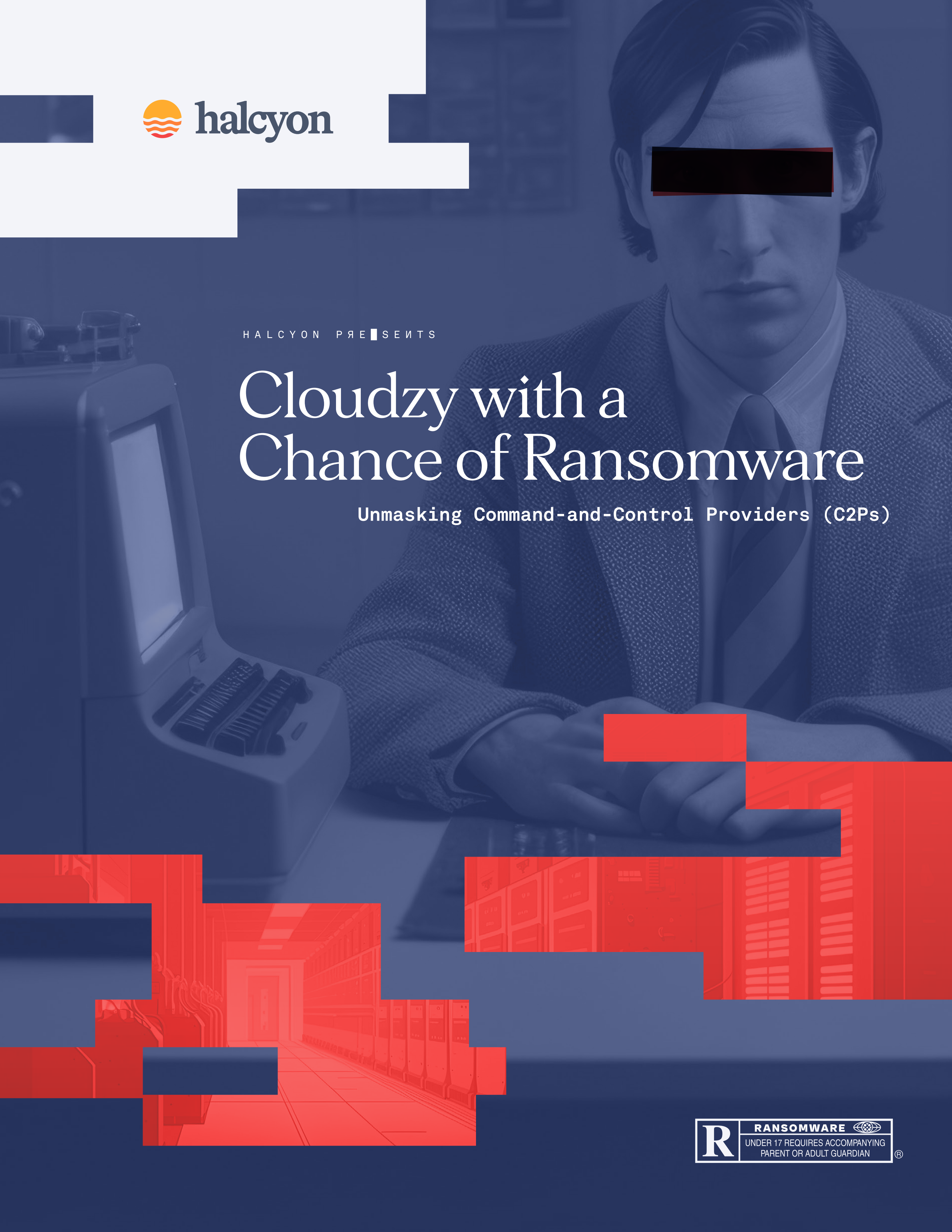
halcyon



HALCYON PRESENTS

Cloudzy with a Chance of Ransomware

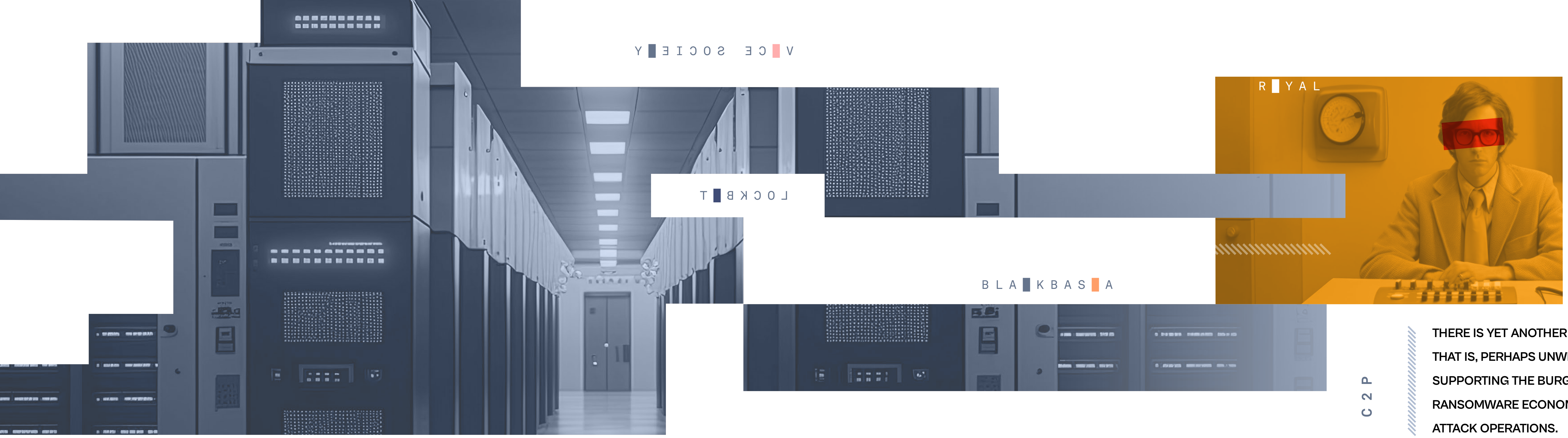
Unmasking Command-and-Control Providers (C2Ps)

R RANSOMWARE
UNDER 17 REQUIRES ACCOMPANYING
PARENT OR ADULT GUARDIAN ®

halcyon

CONTENTS

In this report, Halcyon demonstrates a unique method for identifying C2P entities that can be used to forecast the precursors to ransomware campaigns and other attacks significantly “left of boom.”



C2P

THERE IS YET ANOTHER MAJOR PLAYER THAT IS, PERHAPS UNWITTINGLY, SUPPORTING THE BURGEONING RANSOMWARE ECONOMY AND OTHER ATTACK OPERATIONS.

Executive Summary

The ransomware economy is supported by a number of illicit groups that each provide one small piece of the puzzle that is cybercrime. From initial access brokers (IABs) to crypto money launderers, the criminal ecosystem that has sprung up around ransomware is vast.

Halcyon researchers suggest there is yet another player that is, perhaps unwittingly, supporting the booming ransomware economy and other attack operations: the Command-and-Control Providers (C2P) who sell services to threat actors while assuming a legal business profile.

Bulletproof Hosting (BPH) providers usually operate in jurisdictions which have lenient laws against illicit conduct, as such they openly serve criminal operations unapologetically; C2Ps however attempt to blend in as legitimate business, even going so far as to operate in jurisdictions where they are subject to legal standards of conduct (like Cloudzy in the US) but leverage the anonymity of their clients to serve criminal operations with plausible deniability.

While these C2P entities are ostensibly legitimate businesses that may or may not know that their platforms are being abused for attack campaigns, they nonetheless provide a key pillar of the larger attack apparatus leveraged by some of the most advanced threat actors.

In this report, Halcyon demonstrates a unique method for identifying C2P entities that can potentially be used to forecast the precursors of ransomware campaigns and other attacks significantly "left of boom."

Halcyon also identifies two new, previously undisclosed ransomware affiliates we track as Ghost Clown and Space Kook that currently deploy BlackBasta and Royal, respectively.

We also describe how we used the same method to link the two ransomware affiliates to the same Internet Service Provider, Cloudzy, which accepts cryptocurrencies in exchange for anonymous use of its Remote Desktop Protocol (RDP) Virtual Private Server (VPS) services.

