Vigilocity

Geopolitical Cyber Event Prediction

Using Reverse Attack Surface Analysis - RASA

1401 Lavaca Street
Unit #375
Austin, TX 78701

Table of Contents

1401 Lavaca Street
Unit #375
Austin, TX 78701

Introduction

The analysis of internet domain registrations has emerged as a critical tool for understanding the activities of nation-state adversaries and cyber criminal groups. With the recent dramatic rise of cyber attacks, these actors have relied on scalable and resilient methodologies to conduct their malicious operations that range from phishing attempts to disinformation campaigns and ransomware.

The use of fast-flux DNS and the associated registration of domains for malicious use has been, and continues to be, one of the most formidable weapons in a threat actor's arsenal. Domains are used throughout the attack lifecycle, some of which include phishing, dropper and drive-by sites, command and control (C2), decoy domains, and obfuscation (hop point) utilities. However, the sophisticated analysis of domain registrations not only can assist in identifying the emergence and persistence of these attacks, but also predict them before they occur.

As we have witnessed in the last several years, there has been a resurgence of cyber criminal groups using ransomware to extort money from corporations and governments, however this is not a new phenomenon. In 2017, the WannaCry ransomware attack[1] infected computers in over 150 countries, causing billions of dollars in damages. More recently, the widely publicized REvil ransomware group attacked the software company Kaseya, resulting in a global supply chain attack that affected hundreds of businesses.

While ransomware (and more concerningly, wiperware) is, and should be, of grave concern to global organizations and governments, it isn't possible without first gaining illicit access to the victim's network. This is where phishing and spear-phishing play a key role in the process and have increasingly become the preferred vector of early stage attacks.

For the uninitiated, phishing and spear-phishing are tactics in which attackers use fraudulent emails, text messages, and direct messages (via social media, etc.) to socially engineer individuals into giving away sensitive

[1] "WannaCry ransomware attack: What we know so far." BBC News. May 17, 2017. https://www.bbc.com/news/technology-39914912
"How researchers used the WannaCry kill switch to track the ransomware outbreak." ZDNet. May 15, 2017.
https://www.zdnet.com/article/how-researchers-used-the-wannacry-kill-switch-to-track-the-ransomware-outbreak/
"WannaCry Ransomware Attack: The Role of Domain Registration in Tracking Down the Perpetrators." ICANN. June 15, 2017.
https://www.icann.org/news/blog/wannacry-ransomware-attack-the-role-of-domain-registration-in-tracking-down-the-perpetrators
"How security researchers tracked down the WannaCry ransomware authors." Ars Technica. May 26, 2017.
https://arstechnica.com/information-technology/2017/05/how-security-researchers-tracked-down-the-wannacry-ransomware-authors/

1401 Lavaca Street
Unit #375
Austin, TX 78701

information, install malicious software, and unknowingly escalate the threat actor's privileges. For example, in 2020, a phishing campaign targeting the World Health Organization was discovered, where attackers impersonated the organization to steal login credentials and other sensitive information.

In short, all of these malicious strategies have one thing in common: they start with the purposeful registration of domains. Domains are easily procured, affordable, disposable and most importantly, hard for targeted organizations to effectively limit without a sophisticated intelligence apparatus to do so. This holds true for both cyber criminals working for profit, as well as geopolitically motivated nation-state actors.

For example, if a nation-state adversary registers a domain that is similar to that of a legitimate organization, it may be a sign that they are planning a phishing or disinformation campaign. Similarly, if a cyber criminal group registers a domain that is similar to a corporation which qualifies as a worthy target, it may be a sign that they are intending to launch a spear-phishing campaign or conduct a ransomware attack.

Lastly, and closely related, domain squatting (cybersquatting) and trademark infringement can cause significant harm to businesses and individuals beyond the reasons mentioned above, including loss of brand recognition, damage to reputation, legal costs, and loss of revenue. It is more crucial than ever for businesses and individuals to take preemptive action to protect their domain names and trademarks.

Background

By analyzing and correlating the registration information of a domain, security analysts can identify the owner of the malicious domain, the hosting provider, and the IP address associated with the domain. This information can then be used to take the domain offline, identify related infrastructure, and ideally, prevent further infrastructure set up. Much of this information is derived by using a combination of publicly available via Whois websites, repositories, Internet scanners, and in the case of law enforcement agencies, subpoenas and warrants.

Interestingly, domain registration information is still sometimes perceived to be only valuable for threat actor attribution and only applicable to the intelligence community and law enforcement. While this information does indeed deliver tremendous value in determining the "*who*", it can be equally as valuable in ascertaining the "*what*", "*how*", and "*when*" of a given threat actor initiative.

1401 Lavaca Street
Unit #375
Austin, TX 78701

Several examples, among many, where domain registration information was integral to an intelligence or cybersecurity investigation include:

- The WannaCry ransomware attack: Domain registration information was used by cybersecurity experts to track down the perpetrators of the WannaCry ransomware attack in 2017. By analyzing the registration information of the domains used to spread the malware, researchers were able to identify the attackers and track their movements on the internet.

- Identifying and tracking down malicious actors: In 2019, the U.S. Department of Justice (DOJ) seized a domain associated with a botnet called "JabberZeus"[2] that had infected over one million computers worldwide. The DOJ was able to use information from the domain's registration to identify and track down the botnet's operator, leading to their arrest and the takedown of the botnet.

- The Emotet malware campaign: Domain registration information was used to take down the Emotet malware campaign in 2021. By analyzing the registration data of the domains used to distribute the malware, law enforcement agencies were able to disrupt the infrastructure of the malware and prevent further infections.

Despite multiple successful use cases, domain registration information analysis is not without its imperfections. In many cases, the information is incorrect, incomplete, or intentionally falsified, making linkages and pivots challenging. In other cases, certain domains are not registered by sophisticated threat actors until the attack has reached an appropriate stage (in order to limit early detection) which can result in an investigation going cold.

Likely the most problematic issue is the use of privacy protection services to obfuscate the registrant's identity and nefarious intent. Due to this, and the other limitations stated above, the efficacy of this kind of information has begun to diminish. These obstacles have inspired the Vigilocity team to pursue an novel and asymmetric approach as outlined below.

[2] "JabberZeus Botnet Taken Down in Global Operation," KrebsOnSecurity, September 10, 2019. https://krebsonsecurity.com/2019/09/jabberzeus-botnet-taken-down-in-global-operation/

1401 Lavaca Street
Unit #375
Austin, TX 78701

Methodology

Vigilocity has developed a proprietary methodology called "*Reverse Attack Surface Analysis*" or **RASA**, enabling security, intelligence, and risk professionals to identify emerging events, active and impending malicious cyber campaigns, predict future outcomes with a high degree of accuracy, and ultimately dismantle attacks.

What is RASA?

The premise of the RASA methodology is quite simple: "If an adversary were to attack us, what infrastructure vulnerability would they attempt to exploit and from where and when would that exploitation originate?" RASA operates on six foundational pillars:

1. Critical time-series analysis
2. Geopolitical tension and event analysis
3. Attack surface risk profiling and rating
4. Indexing of historical global domain registration data
5. Ingestion of real time global domain registration data
6. Correlation with open and closed source threat indicators

While this methodology is closely related to adversarial infrastructure analysis, RASA takes into account evidence of threat actor intention, as well as planned and active targets, which substantially assists in preempting future attacks. Additionally, RASA specifically identifies areas where threat actor operational security is faulty or inadequate which in many cases can expand an investigation into fortuitous and unforeseen directions. Most importantly, Vigilocity's unique domain registration intelligence platform uses RASA to deliver a linear perspective of the geopolitical landscape, as it reflects the intentions, plans, and actions of a wide range of actors, including individuals, organizations, and governments as well as their likelihood of overlap. This is crucial to identify visual patterns, outliers, and trends that are difficult, if not impossible, to detect through conventional analysis.

One of the key strengths of Vigilocity's RASA is its ability to identify emerging trends and subtle changes in the geopolitical landscape based on definitive outliers that clearly emerge in the data. This is essential for predicting future events, as even small changes can have significant implications. As articulated earlier, the RASA methodology is not based on intuition or guesswork, but on quantitative analysis, qualitative indicators, and

empirical evidence. This evidence is then used to rapidly respond to the emerging, active, or impending threat accordingly which may include (at minimum) continued surveillance of the threat actor, malicious infrastructure take down, security control updates, and law enforcement notification. The intention of this report is to exhibit several examples of actual events (historical and active) that could have been mitigated and in some cases prevented altogether had actions been taken supported by the findings illustrated herein.

Key Findings

The time period utilized for this analysis spans from January 1, 2020 through March 18, 2023. In that time period, over **12 million domains** were registered, by over **4 million registrants**, located in nearly **360,000 cities**.

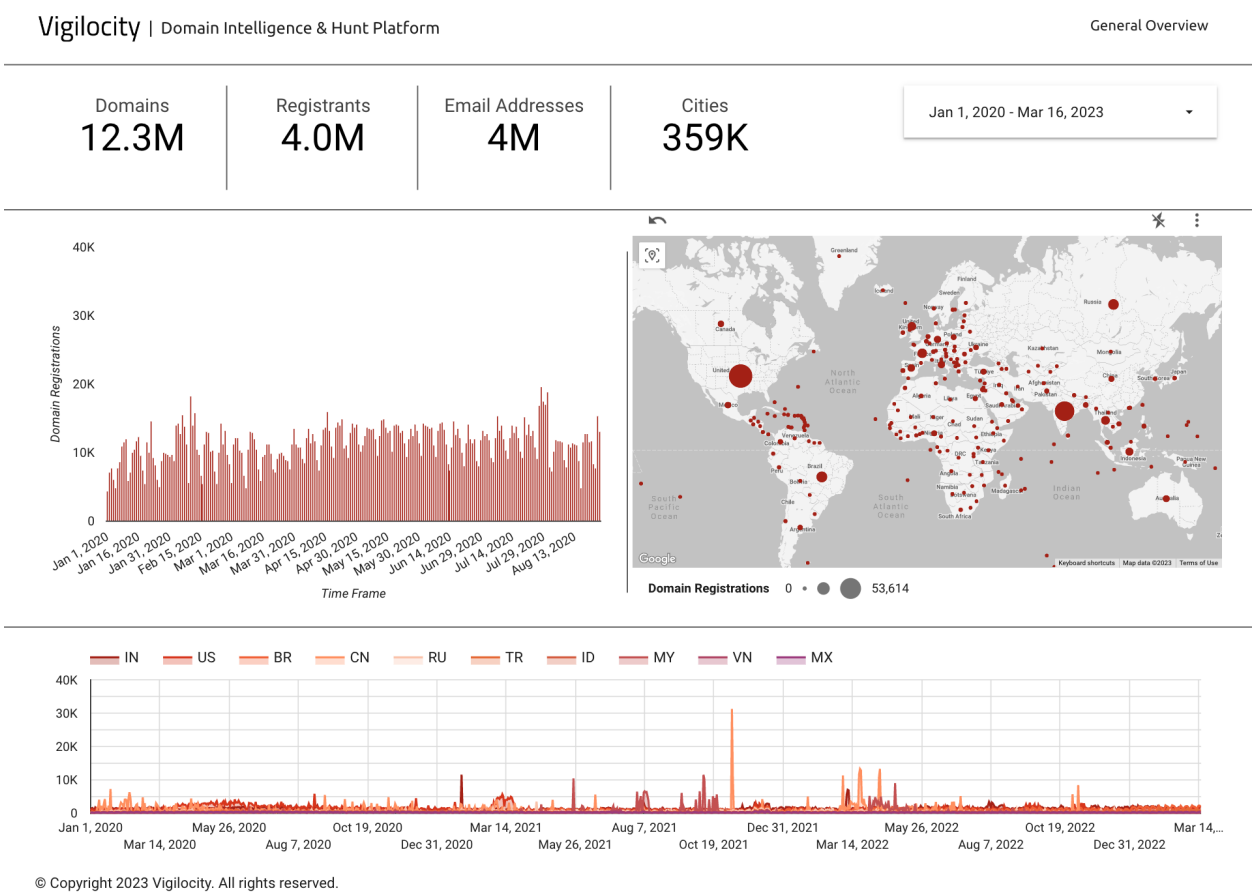


Figure 1. Domain registration sparkline articulating registrations from the top 10 countries from January 1, 2020 through March 16, 2023

In the figure above, the sparkline showcases several clear outliers of interest. Among other less prominent ones, the most notable outlier spikes happen around November of 2021, then April of 2022, and again in November of 2022. These "spikes" are the volume of daily domain registrations, colorized by the registrant's country, and represent an ideal starting point for further investigation.

