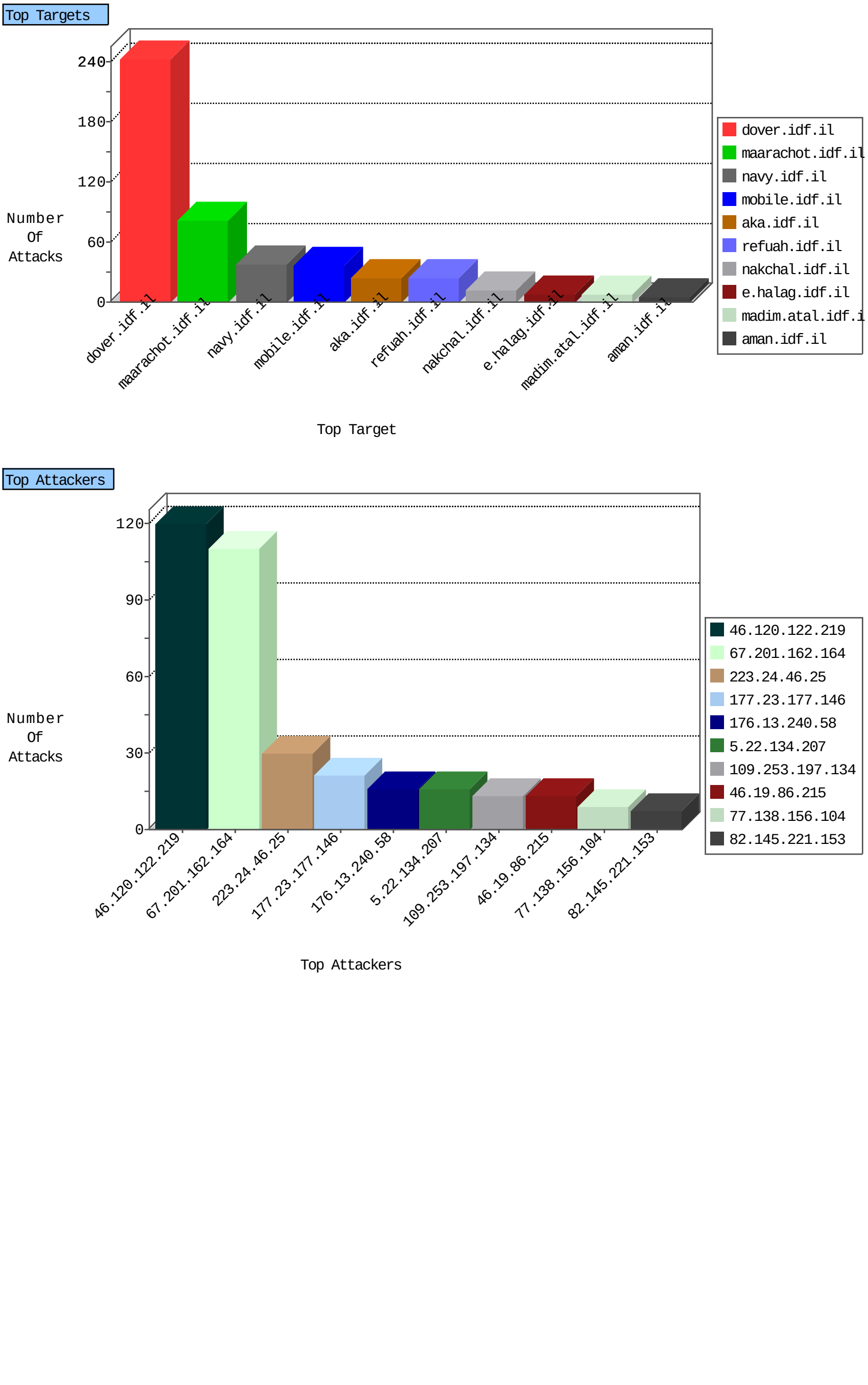
09-30-2016-06:04:07 to 09-30-2016-07:04:07

IDF Under Attack Daily Report



09-30-2016-06:04:07 to 09-30-2016-07:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
67.201.162.164	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
77.138.156.104	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
82.145.221.153	Europe	147.237.76.86	navy.idf.il	Black List	drop	7
67.201.162.164	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
46.120.122.219	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1

09-30-2016-06:04:07 to 09-30-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.232.58	France	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
123.126.68.101	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-30-2016-06:04:07 to 09-30-2016-07:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	76
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	10
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	2
175.156.146.206	147.237.8.50	Singapore	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
116.87.213.138	147.237.8.27	Singapore	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	2
163.172.169.150	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
112.115.92.7	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.231.186.118	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
109.189.51.81	147.237.72.166	Norway	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

09-30-2016-06:04:07 to 09-30-2016-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
67.201.162.164	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
223.24.46.25	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
67.201.162.164	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
177.23.177.146	Brazil	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	21
46.120.122.219	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
176.13.240.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.253.197.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
201.87.232.128	Brazil	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
89.138.105.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.215	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.215	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.120.126.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.133.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.83	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.183.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
150.203.212.254	Australia	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.243.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.146.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.146.246	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
150.203.212.254	Australia	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.138.156.104	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.120.122.219	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
125.77.28.26	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.46.39.133	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.199.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
201.144.222.85	Mexico	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.44	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.76	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.122.219	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
109.66.128.84	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.243.55.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
67.201.162.164	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
176.13.243.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
125.77.28.26	China	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.64.199.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.48	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.139.80	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
49.35.149.105	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.201	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.215	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.210.186.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.81.90.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-30-2016-06:04:07 to 09-30-2016-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	4
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	4
87.71.75.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	2
66.249.64.187	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.187	Block	2
74.6.254.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17348.jpg	Block	1
31.154.81.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
220.181.108.168	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
95.86.110.70	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
54.210.70.235	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
79.177.87.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14686-he/dover.aspx (hebrew)	Block	1
95.86.110.70	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 95.86.110.70	Block	1
66.102.6.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
192.243.55.131	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
84.108.194.218	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
154.47.32.87	United States	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
84.108.194.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.116.32.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.32.164	Block	1
180.76.15.149	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9022-he/refuah.aspx	Block	1
31.154.81.28	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
218.255.22.154	Hong Kong	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
46.116.32.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/_vti_bin/owssvr.dll	Block	1

09-30-2016-06:04:07 to 09-30-2016-07:04:07