It is well known that ransomware syndicates rely on a broad ecosystem of initial access brokers, malware and exploit developers, and criminal affiliates to run their illicit enterprises. But few realize that they also rely on a global system of legitimate service providers, like Cloudzy, who appear to act as Command-and-Control Providers (C2P).

C2Ps end up granting ransomware groups anonymous use of their infrastructure to launch attacks because, in the interest of privacy, it appears they never bother to ask who their customers are. They are not required to. In this way, ransomware activity lines two sets of pockets – the criminals who deploy it and the service providers who may be turning a blind eye to them.

In the case of Cloudzy, that blind eye may have missed a lot. This report documents what is assessed to be a pattern of consistent use or abuse of Cloudzy servers by more than two dozen different threat actors over several years. Included are groups tied to the Chinese, Iranian, North Korean, Russian, Indian, Pakistani, and Vietnamese governments; a sanctioned Israeli spyware vendor whose tools are known to target civil society; and several additional criminal syndicates and ransomware affiliates whose campaigns previously made international headlines.

Halcyon concludes this report by taking a closer look at Cloudzy. We present evidence that even though Cloudzy purports to be a legitimate American company, it appears to operate out of Tehran, Iran in possible violation of U.S. sanctions under the direction of an entrepreneur named Hassan Nozari.

Key Findings

- Halcyon asserts that, based on this research, there is yet another key player supporting the burgeoning ransomware economy: Command-and-Control Providers (C2P) who – knowingly or not–provide services to attackers while assuming a legitimate business profile.
- Threat actors that are assessed to be leveraging Cloudzy include APT groups tied to the Chinese, Iranian, North Korean, Russian, Indian, Pakistani, and Vietnamese governments; a sanctioned Israeli spyware vendor whose tools are known to target civilians; several criminal syndicates and ransomware affiliates whose campaigns have spurred international headlines.
- Halcyon uses an unlikely pivot point – namely RDP hostnames within the metadata of an affiliate's attack infrastructure – that can enable security teams to detect imminent ransomware attacks before they are launched as the attack infrastructure is being stood up.
- Halcyon identifies that Cloudzy – which accepts cryptocurrencies in exchange for anonymous use of its Remote Desktop Protocol (RDP) Virtual Private Server (VPS) services – appears to be the common service provider supporting ransomware attacks and other cybercriminal endeavors.
- Halcyon also identifies a long list of government-sponsored APT-related attacks spanning several years that appear to be using Cloudzy services, where it is assessed that (potentially) between 40%-60% of the overall activity could be considered malicious in nature.
- Halcyon presents evidence that, although Cloudzy is incorporated in the United States, it almost certainly operates out of Tehran, Iran – in possible violation of U.S. sanctions – under the direction of someone going by the name Hassan Nozari.
- Halcyon identified two previously unknown ransomware affiliates dubbed Ghost Clown and Space Kook currently deploying BlackBasta and Royal ransomware strains, respectively.

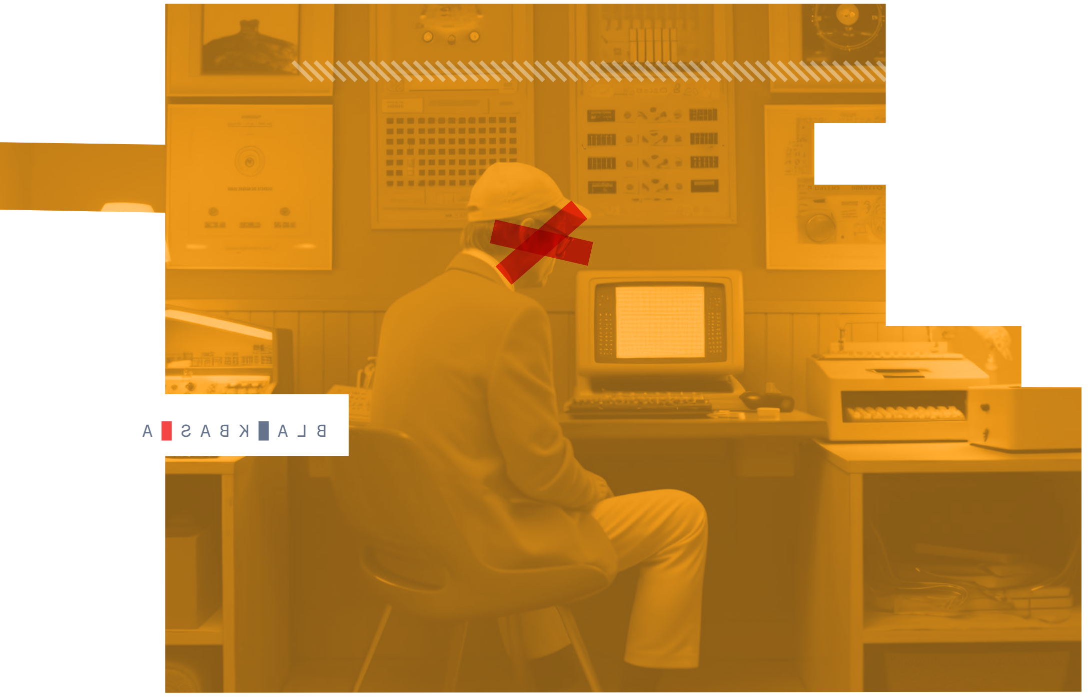
POTENTIALLY 40%–60% OF ACTIVITY LEVERAGING CLOUDZY SERVICES IS MALICIOUS IN NATURE

The Ransomware Economy in Brief

The rise of Ransomware as a Service (RaaS) gangs mimics the more conventional Software as a Service business model in every meaningful measure. The ransomware economy involves multiple players specializing in various aspects of the larger ransomware attack.

These elements generally include the following actors:

- **Initial Access Brokers (IAB):** Highly skilled specialists who are exceptionally good at penetrating and establishing a foothold within secure networks. IABs often sell access to these compromised networks to other threat actors, including ransomware affiliates.
- **RaaS Platform Providers:** RaaS operators provide the software platform and backend to launch attacks. They have development teams constantly improving their feature sets, they assist in negotiations during a successful attack, they manage customer service agents, market to new affiliates, and more all for a slice of the profits.
- **RaaS Affiliates:** The actual ransomware attack is executed by an affiliate after they obtain access via an IAB (or create their own), use a platform or toolkit from a RaaS operator, and execute the attack.
- **Crypto Exchange Money Launderers:** The money launderers do just that – move illicit ransom payments through crypto exchanges with the intent to hide both the origins and the destination of the funds and then take a healthy fee for their services. The overall maturity, the level of organization, and the specialization within the Ransomware Economy means we are dealing with adversaries whose tactics, techniques, and procedures (TTPs) are approaching the sophistication of some nation-state-sponsored attackers.



This research suggests that there is yet another major player in the larger attack ecosystem:

Command-and-Control Providers (C2Ps)

