ONE HOUR UNDER ATTACK

What is the risk of exposing a public IP to the internet? Even for a just a short 1-hour window?

EXECUTIVE SUMMARY

If you wish to have any devices exposed to the internet via either simple port forwards or devices which sit directly on their own public IP address then making sure your device is locked down is of the upmost importance.

Andrew Battersby
Core IP Network Manager
Spitfire Network Services Limited
Nov 2024

Introduction

If your business has an IT department that is doing its job correctly, then worrying about third parties trying to access your network may not be something you have thought about or even considered.

As applications and end points become more interconnected, the need for port forwarding, remote access, and general reachability increases. As a result, the exposure of your network to the internet can also increase, which in turn raises the number of potential attack vectors a third party can use to gain access to your network.

In order to show just how much of a problem it can be to expose a public IP to the internet, Spitfire decided to setup a 'Honeypot' on a public IP and start collecting the number of attacks which can happen in just an hour at a random time in the middle of the day.

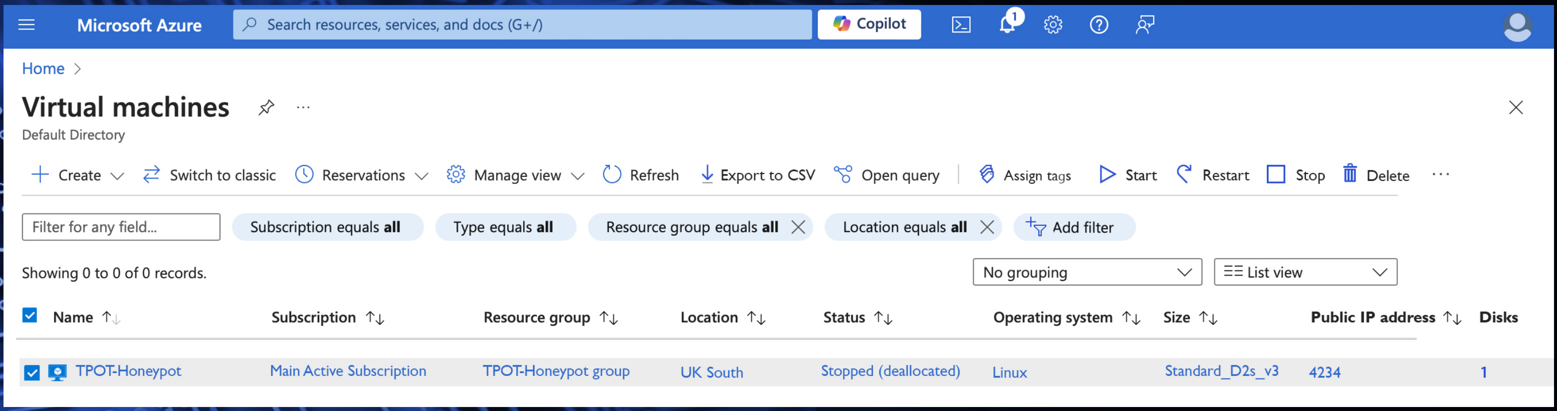
What is a honeypot?

A 'honeypot' is a type of security system used to lure cybercriminals into a trap. Imagine it like a decoy house filled with valuables. In the world of computers, a honeypot is a fake or simulated system such as a website, server, or network that appears to contain sensitive data or vulnerable targets.

The idea is to make it look enticing to hackers or malicious software so they will try to attack it.

For our example we have set up our honeypot on a public IP using a virtual machine on the Azure platform.

The VM Lure



Virtual machines

Default Directory

Subscription equals **all** | Type equals **all** | Resource group equals **all** | Location equals **all**

Showing 0 to 0 of 0 records.

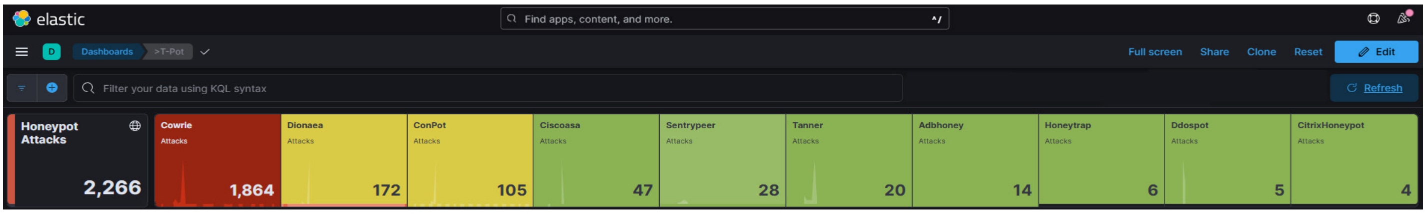
Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
☑ TPOT-Honeypot	Main Active Subscription	TPOT-Honeypot group	UK South	Stopped (deallocated)	Linux	Standard_D2s_v3	4234	1

Using Azure we can set up the VM and allow some very common ports which businesses may have open on their network (SMTP/HTTP/HTTPS/SSH) etc.

