WHITE PAPER

Geopolitical Cyber Event Prediction

Using Reverse Attack Surface Analysis to read adversary intent in the domain registration record.

vigilocity.com

Second edition · 2026 · Originally published 2023

Nearly every campaign that ends in a stolen credential, an encrypted network, or a defaced narrative begins the same way: someone registers a domain. Phishing pages, dropper sites, command and control, decoys, hop points. The domain comes first, and it leaves a record. This paper describes how Vigilocity reads that record at global scale, and what it looked like when we did, across more than twelve million registrations observed between January 2020 and March 2023. The case studies are reproduced from our original 2023 report, with the platform captures that documented them. The tradecraft they illustrate has not gone out of date; if anything, the intervening years have confirmed it.

01 Introduction

Analysis of internet domain registrations has become one of the more reliable ways to understand what nation-state adversaries and criminal groups are doing, and sometimes what they are about to do. The methods these actors depend on are scalable and disposable by design, and domains are the disposable part: cheap to buy, easy to abandon, and hard for a targeted organization to police without a serious intelligence apparatus behind it.

Ransomware is the loudest example of where this leads. WannaCry infected machines in more than 150 countries in 2017 and did billions of dollars of damage[1]; REvil's attack on Kaseya turned one vendor compromise into a supply chain event that touched hundreds of businesses. But ransomware, and the wiperware that increasingly travels with it, cannot begin until the actor is inside somebody's network. Phishing and spear-phishing are how they get there, and both run on freshly registered domains. A campaign impersonating the World Health Organization in 2020 harvested credentials on exactly this model.

The registration is also where these operations are weakest. A nation-state registering a look-alike of a legitimate organization is telling you something about its plans. A criminal group registering variations on a corporate name is telling you who qualifies as a worthy target in its eyes. Cybersquatting and trademark abuse sit on the same spectrum, with their own costs in reputation, legal fees, and lost revenue. All of it starts with a purchase that lands in a public record.

02 What registration data can and cannot do

Registration analysis has a track record. WannaCry's perpetrators were run down in part through the registration details of the domains that spread the malware[1]. The JabberZeus botnet, over a million machines strong, was dismantled in 2019 after the U.S. Department of Justice worked outward from a seized domain's registration[2]. The Emotet takedown in 2021 leaned on the same discipline. Correlating a domain's registrant, hosting, and IP history is how an analyst turns one bad domain into a map of related infrastructure, and it is often perceived as useful mainly for attribution, the *who*. In our experience it is at least as valuable for the *what*, the *how*, and the *when*.

The limits are real, and worth stating plainly. Registration data is frequently wrong, incomplete, or deliberately falsified. Sophisticated actors delay registering some infrastructure until a campaign is well along, precisely to starve early detection. And privacy protection services, which mask a registrant's identity for a few dollars, have eroded the naive version of this analysis badly. Investigations built on registration data alone go cold. Those obstacles are what pushed us toward an asymmetric approach.

03 Methodology: Reverse Attack Surface Analysis

Vigilocity's methodology is called Reverse Attack Surface Analysis, or RASA. The premise fits in one question: if an adversary were going to attack us, what infrastructure would they need, where would it come from, and when would it appear? RASA works from the attacker inward and rests on six pillars:

01	Critical time-series analysis
02	Geopolitical tension and event analysis
03	Attack surface risk profiling and rating
04	Indexing of historical global domain registration data
05	Ingestion of real-time global domain registration data
06	Correlation with open and closed source threat indicators

RASA is a close cousin of adversarial infrastructure analysis, but it admits evidence that infrastructure analysis usually leaves out: signs of the actor's intention, and of their planned and active targets. It also pays deliberate attention to the places where an actor's operational security is sloppy, because a single reused email address or moniker can blow open an investigation in directions nobody planned for. Above all, indexing the registration record over time gives a linear view of the geopolitical landscape as it is expressed in infrastructure: the intentions, plans, and actions of individuals, organizations, and governments, and the odds that they overlap.

None of this runs on intuition. The findings that follow are quantitative, and each one surfaced as an outlier that was visible in the data before anyone went looking for it. When a finding fires, the responses available are concrete: sustained surveillance of the actor, takedown of the infrastructure, security control changes, and law enforcement notification. What this report set out to show in 2023, and still shows, is a series of actual events that could have been blunted, and in some cases prevented outright, had action been taken on these findings at the time.

04 The observational record, 2020 to 2023

The analysis window for the original report ran from January 1, 2020 through March 18, 2023. In that window we indexed over **12 million domains** registered by more than **4 million registrants** across nearly **360,000 cities**.

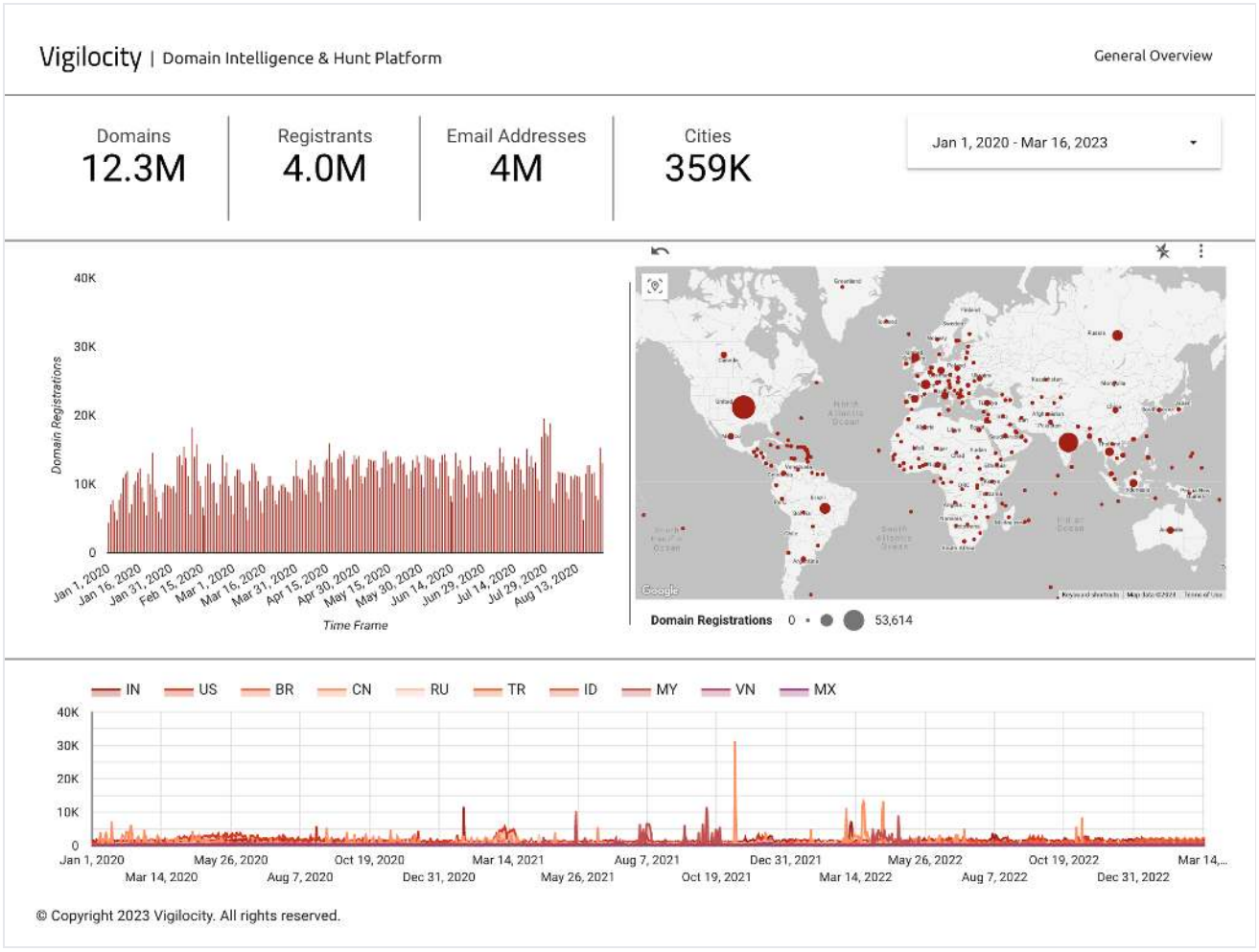

FIG. 1 Domain registration sparkline articulating registrations from the top 10 countries, January 1, 2020 through March 16, 2023.

Colorized by registrant country, the daily registration volume shows several outliers that need no statistical training to spot. The spikes worth pulling on cluster around November 2021, April 2022, and November 2022. Each turned out to reward the attention.

CASE · NOVEMBER 1 TO 7, 2022

Emerging phishing and influence infrastructure

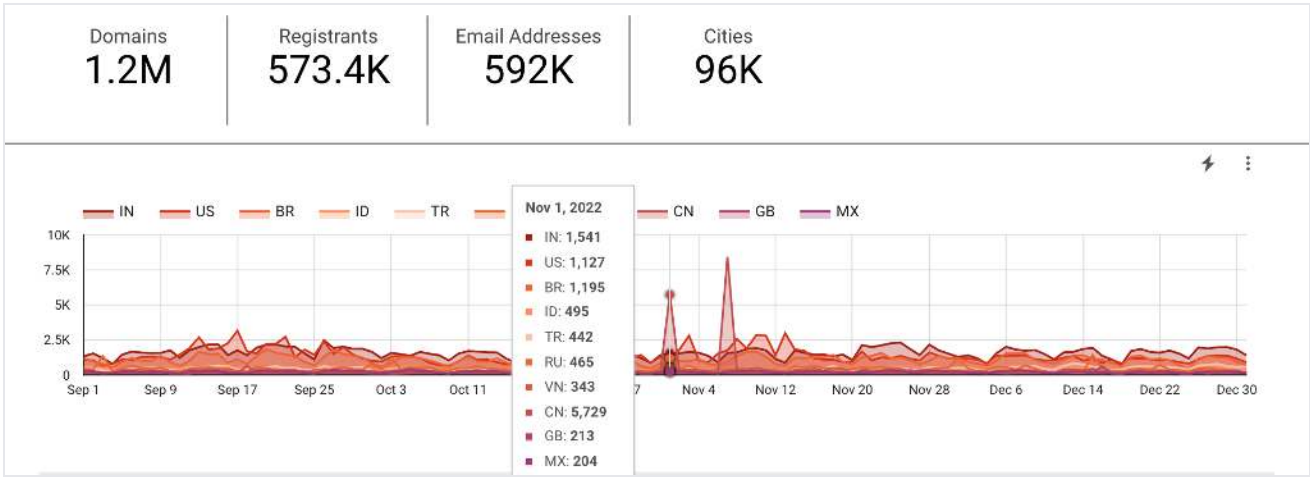

FIG. 2 Domain registrations on November 1, 2022: 5,729 attributed to Chinese registrants in a single day.