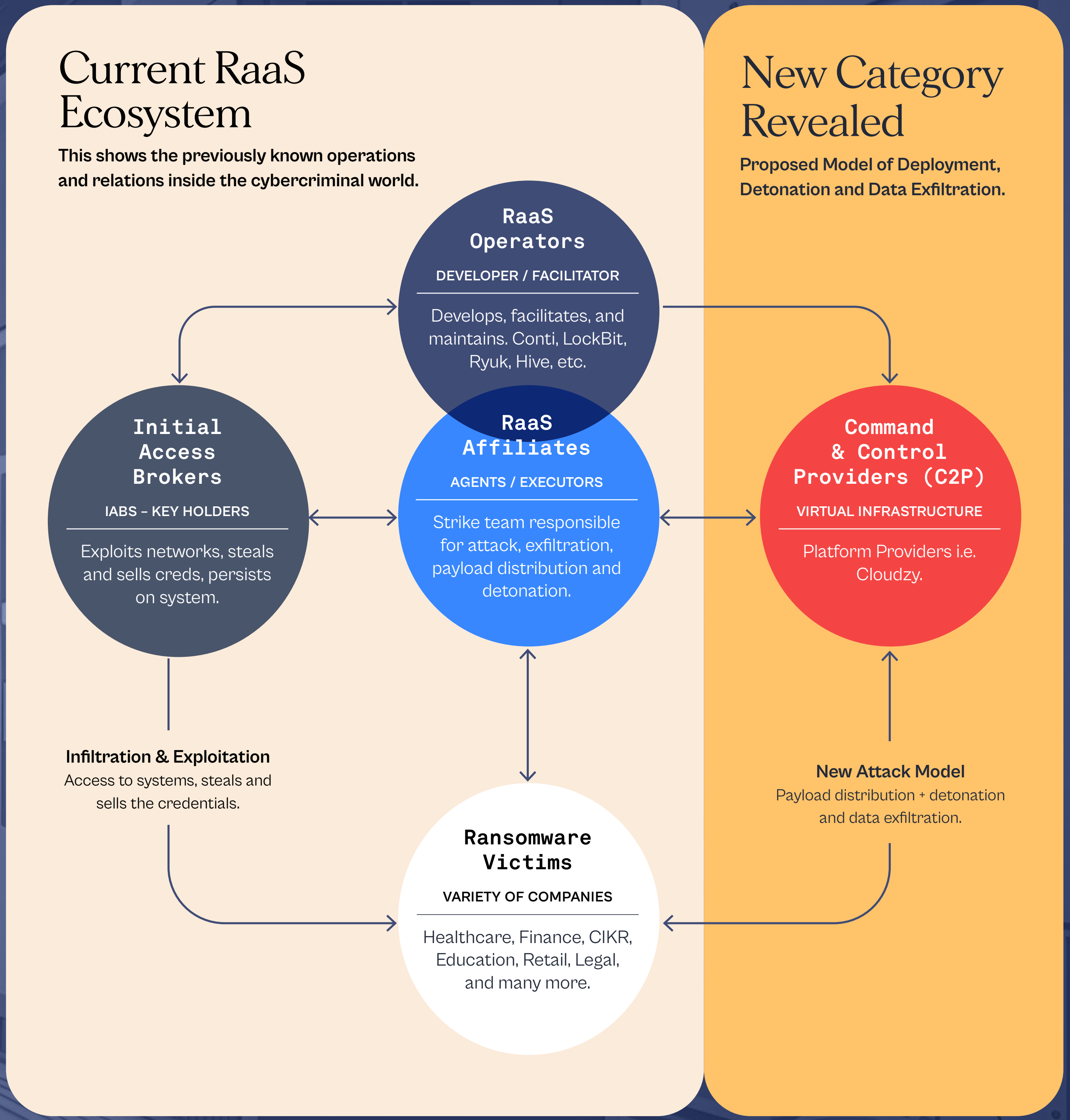
There has already been research that alludes to an overlap between some nation-state attack activity with cybercriminal ransomware gangs. This report demonstrates how some APTs and cybercriminal threat actors are leveraging some of the same attack infrastructure, further blurring the lines between nation-state supported actors and those of the cybercriminal world.

This research suggests that there is yet another major player in the larger attack ecosystem: Command-and-Control Providers (C2Ps) who – knowingly or not – provide services without any vetting to customers who include known APTs and cybercriminal elements involved on conducting ransomware attacks.

C2Ps are legitimate ISPs who provide attackers with VPS and other anonymized services that ransomware affiliates use to carry out the attacks. They enjoy liability loopholes via their TOS and Privacy Policies that does not require them to ensure that the infrastructure they provide is not being used for illegal operations.

During an investigation of two previously unknown RaaS attack affiliates, Halcyon researchers uncovered a C2P called Cloudzy that is linked to attacks carried out by some major APT and ransomware gangs. This report provides further details on how the connection was made and why these infrastructure providers are able to skirt any liability for attacks that use their services.

The RaaS ecosystem has evolved: Command-and-Control Providers (C2P)



Current RaaS Ecosystem

This shows the previously known operations and relations inside the cybercriminal world.

RaaS Operators
DEVELOPER / FACILITATOR
Develops, facilitates, and maintains. Conti, LockBit, Ryuk, Hive, etc.

Initial Access Brokers
IABS – KEY HOLDERS
Exploits networks, steals and sells creds, persists on system.

RaaS Affiliates
AGENTS / EXECUTORS
Strike team responsible for attack, exfiltration, payload distribution and detonation.

Infiltration & Exploitation
Access to systems, steals and sells the credentials.

Ransomware Victims
VARIETY OF COMPANIES
Healthcare, Finance, CIKR, Education, Retail, Legal, and many more.

New Category Revealed

Proposed Model of Deployment, Detonation and Data Exfiltration.

Command & Control Providers (C2P)
VIRTUAL INFRASTRUCTURE
Platform Providers i.e. Cloudzy.

New Attack Model
Payload distribution + detonation and data exfiltration.

Newly Identified Ransomware Affiliates: Ghost Clown & Space Kook

In this section, Halcyon describes two previously unreported ransomware affiliates we identified when we took a Windows Remote Desktop Protocol (RDP) hostname observed in a single attack and pivoted to identify additional malicious infrastructure.

By blocking the network infrastructure associated with these RDP hostnames, a network defender can potentially stop a variety of attackers in their tracks – including malware used for initial access and lateral movement as well as the ransomware itself–from being deployed. A discussion of our methodology follows, as do details linking the two ransomware affiliates to the same service provider, Cloudzy.

Ghost Clown

Ghost Clown regularly used the C2P Cloudzy to host their Cobalt Strike infrastructure. Cobalt Strike, a common penetration testing (pentesting) platform, is routinely abused by threat actors, who often use it for lateral movement within a compromised network. Here, the affiliate deployed Cobalt Strike BEACON after piggybacking on an initial QakBot infection. These BEACON implants regularly led to hands-on-keyboard activity culminating in the deployment of ransomware. The following is a representative hash:

```
4d56e0a878b8a0f04462e7aa2a47d69a6f3a31703563025fb40fb82bab2a2f05
```

BY BLOCKING THE NETWORK INFRASTRUCTURE ASSOCIATED WITH THESE RDP HOSTNAMES, A NETWORK DEFENDER CAN POTENTIALLY STOP A VARIETY OF ATTACKERS IN THEIR TRACKS.

This Cobalt Strike BEACON implant communicated with mojimetigi[.]biz for command-and-control (C2). When the domain was first active it resolved to the IP address 23[.]19[.]58[.]181. Halcyon associated this IP with Cloudzy via its related Remote Desktop Protocol (RDP) hostname during the same time period.

Halcyon observed Ghost Clown historically deploy Conti ransomware to victims from about February of 2021 until a year later. More recently, they switched to deploying BlackBasta. This move followed the dissolution of the Conti group after the public disclosure of internal communications sparked by the war in Ukraine.

Space Kook

Halcyon witnessed Space Kook deploy Cobalt Strike BEACON via infrastructure hosted by the C2P Cloudzy. A representative sample for this group is given below:

```
b27ca5155e42e372d37cf2bcbb1f159627881ecbae2e51d41f414429599d37a7
```

This BEACON payload communicated directly with two IP addresses, 139[.]177[.]146[.]152 and 172[.]93[.]201[.]120. Halcyon noted that Space Kook's infrastructure aligned closely with that of EXOTIC LILY, an initial access broker written about by Google's Threat Analysis Group (TAG) in March of 2022. TAG assessed that the group worked with, but was distinct from, "the Russian cybercrime gang known as FIN12 (Mandiant) / WIZARD SPIDER (CrowdStrike)."

Halcyon observed infrastructure related to Space Kook associated with activity beyond initial access. We observed them leverage an initial BUMBLEBEE infection to deploy Cobalt Strike BEACON. The actor then leveraged the BEACON implant to move laterally in the victim network and ultimately deployed ransomware. Halcyon established that Space Kook previously deployed Quantum Locker ransomware but is currently deploying Royal.

Halcyon was unable to determine with certainty whether Space Kook and EXOTIC LILY were the same group, or whether Space Kook was a customer of EXOTIC LILY, though the latter scenario appears more likely.

Google TAG associated the lone IP address they published with C2 infrastructure tied to BUMBLEBEE. Halcyon linked that IP address to the C2P Cloudzy via our RDP hostname research. Halcyon then looked retroactively within Cloudzy's IP address space and uncovered 26 additional BUMBLEBEE servers controlled by the same group, representing approximately 20% of all BUMBLEBEE servers identified by Halcyon since the beginning of 2023.

