HostingHunter Series: CHANG WAY TECHNOLOGIES CO. LIMITED

medium.com/@joshuapenny88/hostinghunter-series-chang-way-technologies-co-limited-a9ba4fce0f65

Joshuapenny

November 14, 2023

J

Joshuapenny

--

Introduction

Welcome to my first post. I’ve decided to create a new series of blogs, called ‘HostingHunter’. I will document personal research attempts to uncover malicious or interesting activity conducted on various hosting providers on the internet. I will start with as little knowledge as possible, focusing on the unusual and lesser known providers.

This idea was spawned as a result of regularly finding myself looking at IP addresses at work and wondering what other stuff is on the same hosting provider. Normally, I’m looking for more malware C2s from a single IP, or more phishing infrastructure related to an incident for example. However. in this blog, I will look to target my research on a single session and just record and present whatever I find.

I’m looking forward to writing in a more casual format, and share the enjoyment I get in conducting this research. I will break the blog down in to two parts:

1. The Hosting Provider, and
2. Activity linked with Hosting Provider.

So where to start? Well, the first hosting provider that caught my eye is:

Chang Way Technologies Co. Limited.

Part 1 — The Hosting Provider

Chang Way Technologies Co. Limited was incorporated on 23rd September 2020 as a Private company limited by shares registered in Hong Kong. This seems to be a very common registered address for many companies (2.7k Google results):

Chang Way was assigned Autonomous System Number: **AS57523** and allocated 13 IPv4 prefixes in June 2021 — totaling 3,328 unique IPv4 addresses:

The IP addresses are distributed between Saint Petersburg and Moscow with a small number located in Hong Kong.

changway.hk

The domain is visible on the registration information for the company. I first looked at the WHOIS information to uncover any other connections. Using Virus Total and DomainTools I found two interesting observations:

1. The registration email on the domain: bernard.webmail@gmail.com.
2. The name of the individual/company: Victor Zaycev.

The hosting provider “Cat Technologies Co. Limited” is also registered under the same Victor Zaycev name and at the same Hong Kong address.

This email is used on a number of other domains, most no longer active, however it gives a nice timeline of activity associated with this email address. Through the use of Google, Yandex & VirusTotal, I identified the following domains:

Taking a look at the DNS records for the Chang Way domain also lists an SOA record RNAME which looks like another email address — processor.webmail.gmail.com. This record is used for the email address of the admin responsible for the domain:

So to summarise the findings so far:

Of the domains associated with bernard.webmail@gmail.com, all are expired except for changway.hk and 31337.hk. I’ve covered the first, so let’s look at 31337.hk.

Looks like its been marked as a payload delivery host and sits behind Cloudflare. Some of the files include Amadey and SystemBC:

Interesting subdomains here, notably bearhost and billing (will become clear later):

Back to processor.webmail@gmail.com. Remember, this was used on the DNS records for changway.hk. Utilising Group-IB’s Threat Intelligence Platform and Graph Tool, I’m able to connect the domains registered with bernard.webmail@gmail.com to the processor email address. A new persona: “processor”. This user, on a number of forums, appears to be selling bulletproof hosting servers called “UNDERGROUND” and “BearHost”. On these posts, the contact information includes Telegram accounts: underground31337, billing31337 and bear31337. These names match the subdomains and domains linked to the bernard email address:

After collating the accounts and email addresses associated with the “processor” persona, we can make some connections between the processor email from DNS and the bernard email from WHOIS:

If we run a similar search on the newly identified addresses we can see some interesting results. For example, the jabber contact information linked to processor relates to a post on the website crdpro.cc for “UNDERGROUND — Bulletproof servers” on March 2022. The second result, is a recent dump from a security researcher of Jabber IDs linked to various individuals. Included in this dump are email addresses linked to Alphv, BlackByte, Vice Society, Mallox & No_Escape to name a few. I contacted the researcher and he mentioned that these addresses were mined from cyber crime forums.