November 1 - 7 2022 - Emerging Phishing and Influence Campaign Infrastructure

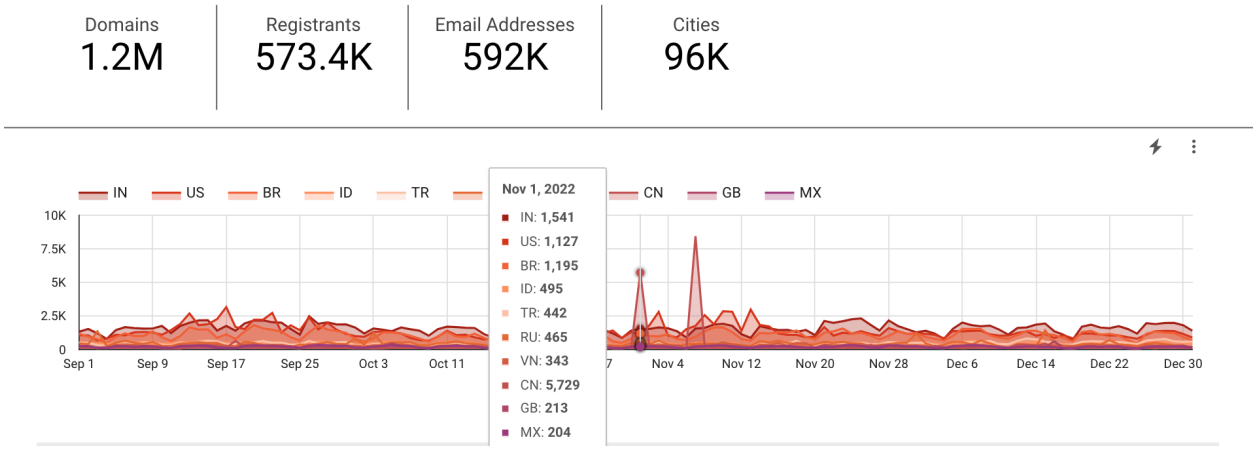


Figure 2. Highlight of domain registrations on November 1, 2022

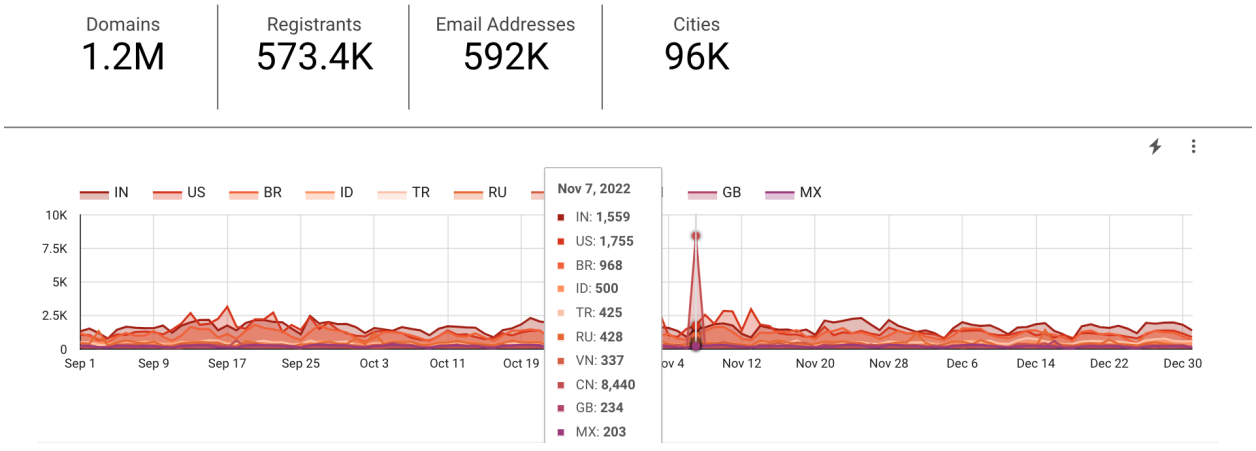


Figure 3. Highlight of domain registrations on November 7, 2022

On November 1, 2022, there were **5,729** domains registered by Chinese actors. Six days later, on November 7, 2022, there were another **8,440** domains registered again by Chinese actors.

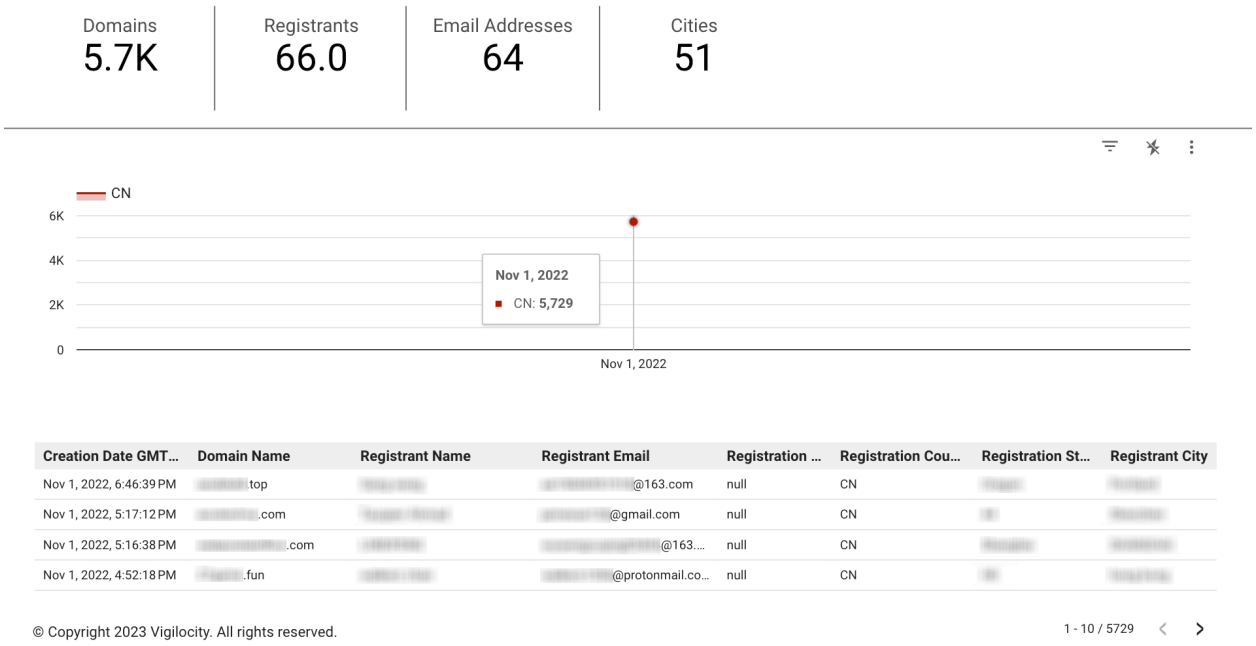


Figure 4. Highlight of domain registrations on November 1, 2022 including redacted registrant details

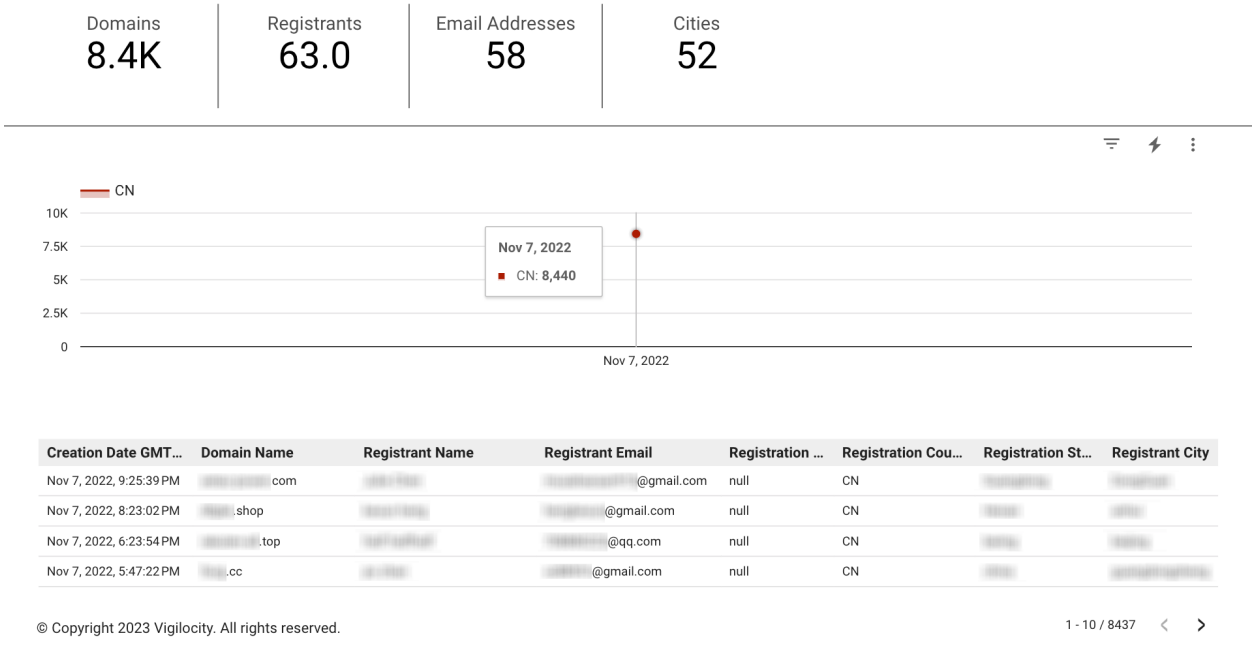


Figure 5. Highlight of domain registrations on November 7, 2022 including redacted registrant details

In the figures above, it is important to note that collectively, over **14,000** domains were registered on November 1, 2022 and November 7, 2022 by only **66** and **63** registrants respectively. By any standard, that is a fairly large number of domains to be purchased at one time by a relatively small number of registrants. Malicious or benign, this could indicate a fairly well-funded operation.

Figure 6. Highlight of domain registrations from October 31, 2022 through November 8, 2022

The single most prolific registrant, responsible for registering almost all of the **14,000** domains in *two days*, has no historical record of any other domain purchases in the timeframe of this report. The vast majority of the domains follow a templated sequence of six digits in consecutive order (ie. 000054) and have either a .click or .top TLD.

Infrastructure Cost

If we consider the economics, assuming that domains were purchased in bulk, the discounted per domain cost would be around $2.00 at minimum. All of the domains have privacy protection enabled which can cost anywhere from $3 to $20 per domain. This is a highly conservative estimate as the domains were all registered for one year which means fewer discounts.

Assuming the cost estimates are accurate at the lowest end of the spectrum, the total cost of this domain infrastructure setup would be approximately **$70,000** by a single registrant over the course of *two days*.

