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.



3

Primary Breach Vectors

> Modern malware is delivered in one of two ways:

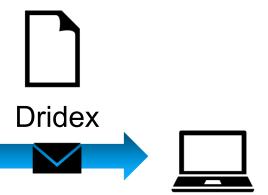
- Executable Content: Binary executables, embedded executable content like macros typically through web or email channels on the network.
- Exploit Driven: An exploit against a software vulnerability such as those against Flash, PDF, Java, Office Docs, Browsers, and other network enabled applications.

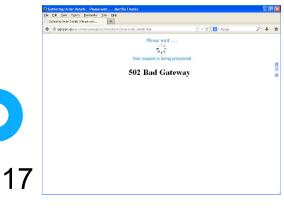
		N: Invoice J-26564395	- message ((Plain Lext)		-	
File Messag	Reply Reply Forward II More -	💱 Create New		OneNote	Aark Unread	a de la como	Com
Delete	All Respond	Quick Steps	¥ 4	Move	Follow Up * Tags G	- 4	Zoom
c abject: ATTN	one@mycompany.com I: Invoice J-26564395 nvoice_J-26564395.doc (64 KB)						ā
invoice.	attached invoice (Microsoft Word	and the	- payment		inc terms instead a	Sector	
	rectate your business!	-					
		-					3

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











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



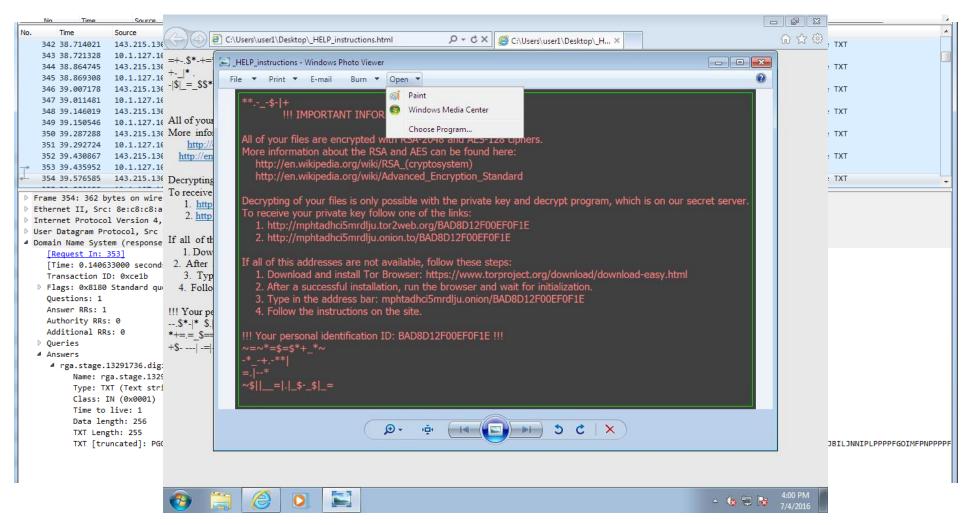
Escalation

- 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

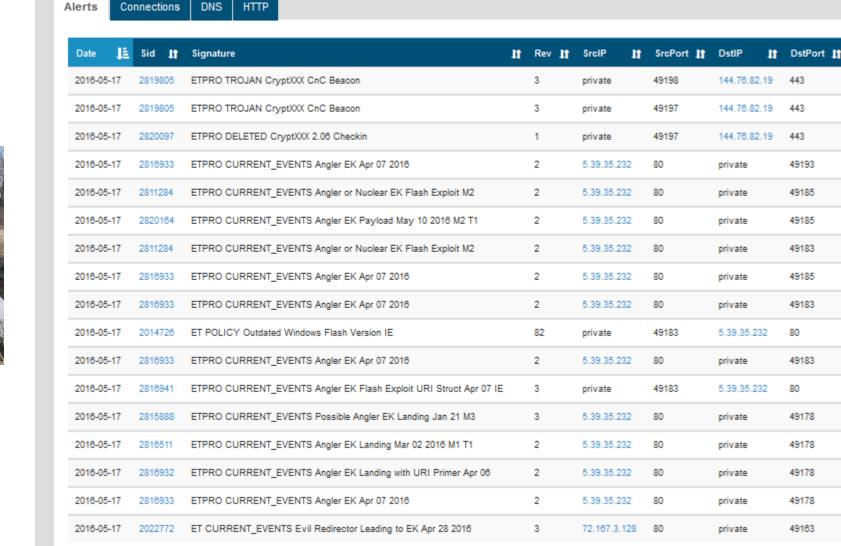
- This phase is where the malware delivers on it's intended purpose
- Exfiltrated data often includes stealing intellectual property, exposing attributes of a target network, or larger escalation of an attack.
- Locky Cataloguing Endpoint Files to C2
- > ZBOT (Zeus variant) DNS Covert Channel





Infection in Action: Angler Exploit Kit

Sample: 26907326de17c8c3f17c13bf32f61810







Target Compromised, C2

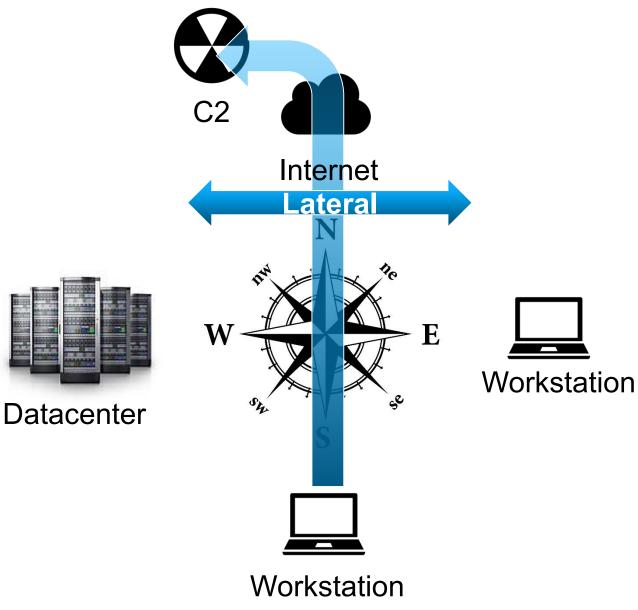
Exploit / Payload Delivered

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.