Ransomware-linked emails included in the same dataset:

- alphv@01337.ru

- avos@thesecure.biz
- blackbytesupp0rt@onionmail.org
- mallox@exploit.im
- No_ESCAPE@exploit.im
- stormouss21@dnmx.org
- vicesociety@onionmail.org
- v-society.official@onionmail.org

Continuing the Yandex searches, we can see what other forums these processor accounts have advertised on:

To summarise some of the findings after part 1 (The Hosting Provider):

- Through WHOIS and DNS, we can connect two Gmail addresses to both domains registered and hosted on Chang Way.
- Bernard is used for new domain registrations. Notably changway.hk and 31337.hk, which contains subdomains linked to processor.
- processer is used for the persona “processor”, advertising Bulletproof hosting named BearHost/Underground.
- processor is a persona of an individual conversing on forums and via Jabber channels with accounts linked to ransomware groups.

Part 2 — Activity linked with the Hosting Provider.

Summary of the findings below:

-
-
-
-
-
-
-
-
-

Tools used: urlScan, Shodan, Maltego, VirusTotal & Greynoise.

Before I look at traffic coming in to the network, e.g. looking for phishing pages, malware C2s, etc. I thought I would start looking at what sort of traffic is coming out of the network via Greynoise.

Greynoise

Greynoise is fantastic for helping to understand whether IP addresses have been classified as potentially malicious from conducted activity such as scanning or being observed exploiting a particular vulnerability. In this case, we can enter the subnets for Chang Way and observe what types of activity has been observed from this network.

After entering the results in to the visualiser, I analysed all of the subnets together:

62.122.184.0/24 appears to contain the most IP addresses tagged as malicious and associated with a variety of scanning activity.

Finding 1 — Threat Actors exploiting CVE-2023–3519 to implant webshells on Citrix Netscaler Gateways

Using urlScan, we can get an idea of the types of domains hosted on the ASN and potentially malicious activity. The ASN feature shows **latest scans, incoming hits, recent screenshots, related screenshots and recently observed hostnames.**

https://urlscan.io/asn/AS57523

Within **related screenshots**, some interesting images of CitrixVPN gateways for various companies appear to be communicating with addresses on this ASN. That definitely requires further investigation.

AS57523 CHANGWAY-AS, HK

urlscan.io - Website scanner for suspicious and malicious URLs

urlscan.io

Digging further we can identify the offending IP address:

Based on this information we’ve found some domains: *cloud-js.cloud* & *jscript.club*.

Looking at the *cloud-js.cloud* domain returns a lot of company Citrix Gateways.

Additionally, looks like some JavaScript files hosted on the domain. Initial looks like POST authentication credentials to this domain on logon.

A quick search on this domain returns two interesting articles:

X-Force uncovers global NetScaler Gateway credential harvesting campaign

IBM X-Force uncovered a campaign where attackers were exploiting the vulnerability identified in CVE-2023-3519 to…

securityintelligence.com

This looks like ongoing activity relating to “Threat Actors Exploiting Citrix CVE-2023–3519 to Implant Webshells”.

Using this URLScan query:

filename:”citrix.js” OR filename:”citrix2.js” OR filename:”citrix3.js” AND page.url:”/vpn/index.html”

We can identify the domains used for credential exfiltration. From here we can run FOFA queries for domains found in webpages of Citrix logon pages:

((“jscloud.ink” || “jscloud.biz” || “cloudjs.cloud” || “cloud-js.cloud” || “cloudjs.live”)) && server!=”cloudflare”

Providing us with a view of global victims:

To note, the threat actors placed these domains behind Cloudflare to evade detection of their backend server but through these tools we’ve identified it:

Additionally, the CISA report mentions the use of NPS:

• Deployed the NPS tunneller [6] to victim networks to the /tmp directory. NPS is an open source tunneller written in Go.

We can also verify that by checking port 8081 for this IP address:

Global view of servers with the same header fingerprint:

NPS: https://github.com/ehang-io/nps

Appears to be written by a Chinese developer and has over 2 million downloads. Predominant distribution of servers using NPS are located in China.

So the first observed activity.The offending IP address behind these domains is: *85.209.11.134*

Utilising this information, we’ve mapped other servers running NPS and used urlScan/FOFA to identify possible global compromised Citrix Gateway servers. We’ve also identified the backend server masked by Cloudflare used for credential exfiltration from the gateways.

Finding 2 — National Crime Records Bureau (India) Credit Card phishing

This finding definitely entertained me and my teenage step-daughter as I ran her through the part of victim. I asked her to figure out what was wrong and why the PC had claimed she'd been blocked until she'd entered credit card details. I asked her to exit off this page and I had great enjoyment watching the resulting confusion.

