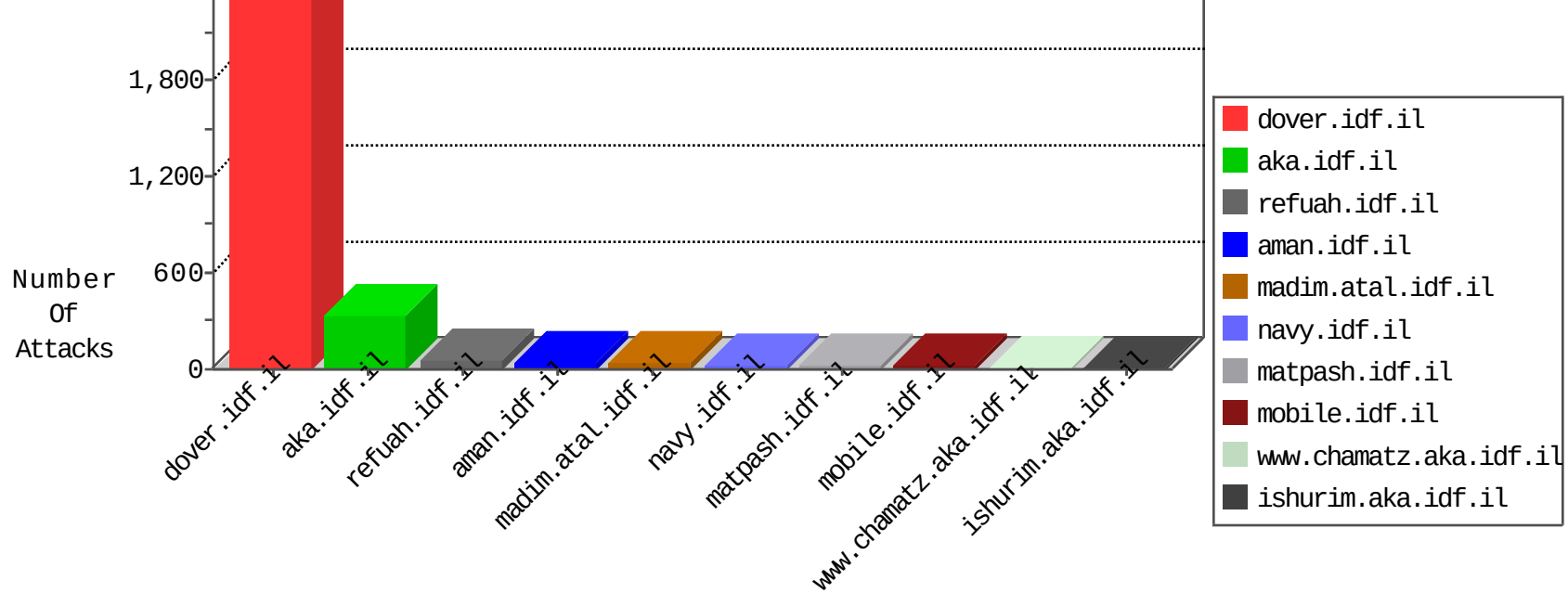
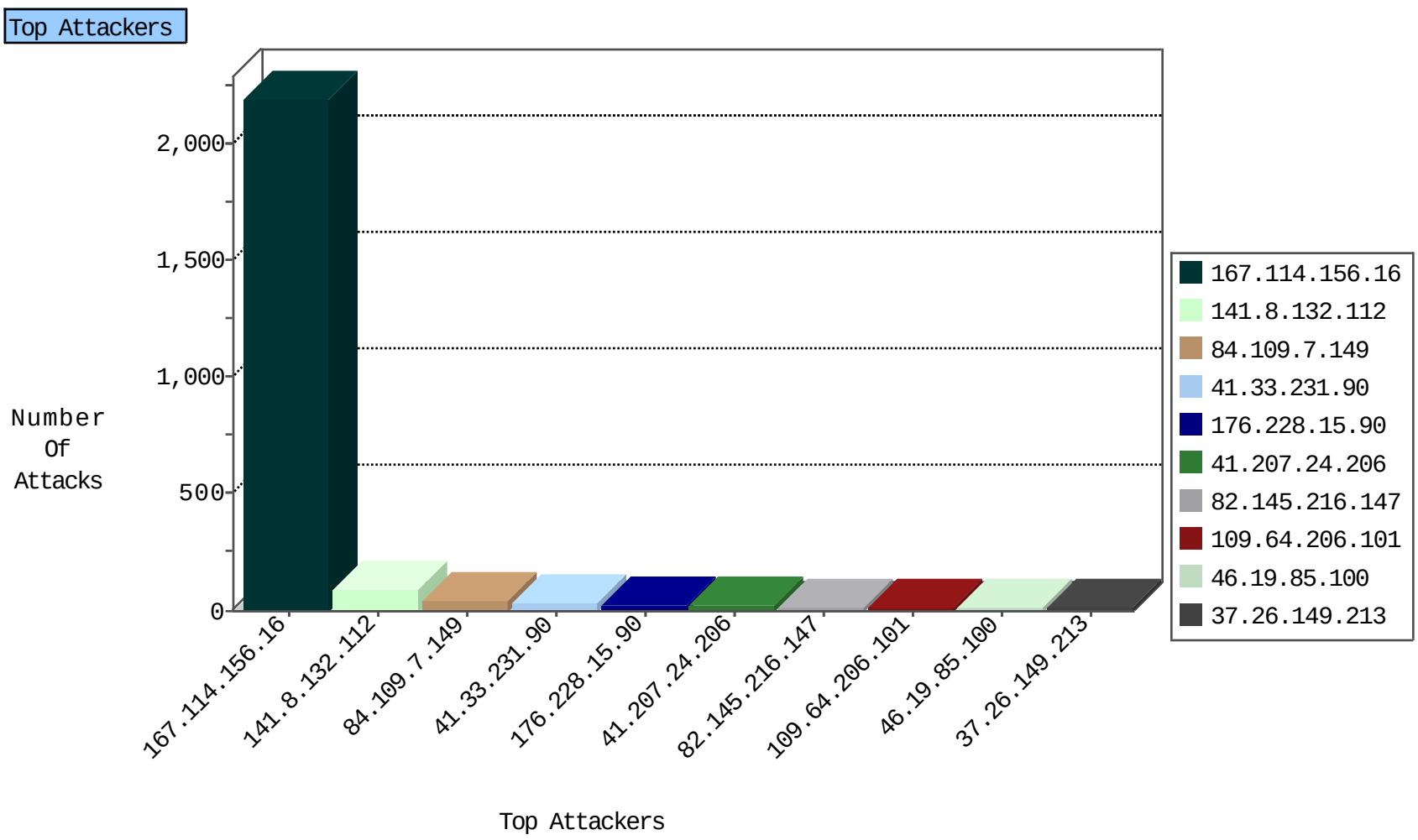
01-22-2016-13:04:09 to 01-22-2016-14:04:09