Halcyon Witnessed Space Kook Deploy Cobalt Strike BEACON via infrastructure hosted by the C2P **Cloudzy.**

RDP Hostnames: An Unlikely Pivot Point

Halcyon identified Ghost Clown and Space Kook by conducting in-depth research into RDP hostnames. RDP hostnames were an unlikely initial pivot point, but they proved to be an effective and high-fidelity means of identifying and linking together seemingly disparate infrastructure. In this section we provide a broad outline of our methodology.

Halcyon began with a large set of previously published and undisclosed ransomware attack network IOCs. Using Internet scanning data from Censys and Shodan, we noticed what seemed to be a group of RDP hostnames recurring frequently within the “Subject Common Name” field of X.509 certificates.

These SSL certificates were most frequently used to secure RDP connections on the default TCP port, 3389. By default, Windows sets the “Subject Common Name” field to match the server’s hostname when first issuing SSL certificates for RDP.

Halcyon linked the above 11 RDP hostnames to ransomware incidents by connecting the SSL certificates where the hostnames appeared to associated IP addresses which matched the known TTPs of ransomware groups we track.

Halcyon noted that several of these RDP hostnames were also called out as indicators of compromise (IOCs) in ransomware incidents by several different security researchers including those at The DFIR Report, Team Cymru, and Intrinsec. This served to confirm our initial findings that these RDP hostnames were associated with malicious infrastructure used in ransomware campaigns.

Halcyon then determined that the IP addresses associated with the SSL certificates containing these hostnames were also connected to one another based upon their distribution over the following same 13 Internet Service Providers (ISPs):

- Combahton
- DR-Soft
- FranTech Solutions
- Hostwinds
- Hydra Communications
- IPXO
- Leaseweb
- MB-Ricarta
- OVH
- Rockion
- Velcom
- Router Hosting / Cloudzy
- Winstri Corporation

Halcyon did not expect to find the same hostnames repeated so often across so many different providers. The fact that they did suggest to us that someone had used an imaging process to quickly copy and then widely deploy servers across them.

Halcyon reached this conclusion based upon the extremely limited number of operating system version numbers observed in association with each RDP hostname over several years’ time, as noted in Table 1, above.

Halcyon then tried to determine how the same server image could appear on IP space allocated to so many different companies. Given the rapid deployment scenario, we strongly suspected that someone was either leasing IP space and/or leveraging the routing services of the ISPs.

Halcyon knew this was possible because some of those ISPs explicitly included leasing services in their marketing. For example, IPXO advertised that it allowed participants to “lease and monetize unused IP resources.” Similarly, Rockion said it leased “premium ARIN IP space for a low monthly fee.”

Table 1: Linked RDP Hostnames

RDP Hostname	Operating System (OS)	OS Build Version
Rhwin7x64-Pc	Windows 7 Enterprise Service Pack 1	6.1.7601
WIN-M5327EF98B9	Windows 7/Windows Server 2008 R2	6.1.7601
WIN-4K804V6ADVQ	Windows Server 2012 R2 Datacenter	6.3.9600
WIN-OQJUIMC71B6	Windows Server 2016 Datacenter	10.0.1607.14393
WIN-799RI0TSTOF	Microsoft Hyper-V Server 2019	10.0.1809.17763.1098
DESKTOP-1H40CJO	Windows 10 Enterprise	10.0.19041 10.0.18362 10.0.1909.18363.720
DESKTOP-LHC2KTF	Windows 10 Enterprise	10.0.19041
DESKTOP-0I0690N	Windows 10 Enterprise LTSC Version 21H2	10.0.19044.1566
DESKTOP-0QT8017	Windows 10/Windows Server (version 2004)	10.0.19041
WIN-SDSIKD9RH2U	Windows Server 2022 Standard 21H2	10.0.20348.2230
DESKTOP-EHS5Q7E	Windows 11 Enterprise 21H2	10.0.22000.318

We learned that these ransomware affiliates were not relying on the same criminal infrastructure broker. Rather, they were relying on the same legitimate one – Cloudzy

Initially, Halcyon suspected that the person or entity doing the leasing was a criminal infrastructure broker, a part of the underground ransomware ecosystem, akin to an initial access broker or malware developer. To investigate further, Halcyon purchased several VPSs from a multitude of identified providers. We expected that when we went directly to the ISPs, we would not find any of the 11 RDP hostnames. But that did not happen.

To our surprise, Halcyon was able to successfully purchase servers with the identified RDP hostnames from one of the ISPs, and only one: the C2P Cloudzy. More precisely, these hostnames appeared on servers provisioned using their "RDP VPS" service. We had our answer.

At the time, Halcyon was unaware that Cloudzy had a nexus with an Iranian company or that it was possibly operating out of Iran. We learned that these ransomware affiliates were not relying on the same criminal infrastructure broker. Rather, they appear to be relying on the same legitimate ISP – Cloudzy.

Historic Activity: More Threat Actors Emerge

Armed with the knowledge that the C2P Cloudzy appears to be hosting several active ransomware affiliates (unwittingly or not), Halcyon looked to see what other activity we could tie to their infrastructure.

Halcyon examined the broader IP space associated with the SSL certificates containing those 11 RDP hostnames. We conducted PDNS analysis within a 90-day window of the RDP hostnames first appearing. We did this to limit the likelihood of any IP-based crossover.

What Halcyon discovered was a staggering array of attack infrastructure which we, and others in the security community, recognized and associated with a wide range of threat actors. Included were government-sponsored APT groups, criminal syndicates, and a commercial spyware vendor called Candiru.

For example, the U.S. government placed Candiru on a 2021 entity list because they stated it "developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."

Historic Activity (Prior to January 2023)

- Chinese APT – PassCV
- Chinese APT – Operation Dragon Castling (FFRat Derivative)
- Chinese APT–APT10 (A41APT Campaign)
- Chinese APT – BlackTech/ CircuitPanda
- Indian APT – Bitter
- Indian APT – Sidewinder
- Iranian APT – Oilrig/APT34
- Iranian APT – Elfin/APT33
- Iranian APT – Bohrium/ RealDoll
- North Korean APT – MATA Framework
- North Korean APT– Cagey Chameleon/BlueNoroff
- North Korean APT – Konni
- North Korean APT – Kimsuky
- Pakistani APT– TransparentTribe
- Russian APT – Nobelium
- Russian APT–Turla
- Vietnamese APT – OceanLotus/APT32
- Israeli Spyware Vendor– Candiru
- Organized Crime – TA505/ TrickBot/EvilCorp/Wizard Spider
- Ransomware– UNC2352– Deployed Ryuk Ransomware
- Ransomware – FIN12 Deployed Ryuk & Blackcat Ransomware

The last threat actor on the list, an activity set Mandiant tracked as UNC2352, made headlines in the fall of 2020 after a blitzkrieg of ransomware attacks impacted the healthcare industry in the U.S. The FBI, DHS, and CISA issued a joint advisory on the activity on October 28, 2020.

Halcyon suspects that these government agencies were unaware that the C2P Cloudzy (then doing business as "Router Hosting") was assessed to be the hosting provider ultimately responsible for at least 40 of the C2 servers used by the group during these attacks.

Cloudzy: Terms and Conditions May Apply

At the time of writing, Halcyon estimated that potentially between 40% - 60% of the total servers currently hosted by the C2P Cloudzy appear to be directly supporting potentially malicious activity. Given the significant amount of threat activity assessed to be tied to Cloudzy and the tangible impact that activity has had on society, Halcyon decided to investigate the business itself.

First, Halcyon found that C2P Cloudzy appears to market itself in a manner that directly appeals not just to privacy enthusiasts, but also to threat actors. Our own experience purchasing VPS services from Cloudzy was cheap, easy, and anonymous – all qualities that threat actors embrace.

Cloudzy only required a working e-mail address and anonymous payment in cryptocurrency. Halcyon was never required to verify our identity beyond confirming the provided e-mail address. Even in the choice of payment, Cloudzy offered what might be if abusers paid a nominal fine, they might be able to continue to use their services an attractive option for criminals: Monero VPS, a solution advertised for the explicit purpose of "staying anonymous." Monero has proven itself even more difficult to track by law enforcement than Bitcoin or Ethereum.

