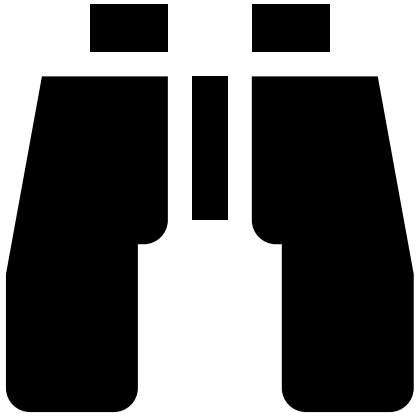
Welcome to NetTects LLC's Ninth Annual Technology Conference and Grand Spirits Tasting April 17th, 2024

Reducing the Enterprises' Attack Surface through Identifying Malicious Behaviors and Actors

Michael Weinstein
CTO, NetTects LLC

Agenda

- Benefits of Minimizing Attack Surface
- Passive Reconnaissance Sources
- Known Bad Actors
- Geo-Fencing
- Discovering Attackers
- Implementing Protections
- The Conclusion



Benefits of Minimizing Attack Surface

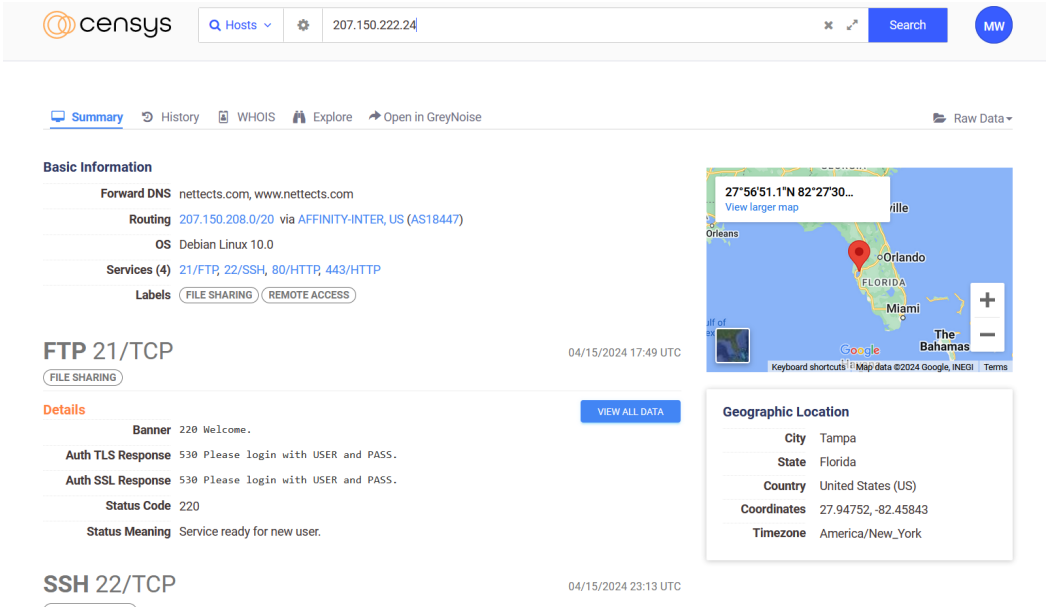
In addition to permitting traffic from the Internet only to legitimate services, there are additional benefits to using advanced features to limit the ANY or ALL sources typically associated with those firewall policies.

By using advanced forensics and features to limit access from known and discovered malicious actors, one can:

- Limit visibility of corporate resources on passive discovery sources
- Reduce logs in permit policies which can shorten time to investigate and respond to incidents
- Limit visibility of the service from “grey and black hat” scanners
- Protect the service from malicious actors

Passive Reconnaissance Sources

There are a number of web resources that enable a malicious actor to discover corporate services without scanning. Some services are free to use, some require a login or an account, and some are paid. These can include corporate entities and research groups. Examples include:



Shodan

Censys

Binary Edge

UK NSC Scanner

Onyphe

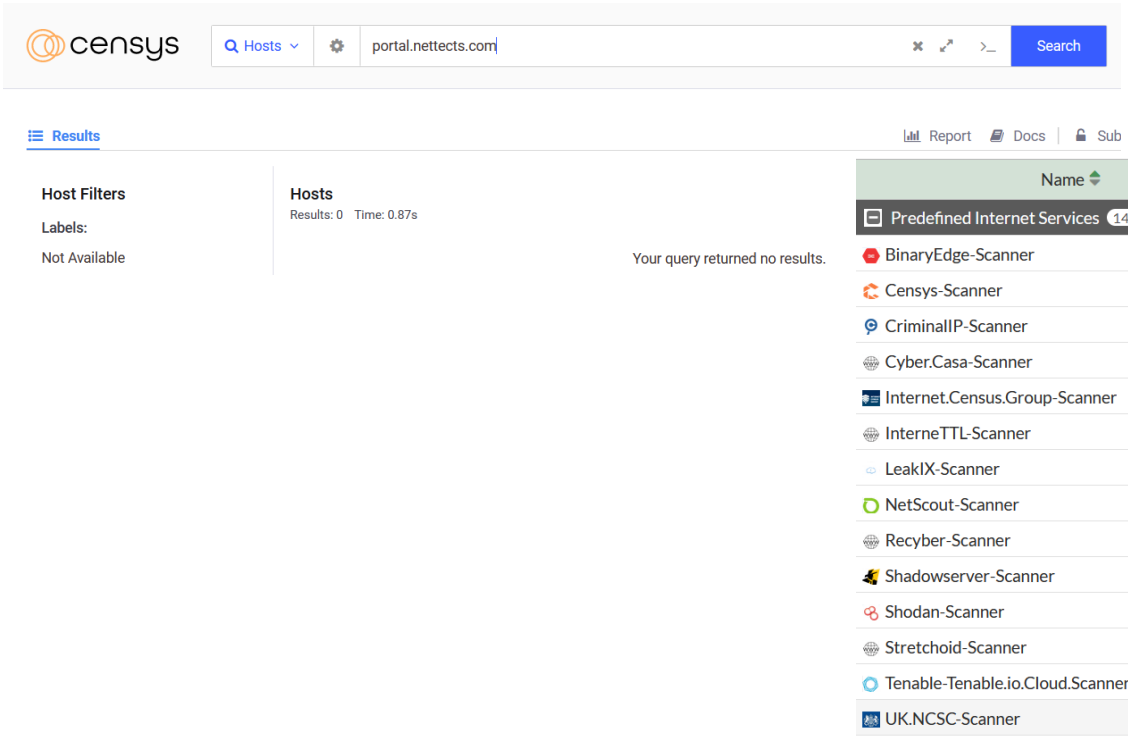
Sysnet at UCSD (ucsd.edu)

