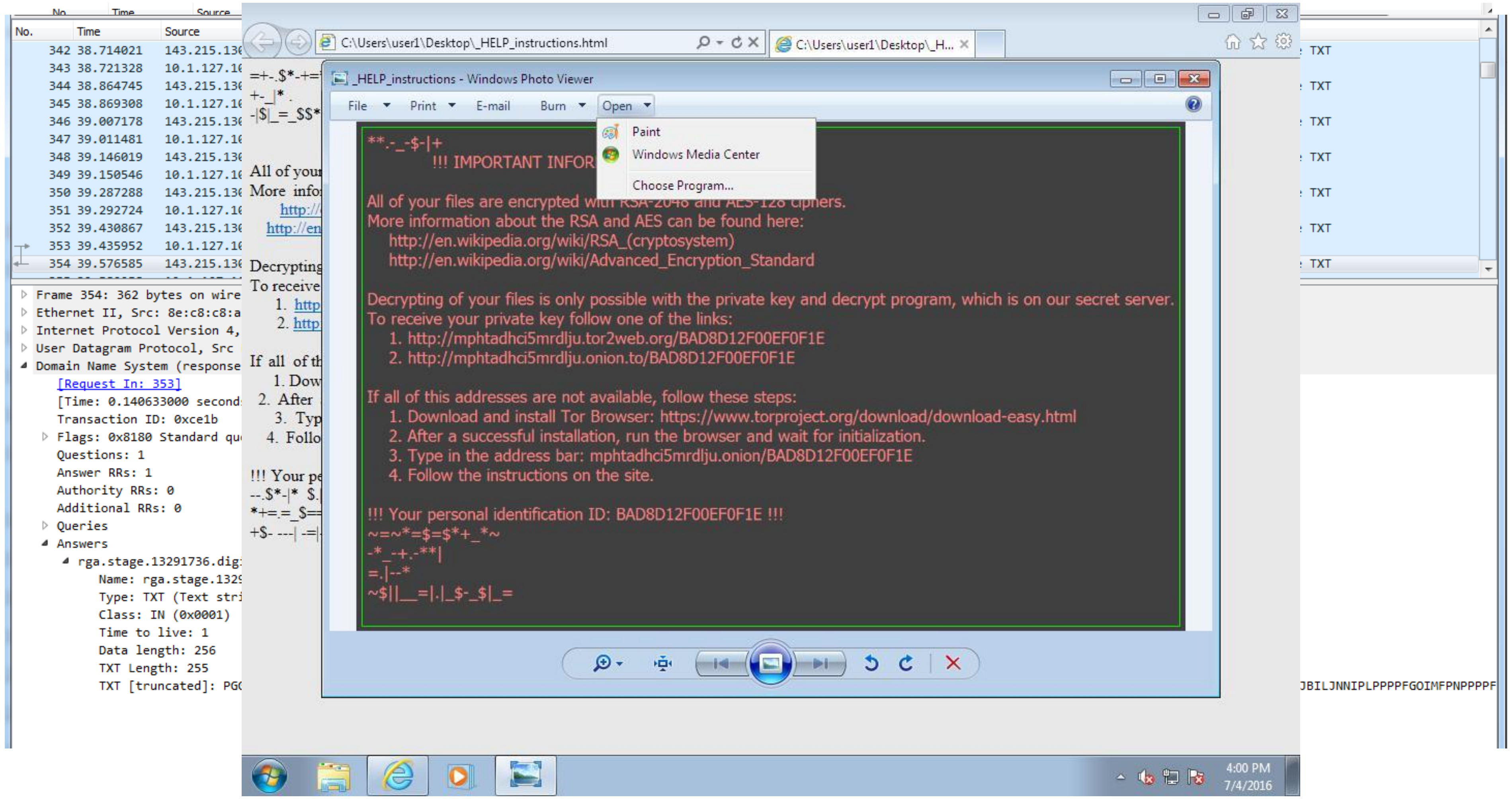
Enter Command and Control

Escalation

- Complete malware breach by acquiring additional executables, payloads, and configurations.
  - May be as simple as a word doc downloading an EXE (e.g. Dridex),
  - Or as complex as a dropper downloading an entirely new malware (e.g. Tinyloader / AbaddonPoS)
- Escalation stage is often carried out by contacting C2 Infrastructure
- This communication often leverages different infrastructure, protocols, and methods than the initial infection.
  - Often because infection infrastructure is rented, and C2 is managed by a different actor.

Exfiltration

- This phase is where the malware delivers on it's intended purpose
- Exfiltrated data often includes stealing intellectual property, exposing attributes of a target network, or larger escalation of an attack.
- Locky Cataloguing Endpoint Files to C2
- ZBOT (Zeus variant) DNS Covert Channel



Infection in Action: Angler Exploit Kit

Sample: 26907326de17c8c3f17c13bf32f61810

Alerts | Connections | DNS | HTTP

Date	Sid	Signature	Rev	SrcIP	SrcPort	DstIP	DstPort
2016-05-17	2819805	ETPRO TROJAN CryptXXX CnC Beacon	3	private	49198	144.76.82.19	443
2016-05-17	2819805	ETPRO TROJAN CryptXXX CnC Beacon	3	private	49197	144.76.82.19	443
2016-05-17	2820097	ETPRO DELETED CryptXXX 2.06 Checkin	1	private	49197	144.76.82.19	443
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49193
2016-05-17	2811284	ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2	2	5.39.35.232	80	private	49185
2016-05-17	2820164	ETPRO CURRENT_EVENTS Angler EK Payload May 10 2016 M2 T1	2	5.39.35.232	80	private	49185
2016-05-17	2811284	ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2	2	5.39.35.232	80	private	49183
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49185
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49183
2016-05-17	2014726	ET POLICY Outdated Windows Flash Version IE	82	private	49183	5.39.35.232	80
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49183
2016-05-17	2816941	ETPRO CURRENT_EVENTS Angler EK Flash Exploit URI Struct Apr 07 IE	3	private	49183	5.39.35.232	80
2016-05-17	2815888	ETPRO CURRENT_EVENTS Possible Angler EK Landing Jan 21 M3	3	5.39.35.232	80	private	49178
2016-05-17	2816511	ETPRO CURRENT_EVENTS Angler EK Landing Mar 02 2016 M1 T1	2	5.39.35.232	80	private	49178
2016-05-17	2816932	ETPRO CURRENT_EVENTS Angler EK Landing with URI Primer Apr 06	2	5.39.35.232	80	private	49178
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49178
2016-05-17	2022772	ET CURRENT_EVENTS Evil Redirector Leading to EK Apr 28 2016	3	72.167.3.128	80	private	49163