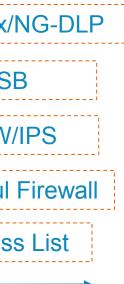




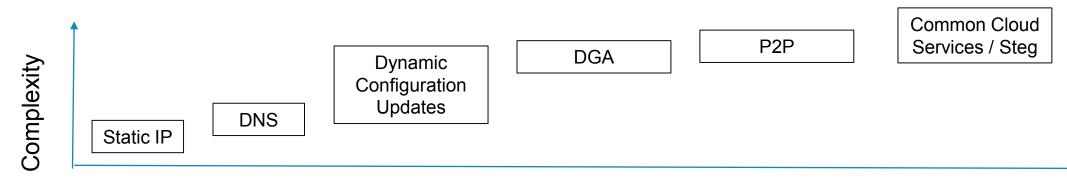
C2 Channel Evolution: Cat and Mouse

Sandbox/	Layer [9] Content Layer (Docs, HTML)
CAS	Layer [8] Software Application Layer (Dropbox)
NGFW	Layer 7 Network Application Layer (HTTP)
Stateful	Layer 4 Transport Layer (TCP/UDP)
Acces	Layer 3 Network Layer (IP)

- Malware noted that keeping explicit strings in the payload would be easy to identify (e.g. Greating and the set of the stranger of the strange > which also leveraged evasion techniques.
- > to Eavely and where after the other view of the standard of the share of the standard of the stegan Borta hier techniques to hide in plain sight. E.g. Sninfs
- > Firfany, 9man varenizationa van even on allewinage 9rtgrny toistase fate Panel 443 bedded communication to the standard for the standard for
- > In Eathriche NGE You which leverage a library of a ward or as in the section of the section of



C2 Hosting Evolution



Timeline

- > 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. >











12

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.

					0	8 16 24 32
No. Time	Source	Destination	Source Port	Dest Port	TCP Flags	is TCP Window Length Info
						0 96 [TCP ZeroWindow] Continuation Data
2 51.344927	1.1.1.1	2.2.2.2	60578	443	0x0000	0 105 [TCP ZeroWindow] Continuation Data
3 102.674005			60584	443	0x0000	0 95 [TCP ZeroWindow] Continuation Data
4 156.862447			60589	443	0x0000	0 93 [TCP ZeroWindow] Continuation Data
5 208.144288			60594	443	0x0000	0 99 [TCP ZeroWindow] Continuation Data
6 259.503938	1.1.1.1		60599	443	0x0000	0 103 [TCP ZeroWindow] Continuation Data
7 310.832959			60604	443	0x0000	0 104 [TCP ZeroWindow] Continuation Data
8 362.178129			60611	443	0x0000	0 90 [TCP ZeroWindow] Continuation Data
9 416.428170			60617	443	0x0000	
10 467.757308	1.1.1.1		60622	443	0x0000	0 102 [TCP ZeroWindow] Continuation Data
11 519.164370	1.1.1.1		60627	443	0x0000	0 89 [TCP ZeroWindow] Continuation Data
12 570.509260	1.1.1.1	2.2.2.2	60633	443	0x0000	0 88 [TCP ZeroWindow] Continuation Data
13 621.868784	1.1.1.1	2.2.2.2	60638	443	0x0000	
14 673.213865	1.1.1.1	2.2.2.2	60647	443	0x0000	0 79 [TCP ZeroWindow] Continuation Data
15 724.511438	1.1.1.1	2.2.2.2	60654	443	0x0000	0 97 [TCP ZeroWindow] Continuation Data
16 775.871858	1.1.1.1	2.2.2.2	60661	443	0x0000	
17 827.153850	1.1.1.1	2.2.2.2	60666	443	0x0000	
18 878.685610	1.1.1.1		60671	443	0x0000	
19 930.030282	1.1.1.1	2.2.2.2	60676	443	0x0000	
20 981.406451	1.1.1.1	2.2.2.2	60681	443	0x0000	
21 1032.750453	1.1.1.1	2.2.2.2	60687	443	0x0000	
22 1084.110698	1.1.1.1	2.2.2.2	60694	443	0x0000	
		68 bits), 96 bytes captured (

Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2

Transmission Control Protocol, Src Port: 60573 (60573), Dst Port: 443 (443), Seq: 1, Len: 42

Source Port: 60573 Destination Port: 443 [Stream index: 0] [TCP Segment Len: 42] Sequence number: 1 (relative sequence number) [Next sequence number: 43 (relative sequence number)] Acknowledgment number: 0 Header Length: 20 bytes ▷ Flags: 0x000 (<None>) Window size value: 0 [Calculated window size: 0] [Window size scaling factor: -1 (unknown)]

- Checksum: 0x2123 [validation disabled]
- Urgent pointer: 0

 Sequence Num

 Acknowledgment

 Data
 C
 E
 U
 A
 P
 R
 S
 F

 Offset
 W
 C
 R
 C
 S
 S
 Y
 I

 Offset
 Checksum
 Options

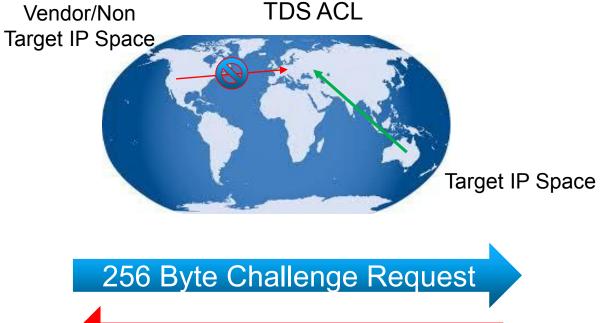
Source: IPv4/V6/TCP Header, LUC <u>http://intronetworks.cs.luc.edu/1/html/tcp.html</u> OpenPuff: http://embeddedsw.net/OpenPuff_Steganography_Home.html



ber	
Number	
Window S	ize
Urgent Poir	nter
	Padding

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 antisandboxing techniques to prevent execution and avoid detection.





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



256 Byte Challenge Response

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
- traditional targeted.
- channels altogether.
- > May leverage insiders as air gaps.



> Far more sophisticated than

> May lack network based C2

well as covert HW to bridge

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.



