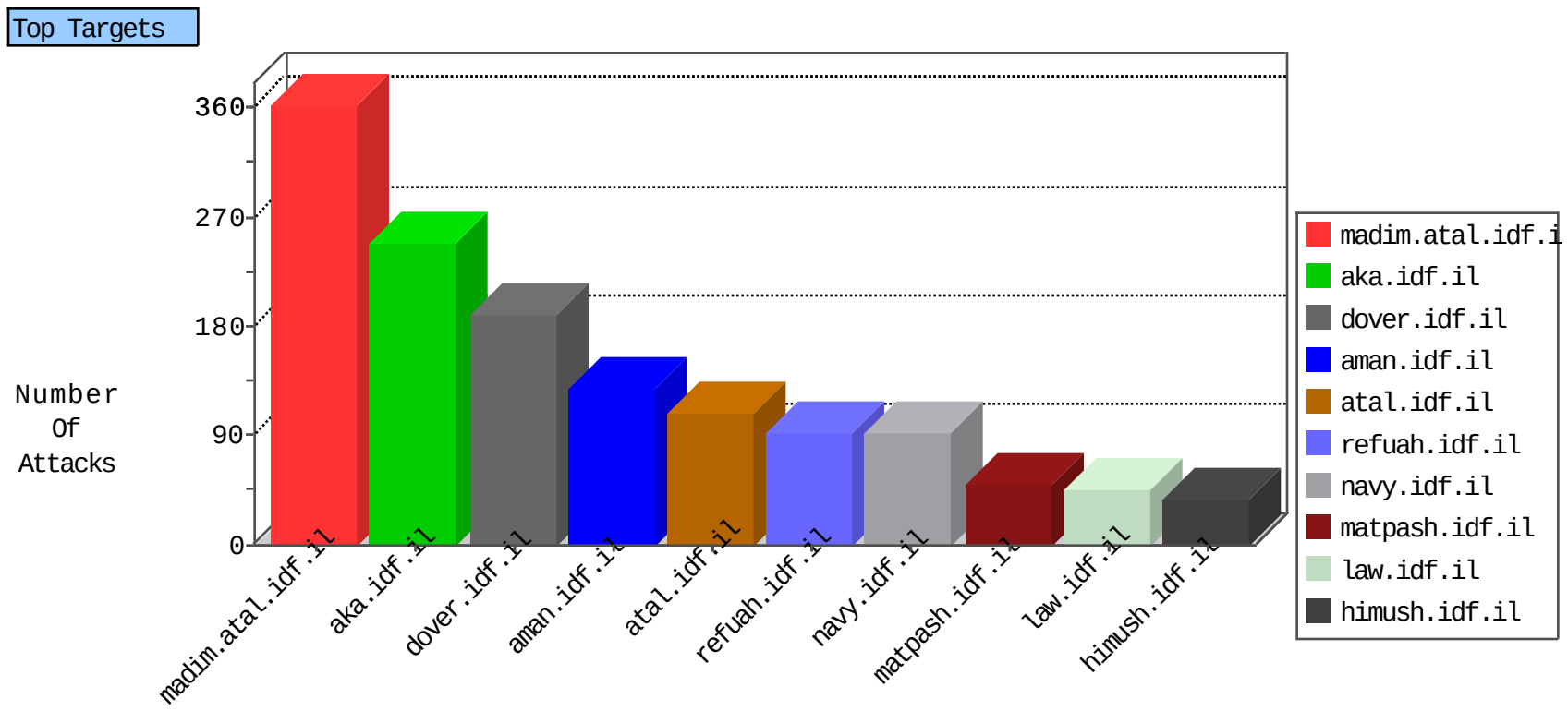
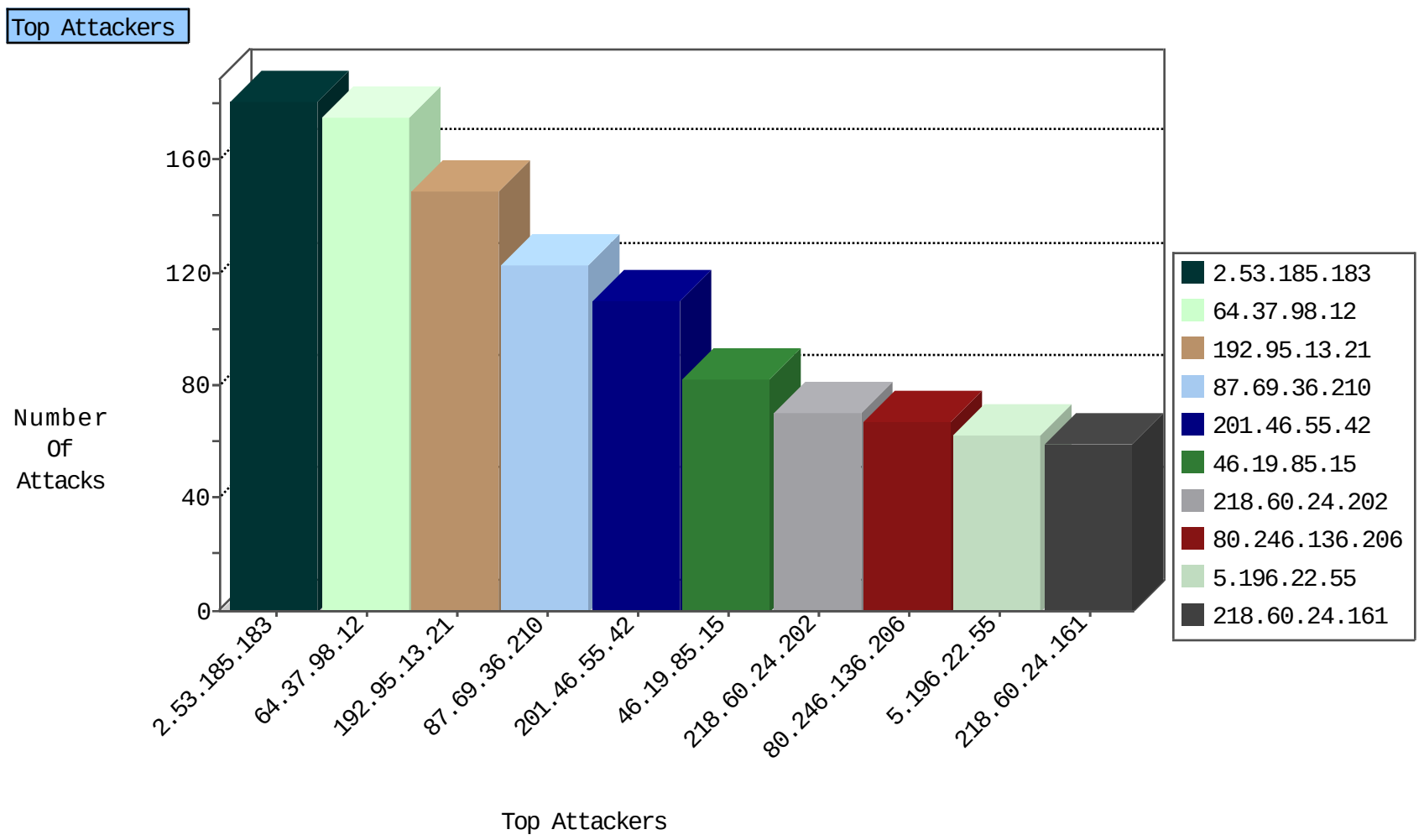
09-07-2016-09:04:00 to 09-07-2016-10:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-07-2016-09:04:00 to 09-07-2016-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.219.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
80.82.77.46	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
93.158.203.199	Netherlands	147.237.76.176	test.ncore.idf.i	Black List	drop	1

