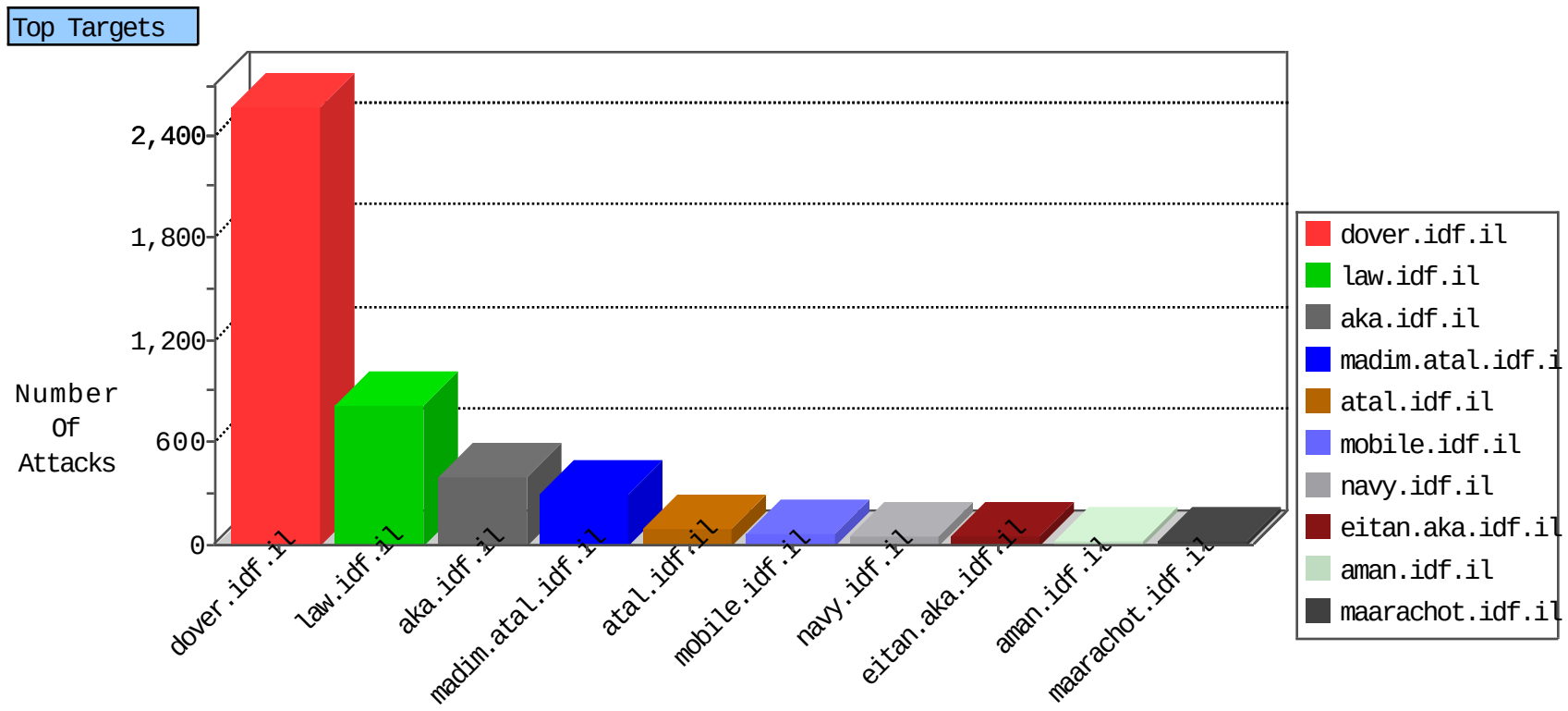
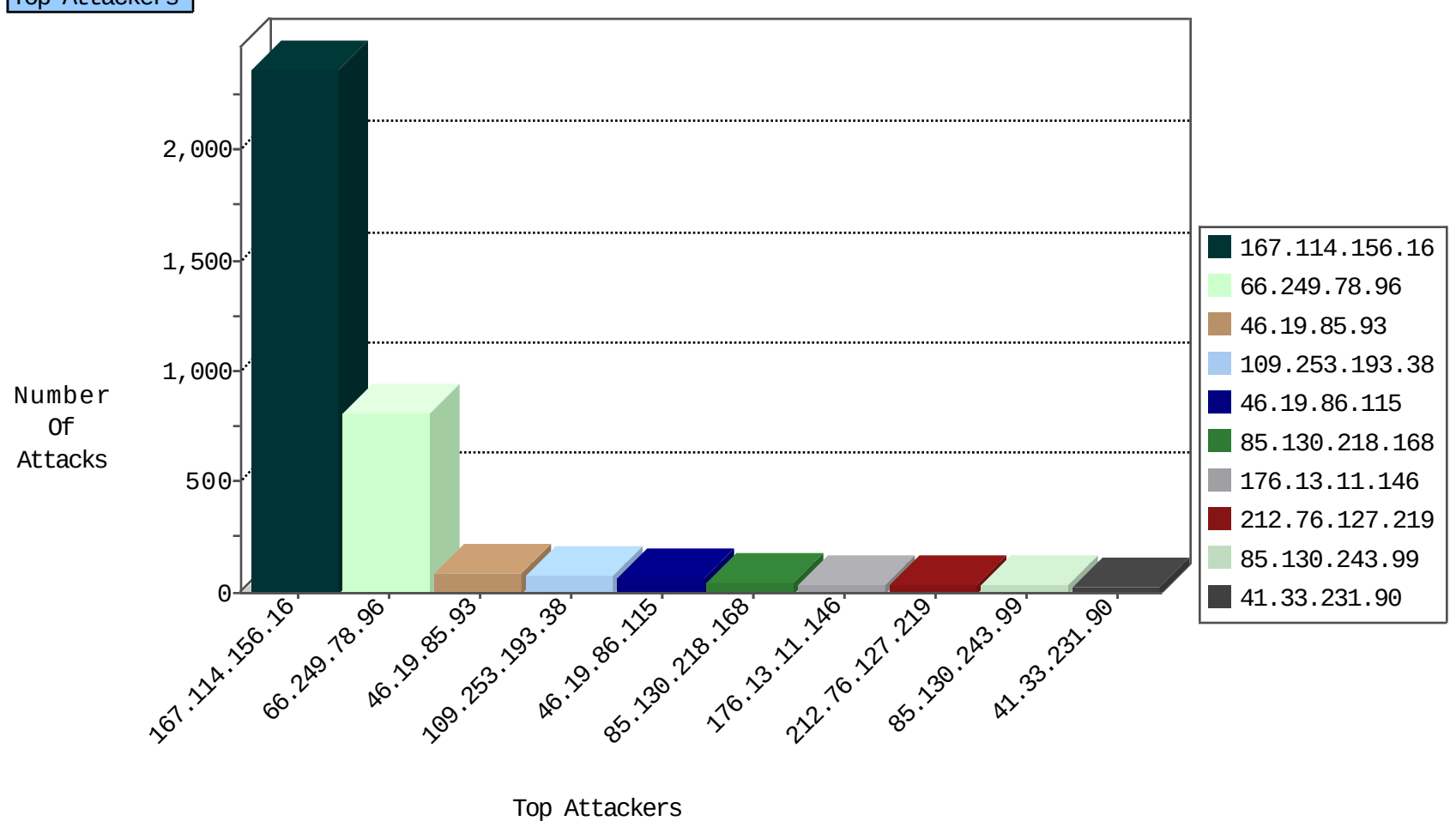
01-23-2016-20:04:06 to 01-23-2016-21:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-23-2016-20:04:06 to 01-23-2016-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3661
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3101
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	745
79.181.120.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.177.197.49	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
173.252.90.105	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
217.23.5.212	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
157.55.39.12	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-23-2016-20:04:06 to 01-23-2016-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
172.245.218.130	United States	147.237.76.42	refuah.idf.il	0543: HTTP: php.cgi Access	Block	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-23-2016-20:04:06 to 01-23-2016-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	809
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.181	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.202	Latvia	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.181	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.77.205	Ukraine	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.199.111.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
85.93.5.66	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential SSH Scan	1
95.86.71.43	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
77.127.202.247	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
93.174.93.181	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.197	United States	e.himush.idf.il	ET DROP Dshield Block Listed Source	1
93.174.93.181	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.174.28	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.199.111.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
80.246.130.229	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
93.174.93.181	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-23-2016-20:04:06 to 01-23-2016-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.11.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
5.28.184.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.86.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
85.130.218.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
85.130.218.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
85.130.218.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.49.216	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.64.166.56	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
