



GREYNOISE

2022


GREYNOISE 2022

Mass Exploitation Report



Contents

Introduction	<u>03</u>
2022 CISA Known Exploited Vulnerabilities Redux	<u>04</u>
A Look Back (And Forward) At Log4j	<u>10</u>
Atlassian Confluence Server and Data Center Vulnerability (CVE-2022-26134)	<u>14</u>
Apache Vulnerability	<u>15</u>
F5 Big IP iControl REST Authentication Bypass	<u>18</u>
Wrapping up 2022	<u>22</u>



Introduction

If you had been using GreyNoise in 2022, what mass exploits would you have known about in advance? That is the purpose of this report: to show you the hours saved, the data aggregated, and the research methodologies laid bare.

GreyNoise is a river of data. We divert its flow into streams and rivulets, lakes, and estuaries. Then, we give you those pools of data with labels and groupings, so you can understand the trends at which you're looking.

Here is the root of the problem: while many threat intelligence providers are great at cybersecurity, they are bad at providing data in a way that is useful for their customers. Based on inaccurate assumptions, the data provided by many threat intel solutions is of poor quality. Some products even lack the conviction to provide guidance on making automated block decisions based on their data. And if a machine can't use the data, how useful can it be?

Clearly, there are gaps in the industry, and the first-ever GreyNoise Mass Exploits Report is here to fill some of them.

At a high level, cyber threat intelligence is the craft of predicting what malicious actors are going to do on the internet – including how, why, and where

they will do their villainy. Unfortunately, most threat intelligence solutions have not delivered on their tradecraft. Within the wider cybersecurity community, threat intelligence is often seen as a commodity that brings unquantifiable business value...and uncertain security value. Over time, this formula has caused waning industry faith around the entire concept of threat intel.

That's why GreyNoise handles the data feeding threat intelligence differently. In this report, you'll find several sections covering some of the bigger mass exploitations of 2022, also known as celebrity vulnerabilities. We invite you to experience your year through the lens of the GreyNoise Research Team and see what 2022 would have looked like, had you been using our datasets to stay ahead of mass exploits on the internet.

//

2022 CISA Known Exploited Vulnerabilities Redux

author: "Bob Rudis"

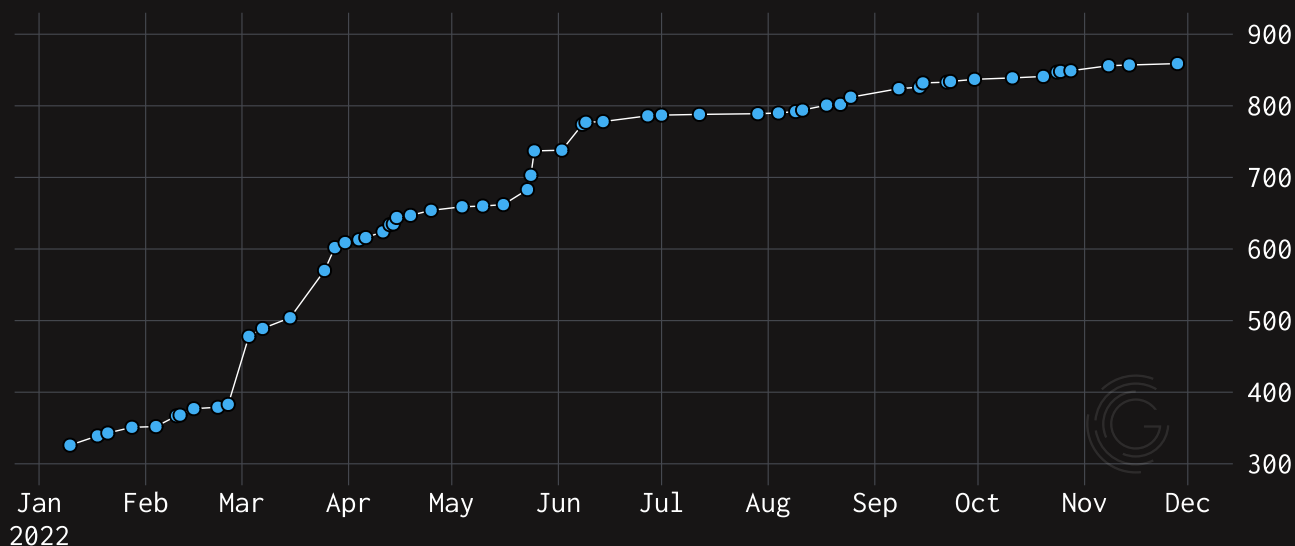
November 2022 marks the first anniversary of the U.S. Cybersecurity & Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) [Catalog](#). While mainly aimed at Federal agencies and critical infrastructure organizations, the KEV Catalog has become an authoritative source for vulnerabilities that have been (or are currently being) exploited in the wild. KEV entries are only made when a vulnerability meets all three criteria:

- It has an assigned [CVE ID](#);
- It is under active exploitation; i.e. there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner; and
- Clear remediation guidance exists.

In 2022, GreyNoise researchers released a [mid-year assessment](#) of the effectiveness of CISA KEV. We'll briefly revisit some of those assessments, check-in to see how the GreyNoise tag creation rate compares to CISA KEV releases, and provide some guidance on how to best keep an eye on actors exploiting KEV catalog CVEs using GreyNoise.

CISA Added 548 New CVEs Across 58 Releases to Their Catalog of Known Exploited Vulnerabilities in 2022¹

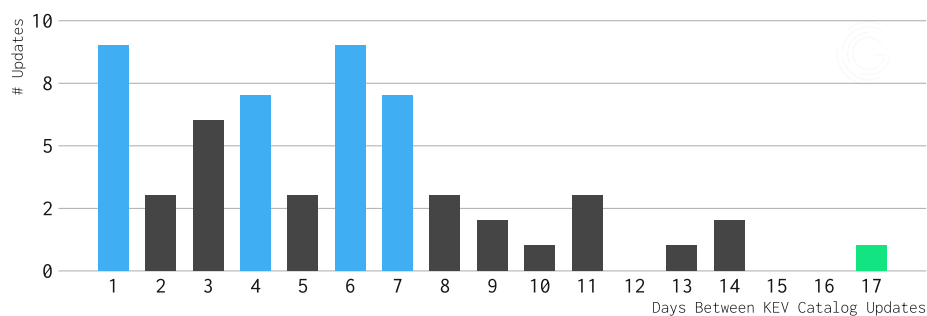
The addition of 226 CVEs in March was due, in part, to the war in Ukraine. A median of 36 CVEs were added monthly.



¹Chart spans January 1, 2022 through November 29, 2022

KEV: The defender's perspective

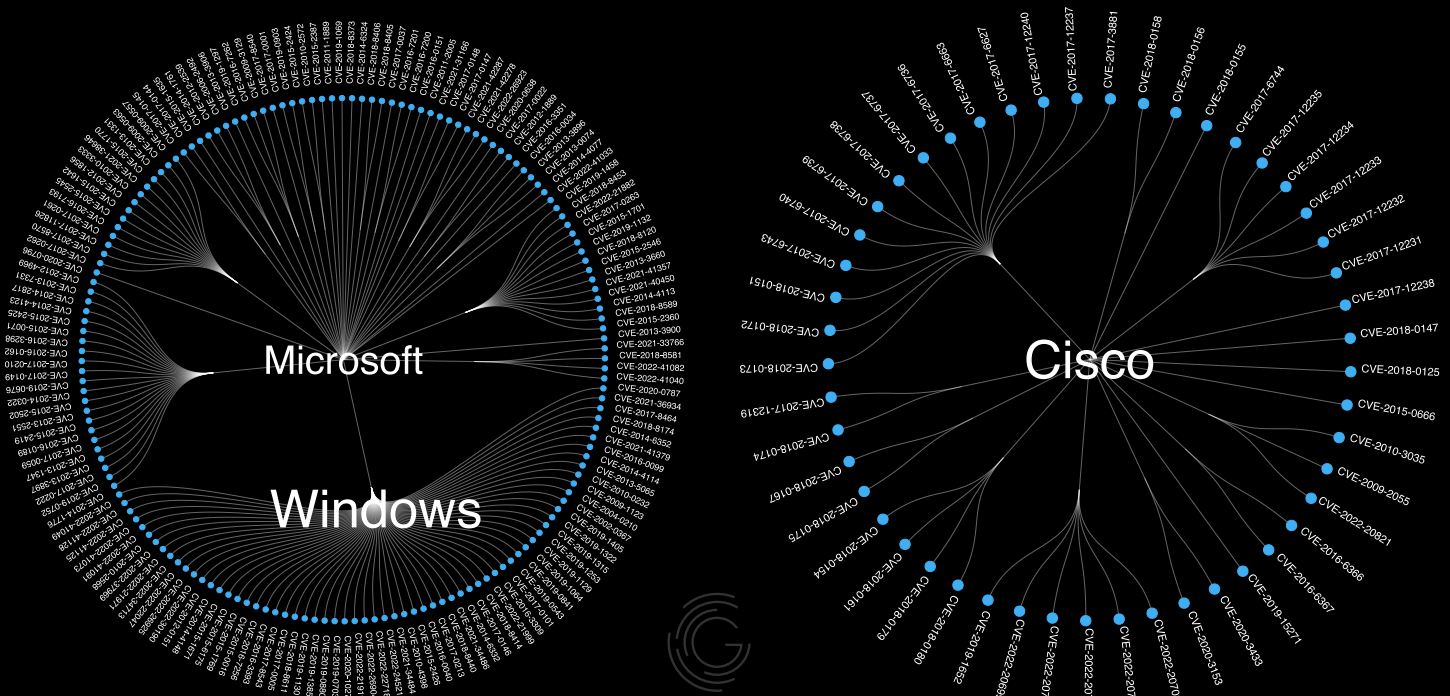
At most, defenders had seventeen days between KEV updates—and usually had to react to new releases every 4-7 days.