Target Compromised, C2

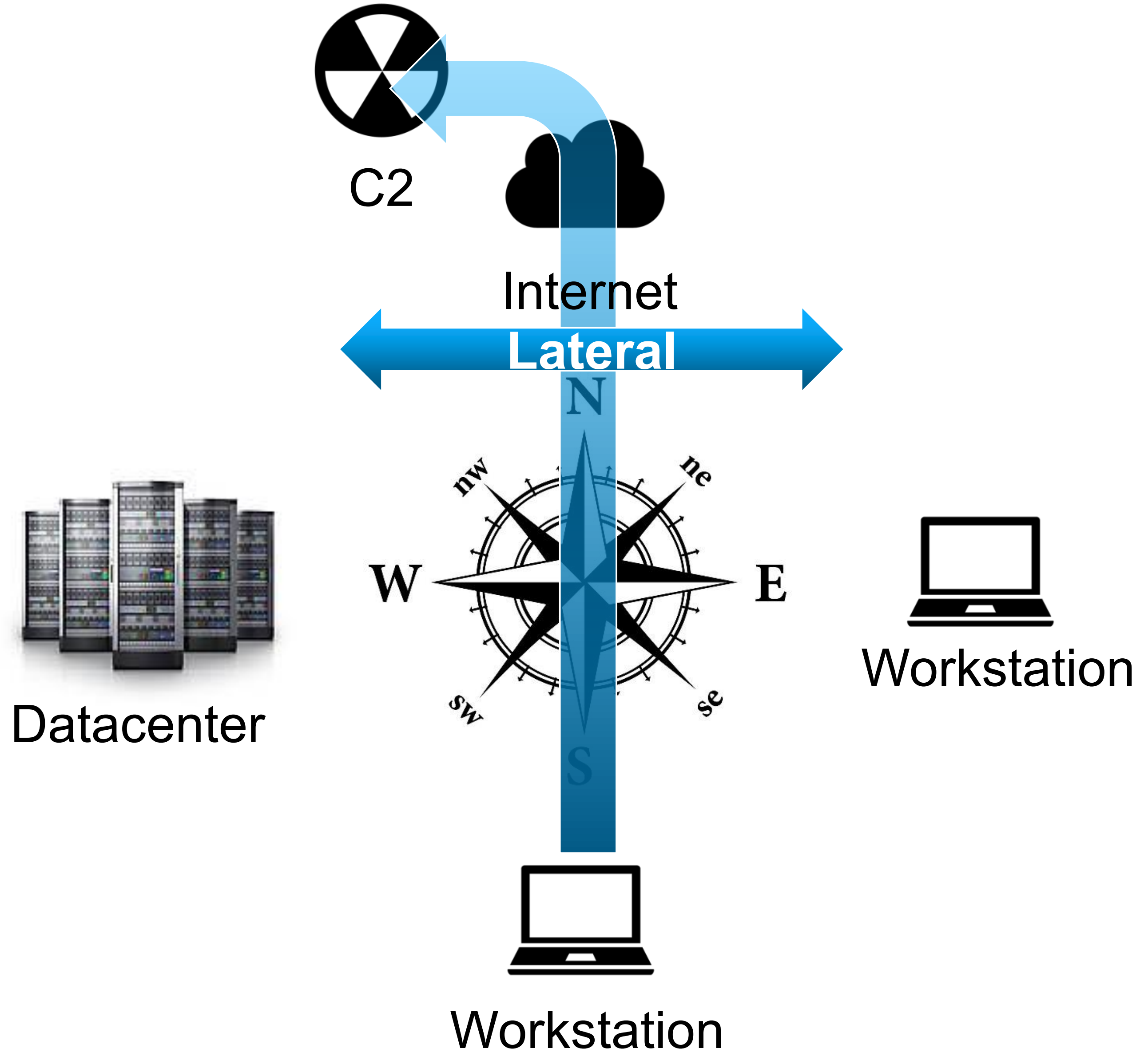
Exploit / Payload Delivered

TDS Evaluates Target Client

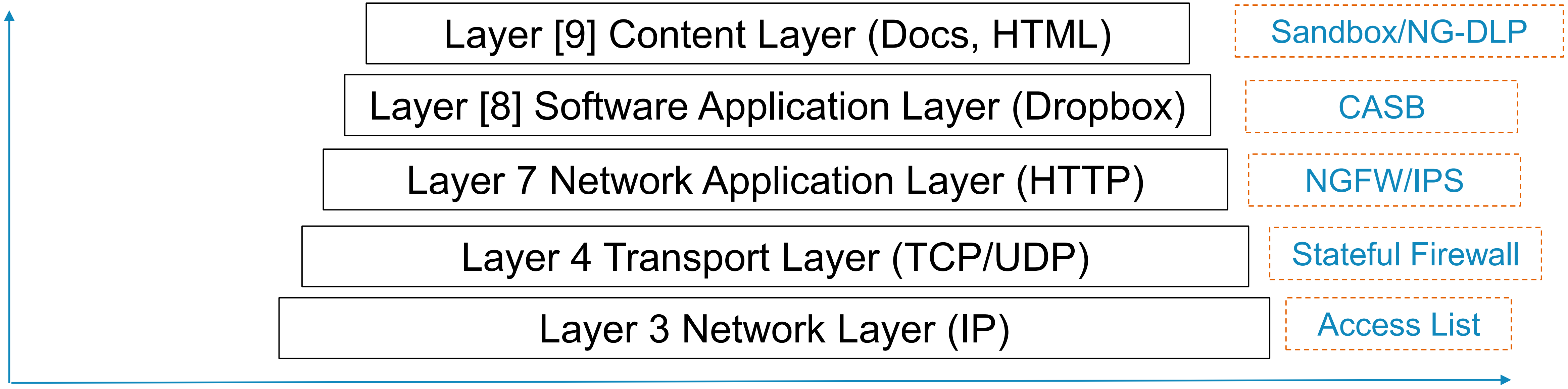
Redirect to Angler Infrastructure

Lateral Infection vs. C2

- Lateral Infection is not the same as C2!
- Lateral Infection focuses on Three Phases:
  - Introspection: Local device scanning
  - Network Scanning: mapping the network for potential targets and pivot points.
  - Exploit and Spread: Compromise other assets.
- LI typically involves using native networking protocols to scan and spread within an organization (e.g. Locky using SMB to encrypt file shares)
- LI often spreads by leveraging standard network protocols like SMB, WMI, SSH, vs. C2 channels which are often over HTTP/S, ToR, or custom protocols.



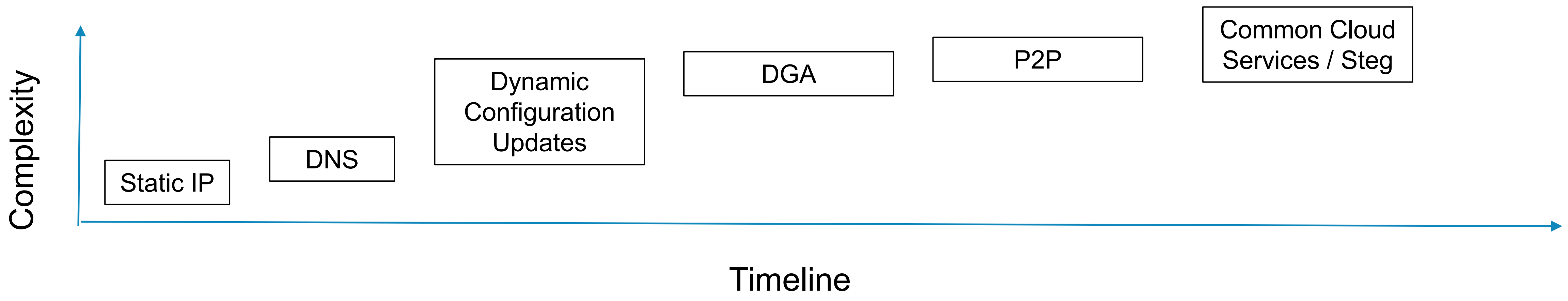
C2 Channel Evolution: Cat and Mouse



- Malware noted that keeping explicit strings in the payload would be easy to identify (e.g. GhostRat). The same is true for potentially unwanted applications like Bittorent / Tor / Skype which also leveraged evasion techniques.
- To evade NGFW and other deep inspection technologies, malware shifted to leverage steganographic techniques to hide in plain sight. E.g. Sninfs
- Finally, malware has evolved even further to leverage highly obfuscated and embedded communication channels like jpgs, flash, encoded ASCII.
- In addition to the advanced obfuscation, malware has gone to great lengths to hide itself in legitimate, cloud applications.

- Early malware just used fixed non-standard ports to communicate e.g. Back Orifice 1998).
- Early malware often heavily leveraged IRC channels for a simple C2 infrastructure e.g. PrettyPark (1999)
- As some organizations tamped down on allowing ports outside of TCP 80/443 to communicate to the internet, so did malware evolve.
- Enter the NGFW which leveraged Layer 7 payload inspection (similar to IPS) to identify applications rather than attacks.

C2 Hosting Evolution



- Early days C2 infrastructure was very fixed. Similar to traditional computing, it was physical machines in data centers with static IP's.
- While DNS was prominent, domain names for malware would not change very quickly.
- Configuration Updates via CNC
- This weak link made for a great target for vendors providing defense mechanisms. So malware evolved as well to domain generation algorithms (DGA's) which could quickly cycle through generated domain names to eliminate single points of failure. E.g. Conficker
- The issue with DGA's is that the algorithm can be reverse engineered, and it still relies on DNS. Enter P2P Mechanisms like GameOver-Zeus
- To offset the potential disruptions for DGA's, malware started leveraging common cloud services which enterprises are adverse to blocking as they may serve a business function.

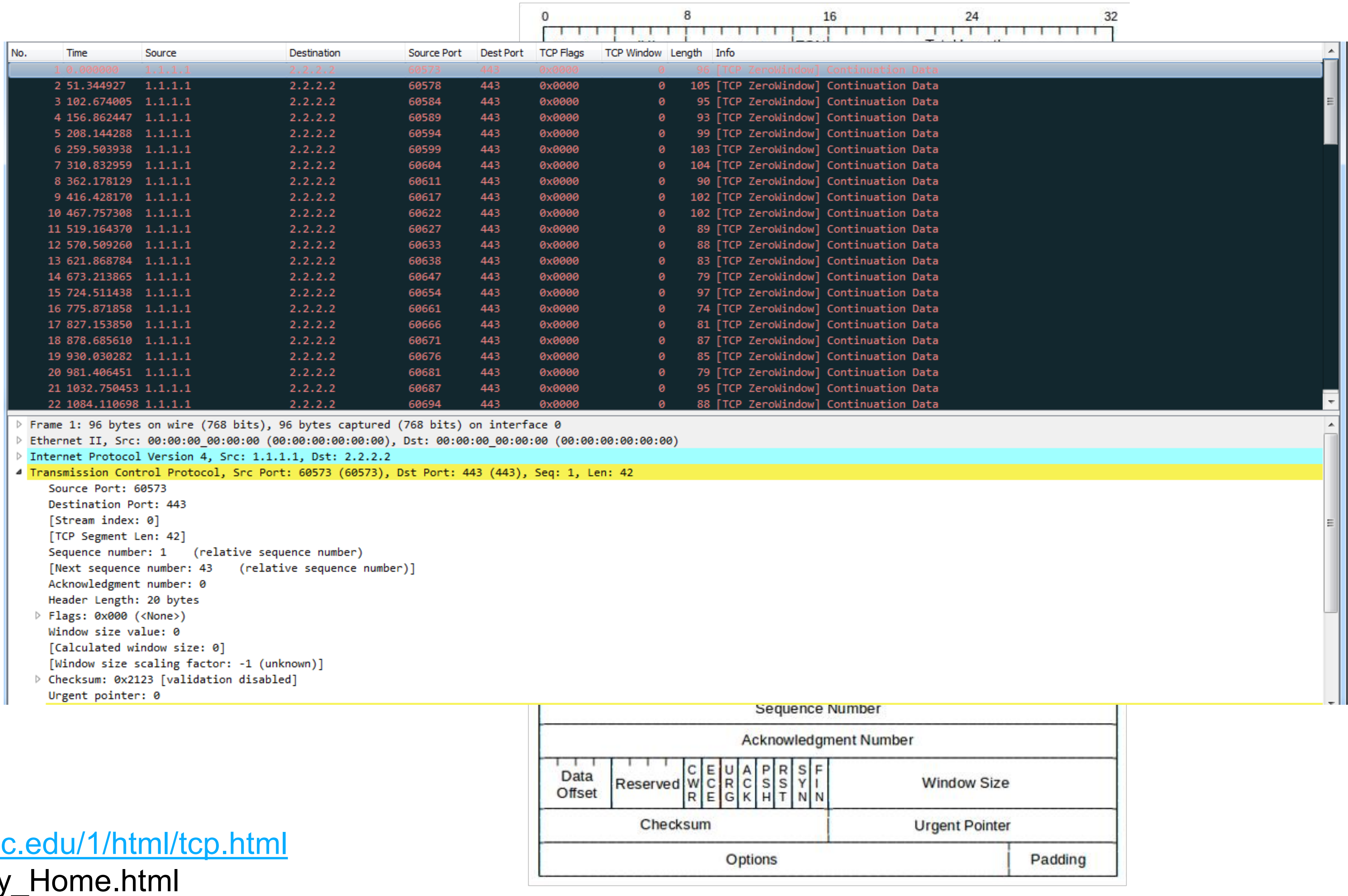
C2 & Steg:

- "Never write if you can speak; never speak if you can nod; never nod if you can wink.“
  - Martin Lomasney, Gangster, Politician (1859-1933)

- Steganography (Steg) is hiding in plain sight. It has been used for centuries and provides plausible deniability.
- Protocol Headers, Metadata in Files, Altering Bits in Data, Unicode &c &c &c.
- Examples of how C2 can leverage Steg includes Embedding Configuration in Images, Audio, Video, File Metadata, and even network protocols!
- You can also layer Steg with encryption/encoding for additional obfuscation.