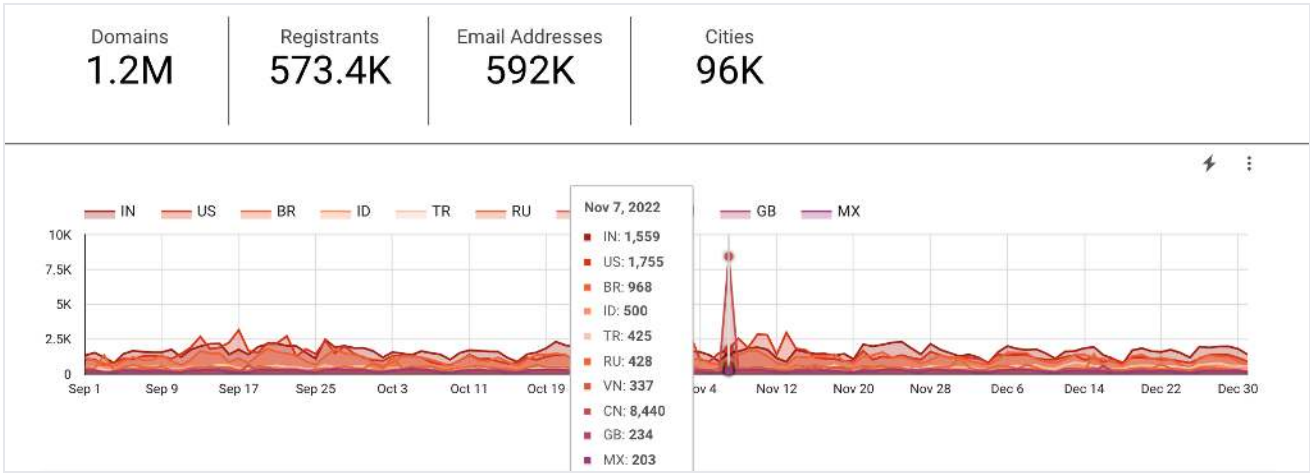

FIG. 3 Domain registrations on November 7, 2022: another 8,440 in one day, same origin.

On November 1, 2022, Chinese actors registered 5,729 domains. Six days later they registered another 8,440. Together that is more than **14,000 domains** in two spikes, bought by **66** and **63** registrants respectively. By any standard that is a large number of domains for a small number of buyers, and malicious or not, it suggests a well-funded operation.

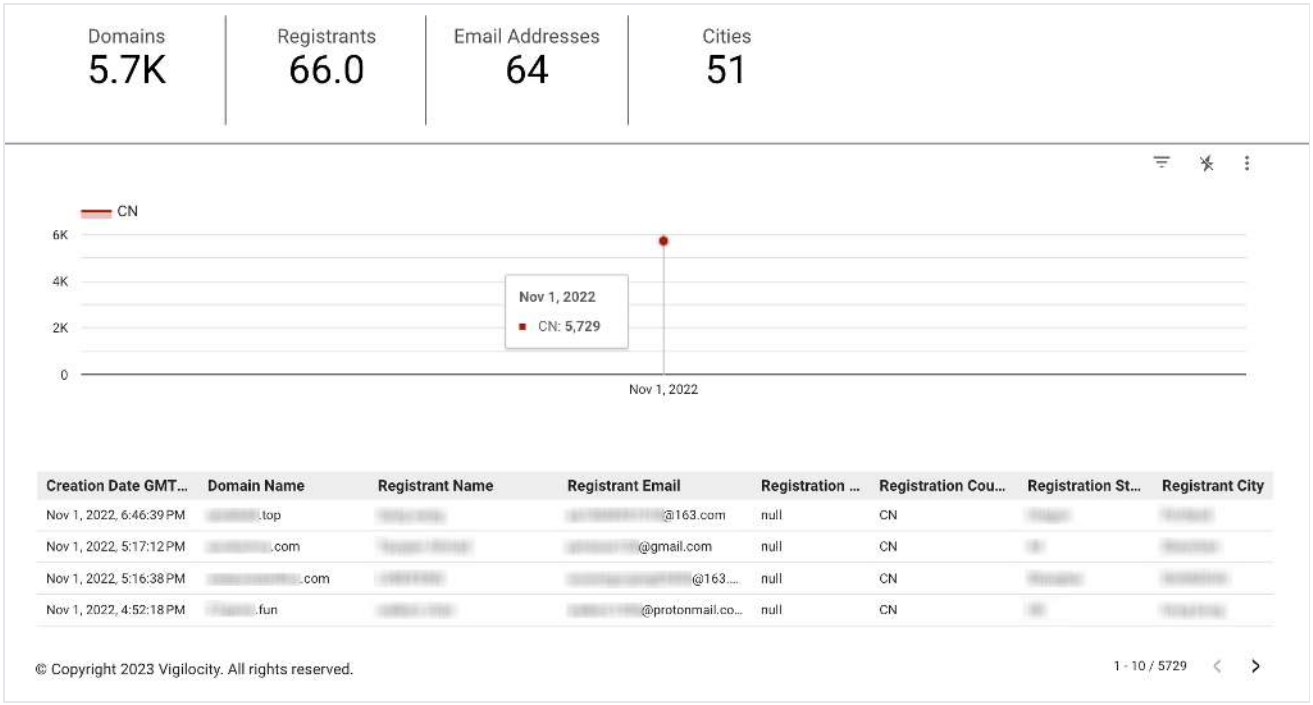

FIG. 4 November 1 registrations with registrant details redacted: 5,729 domains, 66 registrants, 51 cities.

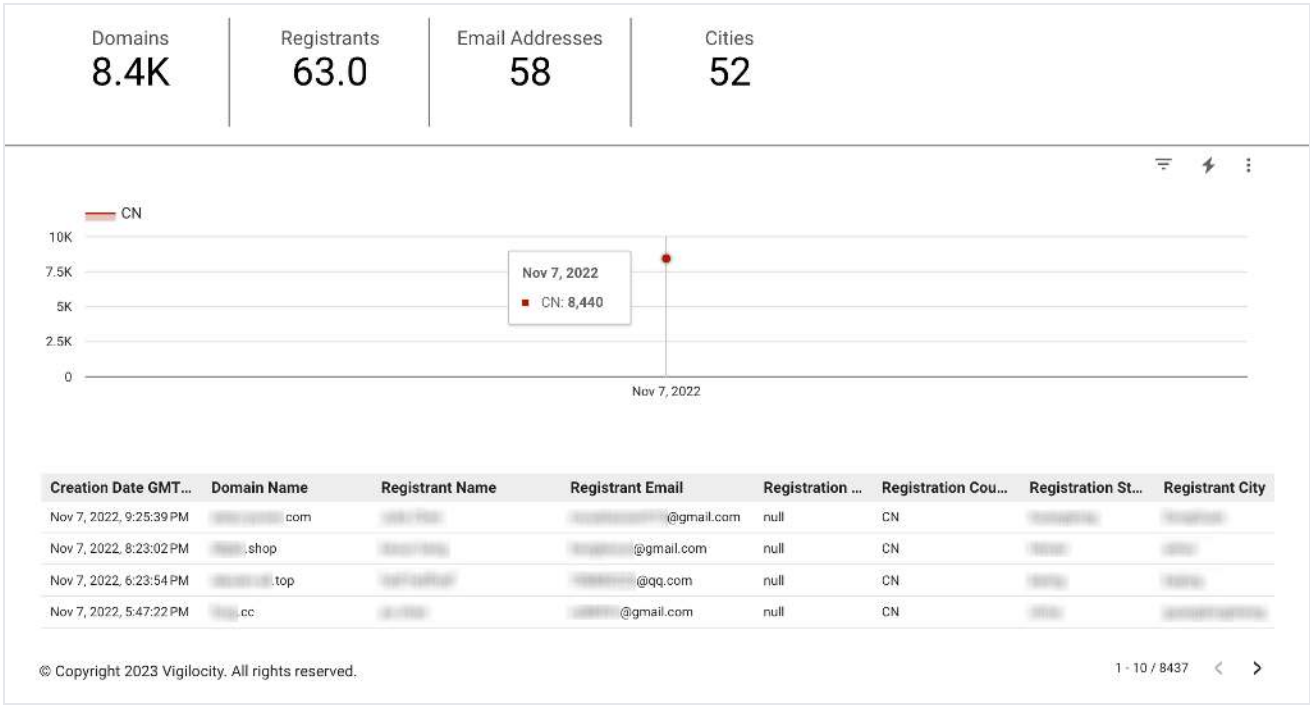

FIG. 5 November 7 registrations, redacted: 8,437 domains, 63 registrants, 52 cities.

The single most prolific registrant bought nearly all of the 14,000 domains across those two days and has no record of any other purchase inside the analysis window. The vast majority of the domains follow a templated sequence of six digits in consecutive order (000054, and so on) under .click or .top.

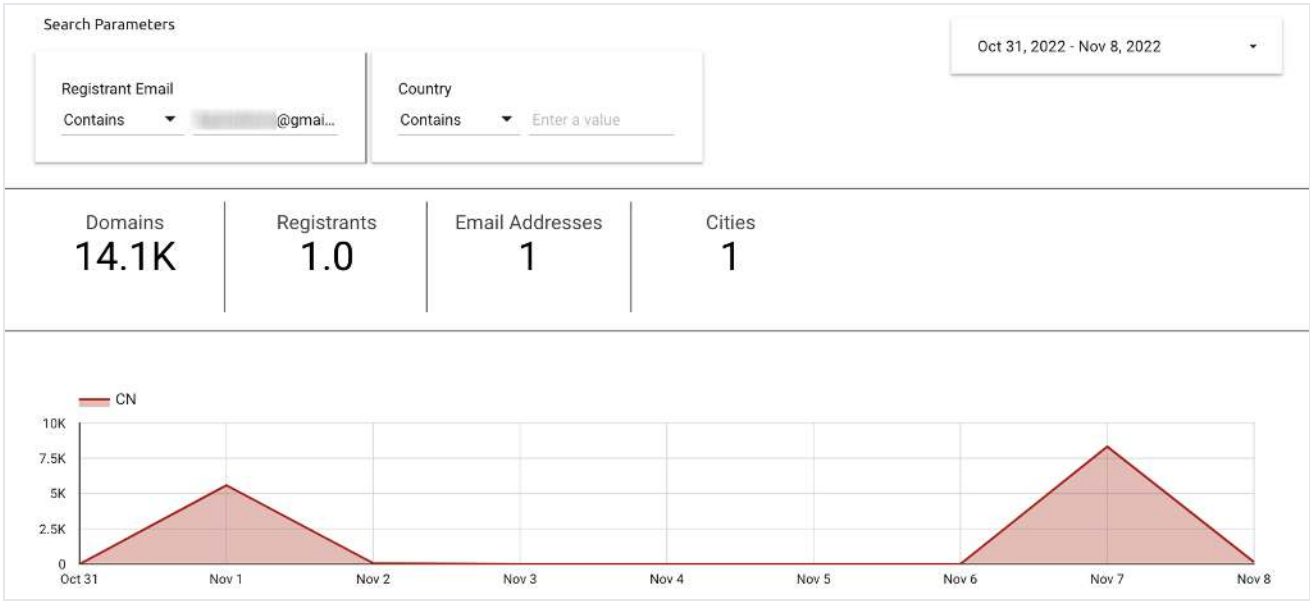

FIG. 6 One registrant\u2019s footprint, October 31 through November 8, 2022: 14.1K domains from a single email address.

> INFRASTRUCTURE COST
>
> Assume bulk purchase at a discounted floor of $2.00 per domain. Every one of these domains also carries privacy protection, which runs $3 to $20 per domain, and all were registered for a single year, which forfeits multi-year discounts, so the estimate is conservative.
>
> At the bottom of that range, this setup cost roughly **$70,000**, spent by one registrant over two days.