March 1, 2022 - April 15, 2022 - Confirmed Chinese Phishing Infrastructure

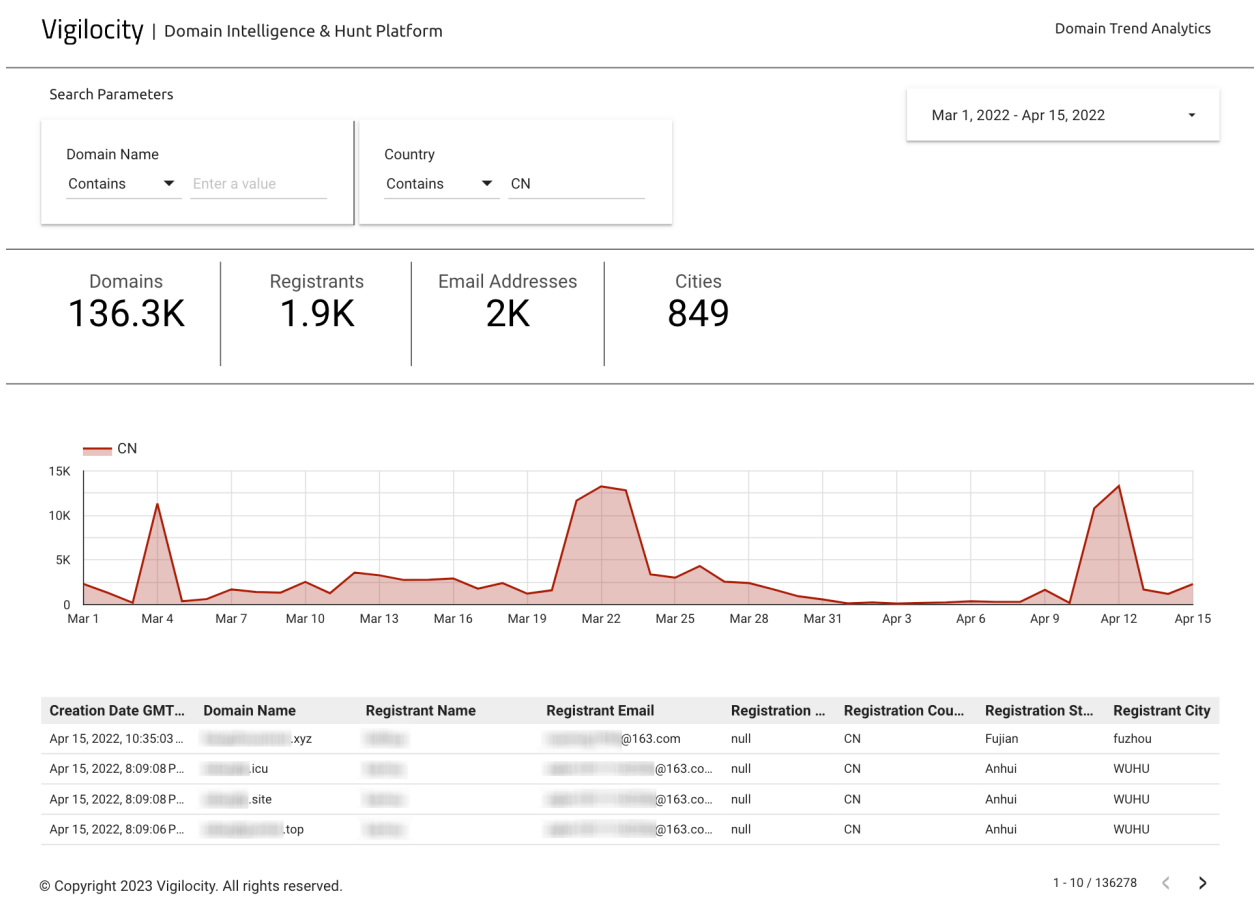


Figure 7. Highlight of domain registrations by Chinese actors between March 1, 2022 and April 15, 2022

As seen in the figure above, between March 1, 2022 and April 15, 2022, over **135,000** domains were registered by Chinese actors. The most notable outliers are as follows:

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 registered all follow a similar DGA construct as earlier examples: a six character mixture of letters and numbers ending in several TLDs (.pw, .net, .icu, etc.). Most interestingly, after a cursory check on whether any of the domains have been flagged for abuse, only a single domain has been suspended on August 18, 2022 due to phishing. This domain was originally registered April 11, 2022 which means that this domain was still actively functioning for more than 5 months. As of this writing, the remaining domains appear to be still active.

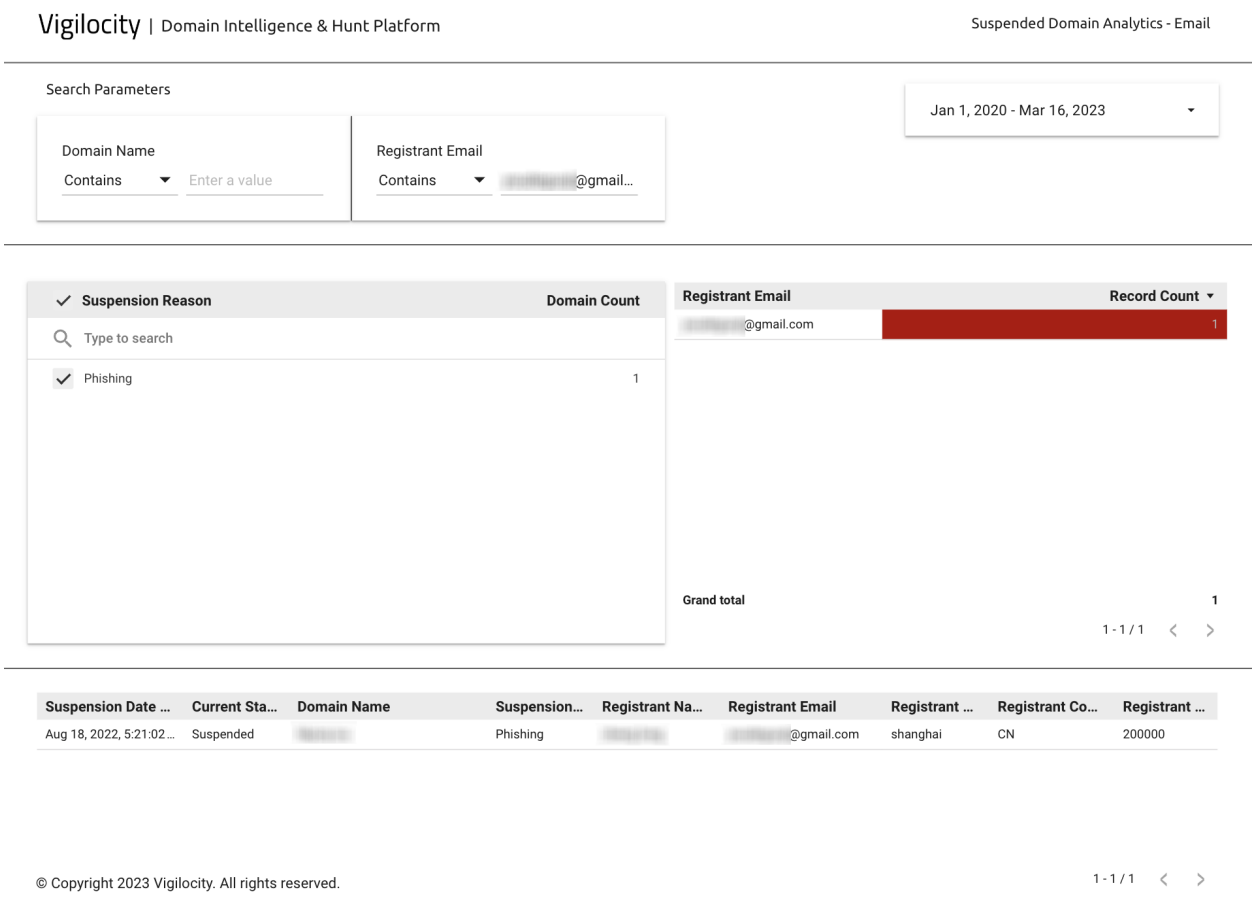


Figure 8. Highlight of only a single domain suspension due to phishing

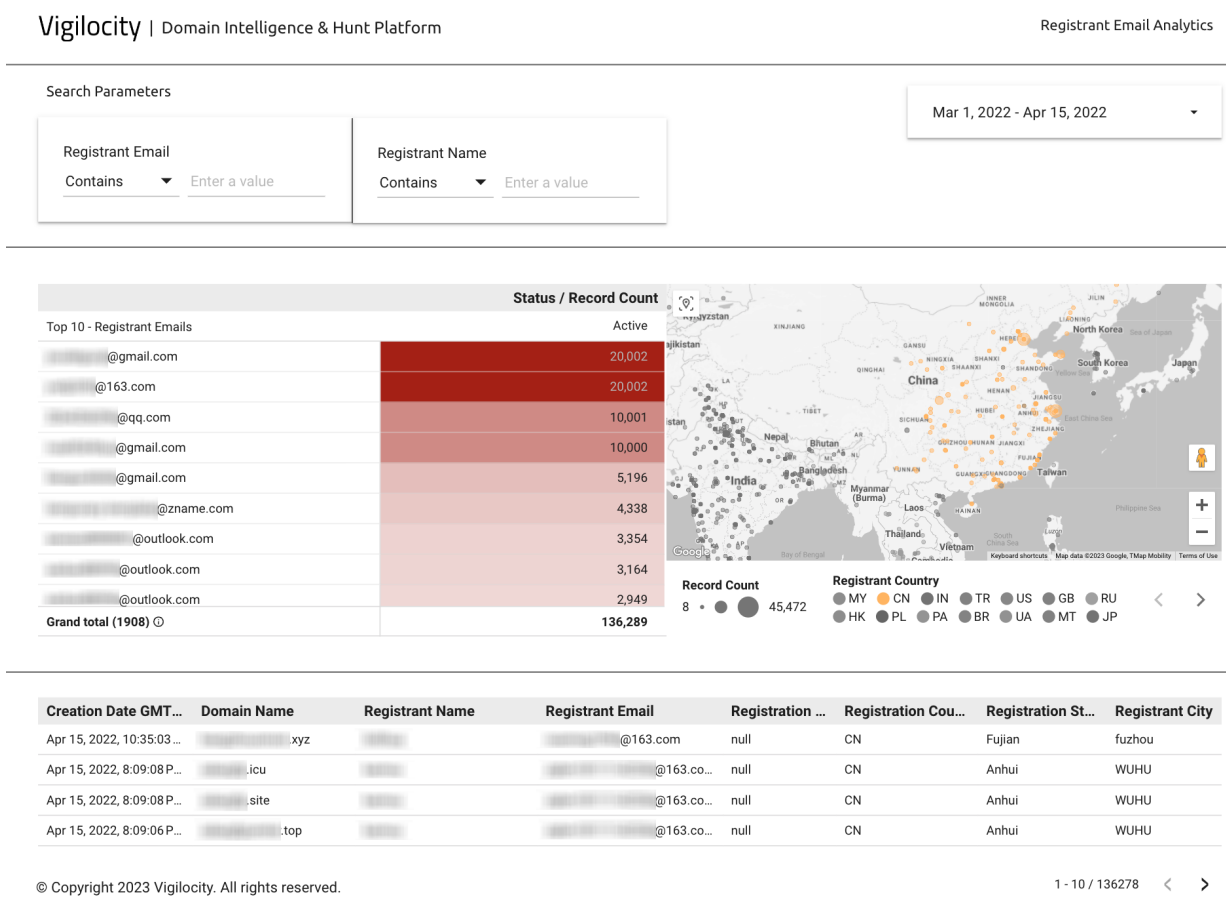


Figure 9. Highlight of domain registrations by Chinese actors between March 1, 2022 and April 15, 2022

Again, the vast majority of domains have been registered by only **4** unique registrants (email addresses).