No Rest For The Weary

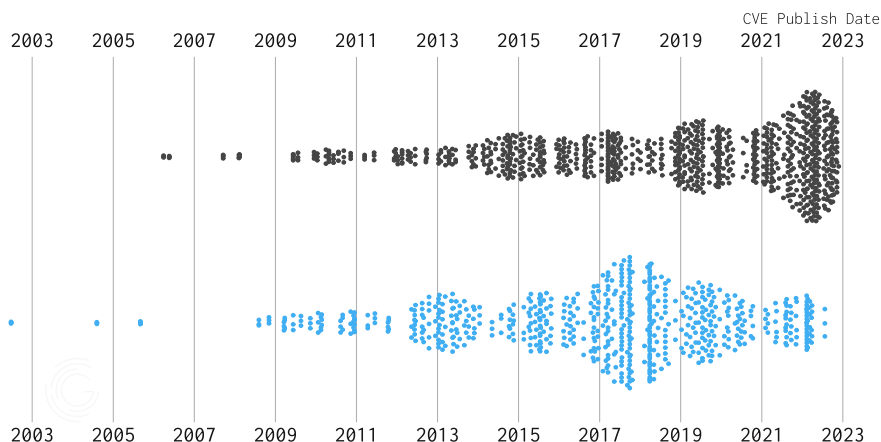
Defenders were nearly just as likely to have a single day's break between KEV Catalog updates as they were **4**, **6**, or **7**. The longest break was **17** days."

When updates happened, chances are they included actively exploited vulnerabilities in Microsoft, Adobe, Cisco, and Apple products; together, they accounted for over 50% of KEV CVEs to date in 2022:



2022 has been a year full of surprises, paramount of which is the Russian aggression against Ukraine. It's worth noting, as CISA's March 2022 KEV update is heavily weighted toward vulnerabilities that nation-state actors have been known to exploit in key business, government, and critical infrastructure environments.

- The chart below shows:
- The distinction between March and the rest of the year (through October 14, 2022); and
- Just how old CVEs that make it into the KEV catalog can be.



Older Vulnerabilities Remain Prominent In KEV Updates

Due to the special nature of the March 2022 KEV updates, we've split them out and associated them with the [Russian aggression against Ukraine](#). When we compare the recency of CVE publish dates by either the traditional release group or the special one, both show that the vast majority (94%; 77%) are still vulnerabilities older than the current year.

Ninety-four percent of the CVEs in March's KEV came out before 2022 (and many were published in the previous two decades). The same can almost be said for the remainder of the 2022 KEV catalog editions.

In summary:

- Keen defenders had to deal with a KEV alert on an almost weekly basis in 2022.
- The aggression against Ukraine added many legacy vulnerabilities and the increased threat of nation-state actors into organization threat models.
- Popular enterprise software, across many versions, made regular appearances, forcing defenders to triage KEV lists against known installed software.

As a result: GreyNoise stands by its original B-/C grade evaluation of CISA's KEV from June. Far more context should be provided, plus tracking proof points beyond "we saw it in a vendor report" will allow defenders to better prioritize remediation efforts.

How Does GreyNoise Stack Up?

GreyNoise has tags for 100 CVEs in the 2022 component of the KEV catalog. KEV CVEs without tags are ones where we would not see internet-facing remote exploit attempts (though there are a tiny number of KEV CVEs we're in the process of developing tags for).

Out of these 100 CVEs, GreyNoise tag creation beat CISA's CVE updates 60% of the time, and we tied these updates 5% of the time.

You can now search GreyNoise by CVE and set up [GNQL queries](#) like [this one we recently published](#) that covers CISA's [published list](#) of the top CVEs most used by Chinese state-sponsored attackers. Defenders can then use the pristine block lists (updated by the hour) to either remove the noise before it has a chance to reach them, or filter out the noise from events and alerts, saving time and enabling teams to focus on patching and remediation efforts.

//

A Look Back (And Forward) At Log4j

author: "Bob Rudis"

It seems like years since the [Apache Log4j vulnerability](#) ruined holiday vacations for countless cybersecurity and information technology professionals. At the writing of this report, we approach the one-year anniversary of a formerly invisible software component making headline news and causing very real problems for many organizations throughout 2022. A seemingly innocuous feature request added a dynamic variable lookup capability to this open-source logging library; failure in threat-modeling opened the exploit door to even the lowest of adversaries. Upon learning of weakness, attackers of all skill levels began their inventory and compromise attempts with great haste. GreyNoise researchers have chronicled the world of Log4j throughout 2022, even dedicating three blog posts to the subject itself:

- 2021-12-10: [Trending: Apache Log4j Vulnerability](#)
- 2022-01-18: [Log4j Analysis: What to Do | Cybersecurity Blog | GreyNoise](#)
- 2022-08-30: [GreyNoise | Analysis and review of CISA's Log4j report](#)

While the full scope of attacks involving the Log4j weakness will never be known, there have been many high-profile ones, including campaigns against governments, financial institutions, and regionally targeted organizations. Furthermore, Log4j weakness exploits have made their way into many kits, including those used by ransomware attackers:

- 2021-12-21: [Hackers Exploit Log4j Flaw at Belgian Defense Ministry](#)
- 2021-12-29: [Fintech firm hit by Log4j hack refuses to pay \\$5 million ransom](#)
- 2022-01-11: [APT35 exploits Log4j vulnerability to distribute new modular PowerShell toolkit](#)



- 2022-06-21: [Avos ransomware group expands with new attack arsenal](#)
- 2022-08-25: [MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations](#)
- 2022-09-08: [North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies](#)

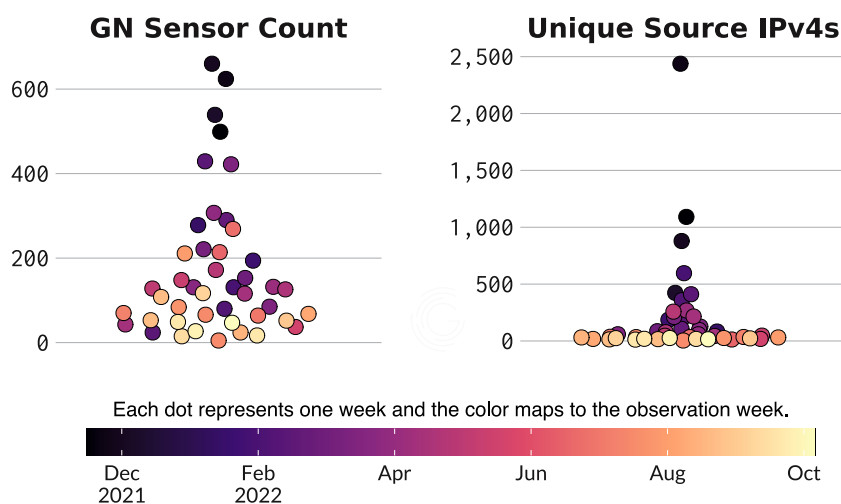
GreyNoise sensors began seeing exploit attempts on December 9, 2021. The chart below shows weekly measurements of three characteristics of Log4j exploit traffic:

- **QN Sensor Count:** The number of GreyNoise sensors seeing Log4j traffic in a given week. We have thousands of IPv4 addresses distributed across the “geographic” internet. Interactions with any given IP address are handled by a cluster of honeypot sensor nodes. At Log4j’s peak, virtually all of our sensors saw exploit attempts.
- **Total Log4j Interactions:** When threat hunting in the [GreyNoise Visualizer](#), the focus is on unique IP addresses, since those are what you need to act on when defending your organization. This “total interaction” statistic shows how many total Log4j exploit attempts we saw across all sensors in a given week. Peak Log4j traffic saw nearly one million exploit attempts.
- **Unique Source IPv4s:** Attackers need infrastructure to target internet hosts. As noted in the previous bullet, you are exposed to unique source counts directly in the GreyNoise Visualizer, but are limited to just 30 days of history. The final chart panel shows the entire history of weekly Log4j infrastructure counts.