C2 Steg Continued

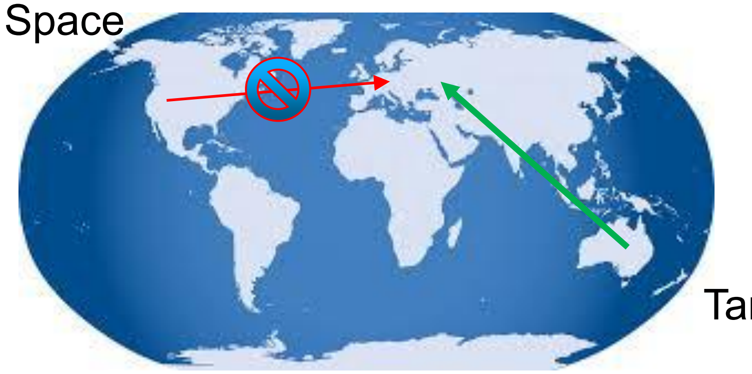
- Deterministically identifying when Steg is in use can be very expensive if not nearly impossible in many scenarios, especially when processing network streams in real time.
- This makes Steg a perfect choice for enhancing the robustness of malware C2.



Source: IPv4/V6/TCP Header, LUC http://intronetworks.cs.luc.edu/1/html/tcp.html
OpenPuff: http://embeddedsw.net/OpenPuff_Steganography_Home.html

C2 - Counter Offense Techniques

- Attackers think economically, want their malware to last as long as possible thus bringing the most ROI.
- Malware authors utilize several counter detection techniques to ensure the viability of their malware.
  - Filter who can connect (e.g. IP filtering to eliminate non-targets, researchers and sandboxing tools.)
  - Secret Handshakes: E.g. leverage custom TCP stacks or special low level handshakes that only illicit responses if correct handshake is used (e.g. Poison Ivy)
  - Encryption: Predefined SSL Certificates embedded in malware for authenticating client/servers
  - Steg:
- Anecdotally, we've seen an increase in anti-sandboxing techniques to prevent execution and avoid detection.



256 Byte Challenge Request

256 Byte Challenge Response

SSL Certificate Information

Subject Common Name:	p292.tbuseourercl.va
Subject:	C=MH, L=Majuro, O=Tfoweingi Tinssisas Co., CN=p292.tbuseourercl.va
Issuer Common Name:	p292.tbuseourercl.va
Issuer:	C=MH, L=Majuro, O=Tfoweingi Tinssisas Co., CN=p292.tbuseourercl.va
SSL Version:	TLSv1
Fingerprint (SHA1):	9663b6799ba20d68734cc99aa83d6bbb0506f064
Status:	**Blacklisted** (Reason: Dridex C&C, Listing date: 2016-07-15 10:57:42)

Source: Abuse.CH
https://sslbl.abuse.ch/intel/9663b6799ba20d68734cc99aa83d6bbb0506f064

C2 Flavors: Crimeware vs. Targeted

Crimeware:

- General Purpose
- Widely distributed
- Go to greater lengths to evade detection from a protocol perspective
- Yet quite chatty on C2 channels

Targeted:

- Highly selective victims
- Will be custom built to navigate individual networks, common platforms.
- Often does not go to great lengths from an obfuscation perspective

Targeted Espionage:

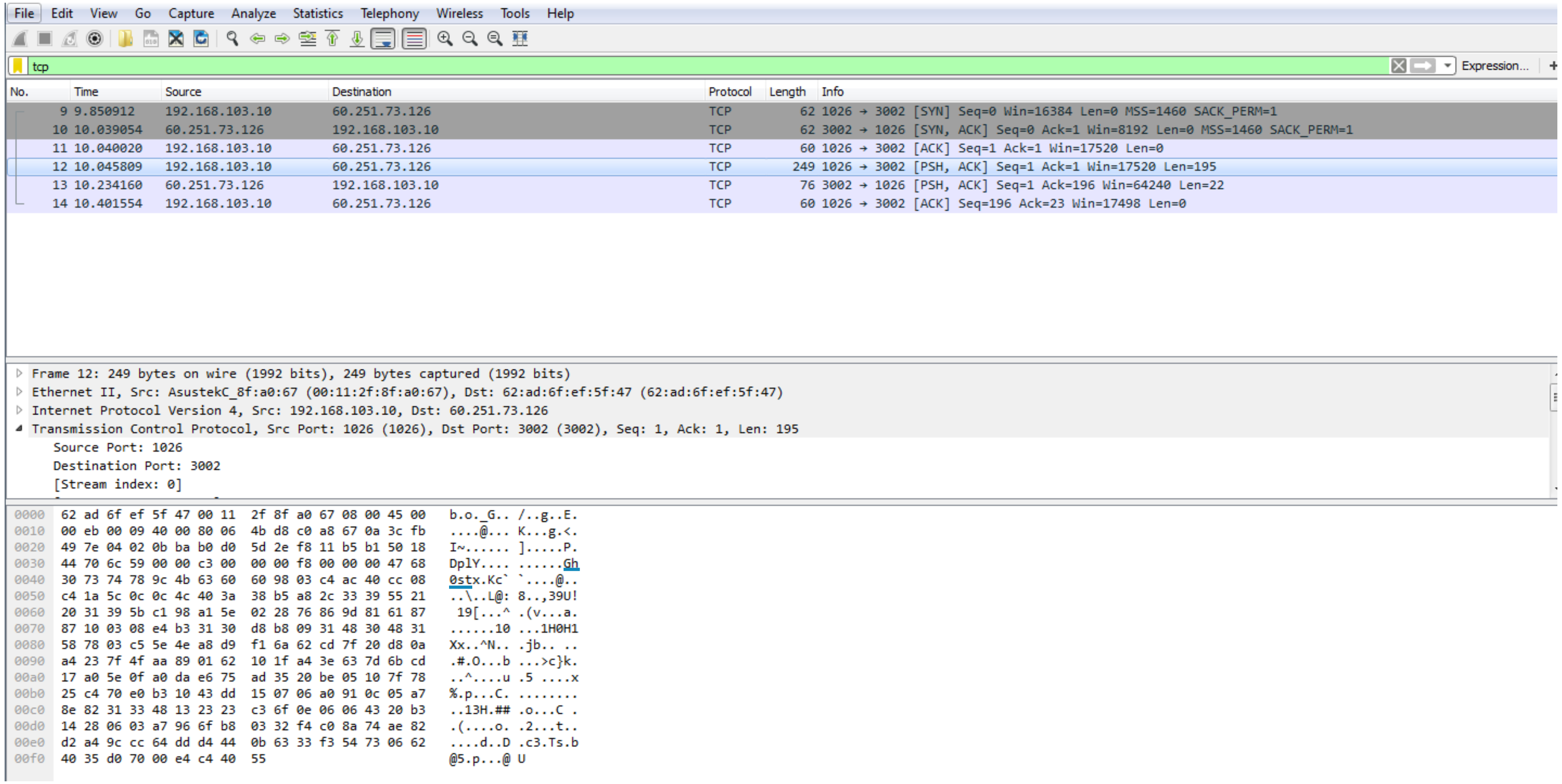
- Most exotic form of malware/C2
- Far more sophisticated than traditional targeted.
- May lack network based C2 channels altogether.
- May leverage insiders as well as covert HW to bridge air gaps.

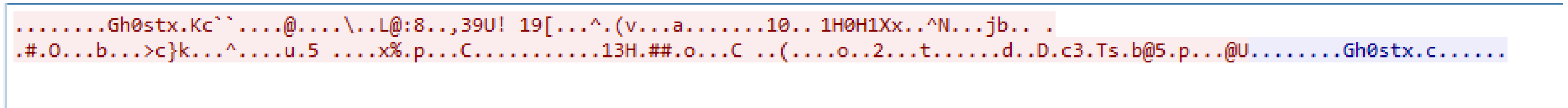
Case Studies

- Now that we've covered the background and evolution, let's take a look at actual malware C2 channels to reinforce our examples.
- Note that there are often a great many variants for each malware and some leverage different communication than the mainstream samples which we will cover.

Gh0stRAT

- Basic C2 Protocol
- Common strains support a basic non-encoded string in the PCAP.
- 'Gh0st' string in initial payload to identify malware
- Non-Standard Port easily filterable