RWTH Aachen University

Cambridge Cybercrime Centre Internet scanner

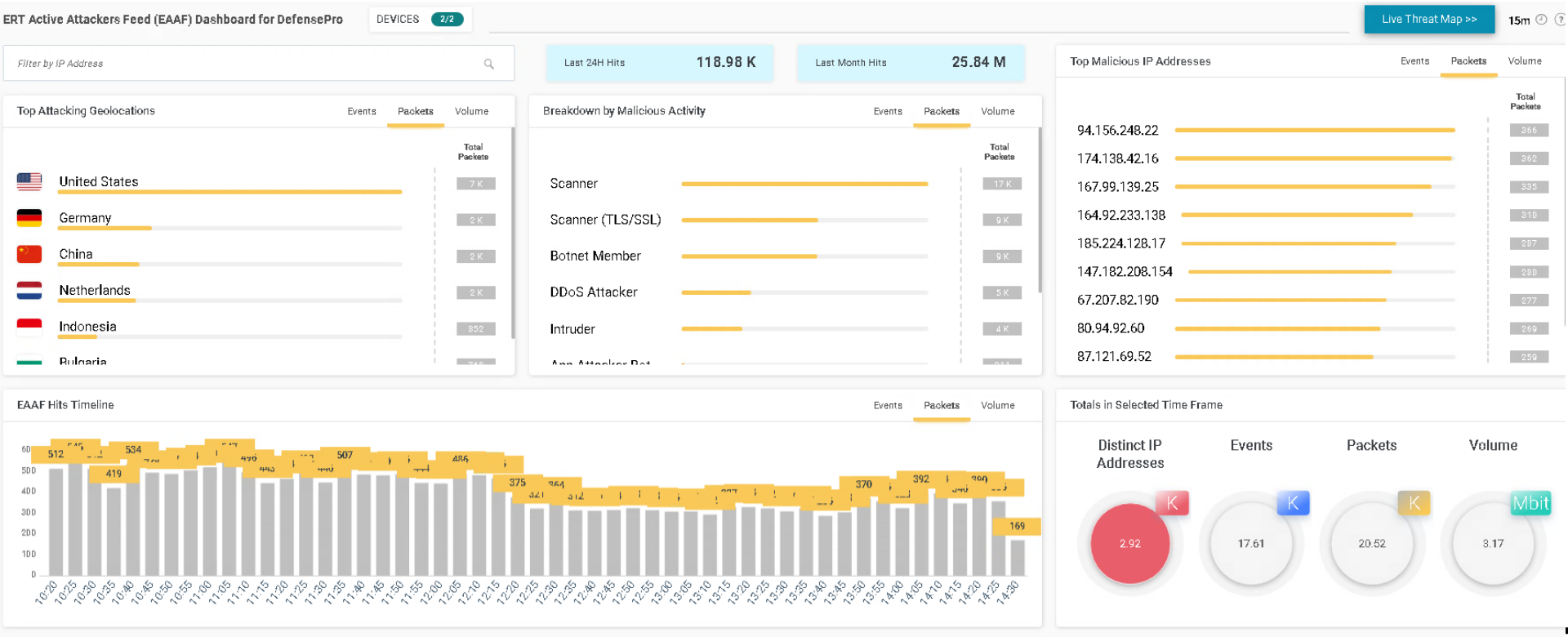
Passive Reconnaissance Sources

By applying rules to block these scanners, information about corporate resources will disappear from these sources. This can remove a tool from malicious actors, denying them the ability to start attacking resources directly based upon passive discovery. Some tools offer predefined services that make blocking these scanners simple.



Known Bad Actors

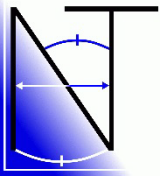
Known bad actors, based upon their source IP should also be blocked from accessing services. This can disrupt the attack and prevent further exploit attempts against publicly available resources. Using feeds from vendors is a great way to provide this protection – like Radware's EAAF



Known Bad Actors

IP reputation databases can provide a similar benefit under another name.