Next, Halcyon looked at C2P Cloudzy's terms of service and other statements about abuse of its services. The terms of service were explicit and straightforward: "Any illegal use of our services for purposes including, but not limited to, terrorism, child pornography, hacking, phishing, or spamming is strictly prohibited and will be directed to the proper authorities. We reserve the right to immediately terminate our services to accounts deemed in breach of this statement."

However, on a different portion of its website called the "Knowledge Base," Cloudzy implied that *if abusers paid a nominal fine, they might be able to continue to use their services,* depending on the type of abuse complaint received.

One statement read: "If your VPS server is suspended because of misuse or abusive usage such as prohibited uses: Phishing, Spamming, Child Pxxn, Attacking other people, etc… There is a $250-$1000 fine or NO WAY for unsuspension; this depends on the complaint type."

Cloudzy did appear to take abuse requests seriously when related to its own registered IPv4 netblocks. But therein lay an important distinction. Halcyon found that Cloudzy seems to treat its own infrastructure differently than it did the infrastructure Halcyon assessed it had leased from other providers.

Under its old name, Router Hosting, Cloudzy is listed as the registered owner of the following IPv4 Netblocks:

- 167.88.160.0/23
- 167.88.164.0/23
- 167.88.166.0/23
- 167.88.168.0/23
- 167.88.172.0/2

Another Router Hosting entity registered under the name "Hannan Nozari" lists an additional 55 netblocks of various sizes. The full list is available in the appendix.

Our research assessed that Cloudzy's RDP services, and nearly all malicious activity we identified were principally run from the IP space owned by other Internet service providers - the 12 other ISPs mentioned earlier in this report.

However, the malicious activity in question typically followed the appearance of one of Cloudzy's unique RDP hostnames. This was assessed to be a sign that C2P Cloudzy recently leased or was assigned the IP address space. Halcyon assessed that roughly 82% of the IP addresses used by Cloudzy were owned by other ISPs.

Halcyon attempted to report abuse to Cloudzy, several times via e-mails to "abuse@cloudzy.com" to alert them to the ransomware activity currently abusing its services at the time of writing. We provided relevant indicators, including an IP address we assessed C2P Cloudzy had leased from another ISP but which we deemed was associated with a Cloudzy RDP hostname.

Cloudzy provided a series of responses that confused us and ultimately contradicted one another. Cloudzy initially offered to suspend the account given additional details could be provided, but then shortly reversed course and directed us to the ISP that had registered the IP instead. Then finally suggested we do a mixture of the two.

C2P Cloudzy: Made in the USA *(On Paper)*

Halcyon next turned its attention to the company's corporate registration records. While we found nothing on file under the name Cloudzy, we did find incorporation records for Router Hosting, the name Cloudzy held until 2022.

Router Hosting LLC was registered as a Wyoming corporation on March 22, 2023 with the following address listed: 1309 Coffeen Avenue STE 1200, Sheridan, WY 82801. Halcyon found that the office building at that address, which in Google Maps appeared to be located in a strip mall, was for sale at the time of this report. Halcyon also found that the same address was present in the incorporation records of more than 2,000 other companies.

What Router Hosting / Cloudzy and these companies had in common was an association with Cloud Peak Law, LLC, a law firm that advertises "registered agent services" and other "anonymous" company formation services. Cloud Peak employee "Andrew Pierce" is listed as the "authorized individual" associated with the registering agent in this case, and the Coffeen Ave. address was listed as a point of contact on the law firm's website. From this Halcyon assessed that it was likely the physical that C2P Cloudzy had no actual physical office space in Wyoming.

HALCYON NEXT TURNED ITS ATTENTION TO THE COMPANY'S CORPORATE REGISTRATION RECORDS. WHILE WE FOUND NOTHING ON FILE UNDER THE NAME CLOUDZY, WE DID FIND INCORPORATION RECORDS FOR ROUTER HOSTING, THE NAME CLOUDZY HELD UNTIL 2022.

Halcyon then noted that the same address was also provided as contact information in the WHOIS information for Router Hosting's netblocks as well as in the registration listing of the company's newly assigned ASN: 14956, a transaction that occurred on May 15, 2023. This told us that the corporate records and the WHOIS and ASN registries were all pointing to the same company.

The ASN and WHOIS information for the netblocks also listed an e-mail address for reporting abuse that differed from the one listed on Cloudzy's website (abuse@cloudzy.com). This drew our attention. The WHOIS and ASN records revealed that this other abuse e-mail address, abuse-reports@cloudzy.com, was paired with a telephone number, (778) 977-8246, and an entirely different address in a different state: 1110 Palms Airport Drive, Las Vegas, NV 89119.

Like the Wyoming address, this Nevada address was also associated with a number of other entities. Halcyon found that it was likely the physical address of SmartHost LLC's Nevada Data Center. Why would Cloudzy list a Wyoming address to register the company and its netblocks and a Nevada address for abuse complaints? And why list a different phone number than the one associated with the Wyoming address?

Halcyon found that the same "abuse" phone number was not unique to C2P Cloudzy. It was also listed in ASN records as the contact information for FranTech Solutions, another hosting provider, also known as PONYNET. This was one of the 12 ISPs from whom Cloudzy had leased IP space. A simple reverse lookup showed the phone number was likely a mobile number owned by Rogers Communications Canada Inc.

PONYNET is associated with two other companies: VPS provider BuyVM and web hosting provider BuyShared. The self-described "mastermind" of all these companies is "Francisco Dias," who touts himself a "true visionary in the VPS and web hosting industry." *The New Yorker* cast "Dias" in a slightly different light, confirming with the man himself that his companies hosted several controversial websites, including those associated with "Neo-Nazis" and "cyberbullies."

In any event, Halcyon assessed via WHOIS and ASN records, as well as the leasing of IP space from FranTech Solutions, that Dias appeared to be directly connected with C2P Cloudzy. Cloudzy also would have required more than one ISP to vouch for them to establish their own ASN earlier this year. We speculate that one of the "Francisco Dias" companies may have filled that role.

In sum, Halcyon's research into the corporate and Internet registration records showed that C2P Cloudzy appears to have established itself recently as an American company with direct ownership of an ASN and several netblocks. Halcyon found it had done so with the help of Cloud Peak Law and "Francisco Dias."

The Iranian Faces of C2P Cloudzy

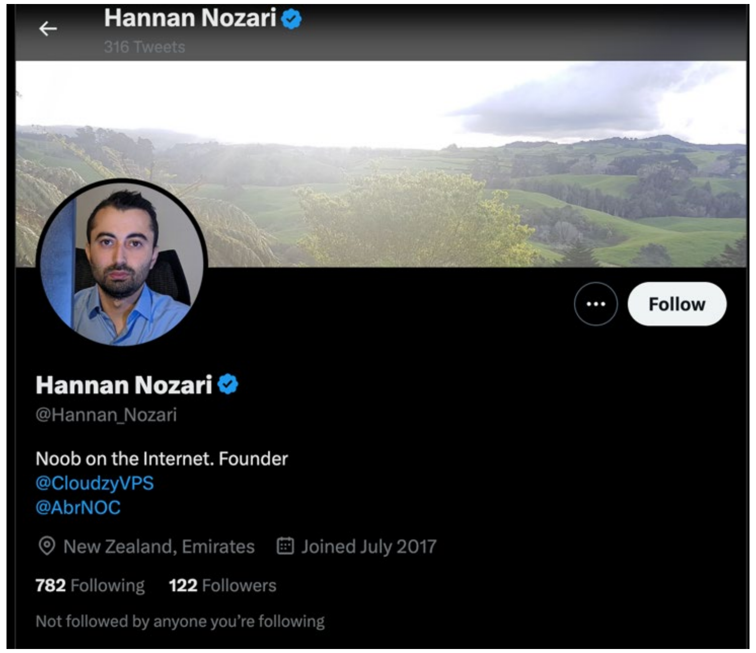
Having researched Cloudzy's corporate records, Halcyon then examined some of the people who worked for Cloudzy. Halcyon discovered what appears to be a mix of seemingly fictitious people and an office full of employees in Tehran, many of whom also appeared to be working for two businesses at the same time: the American company Cloudzy and the Iranian company abrNOC. The self-described founder of both is Hannan Nozari, the man we identified earlier as the point of contact for a large number of Router Hosting / Cloudzy's netblocks.