85.130.243.99	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
85.130.243.99	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.243.99	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
79.177.55.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
41.190.18.67	Nigeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
77.127.202.247	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.102.254.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.67.49.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.234.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.200.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
65.132.59.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.179.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.112.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.72.161	Israel	147.237.72.166	aka.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
31.210.187.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.105.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
86.57.167.45	Belarus	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.200.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.208.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.49.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.32	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.144.19	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.239	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4

01-23-2016-20:04:06 to 01-23-2016-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
109.253.193.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
2.54.180.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
195.154.183.187	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
195.154.183.187	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.154.183.187	Block	4
176.13.17.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.68.242.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.22.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.29.213	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	3
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
197.34.253.134	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
2.54.144.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.159.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.228.217.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main.sachar	Block	2
77.127.202.247	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
87.68.242.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
212.76.122.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
197.34.253.134	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
77.127.202.247	Israel	147.237.77.216	dover.idf.il	NULL Character in Header Name at Âˆ[[#7]]#Ã„Ã¹Â Ã¹Â¼-[[#30]]Â¼[[#2]]Â„Ã¡LÂ·Â–Â¯Â°Â¿TÃ¾iÃ˜hÃ›[[#3]]ÂšÂŸÃ¥(Â³Âµ$Â¤a~cÂ€Ã?Ã±Ln /Â˜Â,[[#4]]VÂ-Ã?Ã–Ã?jÃ¨Â Ã´1(ZÂ¼Â£Â·Ã°Â…Ã¸=[[#23]]`Ã·{Ã‹][[#20]]ÂŠÂ•<Âˆvk F([[#3]]pÂ¬WÂ¹[[#18]]Â,9DÃ ZOhÂ’MÂŸÂ?Ã¥ÂŽzÃºÃƒ[[#23]]•Ã°MÃ,JYÂ¸Âš<[[#11]]"Â?cFÂ’("Â•Ãƒ Ã¢AÂ?bT#•Ã‡[[#16]]X{6Â¨ÃŠWÃ±'[[#18]]b&p}[[#20]]Ã•[[#14]]Ã³ÃŸ ÃµAVÂ?Â,Â‹Â¤(Ãªj Ã˜"Â’V3Ã¨Ã-Â’JÂ´4Â³9Ã³Â¬Ã’ Â¡eQ[[#28]]w[[#2]]Ã¹Â¤Â¢IÂ¦[[#26]]sÂƒÃƒ"Â§Â¡w{6p{[[#15]]Ã“Â°Ã–Âƒ Ã¹[Â»Â´$Ã´Â…CÂ»Â¼ÃƒÃ?Â?[[#21]](ÂžÂªÂƒm[[#6]]lUY Â?z~Â¯HÂ–Ã‰ Ã‰[	Block	1
184.168.200.111	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
86.57.167.45	Belarus	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.22.129.143	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.181.126.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/64816.doc	Block	1
157.55.39.233	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
2.54.130.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	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
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/64817.doc	Block	1
109.64.52.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.41.178	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/109078.pdf	Block	1
89.138.12.58	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
79.176.42.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.71	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
77.127.202.247	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/107610.pdf	Block	1
128.71.53.86	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
5.22.129.143	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â¶Â¤{.Ã²ÃŒÃž[[#15]]Â§=[[#0]]SRÂ— in URL	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
2.52.179.96	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.63.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
65.132.59.34	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.58.129.49	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.127.202.247	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Â˜5!Ã¹Ã?Â”ÃƒÂ¼ÃŽÂ§Ã™ LÂ®Ã¹ylt[[#25]]>[[#15]]6ÃšÃ?ÃœÃ’Â¡Â [[#26]]ÂªÂ¥Âµy3TecÂ³Ã¤DÂ, Â©Ã¤[[#29]]Ã‘&Ã¹Ã®[[#1]]ZÃ¨Ã‘Ã¸Â²Ã‹XÂ“Ã»Ã†S~Â-S[[#1]]Ã—ÃŸ %ÂµÂ?Â³EÂ»•Ã®(Âˆm„9Â°Â€~dÂ˜[0Ã°Â¿>eÂ“#Ã¬Ã“ÂŒ [[#17]]Â½Â¸[[#30]]Â°Ã€ÃŠ[[#25]]Ã¼VÃ¤Â¾Â–ÃŒ[[#7]]Ã…ÃƒvÃ¥ in URL	Block	1

01-23-2016-20:04:06 to 01-23-2016-21:04:06