

Jingle Shells: How Virtual Offices Enable a Facade of Legitimacy

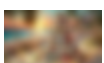
 team-cymru.com/post/how-virtual-offices-enable-a-facade-of-legitimacy

December 20, 2024



Virtual offices have revolutionized the way businesses operate. They provide cost-effective flexibility by eliminating the need for permanent physical spaces. For startups, entrepreneurs, and global companies, virtual offices are powerful tools for establishing a presence in new markets and enhancing professional credibility.

However, this innovation has a darker side. The same features that benefit legitimate businesses also create opportunities for exploitation. Virtual offices have become a low-cost goldmine for cyber criminals, enabling them to establish shell companies, obscure illicit operations, and project an air of legitimacy for their fraudulent activities. While the misuse of shell companies is not a new phenomenon, the post-pandemic world has seen an exponential rise in virtual office service providers and customers, further complicating the landscape.



This growing misuse poses significant challenges for regulators, investigators, and businesses alike, making it increasingly difficult to distinguish legitimate enterprises from fraudulent ones. With hundreds or even thousands of companies registered at the same virtual address, malicious actors can easily hide in plain sight, leveraging these services to facilitate criminal activities ranging from money laundering to phishing schemes.

This blog explores these issues in greater depth, focusing primarily on the "virtual business address" aspect, particularly in the context of cloud hosting providers. While the analysis centers on activities observed in the United Kingdom—where business registration rules are notably lax, even for individuals residing overseas—the techniques discussed can be broadly applied to identify similar patterns of misuse involving virtual office providers in other countries and regions. By recognizing these patterns and employing the investigative techniques shared here, researchers and organizations can better detect and address these hidden threats.

Key Findings

Virtual office services are increasingly leveraged to establish shell companies, sometimes with multiple entities registered at the same address, creating an appearance of legitimacy while obscuring the true nature of operations.

Some hosting providers, including those registered in jurisdictions like the UK, operate infrastructure in regions with less regulatory oversight, such as Mauritius and Seychelles, which can make it easier to circumvent stricter compliance requirements.

The combination of leased IPv4 space, limited "know your customer" (KYC) processes, and weak regulatory frameworks may inadvertently enable the creation of hosting environments that support activities such as phishing and malware command-and-control (C2) servers.

A Singular Example of “Known Bad”

In our first example, we illustrate how a *known bad* IP address can be traced back to its hosting provider and, ultimately, to the “business(es)” operating behind it.

IP **2.57.122.72** is identified as a Metasploit C2 server; based on an X.509 certificate hosted on the server and corresponding inbound network traffic to TCP/3790—the default Metasploit service port.



Figure 1 - Metasploit C2 (Scout GUI)

This IP address is assigned to [AS47890](#), operated by UNMANAGED LTD, with geolocation data suggesting the company is based in the United Kingdom.

In the UK, a public register of companies is maintained by [Companies House](#), which provides registration details, officer information, financial filings, and other related data.

The filing for UNMANAGED LTD reveals that the company was incorporated in February 2020 and lists its business address as being in Rushden, England. Upon further investigation, this address appears to correspond to a self-storage facility operating at the location.



Figure 2 - UNMANAGED LTD Company Record

Unable to locate an online storefront for purchasing hosting infrastructure from UNMANAGED LTD, we turned to examine additional WHOIS information for IP **2.57.122.72**. According to the RIPE database, the /24 subnet containing this IP address is associated with the domain name **dmzhost[.]co**.



Figure 3 - WHOIS Information for 2.57.122.0/24

Based on its website and [forum posts](#) purportedly made by the owners of DMZHost, the company offers “offshore” dedicated and virtual private servers. Notably, they advertise their policy of ignoring DMCA (Digital Millennium Copyright Act) requests related to the content hosted by their customers. While the DMCA is a U.S. law, similar copyright protections exist in the European Union and the UK. A hosting provider that openly disregards such requests raises at least an amber flag regarding their policies and their tolerance for hosting potentially malicious content.

Within the WHOIS records, references are also made to another UK-registered company, TECHOFF SRV LIMITED, with a registered address in London.