This page if impersonating a page from the National Crime Records Bureau in an attempt to demand payment from victims visiting "pornographic and illegal sites". The interesting part is that when you first load the page, you are presented with a popup box asking you to reload the page:

Upon reloading, the screen enters "Full screen mode" and impersonates the browser bar. Resulting attempts to cross the screen off will fail, likely adding to the anxiety of any victims and increasing the likelihood of eventual payment. Interesting social engineering tactics that are likely effective. Utilising the favicon hash of the webpage we can identify 9 more servers dedicated to this scam, hosted on Chang Way:

URLScan link to reload page results:
https://urlscan.io/search/#hash%3A13b787fc7df5bd583e50c3f159fc16296757aa3e3efeaefe954cf33273e58504

Example FOFA search based on a Base64 encoded string found on the webpage:
https://en.fofa.info/result?qbase64=UEdneElHTnNZWE56UFNKaGJHVnlkQzFrWVc1blpYSWlQand2YURFK0RRb2dJQ0FnSUNBZ0lDQWdJQ0FnSUNBZ0lDQWdJRHh3UGp3dmNEND0%3D — this returns more results outside of just Chang Way.

Finding 3 — Android Malware: Hydra, Hookbot, aXedroid, Rusty Droid

Hydra.

I previously wrote an article on Hydra Android banking trojan:
https://www.bridewell.com/insights/blogs/detail/hydra-new-campaign-targeting-android-banking-in-spain-and-latin-america

Here I found 4 servers running C2s for the malware. .apk files are named Chrome.apk and PlatStore.apk. Also found were login panels for Hookbot, aXedroid and Rusty droid:

Finding 4 — Windows Malware: SectopRAT

https://malpedia.caad.fkie.fraunhofer.de/details/win.sectop_rat

Finding 5 — Metasploit, Nessus and Cobalt Strike

Nessus: “Take advantage of the industry’s most trusted vulnerability assessment solution to assess the modern attack surface.”

Use any combination of the following red boxes to find many many many more Nessus servers on the internet:

Quick Description of Metasploit and Cobalt Strike:

MetaSploit: “The **Metasploit Project** is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company **Rapid7**.

Its best-known sub-project is the open-source **Metasploit Framework**, a tool for developing and executing exploit code against a remote target machine.” — Rapid7

Cobalt Strike: “is a commercial adversary simulation software that is marketed to red teams but is also stolen and actively used by a wide range of threat actors from ransomware operators to espionage-focused Advanced Persistent Threats (APTs)”. — Mandiant

The graph above shows the IP addresses running Cobalt Strike or Metasploit on Chang Way. One IP address, 85.209.11.162, has both running on it. A number of the Cobalt Strike servers on Chang Way used the watermark: 1580103824, which is used to identify the version of Cobalt Strike being used. This is the same watermark as the Cobalt Strike server used in the recent Cl0P/SysAid report:

We can focus in another step further by using the SSL jarm on the certificate used by the servers. I touched on this in another recent post regarding the SysAid report: https://twitter.com/josh_penny/status/1722664249162445078. Using the SSL jarm with the watermark version, we can cluster some of the Cobalt Strike servers. Here, we use the ssl jarm from the SysAid IP address and we can see that is shares that fingerprint + watermark with 2 servers, one on Chang Way and one on Cat Technologies.

Finding 7 — 404 TDS

Consider this one more of a “low confidence” assessment. 404 TDS is not something I’ve really attempted to track before but I believe that some part of it runs through Chang Way. What is 404 TDS? TDS stands for Traffic Distribution System. It’s a service that is purchasable by a variety of threat actors in order to deliver different malware. The purpose of the TDS is to redirect traffic through threat actor controlled infrastructure to validate the victim before redirecting to the next in the chain based on certain criteria. This allows threat actors to conduct things like geo-fencing to filter out unwanted traffic (such as researchers) and deliver victims to different malware, think infostealers (personal machine) or Cobalt Strike (enterprise system). Proofpoint do a great job of tracking this and updating the community on payloads and lures used as part of this ecosystem. Payloads delivered via 404 TDS include: Truebot, NetSupport RAT, IcedID, AHK Bot,AsyncRAT, and DarkGate etc.

