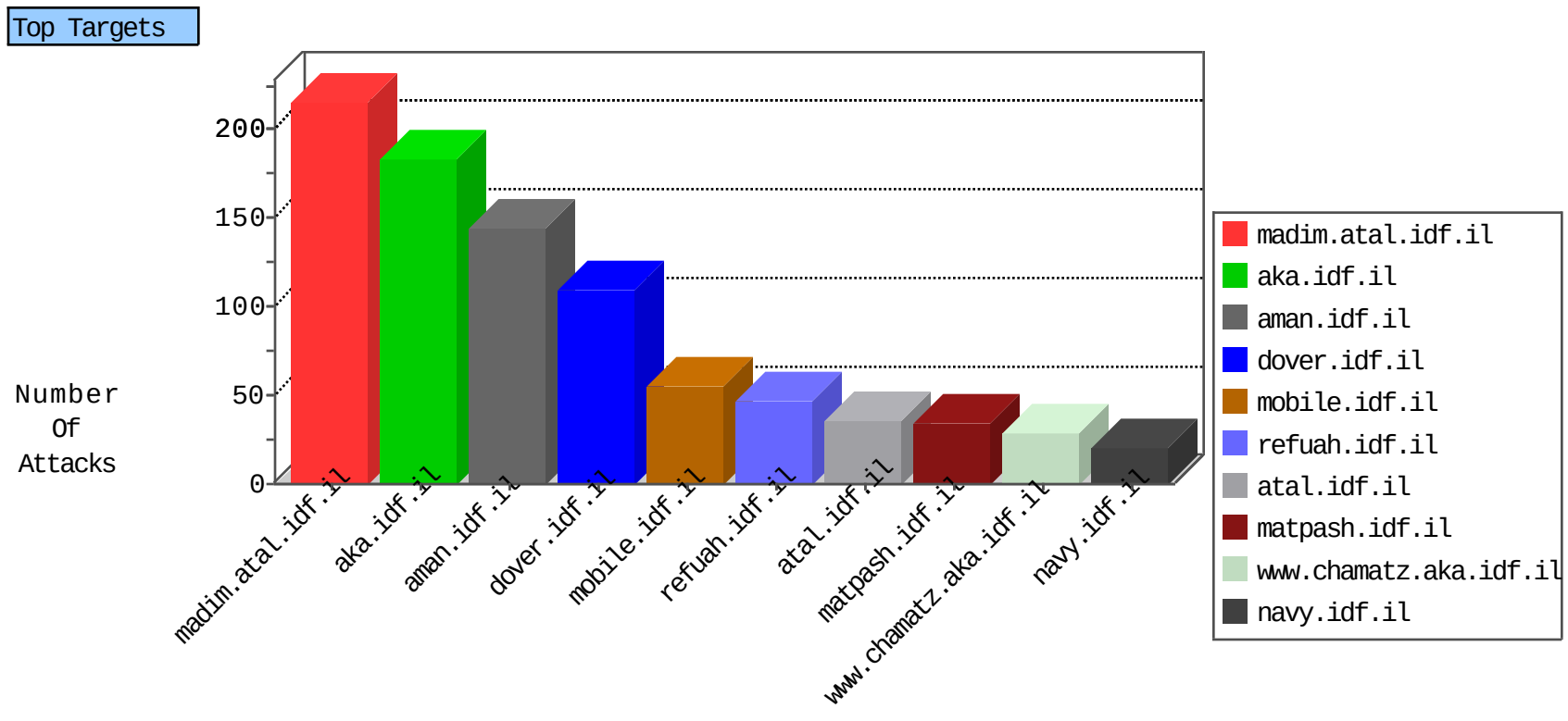
09-20-2016-20:04:01 to 09-20-2016-21:04:01

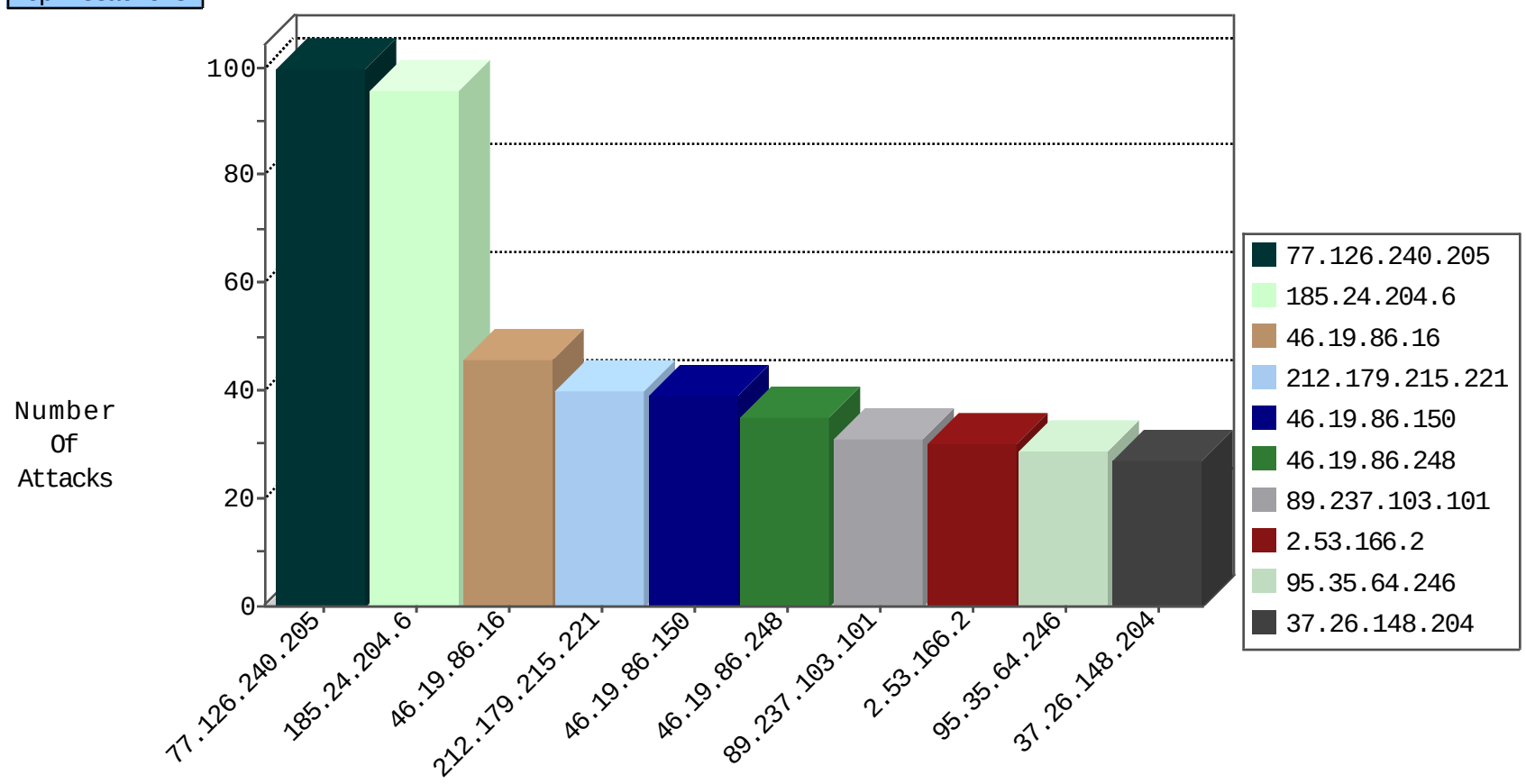
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-20-2016-20:04:01 to 09-20-2016-21:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.149.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
45.32.201.228	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
45.32.205.133	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
93.174.91.37	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
45.32.201.228	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
212.179.215.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-20-2016-20:04:01 to 09-20-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.110.147.80	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-20-2016-20:04:01 to 09-20-2016-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.126.240.205	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
197.161.47.76	147.237.72.156	Egypt	aman.idf.il	ET SCAN NMAP -f -sS	1
92.42.162.161	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
172.246.126.103	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
84.229.93.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.246.126.103	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
77.252.26.51	147.237.8.27	Poland	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
172.246.126.103	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
172.246.126.103	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.1.12	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
50.84.213.146	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
223.197.132.235	147.237.0.33	Hong Kong	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.103.126.194	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.244.79	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
95.156.251.10	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
197.161.47.76	147.237.72.156	Egypt	aman.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.91.29	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.76.197	Switzerland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.155	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
172.246.126.103	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
77.252.26.51	147.237.8.27	Poland	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
172.246.126.103	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
77.252.26.51	147.237.8.27	Poland	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
172.246.126.103	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
68.0.196.45	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
172.243.214.200	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.77.235	Singapore	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
50.84.213.146	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.215.221	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
103.207.36.84	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