Figure 4 - TECHOFF SRV LIMITED Company Record

Noticing that TECHOFF SRV LIMITED was incorporated less than a month ago (at the time of writing) while the RIPE record (Figure 3) was created in 2019, we turned to historical WHOIS information for further investigation.



Figure 5 - Historical WHOIS Information for 2.57.122.0/24

In Figure 5 we can see that, until 04 October 2024, the subnet **2.57.122.0/24** was associated with “pptechnology”. Digging deeper, we discovered a company, PPTECHNOLOGY LIMITED, registered at the same business address as TECHOFF SRV LIMITED.

A review of the filing history for PPTECHNOLOGY LIMITED reveals that, according to records submitted to Companies House, the company has remained dormant since its registration in August 2019.



Figure 6 - PPTECHNOLOGY LIMITED Company Record

As with UNMANAGED LTD, we could find no evidence of an online storefront for either TECHOFF SRV LIMITED or PPTECHNOLOGY LIMITED. Given their filing histories, it is clear that these companies are not being used to process funds related to the sales or leasing of cloud hosting infrastructure. This suggests that their primary purpose—or at least one of their purposes—is to provide the appearance of legitimacy, perhaps for interactions with organizations such as RIPE.

A search for the business address (35 Firs Avenue), shared by both TECHOFF SRV LIMITED and PPTECHNOLOGY LIMITED, reveals over 1,000 active companies registered at the same location. Notably, around 85% of these companies are listed under business code **96090**—a broad category often used as a catch-all for unspecified business activities, effectively providing little meaningful information.

Digging deeper, we identified another company, PARAMOUNT COMPANY FORMATIONS LIMITED, which offers business registration services. These services include the provision of a business address at 35 Firs Avenue for a nominal annual fee.

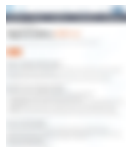


Figure 7 - PARAMOUNT COMPANY FORMATIONS LIMITED Advertisement

Without delving further into this rabbit hole, the findings so far already reveal a highly opaque picture of the operations behind the organization hosting the Metasploit C2 server. At the same time, they demonstrate just how trivially easy it is to establish such an opaque business model. Importantly, nothing highlighted at this stage is illegal under current UK business registration rules..

As a final point, while examining the hosting provider DMZHost—whose website is protected by Cloudflare infrastructure—we identified a subdomain hosted at **45.148.10.41** (AS48090 / DMZHOST, GB).



Figure 8 - Domains resolving to **45.148.10.41**

The domain **pptechnology[.]cc** stands out given the points discussed above, although at the time of writing, it simply hosts an empty open directory. Among the other domains, **alterbizcorpo[.]com** currently displays a page indicating that the domain is suspended, however **calycom[.]com** leads us to another likely related hosting provider.

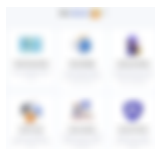


Figure 9 - Advertisement from the Calycom Website

Offshore servers, paid for with cryptocurrency, and no “know your customer” checks—an arrangement that offers significant anonymity, making it appealing to actors with varying intentions.

While this case highlights specific techniques used by malicious actors, the patterns observed extend far beyond a single example.

The Bigger Picture

Having examined an individual case by tracing the trail back from an IP of interest, let's now broaden our focus to explore the prevalence of similar practices among hosting providers—specifically, those that, according to our datasets, host a disproportionately high percentage of malicious activity.

Team Cymru's *Risknet* project provides valuable context by identifying hosting providers with the highest concentrations of malicious activity at any given time. It measures the percentage of IP addresses within a particular Autonomous System (AS) that are associated with threats such as malware C2 servers, phishing infrastructure, and more. The project generates a daily snapshot of these networks, which are typically smaller ASes in terms of assigned netblocks.

Users of Team Cymru's Pure Signal™ Recon and Scout platforms will be alerted to identified networks through the presence of a “risknet” tag displayed alongside IP addresses in their search results. These tags can also be leveraged in complex queries via the Scout interface, enabling users to examine patterns of activity across broader IP address sets.