Once the VM is set up and we've exposed the ports in question, we can then run our honeypot software and start listening to traffic and watching for IP addresses trying to gain entry.

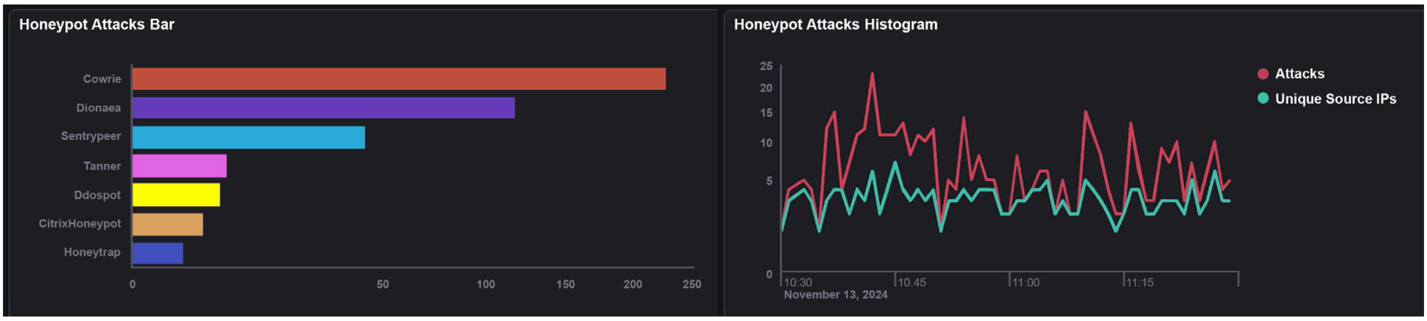
So, what do we see from just a 1-hour window?

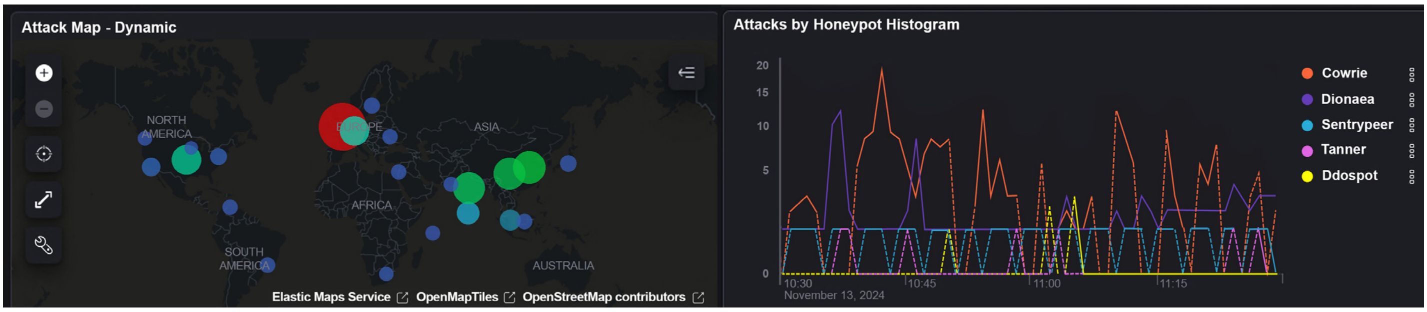
What this diagram shows is that we've had 2,266 attacks come into our Azure public IP. And of these 2,266 attacks they have come from around 120 individual source IP's.

