Uncovering the DNS Underbelly of UNC5174: The Shift from SNOWLIGHT to VShell

Table of Contents

Executive Report

UNC5174, a Chinese-sponsored group known for using the open-source reverse shell tool named “SUPERSHELL,” struck again. In January 2025, they used a new open-source tool and command-and-control (C&C) infrastructure dubbed “SNOWLIGHT.” This time around, they have begun using another tool dubbed “VShell.”

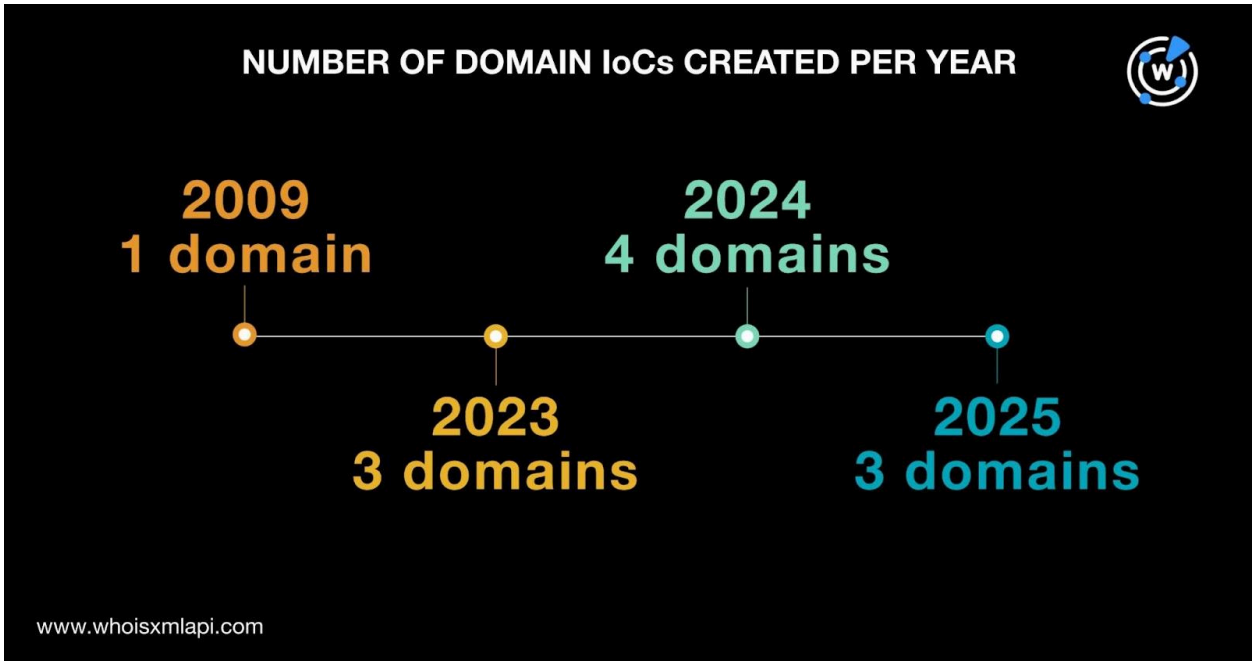
The Sysdig Threat Research Team disclosed their findings about UNC5174’s latest campaign, including 25 indicators of compromise (IoCs) comprising 13 domains and 12 IP addresses. WhoisXML API expanded the current list of IoCs, which led to the discovery of these new artifacts:

- One alleged victim IP record obtained from the Internet Abuse Signal Collective (IASC)
- Eight email-connected domains
- 13 additional IP addresses, 11 of which turned out to be malicious
- 67 IP-connected domains, three of which have already been weaponized for attacks
- 199 string-connected domains, seven of which have already figured in various malicious campaigns

