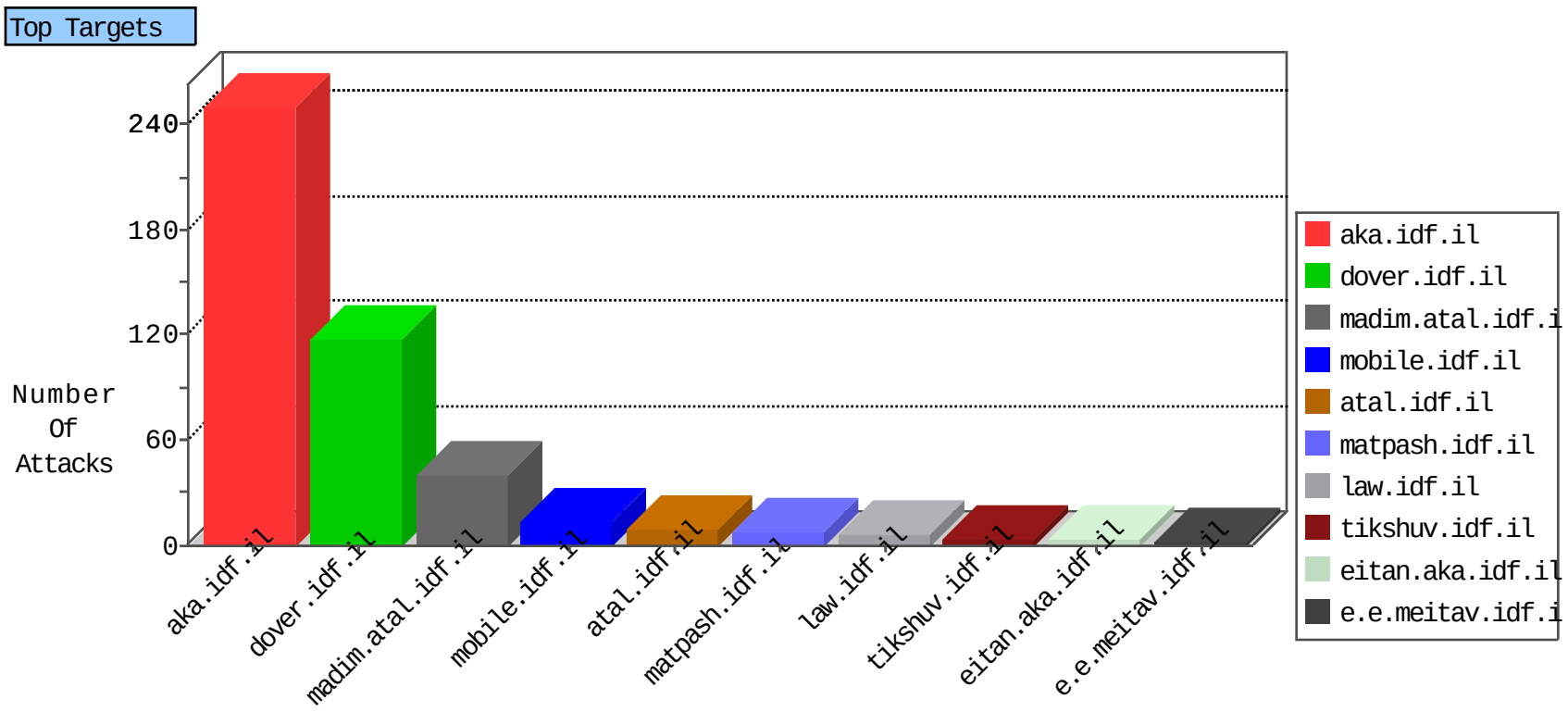
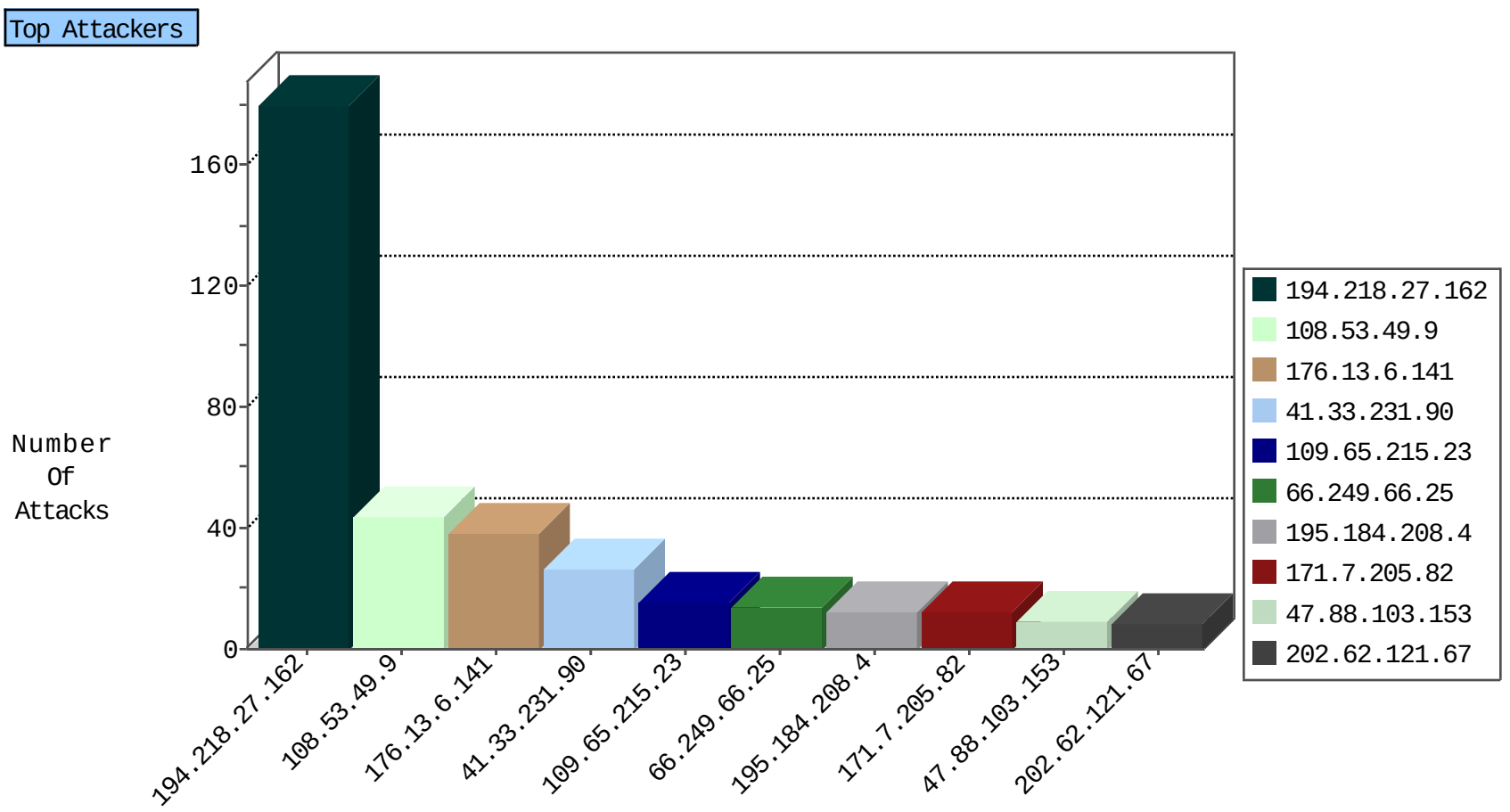
03-02-2016-01:12:34 to 03-02-2016-02:12:34

