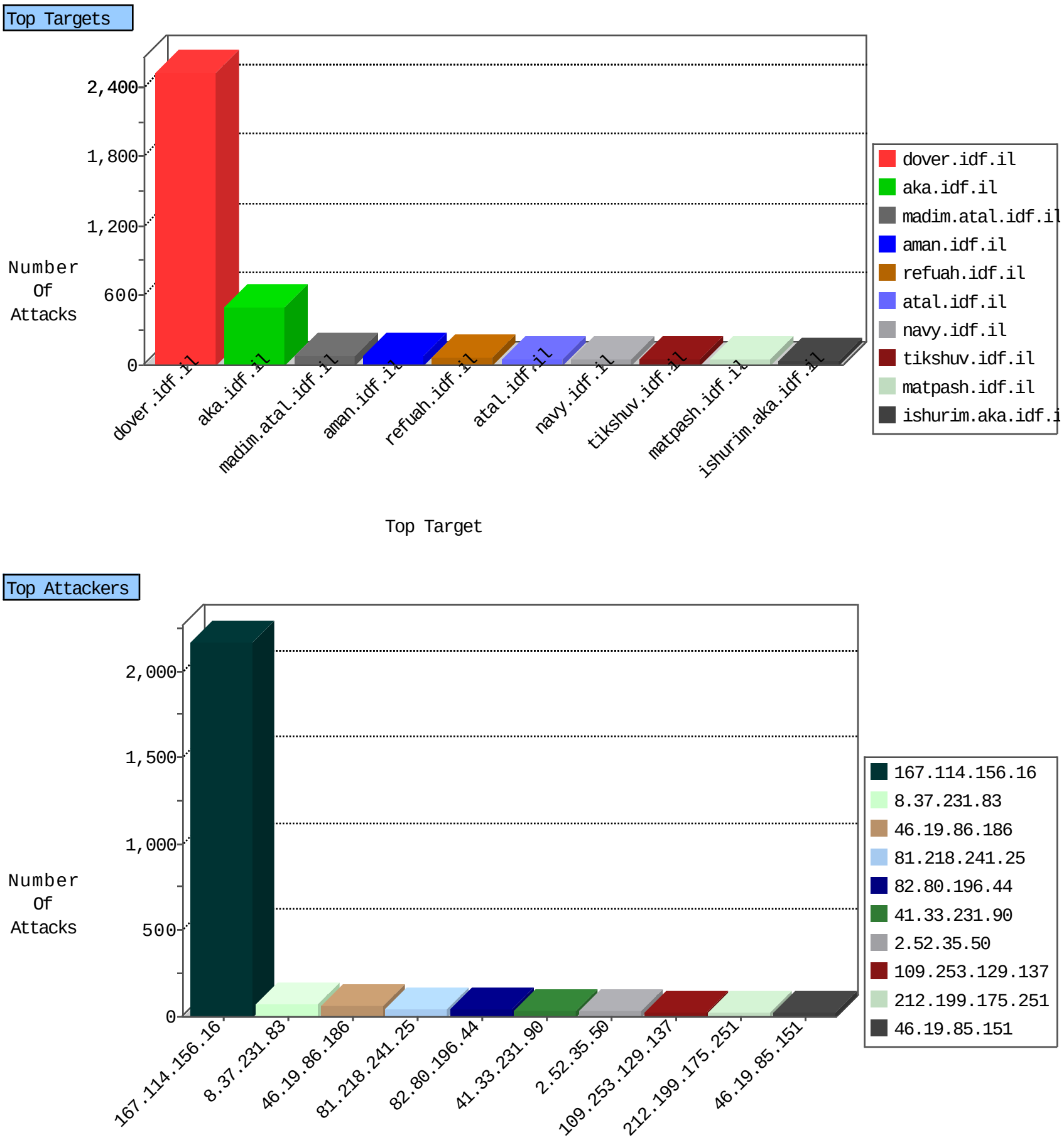
01-13-2016-12:04:05 to 01-13-2016-13:04:05

IDF Under Attack
Daily Report



01-13-2016-12:04:05 to 01-13-2016-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3191
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
109.253.129.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
212.199.175.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
176.13.1.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.54.167.151	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.231.83	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
63.141.227.98	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.243	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
81.218.208.46	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
81.218.208.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1

01-13-2016-12:04:05 to 01-13-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.87.98	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-13-2016-12:04:05 to 01-13-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
124.133.2.85	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.230.93.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.8	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
77.125.114.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.43.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.216	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.216	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
124.133.2.85	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
124.133.2.85	147.237.0.19	China	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.133.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.114.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
8.37.231.83	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.131.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.216	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-13-2016-12:04:05 to 01-13-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.83	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	68
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
77.125.131.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.86.125	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
176.228.168.192	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.19.86.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.184.8.186	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
2.54.185.98	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.186.104.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
79.177.221.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.223.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.28.183.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.19.85.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.130.8	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.161.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.253.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.199.175.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.35.50	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.35.50	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.226.45.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.131.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.224.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.218	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.145.4	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.64.184.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.35.50	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.223.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.133.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.8.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.5.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.5.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.154	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.52.35.50	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.246.130.8	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.73.245.32	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.244.93.158	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
212.199.175.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.35.50	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.62	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

01-13-2016-12:04:05 to 01-13-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	16
31.44.136.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.44.136.131	Block	8
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	6
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.70.243	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	5
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	4
31.44.136.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	4
2.54.43.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.26	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	3
77.125.114.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
188.143.232.26	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	2
79.177.60.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.141.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
95.86.95.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1442-he/refuah.aspx&sa=u&ved=0ahukewikqr67zabkahxcya4khwolciuqfggimaa&usg=afqjcnfkbzumin7zyuiahcdh2tknh2cyzq	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
2.54.158.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.148.208	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.148.208	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	2
46.19.85.151	Israel	147.237.76.31	nakchal.idf.il	Malformed URL _pk_id.119.2366=481e3393cace6511.1452682585.1.1452682585.1452682585.;	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.148.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.11.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.89.217.234		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
80.246.139.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.151	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method a000; in URL _pk_id.119.2366=481e3393cace6511.1452682585.1.1452682585.1452682585.	Block	1
109.253.217.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19133-he/dover.aspx	Block	1
207.241.237.211	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.214.201.107	Moldova, Republic of	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
37.26.146.240	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
81.218.241.25	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 81.218.241.25	Block	1
188.143.232.26	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/faq/faq.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
10.100.35.52		147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.176.227.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl23 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.211	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
176.13.8.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.151	Israel	147.237.76.31	nakchal.idf.il	Multiple Abnormally Long Request from 46.19.85.151	Block	1
109.64.235.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

01-13-2016-12:04:05 to 01-13-2016-13:04:05