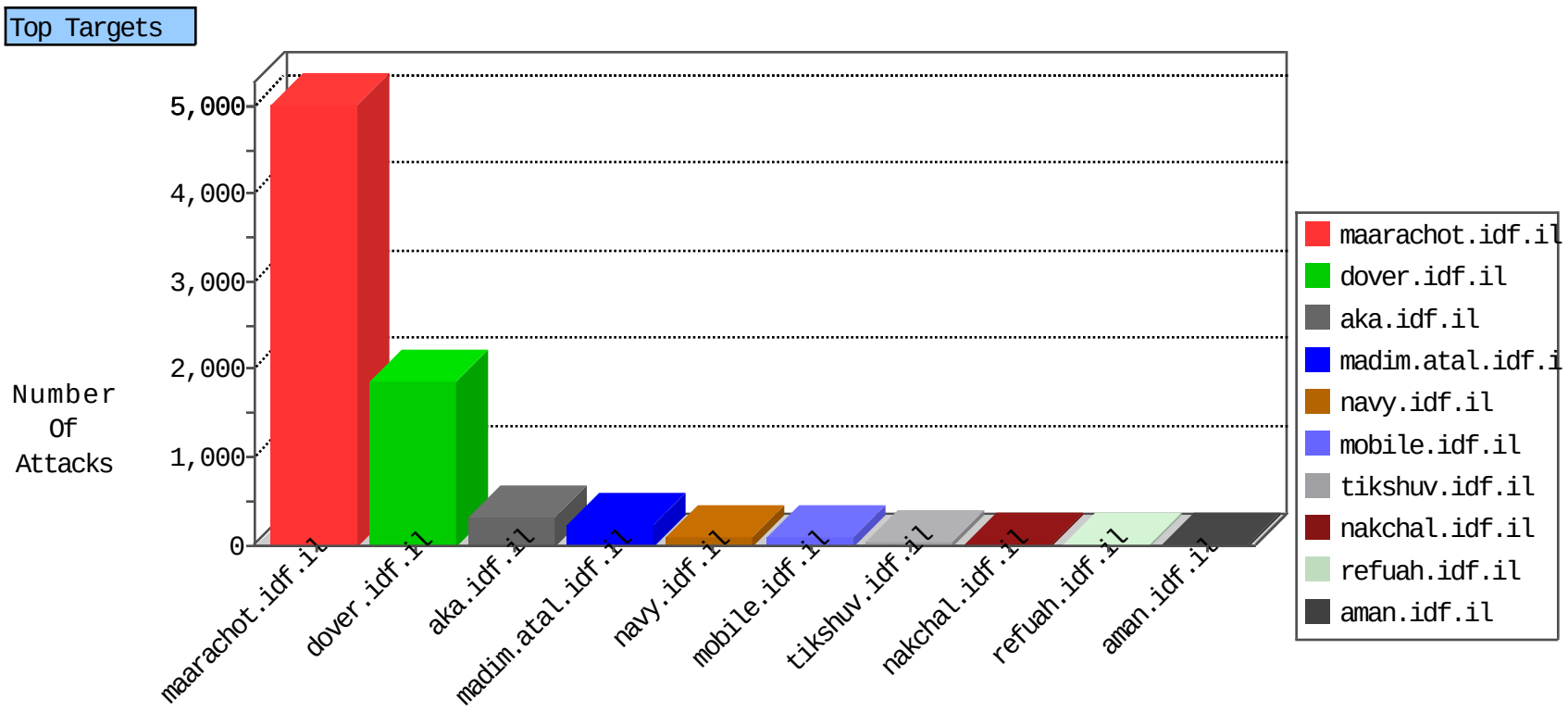
01-10-2016-21:04:00 to 01-10-2016-22:04:00