CASE · MARCH 1 TO APRIL 15, 2022

Confirmed Chinese phishing infrastructure

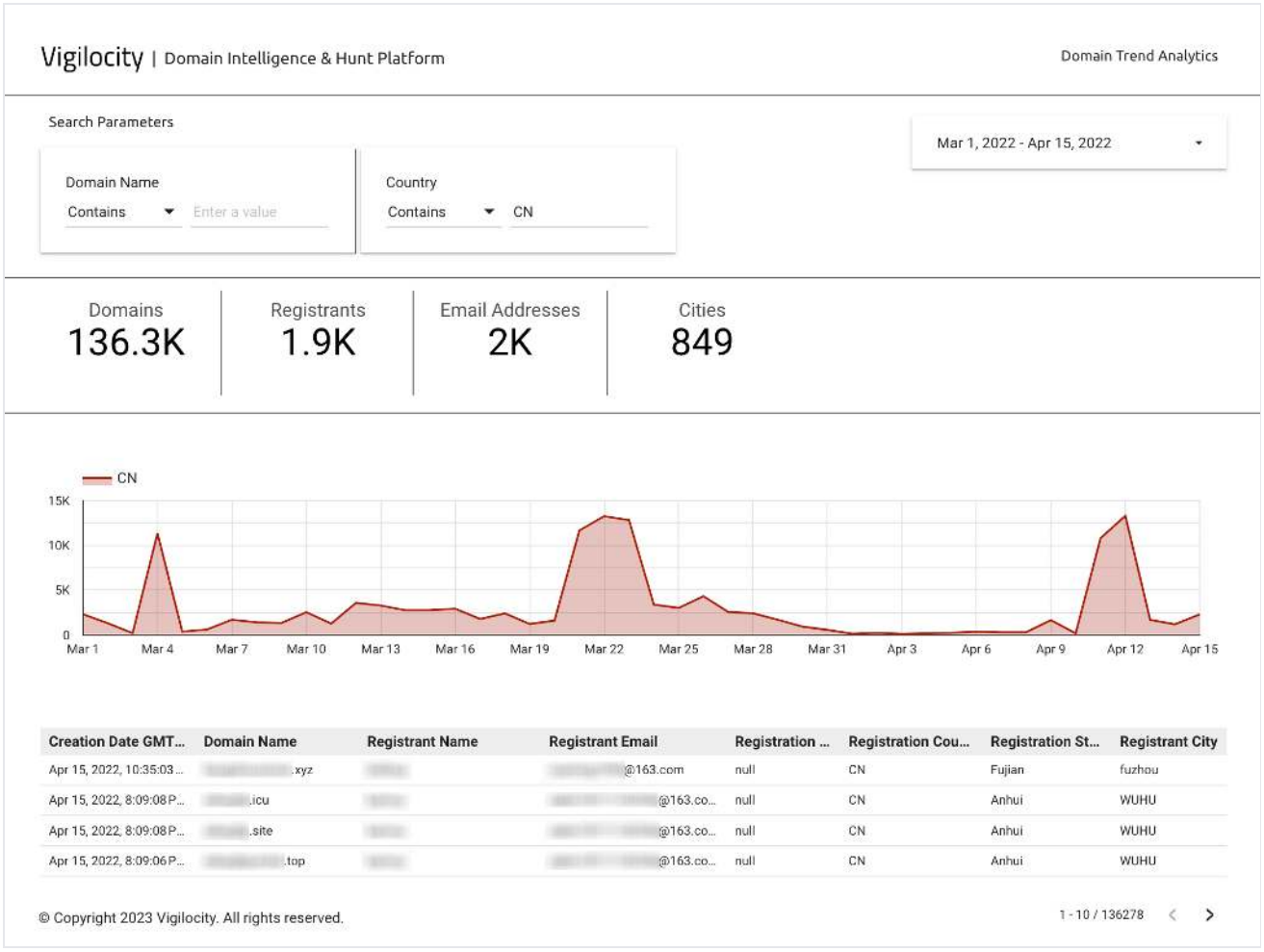

FIG. 7 Registrations by Chinese actors, March 1 to April 15, 2022: 136.3K domains, 1.9K registrants, 849 cities.

Between March 1 and April 15, 2022, Chinese actors registered over **135,000 domains**. The notable single days:

DATE	DOMAINS REGISTERED	REGISTRANTS
March 4, 2022	11,353	86
March 21, 2022	11,669	103
March 22, 2022	13,274	103
March 23, 2022	12,829	107
April 11, 2022	10,793	85
April 12, 2022	13,309	109

The domains follow the same DGA construct as the earlier examples, a six-character mix of letters and numbers spread across .pw, .net, .icu and similar TLDs. The detail that stayed with us: a cursory abuse check found exactly **one** of these domains suspended, on August 18, 2022, for phishing. That domain had been registered on April 11, which means it operated for more than five months before anyone stopped it. As of the close of the analysis window, the rest appeared to still be active.

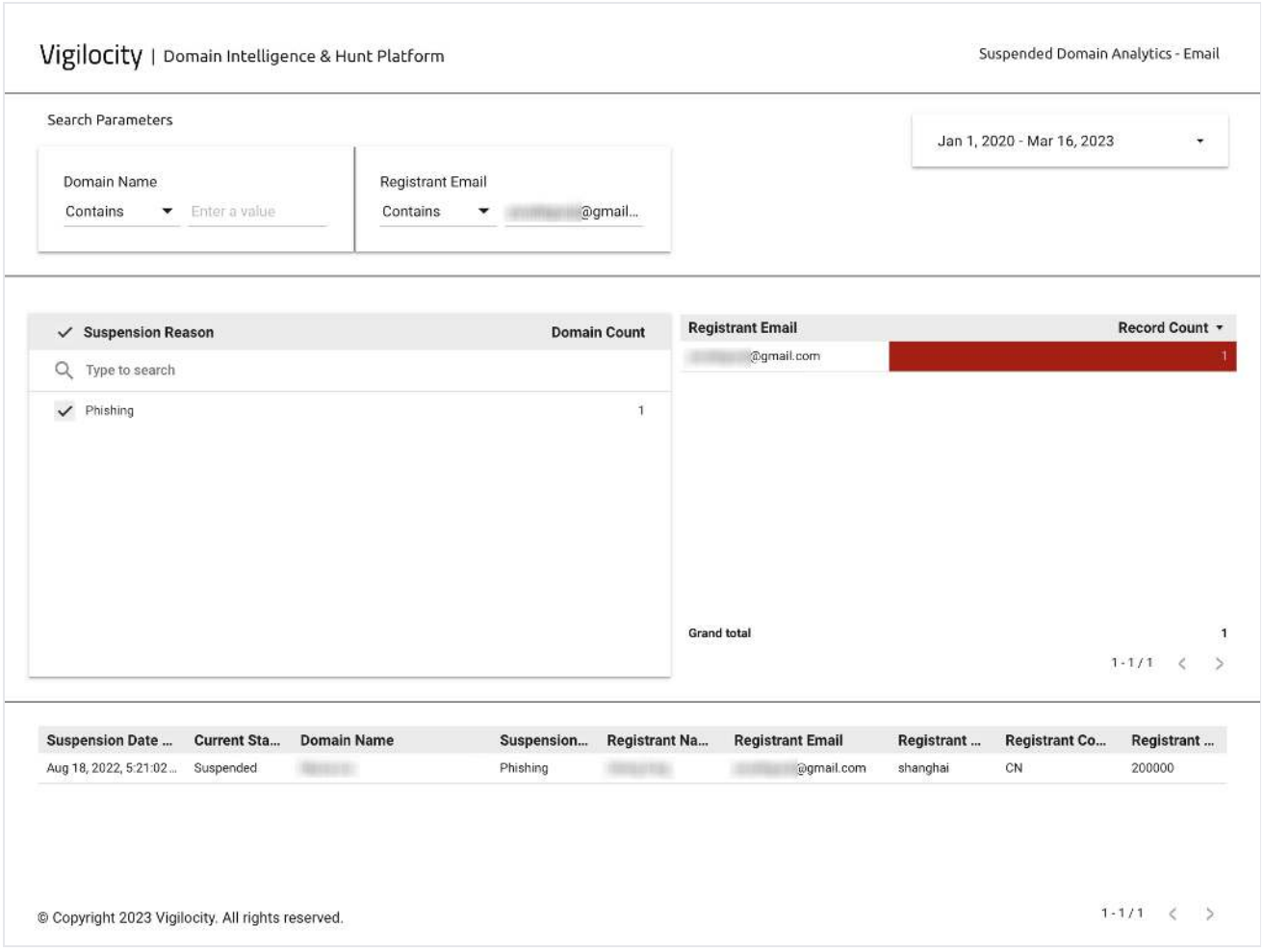

FIG. 8 Suspension analytics across the full window: a single phishing suspension out of 136,000 registrations.

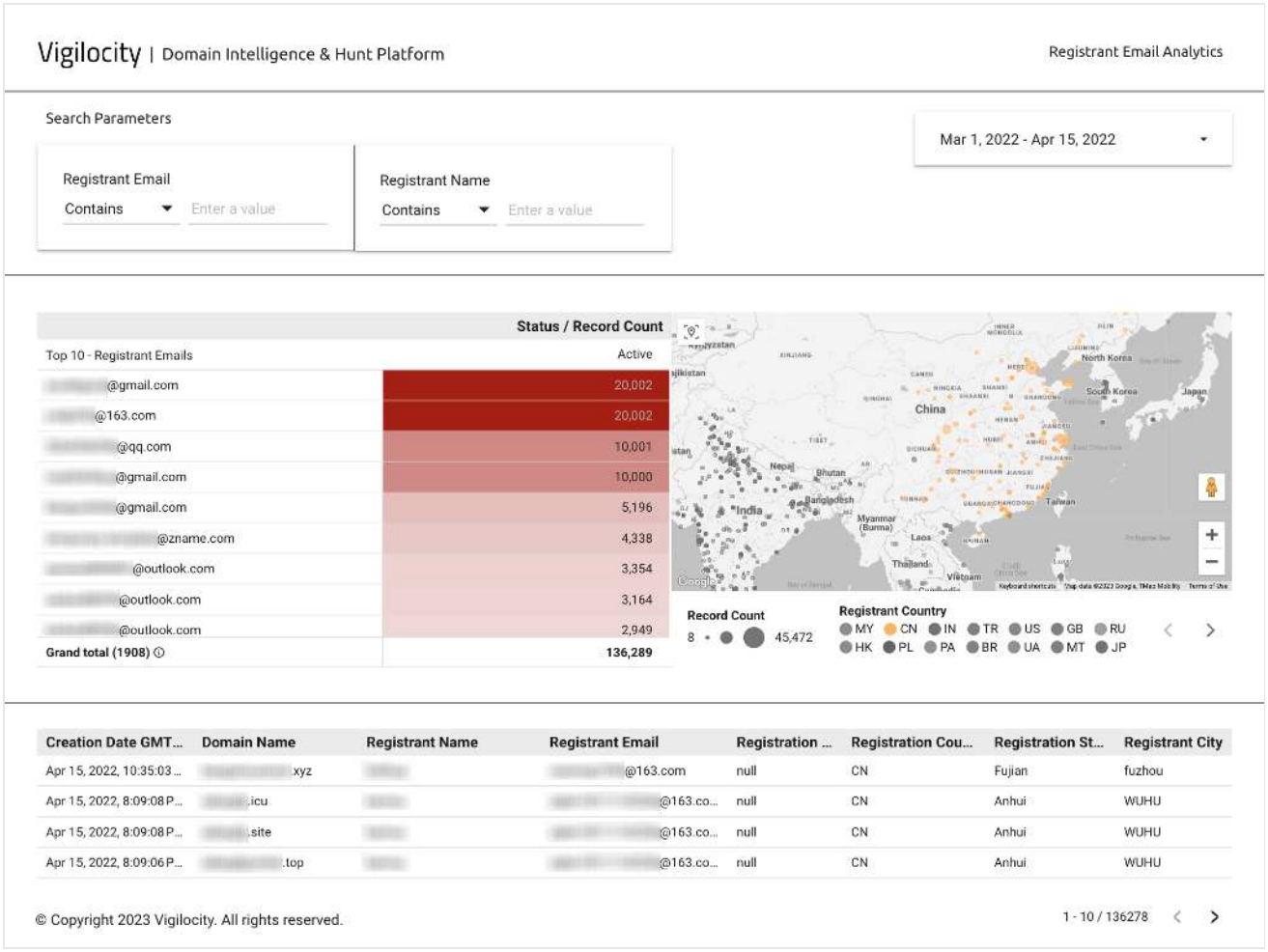

FIG. 9 Registrant email analytics for the March to April 2022 registrations.