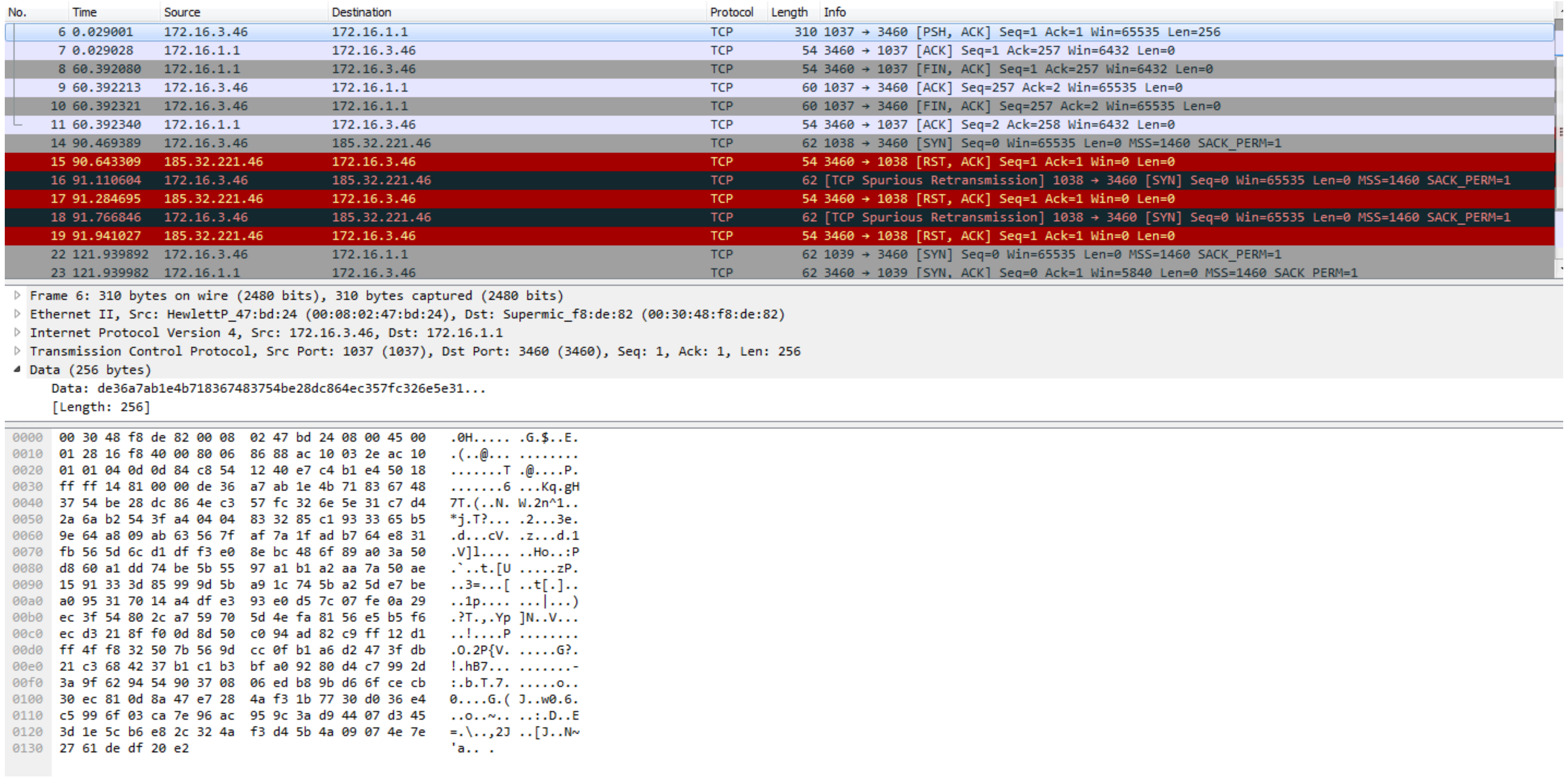




Further Reading: http://malware-unplugged.blogspot.com/2015/01/hunting-and-decrypting-communications.html

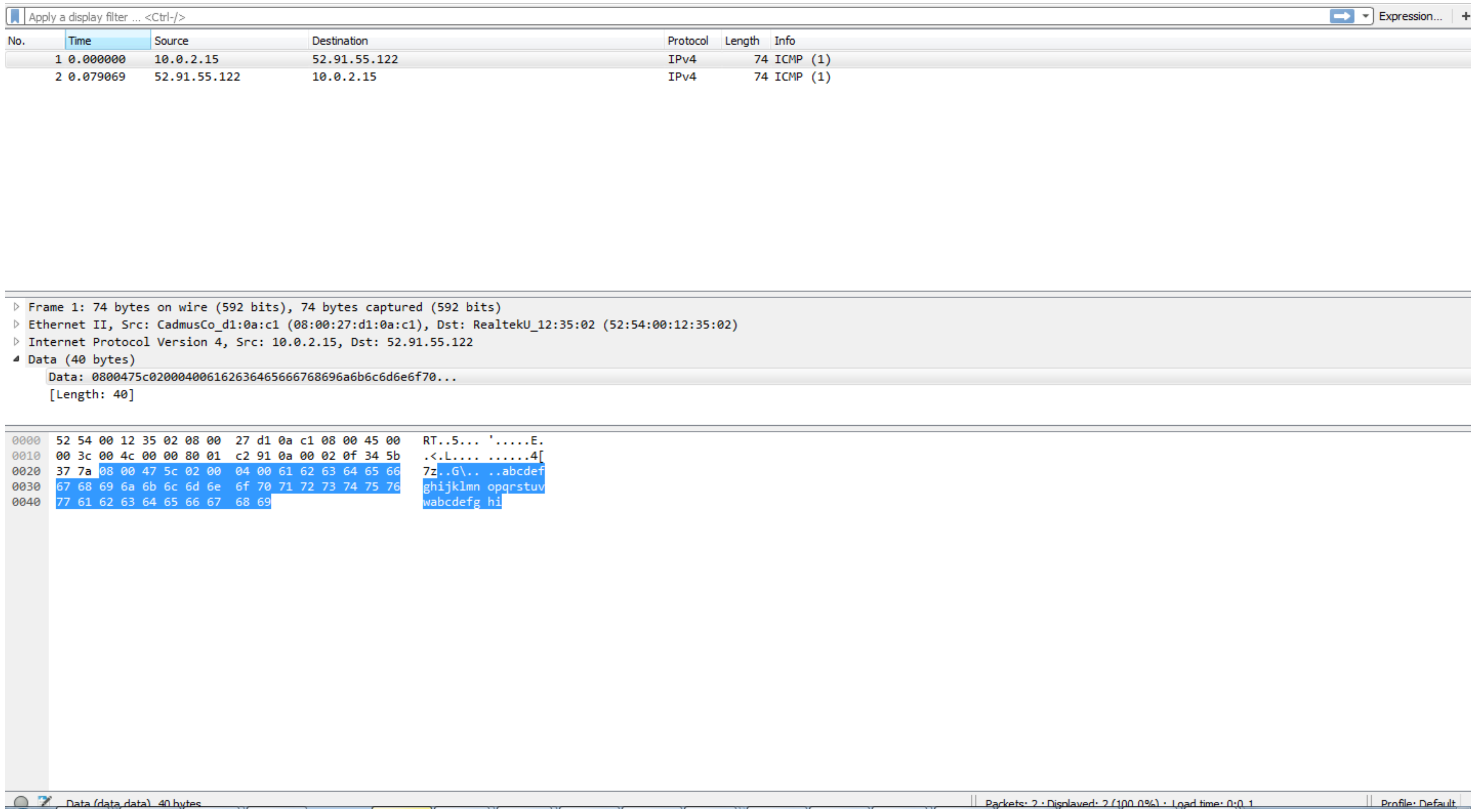
PoisonIvy

- Unknown Encrypted, 256 Byte handshake
- Does not contain explicit strings in handshake which are easy to key on.
- Available since 2005, still very popular and little changed despite being in the wild so long.
- 256 Byte Handshake is exchanged in a CHAP like sequence. Client sends a hello which allows the server to prevent it from communicating with an unknown client.
- The server will only accept the client communication if it has been encrypted with the right password.



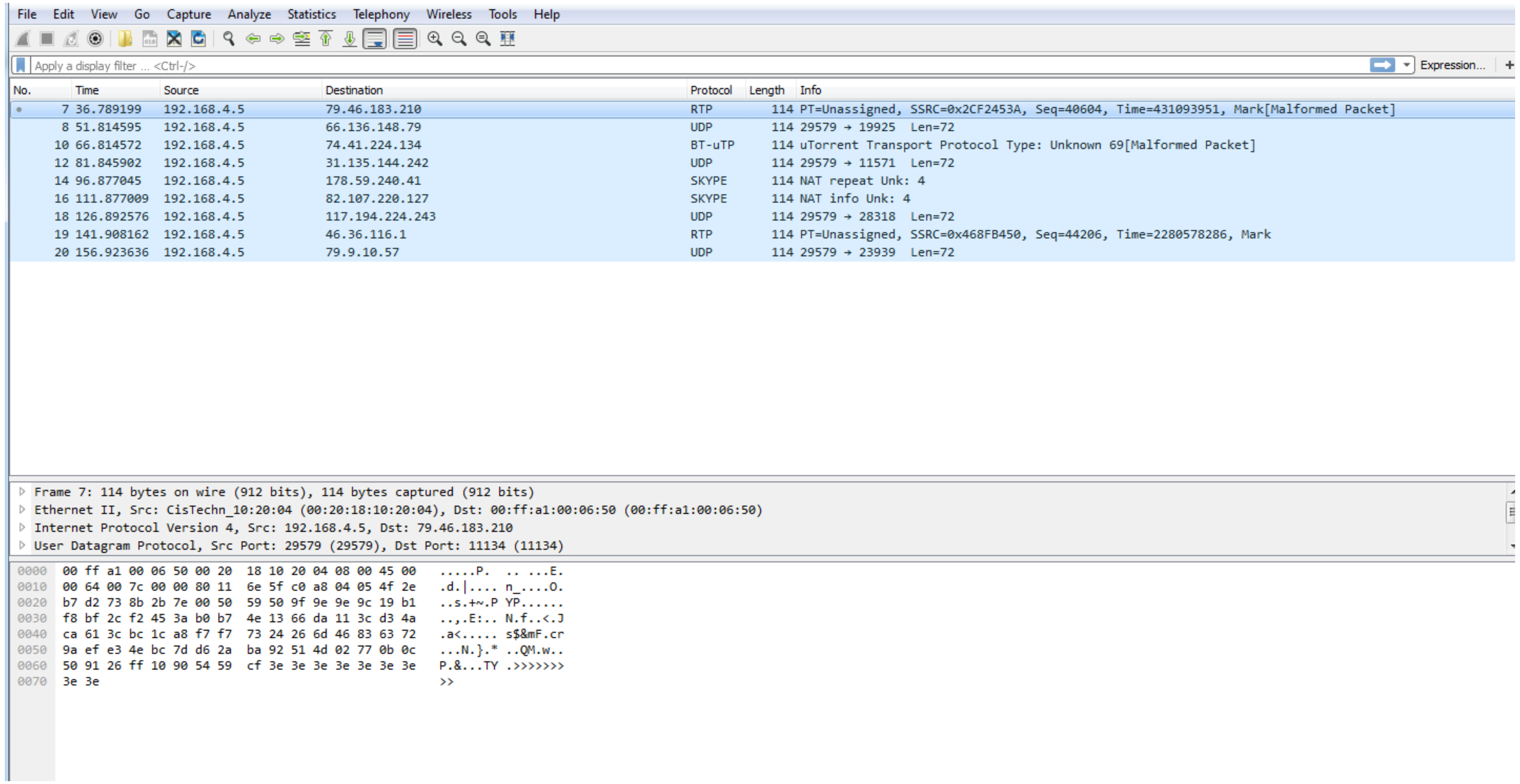
NanoLocker

- Some malware leverage common network utilities and infrastructure to embed C2 functionality
- NanoLocker leverages ICMP to ping a hardcoded address 52.91.55.122 with an ICMP payload of the ransomware Bitcoin address. It will also send follow up payloads of the number of files encrypted on the system.



