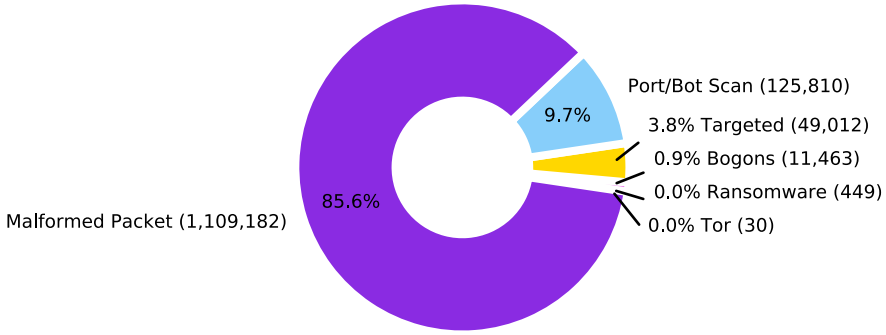
Reporting Period: 08/01/2019 - 08/31/2019

Dear Valued Customer,

This month, your HakTrap firewall (customer network) inspected 1.62 TB of traffic.

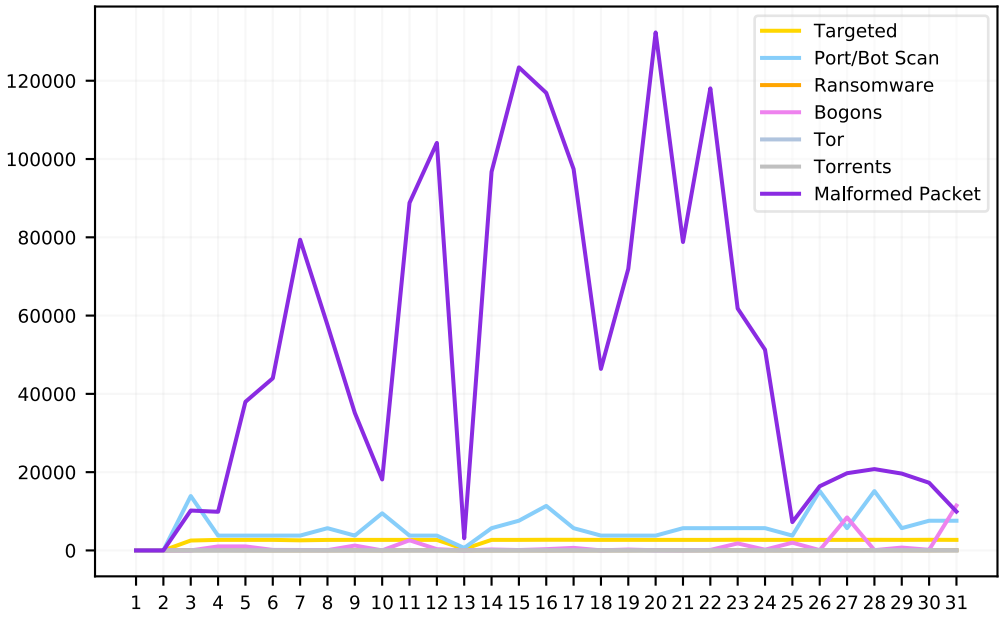


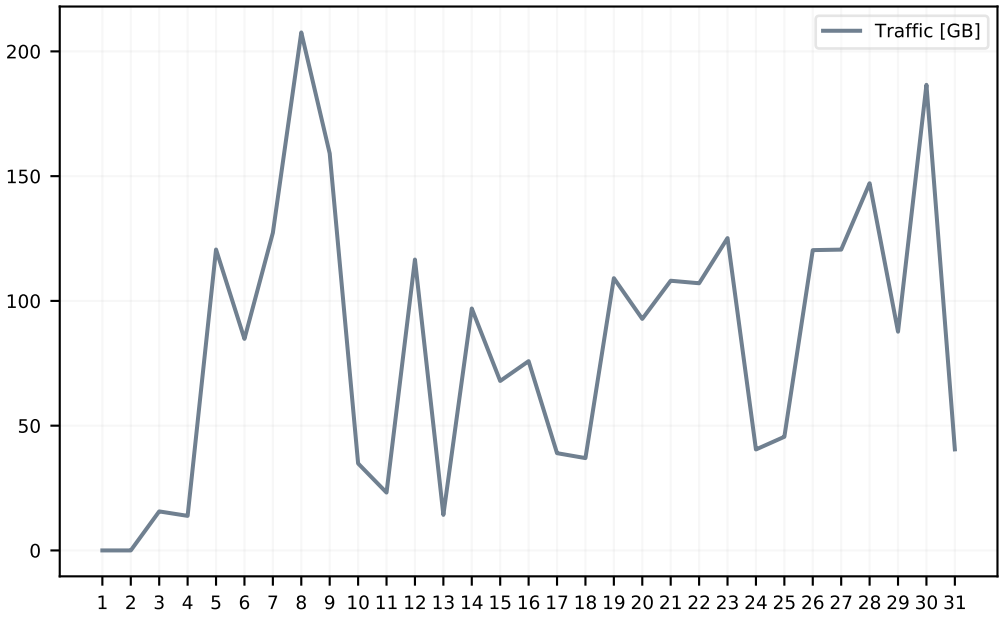
Attack Type	Frequency
DDoS Attack	0
Targeted Attack	49,012
Port/Bot Scan Attempt	125,810
Spam/Phishing Attempt	0
Ransomware Blocked	449
Bogons	11,463
Tor (Dark Web)	30
Torrents	0
Crypto Jacking	0
Management Attack	0
DNS Relay Attack	0
Malformed Packet Drops	1,109,182

Axiom Holdings LV, LLC
10100 W. Charleston Blvd. Suite 130
Las Vegas, NV 89135