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-02-2016-01:12:34 to 03-02-2016-02:12:34

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
122.236.118.216	China	147.237.77.176	matpash.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
47.88.103.153	Canada	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
182.207.134.232	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
47.88.103.153	Canada	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
47.88.103.153	Canada	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

03-02-2016-01:12:34 to 03-02-2016-02:12:34

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.107	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.10	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.20	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.51	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.91	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-02-2016-01:12:34 to 03-02-2016-02:12:34

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
36.37.226.117	147.237.76.39	Cambodia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.254.212	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
118.165.65.161	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	1
82.127.122.114	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.210.69.71	147.237.72.217	France	e.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.116.147	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
118.165.65.161	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
118.165.65.161	147.237.76.176	Taiwan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
60.18.162.244	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1

03-02-2016-01:12:34 to 03-02-2016-02:12:34

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
108.53.49.9	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
109.65.215.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.117.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.50.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
171.7.205.82	Thailand	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
171.7.205.82	Thailand	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
171.7.205.82	Thailand	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
79.181.96.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.18.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
202.62.121.67	Fiji	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.54.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.9.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
202.62.121.67	Fiji	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
202.62.121.67	Fiji	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.135.174	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
37.26.147.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
40.77.167.42	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
149.78.75.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
47.88.103.153	Canada	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.116.147	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.79.130.52	United Kingdom	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
2.52.20.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.199	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.214.27	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
47.88.103.153	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.116.147	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.142.64.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.200	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.90.246.233	United Kingdom	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
47.88.103.153	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.214.27	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
47.88.103.153	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.64.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.206	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.175.219	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
47.88.103.153	Canada	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
202.62.121.67	Fiji	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.193	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.182.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.207	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
47.88.103.153	Canada	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

03-02-2016-01:12:34 to 03-02-2016-02:12:34

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	14
195.184.208.4	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
195.184.208.4	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.184.208.4	Block	5
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	2
66.249.78.158	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
195.184.208.4	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23092-he/dover.aspx	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
213.57.218.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/images/tofes106	Block	1
52.25.116.236	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/l/4574l.pdf.accessed	Block	1
104.236.244.32		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-he/tikshuv.aspxshared/usercontrols/headerupper/	Block	1
109.67.236.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.66.39	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.83.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.53	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1498-he/atal.aspx об этом же в своих исследованиях говорит бригадный генерал раутио	Block	1
66.249.78.93	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/927-he/אגף הטכנולוגיה והלוגיס טיקה.aspx	Block	1

03-02-2016-01:12:34 to 03-02-2016-02:12:34