BLUEHAT

IL 2022

STAYING AHEAD OF INTERNET BACKGROUND EXPLOITATION

Andrew Morris

GREYNOISE
INTELLIGENCE

ANDREW MORRIS

Founder and CEO
GreyNoise Intelligence
@Andrew___Morris
andrew@greynoise.io

1. Intro & Background

1. Part I – What Is The Problem?

2. Part II – Our Solution To The Problem

1. Part III – Things We've Observed

2. Summary & Recap

PART 1 – THE PROBLEM

IN PLAIN TERMS...

Every other month, a really bad vulnerability is identified, disclosed, weaponized, and exploited at scale around the internet, in some piece of common perimeter-facing software and nobody has any idea what to do about it.

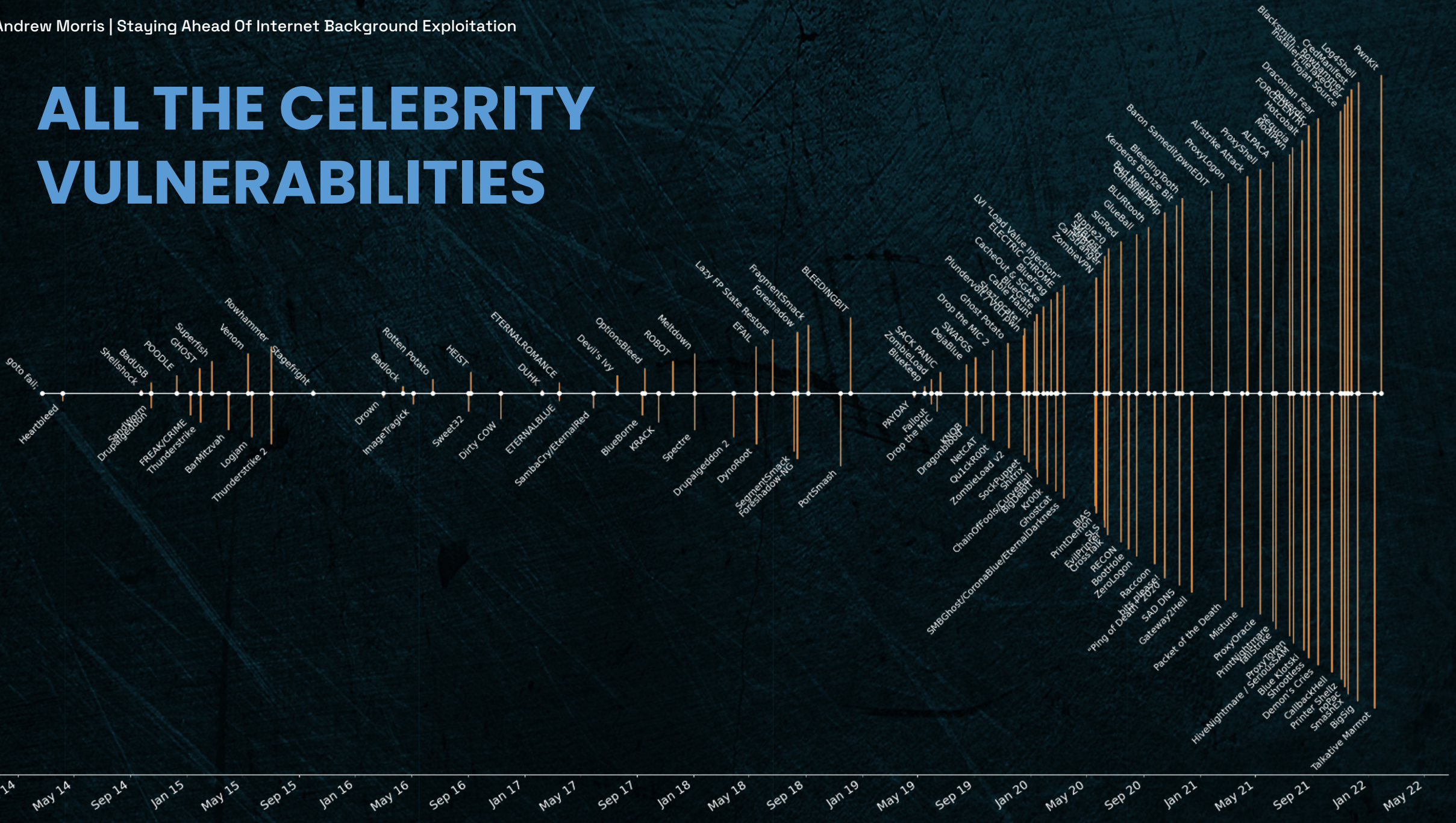
35% of initial infections, according to IBM

"Scan-and-exploit" top infection vector in 2020

Scanning and exploiting vulnerabilities jumped up to the top infection vector in 2020 with a 35% share, surpassing phishing which was the top vector in 2019.

Source: https://www.ibm.com/security/data-breach/threat-intelligence

ALL THE CELEBRITY VULNERABILITIES



HERE'S WHY WE'RE HERE

- **Vulnerability research has evolved**
  - Tooling and development has improved
  - Attack surface has increased
- **Mass scanning has evolved**
  - Tooling is better (Masscan, Zmap, etc)
  - Recyclable IPs are a thing (cloud)
  - The Internet is literally faster

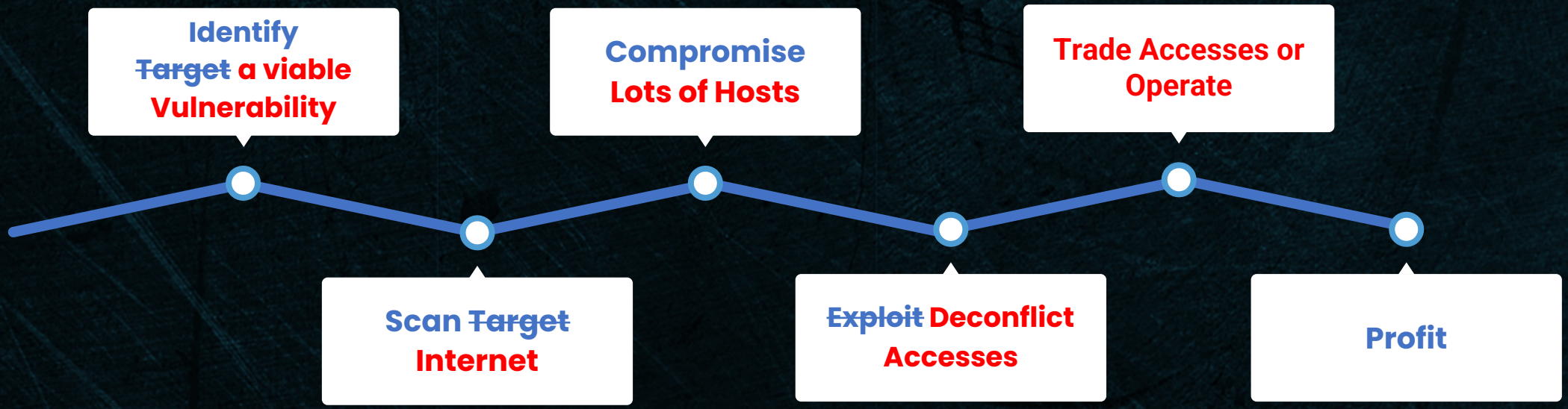
Mass scanning + vulnerability research
=
mass exploitation dying to happen

HACKING IN THE 90's

We used to think about bad guys hacking systems on the internet following this pattern:

HACKING IN THE 20's

Today more closely resembles an assembly line:



THREAT MODEL CREEP

To quote Bruce Potter at some point a few years ago:

- $ACTOR does $ACTION to $ASSET resulting in $OUTCOME because $MOTIVATION

But now:

- $ASSET can increasingly refer to 0.0.0.0/0
- SOMEONE does AN EXPLOIT to **THE ENTIRE INTERNET** resulting in SHELLS AND CHAOS

WHAT IS INTERNET BACKGROUND NOISE?

On a daily basis, every individual routable IP on the Internet sees:

~3,000 unsolicited pings from…
~1,000 distinct IP addresses

Each /24 receives about 46mb of unsolicited network data from ~200,000 IP addresses from SYNs alone

Why so much scanning?

- BAD: Credential stuffing, proxy checking, brute forces, exploit vulnerabilities, etc
- GOOD: Web search, asset discovery, third party risk, security research

The internet is just really noisy, man.

Internet scanning of the internet by source IPv4 address, Jan-21 to Feb-22. Each pixel in this photo is a group of 256 IPs.; the "brightness" of each pixel is how many IPs in that group have been observed by GreyNoise.