"The Cloudzy Story," casts Hassan Nozari as the young entrepreneur whose "mind and passion" and "skill in Virtual Machine technology" helped him found Router Hosting in 2008. With "singular focus," "Nozari" claims he grew Router Hosting from "just one server location" to "15 data centers around the world" by 2020.

Recall that C2P Cloudzy was incorporated in Wyoming with an abuse address in Nevada and a New York City-based phone number (VOIP) on its "Contact Us" page. This made it appear that Nozari, as founder of Cloudzy, was presumably located somewhere in the United States.

And yet, "Nozari" also claimed to be the founder of an Iranian company called abrNOC, a fact he confirms on his "verified" Twitter page, where he Tweets mostly in Farsi and describes himself as a "Noob on the Internet"–slang for an inexperienced newcomer.

A Screenshot of Hannan Nozari's Twitter Profile



Hannan Nozari
316 Tweets

Hannan Nozari
@Hannan_Nozari

Noob on the Internet. Founder
@CloudzyVPS
@AbrNOC

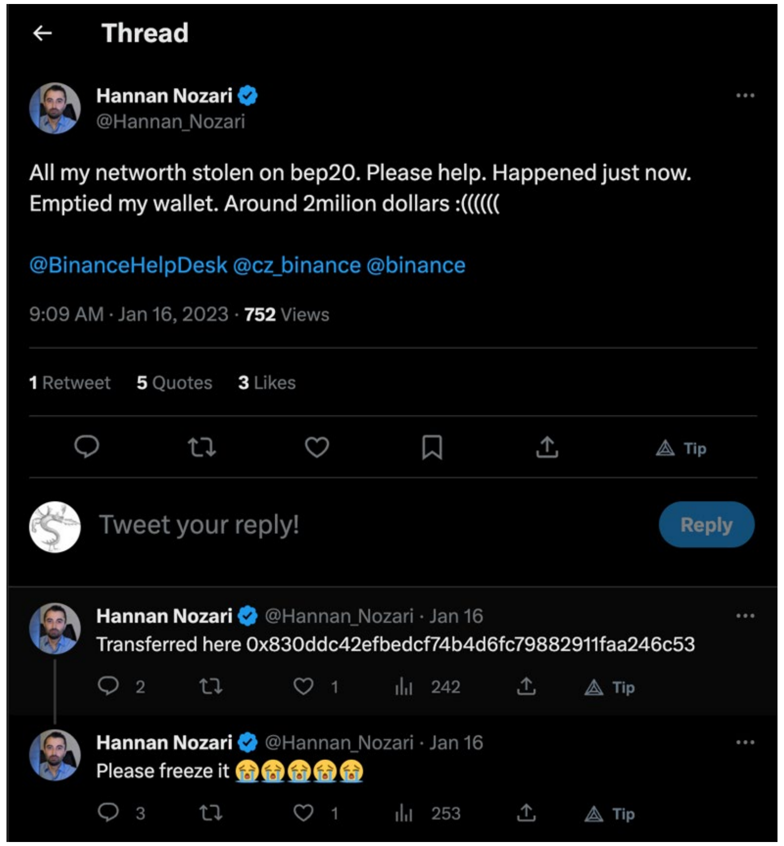
New Zealand, Emirates Joined July 2017

782 Following 122 Followers

Not followed by anyone you're following

The tweets from Nozari revealed an interest in cryptocurrency as well as some measure of financial success. He appears to have made it through an incident in January of 2023 when he claimed to have lost $2 million worth of Binance cryptocurrency.

Mr. Nozari Asking Binance for Help in Recovering Stolen Funds



Hannan Nozari @Hannan_Nozari

All my networth stolen on bep20. Please help. Happened just now. Emptied my wallet. Around 2milion dollars :((((((

@BinanceHelpDesk @cz_binance @binance

9:09 AM · Jan 16, 2023 · 752 Views

1 Retweet 5 Quotes 3 Likes

Hannan Nozari @Hannan_Nozari · Jan 16
Transferred here 0x830ddc42efbedcf74b4d6fc79882911faa246c53
2 1 242

Hannan Nozari @Hannan_Nozari · Jan 16
Please freeze it 😭😭😭😭😭
3 1 253

Atop his Twitter profile, "Nozari" lists New Zealand and the Emirates as his locations. But on a Couchsurfing profile last logged into three years ago he claimed to be "back to live in Tehran" after "15 years of living in New Zealand."

A Facebook profile picture posted on May 3, 2022 appears to show him embracing abrNOC's "Entertainment Lead" "Teddy" at their offices at Fatemi Square (Jahad Square) in Tehran. At the time of writing, Nozari appears on the abrNOC website as the CEO. This left the impression that Nozari was located in Iran running a Tehran-based company while simultaneously running his "American" company based in Wyoming.

He was not the only Cloudzy employee who appears to be making that long commute. Halcyon searched LinkedIn and found eight different employees whose profiles seem to indicate that they currently work for Cloudzy but most of whom are located in Iran.

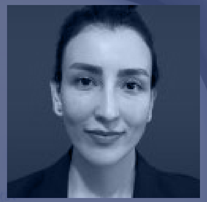
Those few Cloudzy employees who listed their location as somewhere other than Tehran all nevertheless say they attended Iranian universities. We also noticed crossover between some of the above Cloudzy employees and employees of abrNOC based on individuals with the same first name and job function.

Halcyon suspected that C2P Cloudzy didn't actually exist except on paper, and that it was staffed by employees of abrNOC in Tehran. A look at the people writing Cloudzy's blog posts seemed to confirm that Cloudzy employed either fictitious personas or employees of abrNOC. Several Cloudzy bloggers turned out to be more than they appeared.

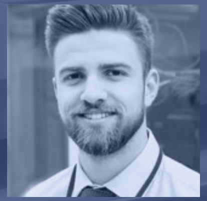
Table 2: Employees of Cloudzy Identified Via LinkedIn

Full Name	LinkedIn URL	Job Title
Hannan Nozari	https://ae.linkedin.com/in/hannan-nozari-a7051b18a	Founder and CEO
Ali Khayyer	https://ir.linkedin.com/in/alikhayyer	Technical Support Engineer
Pantea Ayoubi Nejad	https://ir.linkedin.com/in/pantea-ayoubinejad	Social Media Manager
Parinaz Rasa	https://my.linkedin.com/in/parinaz-rasa-253032173	Technical Writer
Reihaneh Mazahernasab	https://ir.linkedin.com/in/reihaneh-mazahernasab	Search Engine Optimization
Ali Shoeibi	https://www.linkedin.com/in/ali-shoeibi/	Senior Digital Marketing Specialist
Muhamed Krasniqi	https://www.linkedin.com/in/muhamed-krasniqi-19b9331b2	Cisco Router & Firewall Engineer
Mahdi Sajjadpoor	https://www.linkedin.com/in/mahdi-sajjadpoor	Corporate Finance
Ava Joharchi	https://www.linkedin.com/in/ava-joharchi/	Content Writer

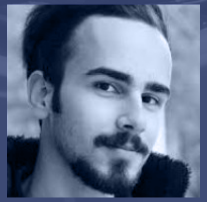
The “Faces” of Cloudzy



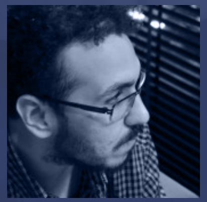
"Paulina Ritter's" headshot matched the one on the LinkedIn profile of "Parinaz Rasa." Rasa was a self-described technical writer at Cloudzy. Her LinkedIn profile listed her location as Malaysia though she recently graduated from the University of Science and Culture in Iran with a degree in electrical and electronic engineering.



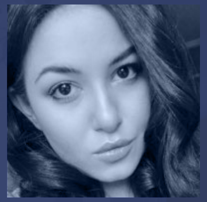
"Matt Schmitt's" picture turned out to be identical to the stock photo of the "Technician" originating on the website of the balladins Group, a hotel group in France and Belgium. Halcyon concluded that "Matt Schmitt" was therefore a fictitious persona.



"Allen's" headshot resembled that of an Iranian person using the name "Ali Shoeibi," according to this website for something called "NP Shop." Cloudzy and npshop.net even used the exact same image URL. "Ali Shoeibi" was also one of the Cloudzy employees identified via LinkedIn. This LinkedIn headshot revealed him to be the same "Ali" listed on the abrNOC website as the "Senior Digital Marketing Specialist."