GameOver/Zeus

- GameOver / Zeus attempted to obfuscate its activities by leveraging P2P protocols to avoid single points of failure similar to how traditional P2P filesharing services work (loosely based on Kademlia DHT techniques
- Zeus leveraged basic rolling XOR for packet payloads to make signature based IDS difficult. UDP Payloads
  - Emphasizes the point that often times the malware authors will just attempt to stay one step ahead of security solutions rather than implement the most state of the art attacks.



Further Reading: https://www.sans.org/reading-room/whitepapers/detection/analysis-gameover-zeus-network-traffic-35742

Dridex using Pastebin as C2 (aka Blind Drop)

- Virtually any cloud service can be used for C2. in this example Pastebin is leveraged.
- While sites like Pastebin might be simple to turn off, Twitter, Amazon, and Facebook may have legitimate business purposes.
- Malware may hide in comments, images, video and uploaded content.

Sample: ce181f45efb519504e54fed5daa45cc7

MD5 ce181f45efb519504e54fed5daa45cc7
Submision Date 2015-08-11 17:38:02
Type PCAP

SHA256 N/A
File Size N/A
VirusTotal 17/57

Alerts | Connections | DNS | HTTP

Date	Sid	Signature	Rev	SrcIP	SrcPort	DstIP	DstPort
2015-08-11	2021621	ET TROJAN Possible Dridex SSL Cert Aug 12 2015	6	94.23.110.45	443	private	49442
2015-08-11	2021621	ET TROJAN Possible Dridex SSL Cert Aug 12 2015	6	195.154.184.240	1443	private	49433
2015-08-11	2812390	ETPRO TROJAN Possible Dridex Exe Command in Pastebin Title	2	190.93.240.15	80	private	49432
2015-08-11	2812389	ETPRO TROJAN Possible Dridex Open Command in Pastebin Title	2	190.93.240.15	80	private	49432
2015-08-11	2014520	ET INFO EXE - Served Attached HTTP	6	185.14.29.178	80	private	49431
2015-08-11	2021076	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	2	185.14.29.178	80	private	49431
2015-08-11	2014520	ET INFO EXE - Served Attached HTTP	6	185.14.29.178	80	private	49431
2015-08-11	2021076	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	2	185.14.29.178	80	private	49431
2015-08-11	10000029	FILE ET magic PE32	2	185.14.29.178	80	private	49431
2015-08-11	2000419	ET POLICY PE EXE or DLL Windows file download	22	185.14.29.178	80	private	49431
2015-08-11	2021244	ET TROJAN Dridex Download June 10 2015	2	185.14.29.178	80	private	49431
2015-08-11	2812388	ETPRO TROJAN Possible Dridex 0 byte POST to Pastebin	3	private	49430	190.93.240.15	80

Dalexis: ToR as a C2 Channel

- After an initial infection, malware hops to TOR2Web a clientless TOR implementation for C2 Activity
- TOR allows botnet operators to evade communication snooping in intermediate systems.

Sample: eef89c15b2625a8614d8c898fb802e04

MD5 eef89c15b2625a8614d8c898fb802e04
Submision Date 2015-02-10 17:03:21
Type PE32 executable (GUI) Intel 80386, for MS Windows

SHA256 c026e9528b880d62e686c837494da9d6fc3ed90374f69c5496de63066eb9f575
File Size 46592
VirusTotal 47/54

Alerts | Connections | DNS | HTTP

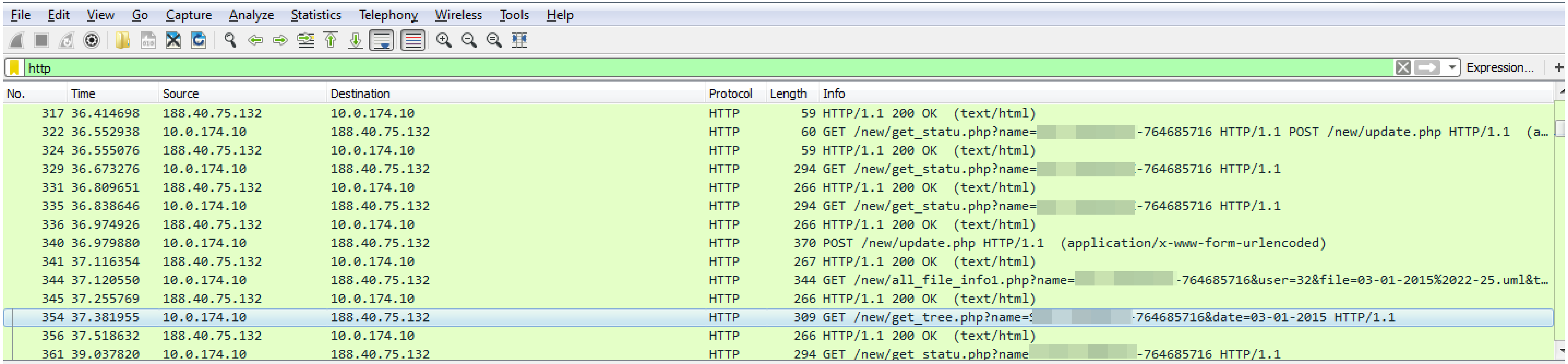
Date	Sid	Signature	Rev	SrcIP	SrcPort	DstIP	DstPort
2015-10-11	2018879	ET POLICY onion.cab tor2web .onion Proxy domain in SNI	1	private	49380	188.138.122.22	443
2015-10-11	2018876	ET POLICY onion.cab .onion Proxy DNS lookup	1	private	53212	8.8.8.8	53
2015-10-11	2020358	ET TROJAN Critroni Variant .onion Proxy Domain	1	private	53212	8.8.8.8	53
2015-10-11	2018876	ET POLICY onion.cab .onion Proxy DNS lookup	1	private	53212	8.8.8.8	53
2015-10-11	2020358	ET TROJAN Critroni Variant .onion Proxy Domain	1	private	53212	8.8.8.8	53
2015-10-11	2015576	ET POLICY DNS Query to .onion proxy Domain (tor2web)	6	private	62661	8.8.8.8	53
2015-10-11	2020358	ET TROJAN Critroni Variant .onion Proxy Domain	1	private	62661	8.8.8.8	53
2015-10-11	2015576	ET POLICY DNS Query to .onion proxy Domain (tor2web)	6	private	62661	8.8.8.8	53
2015-10-11	2020358	ET TROJAN Critroni Variant .onion Proxy Domain	1	private	62661	8.8.8.8	53
2015-10-11	2808413	ETPRO POLICY telize.com IP lookup	2	private	49366	46.19.37.108	80
2015-10-11	2019925	ET TROJAN Win32/Dalexis.A Possible SSL Cert (cargol.cat)	2	217.149.7.213	443	private	49354
2015-10-11	2019924	ET TROJAN Win32/Dalexis.A Possible SSL Cert (ppc.cba.pl)	2	85.17.73.180	443	private	49353