IP Reputation Database 9		
Blockchain-Crypto.Mining.Pool	Destination	248
Botnet-C&C.Server	Both	1,872
Malicious-Malicious.Server	Both	57,040
Phishing-Phishing.Server	Both	815
Proxy-Proxy.Server	Both	17,964
Spam-Spamming.Server	Both	4,972
Tor-Exit.Node	Both	912
Tor-Relay.Node	Both	5,637
VPN-Anonymous.VPN	Both	23,002



Known Bad Actors

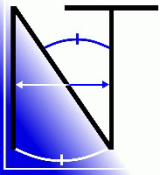
Discovered entities can also be added. For example, an organization known as IP Volume or IP Vol was discovered as scanning many organizations with whom NetTects has worked. Research revealed that all of the networks associated with this entity, by the Autonomous System Number (BGP), could be blocked.

This entity is registered in Seychelles and hosted in Netherlands.

```
[Querying whois.cymru.com]
[whois.cymru.com]
AS      | IP               | AS Name
202425  | 80.82.70.1       | INT-NETWORK, SC
```

```
inetnum:        80.82.70.0 - 80.82.70.255
netname:        NET-1-70
descr:          IPV NETBLOCK
country:        NL
geoloc:         52.370216 4.895168
org:            ORG-IVI1-RIPE
admin-c:        IVI24-RIPE
tech-c:         IVI24-RIPE
status:         ASSIGNED PA
mnt-by:         IPV
mnt-lower:      IPV
mnt-routes:     IPV
created:        2016-01-23T22:53:56Z
last-modified:  2019-02-01T18:29:11Z
source:         RIPE

organisation:   ORG-IVI1-RIPE
org-name:       IP Volume inc
country:        SC
org-type:       OTHER
address:        Seychelles
abuse-c:        IVNO1-RIPE
mnt-ref:        IPV
mnt-by:         IPV
created:        2018-05-14T11:46:50Z
last-modified:  2023-09-08T14:13:20Z
source:         RIPE # Filtered
```



Known Bad Actors

This entity has a history of being a bad actor, with illegal content being hosted on its servers as well as participating in botnets

WIKIPEDIA
De vrije encyclopedie

Search Wikipedia | To search | create

IP Volume

Add languages

Contents hide

Top

History

Article | Discussion | Read | To process | Edit source text | View history | Tools

From Wikipedia, the free encyclopedia

IP Volume (also known as **Ecatel** , **Quasi Networks** and **Novogara**) is a hosting company known as *a bulletproof hoster* . The company is suspected of tolerating child pornography , copyright violations and computer crime . Although today registered in the Seychelles , the company is believed to operate from the Netherlands.

History [edit | edit source text]

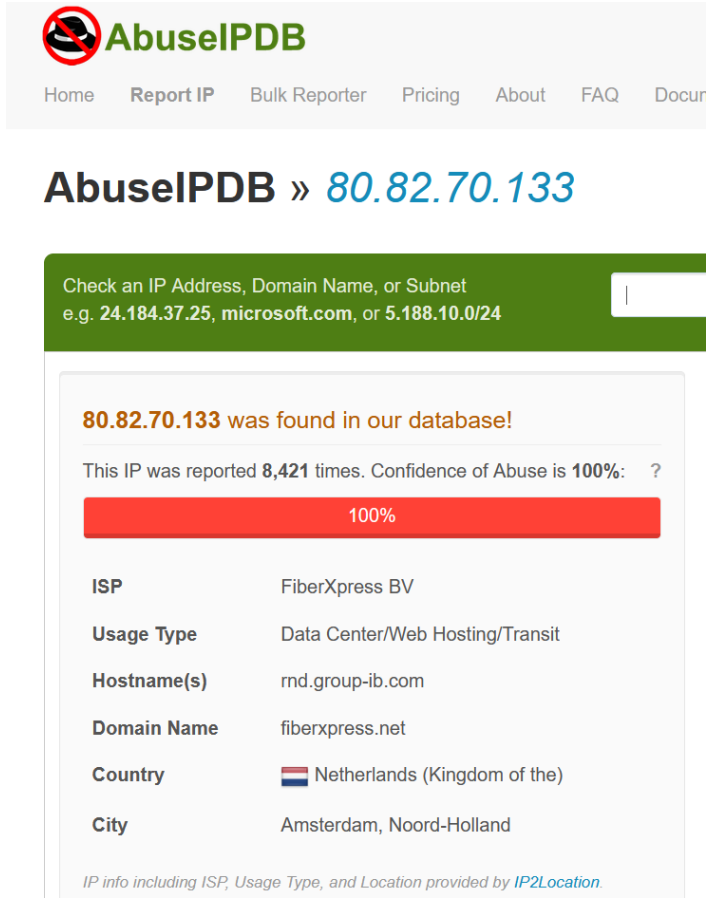
Ecatel was founded in 2005 by two Dutchmen. The company was registered in Kent (United Kingdom) with its head office in The Hague . [1] In 2011, the company had a dispute with the data center in Alphen aan de Rijn where they rented servers. They then decided to start their own data center called DataOne in Wormer . [2]

The company was named the worst hosting company in the world by HostExploit in 2010. [3] In 2012 they dropped to fourth place. [2]

During actions against pedophiles in 2012, Anonymous discovered that Ecatel hosted much of the child pornography found. Under the code name *#OpEcatel,* Ecatel subsequently became the target of DDoS attacks, among other things. [4] At the insistence of cybersecurity company FireEye, Dutch authorities took two Ecatel servers offline in 2012 because they were being used for the Grum botnet . [5]

Known Bad Actors

Validation that an IP belongs to a bad actor can be done via vendor or public resources. AbuseIPdb and Scamlytics are good places to start.