Four registrant email addresses account for the bulk of the volume, and their allocations are almost perfectly even: 20,002, 20,002, 10,001, and 10,000. Nobody buys domains in round-number blocks by hand. The registrations are automated.

	Status / Record Count
Top 10 - Registrant Emails	Active
@gmail.com	20,002
@163.com	20,002
@qq.com	10,001
@gmail.com	10,000

FIG. 10 Four registrant addresses, four near-perfect allocations.

INFRASTRUCTURE COST

Same economics as before: a $2.00 bulk floor plus $3 to $20 of privacy protection per domain, one-year terms throughout.

At the low end, roughly **$300,000** of infrastructure, stood up by allegedly four registrants over six days.

CASE · NOVEMBER 7, 2021

A single-day setup at scale

The most dramatic example of a funded operation in the window: **41,228 domains** registered between November 6 and November 9, 2021 by **171** Chinese registrants, with the bulk of it, **31,275 domains**, landing on November 7 alone.

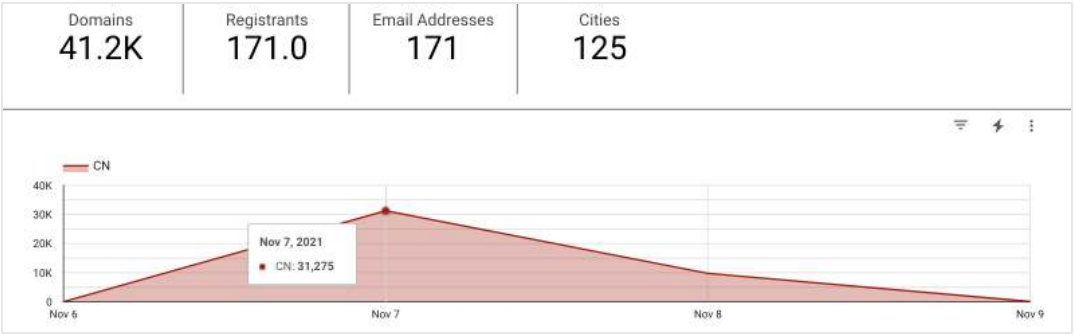

FIG. 11 Registrations by Chinese actors, November 6 through 9, 2021.

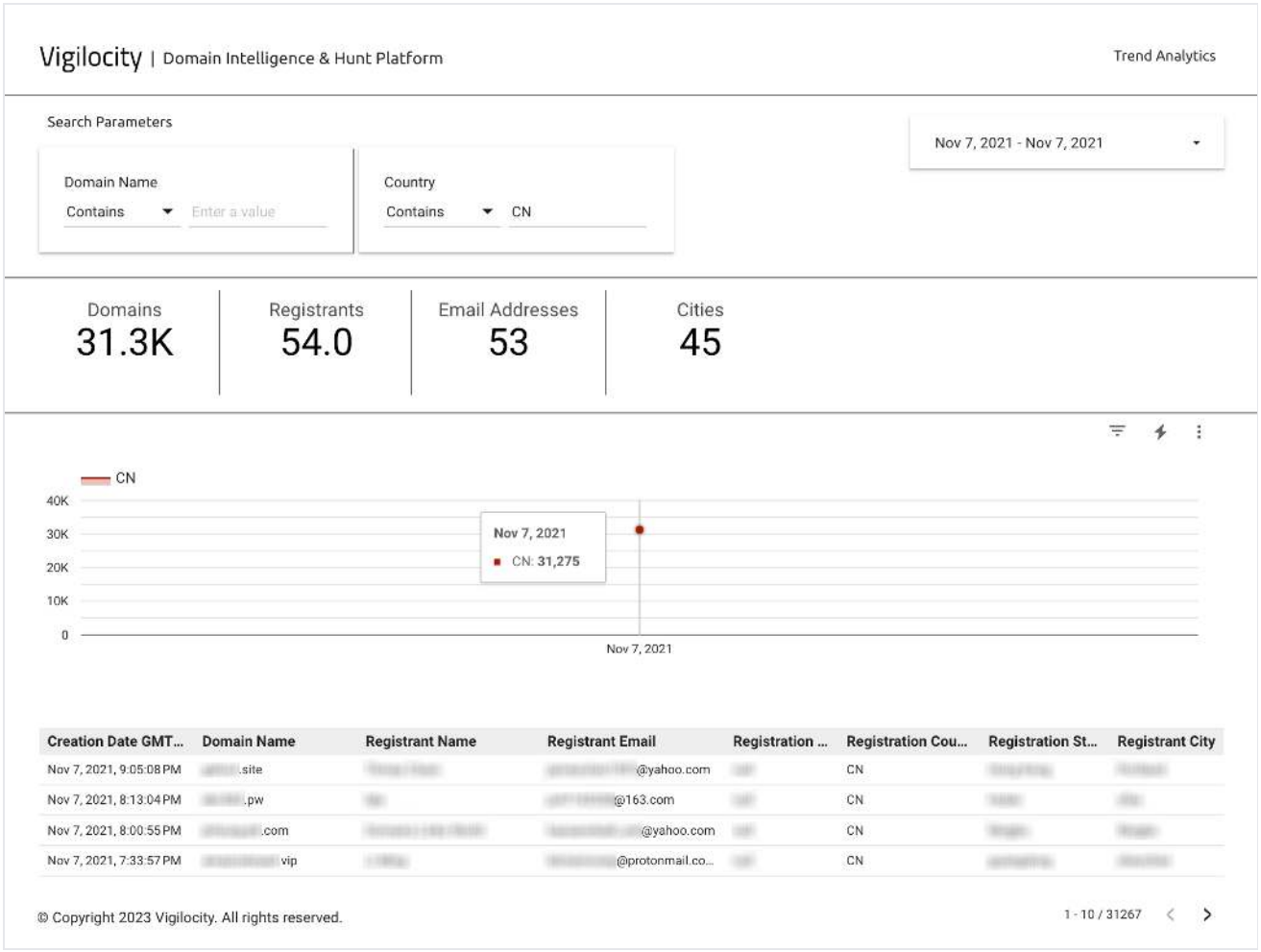

FIG. 12 November 7, 2021 in detail: 31.3K domains from 54 registrants in 45 cities.

Most of the domains are six-character letter-and-number strings across .cl, .uk, .icu and other TLDs, the signature of a domain generation algorithm, and all were registered on the same day, which does not happen by accident. Three registrants alone account for **31,187** of the registrations between November 1 and November 7, and a single registrant for **25,840**. The intended use was never confirmed, but several geopolitical events line up with the timing of the purchase, most notably the passage of the $1.2 trillion U.S. infrastructure bill[3].

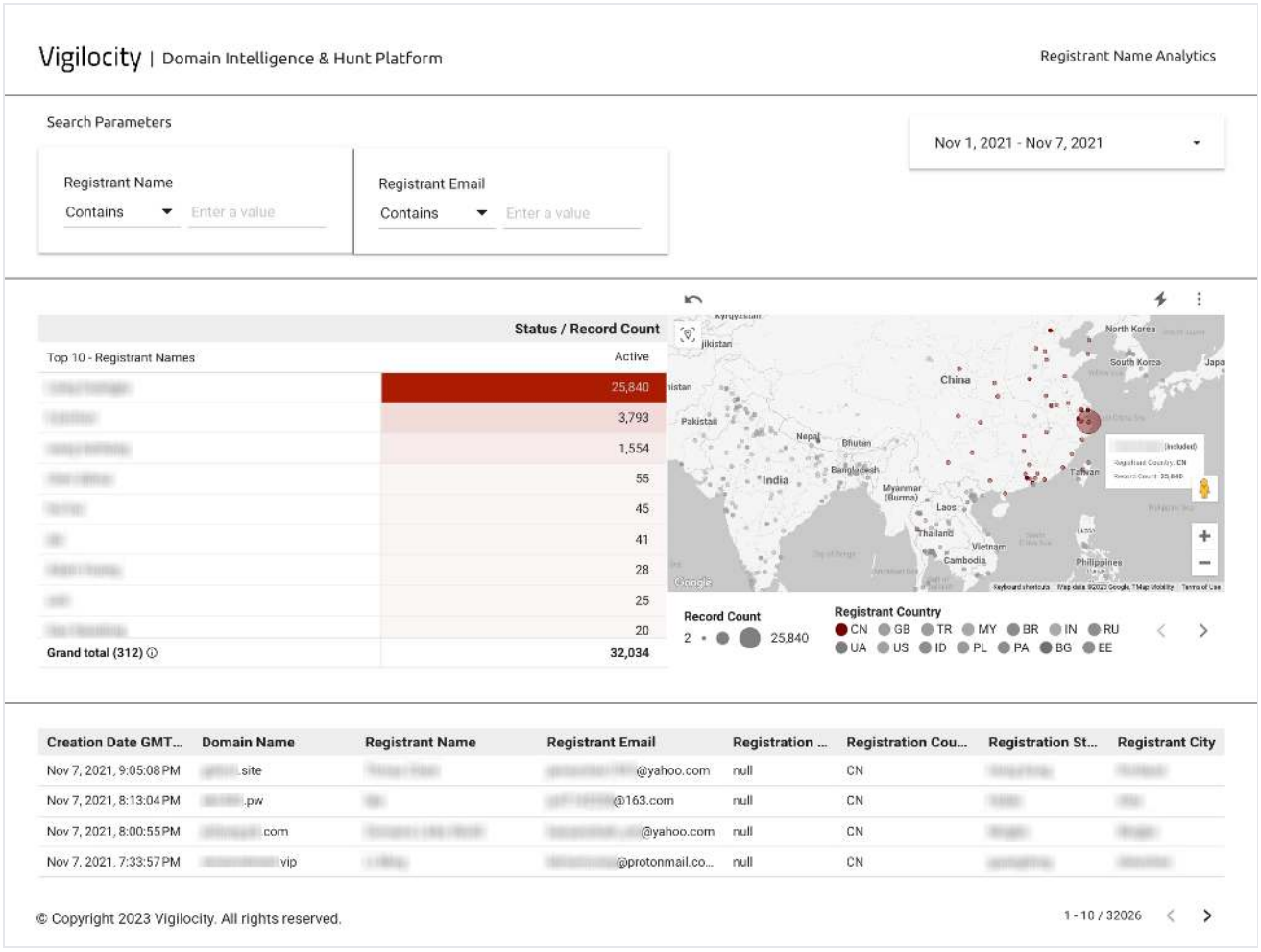

FIG. 13 Chinese registrants, November 1 to 7, 2021: one name accounts for 25,840 registrations.

> INFRASTRUCTURE COST
>
> Same conservative assumptions.
>
> Approximately **$129,200**, spent by allegedly one registrant in a single day.

Pivoting on that actor's name and email address widens the picture: **28,999 domains** registered between January 2020 and March 2023, nearly all inside the November 2021 burst. Outside it, the same identity bought exactly three domains, one each on March 26, April 15, and April 16 of 2022. Whatever this actor was building, they built it in one motion and went quiet.