C2 Connection via Tor2Web

Probing for TOR Endpoint

Initial Compromise

AridViper



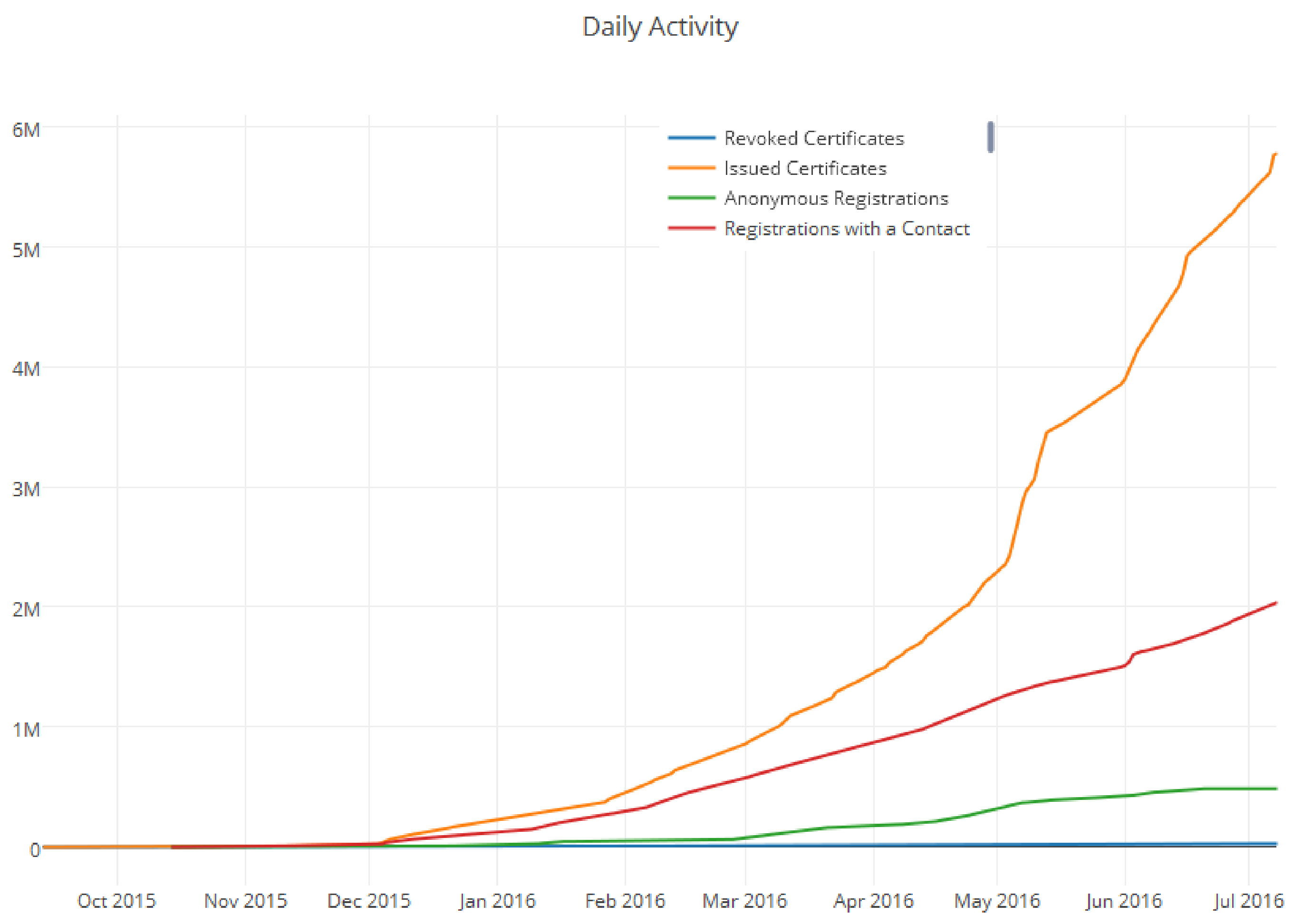
No.	Time	Source	Destination	Protocol	Length	Info
317	36.414698	188.40.75.132	10.0.174.10	HTTP	59	HTTP/1.1 200 OK (text/html)
322	36.552938	10.0.174.10	188.40.75.132	HTTP	60	GET /new/get_statu.php?name=[redacted]-764685716 HTTP/1.1 POST /new/update.php HTTP/1.1 (a…
324	36.555076	188.40.75.132	10.0.174.10	HTTP	59	HTTP/1.1 200 OK (text/html)
329	36.673276	10.0.174.10	188.40.75.132	HTTP	294	GET /new/get_statu.php?name=[redacted]-764685716 HTTP/1.1
331	36.809651	188.40.75.132	10.0.174.10	HTTP	266	HTTP/1.1 200 OK (text/html)
335	36.838646	10.0.174.10	188.40.75.132	HTTP	294	GET /new/get_statu.php?name=[redacted]-764685716 HTTP/1.1
336	36.974926	188.40.75.132	10.0.174.10	HTTP	266	HTTP/1.1 200 OK (text/html)
340	36.979880	10.0.174.10	188.40.75.132	HTTP	370	POST /new/update.php HTTP/1.1 (application/x-www-form-urlencoded)
341	37.116354	188.40.75.132	10.0.174.10	HTTP	267	HTTP/1.1 200 OK (text/html)
344	37.120550	10.0.174.10	188.40.75.132	HTTP	344	GET /new/all_file_info1.php?name=[redacted]-764685716&user=32&file=03-01-2015%2022-25.uml&t…
345	37.255769	188.40.75.132	10.0.174.10	HTTP	266	HTTP/1.1 200 OK (text/html)
354	37.381955	10.0.174.10	188.40.75.132	HTTP	309	GET /new/get_tree.php?name=[redacted]-764685716&date=03-01-2015 HTTP/1.1
356	37.518632	188.40.75.132	10.0.174.10	HTTP	266	HTTP/1.1 200 OK (text/html)
361	39.037820	10.0.174.10	188.40.75.132	HTTP	294	GET /new/get_statu.php?name[redacted]-764685716 HTTP/1.1

- Targeted malware which leverages basic HTTP over standard ports to blend in.
- This stream is composed of initial client registration to C2 server, along with post registration activity to validate interesting files on the system.
- Arid Viper originally focused on Israeli targets

Source: Proofpoint: https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View

C2 Trends and Projections: Encryption

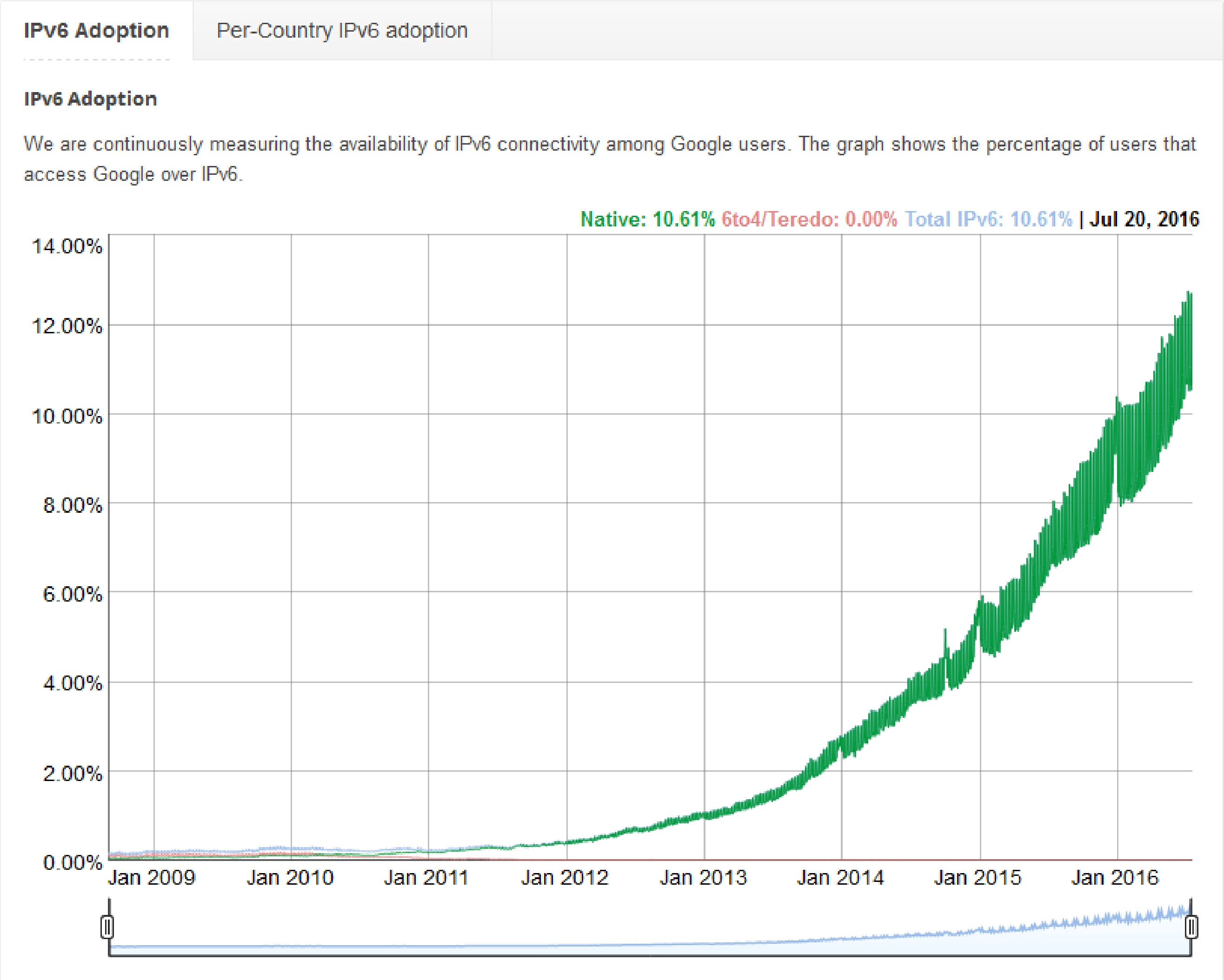
- Encryption:
  - SSL adoption has rapidly gained steam in the last few years, SandVine Projects 70% encryption in 2016
  - Let's Encrypt could be huge game changer for malware
  - Previously cost/overhead was high for SSL, Let's Encrypt eliminates this limitation.
  - Won't impact state sponsored or targeted attacks much, but will impact Crimeware heavily.



Source: Ilya Grigorik, Google: https://plus.google.com/+IlyaGrigorik/posts/GboyXCXxjGr
Source: Let's Encrypt: https://letsencrypt.org/stats/
Source: SandVine Spotlight Encrypted Traffic Report: https://www.sandvine.com/trends/encryption.html