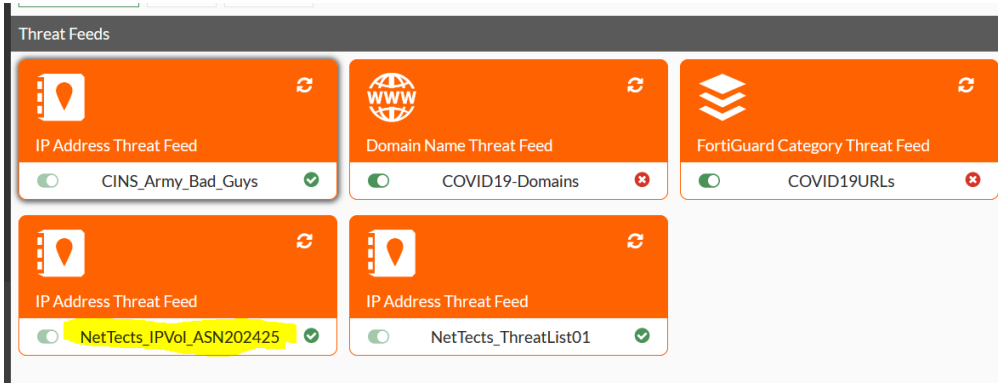


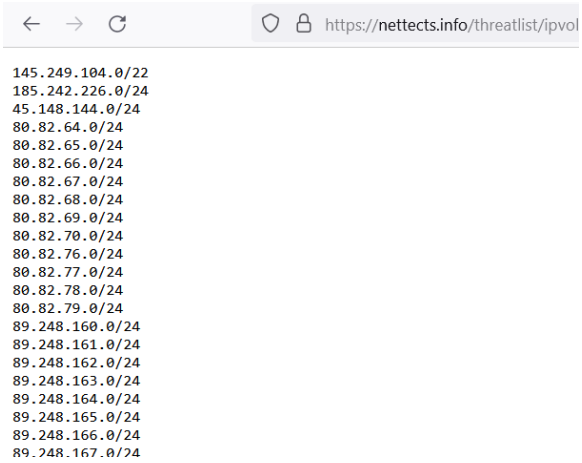
Known Bad Actors

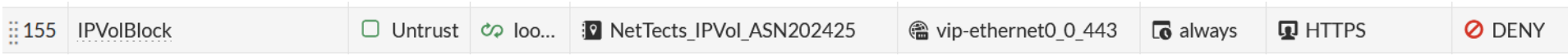
Possibly malicious actors that continually scan include:

- Stretchoid
- Shadowserver
- Criminal IP
- IP Volume

Vendors can maintain these lists for enterprises to apply or provide mechanisms for simple integration into security tools.