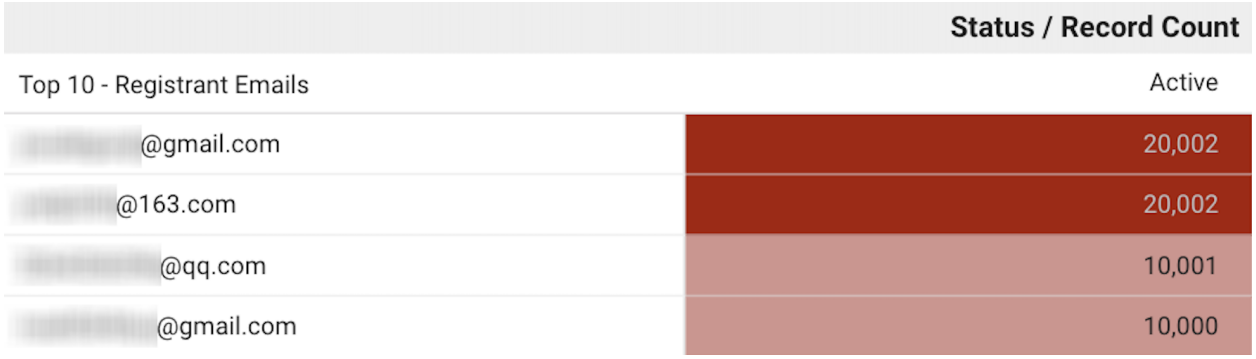


Figure 10. Highlight of an automated domain registration distribution by Chinese actors between March 1, 2022 and April 15, 2022

Furthermore, as seen in the figure above, each of the 4 registrants are responsible for almost perfect allocations (20,002, 20,002, 10,001, and 10,000 respectively) lending further confidence that the registrations are automated.

Infrastructure Cost

Considering the same economics as above, and assuming that domains were purchased in bulk, the discounted per domain cost would be around $2.00 at minimum. All of the domains have privacy protection enabled which can cost anywhere from $3 to $20 per domain. Again this is a highly conservative estimate as the domains were all registered for one year which means fewer discounts.

Assuming the cost estimates are accurate at the lowest end of the spectrum, the total cost of this domain infrastructure setup would be approximately **$300,000** by allegedly **4** registrants over the course of *6 days*.

November 7, 2021 - Massive Single Day Infrastructure Setup

In an even more dramatic example of a likely well-funded operation, in the figure below, an impressive **41,228** domains were registered between November 6, 2021 and November 9, 2021 by **171** Chinese registrants. As can be seen in the figure below, the majority of the domains (**31,275**) were registered on November 7, 2021.

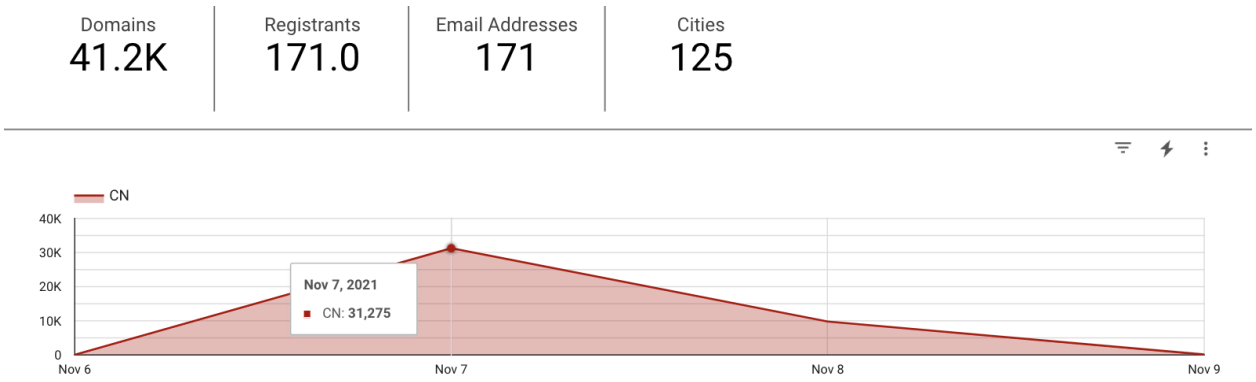


Figure 11. Highlight of domain registrations by Chinese actors between November 6, 2021 and November 9, 2021

It is worth noting that while it is still unconfirmed what the intended use was for such a vast number of domains, several geopolitical events correspond with the timing of the purchase, most critically the passing of Biden's $1.2 trillion Infrastructure Bill by Congress.[3]

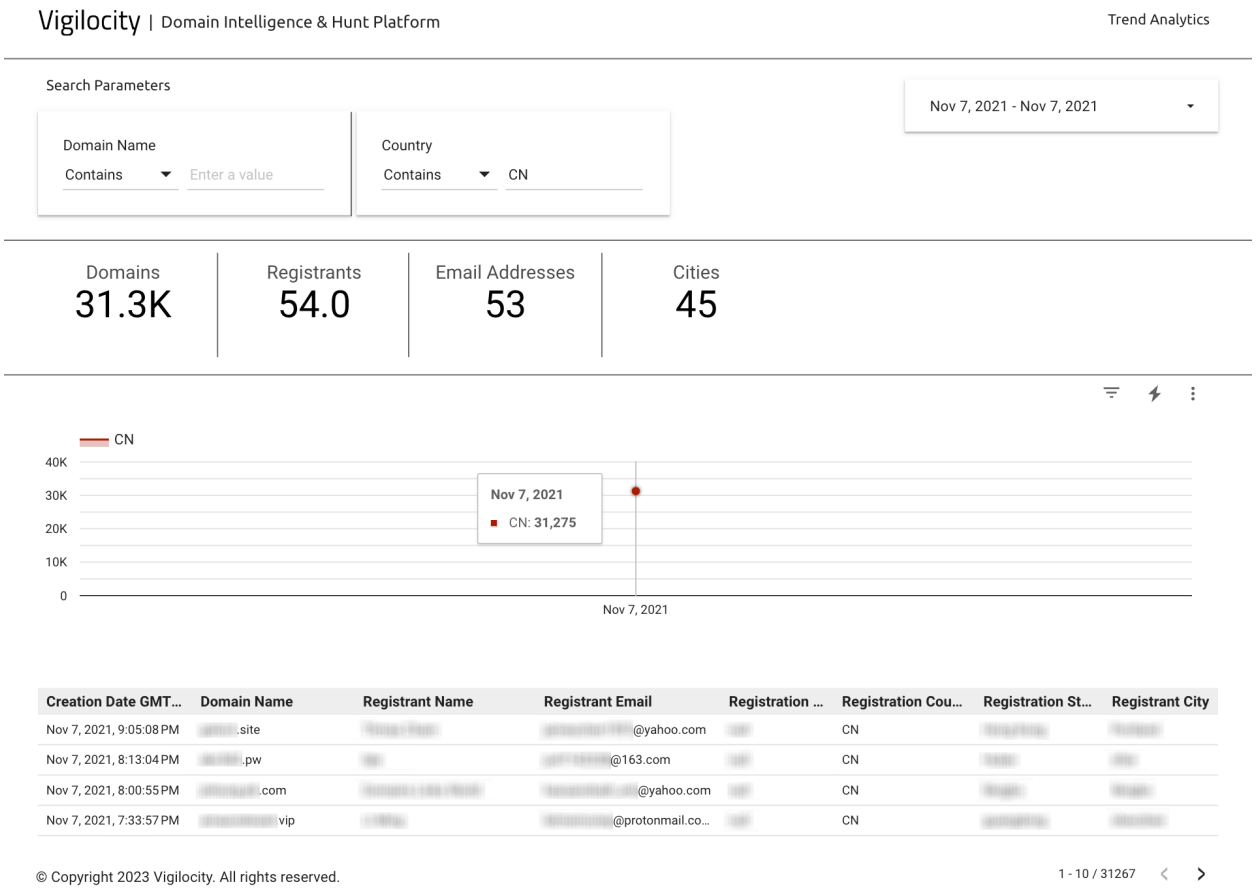


Figure 12. Highlight of domain registrations on November 7, 2021 including redacted registrant details

Most of the domains registered are composed of a string of six numbers and letters utilizing a variety of TLDs (including .cl, .uk, .icu, etc.) indicative of a DGA (domain generation algorithm) utility. In addition, all of the domains were registered on the same day increasing the confidence that the intention of this effort is nefarious. Of the entire list of domains registered, it becomes clear that only three Chinese registrants are alone responsible for **31,187** domain registrations between November 1, 2021 and November 7, 2021 with a single registrant alone responsible for **25,840** registrations.

[3] "'Powerful signal': Biden's infrastructure bill sends message to China." Politico. August 7, 2021
https://www.politico.com/news/2021/08/07/biden-infrastructure-bill-message-china-502739

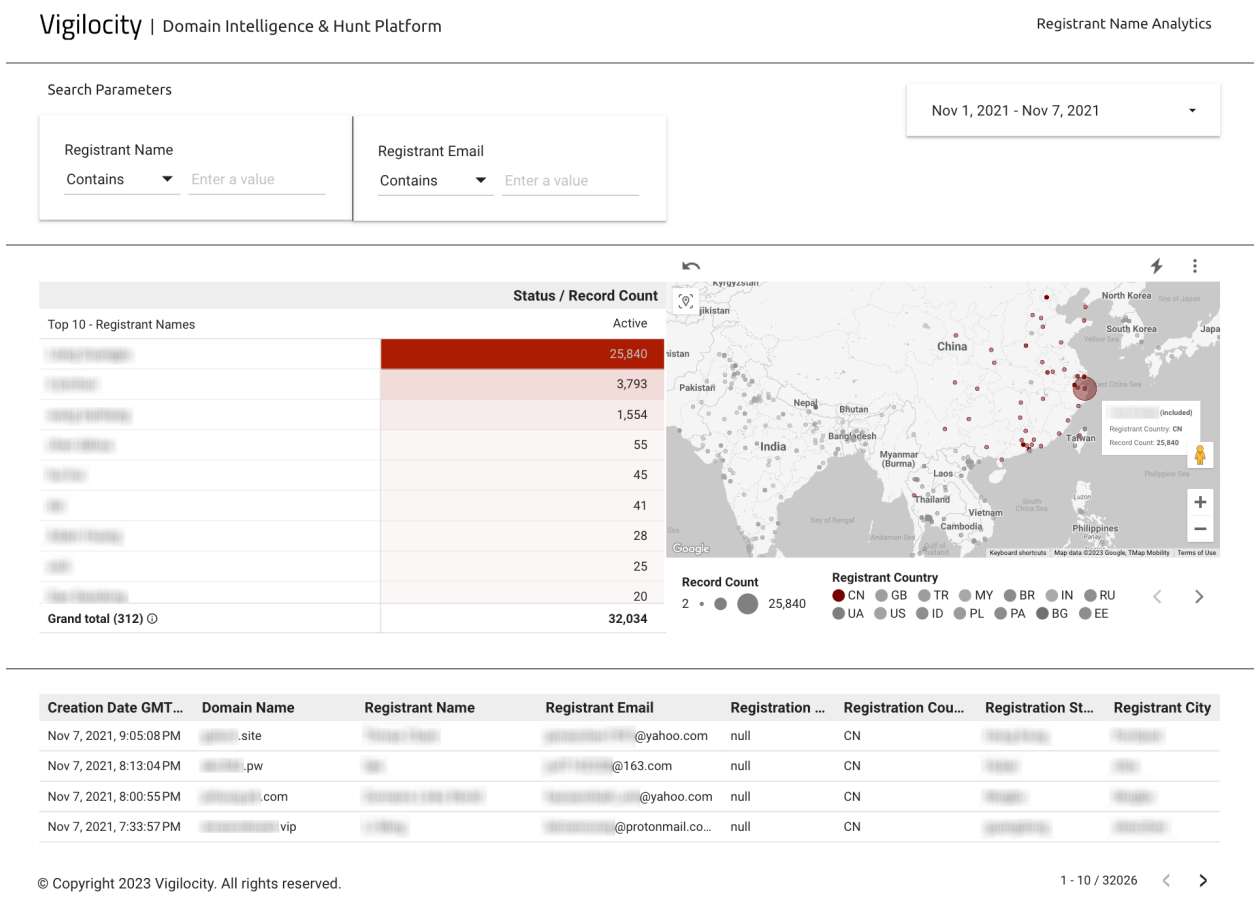


Figure 13. Highlight of Chinese registrants from November 1, 2021 to November 7, 2021

Infrastructure Cost

Considering the same economics as above, and assuming that domains were purchased in bulk, the discounted per domain cost would be around $2.00 at minimum. All of the domains have privacy protection enabled which can cost anywhere from $3 to $20 per domain. Again this is a highly conservative estimate as the domains were all registered for one year which means fewer discounts.