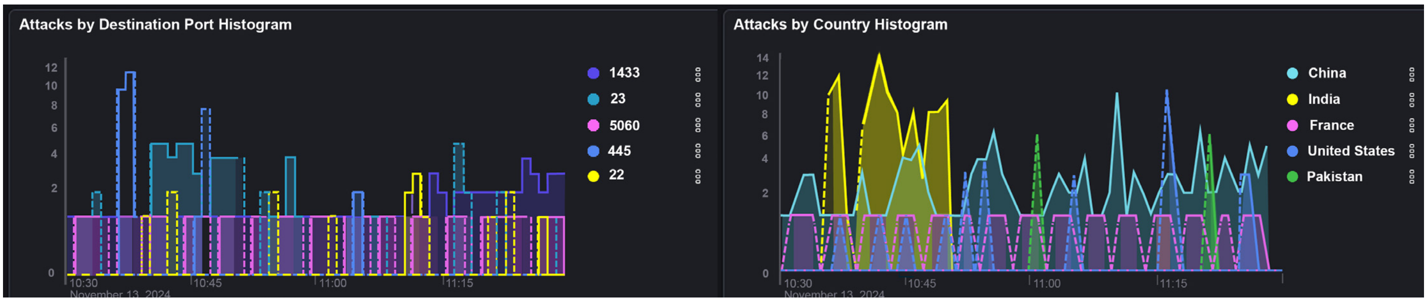

elastic
Find apps, content, and more.
Dashboards
T-Pot
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Refresh

Honeypot Attacks	Cowrie Attacks	Dionaea Attacks	ConPot Attacks	Ciscoasa Attacks	Sentrypeer Attacks	Tanner Attacks	Adbhoney Attacks	Honeytrap Attacks	Ddospot Attacks	CitrixHoneypot Attacks
2,266	1,864	172	105	47	28	20	14	6	5	4

These attacks are then split into different types that attackers have used to try to gain entry to our honeypot device.







Examples:

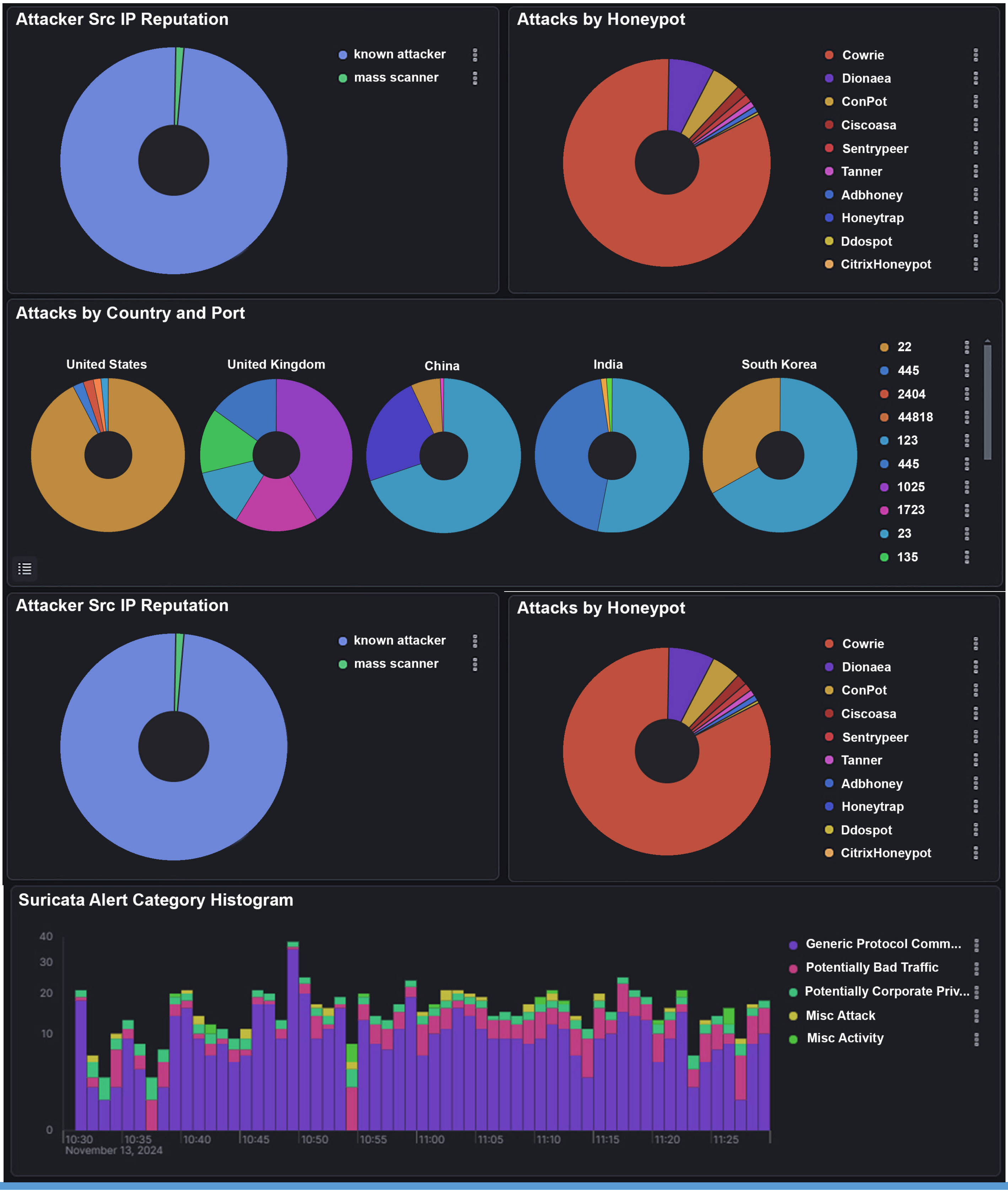
'Cowrie' is logging attacks used against SSH and Telnet and then logging the 'Brute Force' attacks against these ports. Brute force attacks are usually dictionary based. Attackers will use a list of commonly used usernames and passwords to try to gain entry to a system.