IDF Under Attack Daily Report





01-22-2016-13:04:09 to 01-22-2016-14:04:09

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	3110
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1380
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	64
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
85.130.251.227	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
221.176.148.150	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
221.176.148.150	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

01-22-2016-13:04:09 to 01-22-2016-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.236.51.169	United Kingdom	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
174.34.135.242	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1

01-22-2016-13:04:09 to 01-22-2016-14:04:09

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
212.106.77.23	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
212.179.227.181	147.237.8.45	Israel	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.76.176	Latvia	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
159.122.111.166	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
116.117.253.243	147.237.77.61	China	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-22-2016-13:04:09 to 01-22-2016-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
84.109.7.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
82.145.216.147	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
109.64.206.101	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
79.179.33.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.66.35.67	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.253.197.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.207.24.206	Cote D'Ivoire	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.27.105.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.160.240.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.110.144.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.109.112.150	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
84.94.164.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
37.46.39.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
149.78.239.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.161.55	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.239.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.122.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
158.69.215.7	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.121.80.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.130.139.253	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.16	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.41	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.198.151.37	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.161.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.207.24.206	Cote D'Ivoire	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.16	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
149.78.143.43	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.31.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.105.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-22-2016-13:04:09 to 01-22-2016-14:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.228.15.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.54.0.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.161.55	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
213.57.53.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
178.125.196.218	Belarus	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
80.246.136.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
79.183.151.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.183.151.112	Block	1
109.253.220.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gws_rd in www.aka.idf.il/main/home/default.aspx	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.130.241.76	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
41.207.216.181	Cote D'Ivoire	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
157.55.39.137	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
84.109.7.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.186.185.69	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
79.178.125.94	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.117.42.56	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
89.216.77.209		147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
37.26.146.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.130.241.76	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.183.151.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/injections/web of trust	Block	1
132.74.151.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
87.69.252.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.207.216.181	Cote D'Ivoire	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	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
84.109.165.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.197.165	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.178.125.94	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
46.120.229.174	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
93.172.153.167	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
37.26.149.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.147.200	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.130.241.76	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name !Ã©S[[#14]][[#3]]Â”+Ã®Ã‘Â¡Ã¯Â™Ã¦[[#15]]Ã?D[[#3]]Âª Â—Â™Â,AÂ€ÃµÃ˜Â›Â‰[[#22]]1[[#20]]Ã‡Â¬*[[#12]]_Ã‘ÃªÂ¯ÂµÂ™gÃžEÃ”Ã¦Ã•qÂŒÃ£Ã»zV;mÂŠJ[[#16]]sÂ¿\ÃžJBBÃ¬Â‰@-Ã“ ha~M<Â…Ã»Ã£ÂŒ[[#25]]Ã®'St[[#7]][[#19]]Â¼Â,\Â¾Ã¥Â¤Âš"mVÃ¨Â½Ã»Â“Â‹[[#2]]Â^\Â±ÃžÂ§VÂ‘Â„Ã¼(Âœ[[#29]][[#28]]GÂ¥ÃŸXlÃ¥LÂƒÃ'+#eÂ²Â¬Ã‹}ÂŽLÂ^~[[[#31]]hÃ²sÃ¡Ã½Â§Ã—Ã¡IÂ¸ [[#5]]{[[#6]]NQÂª[[#2]]ÂšÂ¹.Âµ^[[#17]]Ãš[[#3]]a+Ã°38[[#27]]Â‰Ã¼ÂŸZÃ°qÃ¶Â¬nÃ…Ã³z*Ã™ÃŠÂ¬Ã“Ã– Ã¹Ã®Ã¶[[#25]]Â-Ã·Ã'V#ÂªWÃ¹[[#5]]Ã?(J[[#21]]ÂºÂ?[[#14]]Ã”/J[ÃŸÃ»+C0Â	Block	1
80.246.130.21	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
149.78.143.43	Israel	147.237.77.234	halag.idf.il	Suspicious Response Code	Block	1
109.67.137.226	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.125.99.228	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
89.138.172.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.190	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.29.6.190	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
173.236.172.8	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
85.130.241.76	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
109.253.199.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.190.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-22-2016-13:04:09 to 01-22-2016-14:04:09