Assuming the cost estimates are accurate at the lowest end of the spectrum, the total cost of this domain infrastructure setup would be approximately **$129,200** by allegedly **1** registrant over the course of *1 day*.

By correlating the most prolific actor's name and email address, we were able to pivot to identify all the domains registered from January 1, 2020 to March 16, 2023 which amount to **28,999** domains as seen in the figure below.

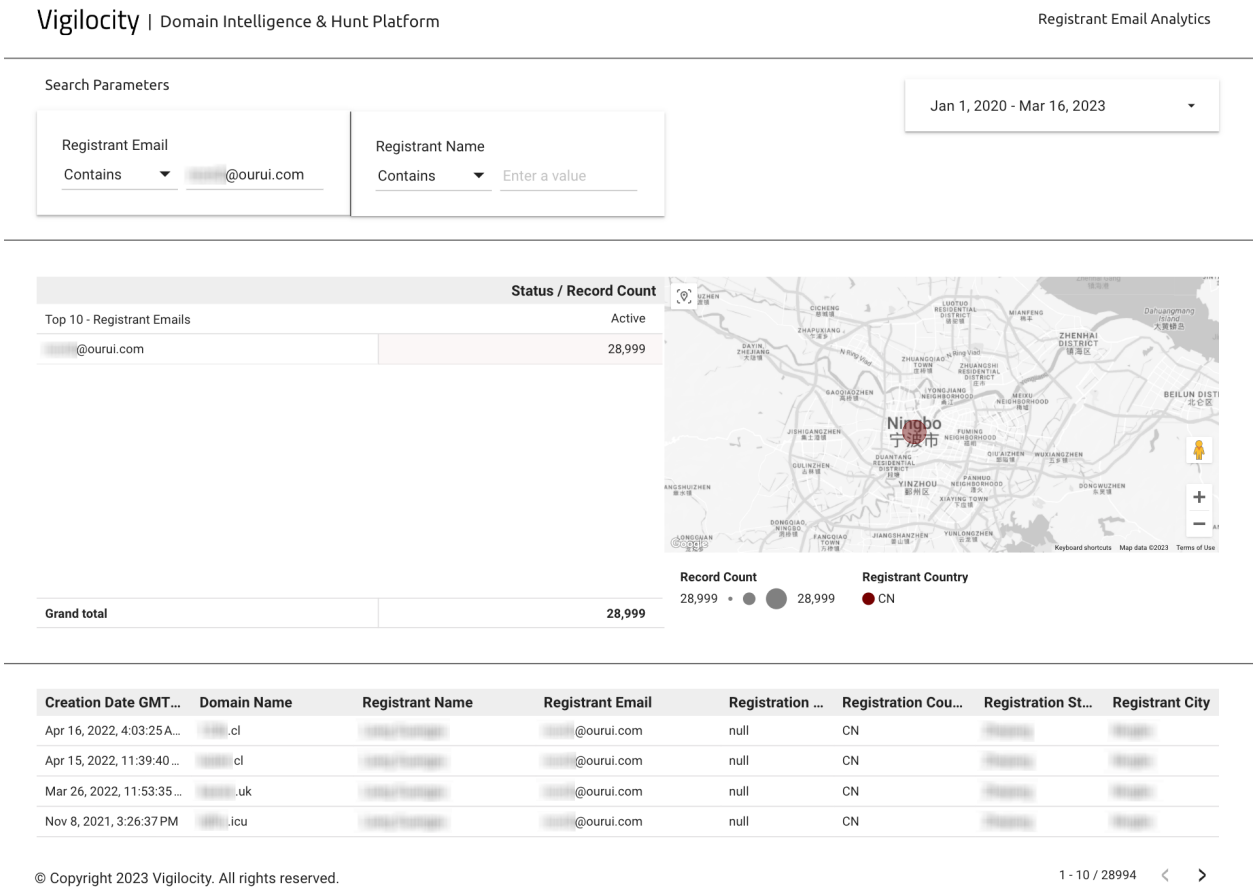


Figure 14. Highlight of a prolific Chinese actor's registrations from January 1, 2020 to March 16, 2023

The additional domains identified by the broader time frame search exhibit repeatability in the registrant's tactics. That being said, there are no domains registered by the actor predating November 7, 2021 and past November 8, 2021, there were only 3 domains purchased. The dates are as follows:

March 26, 2022	1
April 15, 2022	1
April 16, 2022	1

Lazy OpSec and Repeatable Patterns

Even the most sophisticated threat actor will sometimes fail to employ critical operational security (OpSec) to maintain anonymity and obfuscation. Utilization of the same email addresses, moniker (name), address detail, failure to use a proxy or vpn to mask their IP address, or consistent use of the same registrar provide valuable indicators to security analysts to link and pivot otherwise disparate infrastructure. In many cases, the threat actor will choose to enhance their OpSec months or years after starting down a path which leaves an indelible digital trail that can be discovered and used to deobfuscate their activity and infrastructure. In the following example, the actor appears to be running a successful phishing campaign using the same name and email address for over **1,800** DGA generated domain registrations.

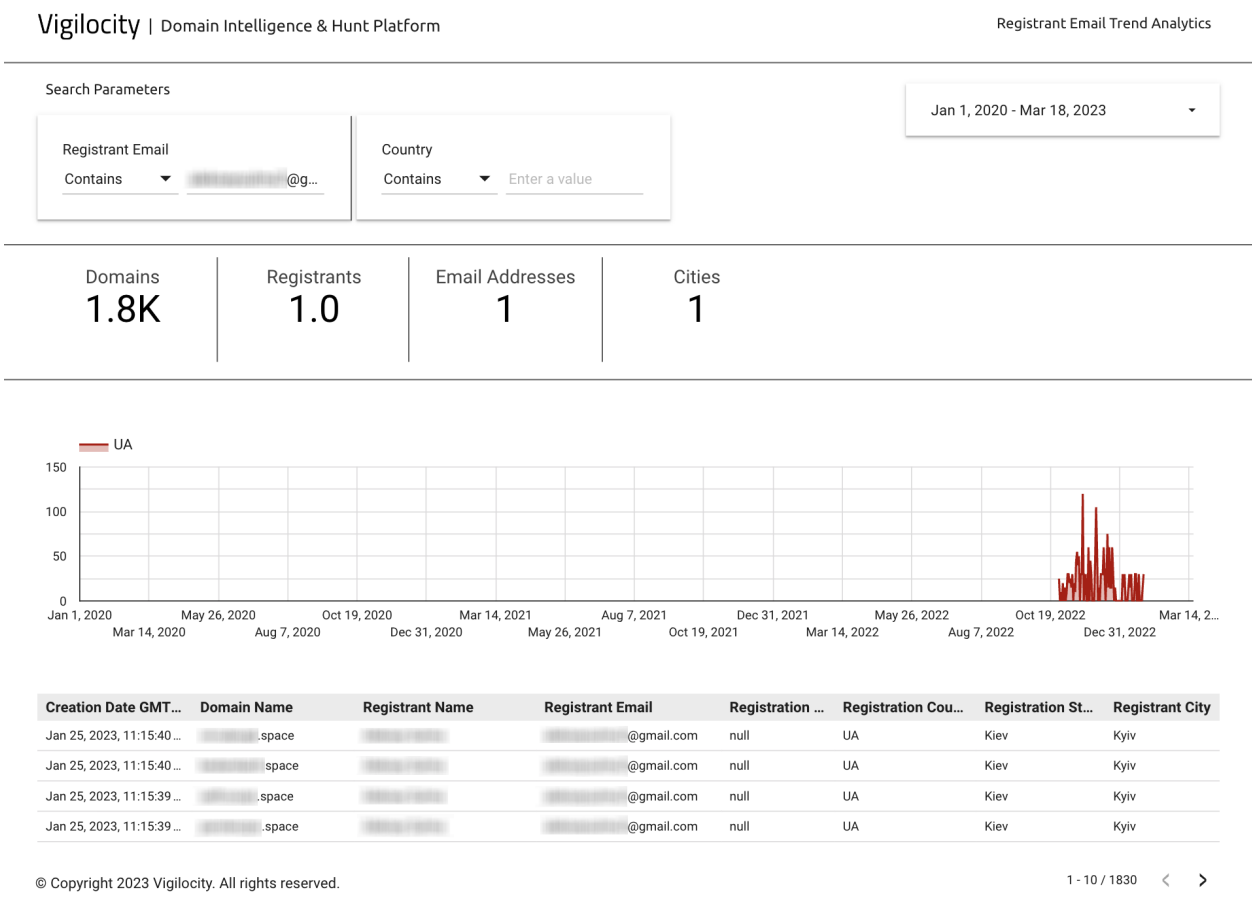


Figure 15. Highlight of DGA generated domains from January 1, 2020 through March 18, 2023

1401 Lavaca Street
Unit #375
Austin, TX 78701

When over **1,160** of the domains were suspended due to being flagged as phishing domains, the actor pivoted to a newly created moniker, email account, and registration account *at the same registrar* and attempted to resurrect the campaign as seen in the figure below.

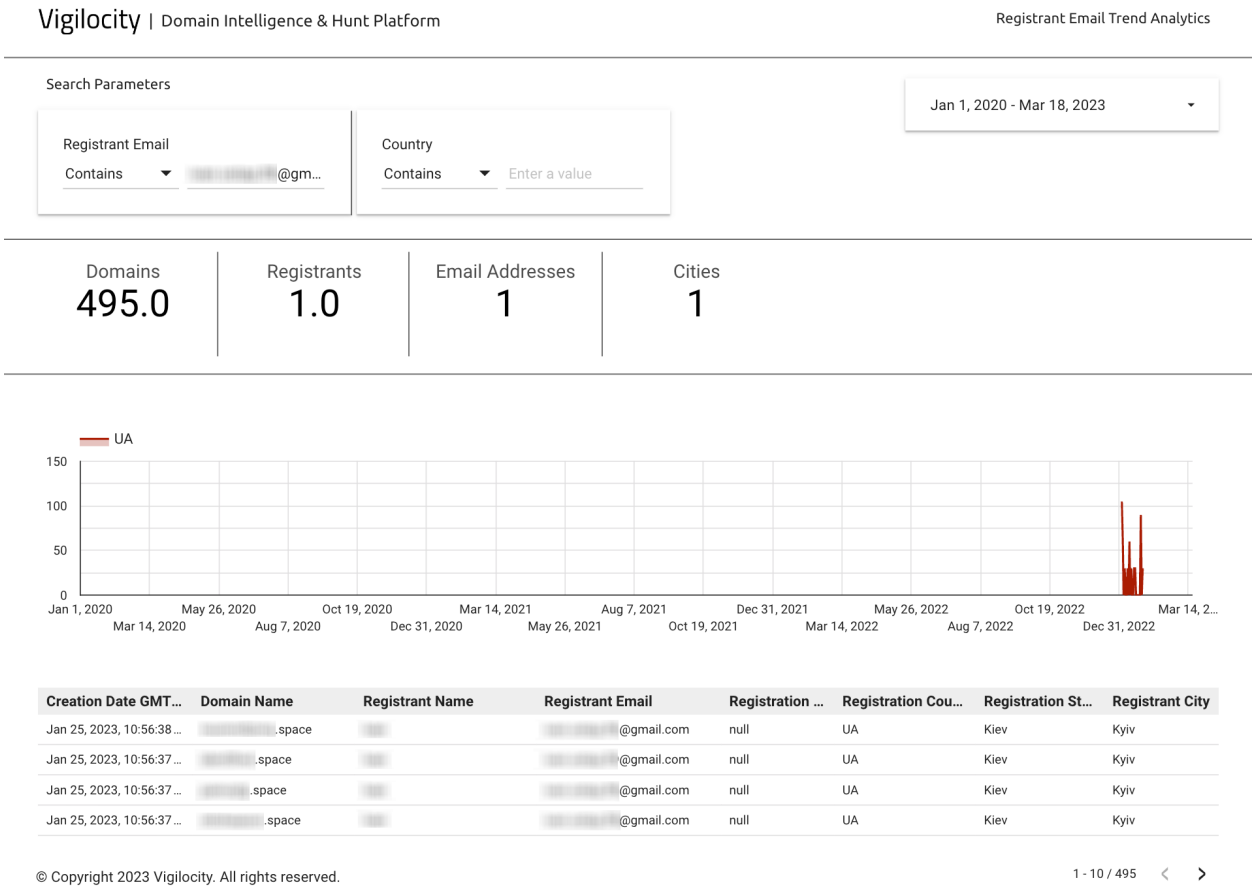


Figure 16. Highlight of DGA generated domains from January 1, 2020 through March 18, 2023

It is important to note that early detection of this behavior can help mitigate the widespread damage caused by phishing campaigns as well as reduce stage escalation leading to ransomware. That being said, it is critical to employ a wide aperture across a broad historical timeline in order to illuminate otherwise hidden patterns and behavior.