'Dionaea' is used to capture SMB (server message block) exploits. SMB is a very common port to forward and is used for things like file shares.

'Conpot' is an ICS (Industrial control system) honeypot listening to common ports used in these systems.

Where's it all coming from?

To get more information we can then start to look at which countries the attackers have initiated their attack from. This is done by looking at the source IP of the attacker, which can be isolated to the country of origin as shown below:

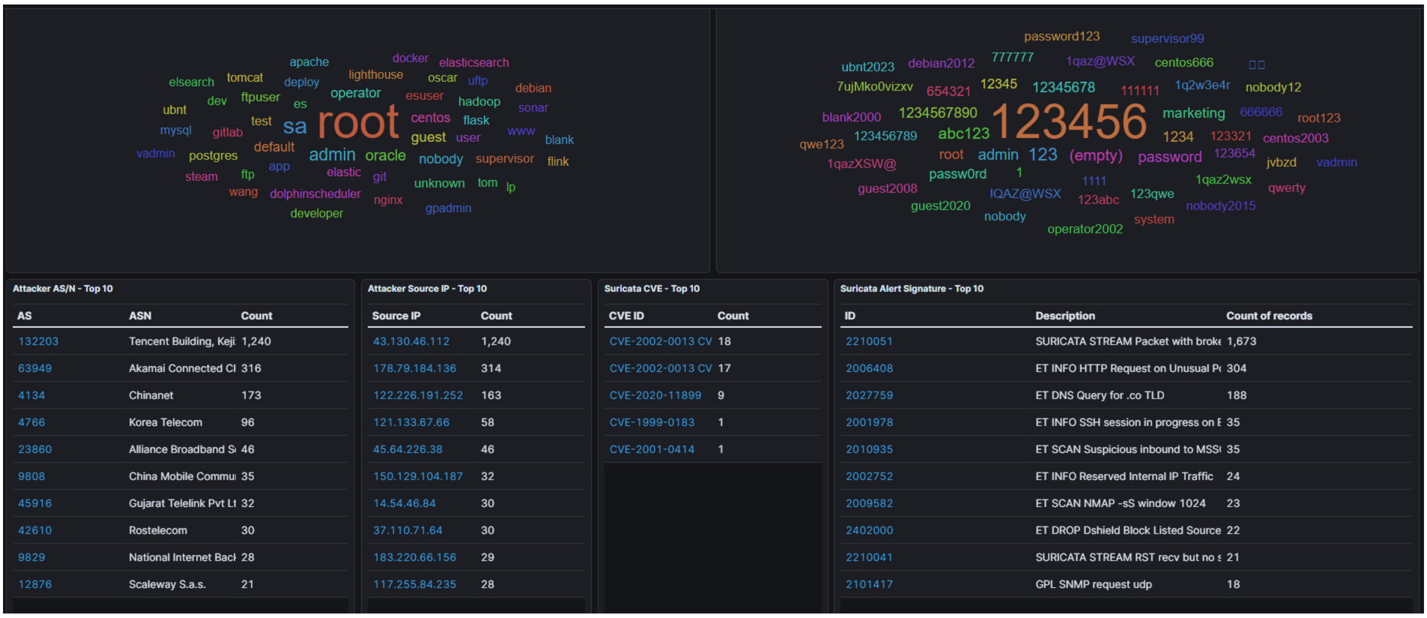


In the window below we can see what username & passwords the dictionary attacks are using to try and gain entry. As expected, we can see lots of 'default' usernames and passwords which unfortunately are still commonly used within many businesses.