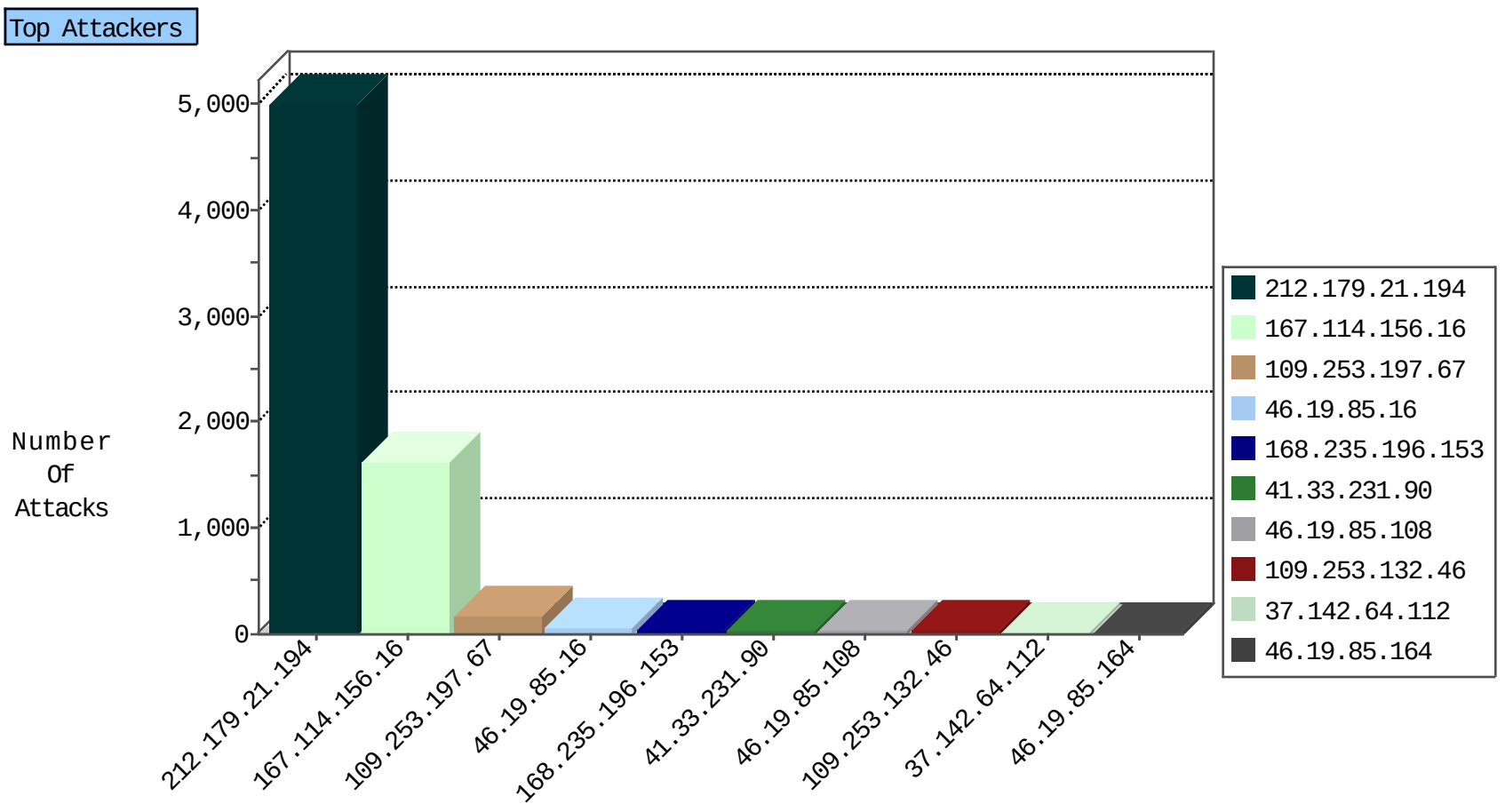
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-10-2016-21:04:00 to 01-10-2016-22:04:00

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	3082
168.235.196.153	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
168.235.196.153	United States	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
89.248.160.138	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

01-10-2016-21:04:00 to 01-10-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.218.71.214	Kazakstan	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	1

01-10-2016-21:04:00 to 01-10-2016-22:04:00

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
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.163	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.108.32.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.175.85.145	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.105.134.220	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.31.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.158.247.64	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -sS window 2048	1
37.142.64.112	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
158.255.6.220	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
125.234.108.75	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
109.64.1.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.150.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.158.247.64	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -sS window 4096	1
177.158.247.64	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -f -sS	1
146.185.250.2	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
125.234.108.75	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
125.234.108.75	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -f -sS	1
221.194.254.184	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-10-2016-21:04:00 to 01-10-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5010
168.235.196.153	United States	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
109.253.132.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.9.173	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
80.246.137.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.212.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.147.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
37.142.68.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.65.140.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.164	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.109.193.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.125.93.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.53.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.38.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.125.151	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.136.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.8.204.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.121.73.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.172.185.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.56	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.213	Israel	147.237.76.86	navy.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
31.168.164.198	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.182.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.171.41	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.3.147.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.145.17.68	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.15.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.197.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	121
46.19.85.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
109.253.197.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
149.78.41.188	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.108	Block	12
79.180.133.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.212.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.197.67	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.197.67	Block	4
46.121.211.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.65.140.166	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
79.178.136.212	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
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	2
188.143.232.21	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
217.197.39.28	Czech Republic	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.idf.il/1038-en/dover.aspx	Block	2
84.94.182.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.0.197	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
37.142.64.112	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.54.38.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/gallery	Block	1
37.142.64.112	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 37.142.64.112	Block	1
37.142.64.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#27]]+Â″Â²[[#30]]JÃ?$Â½f bÃŸlUÃ?9 Â·~[[#11]]lÃ†k]eÃ¤Â«JÃ‡Â«p$Â—Ãœ>Ã´[[#4]]$PÂ¯MÂŒ Ã®QÃ?Â? BÃ¶V[[#20]]K HaÃ±"#qÂ§Ã¢Ã¬3eHÃ¯Â?Â¶Ã…Â‡Ã¨ÂŸ^Ã— `BÂ?Â¹dÂ?[[#6]]UÂƒÂ‡5\Â†%•Ã±Ã„Ã°[[#2]]Â‹Ã˜Â‹Ãœ#pÃ¡ [[#24]]Ã?Ã‰Ã—Â-s=Â¤ÂœÂ†ÂµGÃ?e	Block	1
87.68.244.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.90.69.23	United States	147.237.76.86	navy.idf.il	Directory Traversal - 16	Block	1
185.32.179.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.51.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.137.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.152	Block	1
37.142.64.112	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.253.142.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
199.30.24.182	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/smalim.aspx?catid=58651	Block	1
37.142.64.112	Israel	147.237.72.166	aka.idf.il	Malformed URL [[#4]][[#7]]Ã— Ö¶,Â½a<])[[#18]]Ã»0×ª$v6×°Â rl[[#5]]3[[#23]]×¤^.ÂœbÂ£ÃœÖ²×, Â¾Ã»Ãš-c×¥Âžâ„¢â„¢â€¹v3×?[[#0]]Â¿y×¤â€”Ãžk~×¥tidÂ®[[#7]]×?Ö³	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.121.140.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.55	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
37.142.64.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.89.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.157.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.110.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.43	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
37.142.64.112	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.142.64.112 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.160.147.213	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.160.147.213	Block	1