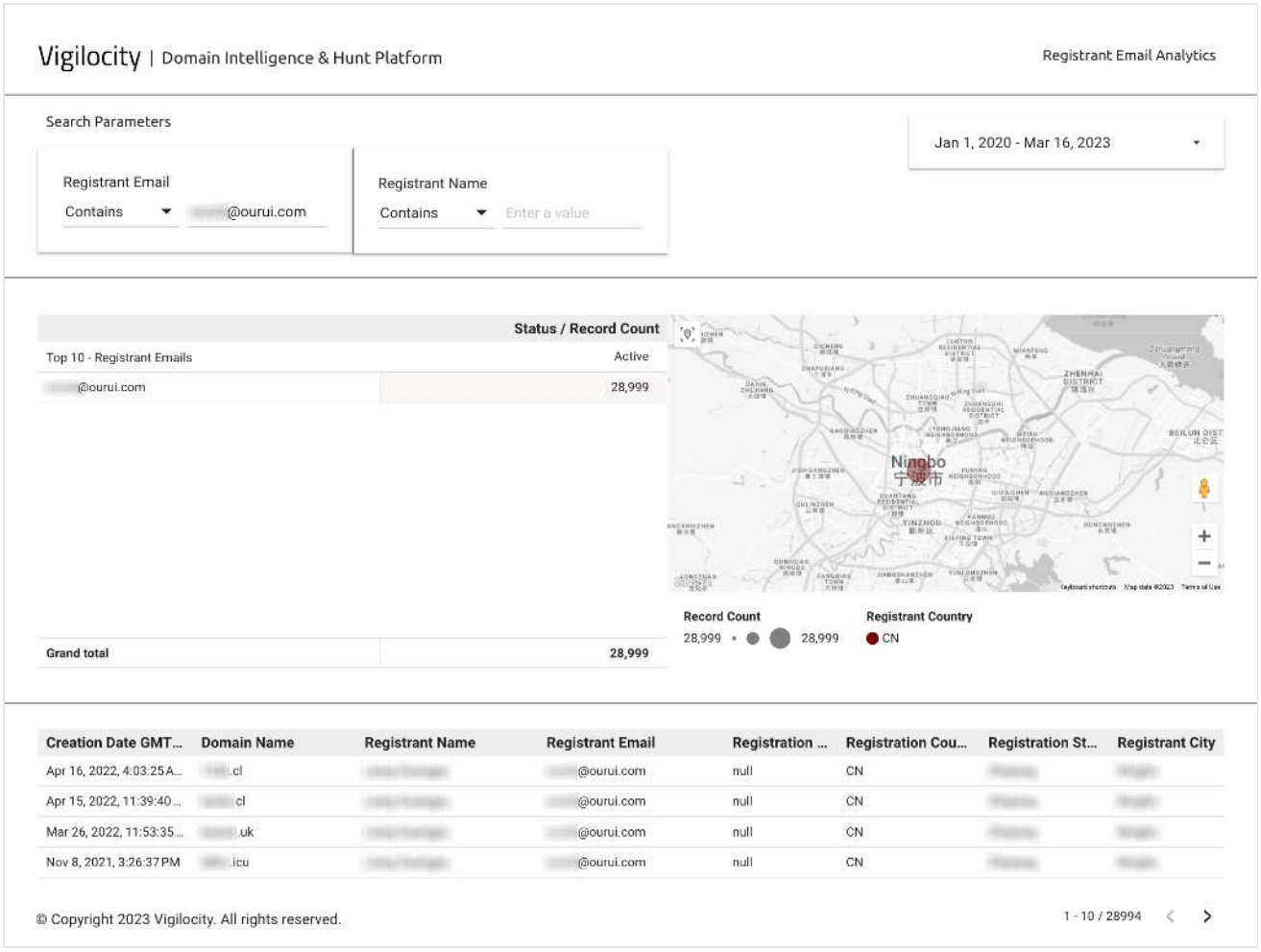

FIG. 14 One prolific actor\u2019s full registration history across the analysis window: 28,999 domains, one city.

PATTERN

Lazy OpSec and repeatable habits

Even competent threat actors fail at operational security, and the failures compound. Reusing an email address or a moniker, skipping the proxy that would mask an IP, returning to the same registrar out of habit: each is a thread an analyst can pull to link infrastructure that was supposed to look unrelated. Many actors tighten their OpSec months or years into a career, which does nothing about the indelible trail already behind them.

One actor in the window ran a successful phishing campaign on more than **1,800** DGA-generated domains registered under a single name and email address.

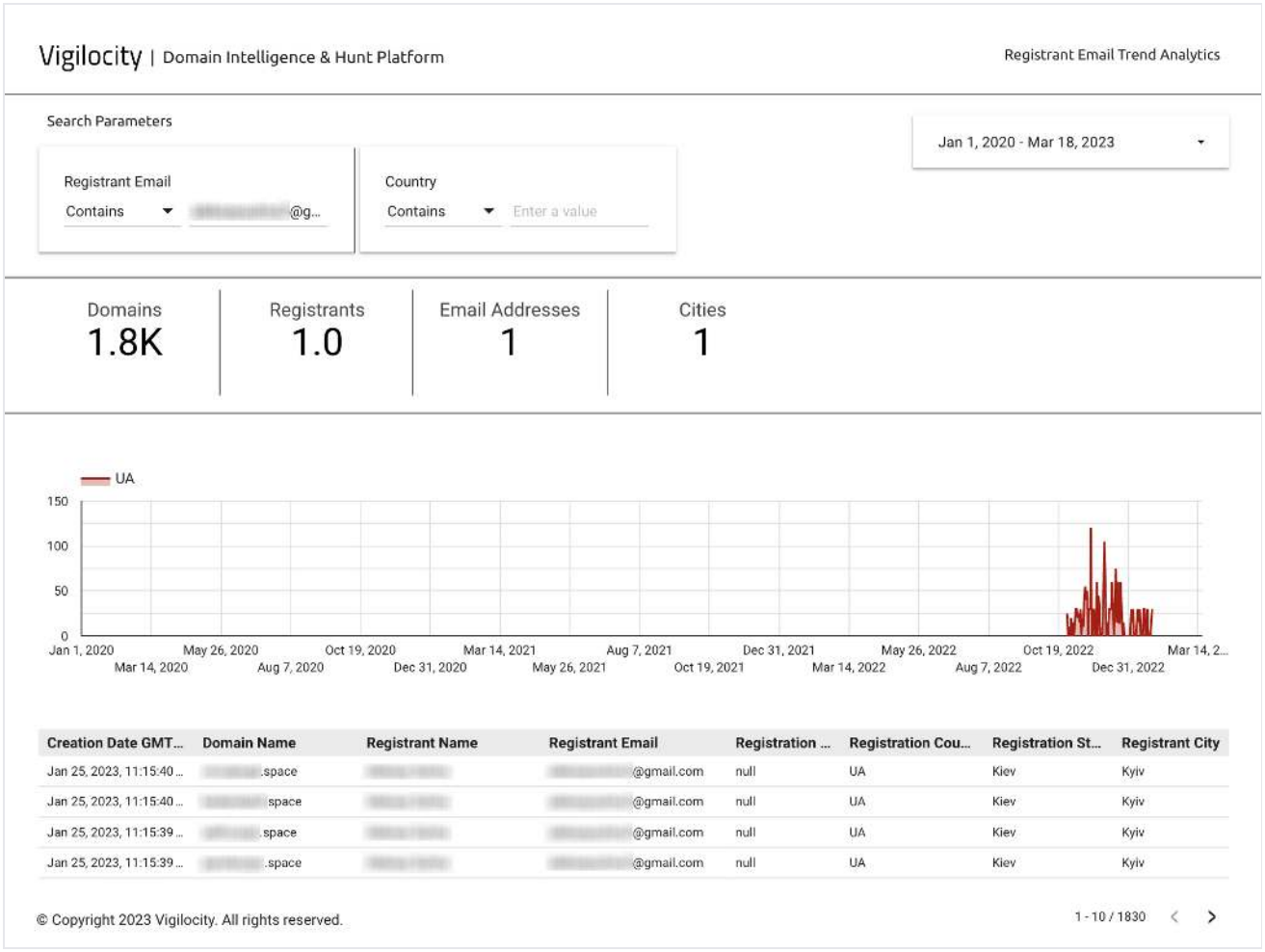

FIG. 15 DGA-generated registrations under one identity, January 2020 through March 2023: 1.8K domains, one city.

When over 1,160 of those domains were suspended for phishing, the actor stood up a new moniker, a new email account, and a new registration account, *at the same registrar*, and tried to resurrect the campaign: 495 more domains, same construct, same city.

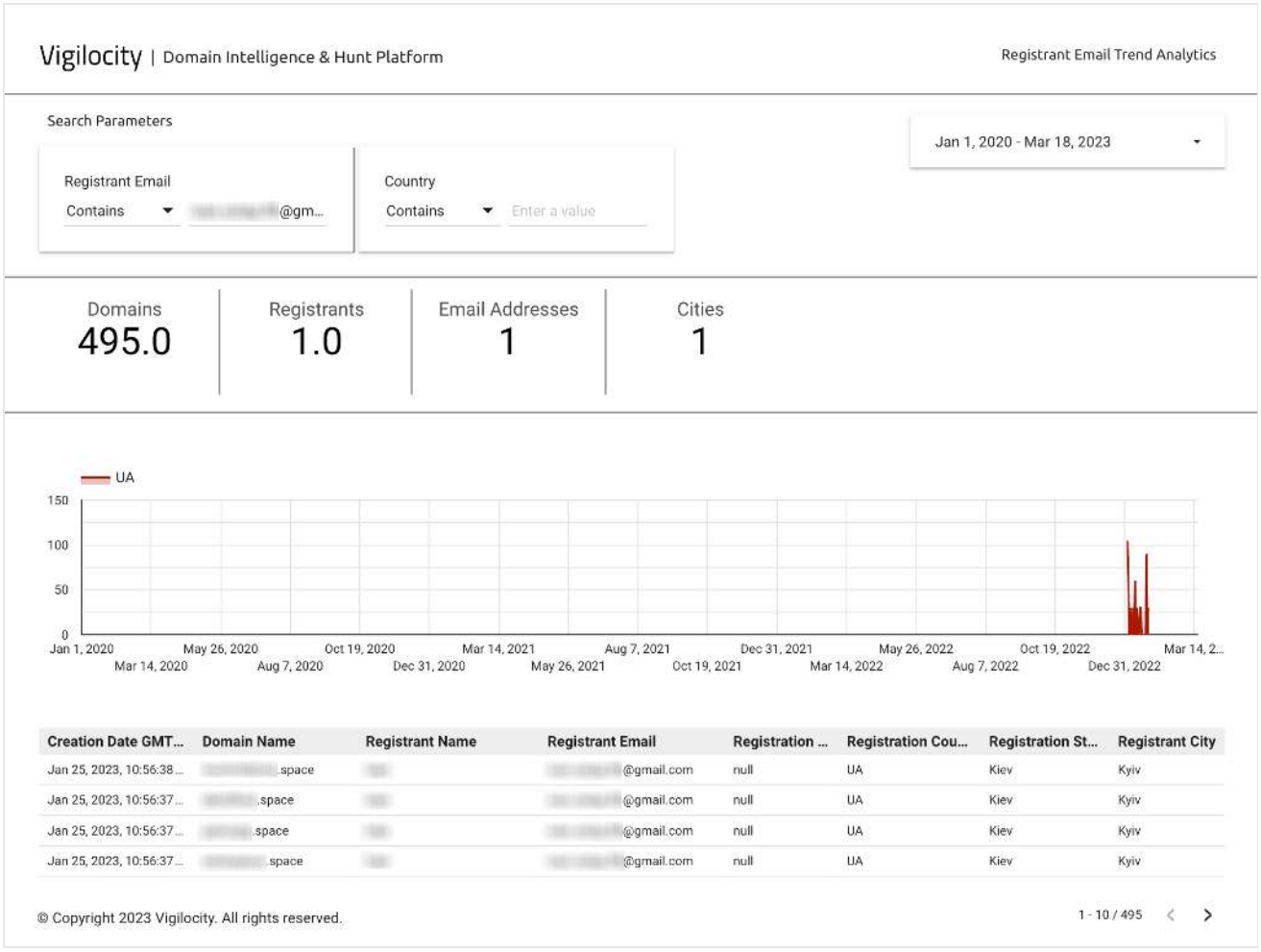

FIG. 16 The resurrection attempt: 495 domains under the new identity, same registrar, same Kyiv origin.