"Alex Robbins" had an associated LinkedIn profile with the name "Alexander Robbins-Rosen." The exact same headshot was also used by an Iranian graduate student at Shiraz University with the name "Mohammad-Ali Rahebi." He bears a strong resemblance to abrNOC's "Mohammed Reza," their "Infrastructure Engineer."



We found "Emma Bennet" to be another content writer who goes by the name of "Ava Joharchi." Her LinkedIn page is here. And a post on Laborx.com lists her previous work experience at Cloudzy as a Senior Content Writer and Editor with an identical headshot. And though the headshot differs, there is also an "Ava" responsible for content creation at abrNOC.

Halcyon assessed that some Cloudzy bloggers may be entirely made up, while others may be either Iranian, employees of abrNOC, or both.

Apart from employees, Halcyon noticed what appears to be additional overlap between Cloudzy and abrNOC. Both stated they first started serving their customers in 2008. abrNOC's website claims it "started out with hosting and VPS services" – both of which are also offered by C2P Cloudzy.

The two companies have almost identical logos. Both claim to have "more than 15 locations all over the world." Notably, they are the exact same 15 locations, none of which appear to correspond to any infrastructure directly owned by C2P Cloudzy (Router Hosting) or abrNOC:

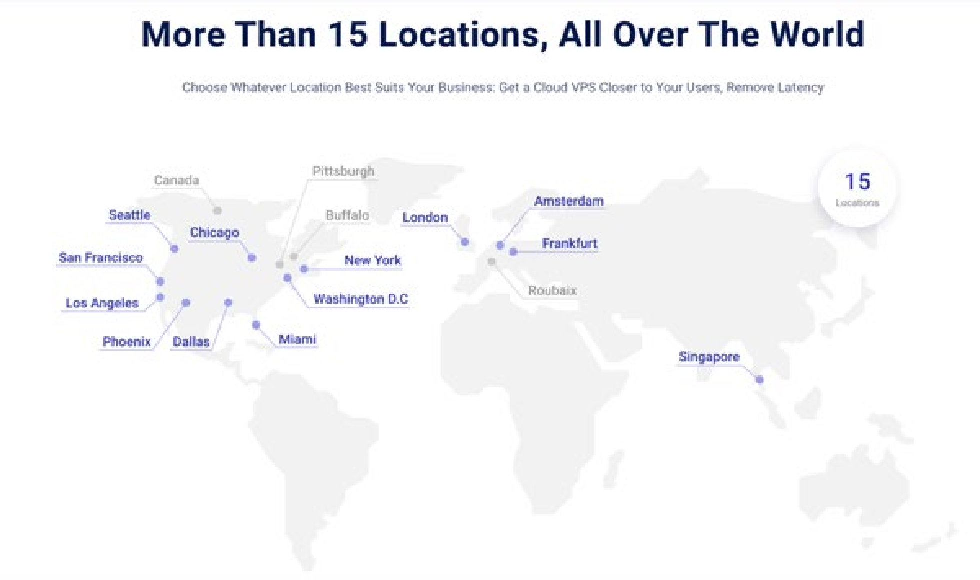


Figure 3: Location Map Taken from Cloudzy's Website

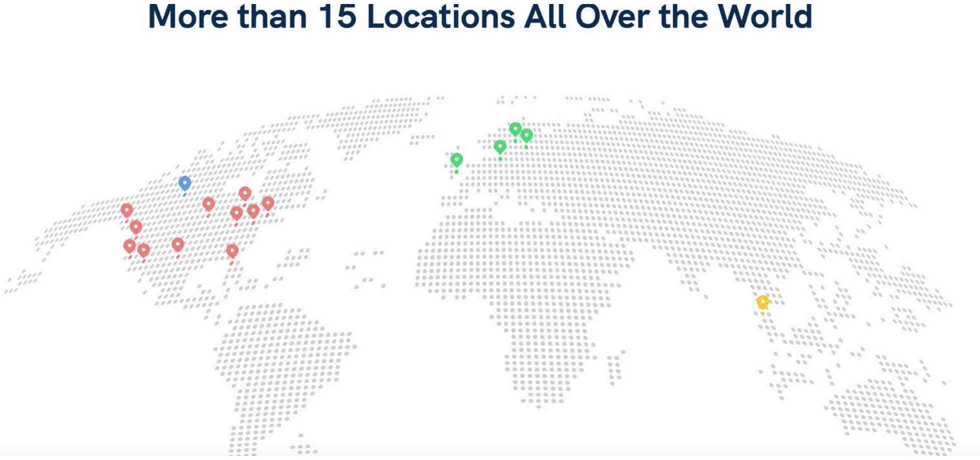


Figure 4: Location Map Taken from abrNOC's Website.

Halcyon therefore assessed with high confidence that C2P Cloudzy is almost certainly a cutout for the actual hosting company, abrNOC, operating out of Tehran, Iran

Recommendations

Halcyon recommends that the technical readers of this report use the indicators of compromise appended below to search their networks for any of the malicious activity we tied to C2P Cloudzy, and that they immediately take note when any of the 11 RDP hostnames we identified surface in their environments.

We recommend that defenders look out for these hostnames both retroactively, to identify possible attacks already in progress, but also proactively, to prevent any malicious activity to begin with.

While Halcyon's focus continues to be on the criminal operations leading to ransomware, we are open to working with the community on other identified malicious activity related to C2P Cloudzy. You can e-mail us at threat_research@halcyon.ai. For future complaints regarding any of the listed hostnames, please direct them to abuse@cloudzy.com.

Our report identified several areas of potential legal liability relating to the apparent operation of an Iranian business in the United States, which if substantiated would raise significant concerns in light of current sanctions requirements, like those listed here: Iranian Transactions Sanctions Regulations (ITSR) (31 CFR Part 560).

We recommend that all U.S. entities or people doing business, wittingly or not, withC2P Cloudzy / Router Hosting, including Cloud Peak Law and ARIN, pause to consider the potential legal implications of their continued association with that company.

Finally, we recommend that Internet service providers learn a lesson from C2P Cloudzy and do a better job of knowing their customers. For even if C2P Cloudzy had no knowledge of the high frequency and volume of the malicious traffic running through its leased infrastructure, significant damage was still done as a result of their policies. And the abuse of legitimate service providers will continue so long as "Internet noobs" like Hassan Nozari allow criminals to act with impunity – all in the name of privacy.