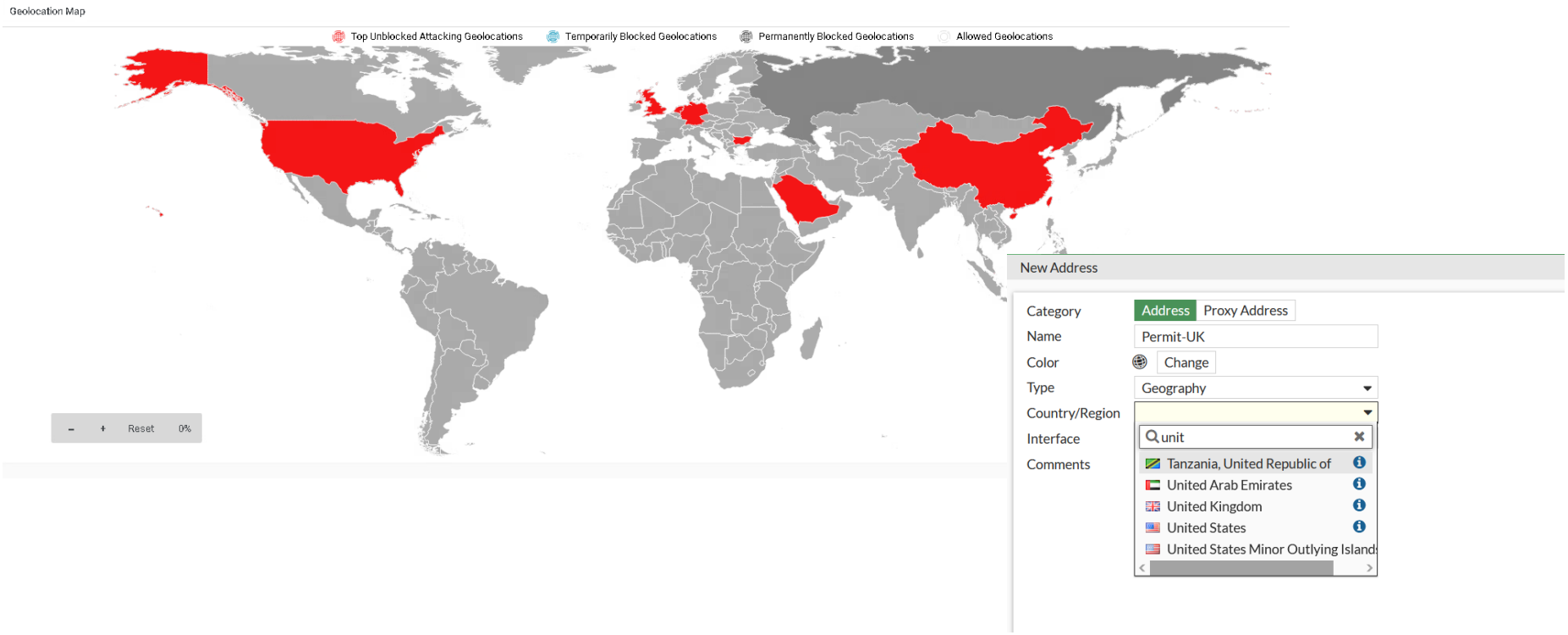






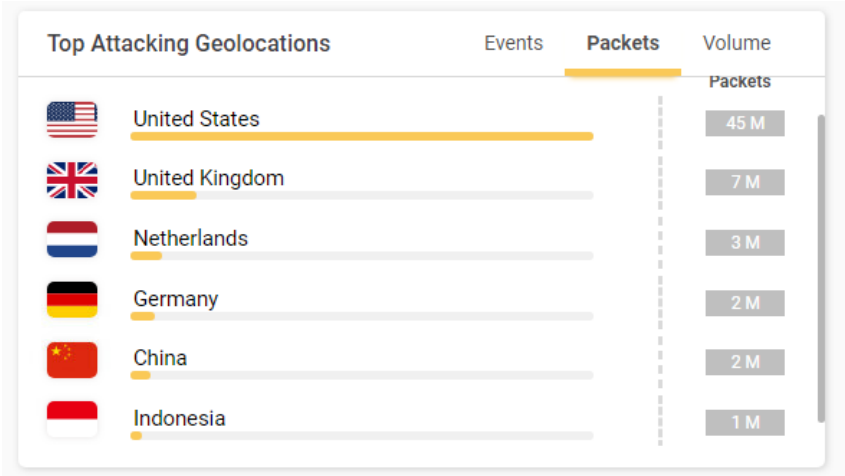
Geo-Fencing

If a service's clients can be geographically limited, or if certain countries are known attackers of a service, they can be blocked by using geographic databases of source IPs. Many vendors offer geo-fencing as a solution



Geo-Fencing

Geo-fencing can be used for positive or negative rules (block country X, or permit country Y). Note that geo-databases have high accuracy, but are not perfect, as they can be based upon IP registrations as well as learned data. Contact the vendor if a discrepancy is expected!

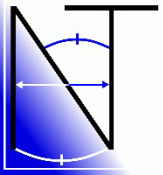


Discovering Attackers

Attackers are probing the enterprise networks constantly. Ascertaining patterns and actively responding to threats and probes is critical to reducing the risk to and the visibility of the enterprises' services. And then one can utilize the logs to identify patterns from tools like:

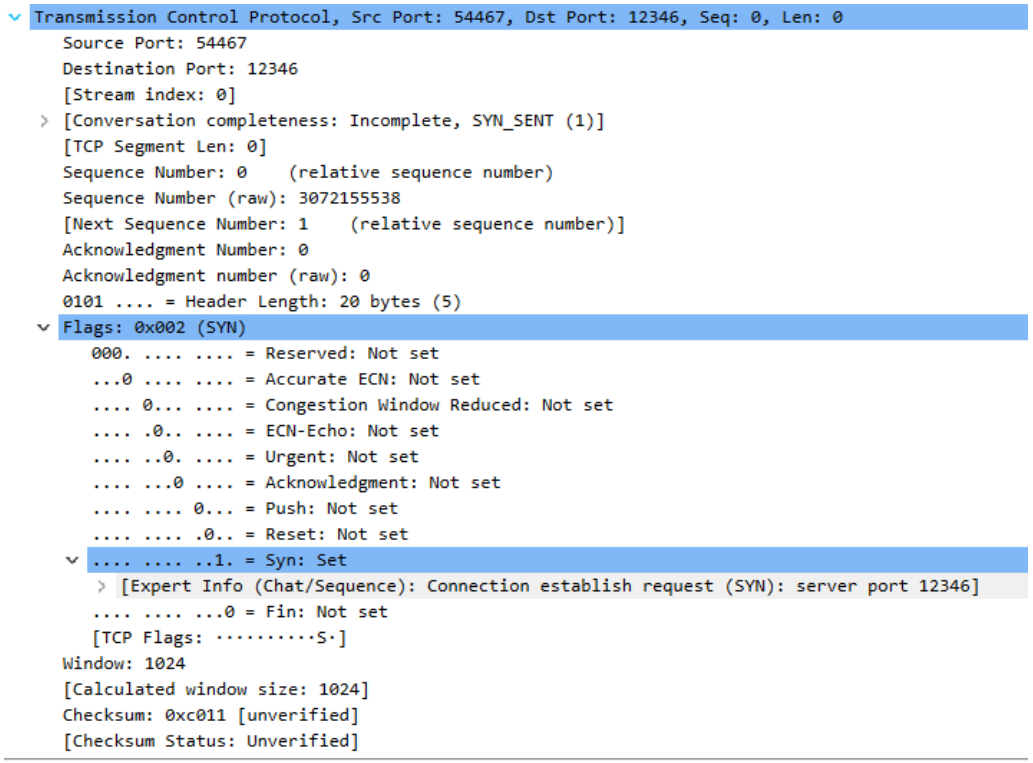
1. Intrusion Prevention Systems/Policies
2. Behavioral DoS engines
3. Access logs from applications and VPNs
4. Packet captures from the above tools

Absolute Date/Time		Severity	Source	Source Country/Region	Prot...	Action	Attack Name
2024-04-16 09:43:32			185.234.216.103	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 08:51:21			185.161.248.192	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 08:35:45			185.11.61.120	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 07:56:32			185.122.204.103	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 07:20:07			185.234.216.103	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 06:31:10			185.122.204.103	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 05:55:06			185.122.204.103	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 05:50:39			185.122.204.103	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 05:40:49			185.230.138.170	Germany	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 05:29:34			185.11.61.120	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...
2024-04-16 05:23:51			185.11.61.120	Russian Federation	6	dropped	TCP_SYN_NoOpt_Win1...



