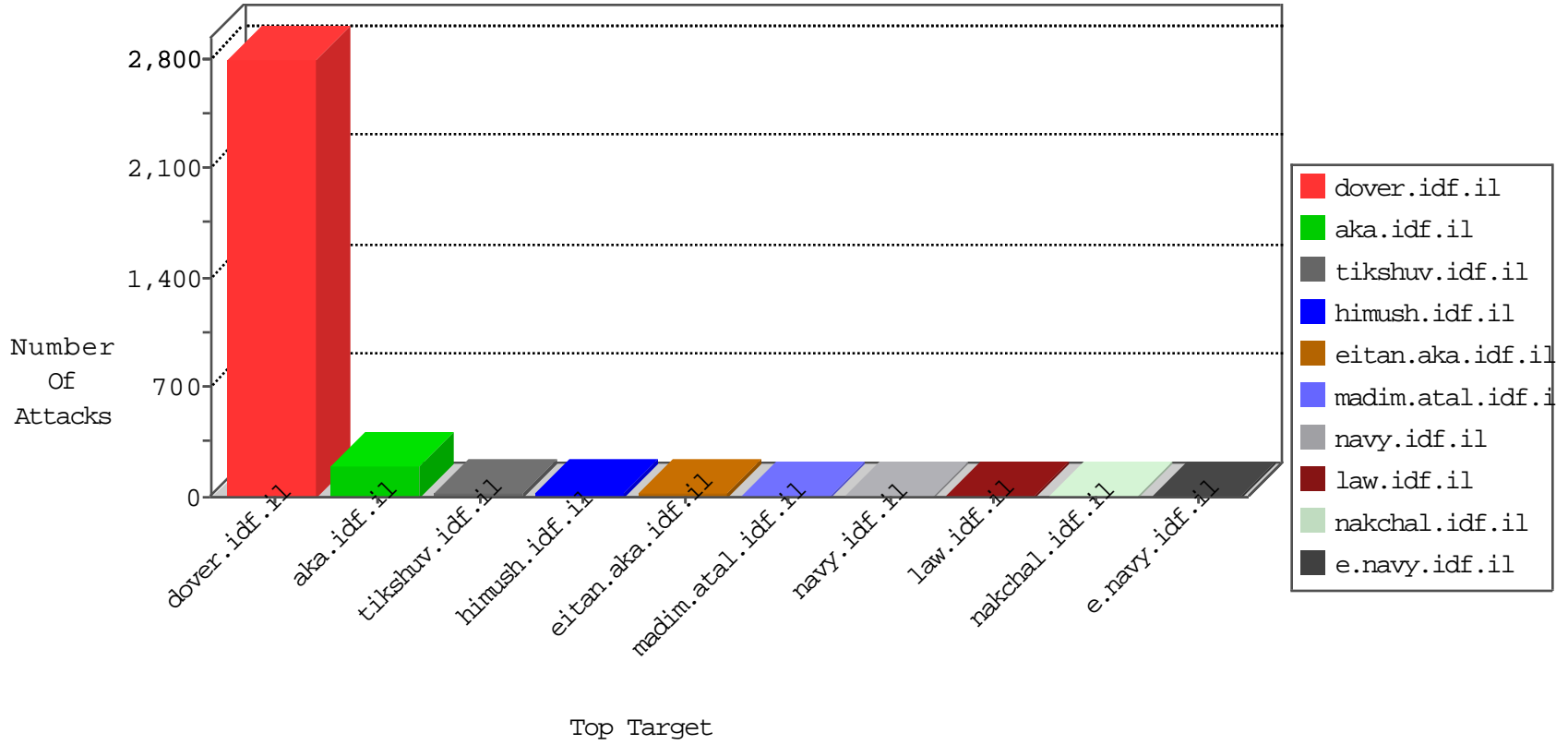


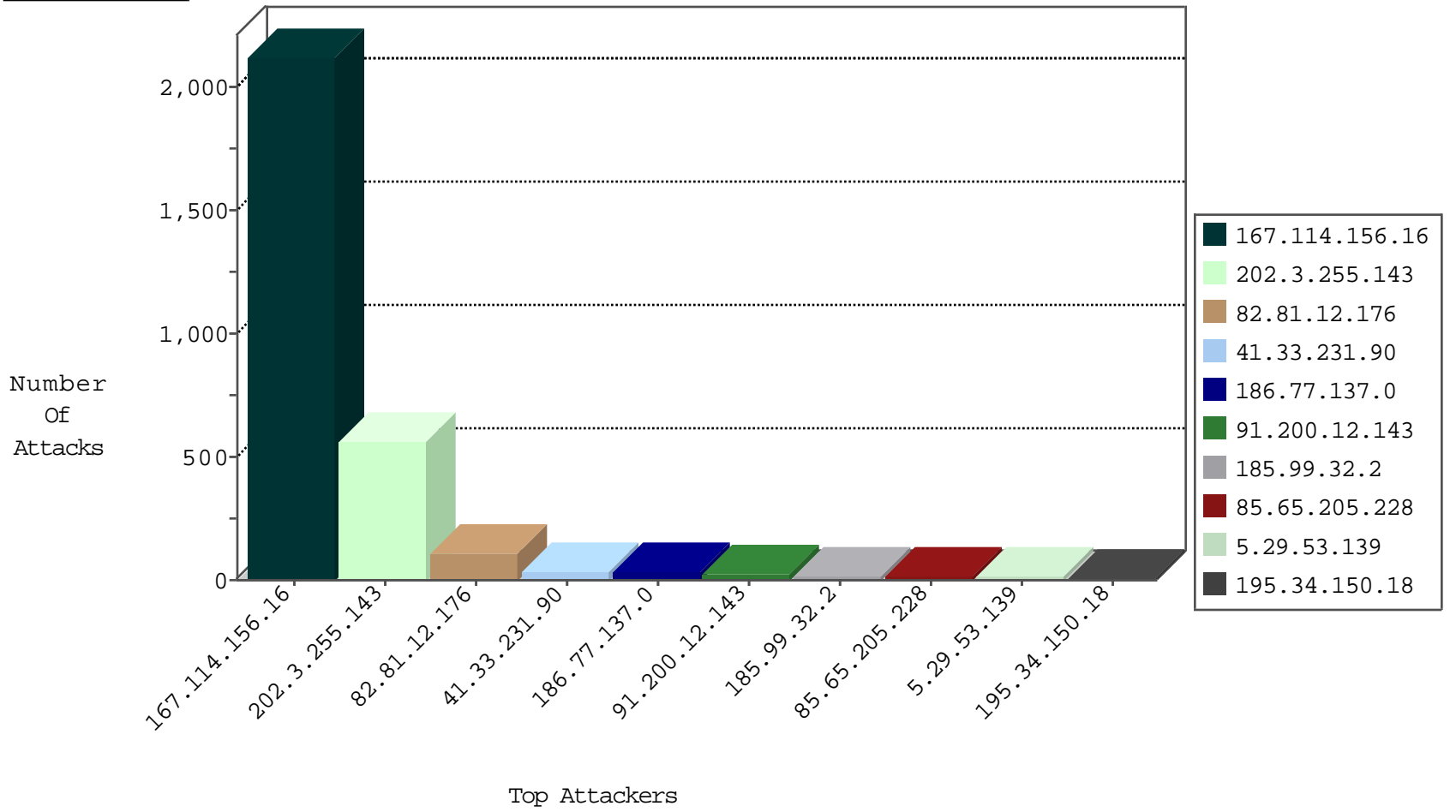
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## 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	3006
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
5.189.146.244	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.248.167.162	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
5.189.146.244	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
194.90.129.41	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.248.167.162	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
5.189.146.244	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
89.248.167.162	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
5.189.146.244	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
89.248.167.162	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.53.139	Israel	147.237.0.34	tikshuv.idf.	C212: HTTP: prefix 1.01 in the URL	Block	11
136.243.103.157	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
199.30.24.91	United States	147.237.0.34	tikshuv.idf.	C212: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.185	United States	147.237.0.34	tikshuv.idf.	C212: HTTP: prefix 1.01 in the URL	Block	2
138.128.20.250	United States	147.237.77.233	atal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	doover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	525
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
93.174.93.181	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.80.155.211	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.174.93.181	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.76	147.237.72.167	United States	ishurim.aka.idf.il	ET DROP Dshield Block Listed Source	1
91.218.246.103	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.66.250.189	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.138.70.153	147.237.77.216	Sweden	dover.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.138.70.153	147.237.76.199	Sweden	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
79.138.70.153	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
115.182.249.11	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
219.127.5.173	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
70.91.101.173	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.179.227.181	147.237.77.121	Israel	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.93.181	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.227.181	147.237.77.121	Israel	e.navy.idf.il	ET SCAN NMAP -f -sS	1
39.68.85.159	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.181	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.218.246.103	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.234.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.138.70.153	147.237.76.202	Sweden	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.138.70.153	147.237.76.177	Sweden	noore.idf.il	ET SCAN Potential SSH Scan	1
120.62.6.124	147.237.0.33	India	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.138.70.153	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
219.127.5.173	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
111.39.110.6	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.138.70.153	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.181	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.227.181	147.237.77.121	Israel	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
50.18.225.195	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
186.77.137.0	Nicaragua	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
85.65.205.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.99.32.2		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
186.77.137.0	Nicaragua	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
40.77.167.105	United States	147.237.76.200	eitan.aka.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
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
157.55.39.197	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.99.32.2		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.108	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.250.182.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.119.121.146	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
2.54.36.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.129.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.88	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.189	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.254.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.99.32.2		147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.81	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.18.225.195	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.94	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.179	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.115	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
73.152.99.234	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.38	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.70	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.109.51.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
50.177.204.2	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.216	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.180	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.120	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.105.28.1	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
212.124.109.166	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
75.137.216.67	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.120.122.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.40	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	12
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.143	Block	11
109.253.221.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
138.134.102.16	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/size338x0/1668.jpg	Block	2
79.183.206.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/index.php	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
46.19.86.89	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/	Block	1
128.70.102.149	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation lang in www.law.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
79.182.145.43	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.207	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/gyus/general.aspx	Block	1
176.13.2.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
103.41.63.11		147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.66.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
185.32.179.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/hilulanebisamuel.aspx	Block	1
141.212.122.177	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
198.20.69.76	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
40.77.167.105	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/kishur/	Block	1
128.70.102.149	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation DocID in www.law.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
157.55.39.197	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/62048	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
46.19.86.42	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
128.70.102.149	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation folderid in www.law.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/	Block	1
157.55.39.242	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1