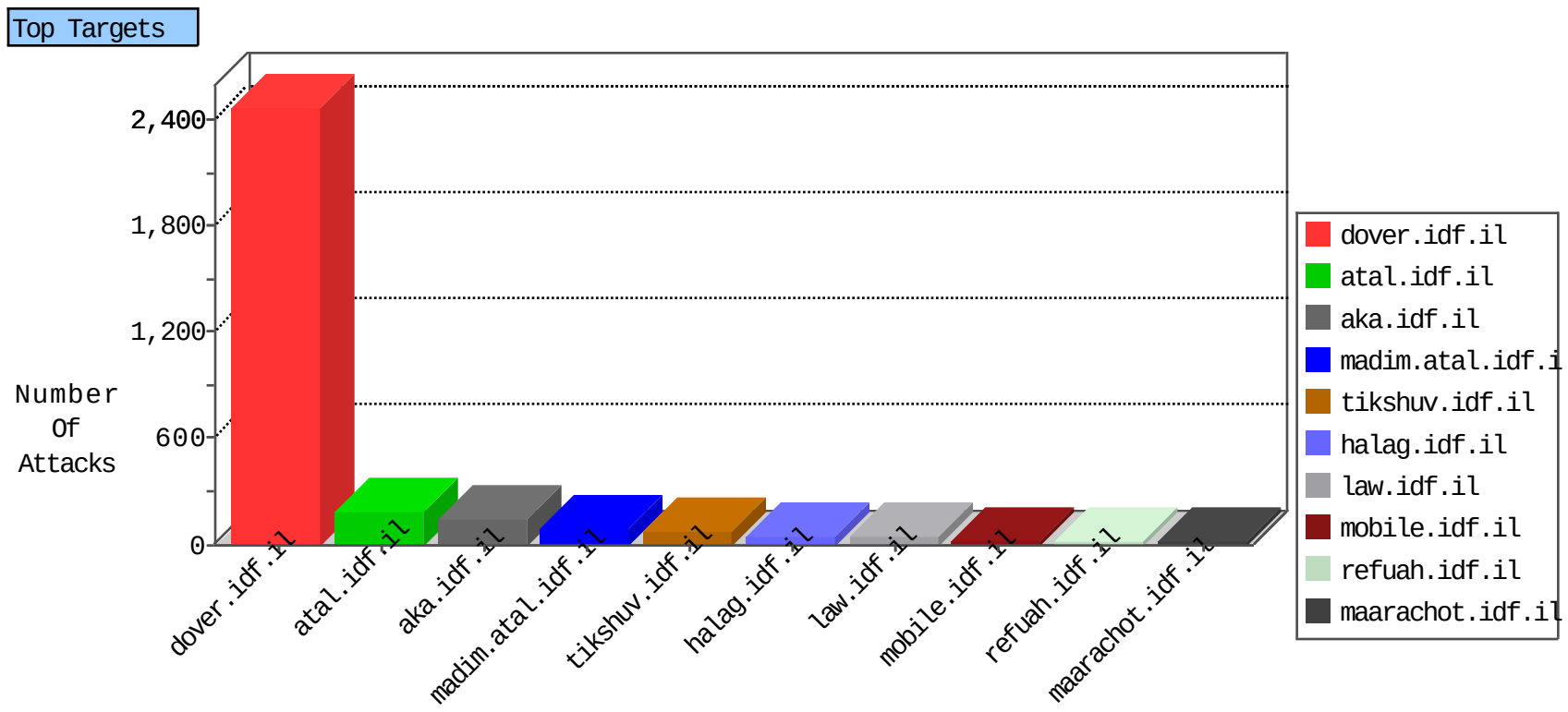
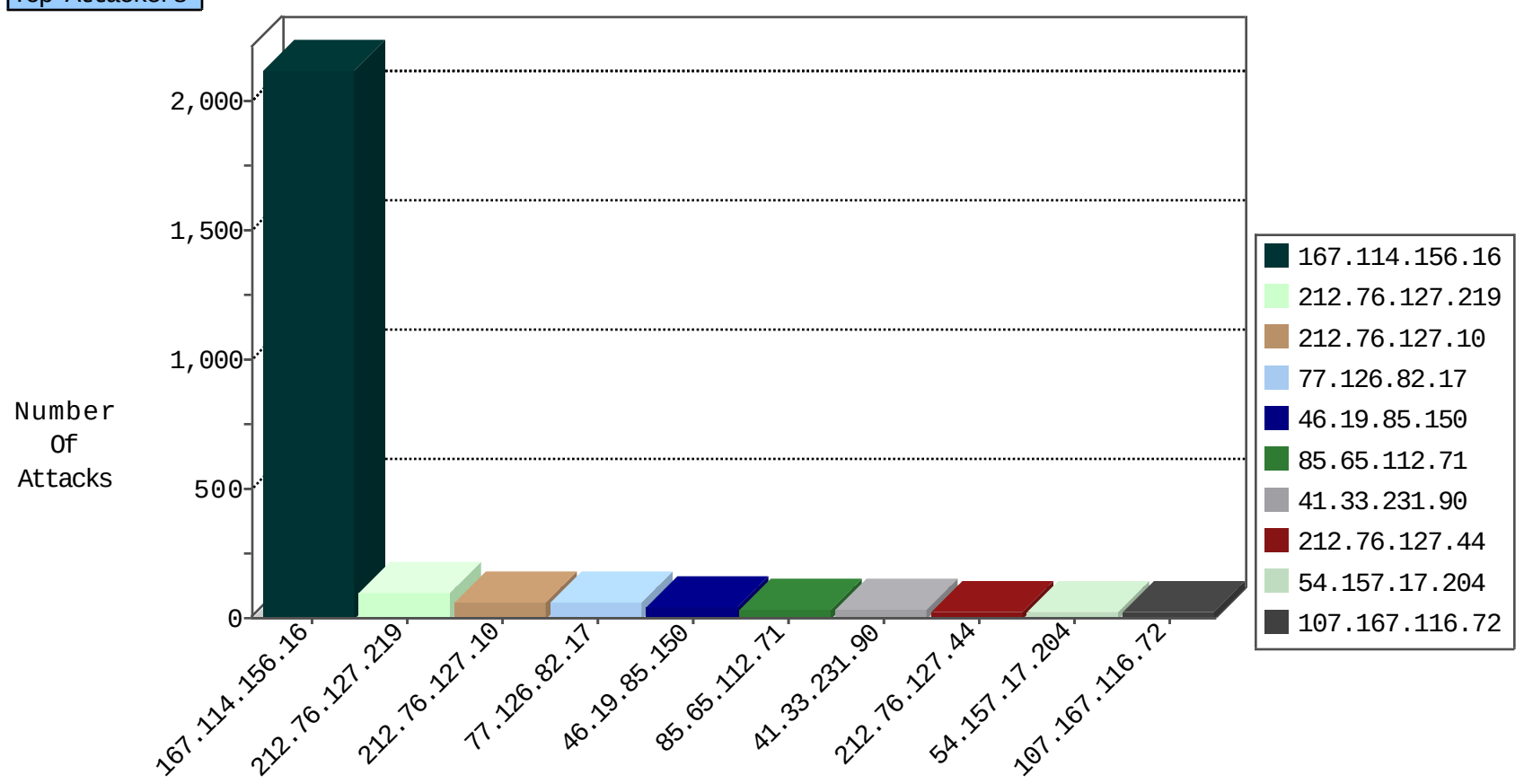
01-20-2016-22:04:09 to 01-20-2016-23:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-20-2016-22:04:09 to 01-20-2016-23:04:09