16

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

	। 🔀 🛅 🍳 👄 🔿	≝♥⊻⊑∎	સ્ટ્ર્			
cp						Expression
Time	Source	Destination		Protocol	Length Info	
9 9.850912	192.168.103.10	60.251.73.126		TCP	62 1026 → 3002 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	
10 10.039054	60.251.73.126	192.168.103.10	0	TCP	62 3002 → 1026 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1	
11 10.040020	192.168.103.10	60.251.73.126		TCP	60 1026 → 3002 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
12 10.045809	192.168.103.10	60.251.73.126		TCP	249 1026 → 3002 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=195	
13 10.234160	60.251.73.126	192.168.103.10		TCP	76 3002 → 1026 [PSH, ACK] Seq=1 Ack=196 Win=64240 Len=22	
14 10.401554	192.168.103.10	60.251.73.126		TCP	60 1026 → 3002 [ACK] Seq=196 Ack=23 Win=17498 Len=0	
	tes on wire (1992 b					
hernet II, Src	: AsustekC_8f:a0:67	(00:11:2f:8f:a0:6	7), Dst: 62:ad:6f:ef:	5f:47 (62:ad:6f:ef:5f:	.47)	
hernet II, Src ternet Protoco	: AsustekC_8f:a0:67 l Version 4, Src: 1	(00:11:2f:8f:a0:6 02.168.103.10, Dst	7), Dst: 62:ad:6f:ef: : 60.251.73.126			
hernet II, Src ternet Protoco ansmission Con	: AsustekC_8f:a0:67 l Version 4, Src: 1 trol Protocol, Src	(00:11:2f:8f:a0:6 02.168.103.10, Dst	7), Dst: 62:ad:6f:ef: : 60.251.73.126	5f:47 (62:ad:6f:ef:5f: ?), Seq: 1, Ack: 1, Len		
hernet II, Src ternet Protoco ansmission Con Source Port: 3	: AsustekC_8f:a0:67 l Version 4, Src: 1 trol Protocol, Src 1 1026	(00:11:2f:8f:a0:6 02.168.103.10, Dst	7), Dst: 62:ad:6f:ef: : 60.251.73.126			
hernet II, Src ternet Protoco ansmission Com Source Port: 3 Destination Po	: AsustekC_8f:a0:67 l Version 4, Src: 19 trol Protocol, Src 1 1026 prt: 3002	(00:11:2f:8f:a0:6 02.168.103.10, Dst	7), Dst: 62:ad:6f:ef: : 60.251.73.126			
nernet II, Src ternet Protoco ansmission Con Source Port: 3	: AsustekC_8f:a0:67 l Version 4, Src: 19 trol Protocol, Src 1 1026 prt: 3002	(00:11:2f:8f:a0:6 02.168.103.10, Dst	7), Dst: 62:ad:6f:ef: : 60.251.73.126			
nernet II, Src ternet Protoco ansmission Con Source Port: : Destination Po [Stream index	: AsustekC_8f:a0:67 l Version 4, Src: 19 trol Protocol, Src 1 1026 prt: 3002	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026),	77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002			
ernet II, Src ternet Protoco ansmission Con Source Port: 1 Destination Po [Stream index 62 ad 6f ef 1	: AsustekC_8f:a0:67 l Version 4, Src: 1 trol Protocol, Src 1 1026 ort: 3002 : 0]	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026), 00 67 08 00 45 00	77), Dst: 62:ad:6f:ef: : 60.251.73.126 Dst Port: 3002 (3002 b.o6 /gE.			
hernet II, Src ternet Protoco ansmission Con Source Port: 1 Destination Por [Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02	: AsustekC_8f:a0:67 l Version 4, Src: 1 trol Protocol, Src 1 l026 prt: 3002 : 0] 	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026), 00 67 08 00 45 00 00 a8 67 0a 3c fb 8 11 b5 b1 50 18	77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002			
hernet II, Src ternet Protoco ansmission Con Source Port: 2 Destination Por [Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02 44 70 6c 59	: AsustekC_8f:a0:67 l Version 4, Src: 1 trol Protocol, Src 1 1026 ort: 3002 : 0] 5f 47 00 11 2f 8f a 10 00 80 06 4b d8 a 10 ba b0 40 5d 2e 30 00 c3 00 00 00	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026), 00 67 08 00 45 00 00 a8 67 0a 3c fb 8 11 b5 b1 50 18 8 00 00 00 47 68	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 b.oG /gE. @ Kg.<. I~P. DplYSh</pre>			
hernet II, Src ternet Protoco ansmission Con Source Port: Destination P([Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 09 49 7e 04 09 30 73 74 78	: AsustekC_8f:a0:67 L Version 4, Src: 1: trol Protocol, Src 1 026 ort: 3002 : 0] 5f 47 00 11 2f 8f 3 40 00 80 06 4b 48 0 20 00 c3 00 00 00 50 00 c3 00 00 00 50 4b 63 60 60 98 0	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026), 00 67 08 00 45 00 0 a8 67 0a 3c fb 8 11 b5 b1 8 8 00 00 04 7 68 03 c4 ac 40 cc 08	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 b.oG /gE. @ Kg.< I~</pre>			
hernet II, Src ternet Protoco ansmission Con Source Port: 3 Destination Pr [Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02 0 44 70 6c 59 30 73 74 78 c4 1a 5c 0c 0	: AsustekC_8f:a0:67 l Version 4, Src: 1: trol Protocol, Src 1 1026 ort: 3002 : 0] 5f 47 00 11 2f 8f a 10 00 80 06 4b 48 10 00 80 06 4b 48 10 00 00 c3 00 00 00 0 c4b 63 60 60 98 10 c4c 40 3a 38 b5 a	(00:11:2f:8f:a0:6 02.168.103.10, Dst 00:67 08 00 45 00 00 a8 67 0a 3c fb 8 11 b5 b1 50 18 8 00 00 47 68 30 c4 ac 40 cc 08 18 2c 33 39 55 21	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 b.oG /gE. @ Kg.< I~]P. DplYGh @stx.Kc``@. @: 8,90!</pre>			
hernet II, Src ternet Protoco ansmission Com Source Port: 2 Destination Por [Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02 0 44 70 6c 59 0 30 73 74 78 30 73 74 78 24 1a 5c 0c 0 20 31 39 5b	: AsustekC_8f:a0:67 l Version 4, Src: 1: trol Protocol, Src 1 0026 ort: 3002 : 0] 5f 47 00 11 2f 8f a 10 00 80 06 4b 48 a 10 00 03 00 00 00 a 10 00 c3 00 00 00 a 10 c4b 63 60 60 98 a c4 c40 3a 38 b5 a : 1 98 a1 5e 02 28 a	(00:11:2f:8f:a0:6 02.168.103.10, Dst 00:11:200 (1026), 00:000 (1026), 00:0000 (1026), 00:0000 (1026), 00:0000 (1026), 0	<pre>b.oG /gE. @ Kg.< Iway and the second second</pre>			