In addition to the emergence of patterns, early testing and experimentation by the threat actor can be identified and used to produce valuable links and correlations between what was formerly thought to be disparate events or infrastructure.

In the example below, the actor utilized a single email address across **1,400** domain registrations but used **96** different monikers (registrant names) and **75** different cities. This is a high confidence indication that some level of automation is being used, lending further evidence that a domain generation algorithm (DGA) is being employed by the actor. The domains are composed of similar word and number combinations coupled with one of two TLDs: .pw and .site

This actor began registering domains as early as January 2, 2020 and has continued to successfully register domains utilizing the same email address as recently as March 1, 2023. This further underscores the ease by which malicious actors are able to stay undetected for long periods of time and conduct phishing campaigns that span months, if not years.

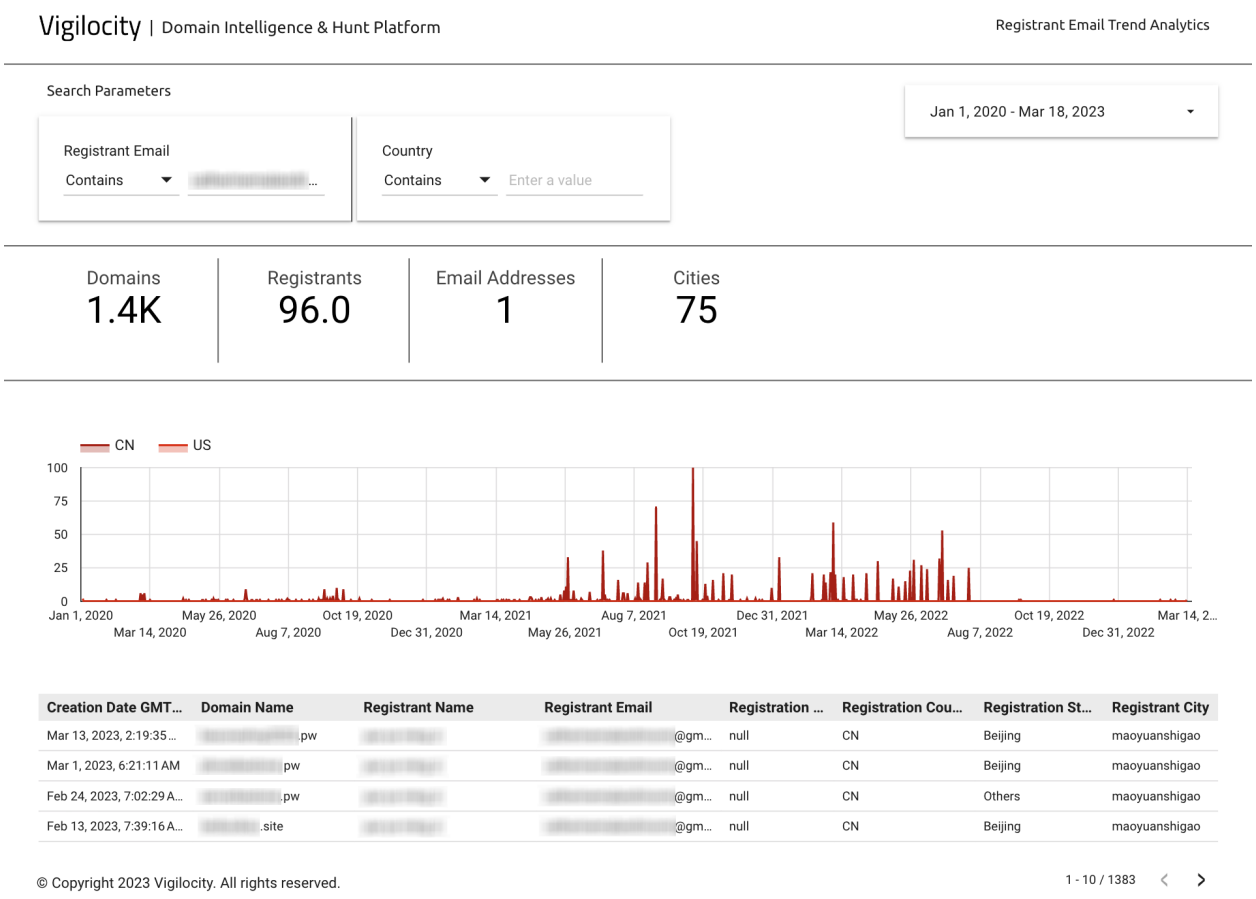


Figure 17. Highlight of DGA generated domains from January 1, 2020 through March 18, 2023 using a single email address tied to 96 different names

Malware and Dropper Domains

Staged attacks often involve the registration of a domain(s) at a designated time in order to prevent early detection. In the following example, this actor was responsible for the widely known PARALAX loader maldoc campaign. The Elastic Security Labs team conducted a thorough analysis of the campaign and shared: "PARALLAX is a full-featured modal backdoor and loader featuring defense evasion and information on stealing capabilities, first observed in 2020 and associated with COVID-19 malspam campaigns. NETWIRE is a mature and cross-platform RAT that was first observed in 2012."[4] It is important to note that there is a distinct gap in the registration timeline between May 17, 2022 and August 8, 2022 as can be seen in the figure below.

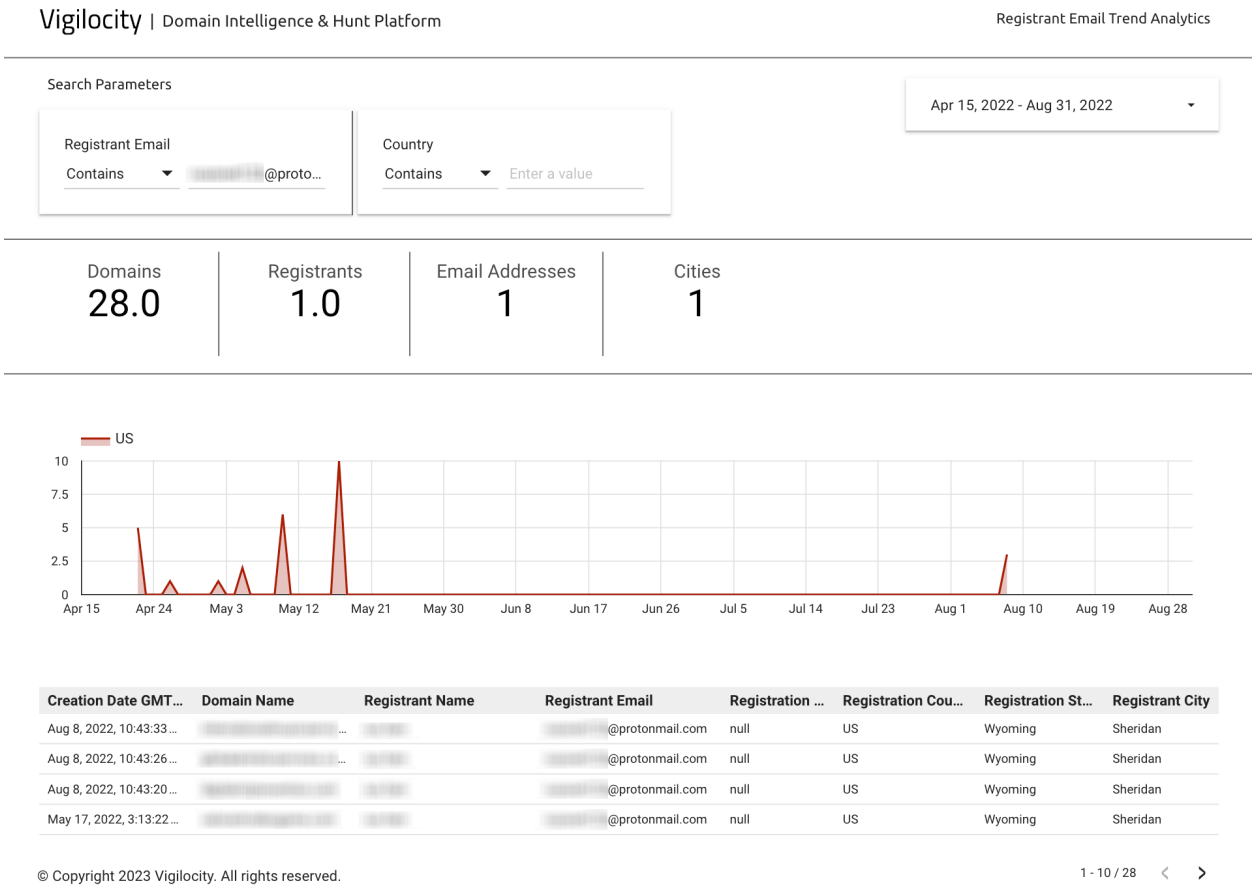


Figure 18. Highlight of the domain registration timeline associated to the PARALAX loader maldoc campaign

[4] "Exploring the REF2731 Intrusion Set" September 30, 2022 https://www.elastic.co/security-labs/exploring-the-ref2731-intrusion-set

While the campaign above appears to have been fully deconstructed, unfortunately many threat actors continue to expand their operations even after a portion of their infrastructure has been successfully identified and rendered inert.

In the following example, this threat actor has continued to engage in a multi-year (November 4, 2021 - present) Crypto Phishing and Credential Stealer campaign with relatively low to zero mitigation. This "*low and slow*" effort has proven to be very effective as unlike the early examples of incredibly vast numbers of domains being registered at once, this actor averages about six domains registered almost daily.

There is clearly an intentional effort to keep the registrations sporadic and moderately low to avoid triggering anti-bot defenses. However, the vast majority of domains, again, match a DGA created template.