09-07-2016-09:04:00 to 09-07-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
5.196.22.55	France	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
5.196.22.55	France	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
5.196.22.55	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
191.236.150.197	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.68.127	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-07-2016-09:04:00 to 09-07-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.196.22.55	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	44
191.236.150.197	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
45.56.96.80	147.237.0.17	United States	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
79.180.135.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.4.180	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.19.86.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.80.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.110.40.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.94.142	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
82.166.91.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.11.27	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1
213.244.123.171	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.119.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.112.28.187	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
177.19.180.3	147.237.76.148	Brazil	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1

09-07-2016-09:04:00 to 09-07-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
87.69.36.210	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
62.0.203.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
87.69.36.210	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32
87.69.36.210	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
176.13.250.131	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
80.246.136.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
80.246.136.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.136.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
75.81.54.58	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.69.36.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.253.242.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
62.0.223.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.253.242.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
75.81.54.58	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
64.37.98.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
64.37.98.12	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.148.134	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
64.37.98.12	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.37.98.12	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
80.246.136.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
37.26.148.134	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
64.37.98.12	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
64.37.98.12	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
64.37.98.12	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
80.246.136.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
40.77.167.95	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6

09-07-2016-09:04:00 to 09-07-2016-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.185.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
46.19.85.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
109.253.131.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.253.146.88	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	16
183.14.17.5	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.14.17.5	Block	15
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.205.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
183.14.17.5	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
37.26.146.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.53.185.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.53.185.174	Block	4
89.139.107.175	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
2.55.27.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.198.164	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.4	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
82.81.88.212	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.185.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	2
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/	Block	2
109.253.140.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
205.250.113.205	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
176.13.233.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.130.166	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
80.82.24.129	Poland	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/61571.swf	Block	1
46.19.85.207	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
176.13.250.131	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
45.56.96.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 45.56.96.80 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.189.28.209	Germany	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.114	Israel	147.237.76.86	navy.idf.il	Distributed Abnormally Long Request	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/sip_storage/files/1/61571.swf	Block	1
46.19.85.207	Israel	147.237.76.42	refuah.idf.il	Distributed Illegal HTTP Version	Block	1
109.253.133.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
45.56.96.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.90.2.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
132.74.1.4	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.19.85.114	Israel	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	1
77.139.186.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.53.17.187	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.207	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
45.56.96.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized HTTP Method	Block	1
82.80.34.248	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.34.248	Block	1
204.79.180.124	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
46.19.85.114	Israel	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
37.26.148.134	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
107.77.224.185	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
79.182.36.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1

09-07-2016-09:04:00 to 09-07-2016-10:04:00