MHN Server (/ui/dashboard/)

Attack Stats

Attacks in the last 24 hours:

1,835 (/ui/attacks/?hours_ago=24)

TOP 5 Attacker IPs:

1. 🇺🇸 **63.232.207.51 (1,011 attacks) (/ui/attacks/?source_ip=63.232.207.51)**
2. 🇷🇺 **77.72.82.101 (74 attacks) (/ui/attacks/?source_ip=77.72.82.101)**
3. 🇨🇳 **111.121.193.209 (33 attacks) (/ui/attacks/?source_ip=111.121.193.209)**
4. 🇨🇳 **123.249.79.250 (32 attacks) (/ui/attacks/?source_ip=123.249.79.250)**
5. 🇷🇺 **5.188.9.25 (30 attacks) (/ui/attacks/?source_ip=5.188.9.25)**

TOP 5 Attacked ports:

1. **3306 (77 times) (/ui/attacks/?destination_port=3306)**
2. **23 (68 times) (/ui/attacks/?destination_port=23)**
3. **445 (45 times) (/ui/attacks/?destination_port=445)**
4. **5060 (22 times) (/ui/attacks/?destination_port=5060)**
5. **8545 (17 times) (/ui/attacks/?destination_port=8545)**

TOP 5 Honey Pots:

1. **dionaea (1,589 attacks) (/ui/attacks/?honeypot=dionaea)**
2. **snort (246 attacks) (/ui/attacks/?honeypot=snort)**

TOP 5 Sensors:

1. **mhn-honeypot-1 (1,589 attacks) (/ui/attacks/?identifier=ef676776-46bd-11e8-9906-42010a800002)**
2. **mhn-honeypot-3 (153 attacks) (/ui/attacks/?identifier=209de16e-46c6-11e8-9906-42010a800002)**
3. **mhn-honeypot-2 (93 attacks) (/ui/attacks/?identifier=876846de-46d8-11e8-9906-42010a800002)**

TOP 5 Attacks Signatures:

1. **ET DROP Dshield Block Listed Source group 1 (93 times) (/ui/feeds/?payload=ET+DROP+Dshield+Block+Listed+Source+group+1&channel=snort.alerts)**
2. **ET CINS Active Threat Intelligence Poor Reputation IP TCP group 4 (33 times) (/ui/feeds/?payload=ET+CINS+Active+Threat+Intelligence+Poor+Reputation+IP+TCP+group+4&channel=snort.alerts)**
3. **ET CINS Active Threat Intelligence Poor Reputation IP TCP group 63 (21 times) (/ui/feeds/?payload=ET+CINS+Active+Threat+Intelligence+Poor+Reputation+IP+TCP+group+63&channel=snort.alerts)**
4. **ET SCAN Sipvicious User-Agent Detected (friendly-scanner) (9 times) (/ui/feeds/?payload=ET+SCAN+Sipvicious+User-Agent+Detected+%28friendly-scanner%29&channel=snort.alerts)**
5. **ET CINS Active Threat Intelligence Poor Reputation IP TCP group 28 (9 times) (/ui/feeds/?payload=ET+CINS+Active+Threat+Intelligence+Poor+Reputation+IP+TCP+group+28&channel=snort.alerts)**

Modern Honeynet Framework is an open source project by: THREATSTREAM (http://threatstream.com)