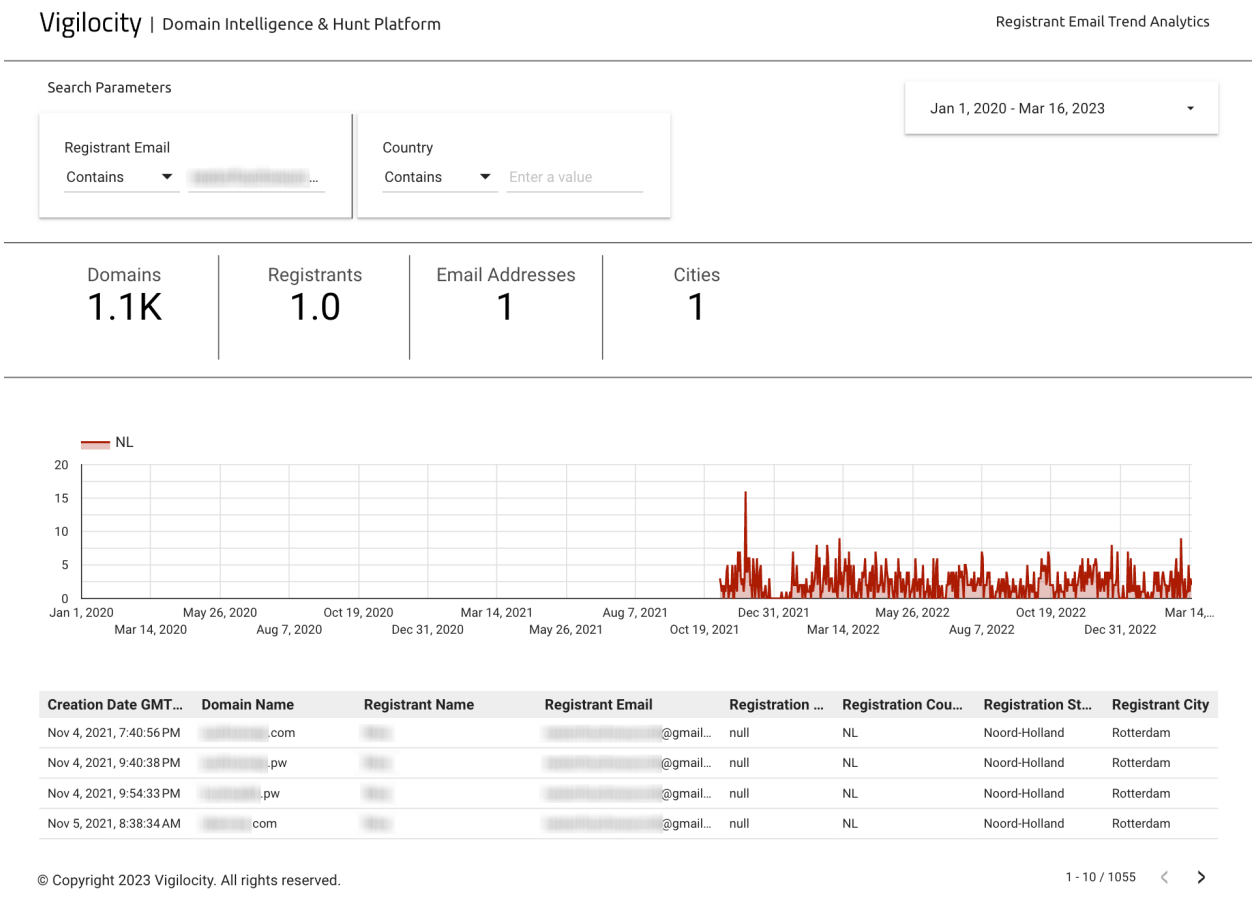


Figure 19. Highlight of an ongoing multi-year (November 4, 2021 - present) Crypto Phishing and Credential Stealer campaign

Reconnaissance and Ransomware

An essential part of any ransomware campaign is the successful reconnaissance of the victim's network. This can be achieved by the deployment and utilization of custom malware, but as witnessed in the last several years, perhaps even more effectively through the use of Cobalt Strike.

Cobalt Strike provides a wide range of features for attackers, including the ability to create custom malware and execute it on compromised systems, conduct port scanning and enumeration, create and manage command-and-control servers, and simulate different types of attack scenarios. Ironically, the tool was designed to be used by security professionals to test the effectiveness of their organization's security defenses.

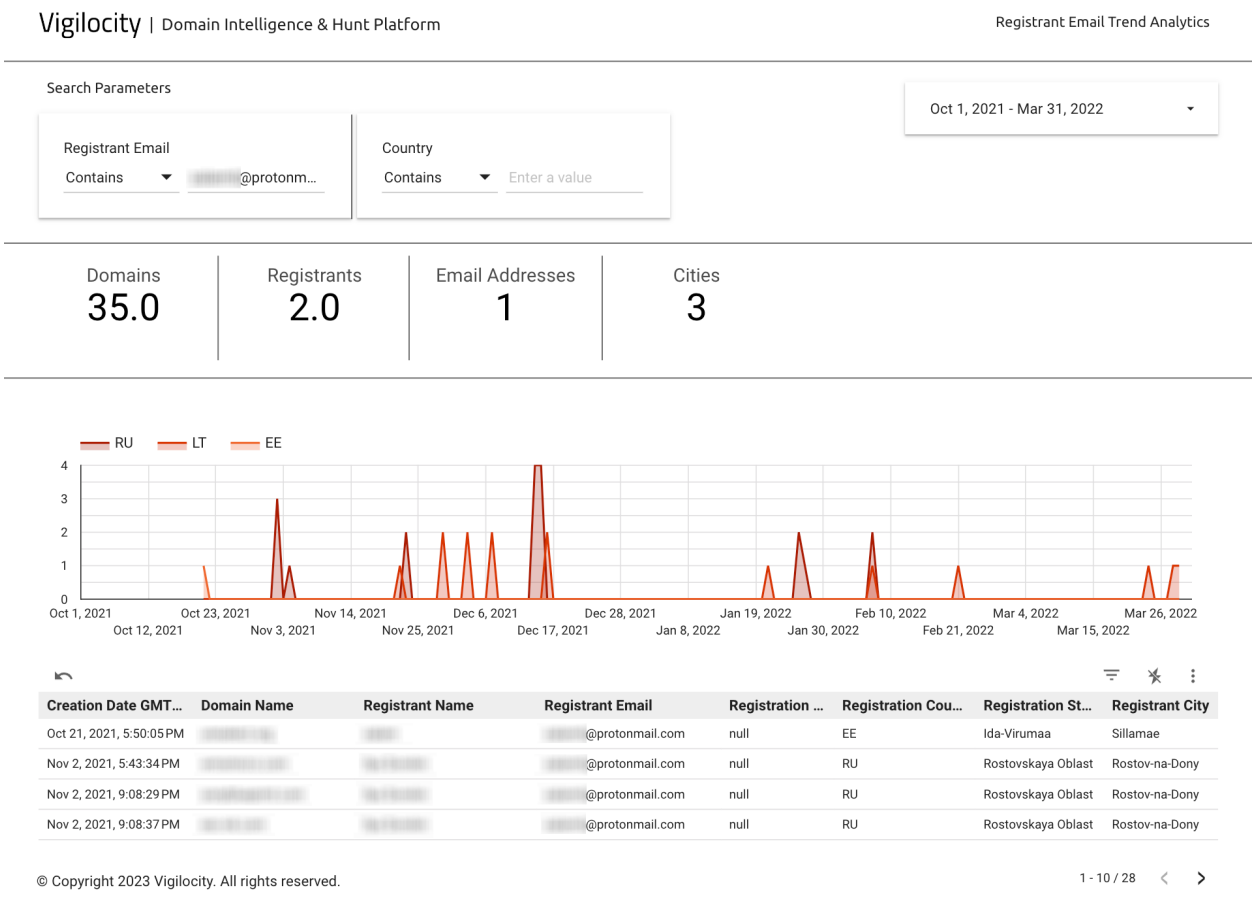


Figure 20. Highlight of domain registrations associated with a number of Cobalt Strike servers as a part of the initial stages of a ransomware campaign in late 2021

1401 Lavaca Street
Unit #375
Austin, TX 78701

In the example above, the threat actor registered the first domain on October 21, 2021 under a specific name and email address. Shortly thereafter, on November 2, 2021, the actor continued to register more domains using a different name, but the same email address and allegedly from a different country.

A total of **35** domains were registered between October 21, 2021 and March 29, 2022, most of which were Cobalt Strike servers. Once a threat actor has collected and analyzed an adequate amount of reconnaissance to proceed to the next stage of the attack, the encryption utilities are deployed rendering the victim generally powerless. As can be seen in the diagram above, unfortunately the threat actor was left uninterrupted and unimpeded for over four months. By efficiently identifying and dismantling the threat actor's reconnaissance infrastructure, attack escalation can be mitigated and in some cases ransomware avoided completely.

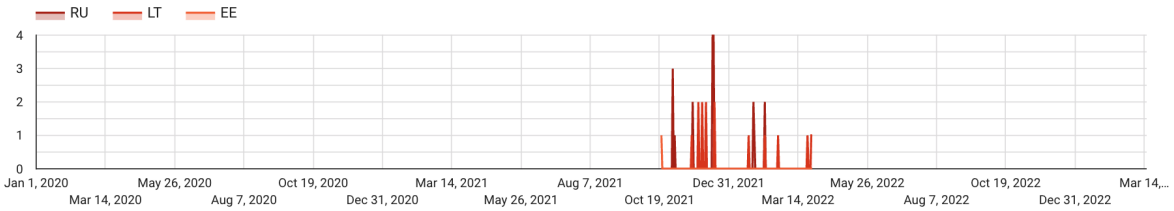


Figure 21. Highlight of a wider aperture of the same actor's activity from January 1, 2020 through March 16, 2023

As can be seen from the diagram above this appears to be an isolated event to collect reconnaissance on victim networks and rapidly move onto subsequent stages of the attack, such as ransomware.

Infrastructure Cost

Looking at this from an inverse angle, and assuming that the domains were not purchased in bulk, the per domain cost would be around $10.00 at minimum, considering they are primarily .com and .org domains.. All of the domains have privacy protection enabled which can cost anywhere from $3 to $20 per domain.

Assuming the highest reasonable costs, this domain infrastructure setup would total approximately **$1,050** by allegedly **1** registrant. Juxtaposed against a lucrative ransomware campaign that can potentially net millions of dollars, one can easily see why this is a popular and motivating tactic among threat actors.

1401 Lavaca Street
Unit #375
Austin, TX 78701

Cybersquatting and Trademark Infringement

Utilizing a quick search for a keyword such as “pepsi” resulted in several domains registered as recently as March 8, 2023 that are likely trademark infringement violations. More concerningly is the potential for these domains to be used to send convincing phishing emails to unsuspecting victims.

A total of **176** domains were registered from January 1, 2020 to March 16, 2023 embedding the word “**pepsi**” as seen in Figure 9 below. Further research indicates that at least two of the domains were suspended by the registrar. The reason provided for the suspension was “Scam website”.

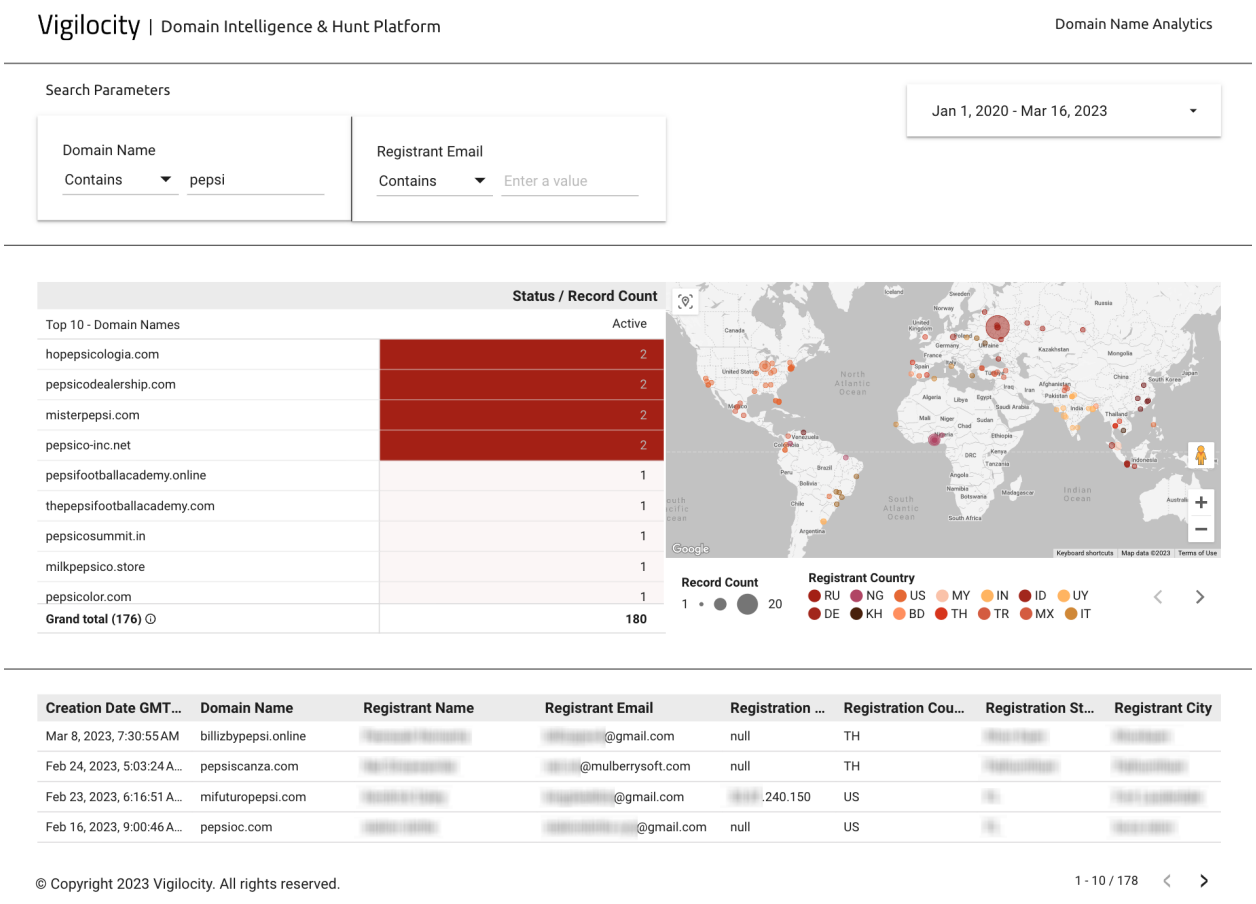


Figure 22. Highlight of potential cybersquatter domains for “pepsi” from January 1, 2020 to March 16, 2023