Catching this behavior early blunts phishing at the stage where it is cheap to stop, before it escalates toward ransomware. Doing so requires a wide aperture across a long historical baseline; the pattern is invisible in any single week of data. The actor's early testing and experimentation, visible in the record, is itself a linking signal between infrastructure that would otherwise read as disparate.

A second actor used one email address across **1,400** registrations while cycling through **96** different monikers in **75** cities. The mismatch is the tell: the identities are synthetic, the automation is real, and the domains, word-and-number combinations under .pw and .site, complete the DGA picture. This actor registered domains from January 2, 2020 through March 1, 2023 without interruption, a reminder of how long a patient operator can run undetected.

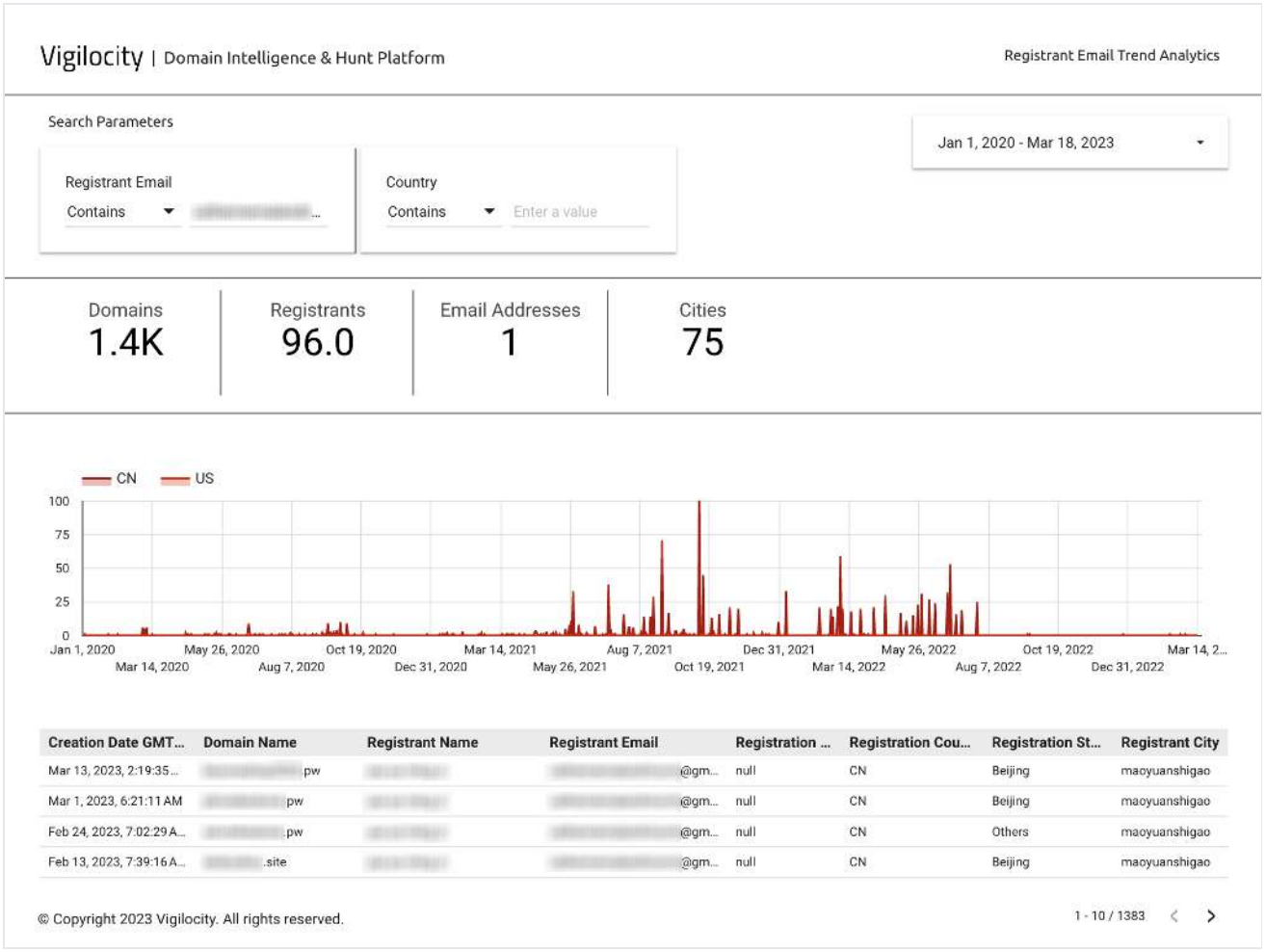

FIG. 17 One email address, 96 names, 75 cities, 1.4K domains: automation wearing a crowd of masks.

PATTERN

Malware and dropper domains

Staged attacks often hold their domain registrations until a designated moment, again to deny defenders early warning. The actor in the next figure was responsible for the widely reported PARALAX loader maldoc campaign. Elastic Security Labs, analyzing the related intrusion set, described PARALLAX as a full-featured modal backdoor and loader with defense evasion and information-stealing capabilities, first observed in 2020 and associated with COVID-19 malspam, alongside NETWIRE, a mature cross-platform RAT dating to 2012[4]. The registration timeline shows a clean gap between May 17 and August 8, 2022: staging, pause, resumption.

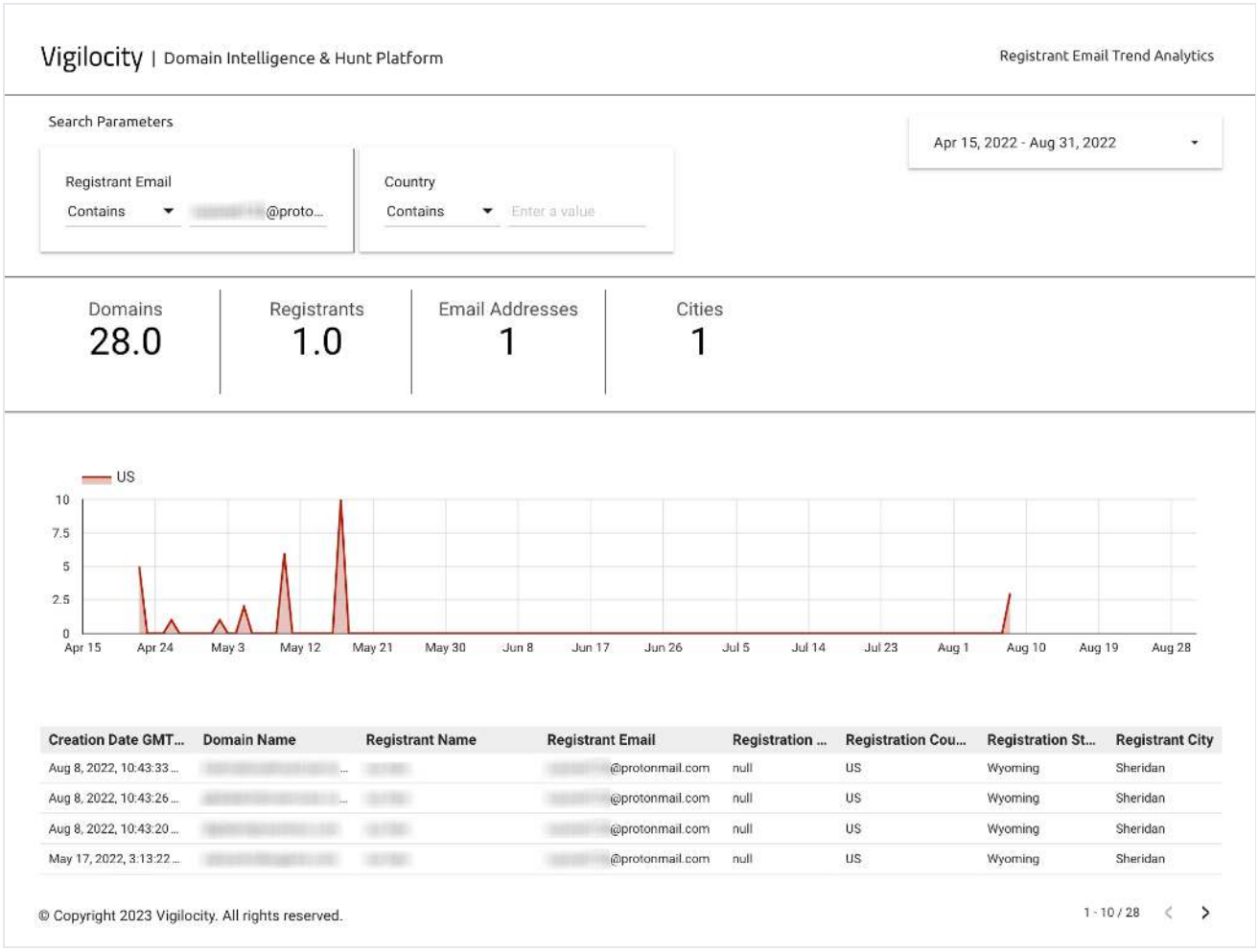

FIG. 18 Registration timeline associated with the PARALAX loader maldoc campaign, April 15 to August 31, 2022.

That campaign was eventually deconstructed. Plenty are not. The actor below has run a crypto-phishing and credential-stealing operation continuously since November 4, 2021 with essentially zero mitigation, registering about six domains a day, nearly every day. The volumes are deliberately unremarkable; nothing about any single day would trip an anti-bot defense. The domains still match a DGA template, and the total now exceeds a thousand.