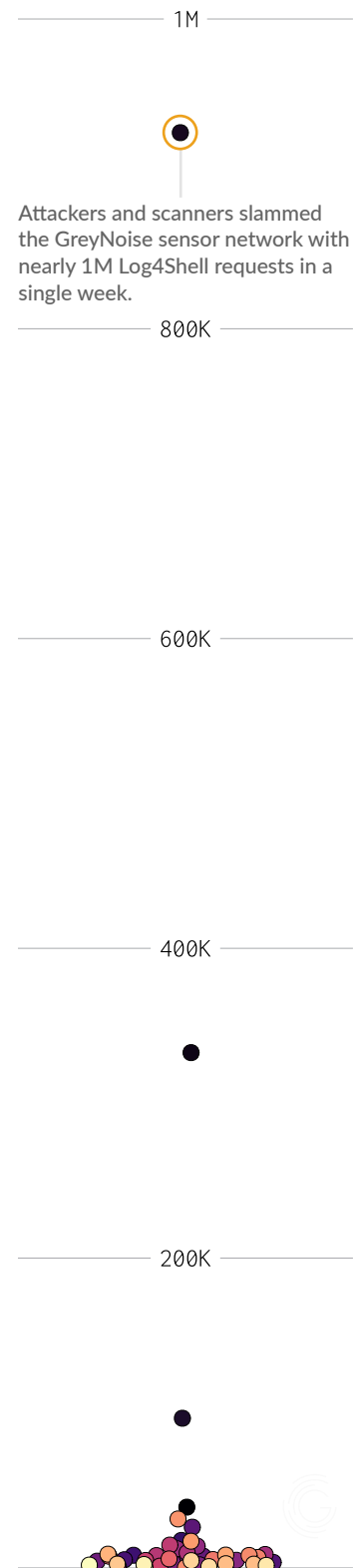
All three charts use color to indicate time. The darker the color, the further back in time the measurement was taken. After the first few weeks of activity: Log4j attacker traffic settled into familiar background patterns, with occasional spikes as adversaries attempted to find new targets.

Log4j Shed Some Opportunistic Luster In 2022

While capable adversaries stealthily used Log4j exploits successfully throughout 2022, the brunt of opportunistic activity came in December 2021 and January 2022, with activity mostly tapering off to the same background noise levels as other vulnerabilities.



Total Weekly Sensor Network Interactions



The three-dimensional, connected scatterplot (below) shows the same information as the two-dimensional panel chart (above). 3D charts aren't always easy to navigate, but this one makes it easier to see the initial upward progression across all three measurements in the first few weeks, followed by a steady downward trend. The spike anomalies are also easier to make out in this view.

What does the Log4j outlook look like for defenders in 2023? Well, as the [Yogi Berra](#) quote goes, "It's tough to make predictions, especially about the future." Nonetheless, we'll give it a go.

♦ **Expect daily, persistent internet-facing exploit attempts.** We see Log4j attack payloads every day. It's part of the new "background noise" of the internet, and the exploit code has been baked into numerous kits used by adversaries of every level. It's very low risk for attackers to look for newly- or re-exposed hosts, with the weakness unpatched or unmitigated. This means organizations must continue to be deliberate and diligent when placing services on the internet.

♦ **Expect more post-initial access internal attacks.** CISA's [database of software affected by the Log4j weakness](#) stopped receiving regular updates earlier this year. The last update showed either "Unknown" or still "Affected" status for ~35% (~1,550) of products cataloged. Attackers know what existing products have embedded Log4j weaknesses, such as the popular [VMWare Horizon](#), and have already used the exploit in ransomware campaigns. If you have not yet dealt with your internal Log4j patching, now would be a good time to get that into Q4 2022 and H1 2023 plans.

♦ **Expect at least a handful of headline-grabbing Log4j-centric attacks.** Organizations have to strive for perfection, while attackers need only persistence and luck to find that one device/service still exposing this weakness. We will see more organizations impacted by this, and it is vital you do what you can to ensure yours isn't one of them.

Defenders can keep an eye on [Apache Log4j RCE Attempts](#) with a free GreyNoise account. Use our hourly updated, finely honed block lists to filter the Log4j noise and keep a watchful eye on targeted/anomalous Log4j log entries from both internal and external systems. You can also use our new [Trends](#) feature to see if Log4j activity is on the rise.

//

Atlassian Confluence Server and Data Center Vulnerability (CVE-2022-26134)

author: "Matthew Remacle"

On 2-Jun-22, Atlassian [released a security advisory](#) to address a remote code execution vulnerability (CVE-2022-26134) affecting all supported versions of Confluence Server and Data Center products. An unauthenticated, remote attacker could exploit this vulnerability to execute code remotely by using [Object Graph Navigation Library](#) (OGNL).

OGNL is a flexible expression language, which quickly became problematic for defenders in the early days of this vulnerability. The use of OGNL allowed attackers to use clever encoding/decoding to evade detection.

```
/%24%7b%28%23%61%3d%40%6f%72%67%2%61%70%61%63%68%65%2e%63%6f%6d%6d%6f%6e%73%2e%69%6f%2e%49%4f%55%74%69%6c%73%40%74%6f%53%74%72%69%6e%67%28%40%6a%61%76%61%2e%6c%61%6e%67%2e%52%75%6e%74%69%6d%65%40%67%65%74%52%75%6e%74%69%6d%65%28%29%2e%65%78%65%63%28%22%65%63%68%6f%20%4f%45%42%63%6c%78%39%53%44%4e%22%29%2e%67%65%74%49%6e%79%75%74%53%74%72%65%61%6d%28%29%2c%22%75%74%66%2d%38%22%29%29%28%28%40%63%6f%6d%2e%6f%70%65%6e%73%79%6d%70%68%6f%6e%79%2e%77%65%62%77%6f%72%6b%2e%53%65%72%76%6c%65%74%41%63%74%69%6f%6e%43%6f%6e%74%65%78%74%49%67%65%74%52%65%73%79%6f%6e%73%65%28%29%2e%73%65%74%48%65%61%64%65%72%28%22%48%6f%73%74%22%2c%23%61%29%29%7d%

/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang
.getRuntime().exec("echo OEBc1x9SDN").getInputStream(),"utf-8"))
.(@com.opensymphony.webwork.ServletActionContext@getResponse()
.setHeader("Host",#a))}/
```

GreyNoise observed 850 unique IPs attempting to exploit this vulnerability within the first 4 days. Our Blocklist (<https://viz.greynoise.io/tag/atlassian-confluence-server-cve-2022-26134-ognl-injection-attempt?days=3>) provided a way for analysts to instantly exclude and block IPs attempting to exploit this vulnerability across the internet, instead allowing defenders to focus on payloads specifically targeting their organization.

While the majority of attackers were observed leveraging an off-the-shelf proof of concept of the exploit, we also saw a significant number of obfuscated variants: payloads attempting to circumvent detection and defensive technologies such as web application firewalls. Through the use of similarity hashing, we also clustered and grouped all exploits to keep our customers and community up to date on the newest obfuscation techniques and payloads observed in the early days of this celebrity vulnerability. These resources were released for free through our [Datashots API](#), including a [PDF](#) containing relevant samples to aid analysts in recognizing obfuscated payloads.

These two features reduced alert fatigue and enabled analysts to quickly and confidently investigate anything targeting their organization.

Because of the valuable information often contained in Confluence (like documentation and credentials), this vulnerability continues to be a high-value target for attackers. We still see a steady baseline of exploitation attempts even four months later, as well as anomalous spikes in exploit activity on our [GreyNoise Trends](#) page:

//



Apache Vulnerability

author: "Brianna Cluck"

On October 4, 2021, Apache disclosed a [path traversal vulnerability](#) CVE-2021-41773 that affects HTTP Server version 2.4.49. The vulnerability was introduced in this version (2.4.49), then was patched in version 2.4.50.

