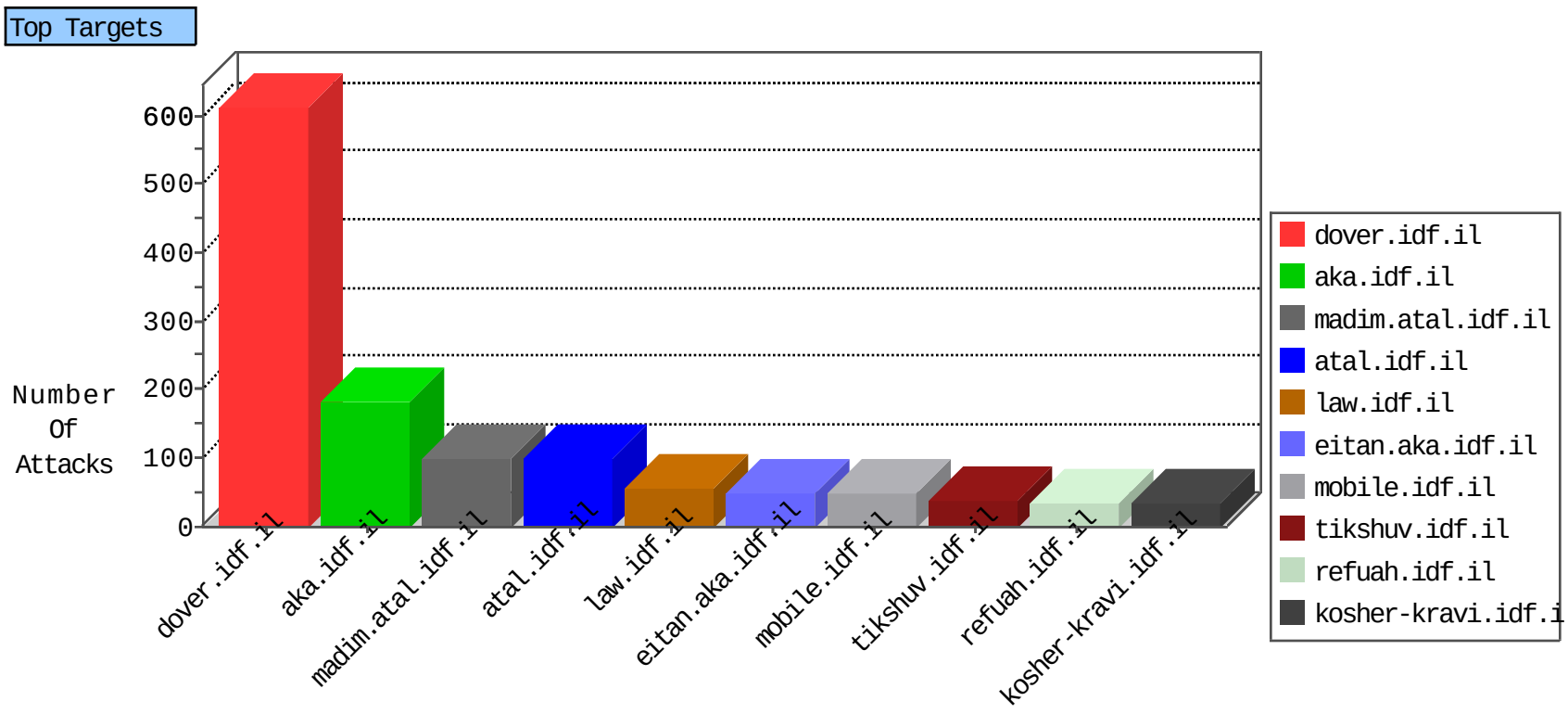
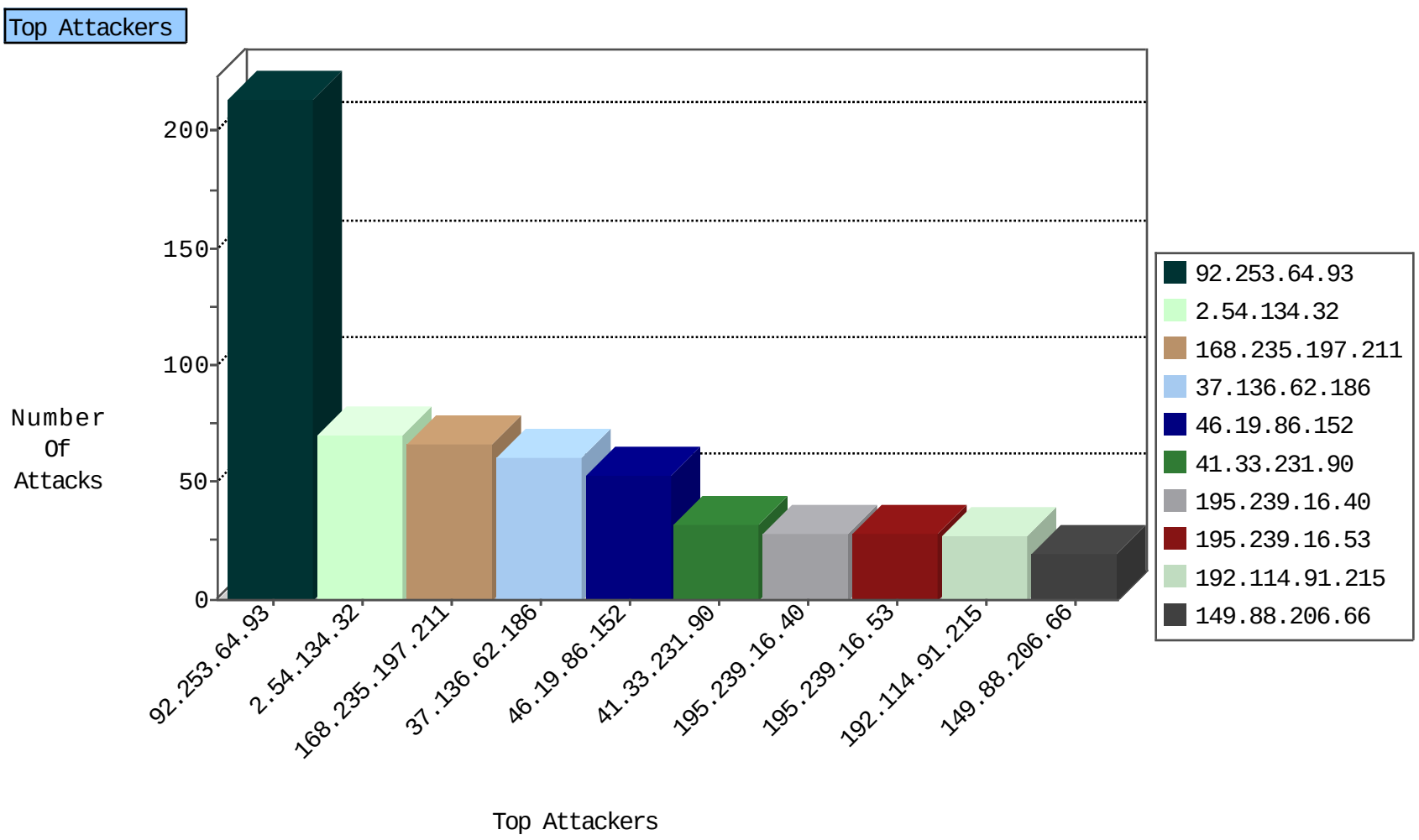
01-27-2016-23:04:09 to 01-28-2016-00:04:09