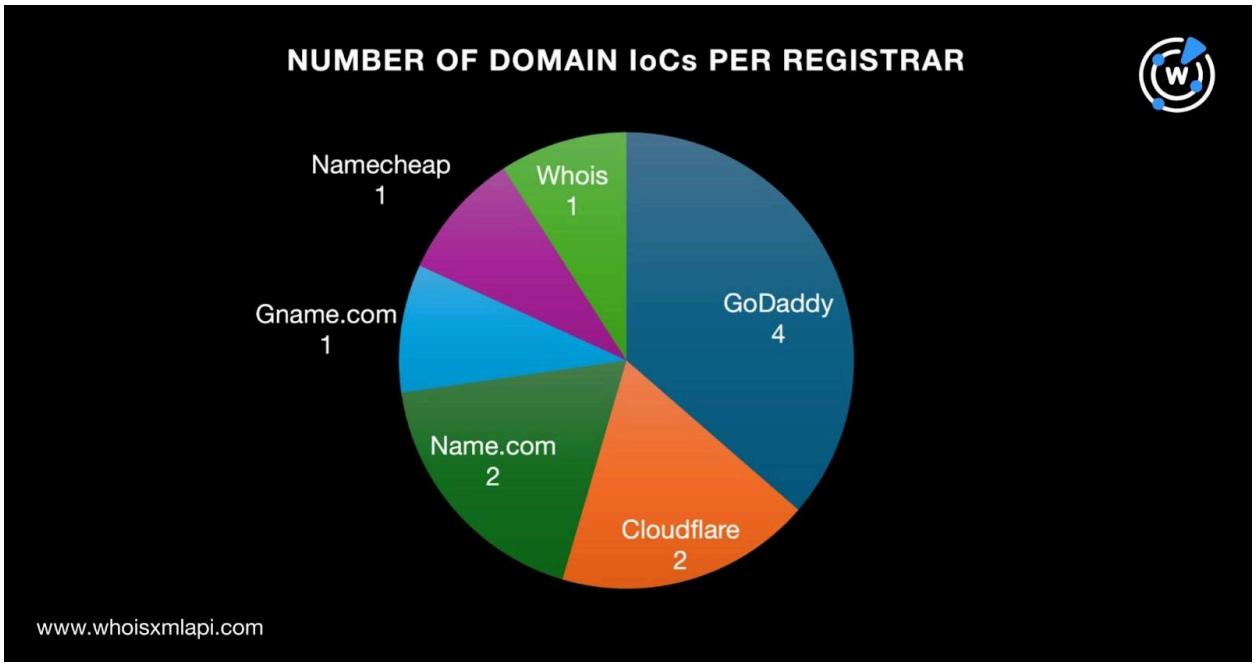
More about the VShell Attack IoCs

Before embarking on our IoC list expansion, we sought to uncover more information about the attack IoCs first. To that end, we queried the 13 domains identified as IoCs on Bulk WHOIS API and found that only 11 of them had current WHOIS records. We also discovered that:

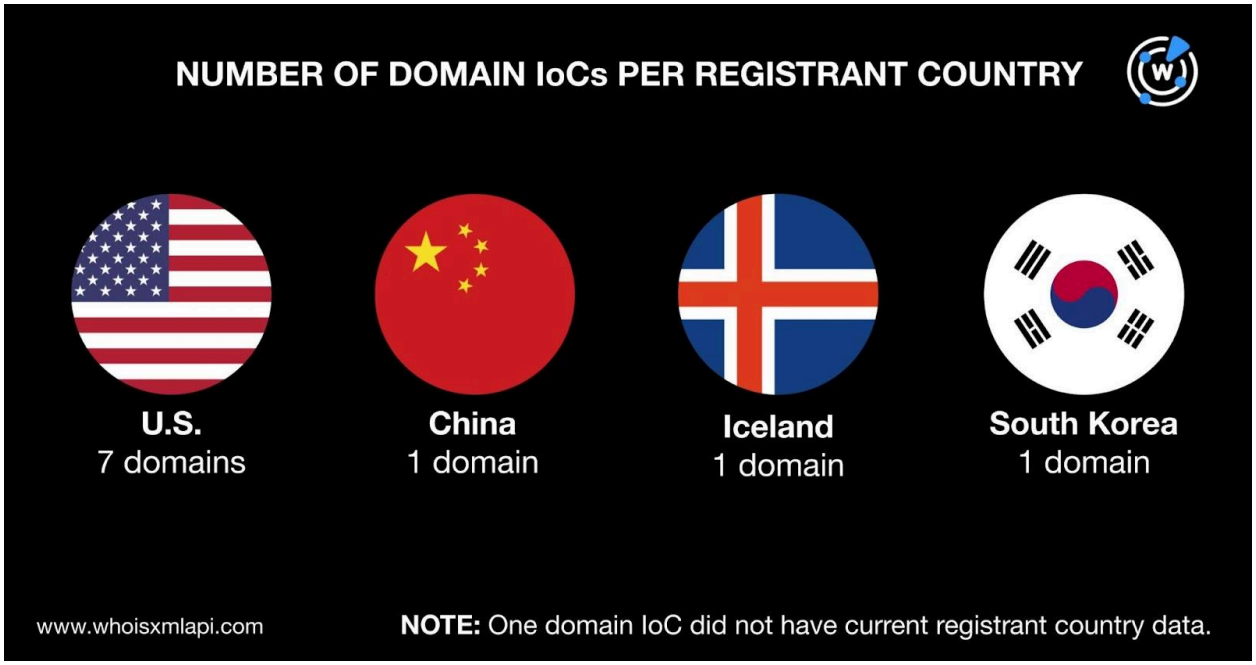
- The 11 domains were created between 2009 and 2025, indicating that the threat actors did not have a preference in terms of domain age. Specifically, one domain was created in 2009, three in 2023, four in 2024, and three in 2025.