On October 3, 2021, at 08:44 UTC, GreyNoise observed the first scan for this vulnerability from 36.68.53.196. This predates the mailing list announcement from Apache on October 5 as well as the [release of 2.4.50](#) on October 4, but after the [patch](#) was committed on September 29, 2021.

Since that time, we've seen 1,464 examples of traffic that match attempts to exploit this vulnerability coming from a number of sources.

What have we learned since then?

There is a spike in activity after a vulnerability disclosure

When polling data from October 2021, we see ~34 unique hits checking for this vulnerability. Data from September 2022 shows six unique hits, demonstrating both how a vulnerability can become less noisy over time (as the chances of exploitation are lower due to patching), and the importance of gathering data long-term to get the big picture. What might seem like no big deal because it was quiet for one month may turn out to be a persistent campaign over several months.

Total activity increases over time

In 2021, the highest number of hits from one unique domain was 106 hits. In 2022, the highest number of hits was 982. That's almost 10 times as many hits. However, let's break down the top number of hits per month.

In 2021, GreyNoise had around three months of data to work with for this vulnerability, and we saw just around 35 hits per month. In 2022, we (as we penned this report) have had nine months of data and saw nearly 110 hits per month: a ~3x bump in exploitation attempts. Such an increase in exploitation is interesting, and shows that a vulnerability can become more popular over time through word of mouth and by finding useful proof of concept code. A contributing factor to this 2022 increase is the proliferation of easy-to-use exploit scripts written in popular language, such as Python and Ruby. The Ruby script is especially interesting, having been released earlier in 2022 and is ready-made to be turned into a Metasploit module.

Exploitation becomes less unique and more focused

It is important to remember that DNS information can be spoofed. But let's look at something that can't be spoofed; what payloads did we see when this vulnerability was initially announced?

Here's the data from 2021:

```
+-----+
| payloads                                                                 |
| /.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/var/www/html/index.html |
| /.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/var/www/html/index.html |
| /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh |
| /img/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd |
| /global-protect/login.esp/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/var/www/html/index.html |
| /uploads/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd |
| /assets/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd |
| /.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/var/www/html/index.html |
| /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd |
| /image/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd |
| /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2ebin/bash |
| /icons/.%2e/.%2e/.%2e/.%2e/_%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd |
+-----+
```

It's interesting to note the plurality of paths being used. When a vulnerability is announced, there's not a lot of great information about how exactly to exploit it yet, so we often see people trying any possible paths.

Also of note in the 2021 data: the number of different files being read. People are trying to open bash and sh shells and read the passwd file on the server. This is indicative that somebody is trying to exploit the machine. What does this look like in 2022? Let's take a look:

```
+-----+
| payloads                                                                 |
| / %2e/%2e/ %2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/var/www/html/index.html |
| / %2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/var/www/html/index.html |
| /global-protect/login.esp/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/.72e/.72e/%2e/%2e/%2e/%2e/var/www/html/index.html |
| / %2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/%2e/var/www/html/index.html |
+-----+
```

In 2022, the variety in the number of paths being tried is reduced to two, and all of them seem to point back to /var/www/html/index.html. This would indicate two things: the community has a greater understanding of which paths work, and more people are scanning for the vulnerability (or at least cleverly disguising themselves as just scanning) as opposed to trying to send file commands to any machine they can find running Apache.

Where do we go from here?

Frequently, as soon as these exploits are patched, new exploits develop to work around the patched vulnerability. Considering the popularity of Apache server software, there are new vulnerabilities being found and exploited all the time...all while the Apache developer team races to patch. Over time, we may see a number of exploits that are functionally similar enough to this vulnerability that we could collate them into a single tag (example: see our HTTP request smuggling tag). Until that time, though, the GreyNoise Research Team will continue to monitor this specific vulnerability and report our findings.

//

F5 Big IP iControl REST Authentication Bypass

CVE-2022-1388 - A Cybersecurity Hype Cycle Story

author: "Kimber Duke"

GreyNoise customers and community members use our data to determine if internet-wide mass exploitation of a particular vulnerability is actively occurring. Labeling a vulnerability as "mass exploitable" in the wild is often the magic keyword that skyrockets awareness and launches a vulnerability to the top of your list of priorities. We provide ground truth information that naturally disrupts or suspends the vulnerability "hype cycle" caused by such language.

Our Research Team proposes a theory regarding the hype cycle around "celebrity vulnerabilities," which affect many internet-facing enterprise-level devices that are relatively trivial to exploit.

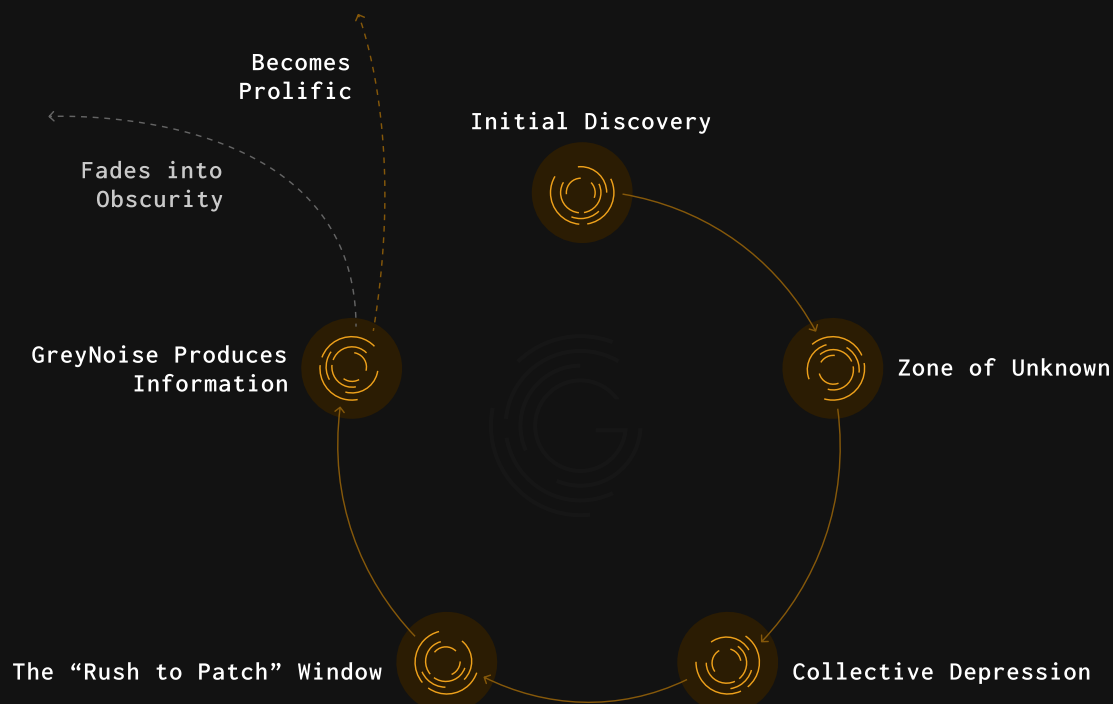
1. **Initial discovery** – This looks like an official security advisory, a post on social media, a blog, or a source that effectively says, "This is going to result in a major CVE that causes root access to enterprise technology." In the worst case scenario, this looks like somebody dropping proof of concept for a zero-day and therefore has no patch issued to fix the vulnerability.
2. **Zone of Unknown** – This makes everybody prepare for the worst. The number of social media posts, news articles, and potential silence from vendors causes confusion as everyone looks for facts to know how bad the situation is. Researchers are scrambling to get the right versioning and patch diffs, perhaps even checking [Censys](#) or [Shodan](#) for how many devices may be affected by the exploit.
3. **Collective Depression** – This occurs when nobody can produce a working proof of concept. The outcomes are still unknown. The cybersecurity collective begins



to acknowledge the severity level of the situation due to the large number of internet-facing devices that are vulnerable to attack. The fact that we can “easily” measure the potential attack surface, and know that effective attack mitigations are generally possible, further drives practitioners into despair. The truth is, many organizations have difficulty securing resources or lack sufficient expertise or buy-in to perform updates or mitigations, and then become unlucky victims of ransomware or persistent malicious behaviors. Even worse, there may be no patch or effective mitigation to solve the problem until hours/days after the initial knowledge drop. This era of the cycle often leads to assuming the worst will happen. We often see the most misinformation during this phase; often false GitHub postings proliferate to profit off uncertainty. Administrators and security engineers become desperate for information in this phase and may often fall victim to scams.