Figure 10 - Risknet Tag Example (Scout GUI)

As of 01 December 2024, seven of the top 30 networks associated with malicious activity had a recorded country code of GB (United Kingdom), including three of the top five and the top two overall. Each network is summarized below:

AS216240 MortalSoft Ltd (Rank 1)

MORTALSOFT LTD has one /24 netblock geolocated to Bulgaria and is associated with **anonvm[.]wtf**, advertising cloud hosting services. Incorporated in September 2023, it was renamed SILENTRoute TECHNOLOGY LTD in November 2024. The company uses a virtual office at 85 Great Portland Street, London (shared by 17,730 companies).

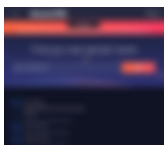


Figure 11 - anonvm[.]wtf Homepage

AS215240 Silent Connection Ltd (Rank 2)

SILENT CONNECTION LTD operates five /24 netblocks geolocated to the Seychelles. Incorporated in March 2024, it uses a virtual office at 321-323 High Road, Romford (685 active companies). No online storefront was found.

AS50580 Mario Networks Limited (Rank 5)

MARIO NETWORKS LIMITED has two /24 netblocks geolocated to Mauritius. It was incorporated in October 2022 and renamed USERCLOUD SOLUTION LTD in October 2023. Financial filings are overdue since July 2024. The company uses a virtual office at 27 Old Gloucester Street, London (4,296 companies). No online storefront was found.

AS215208 Dolphin 1337 Limited (Rank 11)

DOLPHIN 1337 LIMITED has two /24 netblocks geolocated to Mauritius and is associated with **dolphinhost[.]net**, advertising cloud hosting services. Incorporated in March 2024, it shares a virtual office at 321-323 High Road, Romford, with SILENT CONNECTION LTD, using identical incorporation details. The two networks are also BGP peers.



Figure 12 - [IPv4 Routing](#) of AS215240 / AS215208

AS214927 PSB Hosting Ltd (Rank 21)

PSB HOSTING LTD has eight /24 netblocks, seven geolocated to the Seychelles and one to the UAE. It is associated with **psb[.]hosting**, advertising cloud hosting services. Incorporated in April 2024, it uses a virtual office at 17 King Edwards Road, Ruislip (4,433 companies).

AS215766 Emanuel Hosting Ltd (Rank 26)

EMANUEL HOSTING LTD has one /24 netblock geolocated to Bulgaria. It is associated with **emanuelhosting[.]info** and references AS394711, which ceased routing in October 2024. Incorporated in October 2023, it lists a construction site at 26 New Kent Road, London, as its address. Based on open source [information](#), the site has been under construction since 2020 and will not be completed until 2026.



Figure 13 - Timeline of Works at the “Business Address” of Emanuel Hosting

AS215826 Partner Hosting Ltd (Rank 28)

PARTNER HOSTING LTD has eighteen /24 netblocks geolocated across Russia (11), Montenegro (3), Panama (2), Seychelles (1), and the UK (1). It is associated with **altawk[.]com**, advertising cloud hosting services. Incorporated in December 2023, it uses a virtual office at 71-75 Shelton Street, London (68,338 companies).

There are several recurring themes when considering all seven companies/hosting providers collectively.

Aside from EMANUEL HOSTING LTD, which lists a building site as its official address, the remaining companies all utilize virtual offices. This underscores the growing reliance on such services.

For companies registered in the UK, there is a notable lack of UK-based infrastructure or services, with only one /24 netblock geolocated to the UK. This suggests these companies are operating as shell entities, with their physical infrastructure intentionally located in jurisdictions such as Mauritius and the Seychelles, where regulatory and technical oversight is limited.

For companies operating online services, it is surprising that no online storefronts could be identified for several of them, suggesting that their services may be advertised elsewhere, such as in underground forums or via “word of mouth”. For those companies with identifiable storefronts, there was a significant emphasis on their services being “offshore.”

All the companies were registered within the past few years, some as recently as this year. This trend reflects the post-pandemic growth of this phenomenon. However, this does not provide the full picture. Questions arise as to why “new” businesses are immediately attracting malicious content, suggesting that their histories may predate their incorporation dates. It is likely that the individuals behind these companies have long-standing ties to “offshore” hosting, catering to repeat customers who use these opaque services to host malicious content.

Finally, it is important to note that each of these ASs is currently listed on Spamhaus’ ASN-DROP list, a resource that helps network operators block traffic from malicious networks.