hernet II, Src ternet Protoco ansmission Con Source Port: 3 Destination P([Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02 44 70 6c 59 30 73 74 78 c4 1a 5c 00 20 31 39 5b 87 10 03 08	AsustekC_8f:a0:67 Version 4, Src: 1 trol Protocol, Src 1 2026 2017: 3002 301 302 302 303 304 305 47 00 11 2f 8f 3 40 00 80 06 4b d8 6 305 306 00 c3 00 00 00 306 4b 63 60 60 98 307 307 307 307 307 307 307 307	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026), 0 67 08 00 45 00 0 a8 67 0a 3c fb 8 11 b5 b1 50 18 8 00 00 00 47 68 13 c4 ac 40 cc 08 18 c2 33 39 55 21 6 68 69 48 161 87 19 31 48 30 48 31	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 b.oG /gE. @ Kg.< I~]P. DplYGh @stx.Kc``@. L@: 8,39U! 19[^ (va. 101H0H1</pre>			
hernet II, Src ternet Protoco ansmission Con Source Port: : Destination P([Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02 44 70 6c 59 30 73 74 78 c4 1a 5c 0c 20 31 39 5b 87 10 03 08 58 78 03 c5	AsustekC_8f:a0:67 Version 4, Src: 1 trol Protocol, Src 1 (026 ort: 3002 6 6 6 6 7 7 7 8 7 8 9 9 9 9 9 9 9 9 9 9 9 9 9	(00:11:2f:8f:a0:6 02.168.103.10, Dst Port: 1026 (1026), 00 67 08 00 45 00 00 88 67 0a 3c fb 08 11 b5 b1 50 18 18 00 00 04 7 68 03 c4 ac 40 cc 08 18 2c 33 39 55 21 26 86 9d 81 61 87 19 31 48 30 48 31 12 cd 7f 20 d8 0a	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 b.oG /gE. @ Kg.< I~P. DplYP. DplYSh <u>0st</u>x.Kc``@. 1@: 8,39U! 19[^ (va 101H0H1 Xx^Njb</pre>			
hernet II, Src ternet Protoco ansmission Con Source Port: Destination P([Stream index 62 ad 6f ef 9 00 eb 00 09 4 49 7e 04 02 44 70 6c 59 4 30 73 74 78 c4 1a 5c 0c 20 31 39 5b 87 10 03 08 58 78 03 c5 a4 23 7f 4f a	AsustekC_8f:a0:67 Version 4, Src: 1: trol Protocol, Src 1: trol Protocol, Src 1: trol Protocol, Src 1: trol Protocol, Src 1: 1026 51 47 00 11 2f 8f 3: 10 00 80 06 4b 48 3: 10 00 00 03 00 00 00 10 00 00 03 00 00 00 11 00 00 03 00 00 00 12 4b 63 60 60 98 0 12 4b 63 15 60 22 8 13 56 4c 80 9f 16 6a 16 6a 89 01 62 10 1f a	(00:11:2f:8f:a0:6 02.168.103.10, Dst 00:67 08 00 45 00 0 a8 67 0a 3c fb 8 10 55 1 50 18 8 00 00 47 68 03 c4 ac 40 cc 08 18 2c 33 39 55 21 6 86 9d 81 61 87 19 31 48 30 48 31 22 cd 7f 20 d8 0a 14 3e 63 7d 6b cd	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 Dst Port: 3002 (3002 Interpretation of the second Interpretation o</pre>			
hernet II, Src ternet Protoco ansmission Com Source Port: 3 Destination Pr [Stream index 62 ad 6f ef 9 00 eb 00 09 49 7e 04 02 0 44 70 6c 59 30 73 74 78 c4 1a 5c 0c 0 20 31 39 5b 87 10 03 08 58 78 03 c5 a4 23 7f 4f a17 a0 5e 0f a	: AsustekC_8f:a0:67 l Version 4, Src: 1: trol Protocol, Src 1 4026 ort: 3002 5 0 6 47 00 11 2f 8f a 40 00 80 06 4b 48 a 40 00 80 06 4b 48 a 40 00 c3 00 00 00 0 5 4c 40 3a 38 55 a 5 1 98 a1 5e 02 28 a 5 49 a1 5e 02 28 a 5 4e 48 39 f1 6a 6 5 4e 48 49 f1 6a 6 5 4e 48 49 f1 6a 5 5 4e 48 49 f1 6a 5 5 4e 48 49 f1 6a 5 5 4e 48 5 10 11 16 16 5 5 4e 36 35 2 5 5 5 6 5 6 5 6 5 5 6 5 5 5 5 5 5 6 5 6 5 5 6 5 5 6 5 5 5 5 5 5 5 5 5	(00:11:2f:8f:a0:6 02.168.103.10, Dst 00:11:2f(1026), 00:67 08 00 45 00 00 a8 67 0a 3c fb 8 11 b5 b1 50 18 8 00 00 047 68 13 c4 ac 40 cc 08 18 2c 33 39 55 21 16 86 9d 81 61 87 19 31 48 30 48 31 12 cd 7f 20 d8 0a 14 3e 63 7d 6b cd 10 be 05 10 7f 78	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 Dst Port: 3002 (3002 I~</pre>			
hernet II, Src ternet Protoco ansmission Con Source Port: 3 Destination Pd (Stream index 62 ad 6f ef 9 49 7e 04 02 44 70 6c 59 30 73 74 78 9 c4 1a 5c 06 20 31 39 5b 87 10 03 08 58 78 03 c5 a4 23 7f 4f a1 7a 0 5e 0f 25 c4 70 e0	AsustekC_8f:a0:67 Version 4, Src: 1: trol Protocol, Src 1: trol Protocol, Src 1: trol Protocol, Src 1: trol Protocol, Src 1: 1026 51 47 00 11 2f 8f 3: 10 00 80 06 4b 48 3: 10 00 00 03 00 00 00 10 00 00 03 00 00 00 11 00 00 03 00 00 00 12 4b 63 60 60 98 0 12 4b 63 15 60 22 8 13 56 4c 80 9f 16 6a 16 6a 89 01 62 10 1f a	(00:11:2f:8f:a0:6 22.168.103.10, Dst Port: 1026 (1026), 0 67 08 00 45 00 0 88 67 0a 3c fb 8 11 b5 b1 50 18 8 00 00 00 47 68 13 c4 ac 40 cc 08 18 c2 33 39 55 21 16 86 9d 81 61 87 19 31 48 30 48 31 12 cd 7f 20 d8 0a 14 36 37 d6 bc d 10 be 05 10 7f 78 10 a0 91 0c 05 a7	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 b.oG /gE. @ Kg.< I~]P. DplYGh @stx.Kc``@. l0: 8,39U! 19[^ (va. 101H0H1 Xx^Njb .#.Ob>c}k. ^u.5x %.pC.</pre>			
thernet II, Src nternet Protoco ransmission Com Source Port: 3 Destination Po [Stream index 62 ad 6f ef 9 0 eb 00 eb 00 9 49 7e 04 02 4 0 49 7e 04 02 4 0 40 40 4 0 40 40 40 40 40	AsustekC_8f:a0:67 Version 4, Src: 1 trol Protocol, Src 1 2026 Sort: 3002 30 30 30 30 40 30 40 40 30 40 50 40 50 40 50 40 50 40 50 50 50 50 50 50 50 50 50 5	(00:11:2f:8f:a0:6 02.168.103.10, Dst 00:11:2f:8f:a0:6 02.168.103.10, Dst 00:0 a8 67 0a 3c fb a8 67 0a 3c fb a8 11 b5 b1 50 18 a8 00 00 04 47 68 b3 c4 ac 40 cc 08 b3 c4 ac 40 cc 08 b4 c4 ac 40 c	<pre>77), Dst: 62:ad:6f:ef: :: 60.251.73.126 Dst Port: 3002 (3002 Dst Port: 3002 (3002 I~</pre>			