4. **GreyNoise Produces Information** – Our research team has service-level agreements with themselves regarding trending events. We try to insert ourselves into the hype cycle the moment we can confirm information that identifies actors attempting to exploit vulnerabilities. We comb our historical data sets to see if we find anything matching the potential paths of the exploit. As soon as we have enough knowledge to produce a tag, we start tagging IPs that attempt to exploit the vulnerability at scale.
5. **The Rush to Patch Window** – As the proof of concept code makes its way through

Celebrity Vulnerability Hype Cycle



the community, GreyNoise continues to observe all associated activity. We see mainstream adoption into script kiddie culture become prevalent. GreyNoise sees the POC code evolve into multiple paths of exploit opportunities. The code can continue to develop into a multitude of scripts and variations. The primary objective for the community at this time is to patch their devices ASAP.

6. **Fade into obscurity or become prolific** – There are only two outcomes from a hype cycle event – the technique becomes an obscure and niche use in situations where devices aren't properly maintained or secured, or becomes a prolific and constant source of noise on the internet.

Let's examine one of the best examples of a classic hype cycle detected by GreyNoise: the tale of CVE-2022-1388, an [F5 Big IP](#) iControl REST Authentication Bypass. The consequences can be brutal whenever an authentication bypass emerges—especially on network hardware. Network hardware has internet-facing endpoints that provide simple initial access to an enterprise. On the F5 Big IP iControl in particular, this was a [REST](#) authentication bypass, which raised concern levels due to the lack of authentication involved.

- **Initial Discovery** – Thanks to people who pay attention to updates and security alerts released on network enterprise hardware, the GreyNoise Research Team heard rumblings of F5 support publishing an article regarding a security advisory. F5 issued an [official security advisory](#) on May 4, 2022. The advisory stated, “Undisclosed requests may bypass iControl REST authentication.” Since the advisory officially issued the words authentication bypass, this escalated the severity of the issue and factored into the amount of hype received.
- **Zone of Unknown** – Though the vulnerability was assigned CVE-2022-1388, F5 distributed no further information about potential exploitation paths. Multiple researchers had theories about what this would look like – and our research team set up monitoring on the F5 REST API paths to detect any new changes. We also pulled historical data on these paths to verify if we had seen any potentially related behavior. There was a spike of data that looked similar - but ended up being a past vulnerability on the paths.
- **Collective Depression** – As the gap in time between a published security advisory and a proof of concept based on a patch diff increased, the uncertainty of the consequences grew. The large amounts of social media posts and articles speculating on the manner grew. False GitHub postings were seen and quickly removed due to their pleas for cryptocurrency trades in exchange for the supposed exploit script.
- **GreyNoise Produces Information** – by Saturday, May 7th, we were able

to publish a tag based upon a [proof of concept from Horizon3](#). Information sharing in the research community allows us to be ahead of mass exploitation, assuring our tags are issued quickly and efficiently to help inform the internet at large.

- **The Rush to Patch Window** – Unfortunately, there may have been multiple companies that had to weekend-patch this one – proof of concept exploits for this vulnerability were out on Twitter by Monday morning, May 9, 2022. Those who patched before news broke on social media were safe.
- **Potential for becoming prolific?** – On May 10th, there were claims of mass exploitation of this vulnerability, including the `rm -rf` statement, which could potentially wipe portions of the configuration of the device. GreyNoise did not see any traffic that would account for this behavior on a mass exploitation scale – though targeting F5 devices more specifically could account for this but would not account for a large scale.

Eventually, the hype slowly dissipates. This vulnerability stayed in the news for a long time, yet frequently has no results in the last 30 days of traffic, unlike the approximately 120 IPs seen per 30 days on the Log4j tag.

When a new hype cycle starts, the GreyNoise Research team is first and foremost responsible for fact-finding and providing authoritative data on what is true about the vulnerability. The cybersecurity community as a whole, with a common goal of enthusiastic and factual information-sharing, can keep the hype cycle focused on solving the problem of mass exploitation forever.

//

Wrapping up 2022

As the chart on the following pages shows, the volume and velocity of both legitimate and merely annoying celebrity/critical vulnerabilities continues to increase with nearly each passing year. This puts significant pressure on resource-strapped defenders and IT teams in every industry sector.

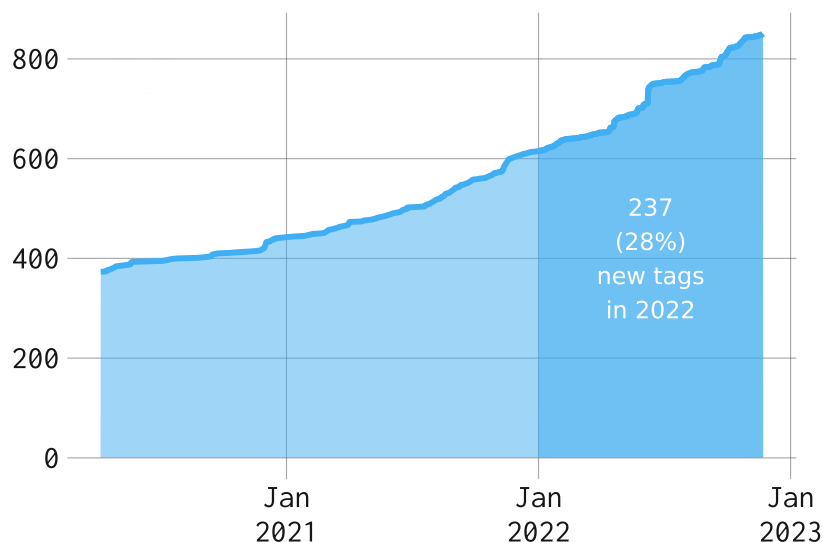
With GreyNoise, you can:

- accelerate alert triage and hunting
- defend against mass exploitation
- automate alert reduction

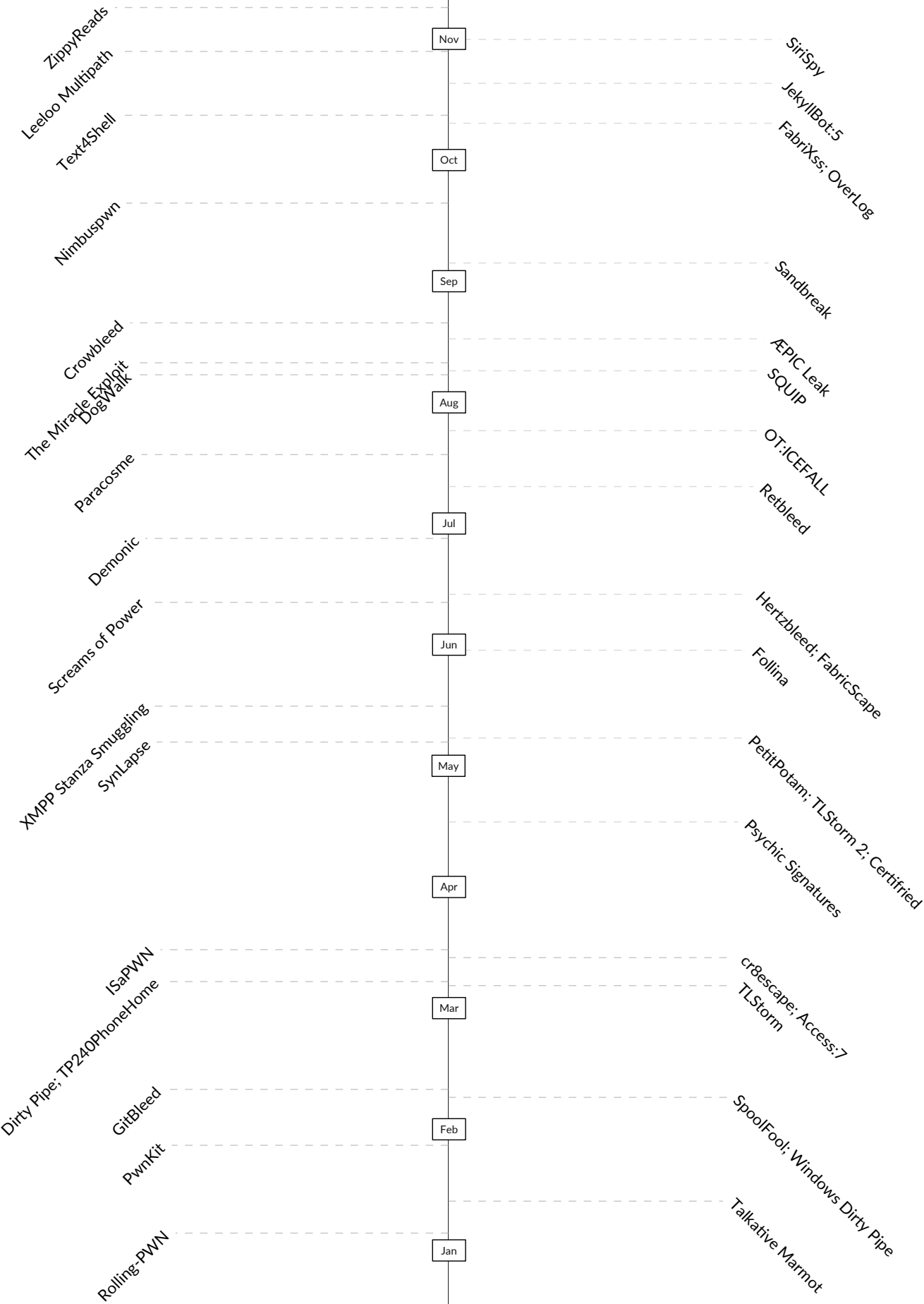
and gain the fastest and clearest insights into the relevance of emergent vulnerabilities, letting you focus on what matters most to your organization. [Sign up](#) for a free account or [request a demo](#) today!