Source: GreyNoise Intelligence

SOME SOURCES OF "BENIGN" INTERNET BACKGROUND NOISE

- Alpha Strike Labs
- GoogleBot
- BinaryEdge.io
- Project Sonar
- Bitsight
- Censys
- ShadowServer.org
- cyber.casa
- ONYPHE
- InterneTTL
- BingBot
- Yandex Search Engine
- Cortex Xpanse
- ipip.net
- Shodan.io
- IPinfo.io
- Cloud System Networks
- Net Systems Research
- OpenIntel.nl
- Facebook Crawler
- AdScore
- Ahrefs
- Intrinsec
- DomainTools
- CriminalIP
- BLEXBot
- Arbor Observatory
- Technical University of Munich
- Mail.RU
- Palo Alto Crawler
- Petalbot
- Caida
- LeakIX
- Quadmetrics.com
- Archive.org
- Moz DotBot
- RWTH AACHEN University
- VeriSign
- Bit Discovery
- Project25499
- Applebot
- CyberGreen
- ESET
- FH Muenster University
- Knoq
- Mojeek
- SecurityTrails
- University of Colorado

2004

"[A] telescope monitoring a single IP address (a /32) the average time to observe a host at 10 addresses per second is over 13 years and the time to observe with 95% likelihood is over 40 years."

http://www.cs.unc.edu/~jeffay/courses/nidsS05/measurement/moore-telescopes04.pdf

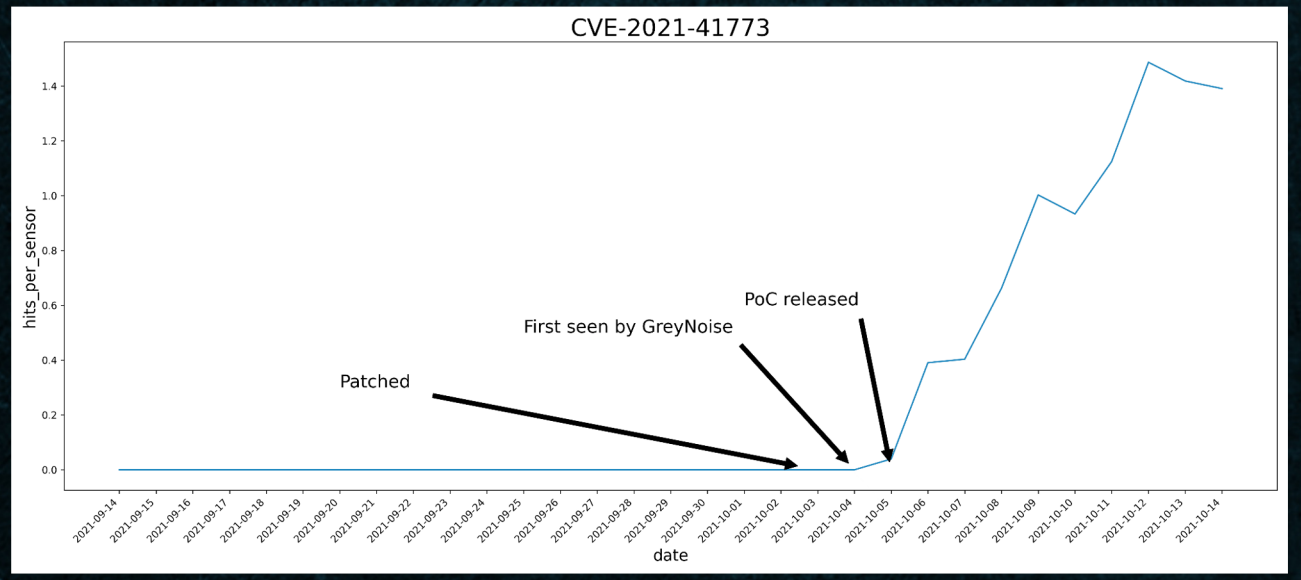
2013

"[Masscan] can scan the entire Internet in under 5 minutes, transmitting 10 million packets per second, from a single machine."

https://github.com/robertdavidgraham/masscan

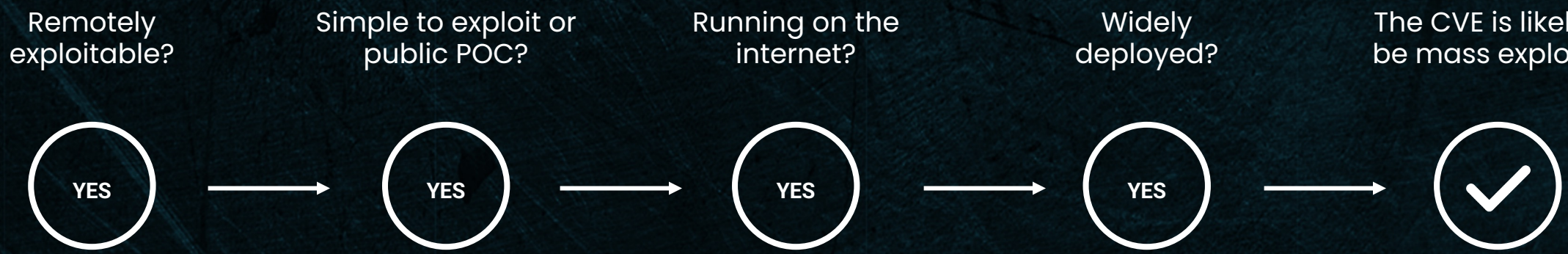
APACHE PATH TRAVERSAL

- Sept 29, 2021:
  - Patch submitted
- Oct 03, 2021:
  - GreyNoise observes first internet-wide vuln scan
- Oct 04, 2021:
  - Apache version update, patch is GA
- Oct 05, 2021:
  - Apache discloses vulnerability to CVE



https://www.greynoise.io/blog/a-patchy-server-greynoise-observes-path-traversal-and-remote-code-execution-in-apache-http

WILL CVE-BLAH-BLAH BE "MASS EXPLOITED"?



WHO EXPERIENCES THE PAIN?

Defenders

- "Are you kidding me? Another one? Again?"

Cyber Security Vendors

- "This is either an opportunity to make money, OR this makes us look like idiots"

Software Vendors

- "This makes people afraid to run our software"

Hosting Providers

- "Please stop popping boxes from our network, we can't handle any more FBI calls or abuse complaints"

WHY IS THIS PROBLEM HARD?

Trust

- Lots of data is bad
- Lack of filtering and quality assurance means nobody is willing to make automated decisions based on someone else's data

Money

- Accidentally blocking revenue-generating users

Speed

- There is a "time-to-get-something-useful-to-say"
- There is a "time-to-say-it"
- If both do not happen prior to an attack hitting the perimeter, you lose the race`

Scale issues

NEXT TIME THE SH*T HITS THE FAN?

- "Whack-a-mole"-style short term blocking has surprisingly good results.
  - Reduces successful attacks by 70%, but needs to be fast
  - Hunting is more straightforward but obviously this means the compromise has already occurred
- More collective defense, more info sharing from vendors and groups who have ***good*** data
- **Fewer** well-intentioned security researchers and vendors spraying exploits around
- Assume every service on your perimeter can suddenly become vulnerable on very little notice

TL;DR

Super bad vulnerabilities are coming out every other month, bad guys exploit them at scale, and it's a differently flavored dumpster fire every time

Stopping the vulns from existing seems unlikely, so let's try to detect and block before it hits a network we care about

PART II – OUR SOLUTION TO THE PROBLEM

WHO'S TRACKING VULN EXPLOITATION IN THE WILD?

CVES EXPLOITED IN THE WILD

GreyNoise	AttackerKB	US CISA
201	639	377
March 2020-Present	June 2020-Present	Nov. 2021-Present

*United States Cybersecurity Infrastructure & Security Agency

ONE WAY TO SOLVE THE PROBLEM

- Deploy a huge network of sensors across the internet
- “Listen” to internet background noise (scans/probes) and internet background exploitation
- Make the sensors look like lots of different software
- Fingerprint every exploit request we find
- Temporarily block offenders BEFORE an attack lands on the perimeter

GREYNOISE ORIGIN STORY

Years ago, someone with a lot of money and a lot of weird problems wanted to know if the computers they were running on the internet were seeing a “normal” amount of scans, or an undue amount of attention. I became obsessed and here we are years later: **GreyNoise**.

GREYNOISE TL;DR

- **Thousands of sensors** - we operate thousands of sensors (kinda like honeypots) across the globe
  - Centrally managed
  - Distributed and geographically diverse
  - What they masquerade as is programmable
  - Every host is ephemeral
- **Billions of events** - as of March 2022 we're processing and storing several billion events per day
- **Tagging** - we add and maintain signatures on exploit, actor, and other patterns using an internally developed tagging engine and DSL
- **Use cases** - GreyNoise is useful for several use-cases; one of the increasingly popular use-cases is protecting orgs from opportunistic compromise
- **Free data** - we give away an insane amount of free data. Seriously.