And then to the right we have the CVE's which are being used to attack our honeypot. A CVE is a 'Common Vulnerabilities and Exposures' notice which advises the public of potential security flaws.

Once a CVE is released it is the software/hardware vendors responsibility to act on that and patch their software/hardware to make sure they are not exposed to the flaw, although there is no guarantee this will take place and would largely depend on that system having some sort of maintenance agreement.

If we look at the first few CVE's being hit on our system, then we can get an idea of which exploits/vulnerabilities are being used:



Attacker AS/N - Top 10

AS	ASN	Count
132203	Tencent Building, Keji	1,240
63949	Akamai Connected Cl	316
4134	Chinanet	173
4766	Korea Telecom	96
23860	Alliance Broadband S	46
9808	China Mobile Commu	35
45916	Gujarat Telelink Pvt Lt	32
42610	Rostelecom	30
9829	National Internet Bacl	28
12876	Scaleway S.a.s.	21

Attacker Source IP - Top 10

Source IP	Count
43.130.46.112	1,240
178.79.184.136	314
122.226.191.252	163
121.133.67.66	58
45.64.226.38	46
150.129.104.187	32
14.54.46.84	30
37.110.71.64	30
183.220.66.156	29
117.255.84.235	28

Suricata CVE - Top 10

CVE ID	Count
CVE-2002-0013 CV	18
CVE-2002-0013 CV	17
CVE-2020-11899	9
CVE-1999-0183	1
CVE-2001-0414	1

Suricata Alert Signature - Top 10

ID	Description	Count of records
2210051	SURICATA STREAM Packet with broke	1,673
2006408	ET INFO HTTP Request on Unusual Pı	304
2027759	ET DNS Query for .co TLD	188
2001978	ET INFO SSH session in progress on E	35
2010935	ET SCAN Suspicious inbound to MSS(	35
2002752	ET INFO Reserved Internal IP Traffic	24
2009582	ET SCAN NMAP -sS window 1024	23
2402000	ET DROP Dshield Block Listed Source	22
2210041	SURICATA STREAM RST recv but no s	21
2101417	GPL SNMP request udp	18

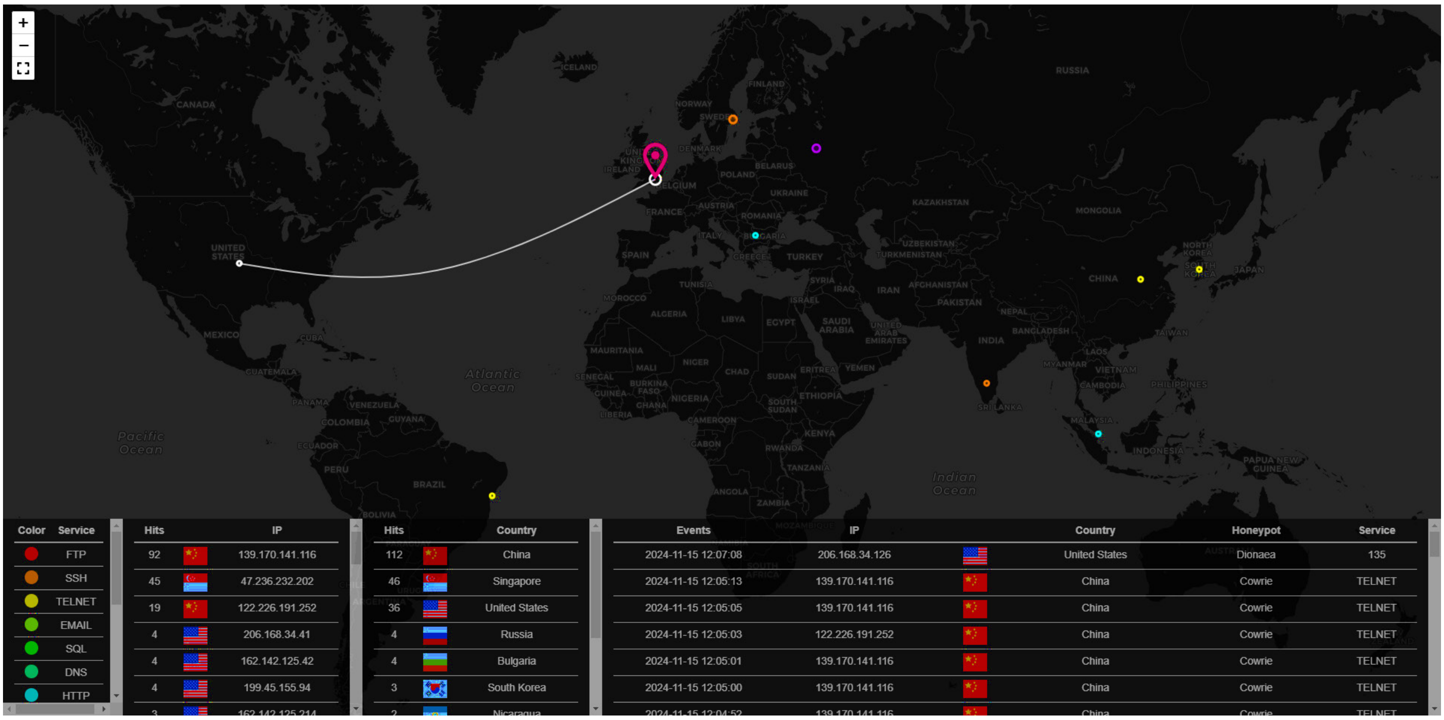
CVE-2002-0013 = "Vulnerabilities in the SNMPv1 request handling of a large number of SNMP implementations allow remote attackers to cause a denial of service or gain privileges"