In a related search, a total of **63** domains were registered embedding the word "**cocacola**" in the same time period as seen in the figure below.

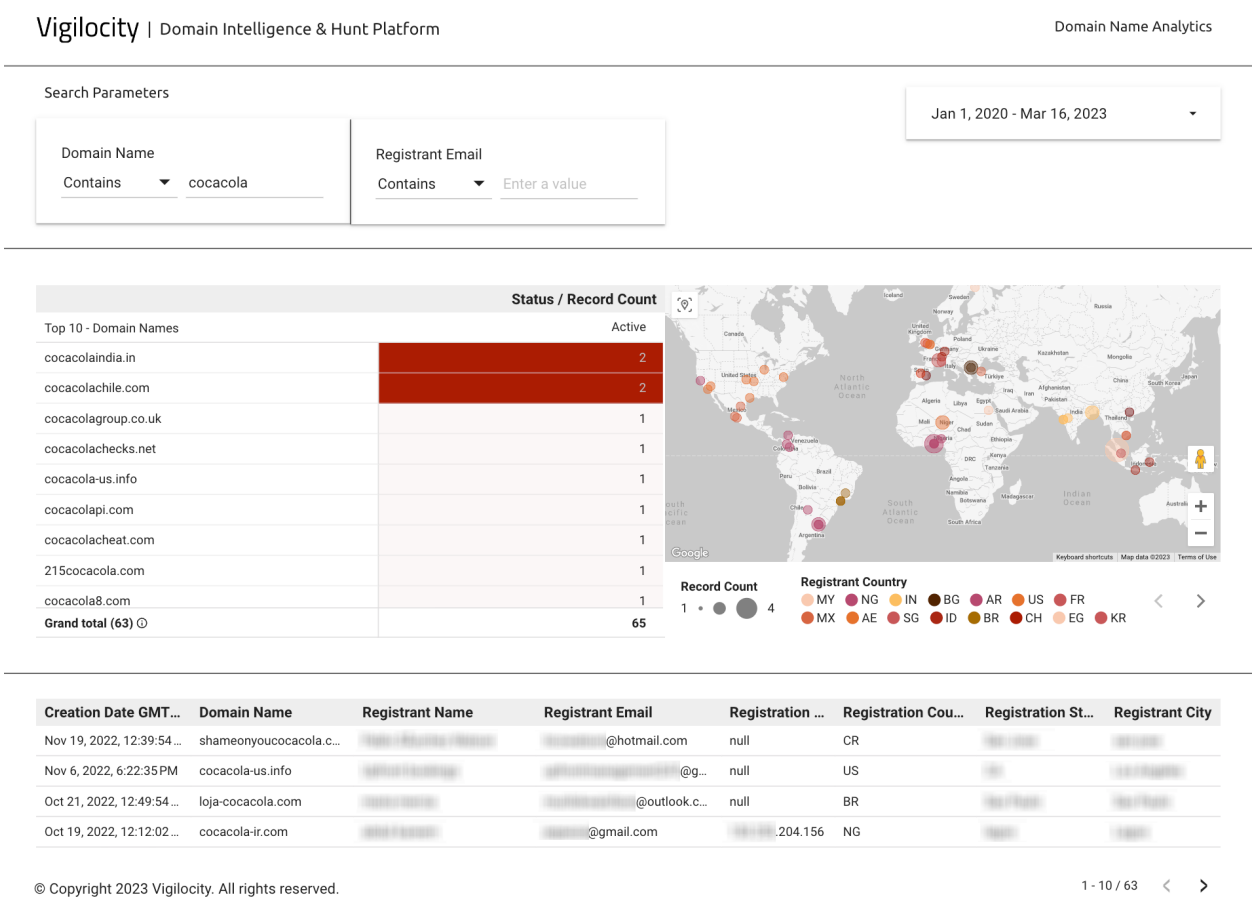
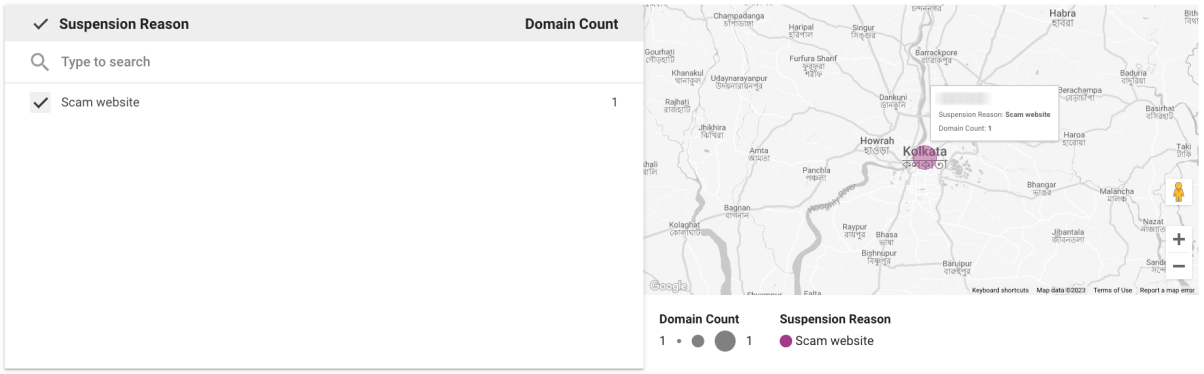


Figure 23. Highlight of potential cybersquatter domains for "cocacola" from January 1, 2020 to March 16, 2023

In dealing with cybersquatters, companies can file a complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) to recover domain names that are identical or confusingly similar to their trademark. Companies can also seek legal action against cybersquatters who are using their domain names in bad faith, such as for phishing scams or other fraudulent activities.

While these strategies can be effective in dealing with trademark infringement and cybersquatting, success may vary depending on the severity of the infringement and the resources available to the company. It is essential for companies to take proactive steps to protect their intellectual property and be prepared to take legal action when necessary.

As can be seein the figure below, only one of the domains was successfully deleted by the registrar on July 14, 2022, however it was registered on December 1, 2021. That represents approximately eight and a half months that the domain was live and resolving.



Suspension D...	Current Status	Domain Name	Suspension R...	Registrant Na...	Registrant E...	Registrant Ad...	Registrant City	Registrant Co...	Registrant Zip
Jul 14, 2022, 5:1...	Deleted	cocacolaindia.in	Scam website	[redacted]	[redacted]	[redacted]	[redacted]	IN	700001

Figure 24. Highlight of the deletion of a domain embedding the word "cocacola" from July 14, 2022

Several other likely trademarked and phishing keywords were searched for within the same period (January 1, 2020 - March 16, 2023) and the results were as follows:

Keyword	Domains Registered	Registrants	Top 10 Countries
internalrevenue	12	12	US, NG, SG, MX
blackrock	88	71	US, IN, IE, GB, FR, RU, NG, BR, VE, CR
jpmorgan	87	68	US, NG, GB, IN, BG, PL, CN, TR, BR, MY
bloomberg	41	34	US, IN, KE, CN, NG, ZA, RU, PK, TR, GB
americanexpress	46	36	US, IN, NG, IT, ID, GB, CN, MX, DE, CA

1401 Lavaca Street
Unit #375
Austin, TX 78701

wellsfargo	230	157	US, NG, IN, CN, BG, GB, AU, MY, CA, GH
nasdaq	76	50	CN, IN, US, BR, AS, TH, PL, UA, GB, NL
nike	2,100	1,500	IN, US, TR, CN, RU, MY, DE, ID, NG, SG
covid	7,800	4,600	US, IN, NG, CA, CN, RU, MX, GB, BR, TR
pfizer	94	63	US, IN, NG, GB, AE, CL, CN, ZA, RU, PE
moderna	850	754	BR, US, IN, CO, MX, TR, ES, CA, RU, AR
worldhealth	117	88	IN, US, PH, TR, GB, BR, RU, PK, NG, CA
walgreens	32	24	US, IN, NG, CN, PA, PL, DE, UA, SG, BD
amazon	4,600	2,700	US, BR, IN, CN, CA, GB, CO, VN, BD, PK
walmart	318	150	US, CN, NG, GR, BD, IN, RU, CA, PK, PA

While brand protection efforts have mitigated some of the risk and damage posed by cybersquatting, the numbers above illustrate that there is still substantial work to be done to more rapidly identify domains as they are registered and take the appropriate action. It is critical to consider that many of these domains fly under the radar of various scanners and crawlers as they are not indexed and are used exclusively as email domains and are only activated once related infrastructure has been set up and weaponized. This underscores the importance of efficient and rapid detection and response of which domain registration analysis facilitates.

1401 Lavaca Street
Unit #375
Austin, TX 78701

Conclusion

Domain registration analysis has evolved into an important component of cyber threat intelligence, allowing cybersecurity professionals to detect potential threats before they materialize. Experts can obtain useful insights into threat actors' intentions, plans, and actions by monitoring and analyzing domain registrations. This data can then be used to implement preventative steps to counter potential attacks, limit damage, and avoid future cyber threats.

The ability to anticipate trends in cyber attacks, especially phishing campaigns and ransomware attacks, is one of the main advantages of domain registration analysis. Phishing campaigns pose a significant risk to both businesses and individuals, as they can result in the theft of private data, the installation of malware, and financial losses. Cybersecurity experts can identify domains that are likely to be used in phishing attacks and implement targeted defenses to counter them by analyzing domain registrations. Similarly, ransomware attacks can be discovered in advance through domain registration analysis, allowing organizations to take preventative or mitigation measures.

Domain registration research, on the other hand, is not without difficulties. The use of privacy protection services to conceal the registrant's identity and malicious purpose is one of the most significant barriers. Furthermore, some domains may not be registered until the assault has progressed sufficiently, limiting early detection and causing investigations to stall.

Vigilocity's RASA considers evidence of threat actor intent, planned and current targets, and operational security flaws or inadequacies. It provides a distinct linear view of the geopolitical landscape, reflecting the intentions, plans, and actions of a diverse set of players, including people, organizations, and governments. This method enables cybersecurity professionals to discover visual patterns, outliers, and trends that would be difficult, if not impossible, to detect using traditional analysis methods. Domain registration analysis is likely to become an even more important tool in the battle against cybercrime as innovative methods like RASA continue to be developed.

For more information, contact Vigilocity at info@vigilocity.com