Discovering Attackers

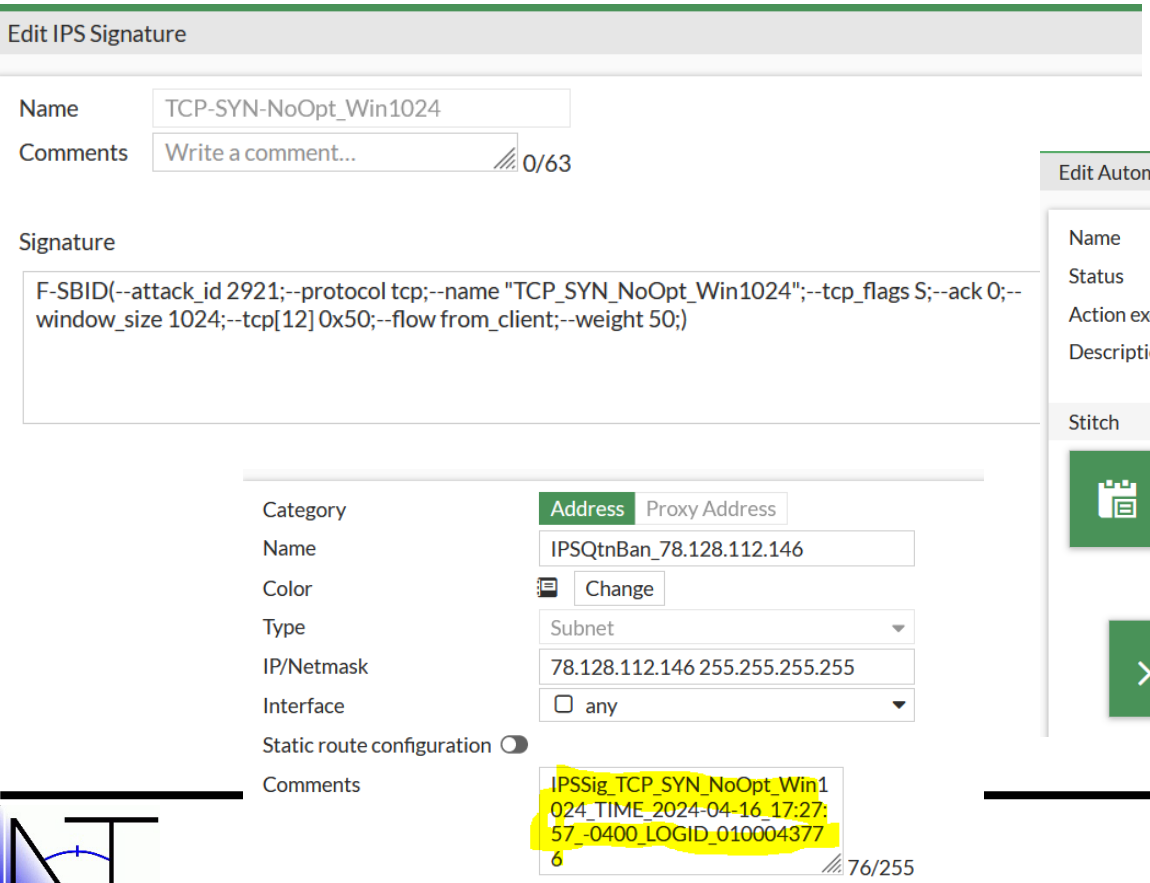
Behavioral Denial of Service tools can identify attackers based upon volumetric and patterns in packet headers. In addition to identifying and stopping individual attacks, this can assist in identification of new attack signatures and new entities.

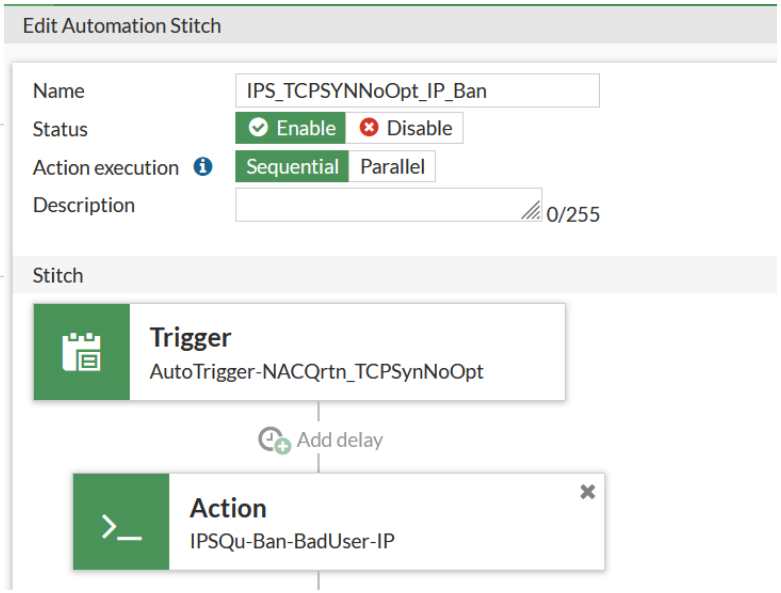


For example, in reviewing packet captures of BDoS attacks, it was discovered that there was a new pattern of attack that could be applied to TCP SYN scans. The SYNs lacked ANY options (MSS, SACK, etc.) and all had a window size of 1024. This meant that these attacks could be identified with a single packet, versus volumetrically