.....Gh0stx.Kc``...@....\..L@:8..,39U! 19[...^.(v...a.....10.. 1H0H1Xx..^N...jb.. . .#.0...b...>c}k...^..u.5x%.p...C......13H.##.o...C ..(....o..2...t.....d..D.c3.Ts.b@5.p...@U......Gh0stx.c.....



-

Poisonlvy

- 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.

No.	Time	Source	Destination	Protocol Le	ength Info
	6 0.029001	172.16.3.46	172.16.1.1	TCP	310 1037 → 3460 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=256
	7 0.029028	172.16.1.1	172.16.3.46	TCP	54 3460 → 1037 [ACK] Seq=1 Ack=257 Win=6432 Len=0
	8 60.392080	172.16.1.1	172.16.3.46	TCP	54 3460 → 1037 [FIN, ACK] Seq=1 Ack=257 Win=6432 Len=0
	9 60.392213	172.16.3.46	172.16.1.1	тср	60 1037 → 3460 [ACK] Seq=257 Ack=2 Win=65535 Len=0
1	10 60.392321	172.16.3.46	172.16.1.1	ТСР	60 1037 → 3460 [FIN, ACK] Seq=257 Ack=2 Win=65535 Len=0
L :	11 60.392340	172.16.1.1	172.16.3.46	TCP	54 3460 → 1037 [ACK] Seq=2 Ack=258 Win=6432 Len=0
1	14 90.469389	172.16.3.46	185.32.221.46	TCP	62 1038 → 3460 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1	15 90.643309	185.32.221.46	172.16.3.46	тср	54 3460 \rightarrow 1038 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	16 91.110604	172.16.3.46	185.32.221.46	тср	62 [TCP Spurious Retransmission] 1038 \rightarrow 3460 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
	17 91.284695	185.32.221.46	172.16.3.46	тср	54 3460 → 1038 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	18 91.766846	172.16.3.46	185.32.221.46	тср	62 [TCP Spurious Retransmission] 1038 → 3460 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1	19 91.941027	185.32.221.46	172.16.3.46	тср	54 3460 → 1038 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1	22 121.939892	172.16.3.46	172.16.1.1	TCP	62 1039 → 3460 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK PERM=1
	23 121.939982	172.16.1.1	172.16.3.46	тср	62 3460 → 1039 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK PERM=1

Ethernet II, Src: HewlettP 47:bd:24 (00:08:02:47:bd:24), Dst: Supermic f8:de:82 (00:30:48:f8:de:82)

Internet Protocol Version 4, Src: 172.16.3.46, Dst: 172.16.1.1

Transmission Control Protocol, Src Port: 1037 (1037), Dst Port: 3460 (3460), Seg: 1, Ack: 1, Len: 256 Data (256 bytes)

Data: de36a7ab1e4b718367483754be28dc864ec357fc326e5e31.

[Length: 256]

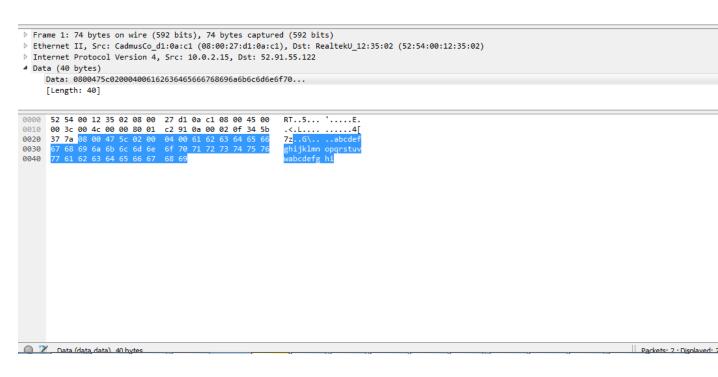
f8 de 82 00 08G.\$..E. 02 47 bd 24 08 00 45 00 .(..@......... 7T.(...N. W.2n^1... *i.T?... .2...3e. .d...cV. .z...d.1 .V]1.... ..Ho...:P `..t.[UzP. 97 a1 b1 a2 aa 7a 50 ae ...3=...[...t[.].. a2 5d e7 be .?T.,.Yp]N..V... c9 ff 12 d1 .0.2P{V.G? !.hB7....-:.b.T.7.o.. 0....G.(J...w0.6. c5 99 6f 03 ca 7e 96 ac 95 9c 3a d9 44 07 d3 45 ..o..~.. ..:.D..E 3d 1e 5c b6 e8 2c 32 4a f3 d4 5b 4a 09 07 4e 7e =.\..,2J ..[J..N~ 0130 27 61 de df 20 e2 'a.. .