C2 Trends and Projections: IPv6

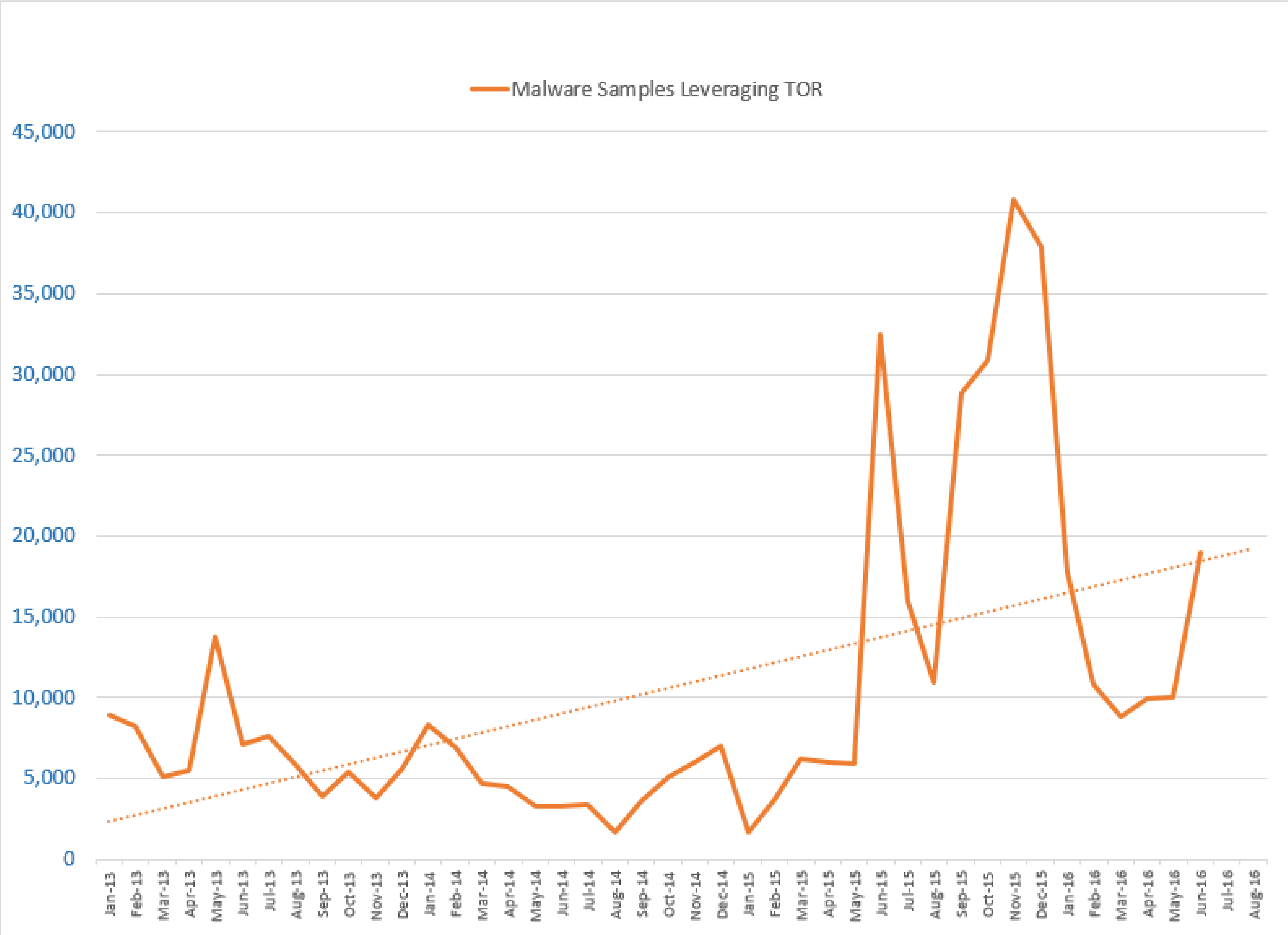
- IPv6
  - Today IPv4 is still the predominate routed protocol on the internet, particularly outside of APAC and universities. This is changing.
  - IPv6 presents a big challenge because of the massive number of IPv6 addresses. E.g. Hurricane Electric will give you your own /48 of IPv6. That's 65535 /64 networks, each with 18,446,744,073,709,551,616 hosts!!!
  - IPv6 also may expose weaknesses in security software that does not support it yet or has underlying flaws and vulnerabilities.
  - It is enabled by default in virtually every modern OS!



Source: Google: https://www.google.com/intl/en/ipv6/statistics.html
Source: Hurricane Electric: https://tunnelbroker.net/
Source: Jaws, Roy Schneider 1975

C2 Trends and Projections: TOR

- TOR
  - We're already seeing an increase in malware using TOR
  - Ideal channel for concealment of the C2
  - TOR can even be implemented without a client using Tor2Web.



Source: Proofpoint ET Intelligence, Unique Malware Samples leveraging TOR
Source: Tor2Web Project: https://www.tor2web.org/

Leveraging Cloud Apps

- Hiding C2 in Cloud/Web Apps
  - This is likely to be a continuing trend. It helps to solve the attacker challenge of hosting and potential blacklisting of standalone C2 infrastructure by overlaying it on top of cloud applications which often have business legitimacy.
  - This makes it harder to detect and harder for organizations to take action on because they cannot block these apps.
  - Puts the onus on Cloud providers to detect malicious activity. The effectiveness will vary widely depending on how invested these providers are.
  - Cloud apps can be deployed with little more than an email address, often free compute infrastructure for attackers!

Site	Domain	Alexa top 100 websites (As of March 23, 2016)[3]	SimilarWeb top 100 websites (As of April 4, 2016)[4]	Type	Principal country
Google	google.com	1	2	Internet services and products	U.S.
YouTube	youtube.com	2	3	Video sharing	U.S.
Facebook	facebook.com	3	1	Social network	U.S.
Baidu	baidu.com	4	16	Search engine	China
Yahoo!	yahoo.com	5	5	Portal and media	U.S.
Amazon	amazon.com	6	14	E-commerce and cloud computing	U.S.
Wikipedia	wikipedia.org	7	9	Encyclopedia	U.S.
Tencent QQ	qq.com	8	42	Portal	China
Google India	google.co.in	9	17	Search engine	India
Twitter	twitter.com	10	11	Social network	U.S.
Windows Live	live.com	11	6	Email, web services and software suite	U.S.
Taobao	taobao.com	12	48	Online shopping	China
MSN	msn.com	13	22	Portal	U.S.
Sina Corp	sina.com.cn	14		Portal and instant messaging	China
Yahoo! Japan	yahoo.co.jp	15	36	Portal	Japan
Google Japan	google.co.jp	16	19	Search engine	Japan
LinkedIn	linkedin.com	17	30	Professional Social network	U.S.
Sina Weibo	weibo.com	18	56	Social network	China
Bing	bing.com	19	32	Search engine	U.S.
Yandex	yandex.ru	20	10	Search engine	Russia
VK	vk.com	21	4	Social network	Russia
Hao123	hao123.com	22		Web directories	China
Instagram	instagram.com	23	8	Photo sharing and social media	U.S.
eBay	ebay.com	24	31	Online auctions and shopping	U.S.
Google Germany	google.de	25	20	Search engine	Germany

Source: Alexa Top Websites: https://en.wikipedia.org/wiki/List_of_most_popular_websites

Layered Evasions: Ripe for the Picking

- Layered Evasions
  - Stacking numerous evasions from the IP level up the chain into the application layer to try to evade malicious activity detection by trying to fool detection capabilities (similar to traditional IDS layering evasion techniques.

Embedded Content (Encoding, Compression, Metadata, Dynamic Content)
HTTP: Chunking, GZIP, Base64,
SSL Encryption
TCP Segment Overlaps
IP Fragmentation
IP Protocol 41 (IPv6 in IPv4)

Steg Adoption

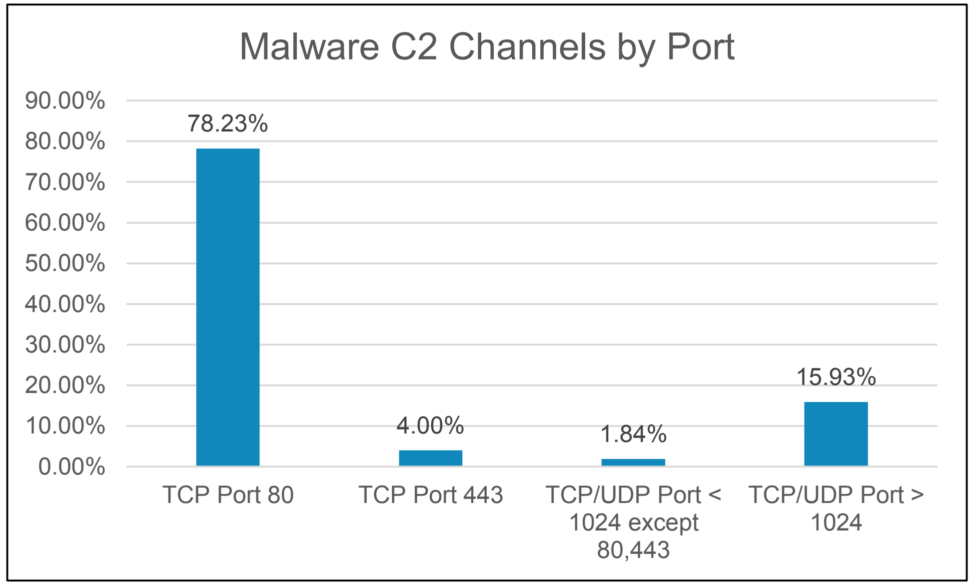
- Steganography
  - Hiding in plain sight really is a powerful covert channel.
  - Attackers may choose to take techniques which are not computationally difficult to generate, but are computationally difficult to detect, especially in real time network streams.
  - Trends will likely be dictated by pace of security industry defenses

- Further Reading: http://embeddedsw.net/doc/Thwarting_audio_steganography_attacks_in_cloud_storage_systems.pdf
- http://embeddedsw.net/doc/Data_hiding_and_steganography_annual_report_2012.pdf
- Image Source: Inception, Christopher Nolan, 2010

C2 Detection Is Critical!

- High fidelity Indicator
- May prevent malware from successfully executing
- May prevent escalation to attack other hosts inside/outside the network
- May prevent sensitive data from making it out
- Makes more hoops for the attacker to jump through and therefore more opportunities to make a mistake.

Defense Mechanisms Part 1



- Eliminate the Known Bad
  - Block access to known bad IP's, countries
  - Block Access to Malicious Domains/URL's
- Minimize the network attack surface
  - Restrict FW/NGFW to least privilege including
    - Restrict Firewall Ports!, no ~~any any any~~ policy
    - Block unnecessary / undesirable L7 applications with an NGFW/IPS
      - E.g. ToR, ToR2Web, Unknown Binary Strings
    - Block unknown / unknown encrypted applications at the perimeter with an NGFW/IPS
      - NGFW's can identify low hanging fruit with AppID, IPS can help to identify potential protocol anomalies used when malware attempts to masquerade over HTTP/HTTPS ports.