CHALLENGES

- Speed
- Provider
- OpSec
- Cost
- Automation
- Geography
- Data / Scale
- Masqueraders / Fakers

SPEED CHALLENGES

- Staying “in front of” the exploit is hard
- We only have a few minutes maximum to go from:
  - Malicious traffic hitting the first few sensors..
  - ...classifying the traffic as XYZ exploit...
  - And finally pushing a “block decision”
- It isn’t enough to classify traffic correctly; you have to classify correctly in time.

SELECTING PROVIDERS

- Major cloud providers are easy
  - AWS, Google, Azure, DigitalOcean…
- Language barriers
- Automation maturity
- Infrastructure reliability
- Cost
- GeoIP is fakeish
- No colos

ELEVATING CLOUD PROVIDERS

- AWS is the standard for maturity
- API/Deployment Automation
- Minimum viable features
- Cost
  - Smallest instance
  - Many IPs to one instance
- Reliability

COST CHALLENGES

- Lacking financial automation
  - Pre-payment model
  - Remember to top up…
- IPs per host
  - One IP per host is expensive
  - Many IPs to one host is “expensive”
    - Indirect automation and complexity costs

AUTOMATION CHALLENGES

- Find the lowest common denominators for deployment and automation
  - Templating/code generation
  - Custom Terraform providers
  - “metacloud”
- Testing is *really* hard
- No common standard

RELIABILITY CHALLENGES

- Unreliable APIs
- Unreliable infrastructure
- Latency
- Debugging across multiple providers

GEOGRAPHICAL CHALLENGES

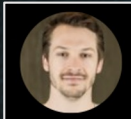
- Do you have sensors in X country?
  - GeoIP is fake… sometimes
  - Ambiguous regions
- No colos
- Dependant on
  - Automation maturity, cost, reliability
- Do you know how hard it is to find cloud hosting providers in most areas of the world???
- Once you hit a critical mass you can do cool stuff like… identify all IPs that are specifically scanning Israel's IP space…

HERE ARE ALL THE IPS SPECIFICALLY **SCANNING/CRAWLING/ATTACKING** ISRAEL'S IP SPACE, & NOBODY ELSE'S

https://api.greynoise.io/datashots/bluehat/israel.csv

OTHER CHALLENGES

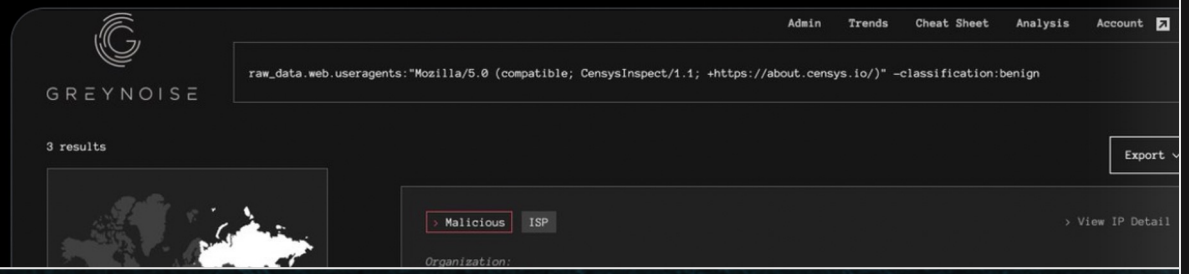
- Account freezes
  - Russia, Ukraine, China
  - Photo verification (sorry Greg)
  - Vetting process
  - Flagged for churning sensors
- Typical big data/scaling challenges
- Shout out to the masqueraders

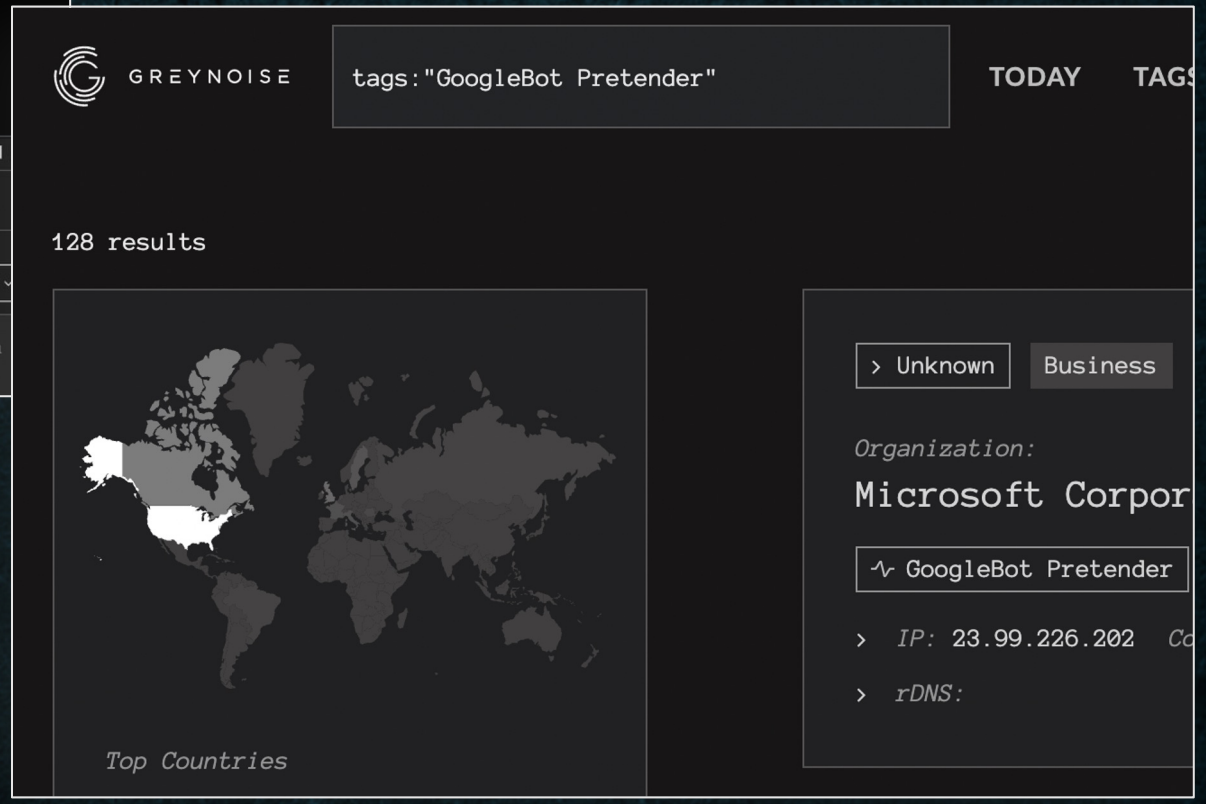


Andrew Morris
@Andrew__Morris

Someone is crawling the internet for SSH private keys, git configs, and .env files masquerading as legitimate security company Censys (@censysio) using their user agent but coming from a network that they usually do not originate from.

viz.greynoise.io/query/?gnql=ra...