Discovering Attackers

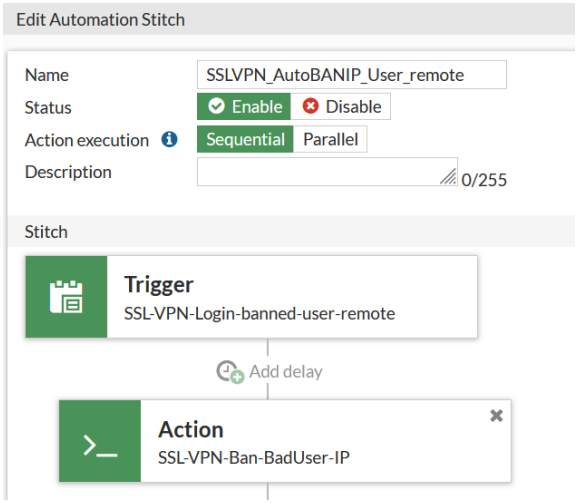
Making a custom IPS signature for this attack permits identification of NEW attackers using SYNs with this profile. NetTects has successfully utilized this signature with an auto block of any IP address probing with this packet





Discovering Attackers

Attackers can also utilize advanced scanners to log into applications. NetTects has seen this at multiple clients – VPN portals will be scanned and attacked constantly. In addition to brute force detection and defense, some of these scanners will use the same log in names to probe for access. By detecting these "usernames", additional IPs can be added to the block list – even dynamically.



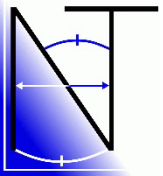
SSLVPN_AutoBANIP_User_Test	Enabled	SSL-VPN-Login-banned-user-test	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_TestSTAR	Enabled	SSL-VPN-Login-banned-user-testSTAR	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_abc	Enabled	SSL-VPN-Login-banned-user-abc	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_acnt	Enabled	SSL-VPN-Login-banned-user-acnt	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_admin	Enabled	SSL-VPN-Login-banned-user-admin	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_adminSTAR	Enabled	SSL-VPN-Login-banned-user-adminSTAR	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_badmin	Enabled	SSL-VPN-Login-banned-user-badmin	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_canon	Enabled	SSL-VPN-Login-banned-user-canon	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_checkSTAR	Enabled	SSL-VPN-Login-banned-user-checkSTAR	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_cisco	Enabled	SSL-VPN-Login-banned-user-cisco	SSL-VPN-Ban-BadUser-IP
SSLVPN_AutoBANIP_User_dev	Enabled	SSL-VPN-Login-banned-user-dev	SSL-VPN-Ban-BadUser-IP

Discovering Attackers

By utilizing existing tools and investigating reported attacks, patterns will emerge. This will permit the enterprise to augment vendor provided lists with additional attacker IPs. Many times, these IPs will be added to the vendor lists in time, so periodic maintenance of the lists to purge older data may be prudent.

IP Range/Subnet 4823/6486		
IPSQtnBan_5.181.17.86	5.181.17.86/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_12:46:11_-0500_LOGID_0100043...
IPSQtnBan_176.235.151.29	176.235.151.29/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_13:27:11_-0500_LOGID_0100043...
IPSQtnBan_163.172.147.100	163.172.147.100/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_13:40:38_-0500_LOGID_0100043...
IPSQtnBan_98.152.200.65	98.152.200.65/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_13:42:24_-0500_LOGID_0100043...
IPSQtnBan_198.12.68.106	198.12.68.106/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_14:02:38_-0500_LOGID_0100043...
IPSQtnBan_190.248.68.78	190.248.68.78/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_14:05:38_-0500_LOGID_0100043...
IPSQtnBan_81.82.249.129	81.82.249.129/32	IPSSig_TCP_SYN_NoOpt_Win1024_TIME_2023-12-21_14:11:27_-0500_LOGID_0100043...

SSLVPN_BAN_138.124.183.51	138.124.183.51/32	USER_admin_TIME_2024-03-09_20:19:03_-0500_LOGID_010...
SSLVPN_BAN_138.199.43.100	138.199.43.100/32	USER_scanner_TIME_2024-01-20_07:42:26_-0500_LOGID_01...
SSLVPN_BAN_138.199.43.101	138.199.43.101/32	USER_scanner_TIME_2023-12-26_01:04:50_-0500_LOGID_01...
SSLVPN_BAN_138.199.43.69	138.199.43.69/32	USER_scanner_TIME_2024-02-08_04:40:58_-0500_LOGID_01...
SSLVPN_BAN_138.199.43.70	138.199.43.70/32	USER_support_TIME_2024-04-01_02:41:26_-0400_LOGID_01...
SSLVPN_BAN_138.199.43.73	138.199.43.73/32	USER_reception_TIME_2024-03-02_01:29:07_-0500_LOGID_0...
SSLVPN_BAN_138.199.43.74	138.199.43.74/32	USER_scanner_TIME_2024-01-22_03:24:40_-0500_LOGID_01...