CVE-2020-11899 = "The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read. It is caused by improper input validation in the IPv6 component when handling a packet sent by an unauthorized network attacker. Potential Denial of Service."

CVE-1999-0183 = "Linux implementations of TFTP would allow access to files outside the restricted directory."

A global view

This offers a geographical layout of live 'hits' as they come into our honeypot, including the source country and the source IP where the attacker originates:



Color	Service
🔴	FTP
🟠	SSH
🟡	TELNET
🟢	EMAIL
🟢	SQL
🟢	DNS
🔵	HTTP

Hits		IP
92	🇨🇳	139.170.141.116
45	🇸🇬	47.236.232.202
19	🇨🇳	122.226.191.252
4	🇺🇸	206.168.34.41
4	🇺🇸	162.142.125.42
4	🇺🇸	199.45.155.94
3	🇺🇸	162.142.125.214

Hits		Country
112	🇨🇳	China
46	🇸🇬	Singapore
36	🇺🇸	United States
4	🇷🇺	Russia
4	🇧🇬	Bulgaria
3	🇰🇷	South Korea
2	🇳🇮	Nicaragua

Events	IP		Country	Honeypot	Service
2024-11-15 12:07:08	206.168.34.126	🇺🇸	United States	Dionaea	135
2024-11-15 12:05:13	139.170.141.116	🇨🇳	China	Cowrie	TELNET
2024-11-15 12:05:05	139.170.141.116	🇨🇳	China	Cowrie	TELNET
2024-11-15 12:05:03	122.226.191.252	🇨🇳	China	Cowrie	TELNET
2024-11-15 12:05:01	139.170.141.116	🇨🇳	China	Cowrie	TELNET
2024-11-15 12:05:00	139.170.141.116	🇨🇳	China	Cowrie	TELNET
2024-11-15 12:04:52	139.170.141.116	🇨🇳	China	Cowrie	TELNET

For those in the IT industry, seeing this level of attacks coming into our honeypot will be of no surprise.

It's our job to make sure we are able to lock down these devices/services and make sure we are reducing exposure as much as possible while making sure our systems are also useable for staff.

Most attackers know that UK staff are likely to be out of the office by 6pm-8pm in the evening so they will wait until after these hours before they start looking for vulnerabilities, to avoid alerting anyone who may be looking out for them.

Summary

As can be seen if you wish to have any devices exposed to the internet via either simple port forwards or devices which sit directly on their own public IP address then making sure your device is locked down is of the upmost importance.

Having someone setup a simple port forward but forget to lock down that port forward can have a devastating effect on a business's network. Once an attacker has access to a single device on a network they can use that to then hop onto other devices in that network.

In the worst cases they will make sure you are unaware of this vulnerability as long as possible before potentially launching something like a ransomware attack on your network.

A ransomware attacker can infect your network in just a few hours, but some attackers will stay on your network from days to weeks making sure as many systems as possible are infected before then locking all systems and files via encryption and then sending the ransom note to the unfortunate victim.