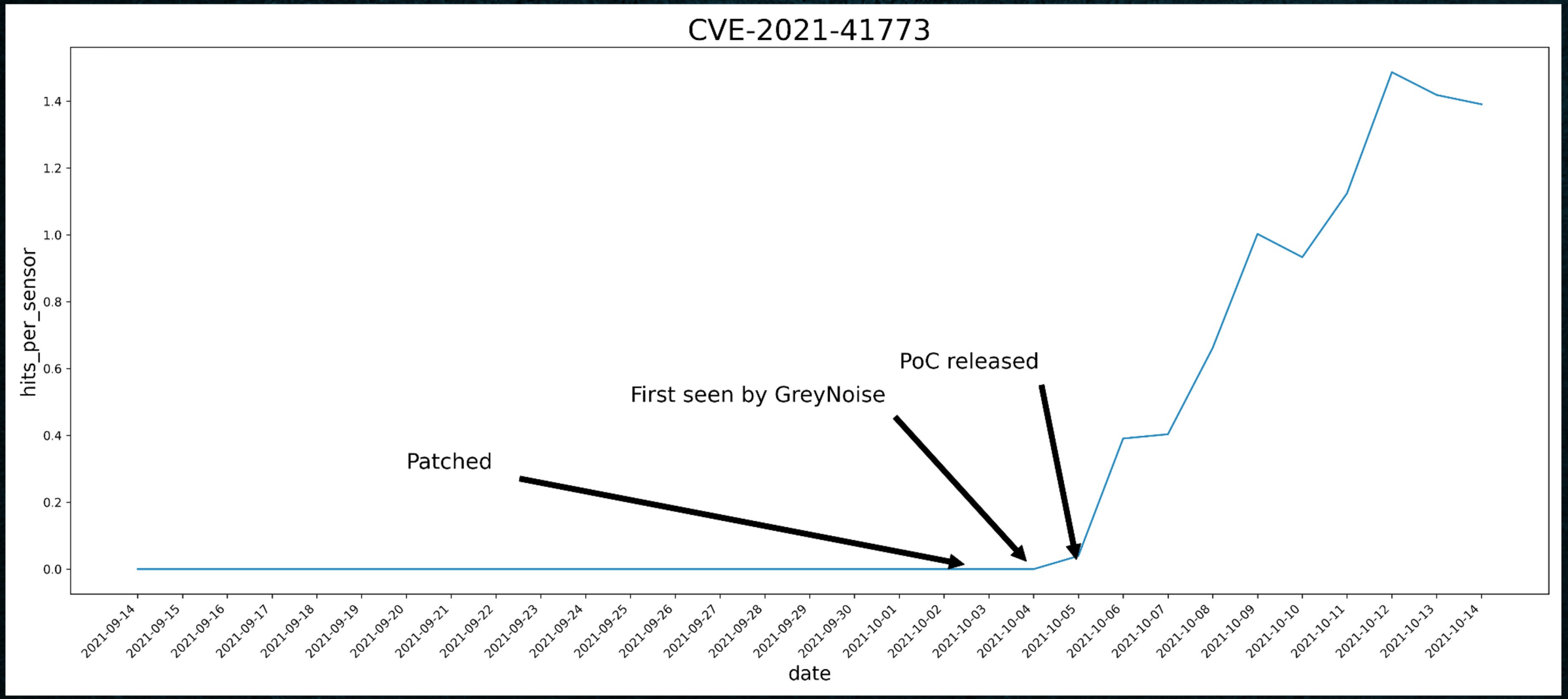
PART III – THINGS WE'VE OBSERVED

CASE STUDIES

- CVE-2021-41773, Apache Path Traversal
- CVE-2021-38647, OMIGOD
- CVE-2021-26084, Atlassian Confluence OGNL Injection
- CVE-2021-44228, Log4Shell

APACHE PATH TRAVERSAL

(CVE-2021-41773)



https://www.greynoise.io/blog/a-patchy-server-greynoise-observes-path-traversal-and-remote-code-execution-in-apache-http

TIMELINE

September 29, 2021
Patch Submitted

October 03, 2021
GreyNoise observes first internet-wide vuln scan

October 04, 2021
Apache version update, patch is GA

October 05, 2021
Apache discloses vulnerability to CVE

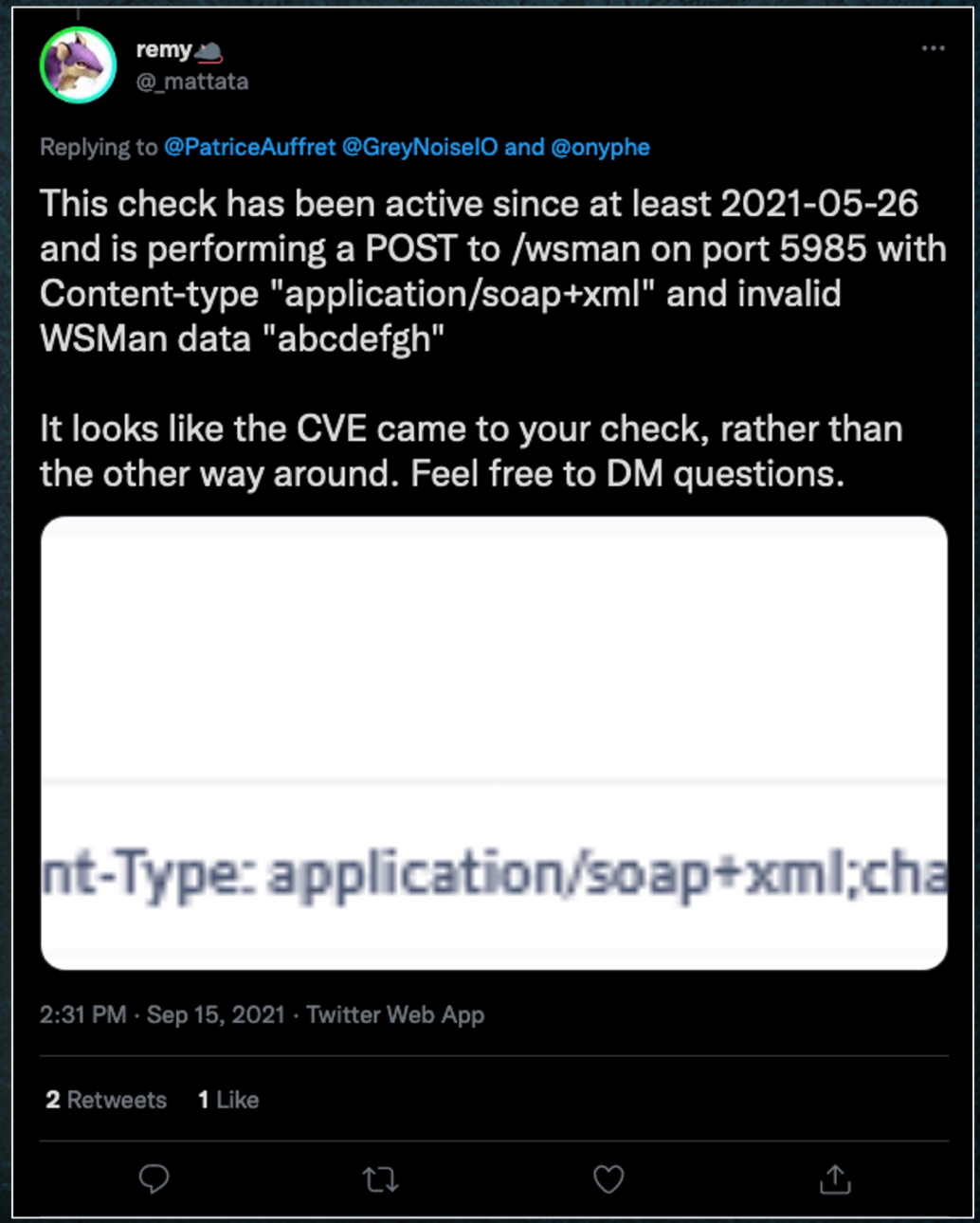
OPPORTUNISTIC EXPLOITATION/SCANNING ONE DAY BEFORE MAJOR POC RELEASE

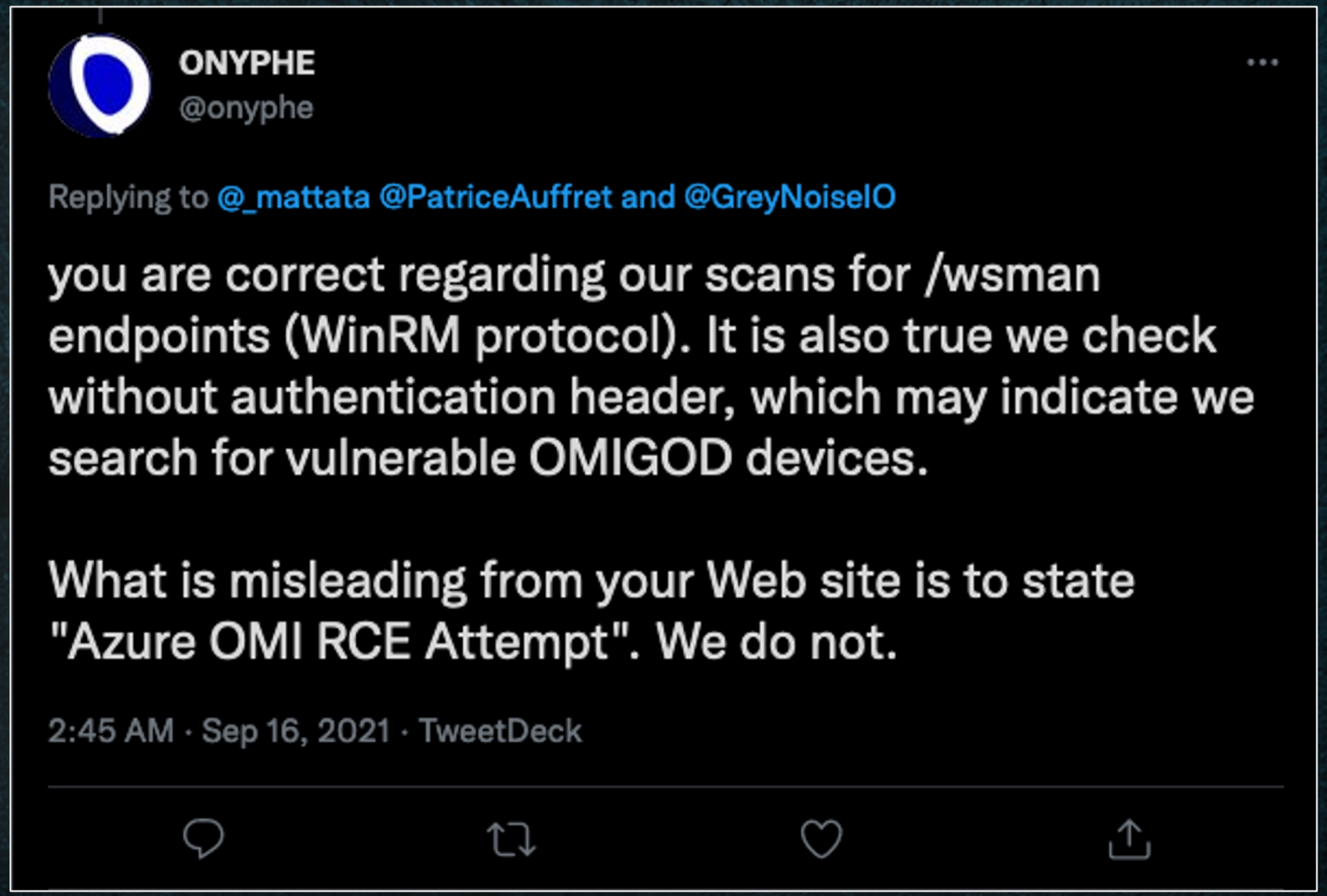
OMIGOD

(CVE-2021-38647)