Defense Mechanisms Part 2

- Fingerprint Known Malware
  - Where possible, identify malware with both pattern matching and behavioral identification from a high fidelity source. If you can accurately identify malware itself, then you can have a higher degree of confidence of an infection.
  - Especially if you can identify the malware by it’s C2 channel

```
POST /upload/_dispatch.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://xllrawxmhbsoxmu.xyz/upload/
x-requested-with: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Host: xllrawxmhbsoxmu.xyz
Content-Length: 1166
Connection: Keep-Alive

BehhJm=%B8t%B2I%2B8%93%FE%8E%3BV%D8%C1%13%AD%2CD%F2%88%D2n&ctSxHeVl=%E7%96%FD%A5%2F4%89K%DF%17%12.%97O%1F%FD%FC%A8%04%C3%07%15%FDv
%98p%2B%9FR%91%D7%AA%D1%C3%A3%06%96%FA%94%2Bs%E8%83o&Zhu=ZO%E0%1E%82%95%DD6%B8%88%B0%3D%97%EF%06%D1&ZlgwgQiL=%EA%D3%99%83r%BE0e%27
%E6%40%C6Q%8Bt%ED%E7%FCp%18%8B%AE%BA%0A%25%B3%9B4%19y%B2%5E%26%0B%7D&RgaQUQ=%91%8A4%D5%2F%E5l%DB%2A%97%A9%5D%B4r%27%C1oI%86%0A%D5%2C
%D0%E3%89%A8e%99%A5%02%EAy%0C%5Ed47%A9%E7I%23&ZIXH=%23%0D%AFr%60uZ%D4%03%A9%D8j%D9%CE%0F%B63%5D%CCs%3F%8C%E8V%D8%F9%D3%F6%F0%CA
%26%7E%25%13%88g%E4%94%3E%E6%02%06i%21&yiN=%E4W5%A5%0F%EAp%85%E8%C4%F2%3E%00%B4K%BDn%7B%22%AFs%90%C4%9B%C6%9F%F8%C9%3E%82%C3%7F
%12%09%81%3D%21W%BB%2AA%9F%ACd%AALx_%2C&oZhroNa=R%C7%92%F5n%D7%5D%9B%14%0D%0Ee%A3%40O%EA%8C&czGrK=%87%24_%DCZ%9F%AC%1C%9Bmt%91o
%85%13%E6%A2%3F&XIDPBv=r%89%BB%EC%21%B1U%AA%09f_%3B%B7y%2CV8%CA%AE%9C%C2%B9eQ8%07%CE%C0%2F%81%91&lmHVT=%A5%DE%DC%5E%16%AD%ECGX-7w
%11%D1%27%DEQ%D95%26y%E62%212t%7C%B4%03%F8%2F&ICU=%9C%22D%F0%7B%E8%CB%A5%EB%CB%B7%D5%1B%FC%A8%BD%28%0E%D5%0Fh21%BFP%AD%C5J%C4Juon%
%E6%23%EA&AAgWfx=%C0%DF%D0%27%96%08%C0%A7%95%EB%03%EAw%F7H%066Y2%E9%5C%1B%25%15%E9%DA%18%99w%15%19%17&msA=q%9C%90%29%93%9D%91%AC
%2FHTTP/1.1 404 Not Found
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 11 Jul 2016 19:19:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip

c5
.............
.0..w.w8;...Bq.YD.A...Rs&.4...}{.. .....w...tl-...F!9.&Z...........BF.HB./{h..[...M..EV..E.......F.v....r..;...
\...t.v.O..eYN..N....!.q
..i......v
.IX..[.s0....C.!M(.B...../.....C...
0
```

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Ransomware Locky CnC Beacon 21 May"; flow:established,to_server; content:"POST"; http_method; content:"/_dispatch.php"; fast_pattern; content:"www-form-urlencoded|0d 0a|"; http_header; content:"|0d 0a|x-requested-with|3a 20|XMLHttpRequest|0d 0a|"; http_header; pcre:"/^[0-9a-zA-Z=%-]{0,48}(?:%[A-F0-9]{2}){4}/Psi"; reference:md5,6f8987e28fed878d08858a943e7c6e7c; classtype:trojan-activity; sid:2022952; rev:2;)
```

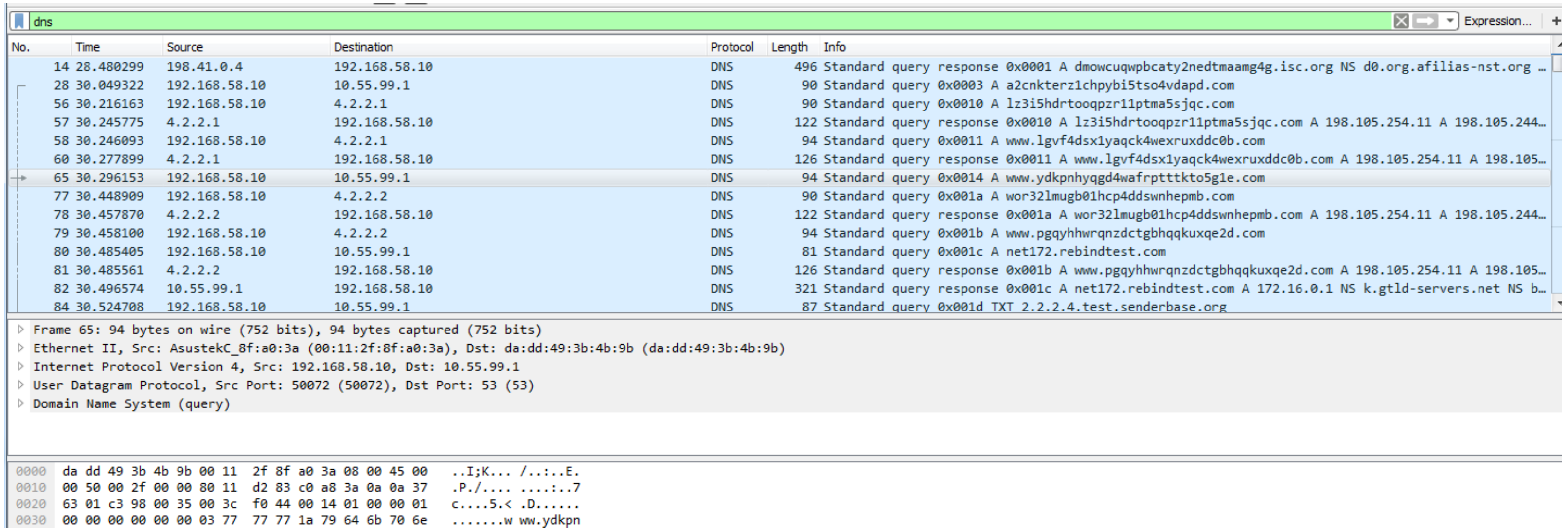
Defense Mechanisms Part 3

- Eliminate SSL Blind Spot with Interception
  - SSL Interception is an increasingly important function if it can be leveraged.
  - It allows you to not only inspect encrypted streams, but also breaks any malware that uses predefined certificates / unsupported configurations.
  - Try to limit Trusted CA certs wherever possible, especially on SSL Proxy and on endpoints. This can help to mitigate malware being able to connect to suspicious systems signed by low trust partners.
  - Restrict SSL MiTM to using strong ciphers to potentially break malware using weak / outdated ciphers.
- Detect/Block Known Bad SSL Certs
  - Where possible, use IDS or other technology to detect known malicious SSL certs which provide high fidelity indicators of an attack (even if SSL MiTM isn't possible)
  - Record TLS Certificates observed on network with tools like Suricata or Bro.
  - Abuse.CH!

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)"; flow:established,from_s
erver; content:"|03 02 01 02 02 09 00|"; fast_pattern; content:"|30 09 06 03 55 04 06 13 02|"; distance:0; pcre:"/^[A-Z]{2}/R"; content:!"|55 04 08|"; di
stance:0; content:"|55 04 07|"; distance:0; pcre:"/^.{2}[A-Z][a-z]+(?:\x27[a-z]+|(?:\x20[A-Z][a-z]+){1,2})?[01]/Rs"; content:"|55 04 0a|"; distance:0; pc
re:"/^.{2}[A-Z][a-z]{3,}\s[A-Z][a-z]{3,}\s(?:[A-Z](?:[A-Za-z]{0,4}?[A-Z]|(?:\.[A-Za-z]){1,3})|[A-Z]?[a-z]+)\.?[01]/Rs"; content:"|55 04 03|"; distance:0;
 byte_test:1,>,7,1,relative; pcre:"/^.{2}(?:[a-z]{1,4}(?:\d{3})?\.)?[a-z]{5,}\.(?!(?:com|net|org)[01])[a-z]{2,}[01]/Rs"; content:!"|2a 86 48 86 f7 0d 01
09 01|"; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022627; rev:8;)
```

Defense Mechanisms Part 4

- Heuristics / Anomaly Detection
  - Heuristics/Pattern matching is not a perfect catch all for identifying suspicious activity due to highly evasive techniques, especially when it can be corroborated with other IOC's.
  - One high fidelity indicator of compromise can be to examine DNS data to try to identify domain generation algorithms used by modern malware.
  - Some IDS can also identify this activity, but placement is very important because it needs to be between the client and the DNS server, otherwise all attacks will look like they are coming from the DNS server.



- Network Anomaly Detection:
  - By itself a low fidelity indicator and FP prone, when combined with other techniques, anomaly detection can provide valuable insight. Particularly when network based steganography and evasion techniques are used, a good IDS anomaly engine will light up like a Christmas tree.

Defense Mechanisms: Part 5

- Review, Tune, and Listen to your Security Infrastructure! (Give a shit)
  - As we've seen with many high profile breaches, it is often the case that malicious activity is detected, but it isn't acted upon.
  - Most off the shelf malware and attacks provide many IOC's to key on which can be detected by freely available software and systems.
  - There are commercial and open source solutions available that can help to solve the problem of the signal to noise, auxiliary endpoint verification, and end to end IR containment.

Most Importantly

- Get Involved!
  - Contribute to ET Open, Free Open Source IDS Rules for Suricata and Snort
    - http://doc.emergingthreats.net/bin/view/Main/EmergingFAQ
    - emerging@emergingthreats.net
  - Contribute to OISF / Suricata Development
    - https://oisf.net/
    - https://suricata-ids.org/

Summary

- In modern computer security, it’s not a matter of if, but when, and what they will take, and how much it will cost you to deal with it.
- The attack surface is simply too massive, to put all of your hopes in the fact that you might be able to keep malware out.
- In taking the fight to the attackers, we need to be smart, and to holistically detect breaches. Not only on the initial phases, but perhaps where the attackers are most exposed and we have the most defensive capabilities to detect them by detecting the C2 channels.
- As we continue to up our game, we should expect that the malicious actors will do the same, and come up with even more creative ways to leverage the same technology which can be used for incredible good for their own malicious purposes.
- But at the very least, we can keep them on their game, and further tip the economics of hacking by making their job that much harder. We’ll do it by exploiting them for a change; at their weakest point, the command and control channel.


Thank You!