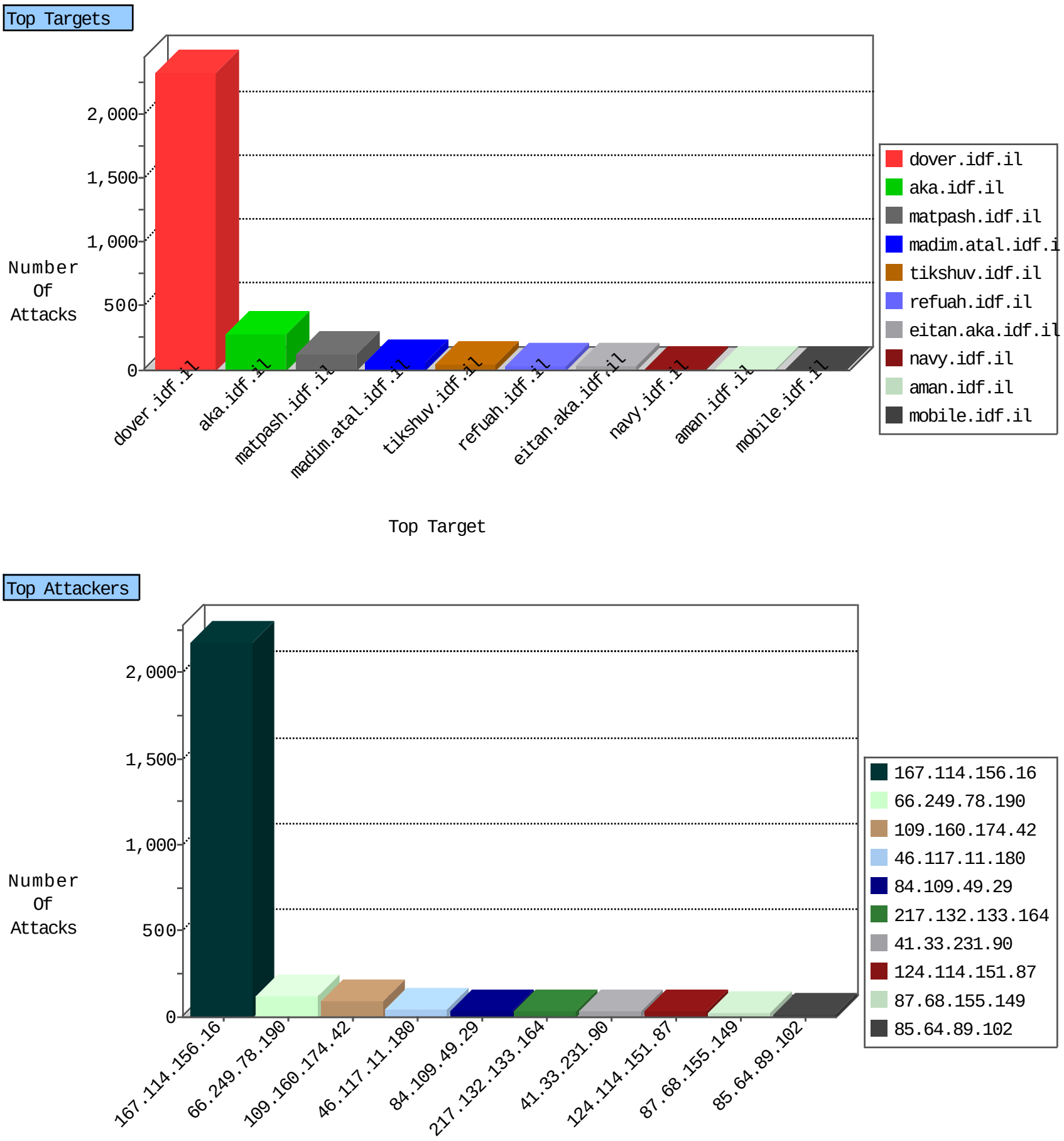
01-22-2016-19:04:02 to 01-22-2016-20:04:02

IDF Under Attack
Daily Report



01-22-2016-19:04:02 to 01-22-2016-20:04:02

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	3064
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
142.54.169.163	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

01-22-2016-19:04:02 to 01-22-2016-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.207		147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
188.165.15.202	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-22-2016-19:04:02 to 01-22-2016-20:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.190	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	120
124.114.151.87	147.237.72.166	China	aka.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
50.240.184.154	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -sS window 4096	1
50.240.184.154	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -f -sS	1
41.140.253.9	147.237.76.200	Morocco	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
189.198.96.102	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.207	147.237.77.216		dover.idf.il	SERVER-WEBAPP Setup.php access	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
177.106.47.246	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
91.218.15.202	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
50.240.184.154	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -sS window 2048	1
41.140.253.9	147.237.76.200	Morocco	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
189.198.96.102	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.207	147.237.77.216		dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
169.50.77.72	147.237.8.14	Switzerland	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