remy
@_mattata
@GreyNoiseIO is now tracking CVE-2021-38647, Azure Open Management Infrastructure Remote Code Execution Vulnerability
greynoise.io/viz/query/?gnq...
Kevin Beaumont @GossiTheDog · Sep 14, 2021
Microsoft Azure silently install management agents on your Linux VMs, which now have RCE and LPE vulns.
Microsoft don't have an auto update mechanism, so now you need to manually upgrade the agents you didn't know existed as you didn't install them. wiz.io /blog/secret-ag...
Show this thread
11:25 AM · Sep 15, 2021 · Twitter Web App
23 Retweets
4 Quote Tweets
42 Likes


GomoR
@PatriceAuffret
Replying to @_mattata and @GreyNoiseIO
Hello. @onyphe does not check this CVE (yet).
1:48 PM · Sep 15, 2021 · Owly
1 Like


remy
@_mattata
Replying to @PatriceAuffret @GreyNoiseIO and @onyphe
This check has been active since at least 2021-05-26 and is performing a POST to /wsman on port 5985 with Content-type "application/soap+xml" and invalid WSMan data "abcdefgh"
It looks like the CVE came to your check, rather than the other way around. Feel free to DM questions.
nt-Type: application/soap+xml;cha
2:31 PM · Sep 15, 2021 · Twitter Web App
2 Retweets 1 Like

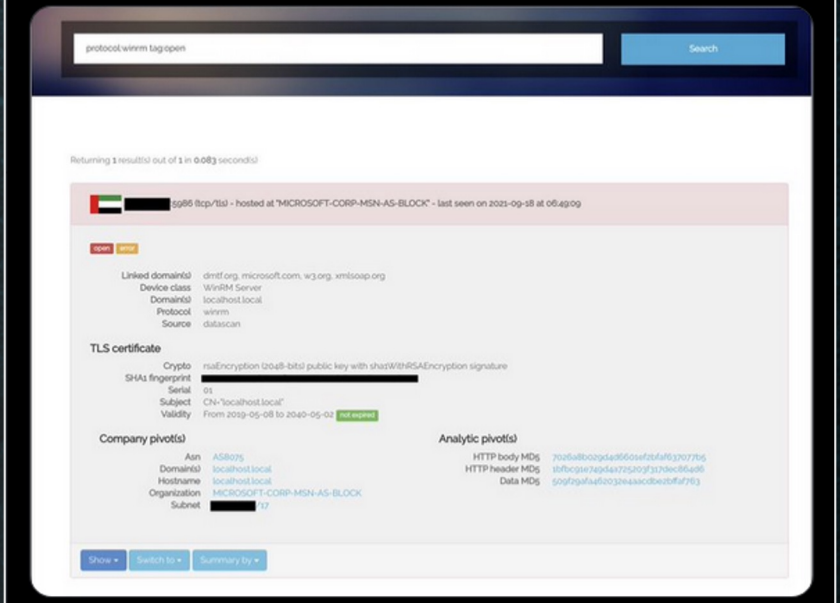

ONYPHE
@onyphe
Replying to @_mattata @PatriceAuffret and @GreyNoiseIO
you are correct regarding our scans for /wsman endpoints (WinRM protocol). It is also true we check without authentication header, which may indicate we search for vulnerable OMIGOD devices.
What is misleading from your Web site is to state "Azure OMI RCE Attempt". We do not.
2:45 AM · Sep 16, 2021 · TweetDeck

ONYPHE
@onyphe

It appears we were able to detect #OMIGOD #CVE-2021-38647 since 2021-05-26. Thanks @GreyNoiseIO :)

We have added tags to datascan dataset so our customers can cgeck their own perimeters:

category:datascan ?domain:example.com ?ip:172.16.0.0/16 tag:open protocol:winrm

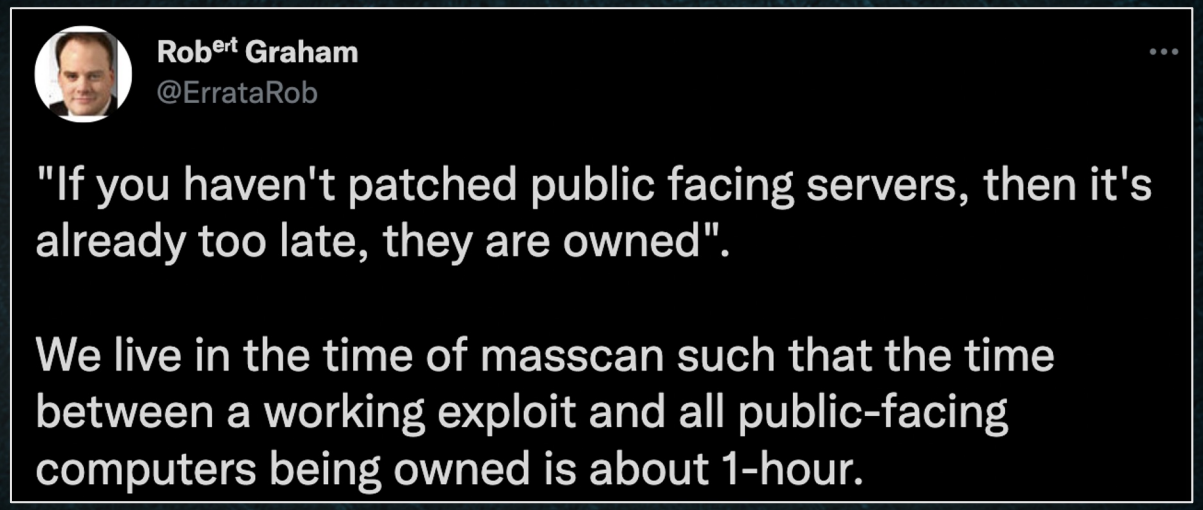


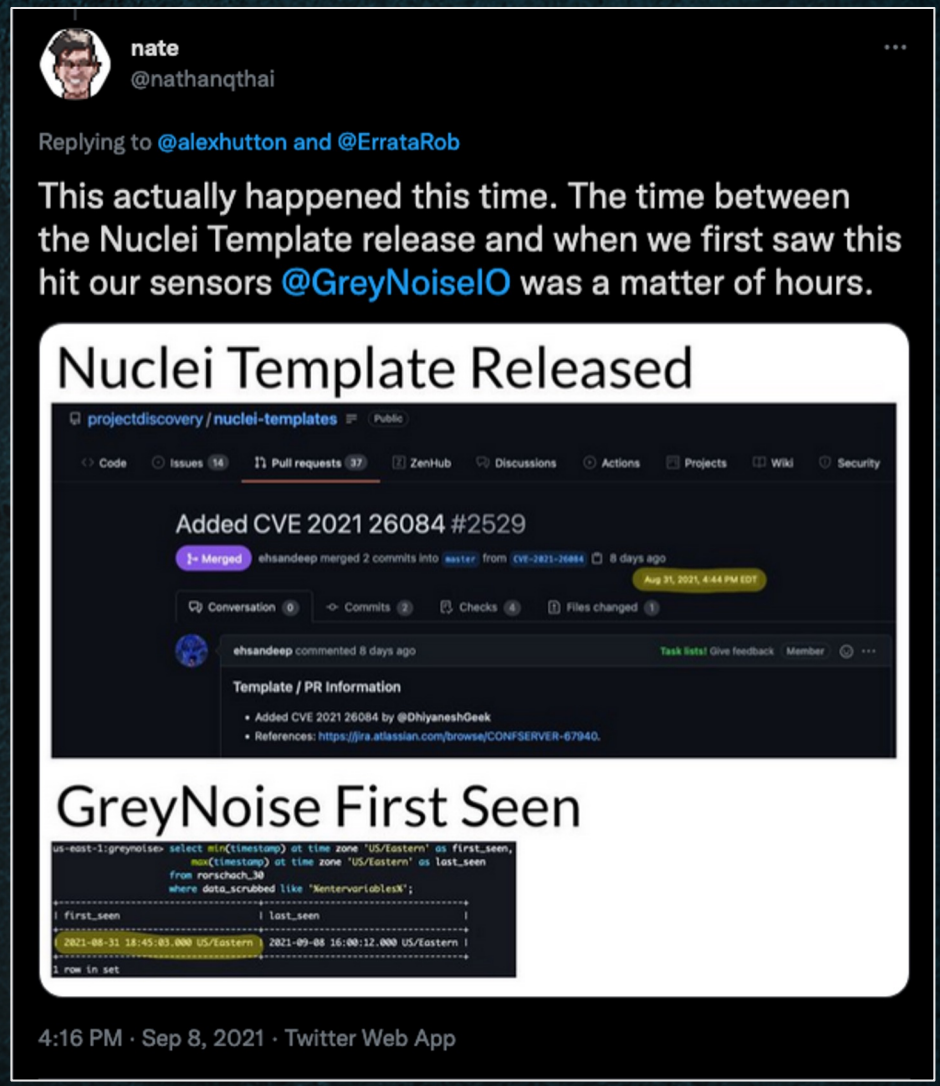
3:40 AM · Sep 18, 2021 · TweetDeck

3 Retweets **1** Quote Tweet **4** Likes

ACCIDENTAL “EXPLOITATION” 4 MONTHS BEFORE PUBLICLY KNOWN

CONFLUENCE OGNL CVE-2021-26084

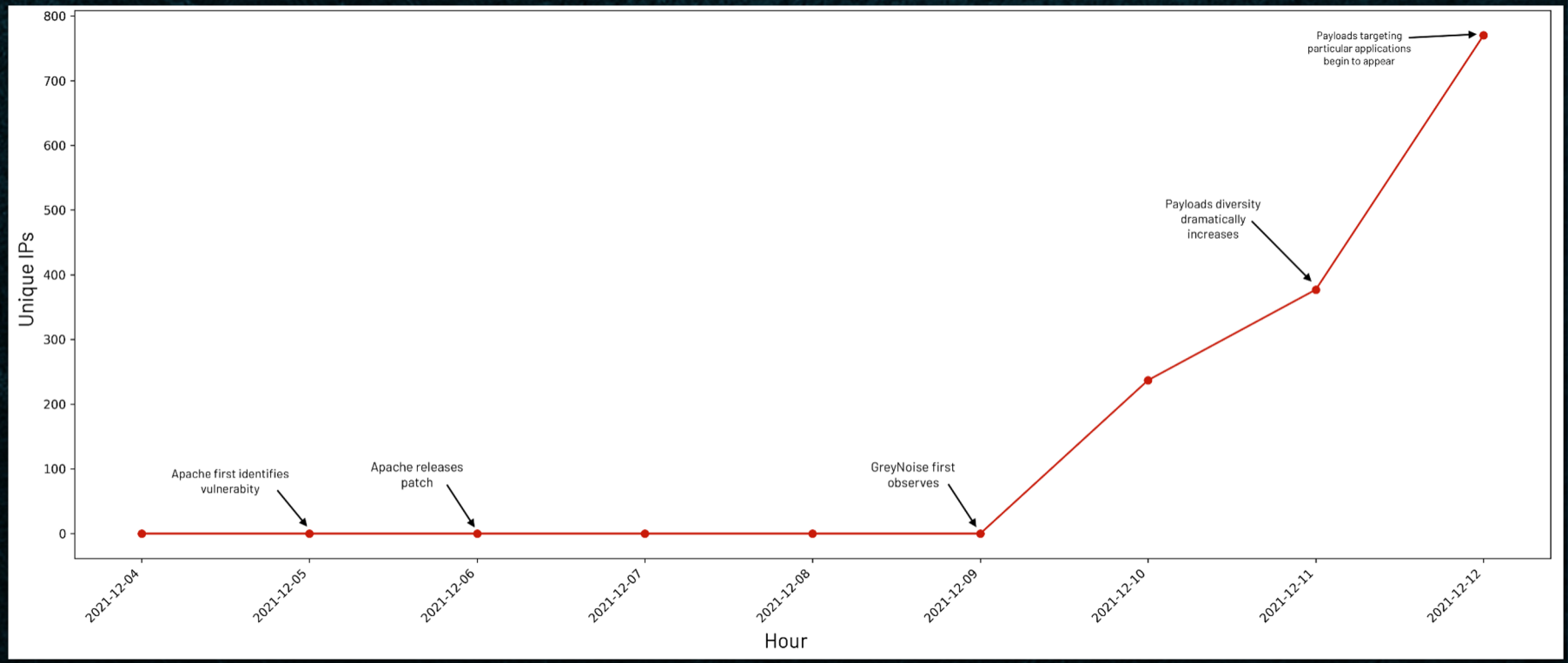




OPPORTUNISTIC EXPLOITATION/SCANNING IN LESS THAN 4 HOURS AFTER TOOLING RELEASED

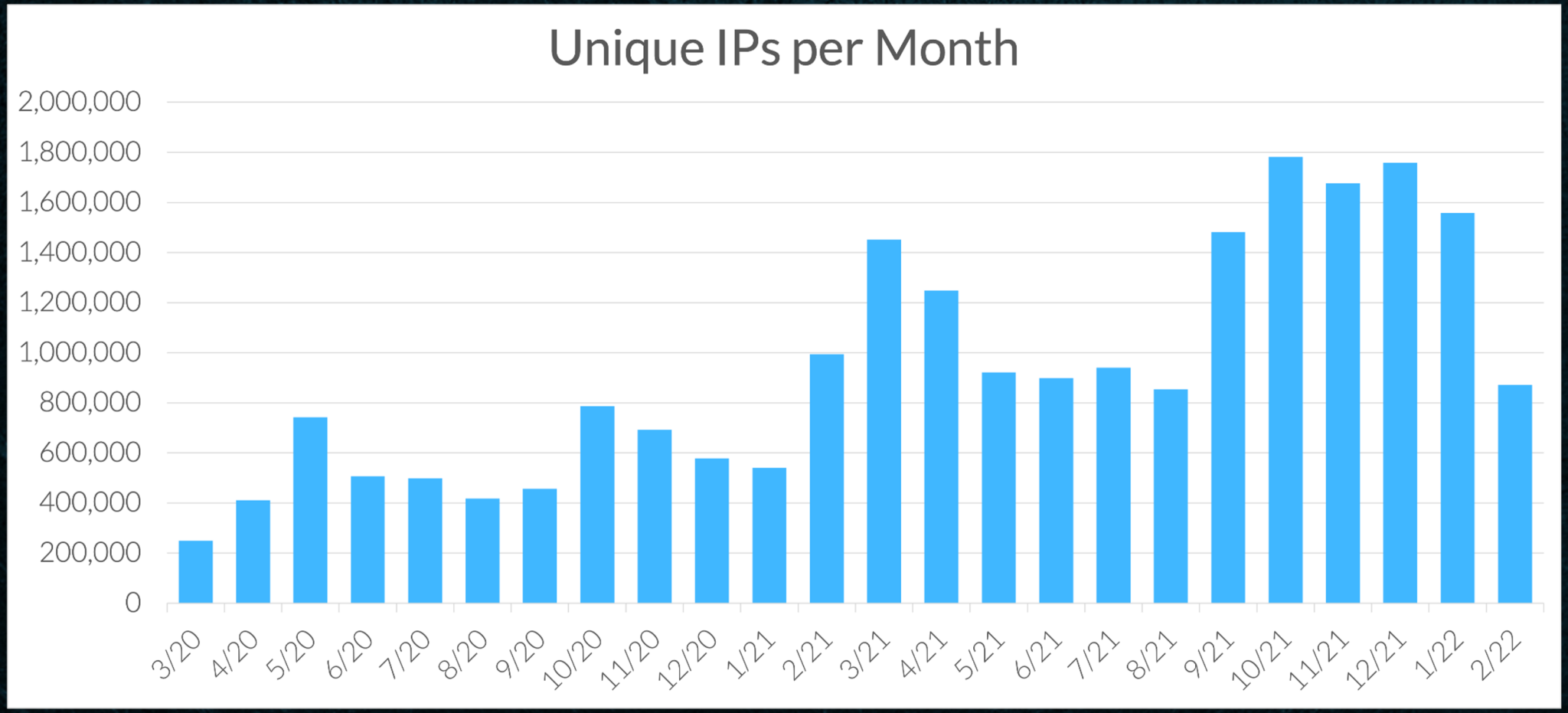
LOG 4J

- Interestingly, the first huge wave came from exclusively Tor nodes
- Most attempts at the start were just stuffing the Log4Shell string in random places.
- Shortly after, custom product-specific payloads