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.

Ap	ply a display filter	<ctrl-></ctrl->		
No.	Time	Source	Destination	Protocol Length Info
	1 0.000000	10.0.2.15	52.91.55.122	IPv4 74 ICMP (1)
	2 0.079069	52.91.55.122	10.0.2.15	IPv4 74 ICMP (1)





Expression	+
	_

Packets: 2 · Displayed: 2 (100.0%) · Load time: 0:0.1

Profile: Default

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.

	File Edi	it View Go	Capture Analyze Stati	stics Telephony Wireless Tools Help			
		1 💿] 🖪	🔀 🛅 🤇 🗢 🔿 🕾	T 🕹 🚍 🚍 Q, Q, Q, 🏨			
(Apply a	a display filter ·	<ctrl-></ctrl->				
	No.	Time	Source	Destination	Protocol	Length	Info
	• 7	36.789199	192.168.4.5	79.46.183.210	RTP	114	PT=Unassigned, SSRC=0x2CF2453A,
	8	51.814595	192.168.4.5	66.136.148.79	UDP	114	29579 → 19925 Len=72
	10	66.814572	192.168.4.5	74.41.224.134	BT-uTP	114	uTorrent Transport Protocol Type
	12	81.845902	192.168.4.5	31.135.144.242	UDP	114	29579 → 11571 Len=72
	14	96.877045	192.168.4.5	178.59.240.41	SKYPE	114	NAT repeat Unk: 4
	16	111.877009	192.168.4.5	82.107.220.127	SKYPE	114	NAT info Unk: 4
	18	126.892576	192.168.4.5	117.194.224.243	UDP	114	29579 → 28318 Len=72
	19	141.908162	192.168.4.5	46.36.116.1	RTP	114	PT=Unassigned, SSRC=0x468FB450,
	20	156.923636	192.168.4.5	79.9.10.57	UDP	114	29579 → 23939 Len=72

▷ Fr	ame 7: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
D Et	hernet II, Src: CisTechn_10:20:04 (00:20:18:10:20:04), Dst: 00:ff:a1:00:06:50 (00:ff:a1:00:06:50)
Þ In	nternet Protocol Version 4, Src: 192.168.4.5, Dst: 79.46.183.210
⊳ Us	er Datagram Protocol, Src Port: 29579 (29579), Dst Port: 11134 (11134)
0000	00 ff al 00 06 50 00 20 18 10 20 04 08 00 45 00PE.
	00 64 00 7c 00 00 80 11 6e 5f c0 a8 04 05 4f 2e .d. n0.
0020	b7 d2 73 8b 2b 7e 00 50 59 50 9f 9e 9e 9c 19 b1
0030	f8 bf 2c f2 45 3a b0 b7 4e 13 66 da 11 3c d3 4a,E: N.f<.J
0040	ca 61 3c bc 1c a8 f7 f7 73 24 26 6d 46 83 63 72 .a< s\$&mF.cr
0050	9a ef e3 4e bc 7d d6 2a ba 92 51 4d 02 77 0b 0c
0060	50 91 26 ff 10 90 54 59 cf 3e 3e 3e 3e 3e 3e 3e 9eTY
0070	3e 3e >>

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



Expression 🕇
Seq=40604, Time=431093951, Mark[Malformed Packet]
e: Unknown 69[Malformed Packet]
Seq=44206, Time=2280578286, Mark

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 "It	Signature	łt	Rev 🛔	SrcIP It	SrcPort 🛔	DstIP I	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

Alerts

- 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

HTTP

MD5 eef89c15b2625a8814d8c898fb802e04 Submision Date 2015-02-10 17:03:21 Type PE32 executable (GUI) Intel 80388, for MS Windows

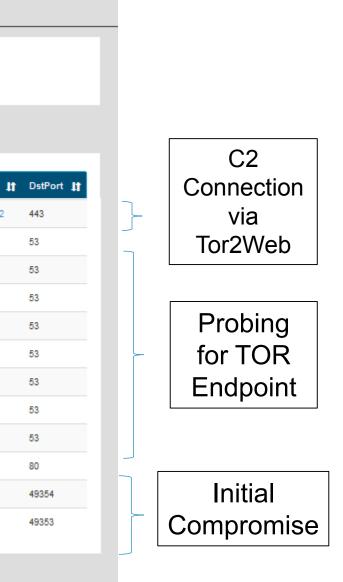
DNS

Connections

SHA256 c026e9528b880d62e686c837494da9d6fc3ed90374f69c5496de63066eb9f575 File Size 46592 VirusTotal 47/54