1.34.172.28	147.237.77.243	Taiwan	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.241.137.4	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-20:04:01 to 09-20-2016-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.166.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
95.35.64.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
89.237.103.101	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
89.237.107.221	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
77.126.76.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.225.106	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
37.26.148.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
109.253.216.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.117.108.210	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
217.132.33.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.250.127.125	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
212.179.215.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.154.81.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.141	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.14.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.141	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.215.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.179.215.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.165.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.111.182.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.140	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.160.60	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.141	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.240	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.140	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
113.23.59.111	Vietnam	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.215.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.115.83.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.154.81.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
84.109.176.170	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.150	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.111.182.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.3.147.173	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.179.215.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.137.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.136.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
97.114.98.246	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.111.5.55	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-20-2016-20:04:01 to 09-20-2016-21:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.24.204.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
2.53.30.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 77.126.240.205	Block	9
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 77.126.240.205	Block	9
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 77.126.240.205	Block	9
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 77.126.240.205	Block	8
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.126.240.205	Block	7
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 77.126.240.205	Block	5
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 77.126.240.205	Block	5
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 77.126.240.205	Block	5
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 77.126.240.205	Block	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 77.126.240.205	Block	4
79.182.145.113	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 77.126.240.205	Block	3
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
188.23.151.54	Austria	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	3
77.138.37.102	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	2
1.20.202.235	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
217.132.9.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.37.102	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.37.102	Block	2
109.65.39.239	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Name ^ПTx›Þ’TK»4t SW· W¯5[[#5]]Ɔ•W Sƒ`Q†1tûQ[[#18l”¯•¼©fy0 0 …µ ni]]ר	Block	1
176.13.3.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.227.23	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	NULL Character in Method [[#0]]àÄ>[[#14]]×óè‰[ç8•sº0tyºF´ÛÑÑ8àà\z,z[[#27]]RÂãçÎÜöYÍì	Block	1
31.154.81.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Query String e¹ v[[#14]]/-eh§[[#0]]•¥U ×{) Nÿ† ¢[[#11]] K[[#15]]¢'/ЖÛ@ [[#26]]³ƆnZ[[#14]]”^ ,,ßY[[#15]][[®•¥œ &Ɔ#8]]7 ¢Š4Û \X¯ ‡[[¬#31¦J¹•-]]71#[[]]62#[["Н» }]]ר[[8#]]°ıı'2JɹOMS«ıı ¼?¹Ý[[#1]]H¹•”*…¶ •O\šaft'…Ÿ [[ʋ#5]]8#[[Ê'Þl no •]]ע[[4#]]3q[[#25]]ע ±e[[#23]]=	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
217.147.162.203	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
89.237.103.101	France	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
157.55.39.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 109.65.39.239 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name J,•lÀ3Mâ•m…ÚüCÞÒE[[#21]]ýu>™õÊb,%$´õE,3/¤ï-Ó[[#3]],„[[#8]]Ï"µwd.[[#19]]áÂ+åfN,ôÍ[[#6]]N[[#7]]0ó[[#20]]+š~n¯=•ñK[[#11]]•7'ŸÆÎ°nžÖ[[#30]]E»¤[[#25]]äË[[#17]]¿çòØüHÖ[[#25]]b=•[[#12]]ÈDL_ãúÑ²áù;¢…Vl§©*ø)vŠ[[#25]][[#22]]^6Àà][[#28]],#ÚH-(7[[#29]]Š'ü\TšÌ.´–ø[[#27]]?[[#11]]‡	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Query String ^ПTx›Þ’TK»4t SW· W¯5[[#5]]Ɔ•W Sƒ `Q†1tûQ[[#18l”¯•¼©fy0 0 …µ no]]ר	Block	1
176.13.234.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.12.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.117.28.67	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ï“ÆÚ in URL lÞ’Ê[[#8]][[ע#4]]3]]52#[[qע ±e[[#23]]=	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	NULL Character in URL +u}› Ð@ph±[[#16]]:¬w[[#31]]u "tp\~ ¯ _[[#25]]r[[#0]][[#19]] Ъ%Ъ•Ún [[#17]] e [;ƒi€$¥$[[#22]]8.5¥µ¥6©	Block	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL lÞ’Ê[[#8]][[ע#4]]3]]52#[[qע=]]32#[[e±	Block	1
89.237.103.101	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Malformed URL µ… 0 0yf ©q¼• ¯”lר	Block	1
77.138.41.119	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

09-20-2016-20:04:01 to 09-20-2016-21:04:01