01-22-2016-19:04:02 to 01-22-2016-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.160.174.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
109.160.174.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
87.68.155.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
124.114.151.87	China	147.237.72.166	aka.idf.il	SQL Injection	SQL injection detected in URL: 'varChar'	monitor	10
109.66.27.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
188.120.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.64.89.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
85.64.89.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.203	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
46.19.85.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.117.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.109.9.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
77.127.205.68	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.65.210.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.161.55	Israel	147.237.72.167	ishurim.aka.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
77.127.205.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.229.72.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.168.137.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.72	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.188.68	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
82.166.118.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.32.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.96.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.50.211	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.229.72.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.163.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.123.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.201.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.137.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.254.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.159.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.113.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.10		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.8.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.201.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.133.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.11.177	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
31.210.188.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

01-22-2016-19:04:02 to 01-22-2016-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.11.180	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
217.132.133.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
124.114.151.87	China	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 124.114.151.87	Block	9
80.246.136.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 84.109.49.29	Block	5
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 84.109.49.29	Block	4
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 84.109.49.29	Block	4
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.109.49.29	Block	4
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.109.49.29	Block	3
84.109.114.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.156.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.216.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.191.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
2.54.180.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.125.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.125.250	Block	2
109.253.213.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.132.15.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.120.148.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.89.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Ã¢Ã¨Â¿MÃ¹Ã‚:Ã„H7Ã› Â³[[[#25]]Â¡Ã¬+NÂ§[[#23]]>Ã /Â¶Ã¡kÃ˜Â»Â¦[[#20]]Â?Â½Ã©[[#19]]ÂžÂŸ Â Ã¼Ã½Ã·Â«tÃŽ+VÃŽ;v{5Ã—AÃ?(Â°ÃŸGÂ	Block	1
217.113.50.61	Hungary	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
41.237.101.190	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
185.120.125.27		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.54.138.194	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.54.138.194	Block	1
79.182.96.48	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
93.173.37.53	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res ources/images/innerpage/goback.gif	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.109.49.29 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
40.77.167.64	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.64	Block	1
142.54.169.163	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.366901.com/	Block	1
2.52.139.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.157.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.192.84	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
217.113.50.61	Hungary	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
185.130.5.207		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scripts/setup.php	Block	1
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 84.109.49.29	Block	1
2.54.138.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idg	Block	1
115.133.89.97	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#30]]e4Xqau[[#2]][[#15]]Â¸Â’ yÃ‹Ã‹Â²Â?MÂ Â»Ã«Ã¥t•ÂºÂ»/Ã±OÂ–A[[#5]]4vÃ¬!EJÃ©Â– kfJc[[#19]]Â-MZ[[#2]]Ã->]ÃŸÃ°}kÂ¸Â·[[#3]]Ã?Ã¥[Ã²vvÂ,ÃœÃªÂ©>ÂšÃ¤ÂœÂ *FÂ™Ã’Ã‹Â©Â¿bÃ¿[[#20]]JÃ¦MÂ©Ã§\CÃªÂ§[[#14]]Â£-Â¹[[#8]]Â–0Âƒ Â¯Â±ÂœÃ•?Â“Â†[[#23]][[#2]]Ãž[[#25]]Â‹Ã«Â¾Ã¨Â’FÃˆ zu>[[#26]]WjÃ?ÃµÃ¦ Ã³Â±Ã°[[#29]]Ã¿Â„Ã·Ã¹Â´Ã–Â…Ã’KÂ¦Ã¼Â›Ã»ÃŒaÃŒÃ´Â¿\ ZÃ¦wÂ,Â¾Ã¤QÃ®c[[#8]]Ã¸Â Ã£GÃ»"ÂªÃ·ÃŠPÂ,	Block	1
93.173.37.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 93.173.37.53	Block	1
84.109.49.29	Israel	147.237.72.166	aka.idf.il	NULL Character in Method [[#31]]ENÃ½<[[#0]]Â©[[#8]]Ã·[[#1]][[#2]][[#27]][[#24]]Ã˜ [[#29]]e+I6Â²Â¬1Ã„Ã“Ã?Ã¢&tP[[#14]]Â»Â¶Â»[[#20]]	Block	1
212.199.57.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.49.29	Israel	147.237.72.166	aka.idf.il	Malformed URL *2×ŸÂ½hj[[#11]]2re×€ÃŸâ€™Ã›tkj[Æ’0[[#4]]^	Block	1
41.237.101.190	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
157.55.39.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1

01-22-2016-19:04:02 to 01-22-2016-20:04:02