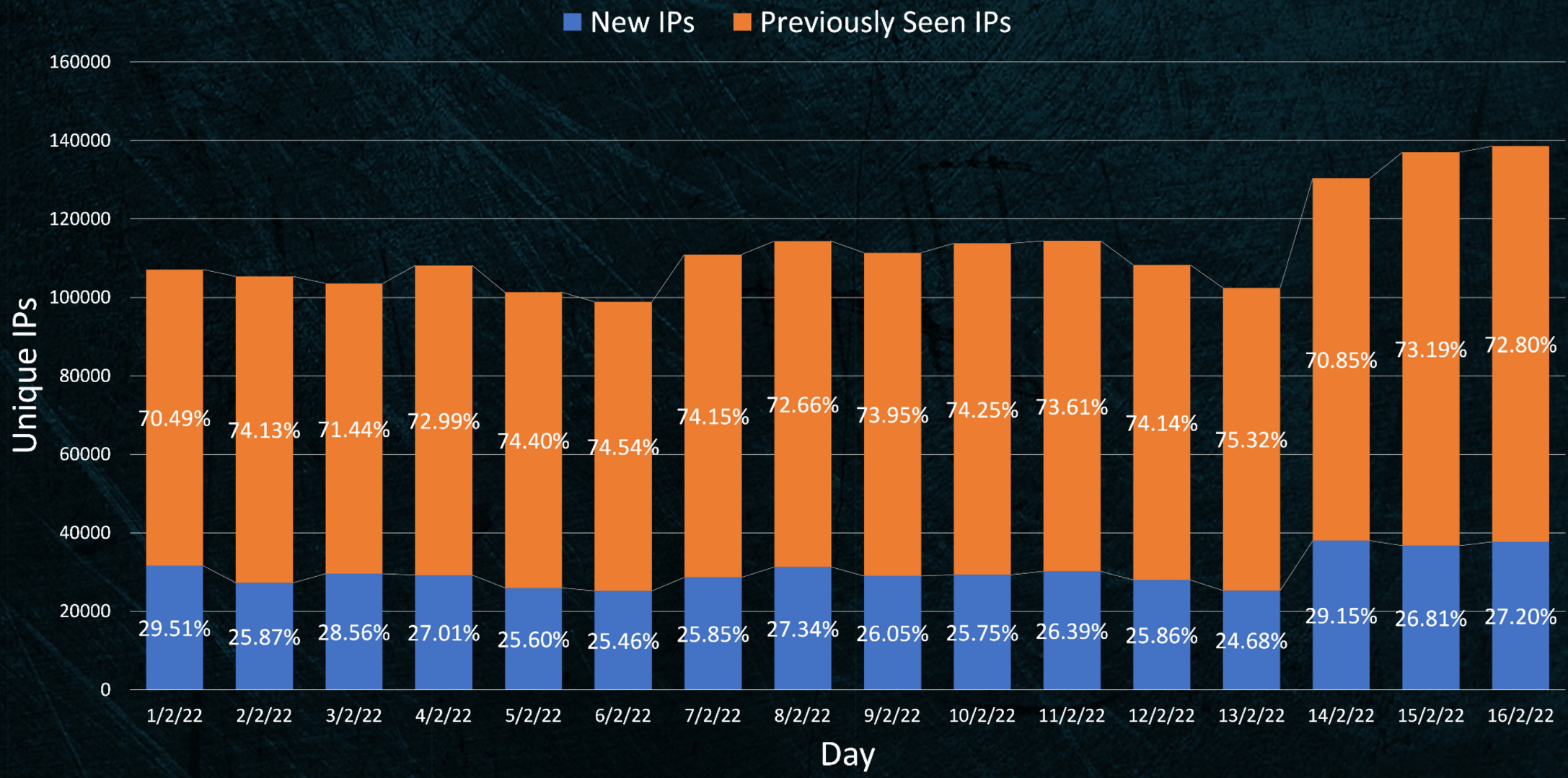


“scanning != exploiting” except when scanning == exploiting, like with Log4j

Security companies and researchers who exploit vulns with good intentions **make this worse** while trying to be helpful


Unique IPs per Month
2,000,000
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
3/20
4/20
5/20
6/20
7/20
8/20
9/20
10/20
11/20
12/20
1/21
2/21
3/21
4/21
5/21
6/21
7/21
8/21
9/21
10/21
11/21
12/21
1/22
2/22

Noise Floor


New IPs
Previously Seen IPs
160000
140000
120000
100000
80000
60000
40000
20000
0
Unique IPs
70.49%
74.13%
71.44%
72.99%
74.40%
74.54%
74.15%
72.66%
73.95%
74.25%
73.61%
74.14%
75.32%
70.85%
73.19%
72.80%
29.51%
25.87%
28.56%
27.01%
25.60%
25.46%
25.85%
27.34%
26.05%
25.75%
26.39%
25.86%
24.68%
29.15%
26.81%
27.20%
1/2/22
2/2/22
3/2/22
4/2/22
5/2/22
6/2/22
7/2/22
8/2/22
9/2/22
10/2/22
11/2/22
12/2/22
13/2/22
14/2/22
15/2/22
16/2/22
Day

On any given day, **73%** of IPs responsible for opportunistic scan/exploit noise were seen the day before.

Only **27%** are “new”.

WEIRD STUFF

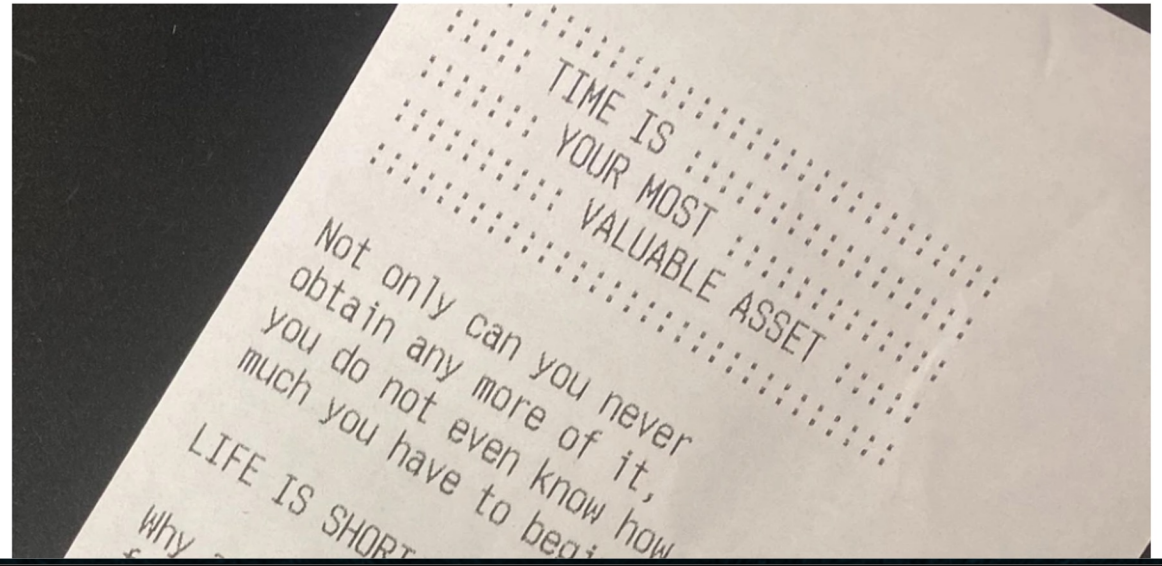
- Spoofed noise storms
- Bad guys acting like security companies that scan the internet
- Upstream blocks
- Just like bad guys, security companies think they're super sneaky 🤫
- Printjacking

Hackers Are Spamming Businesses' Receipt Printers With 'Antiwork' Manifestos

Dozens of printers across the internet are printing out a manifesto that encourages workers to discuss their pay with coworkers, and pressure their employers.