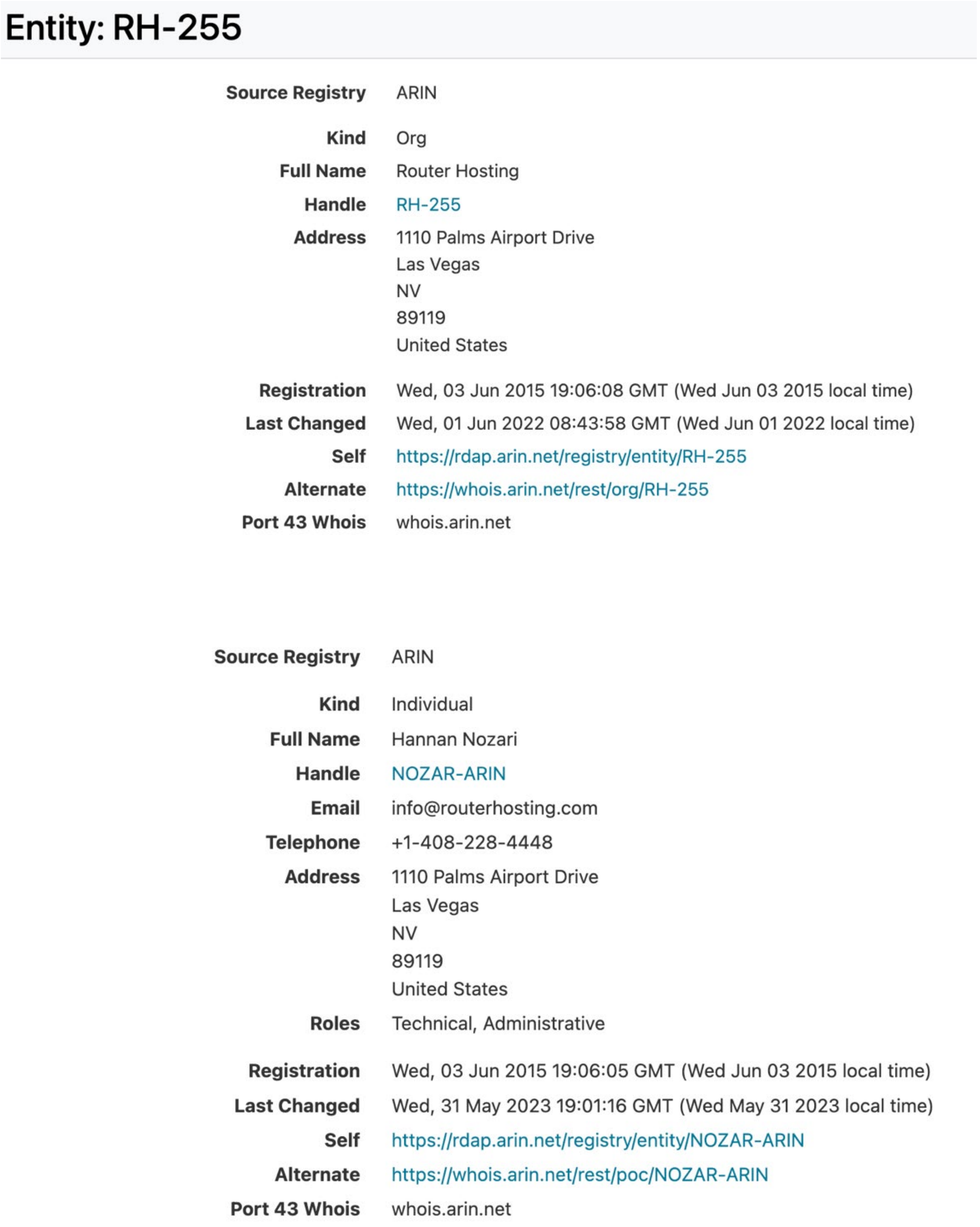
Appendix

Table 3: TLDR – Indicators of Compromise

Indicator Type	Indicator Value
SHA256	4d56e0a878b8a0f04462e7aa2a47d69a6f3a31703563025fb40fb82bab2a2f05
SHA256	b27ca5155e42e372d37cf2bcbb1f159627881ecbae2e51d41f414429599d37a7
IP Address	23.19.58[.]181
IP Address	139.177.146[.]152
IP Address	172.93.201[.]120
Domain	mojimetigi[.]biz

Additional Netblocks Owned by Hannan Nozari (RH-255):

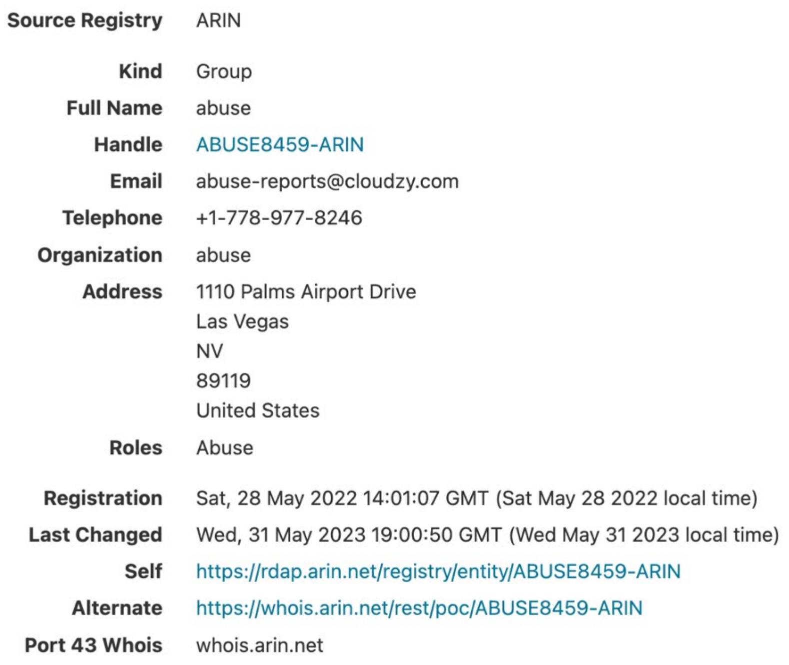
- 104.237.193.40/29
- 104.237.193.56/29
- 104.237.194.152/29
- 104.237.219.32/29
- 104.237.219.40/29
- 167.88.4.0/29
- 167.88.4.112/29
- 167.88.4.16/29
- 167.88.4.24/29
- 167.88.4.8/29
- 172.86.120.0/22
- 172.93.179.8/29
- 172.93.179.24/29
- 172.93.179.32/29
- 172.93.179.40/29
- 172.93.179.72/29
- 172.93.179.96/29
- 172.93.179.104/29
- 172.93.179.112/29
- 172.93.179.120/29
- 172.93.179.128/29
- 172.93.179.144/29
- 172.93.179.152/29
- 172.93.179.160/29
- 172.93.179.176/29
- 172.93.179.184/29
- 172.93.179.192/29
- 172.93.179.200/29
- 172.93.179.208/29
- 172.93.179.224/29
- 172.93.179.232/29
- 172.93.179.240/29
- 172.93.179.248/29
- 172.93.181.0/24
- 172.93.193.0/24
- 172.93.201.0/24
- 172.93.204.120/29
- 172.93.205.128/29
- 172.93.205.136/29
- 172.93.205.144/29
- 64.44.101.0/24
- 64.44.102.0/24
- 64.44.134.0/29
- 64.44.134.16/29
- 64.44.134.24/29
- 64.44.134.32/29
- 64.44.134.40/29
- 64.44.134.48/29
- 64.44.134.56/29
- 64.44.135.0/24
- 64.44.140.232/29
- 64.44.141.0/24
- 64.44.51.168/29
- 64.44.98.0/24



Entity: RH-255

Source Registry	ARIN
Kind	Org
Full Name	Router Hosting
Handle	RH-255
Address	1110 Palms Airport Drive Las Vegas NV 89119 United States
Registration	Wed, 03 Jun 2015 19:06:08 GMT (Wed Jun 03 2015 local time)
Last Changed	Wed, 01 Jun 2022 08:43:58 GMT (Wed Jun 01 2022 local time)
Self	https://rdap.arin.net/registry/entity/RH-255
Alternate	https://whois.arin.net/rest/org/RH-255
Port 43 Whois	whois.arin.net

Source Registry	ARIN
Kind	Individual
Full Name	Hannan Nozari
Handle	NOZAR-ARIN
Email	info@routerhosting.com
Telephone	+1-408-228-4448
Address	1110 Palms Airport Drive Las Vegas NV 89119 United States
Roles	Technical, Administrative
Registration	Wed, 03 Jun 2015 19:06:05 GMT (Wed Jun 03 2015 local time)
Last Changed	Wed, 31 May 2023 19:01:16 GMT (Wed May 31 2023 local time)
Self	https://rdap.arin.net/registry/entity/NOZAR-ARIN
Alternate	https://whois.arin.net/rest/poc/NOZAR-ARIN
Port 43 Whois	whois.arin.net



Source Registry	ARIN
Kind	Group
Full Name	abuse
Handle	ABUSE8459-ARIN
Email	abuse-reports@cloudzy.com
Telephone	+1-778-977-8246
Organization	abuse
Address	1110 Palms Airport Drive Las Vegas NV 89119 United States
Roles	Abuse
Registration	Sat, 28 May 2022 14:01:07 GMT (Sat May 28 2022 local time)
Last Changed	Wed, 31 May 2023 19:00:50 GMT (Wed May 31 2023 local time)
Self	https://rdap.arin.net/registry/entity/ABUSE8459-ARIN
Alternate	https://whois.arin.net/rest/poc/ABUSE8459-ARIN
Port 43 Whois	whois.arin.net

+1-855-8-HALCYON | halcyon.ai

Halcyon is the world's first cyber resilience platform designed from day one to defeat ransomware. Global 2000 companies rely on Halcyon to augment existing EPP, EDR and XDR platforms and undo attacks in minutes with bypass and evasion protection, key capture and automated decryption, as well as exfiltration and extortion prevention. For more information, visit https://www.halcyon.ai/