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	3055
79.182.39.164	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
219.250.228.44	Korea, Republic of	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	3
31.168.184.16	Israel	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
66.249.81.209	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
31.168.184.16	Israel	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

01-20-2016-22:04:09 to 01-20-2016-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.63.188.120	Russian Federation	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-20-2016-22:04:09 to 01-20-2016-23:04:09

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
182.162.73.59	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
95.86.124.198	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
82.102.199.21	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.241	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
60.217.72.16	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.218.113.195	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
60.217.72.16	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
85.93.5.66	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
213.57.200.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.213.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.249.184.162	147.237.0.35	Colombia	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
60.217.72.16	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.140.253.9	147.237.77.61	Morocco	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
182.162.73.59	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
60.217.72.16	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
60.217.72.16	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.178.56.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.249.184.162	147.237.0.35	Colombia	akaws.idf.il	ET SCAN NMAP -f -sS	1
41.140.253.9	147.237.77.61	Morocco	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
182.162.73.59	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.236.216.45	147.237.8.27	Iran, Islamic Republic of	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
60.217.72.16	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1

01-20-2016-22:04:09 to 01-20-2016-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	81
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
107.167.116.72	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
54.157.17.204	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	23
66.249.81.174	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	17
77.125.125.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
50.232.189.90	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.76.127.219	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.86.161	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
46.19.86.161	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
37.26.148.176	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
149.78.136.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.176.24.127	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
79.176.24.127	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.180.138.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.146.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
132.64.26.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.228.144.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.76.127.10	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.150	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
66.249.81.144	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
176.228.144.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.104.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.220.88	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.187.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.1.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.106	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.226.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.182.161.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.138.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.111	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.218.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.126.69.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.81.178	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
79.182.161.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

01-20-2016-22:04:09 to 01-20-2016-23:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.82.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
85.65.112.71	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
2.54.39.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
37.26.146.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.6.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.192.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.166.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giuys	Block	3
2.52.37.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.129.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	3
2.52.6.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
212.76.111.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21570-he/idfgdover.aspx&sa=u&ved=0ahukewievq7xnrnkahvc6cwkhvj6dpaqfggpmai&sig2=tfyqoddxqr4brrzgbgpmmw&usg=afqjcngkxkptobpol8pgxzxftd95sstiiw	Block	2
2.54.58.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.119.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.119.236	Block	2
166.170.5.127	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	2
176.13.11.40	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.177.22.48	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/xmlrpc.php	Block	1
132.64.26.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
84.229.145.201	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.54.5.59	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.108.181.23	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ^Â³Ã¡ÃšÃŸÃ¾Â?}XÂ¿l_Â»Â•[[#5]][[#17]]Â©Ã¶[[#4]]ÃŽÂ€Ãµ"Ã±Â¿[[#14]]v,Ã^Â³Ã'ÃŸÃ»[[#27]][[#27]]KÃ†[[#21]]{Ã³Â^&@Ã'Ã§pGwÂ?s@Â RÂœÃ,[[#23]]•[[#2]]-Â¥Ã…ÂµpÂ,Ã?[[#17]]Â²<sÃ¢Â?9Â¤[[#26]]Ã'Ã…[[#20]]Ã¬06e[[#17]]NIpÂŽÂ¯[[#5]]qoÃ¯Â¤Ã§Â^Ã·3[[#25]][[#25]]Â"Ã³Ã„[[#7]]BÂ¢Ã-Â¯Â¾l>[[#15]]Ã£Â¶Ãº[[#23]]Ã°ÃºÃ·Ã¾Â"Ã¹U[[#27]]rÃ—Ã¦Ã³fÃš•Â‰eNYsÂŒÂ?Â†Â?o[[#21]]Â–)Â'Ã¨Â·Ã£[[#20]]ÂƒÃ [[#1]]:Âž?Â¨+Ã‡Â›9Ã£Â¹Ã†Ã?Â?j[[#19]]$:Ã¶Ã¤Ã†Q[[#11]]Â¯![[#0]]&a;ÃµÂ"Ã…Ã'Ã±rÃ´`[bÂ±'Ã†Âº)ÃŽÂ"Â·Â™Ã‡Â¾Ã©3Â·Ã,Ã™Â¤Ã¤Ã¼(Ã¼Ã,•Ã½ÃŠRÃ	Block	1
109.160.146.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.146.100	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
197.39.130.152	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/113010.pdf	Block	1
93.172.244.46	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
85.64.96.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.202.245	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
157.55.39.125	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
79.176.25.43	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
128.70.102.149	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
24.213.216.70	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
84.229.145.201	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8942-he/refuah.aspx	Block	1
95.86.124.198	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
84.108.181.23	Israel	147.237.72.166	aka.idf.il	Malformed URL {â,¬Ö»Â¼$yÂŒm	Block	1
212.76.111.33	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-8064-he/eitan.aspx&sa=u&ved=0ahukewjhyz_qm7nkahwfdywkhsr-ahiqfggrma4&usg=afqjcneoibxl8oo7zgnvyplyr39enu7vlq	Block	1
79.183.146.100	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
178.255.168.90	Czech Republic	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 178.255.168.90 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.28.50.180	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
87.69.244.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.22.48	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
149.78.136.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.142.68.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.229.145.201	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
84.109.73.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/109940.pdf	Block	1
94.23.12.207	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	1

01-20-2016-22:04:09 to 01-20-2016-23:04:09