By Lorenzo Franceschi-Bicchierai

December 2, 2021, 11:17pm



FINAL THOUGHTS

BLOCKING NOISE

Whack-a-mole shows a surprising amount of promise

"WHACK A MOLE" EXPERIMENT

Hypothesis:

- Blocking extremely fresh internet background exploitation IPs will meaningfully increases the amount of time it takes for a vulnerable host on the internet to be compromised

Method:

- Stand up two identical vulnerable hosts, open to the internet, running poorly credentialed services
  - SSH and telnet
  - admin/aSdmin
  - root/admin
- Measure time to first compromise; total number of compromises

"WHACK A MOLE" RESULTS

Unblocked Host
Mean Time to Compromise

19 Minutes

- 32 compromises/day
- 206 compromise attempts/hour

Blocked Host
Mean Time to Compromise

4 Days 6 Hours

- 4 compromises/day
- 35 compromise attempts/hour

Tiny fast IP blocklists (whack-a-mole) are gross but they work better than you'd expect

STAYING AHEAD OF THE NEXT LOG4J

There is relatively little we can do to prevent the next Log4J, but we can make it suck less by centralizing information and providing ready-use real-time block lists

GreyNoise Community Trends

GREYNOISE TRENDS BETA

Apache Log4j RCE Attempt

TAG INTENT
Malicious

TAG CATEGORY
Activity

This IP address has been observed attempting to exploit CVE-2021-44228 and CVE-2021-45046, a remote code execution vulnerability in the popular Java logging library Apache Log4j. CVE-2021-44228 affects versions 2.14.1 and earlier, CVE-2021-45046 affects versions 2.15.0 and earlier.

CVEs:

CVE-2021-44228

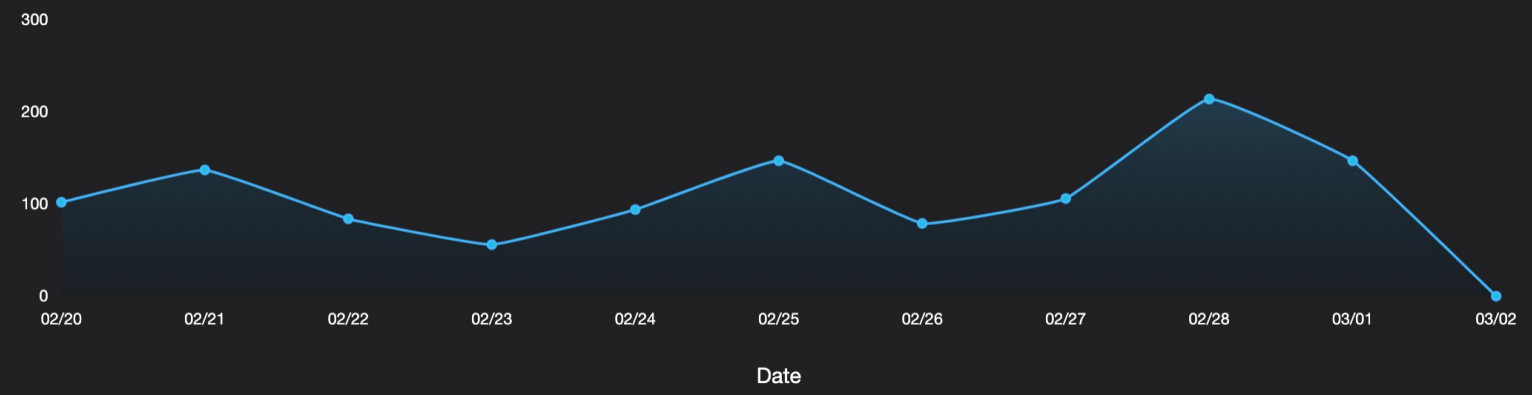
CVE-2021-45046

3 DAYS | 10 DAYS | 30 DAYS

Feb 20 2022 - Mar 02 2022

508

UNIQUE IPS OBSERVED BY GREYNOISE



Timeline

Sequence of recorded events

CVE-2021-45046 Published 2021-12-14 19:15 UTC

CVE-2021-45046 was published by MITRE

CVE-2021-44228 Published 2021-12-10 10:15 UTC

CVE-2021-44228 was published by MITRE

View Tagged IPs →

Actions

Manual

Download IP List

Automated

› Block at NG Firewall

Related Tags:

No related tags associated with this tag

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
- https://www.lunasec.io/docs/blog/log4j-zero-day/
- https://github.com/apache/logging-log4j2/pull/608
- https://www.lunasec.io/docs/blog/log4j-zero-day-severity-of-cve-2021-45046-increased/

[-]Show less

PRICING BLOG RESOURCES COMPANY

GREYNOISE Enter GNQL query... TODAY TAGS TRENDS ANALYSIS ALERTS ADMIN

GREYNOISE TRENDS BETA

Apache Log4j RCE Attempt

TAG INTENT
Malicious

TAG CATEGORY
Activity

This IP address has been observed attempting to exploit CVE-2021-44228 and CVE-2021-45046, a remote code execution vulnerability in the popular Java logging library Apache Log4j. CVE-2021-44228 affects versions 2.14.1 and earlier, CVE-2021-45046 affects versions 2.15.0 and earlier.

CVEs:
CVE-2021-44228
CVE-2021-45046

View Tagged

Actions

Manual

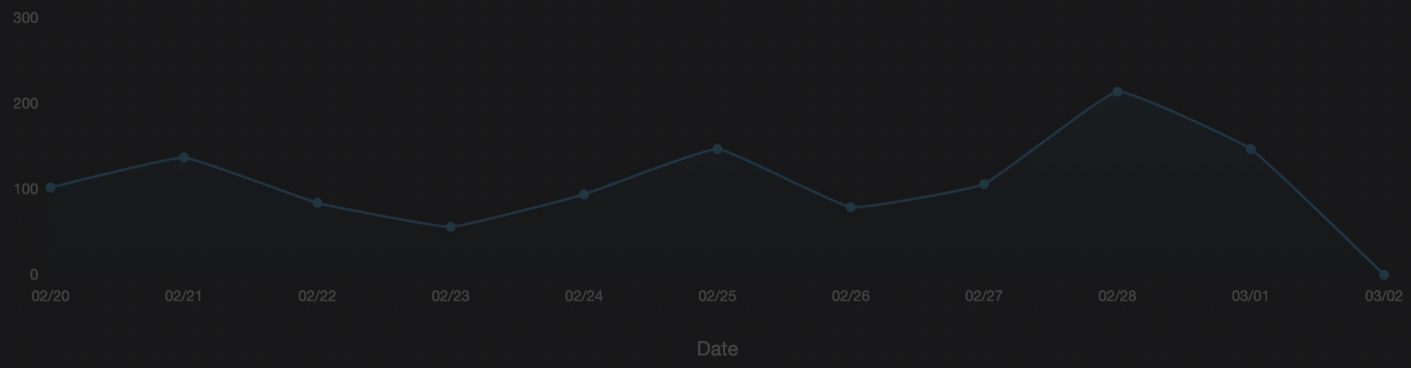
Download

Automated

Block at

3 DAYS 10 DAYS 30 DAYS Feb 20 2022 - Mar 02 2022

508
UNIQUE IPS OBSERVED BY GREYNOISE



Related Tags:
No related tag
tag

References:
- https://cve
e.cgi?name=
- https://cve
e.cgi?name=
- https://www
4j-zero-day
- https://git
g4j2/pull/6
- https://www
4j-zero-day
46-increase

[-]Show less

Timeline
Sequence of recorded events

CVE-2021-45046 Published 2021-12-14 19:15 UTC
CVE-2021-45046 was published by MITRE

CVE-2021-44228 Published 2021-12-10 10:15 UTC
CVE-2021-44228 was published by MITRE

GreyNoise Created Tag 2021-12-09 00:00 UTC
GreyNoise created the tag APACHE LOG4J RCE ATTEMPT and started monitoring for related activity

Block at Nex-Gen Firewall

The endpoint below returns a list that refreshes every hour and contains all of the IPs GreyNoise has seen with the “Apache Log4j RCE Attempt” tag in the last 24 hours. Paste this endpoint into one of the supported NGFWs below to automatically block traffic from tagged IPs.

Compatible Next-Gen Firewalls

paloalto NETWORKS cisco FORTINET

View Instructions

Blocklist URL

https://api.greynoise.io/v3/tags/80592a05-bbd6-4813

Copy

```
andrew@marathon ~ curl https://api.greynoise.io/v3/tags/80592a05-bbd6-4813-836d-9ef9f822e951/ips\?format\=txt
82.148.6.126
181.239.184.21
90.150.90.146
178.34.191.44
187.144.138.213
190.190.246.219
27.66.126.87
27.209.142.169
77.75.135.72
84.213.186.165
118.232.239.209
182.180.163.137
193.218.118.177
196.218.27.162
201.165.83.6
212.56.203.42
217.170.246.146
8.24.209.4
79.13.52.59
81.167.11.168
84.255.173.109
85.55.242.228
87.205.120.162
88.201.42.91
93.49.247.80
95.9.96.168
103.70.155.156
114.32.11.141
```

GREYNOISE COMMUNITY TRENDS

This is live right now:
https://greynoise.io/

CONCLUSION

- Internet mass exploitation is quantifiably getting worse. I expect this to continue.
- A huge, distributed, sensor system such as GreyNoise is effective at reducing opportunistic compromises
- Running this huge sensor network has challenges but they’re all addressable
- Instead of hoping another Big Bad Vuln doesn’t happen, let’s prepare for when it does

THANK YOU!