- The 11 domains were administered by six registrars led by GoDaddy, which accounted for four domains. Cloudflare and Name.com tied in second place with two domains each. Finally, one domain each was administered by Gname.com, Namecheap, and Whois.



- Only 10 of the 11 domains had registrant countries on record. Specifically, they were registered in four countries led by the U.S., which accounted for seven domains. Finally, one domain each was registered in China, Iceland, and South Korea.

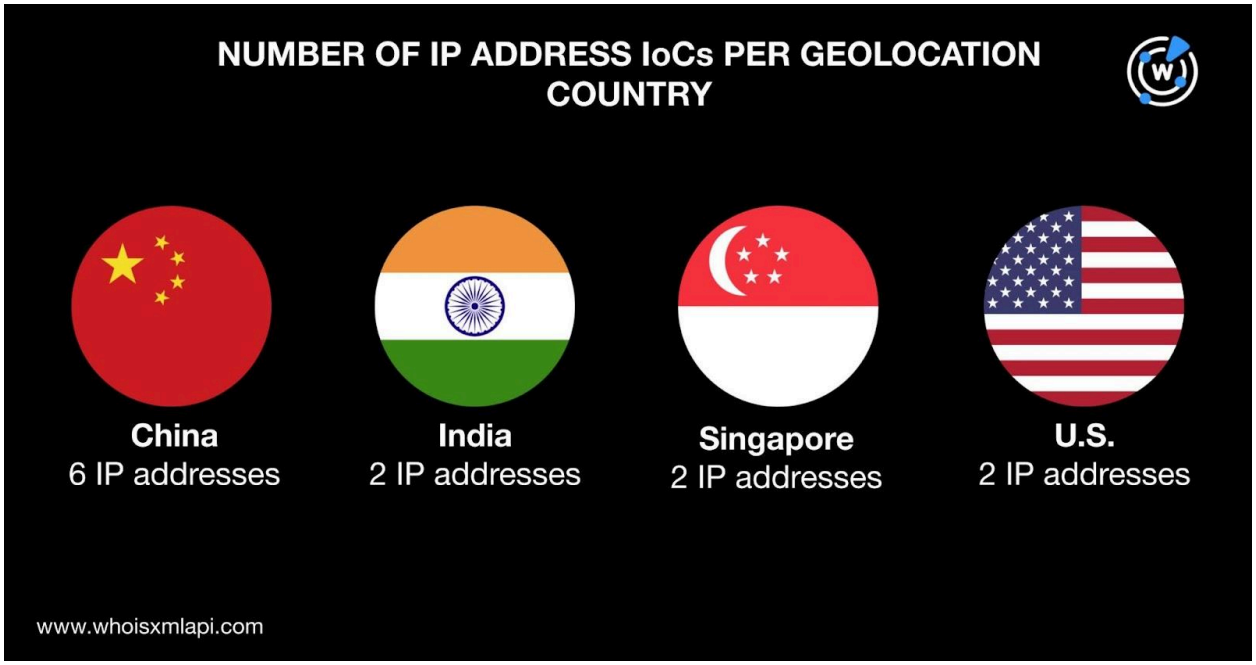


We also queried the 13 domains identified as IoCs on DNS Chronicle API and found that only nine of them had historical domain-to-IP resolutions. Altogether, the nine domains posted 207 resolutions over time. The domain c1oudf1are[.]com recorded the oldest IP resolution date. In particular, it resolved to the IP address 104[.]18[.]52[.]126 on 16 October 2019. Take a look at the historical DNS details for three other domains below.