Date	Æ	Sid	lt	Signature	łt	Rev	łt	SrcIP	łt	SrcPort 👫	DstIP
2015-10)-11	20188	79	ET POLICY onion.cab tor2web .onion Proxy domain in SNI		1		private		49380	188.138.122.22
2015-10)-11	20188	76	ET POLICY onion.cab .onion Proxy DNS lookup		1		private		53212	8.8.8.8
2015-10)-11	20203	58	ET TROJAN Critroni Variant .onion Proxy Domain		1		private		53212	8.8.8.8
2015-10)-11	20188	76	ET POLICY onion.cab .onion Proxy DNS lookup		1		private		53212	8.8.8.8
2015-10)-11	20203	58	ET TROJAN Critroni Variant .onion Proxy Domain		1		private		53212	8.8.8.8
2015-10)-11	20155	76	ET POLICY DNS Query to .onion proxy Domain (tor2web)		6		private		62661	8.8.8.8
2015-10)-11	20203	58	ET TROJAN Critroni Variant .onion Proxy Domain		1		private		62661	8.8.8.8
2015-10)-11	20155	76	ET POLICY DNS Query to .onion proxy Domain (tor2web)		6		private		62661	8.8.8.8
2015-10)-11	20203	58	ET TROJAN Critroni Variant .onion Proxy Domain		1		private		62661	8.8.8.8
2015-10)-11	28084	13	ETPRO POLICY telize.com IP lookup		2		private		49366	46.19.37.108
2015-10)-11	20199	25	ET TROJAN Win32/Dalexis.A Possible SSL Cert (cargol.cat)		2		217.149.7.21	3	443	private
2015-10)-11	20199	24	ET TROJAN Win32/Dalexis.A Possible SSL Cert (ppc.cba.pl)		2		85.17.73.180		443	private





AridViper

<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze	<u>S</u> tatistics Telephon <u>y</u> <u>W</u> ireless <u>T</u> ools	<u>H</u> elp		
	🔳 🔬 💿] 🔚 🔚	े 🔀 🛅 🤇 🗢 🔿	🕾 🗿 👲 🚍 🚍 🍳 Q, Q, 🦉			
	nttp					Expression +
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=	-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=	-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=	-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 (a	pplication/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=	-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=	·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	-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



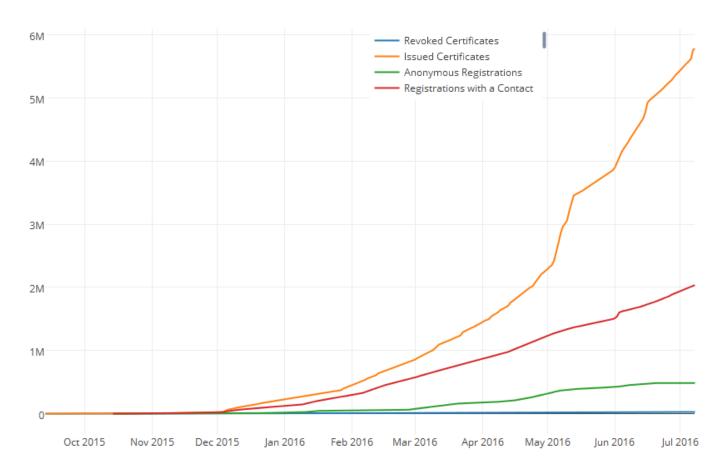
l in. post

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.

Daily Activity



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



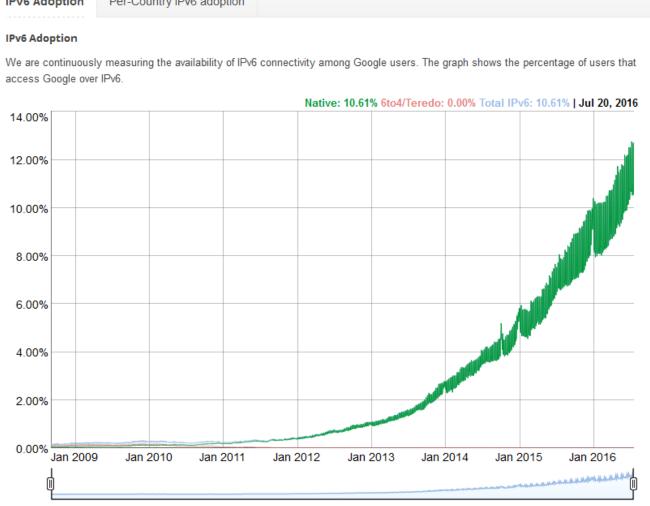
C2 Trends and Projections: IPv6

> 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! —



Per-Country IPv6 adoption



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.

	Malware Samples Leveraging TOR
45,000	
40,000	
35,000	
30,000	
25,000	
20,000	
15,000	٨
10,000	
5,000	
0	Jan-13 Mar-13 Mar-13 Jun-13 Jun-13 Jun-13 Jun-13 Sep-13 Sep-13 Jun-14 Jan-14 Jun-14 Jun-14 Jun-14 Jun-14 Jun-14 Jun-15 Sep-14 Sep-15 Mar-15 Anct 15

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





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]	Туре 🗢	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

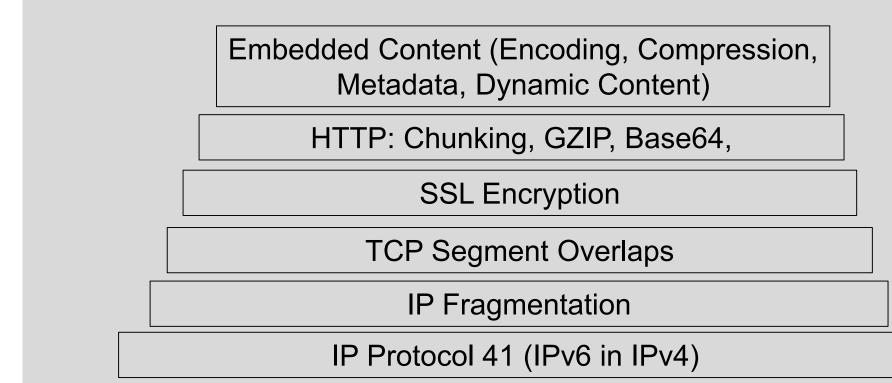
Source: Alexa Top Websites: https://en.wikipedia.org/wiki/List_of_most_popular_websites



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.



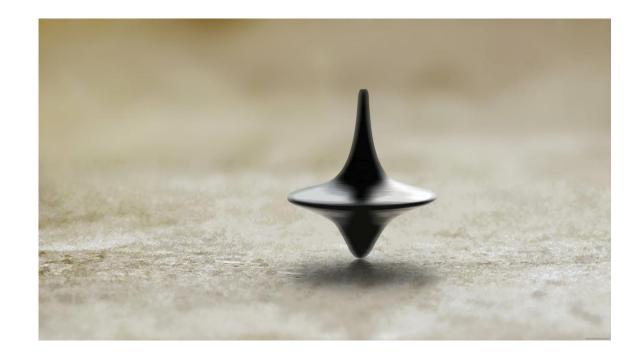


28

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



- <u>http://embeddedsw.net/doc/Data_hiding_and_steganography_annual_report_2012.pdf</u>
- Image Source: Inception, Christopher Nolan, 2010



[•] Further Reading: http://embeddedsw.net/doc/Thwarting_audio_steganography_attacks_in_cloud_storage_systems.pdf

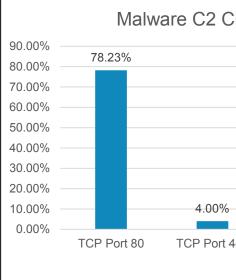
C2 Detection Is Critical!