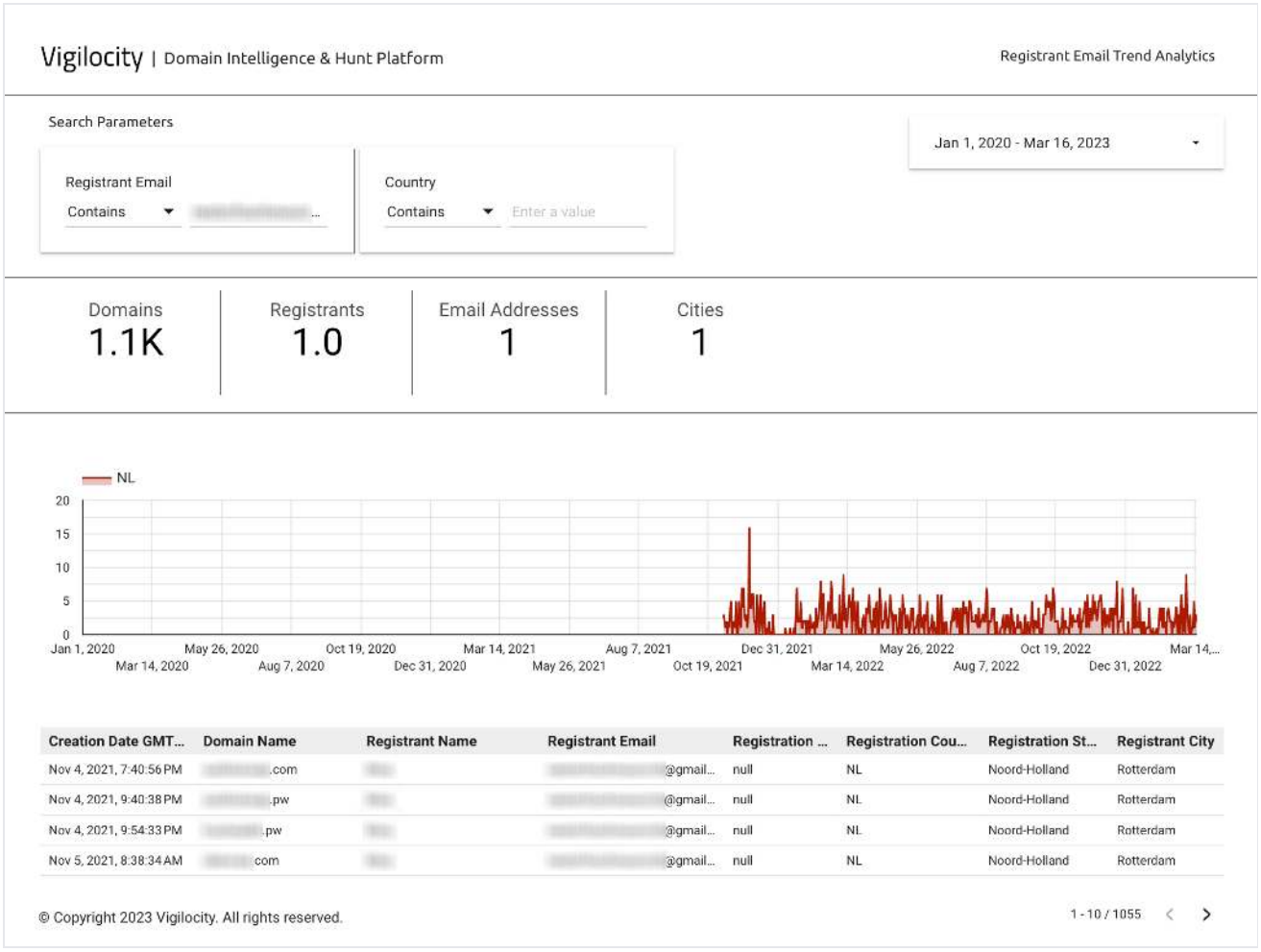

FIG. 19 Low and slow: a multi-year crypto phishing campaign averaging six registrations a day from Rotterdam.

CASE · OCTOBER 2021 TO MARCH 2022

Reconnaissance before ransomware

Ransomware campaigns begin with reconnaissance of the victim's network, and in recent years the tool of choice for that phase has often been Cobalt Strike: custom malware execution, port scanning and enumeration, command and control management, attack simulation. It was built for defenders to test their own organizations. The irony writes itself.

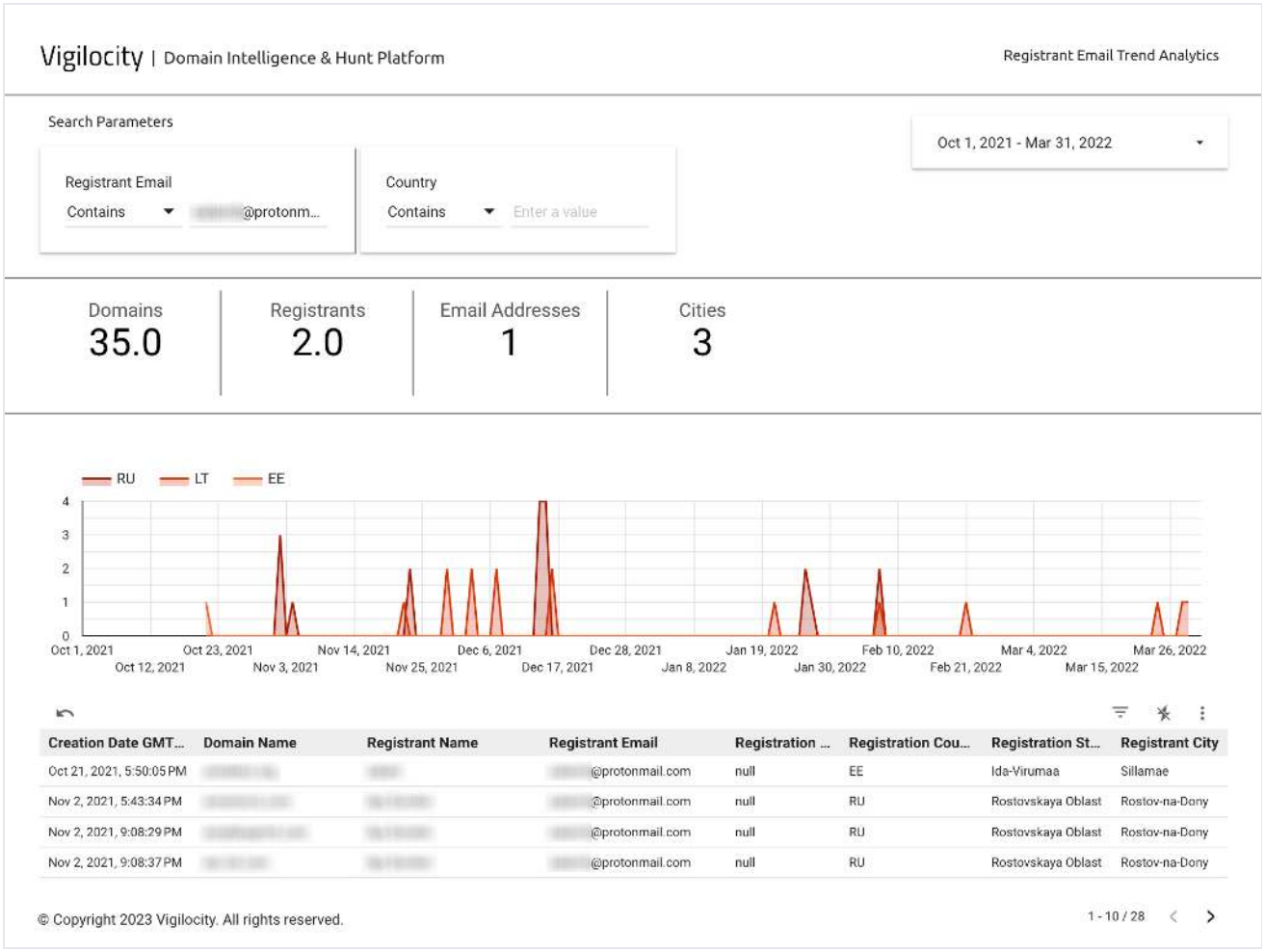

FIG. 20 Domain registrations tied to a cluster of Cobalt Strike servers, October 2021 through March 2022.

The actor here registered a first domain on October 21, 2021 under one name and email address, then continued on November 2 under a different name, the same email, and allegedly a different country. In total, **35 domains** registered between October 21, 2021 and March 29, 2022, most of them Cobalt Strike servers. Once an actor has gathered enough reconnaissance, the encryption utilities deploy and the victim is largely out of options; this one worked uninterrupted for over four months. Dismantling reconnaissance infrastructure while it is still reconnaissance is one of the few points where ransomware can be avoided entirely rather than survived.

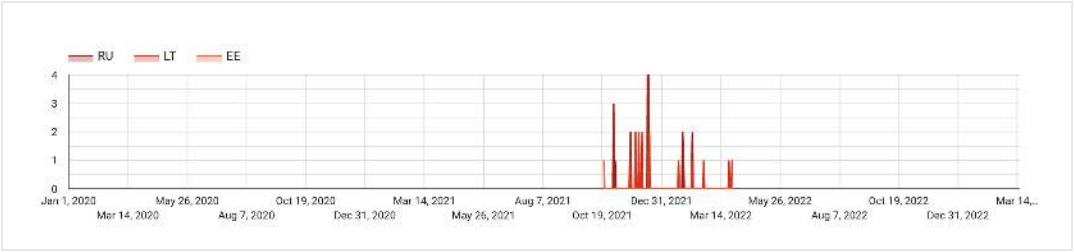

FIG. 21 The same actor at full aperture, January 2020 through March 2023: an isolated burst, then straight to the next stage.

INFRASTRUCTURE COST

From the inverse angle: these were primarily .com and .org domains, not bulk purchases, so figure $10.00 per domain plus the usual $3 to $20 of privacy protection.

At the highest reasonable estimate, about **$1,050**, by allegedly one registrant. Set against a ransomware campaign that can net millions, the popularity of the tactic explains itself.

PATTERN

Cybersquatting and trademark infringement

A quick keyword search makes the brand problem concrete. Searching "pepsi" across the window returned **176 domains** registered between January 2020 and March 2023, some as recently as the week of the search, most of them likely trademark violations and all of them candidates for convincing phishing lures. Follow-up research found two suspended by the registrar, reason given: "Scam website".

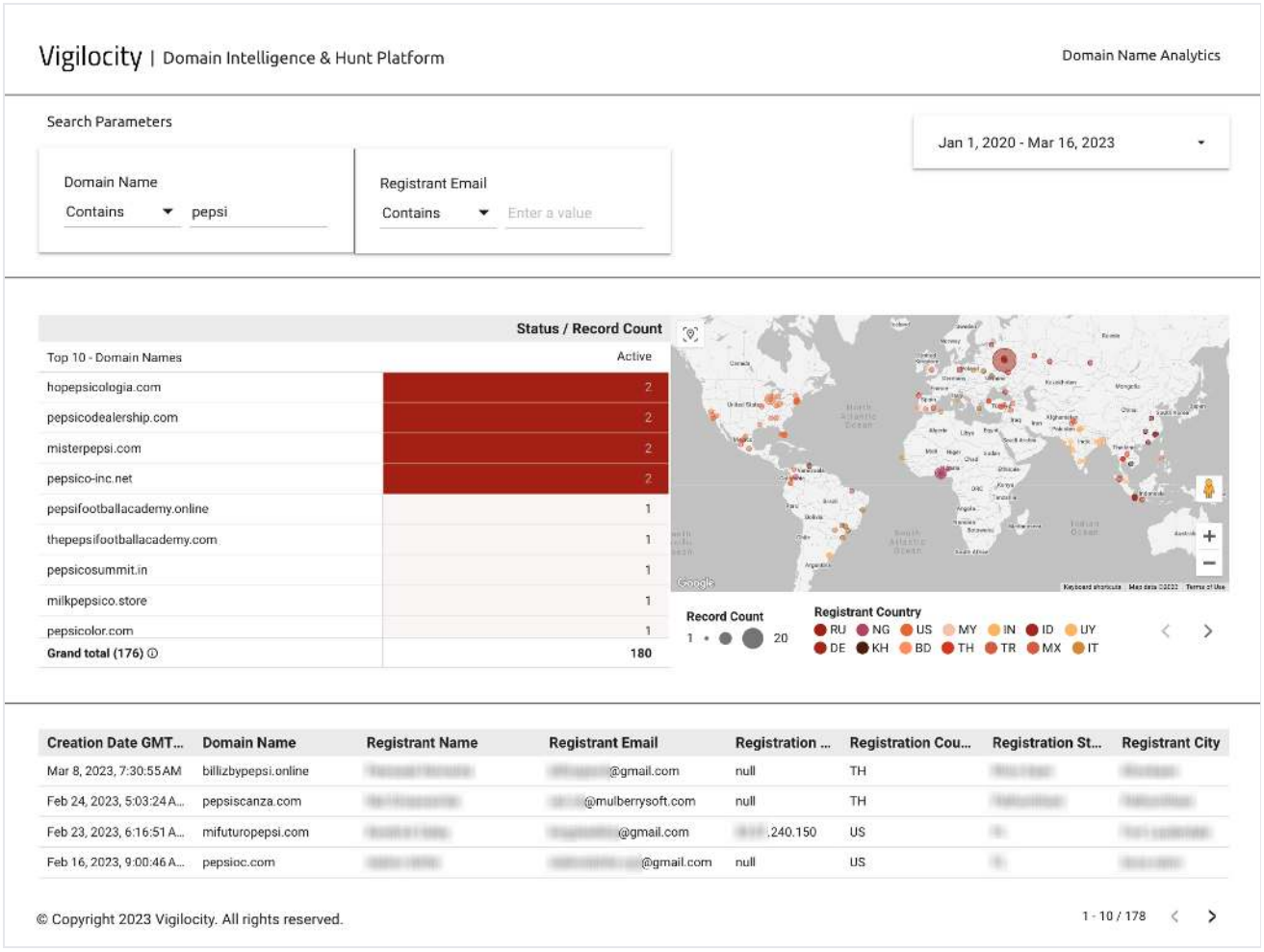

FIG. 22 Potential cybersquatter domains embedding \u201cpepsi\u201d, January 2020 to March 2023.