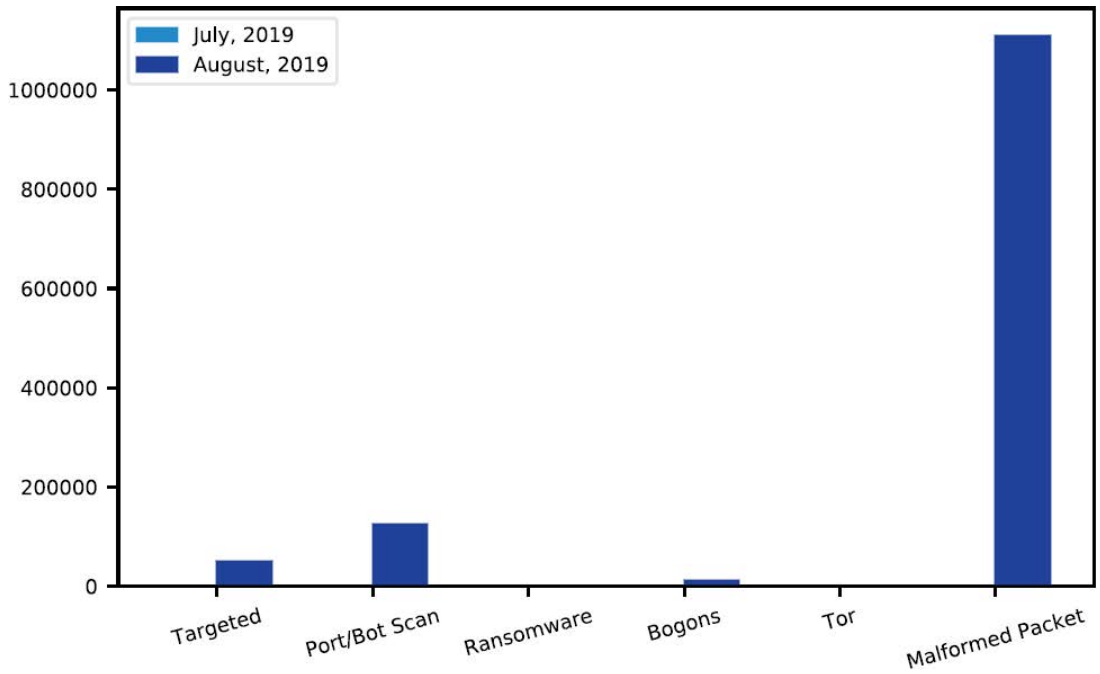
1-800-519-5070
Info@HakTrap.com
www.HakTrap.com

Monthly Attacks and Total Traffic





Last Month vs Current Month



DDoS – Distributed Denial of Service. This is when your firewall sees a traffic flood and blocks suspected traffic. Traffic floods occur more often than you think. Because they often come in low volumes, you may or may not see the effects on your network. Hackers use these as "probes" to test networks and infrastructure for vulnerabilities. The HakTrap firewall is designed to absorb these and not reply. This leaves the attacker no information helping your business stay invisible.