- > 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.



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.





har	nnels by Port	
		45.000/
	1.84%	15.93%
143	TCP/UDP Port < 1024 except 80,443	TCP/UDP Port > 1024

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&ctSxHeV1=%E7%96%FD%A5%2F4%89K%DF%17%12.%970%1 %98p%2B%9FR%91%D7%AA%D1%C3%A3%06%96%FA%94%2Bs%E8%83o&Zhu=Z0%E0%1E%82%95%DD6%B8%88%B0%3D%97%EF%06%D1&Z1gwgOiL=%EA%D3%9 %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%E51%DB%2A%97%A9%5D%B4r%2 %D0%E3%89%A8e%99%A5%02%EAv%0C%5Ed47%A9%E7I%23&ZIXH=%23%0D%AFr%60uZ%D4%03%A9%D81%D9%CE%0F%B63%5D%CCs%3F%8C %26%7E%25%13%88g%E4%94%3E%E6%02%06i%21&viN=%E4W5%A5%0F%EAp%85%E8%C4%F2%3E%00%B4K%BDn%7B%22%AFs%90%C4%9B%C6% %12%09%81%3D%21W%BB%2AA%9F%ACd%AALx %2C&oZhroNa=R%C7%92%F5n%D7%5D%9B%14%0D%0Ee%A3%400%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%B7v%2CV8%CA%AE%9C%C2%B9e08%07%CE%C0%2F%81%91&1mHVT=%A5%DE%DC%5E% %11%D1%27%DE0%D95%26v%E62%212t%7C%B4%03%F8%2F&ICU=%9C%22D%F0%7B%E8%CB%A5%EB%CB%B7%D5%1B%FC%A8%BD%2 %E6%23%EA&AAgWfx=%C0%DF%D0%27%96%08%C0%A7%95%EB%03%EA %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...
```

alert http \$HOME NET any -> \$EXTERNAL NET any (msg:"ET TROJAN Ransomware Locky CnC Beacon 21 May"; flow:established,to server; content:"POST"; http metho d; 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:202 2952; rev:2;)





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; pore: //.{2}[A-Z][a-z]+(?:\x27[a-z]+)(?:\x20[A-Z][a-z]+){1,2})?[01]/Rs"; content: [55 04 0a]"; distance:0; po 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;)



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.

14 28.480299 1 - 28 30.049322 1		Destination 192.168.58.10	Protocol Ler DNS	ngth Info 496 Standard query response 0x0001 A dmowcuqwpbcaty2nedtmaamg4g.isc.org NS d0.org.afilias-nst.or
28 30.049322 1			DNS	496 Standard query response 0x0001 A dmowcuqwpbcaty2nedtmaamg4g.isc.org NS d0.org.afilias-nst.or
	192.168.58.10	10 55 00 1		
56 30.216163 1		10.55.99.1	DNS	90 Standard query 0x0003 A a2cnkterz1chpybi5tso4vdapd.com
	192.168.58.10	4.2.2.1	DNS	90 Standard query 0x0010 A lz3i5hdrtooqpzr11ptma5sjqc.com
57 30.245775 4	4.2.2.1	192.168.58.10	DNS	122 Standard query response 0x0010 A lz3i5hdrtooqpzr11ptma5sjqc.com A 198.105.254.11 A 198.105.2
58 30.246093 1	192.168.58.10	4.2.2.1	DNS	94 Standard query 0x0011 A www.lgvf4dsx1yaqck4wexruxddc0b.com
60 30.277899 4	4.2.2.1	192.168.58.10	DNS	126 Standard query response 0x0011 A www.lgvf4dsx1yaqck4wexruxddc0b.com A 198.105.254.11 A 198.1
65 30.296153 1	192.168.58.10	10.55.99.1	DNS	94 Standard query 0x0014 A www.ydkpnhyqgd4wafrptttkto5g1e.com
77 30.448909 1	192.168.58.10	4.2.2.2	DNS	90 Standard query 0x001a A wor321mugb01hcp4ddswnhepmb.com
78 30.457870 4	4.2.2.2	192.168.58.10	DNS	122 Standard query response 0x001a A wor321mugb01hcp4ddswnhepmb.com A 198.105.254.11 A 198.105.2
79 30.458100 1	192.168.58.10	4.2.2.2	DNS	94 Standard query 0x001b A www.pgqyhhwrqnzdctgbhqqkuxqe2d.com
80 30.485405 1	192.168.58.10	10.55.99.1	DNS	81 Standard query 0x001c A net172.rebindtest.com
81 30.485561 4	4.2.2.2	192.168.58.10	DNS	126 Standard query response 0x001b A www.pgqyhhwrqnzdctgbhqqkuxqe2d.com A 198.105.254.11 A 198.1
82 30.496574 1	10.55.99.1	192.168.58.10	DNS	321 Standard query response 0x001c A net172.rebindtest.com A 172.16.0.1 NS k.gtld-servers.net NS
84 30.524708 1	192.168.58.10	10.55.99.1	DNS	87 Standard query 0x001d TXT 2.2.2.4.test.senderbase.org
Ethernet II, Src: / Internet Protocol V	AsustekC_8f:a0:3a (00 Version 4, Src: 192.1 ocol, Src Port: 50072	94 bytes captured (752 bits) :11:2f:8f:a0:3a), Dst: da:dd:49:3b:4b:9b (da:dd:44 68.58.10, Dst: 10.55.99.1 (50072), Dst Port: 53 (53)	9:3b:4b:9b)	

> 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.



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
 - <u>http://doc.emergingthreats.net/bin/view/Main/EmergingFAQ</u>
 - 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!