"cocacola" returned **63 domains** in the same period. Exactly one was deleted by its registrar, on July 14, 2022, and it had been registered on December 1, 2021: eight and a half months live and resolving.

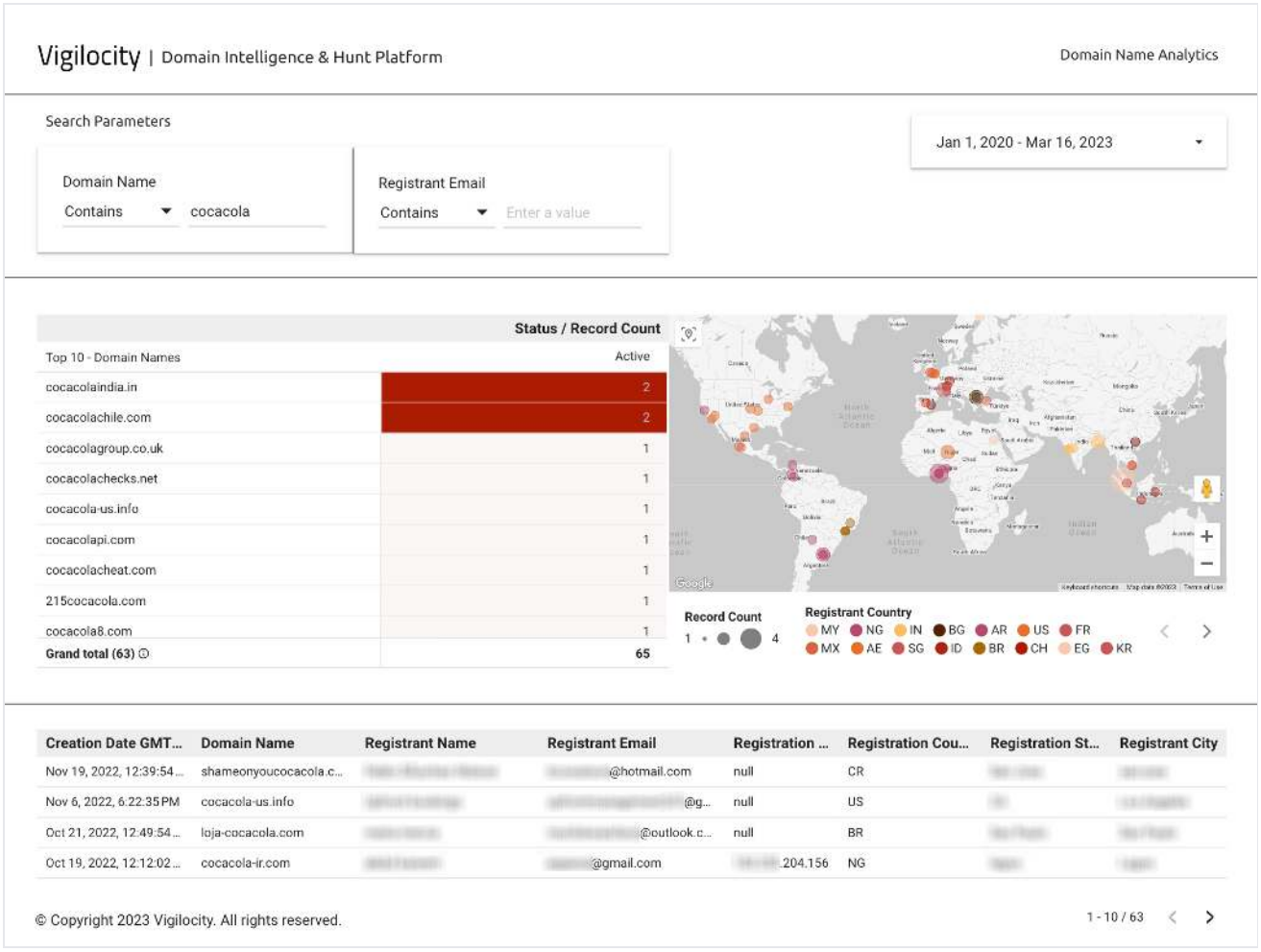

FIG. 23 Potential cybersquatter domains embedding \u201ccocacola\u201d over the same period.

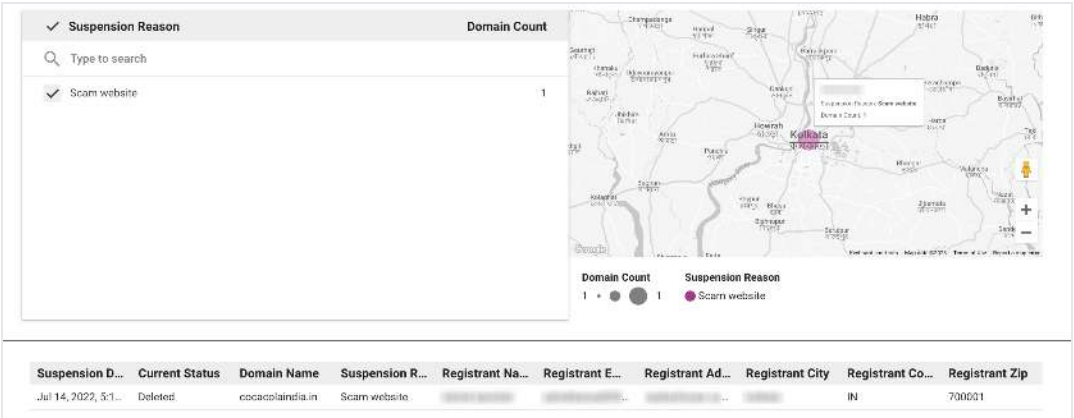

FIG. 24 The one deletion: a \u201ccocacola\u201d domain removed July 14, 2022, eight and a half months after registration.

UDRP complaints and bad-faith litigation exist for exactly this, and they work, unevenly, at the speed of lawyers. The wider sweep below is the part that should worry a brand owner. Many of these domains never host a website at all. They are registered as email domains, invisible to scanners and crawlers that index the web, and are activated only when the surrounding infrastructure is armed. Detection at registration time is the only stage where that class of abuse is cheap to catch.

KEYWORD	DOMAINS REGISTERED	REGISTRANTS	TOP COUNTRIES
internalrevenue	12	12	US, NG, SG, MX
blackrock	88	71	US, IN, IE, GB, FR, RU
jpmorgan	87	68	US, NG, GB, IN, BG, PL
bloomberg	41	34	US, IN, KE, CN, NG, ZA
americanexpress	46	36	US, IN, NG, IT, ID, GB
wellsfargo	230	157	US, NG, IN, CN, BG, GB
nasdaq	76	50	CN, IN, US, BR, AS, TH
nike	2,100	1,500	IN, US, TR, CN, RU, MY
covid	7,800	4,600	US, IN, NG, CA, CN, RU
pfizer	94	63	US, IN, NG, GB, AE, CL
moderna	850	754	BR, US, IN, CO, MX, TR
worldhealth	117	88	IN, US, PH, TR, GB, BR
walgreens	32	24	US, IN, NG, CN, PA, PL
amazon	4,600	2,700	US, BR, IN, CN, CA, GB
walmart	318	150	US, CN, NG, GR, BD, IN

05 What the record shows

Read together, the cases reduce to a short list of durable facts. Malicious infrastructure is bought in patterns that automation cannot hide: round-number allocations, templated domain strings, single-day bursts, one identity where there should be hundreds. The economics run heavily in the attacker's favor, seventy thousand dollars for an influence apparatus, a thousand for the front end of a ransomware campaign, which is precisely why volume keeps rising. Suspension and takedown, measured against those volumes, barely register; one suspension in 136,000 registrations is not a control, it is a rounding error. And operational security decays in ways that reward anyone keeping a long enough memory of the record.

Every one of those facts favors the observer, provided the observation starts at registration time rather than detonation time.

06 From prediction to confirmation

The original edition of this paper closed by arguing that domain registration analysis would only grow in importance as methods like RASA matured. That prediction, at least, we can grade. In the years since, this line of analysis became the front end of Mythic, Vigilocity's breach intelligence platform. RASA still watches

infrastructure being acquired and staged; Mythic then watches the other side of the exchange, identifying victim networks in live communication with that infrastructure and confirming material impact with timestamped, empirical evidence. Prediction tells you a campaign is being built. Confirmation tells you, with dates, addresses, and the data taken, whom it reached. The two together close the loop this paper opened.

07 Conclusion

Domain registration analysis lets a defender see potential threats before they materialize, and the observational record above shows what that looks like in practice: influence infrastructure caught assembling over two days in November, phishing fleets that ran five months past their first suspension, reconnaissance servers that sat unexamined for a third of a year. Phishing and ransomware campaigns in particular can be identified while they are still a shopping list.

The difficulties have not gone away. Privacy services still mask registrants; some infrastructure still appears late by design. RASA was built to hold up under exactly those conditions, by weighing intent, targets, and operational security failures alongside the registration record, and by refusing to treat any single domain as the unit of analysis. The unit of analysis is the actor, over years. Watched that way, the registration record remains what it was in 2023: the earliest reliable warning the defender is ever offered.

08 Sources

1. "WannaCry ransomware attack: What we know so far." BBC News, May 17, 2017. bbc.com/news/technology-39914912 · "How researchers used the WannaCry kill switch to track the ransomware outbreak." ZDNet, May 15, 2017. · "WannaCry Ransomware Attack: The Role of Domain Registration in Tracking Down the Perpetrators." ICANN, June 15, 2017. · "How security researchers tracked down the WannaCry ransomware authors." Ars Technica, May 26, 2017.
2. "JabberZeus Botnet Taken Down in Global Operation." KrebsOnSecurity, September 10, 2019. krebsonsecurity.com/2019/09/jabberzeus-botnet-taken-down-in-global-operation/
3. "'Powerful signal': Biden's infrastructure bill sends message to China." Politico, August 7, 2021. politico.com/news/2021/08/07/biden-infrastructure-bill-message-china-502739
4. "Exploring the REF2731 Intrusion Set." Elastic Security Labs, September 30, 2022. elastic.co/security-labs/exploring-the-ref2731-intrusion-set

Figures are captures from the Vigilocity domain intelligence platform as published in the 2023 edition. Registrant names, email addresses, and domain names are redacted. Registration counts and dates are as observed during the January 1, 2020 to March 18, 2023 analysis window.

ABOUT VIGILOCITY

Vigilocity builds technology for identifying and eliminating threat actor infrastructure, drawing on decades of counterintelligence operations inside adversary networks. Its platform, Mythic, confirms material breaches by observing them from the adversary's side.

BRIEFINGS

Request a briefing

vigilocity.com/contact