This ProofPoint post in October: (https://www.proofpoint.com/uk/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader), gave us indicators for 404 and IcedID. Let's look at the 404 TDS ones:

All of these domains resolve to a single IP: 193.3.19.160. Guess which Organisation that sits on…

Let's put this into Maltego and find out what else we can find on Chang Way relating to 404 TDS:

In total that's 12 IP addresses. All of which contain a number of domains that don't resolve to a webpage and have communicating files in VirusTotal all matching what you would expect from typical email attachment lures (in HTML and PDF formats). I'm confident these IP addresses are all related, however, its interesting to me that my searches only found those hosted on Chang Way despite this being a well used Traffic Distribution System.

So you'll know what this is from part 1. Looks like processor's UNDERGROUND/BEARHOST.

UNDERGROUND/BEARHOST Login Panel

Below is a translation from one of the adverts provided for this service:

You can read all about my findings here: https://www.bridewell.com/insights/blogs/detail/bridewell-and-group-ib-uncover-possible-blackbyte-victim-data-notify-victims?utm_source=LinkedIn&utm_medium=Linkedin_Organic&utm_term=cti-blog-blackbyte&utm_content=blackbyte_cti_blog&utm_campaign=cti_bridewell

To summarise, I identified a server hosted on Chang Way that appeared to contain victim data from the BlackByte ransomware group. The server was located here:

We assessed that this is likely an operational security failure by the owner/ operators of the server. The directory names were named after what appeared to be organisations around the globe. After analysing these directories, Bridewell and Group-IB were able to link a large portion of the organisations to the Data Leak Site for the ransomware group BlackByte. The open server contained 37 directories, with 19 named after organisations posted to the BlackByte data leak site between January and September 2023. 15 subdirectories were named after organisations not posted. The organisations are located in the US, Turkey, Germany and Denmark. It is currently assessed with moderate confidence that these organisations could be victims of the BlackByte ransomware group and either paid the ransom or are potentially unaware of any compromise.

Bridewell and Group-IB specialists acquired the dataset to allow organisations to verify the plethora of archive files contained within the open directory. All files were compressed .zip files named “Archive1”, “Archive 2”, etc. with each file approximately 1 GB in size.

- Total number of files: 140,135.
- Total Directory size: 1.2TB

Finding 10 — TacticalRMM

“Tactical RMM is a remote monitoring & management tool built with Django, Vue and Golang. It uses an agent written in Golang and integrates with MeshCentral.” — https://docs.tacticalrmm.com/

This is another RMM tool that has been used before by Threat Actors as a form of persistent remote access into a corporate network and should be monitored for very closely.

Last year, the DFIR report released an article whereby TacticalRMM was used in the intrusion.

Emotet Strikes Again - LNK File Leads to Domain Wide Ransomware - The DFIR Report

In June of 2022, we observed a threat actor gaining access to an environment via Emotet and operating over a eight day…

thedfirreport.com

In this case, I found only one IP address linked to TacticalRMM on Chang Way (there are over 1,000 on the internet). This IP is interesting as the domain and SSL cert seem to be impersonating “delltechnologies.com”, Dell Inc:

Now I won’t assume this is set up to use against Dell but if I were them, I’d maybe monitor for this IP address and/or domain coming in and out of their network. But, it could easily be used against anyone in an attempt to mask remote support from Dell for example. Doesn’t look like it will be used legitimately that’s for sure.

This forum is littered with links to Credit Card selling sites, fake document services and a forum with links to interact with bots on Telegram to purchase cards.

Conclusion

Well, there was a lot to digest here and next time I might have to pick a top 5 list. However, I feel like a know Chang Way technologies far more intimately now after this. I have a good idea of the sort of criminal activities being conducted on this ASN. There appear to be some interesting connections between the company Chang Way and the users behind it running some form of bulletproof hosting. Additionally, it was interesting to find a backend server receiving Citrix VPN credentials. And I definitely didn't expect to find BlackByte victim data. Ultimately, I definitely learn some new techniques and methods for utilising some of these tools and have some more ideas so I enjoyed the exercise personally.

Now that I've had a good look at Chang Way, I will look for investigate another Organisation. However, I'd love to hear feedback on whether you enjoyed this article and whether you found it interesting. I would certainly like to take the research further with anyone who is interested and willing to assist.

Thanks for reading!

Josh