IDF Under Attack Daily Report





01-27-2016-23:04:09 to 01-28-2016-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
168.235.197.211	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
119.97.137.184	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
54.67.38.74	United States	147.237.0.19	madim.atal.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
78.186.57.235	Turkey	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-27-2016-23:04:09 to 01-28-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-27-2016-23:04:09 to 01-28-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
94.76.23.7	147.237.77.61	Bahrain	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
119.146.221.68	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
96.35.144.107	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.23.7	147.237.77.61	Bahrain	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
94.76.23.7	147.237.0.19	Bahrain	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.134.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
154.73.170.162	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
154.73.170.162	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
119.146.221.68	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
119.146.221.68	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
94.76.23.7	147.237.76.31	Bahrain	nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
66.240.213.93	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
182.91.218.54	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
154.73.170.162	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
137.117.105.139	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1

01-27-2016-23:04:09 to 01-28-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.197.211	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
37.136.62.186	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
92.253.64.93	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
192.114.91.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
92.253.64.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	23
2.54.134.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
79.177.205.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
92.253.64.93	Jordan	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	20
66.249.81.196	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	19
92.253.64.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
80.178.11.143	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
2.52.27.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
92.253.64.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
92.253.64.93	Jordan	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
92.253.64.93	Jordan	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
92.253.64.93	Jordan	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.54.134.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
92.253.64.93	Jordan	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
2.54.134.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
92.253.64.93	Jordan	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.134.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
92.253.64.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
92.253.64.93	Jordan	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence		monitor	11
185.32.179.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.20.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
92.253.64.93	Jordan	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
149.88.229.142	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.81.199	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
176.13.3.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.154.94.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
92.253.64.93	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.116.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.206.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.94.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

01-27-2016-23:04:09 to 01-28-2016-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
149.78.185.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.13.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.6.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.162.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.13.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.148.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.190	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
85.250.229.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.46.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
149.78.148.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlace in www.aka.idf.il/main/giyus/atuda/atuda.aspx	None	1
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
89.161.198.15	Poland	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
79.178.26.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.71.32.12	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
2.54.98.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.156.29	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.19.86.81	Israel	147.237.76.42	refuah.idf.il	Redundant HTTP Headers Referer	Block	1
41.207.15.46	Cote D'Ivoire	147.237.72.166	aka.idf.il	E-mail collector robots 14	Block	1
80.246.130.78	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 80.246.130.78	Block	1
5.102.254.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/menu-ending.gif	Block	1
46.121.37.45	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.121.37.45	Block	1
149.78.148.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
79.178.181.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.35.62.11	Switzerland	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/sidebar/bulletpurple.gif	Block	1
2.54.139.225	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
41.207.15.46	Cote D'Ivoire	147.237.72.166	aka.idf.il	eMail Hoarding	Block	1
84.228.18.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
31.154.94.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/logo.jpg	Block	1
46.121.37.45	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
2.52.157.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.35.75.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
79.179.197.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.147.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.35.62.11	Switzerland	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1

01-27-2016-23:04:09 to 01-28-2016-00:04:09