BLOCK EVERY THREAT.

Bill Franklin- VP Engineering and Business Development
LAUSD

Ransomware Attack

Who was the Threat Actor?

Vice Society

Cyber attackers remain #1 global threat to organizations
Cyber Crime Costs

$10.5 Trillion – 2025

https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
Story of a Hacker
Story of a **Hacker**

**Conti Ransomware**
Aggressive ransomware operation
Saint Petersburg, Russia

**Vice Society**
Russian cyber espionage group
Russia

**Chinese APT**
Chinese Cyber Espionage Group
China

- **Product(s)**
- **Marketing**
- **Finance**
Story of a Hacker

Hacker Inc

Distribution

Customers

Customer 1
- EDR
- MFA
- Backup

Customer 2
- M/EDR
- MFA
- DRaaS

Customer 3
- SSO/MFA
- EDR/MDR
- Backup/IBU

Vehicle: IP address(es)
- Russia
- Netherlands
- Brazil
- USA
- AWS

Internet

50+ Cyber Intelligence Feeds

Access to tens of millions of cyber intelligence indicators

Hacker: Conti Ransomware, Vice Society, Chinese APT

50+ Cyber Intelligence Feeds

50+ Cyber Intelligence Feeds

50+ Cyber Intelligence Feeds

50+ Cyber Intelligence Feeds

50+ Cyber Intelligence Feeds

Open Door

Open Door
Threat Blocking ‘as a Service’ (TBaaS)
Technical Architecture Overview

50+ Cyber Intelligence Feeds

Access to tens of millions of cyber intelligence indicators

DC/HQ
REMOTE OFFICE
CLOUD
Architecture – Customer Premise

Protected Devices Inside Your Network

SIEM & Router – Managed Path Switching

ISP 1

ISP 2

THREAT BLOCKR®

THREAT BLOCKR®
Want proof we can make you more secure?

Let’s do a rapid analysis of your security logs to see how ThreatBlockr would have blocked threats that your security stack missed.
This report shows the number of known-bad connections and IP addresses allowed through your firewalls **that would have been blocked by ThreatBlockr**. In today's threat landscape, it only takes one malicious connection coming into or leaving your network to cause a cyber attack.

### Assessment Details (continued)

**Known Bad traffic that was allowed by your firewall came Inbound from these Countries**
- Australia, Belgium, Belize, Brazil, Bulgaria, Canada, France, Germany, Hong Kong, India, Japan, Lithuania, Netherlands, Pakistan, Panama, Poland, Romania, Russia, Turkey, United Kingdom, United States, Vietnam

**Known Bad traffic that was allowed by your firewall went Outbound to these Countries**
- Australia, Brazil, Canada, France, Germany, Hong Kong, India, Japan, Mexico, Netherlands, Poland, Singapore, South Africa, Spain, Taiwan, United Arab Emirates, United Kingdom, United States

**Known Threat categories** identified from Inbound traffic
- Botnet, Brute Force Password, Command and Control, DDOS, Endpoint Exploits, Fraudulent Activity, P2P Node, Proxy / VPN, Scanner, Spam, TOR / Anonymizer

**Known Threat categories** identified to Outbound traffic
- Command and Control, Endpoint Exploits, Fraudulent Activity, P2P Node, Proxy / VPN, Remote Access Server, Spam

Number of unique ASN's where known bad traffic was found
- Inbound: 40
- Outbound: 21
Results

INBOUND example: 162.243.131.15
  - This hails from the US, on ASN Digital Ocean .. a known bad-guy's playground
  - It is on the open source CINS Army list as well as on Webroot as an endpoint exploit generator with very high confidence
  - It seemed to target a NAT'ing IP (we believe this to be their Sophos firewall IP): 4.2.64.130, with both ICMP and UDP
  - These kinds of attack patterns (ICMP and UDP) have been known to be used in targeted ways for purposely attacking zero-day vulnerabilities in a variety of firewalls (that is not to say that is what is happening here, but neither can it be ruled out)
  - ThreatBlockr would have blocked this activity.

Example OUTBOUND IPs: 85.133.128.249, 185.252.31.66
  - Both of these are IRANIAN
  - (Interestingly enough, true *INBOUNDS* from Iran seem to be locked down and not happening, but *OUTBOUNDS* seem to NOT be fully locked down.)
  - 85.133.128.249 is on Webroot as a very high confidence malicious Proxy/VPN source
  - 185.252.31.66 is on Webroot as a very high confidence fraudulent activity source (which is often used as a catch-all for a variety of non-specific malicious activity). In fact, over the timeframe in question (Jan 18-19), the confidence score went UP.
  - Customer - IPs 192.52.233.236 and 192.52.233.237 were in contact with BOTH of these known malicious IPs.
  - Additionally, customer IP 128.170.60.99 was also in contact with 85.133.128.249 (but not 185.252.31.66.
  - ThreatBlockr would have blocked this activity (if so configured*) in all cases.
“...My network guys are happy that we put ThreatBlockr in place – **ThreatBlockr blocks 1.1B threats per month** that don’t hit the firewall resulting in firewall CPU & memory utilization efficiencies...”

Richard Timbol, CISO, Davis Polk & Wardwell LLP
Thank You

Questions?
Bill Franklin and Dan Velando

Dan Velando

Tier4 Advisors - Regional President

dan@tier4advisors.com

425-220-8193

Dan Velando | LinkedIn

threatblockr.com
ThreatBlockr is Layer Zero of an active defense strategy.

- Proactive
- Autonomous
- Agnostic
- Scale

We are the **only solution** that blocks every known threat from every path in your network.

**Block. Every. Threat.**