IPv4 For Lease

When examining enabling factors, another broad trend identified in recent investigations is the utilization of leased IPv4 space. These services are generally offered by larger Internet Service Providers (ISPs), where IP space—typically a /24 or /23 netblock—is leased for a specified period, often in packages of 30, 90, or 365 days.

In the case of three of the providers mentioned above (MORTALSOFT LTD, DOLPHIN 1337 LIMITED, and EMANUEL HOSTING LTD), WHOIS records contain references to “NETERRA”.

Neterra is a Bulgarian ISP that, through its Neterra Cloud division, leases and sells IPv4 space.



Figure 14 - Neterra Cloud Advertisement Page

While there is no evidence to suggest that Neterra is complicit in hosting malicious content, it is likely that their terms of service for IPv4 leasing shift responsibility onto the “lessee.” However, it is apparent that these services may be subject to abuse.

The observation that three seemingly distinct organizations are utilizing Neterra Cloud’s services suggests a preference for this provider. This preference likely stems from practical factors, such as affordability, rather than any explicit tolerance for misuse..

This highlights the broader issue of unclear responsibility within the Internet hosting ecosystem. Nevertheless, stakeholders across the Internet hosting ecosystem must take proactive steps to minimize abuse and deny malicious actors a safe haven.

Conclusion

The abuse of virtual office services and hosting infrastructure highlights a growing global challenge in the fight against cybercrime. As demonstrated, malicious actors exploit gaps in regulatory frameworks, the anonymity provided by virtual offices, and the availability of leased IPv4 space to obscure their operations and carry out illicit activities. These tactics allow them to establish shell companies and hosting environments that appear legitimate while leveraging jurisdictions with minimal oversight to evade accountability.

While this blog examines trends observed in the United Kingdom, it is important to note that similar patterns are prevalent worldwide. Jurisdictions known for simplified business registration processes, such as certain U.S. states like Delaware and Wyoming, or tax havens like the British Virgin Islands and the Cayman Islands, foster comparable opportunities for criminals. The UK’s open and accessible business registration system, while intended to nurture entrepreneurship, has also inadvertently provided opportunities for misuse. Understanding how different jurisdictions balance accessibility with oversight can offer valuable insights into effective regulatory approaches.

Addressing these issues requires a coordinated global effort. Stakeholders across the hosting ecosystem must collaborate to strengthen vetting processes, enforce stricter "know your customer" (KYC) requirements, and improve transparency in business registration practices. Moreover, adopting best practices from jurisdictions with robust regulatory frameworks—such as mandatory verification of business owners and enhanced oversight of service providers—can help reduce opportunities for abuse while preserving the benefits of business-friendly environments.

By taking proactive steps to close these gaps, stakeholders can help disrupt the infrastructure that enables malicious activities and reduce the prevalence of abuse in virtual office and hosting services. The patterns and investigative techniques outlined in this blog serve as a starting point for further exploration. By recognizing the warning signs of misuse and leveraging available tools, organizations can better detect and mitigate these hidden threats. Safeguarding the integrity of the digital ecosystem requires a unified and comprehensive approach, as the fight against cybercrime transcends borders and affects us all.

Recommendations

Leverage Risknet Tags: Use Team Cymru's Risknet tags in Pure Signal™ Recon and Scout to identify networks with high malicious activity and analyze patterns across broader IP address ranges.

Monitor and Mitigate: Regularly scan for flagged IP addresses, proactively blacklist high-risk ASes, and use threat intelligence to mitigate exposure to malicious traffic.

Investigate Suspicious Entities: Cross-reference IPs, domains, and business registration data to uncover signs of abuse, such as shared virtual office addresses or operations in high-risk jurisdictions.

Enhance Due Diligence: Verify the legitimacy of partners and vendors by investigating their hosting practices, public-facing presence, and compliance with regulatory requirements.

- **Advocate for Better Policies:** Support stricter regulations for virtual offices and IPv4 leasing, including robust "know your customer" (KYC) requirements and increased transparency in business registrations.
- **Collaborate Across the Ecosystem:** Share intelligence on emerging threats and abuse patterns with peers, leveraging tools like Team Cymru's platforms for broader insights.