Targeted Attack – This is when someone puts in your IP address for a specific attack. This could be many different vectors such as SQL Injection attempt, Cross Site Scripting attempt or a vulnerability scanner. This generally happens with someone has scanned and found your IP with the Bot Scan or they have found your IP from and email or web response. In any event, the HakTrap firewall will block these attacks. The HakTrap firewall keeps track of these offenders and will block them after several attempts.

Ransomware – This is when Ransomware has been activated on your network and is reaching out for the encryption key exchange. Ransomware malware makes hundreds, if not thousands of calls out of the business and this number represents the number of packets blocked. This is targeting a specific protocol that Ransomware must have to activate.

Port / Bot Scan – This is when servers or bots on the internet are scanning for open ports or known devices on IP ranges. Each day, thousands of servers (both legitimate and illegitimate) are scanning

the internet doing an inventory or discovery. Hackers use this information to proceed with targeted attacks. The HakTrap firewall absorbs these packets and makes your business invisible to scanners thereby keeping you off their radars.

Spam / Phishing Schemes – This is when the HakTrap firewall identifies known spam or phishing schemes that are identified by the IANA (Internet Assigned Numbers Authority), the Internet Storm Center or other highly respected cybersecurity sharing sites. The HakTrap firewall is able to scan all traffic coming into and out of the business and is able to identify spam / phishing schemes that other stateful firewalls just can't.

Bogons - Bogons are bogus IP addresses that have no legitimate use. They are usually the result of accidental misconfiguration but sometimes can be due to malicious configuration and therefore are blocked.

Tor (DarkWeb) - The dark web is the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific software, configurations or authorization to access. communication between darknet users is highly encrypted allowing users to talk, blog, and share files confidentially, for this reason, the dark web is also used by cyber-criminals to conduct their trade.

Torrent - Torrenting is a peer-to-peer technology that doesn't have a single point of failure but its most common use it to share copyrighted material (movies, music, software) which is often infected with malicious content.

Crypto Jacking - CryptoJacking is a form of cyber-attack in which a hacker hijacks a target's processing power in order to mine cryptocurrency on the hacker's behalf. This can be done through a malicious ad on a website that runs an attack through a vulnerable web browser or website. The objective of the attack is to use your processing power to mine crypto currency for the attacker, thus making them money at the expense of your resources such as electricity and CPU Processing power.

Management Attacks - Devices are strictly managed via certain protocols or methods and will only permit a handful of trusted IPs from connecting via these methods. If an attacker or port scanner hits on the ports that would otherwise be for management, these are tracked to report that an attempt to access the device was made and was blocked.

Malformed Packet Drops - Packets are invalid or malformed if they appear to be marked as established in the TCP header of a packet, but the firewall has never seen the TCP three-way handshake before this transmission. Example: if an attacker is spoofing IP traffic, then they are sending data regardless of having a proper three-way handshake. The firewall looks at those packets and is able to determine by connection tracking, I have never seen the handshake, so, we assume those packets are invalid and should be dropped.

DNS Relay Attack - DNS or Domain Naming System is how the internet can take a website such as www.example.com and resolve it to an IP address such as 1.2.3.4 so that computers, routers and servers can speak to each other. Through the use of port scanning, or DNS reflection attacks, an

attacker can employ numerous nodes to try and abuse the DNS system and take down your device by overwhelming it with queries. Each hit is quantified as a single attempt to try and use your firewall as a DNS source. There is no reason why the internet should ever need to utilize your firewall as a source for DNS resolution and so we block these attacks.

Thank you for being part of the Axiom Holdings LV, LLC family of protected businesses.
If you have any questions, please feel free to contact us at Support@HakTrap.com or (800) 519-5070. #FightBackwithHakTrap

@HakTrap

/HakTrap

@HakTrap

/company/HakTrap/