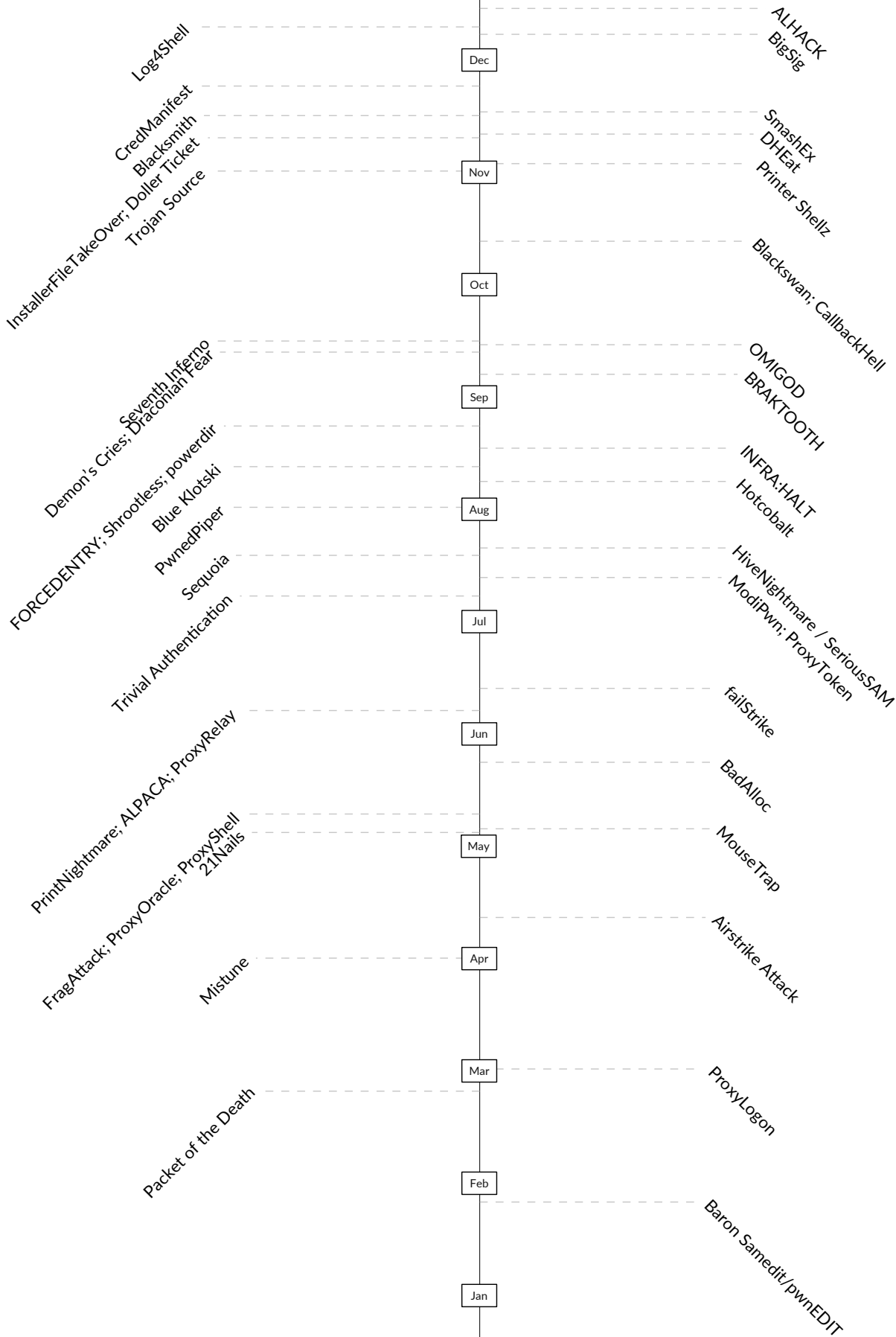
When new vulnerabilities emerge, organizations need timely guidance they can rely on, and intelligence they can both trust and use to make critical decisions. Whether it be legacy, known, actively exploited in-the-wild vulnerabilities (e.g. CISA's KEV Catalog) or emergent, critical flaws in ubiquitous services or devices (e.g. Atlassian Confluence, Apache httpd, F5 BigIP, or hidden components such as Log4j), GreyNoise has the most comprehensive coverage of, and the widest lens on malicious and benign activity — 820 tags as of this report writing date covering known actors and internet-capable exploits.