Implementing Protections

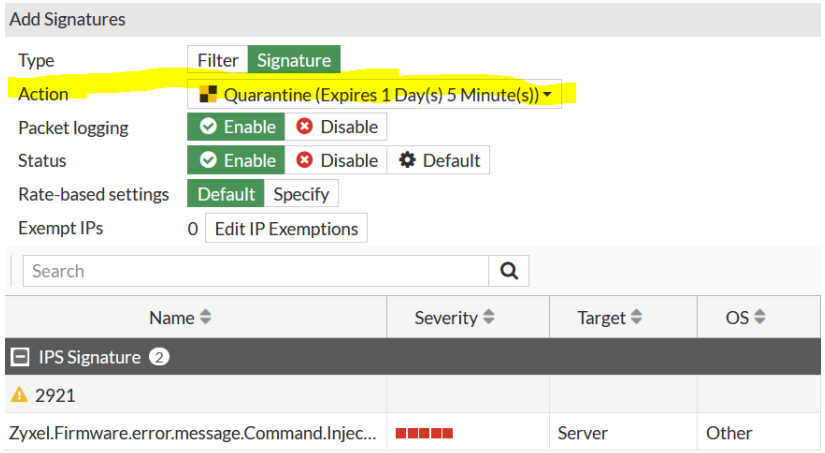
In review, the following protections have been illustrated

1. IP reputation lists from vendors
2. Grey/Black hat lists from vendors
3. Custom IP reputation lists
    a) Lists derived from logs – IPS, denied users, etc
    b) Via dynamic actions – scripts, etc
    c) Via custom feeds/API
    d) Static lists
4. Geo-fencing via vendor provided database

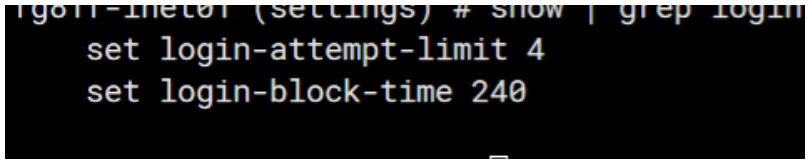
Additional mechanisms and data sources are also available.

Implementing Protections

For example, vendors may provide native quarantine options, for IPS signatures – choose signatures that indicate scanners and malicious intent and apply a quarantine action.



Ensure that brute force protection is enabled for logins – and a block time is configured for offending IPs.



Implementing Protections

Explore options to provide additional feeds/data

AbuseIPDB

Home Report IP Bulk Reporter Pricing About FAQ Documentation Statistics IP Tools Contact LOGIN SIG

AbuseIPDB > Documentation > AbuseIPDB + FortiGate

FORTINET + AbuseIPDB

Integrating AbuseIPDB with Fortinet FortiGate - Automatically Block Abusive IPs

https://feeds.dshield

```
#
#   DShield.org Recommended Block List
#    (c) $year DShield.org
#   some rights reserved. Details http://creativecommons.org/licenses/by-nc-sa/2.5/
#   use on your own risk. No warranties implied.
#   primary URL: https://feeds.dshield.org/block.txt
#     PGP Sign.: https://feeds.dshield.org/block.txt.asc
#
#   comments: systems@isc.sans.edu
#    updated: 2024-04-16T23:00:23.032715
#
#    This list summarizes the top 20 attacking class C (/24) subnets
#   over the last three days. The number of 'attacks' indicates the
#   number of targets reporting scans from this subnet.
#
#
```

cinsscore.com/#list

The CINS Army List

We are joined together in our mutual belief that Internet security should be honored as a fundamental human right. We believe in your right to be connected, to be secure, and to use the Internet with freedom from malicious threats. No one should be allowed to take that away from you.

Based on these beliefs, we created the CINS Army list. CINS Army is a way for our company to give back to the community by sharing valuable threat intelligence harvested from our CINS system. The CINS Army list is a subset of the CINS Active Threat Intelligence ruleset, and consists of IP addresses that meet one of two basic criteria: 1) The IP's recent Rogue Packet score factor is very poor, or 2) The IP has tripped a designated number of 'trusted' alerts across a given number of our Sentinels deployed around the world.

The CINS Army list is here and at Emerging Threats as part of their Open Source Community. The link below is provided as a simple text file, with which you can parse and use in any way you see fit. We assume Network Administrators will use the IP addresses from this file in their firewall blacklists and possibly in custom IDS and IPS signatures.

Download the CINS Army list


```
ted):
ck
 class C)
ts scanned

ddress

ned to multiple users, the first one is listed.

98.255  24      1999    CHANGWAY-AS     HK      noc@ameurotel.c
226.255 24      1742    AS49870-BV      NL      abuse@westcall.
24.255  24      1657    GOOGLE-CLOUD-PLATFORM   US      None
31.255  24      1625    GOOGLE-CLOUD-PLATFORM   US      None
34.255  24      1533    -       -       -
```

In Conclusion

Protecting the enterprise effectively requires a layered approach to security.

IP Based filtering based upon a number of sources and databases can reduce both the attack surface of the enterprise and its visibility to attackers

Logging all traffic, attacks, and failed logins and reviewing these logs can detail attackers and scanners

Incident and forensic data review can expose new attack trends and methodologies

Questions