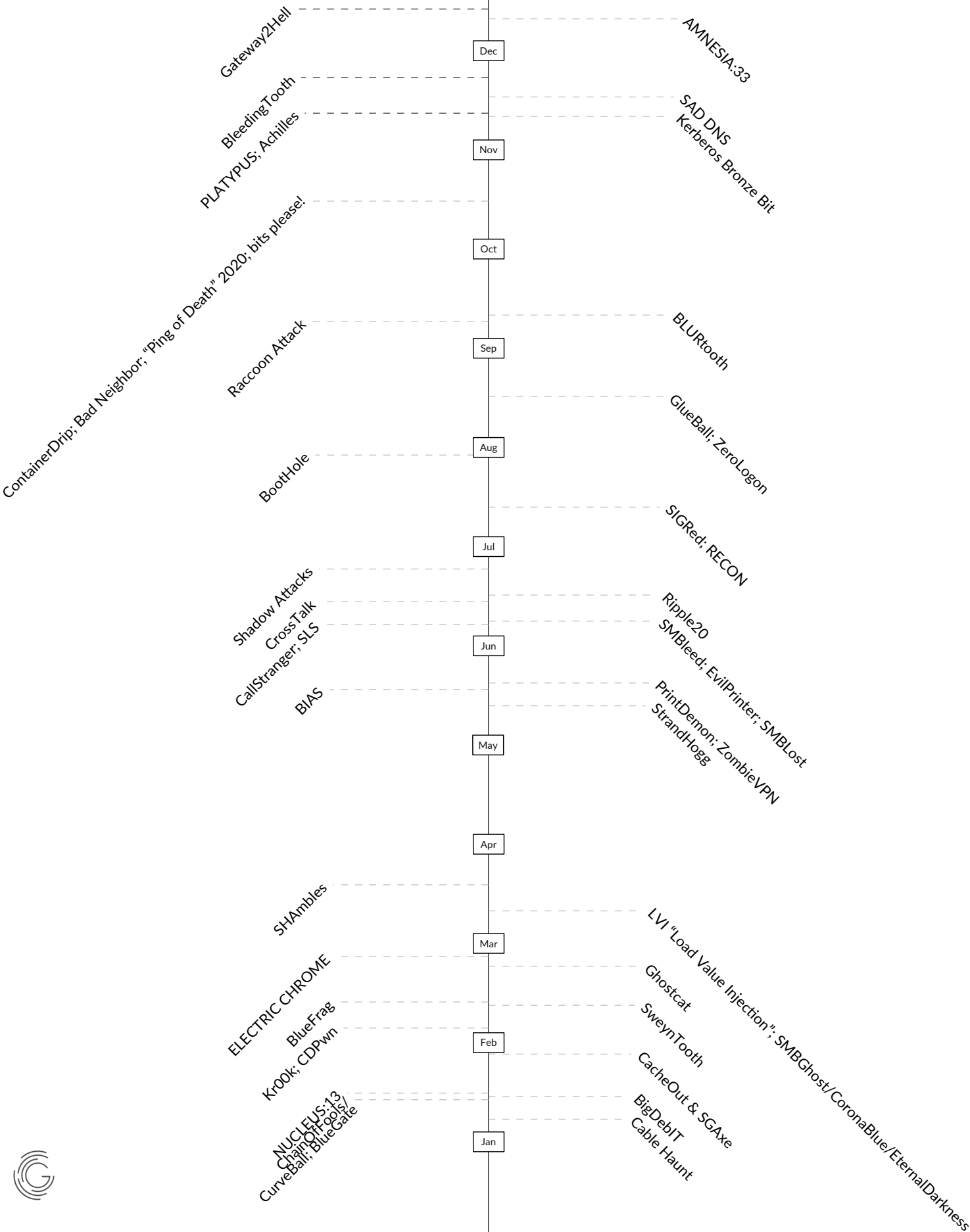
//

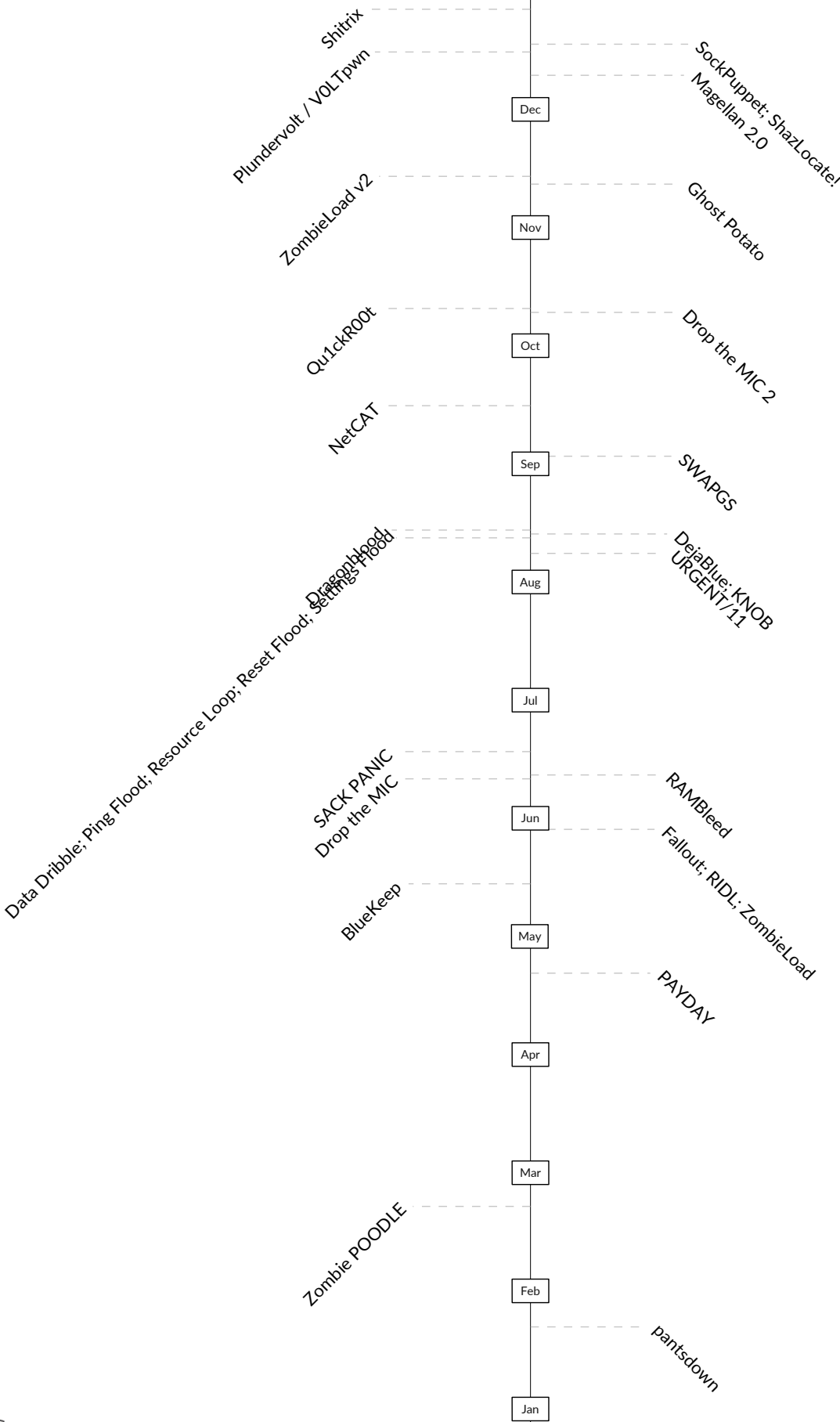


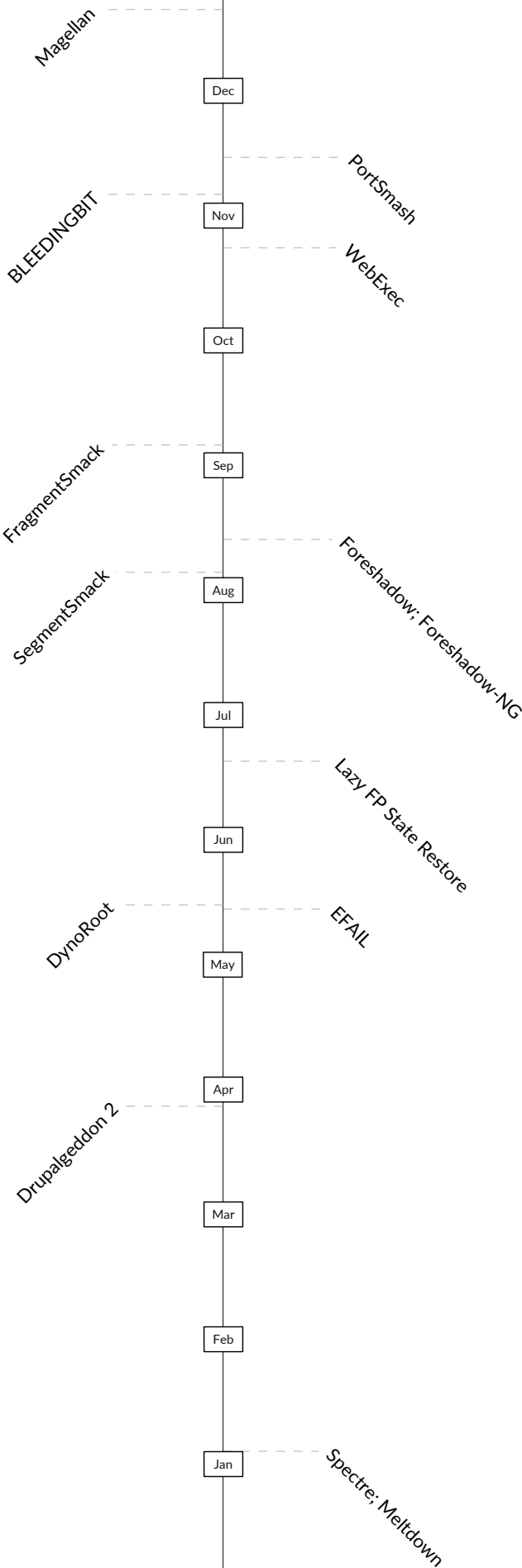
GreyNoise Researchers
Have Created 850
Tags Since We Started
Observing Internet Noise

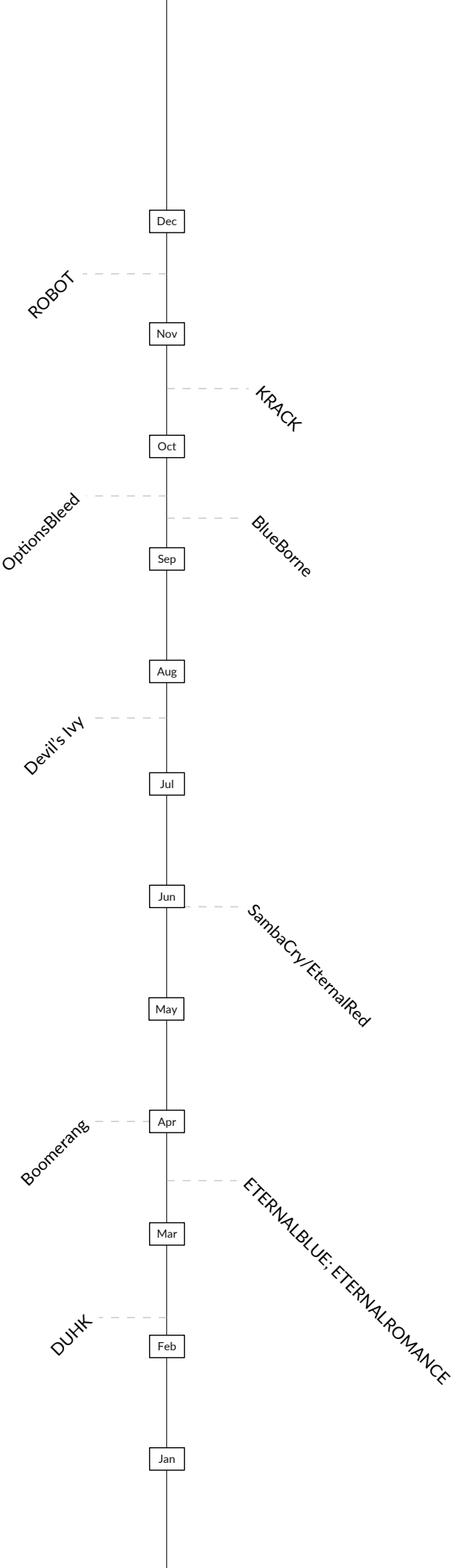


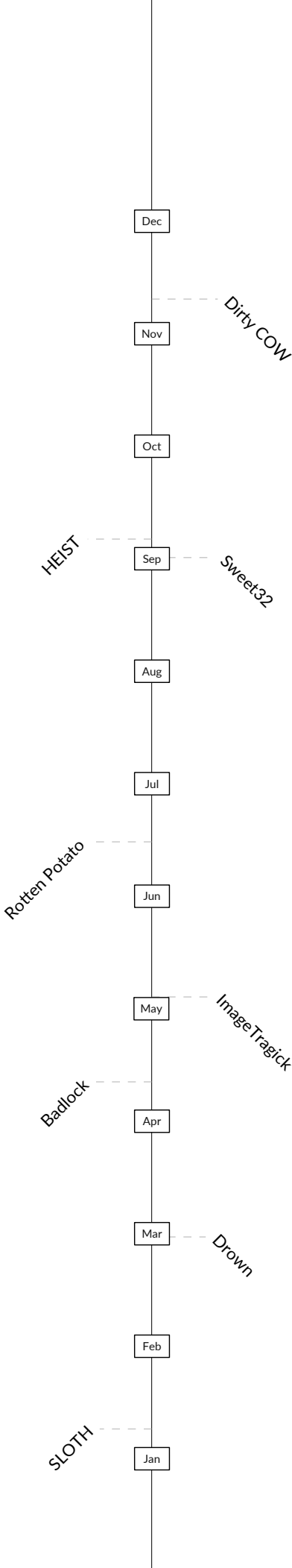


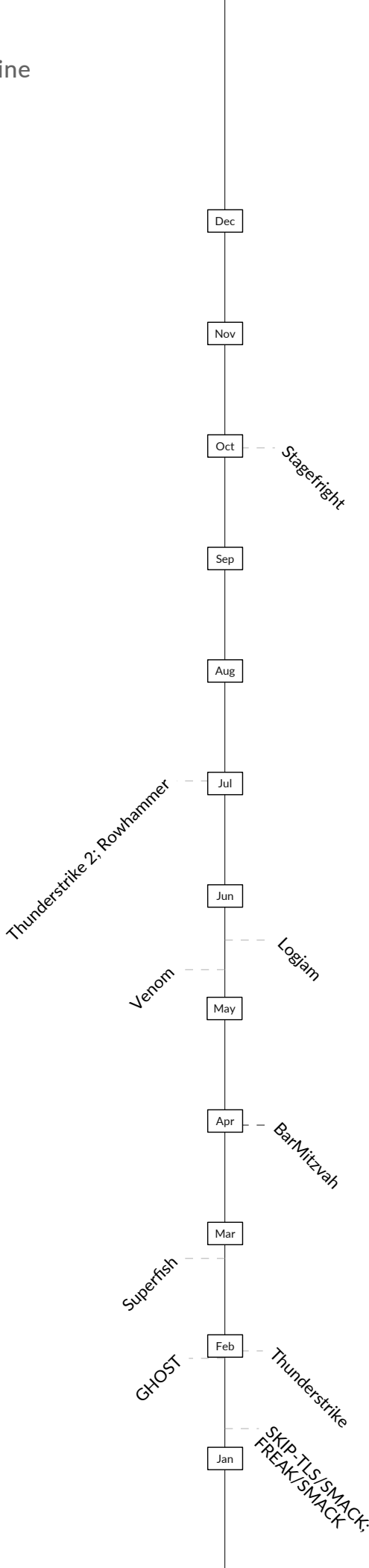


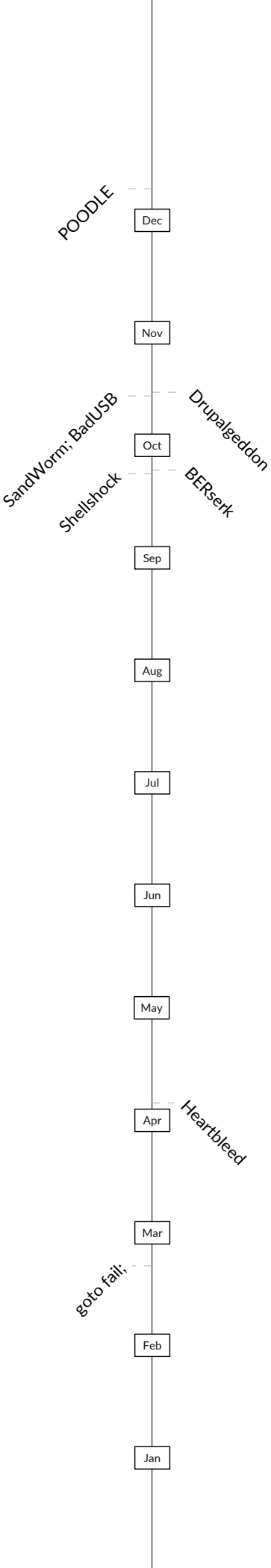












Dec

Nov

3SHAKE

Oct

Sep

Aug

Jul

Cookie Cutter

Jun

May

Apr

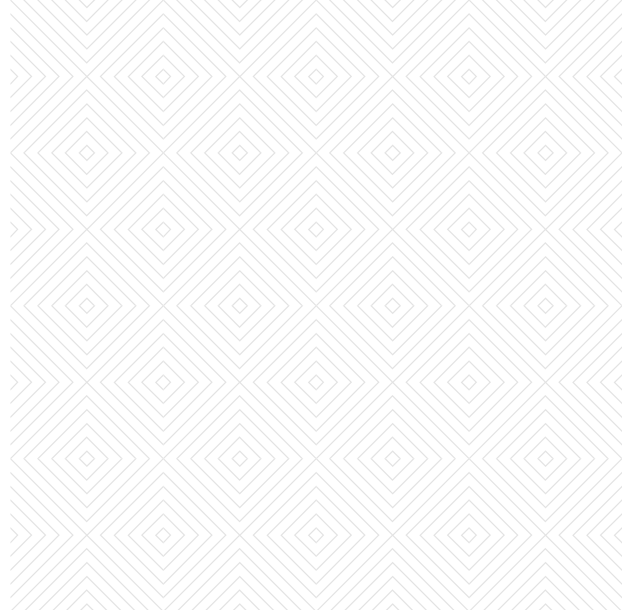
Mar

Feb

Lucky Thirteen

Jan





2022 – A Year of Mass Exploits

December 2022

Authors

Brianna Cluck, Kimber Duke, Nathan Thai, Matthew Remacle, Bob Rudis

Production

Carrie Landry, Gala Aranaga, Austin Price, Donna Becarra

About GreyNoise

GreyNoise helps security teams focus on threats that really matter, and ignore the ones that don't. We collect, analyze and label data on IP addresses that scan and attack the entire internet, saturating security teams with alerts. This unique perspective helps analysts focus their time on targeted and emerging threats, and waste less time on irrelevant or harmless activity.