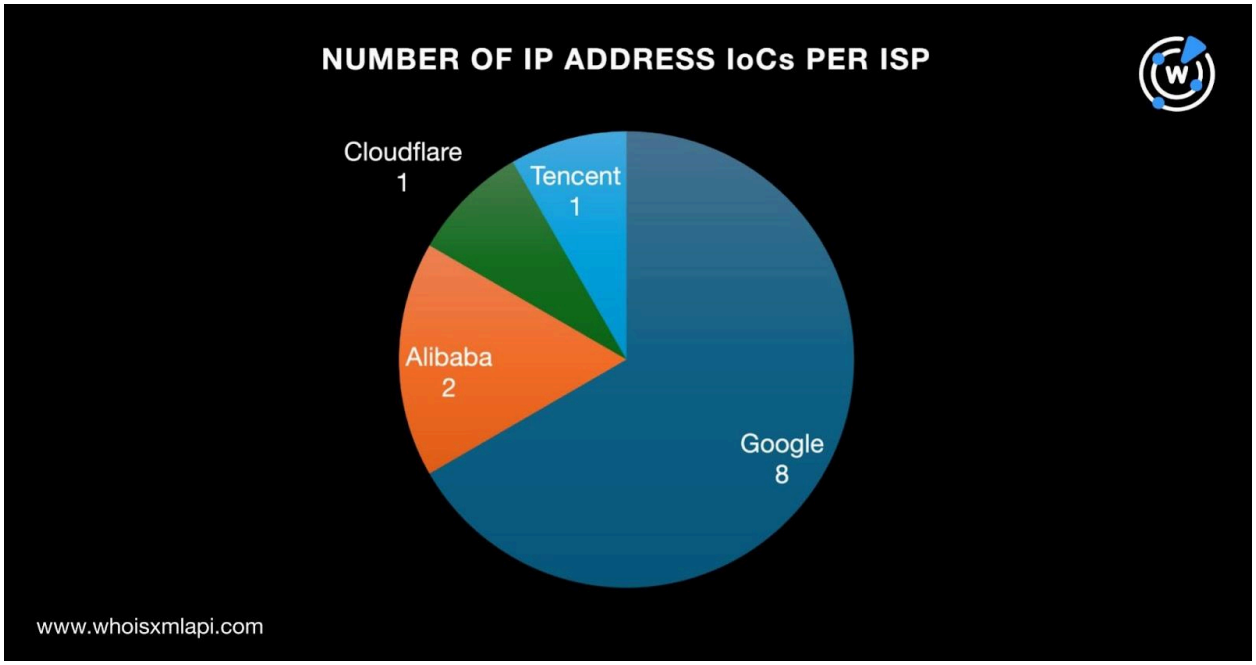
DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
bing-server[.]com	12	1 August 2023
ciscocdn[.]com	32	6 December 2019
gooogleasia[.]com	27	4 September 2023

Next, we queried the 12 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and found that:

- They were geolocated in four countries led by China, which accounted for six IP addresses. Finally, two IP addresses each were geolocated in India, Singapore, and the U.S.



- They were administered by four ISPs led by Google, which accounted for eight IP addresses. Alibaba came in second place with two IP addresses. Finally, one IP address each was administered by Cloudflare and Tencent.



Like the domains identified as IoCs, we queried the 12 IP addresses on DNS Chronicle API as well. We found that 10 of them had historical IP-to-domain resolutions. Specifically, the 10 IP addresses resolved to 1,180 domains so far. Interestingly, six of the 10 IP addresses recorded the oldest resolution date, that is, 19 November 2021. Take a look at five examples below.

IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST DOMAIN RESOLUTION DATE
188[.]114[.]97[.]3	1,000	25 January 2022
34[.]131[.]20[.]34	12	19 November 2021
34[.]150[.]33[.]237	12	19 November 2021
34[.]92[.]255[.]51	13	19 November 2021
34[.]96[.]239[.]183	42	19 November 2021

In addition, using sample netflow data our researchers obtained from the IASC, we found additional information on the IP address 45[.]43[.]208[.]31 that was identified as an IoC. The sample data revealed one alleged victim IP record.

UNC5174 Attack IoC List Expansion Findings

Our analysis began with a WHOIS History API query for the 13 domains identified as IoCs. The results showed that only three domains had email addresses in their historical WHOIS records. In particular, the three domains had 15 email addresses in their records after duplicates were filtered out. Further scrutiny revealed that only two were public email addresses.

A Reverse WHOIS API query for the two public email addresses revealed that they were not present in any domain's current WHOIS records but they did appear in the historical records of eight email-connected domains after duplicates and those already identified as IoCs were filtered out.

Next, we queried the 13 domains identified as IoCs on DNS Lookup API and found that seven of them actively resolved to IP addresses. Specifically, the seven domains resolved to 13 unique IP addresses after duplicates and those already tagged as IoCs were filtered out.

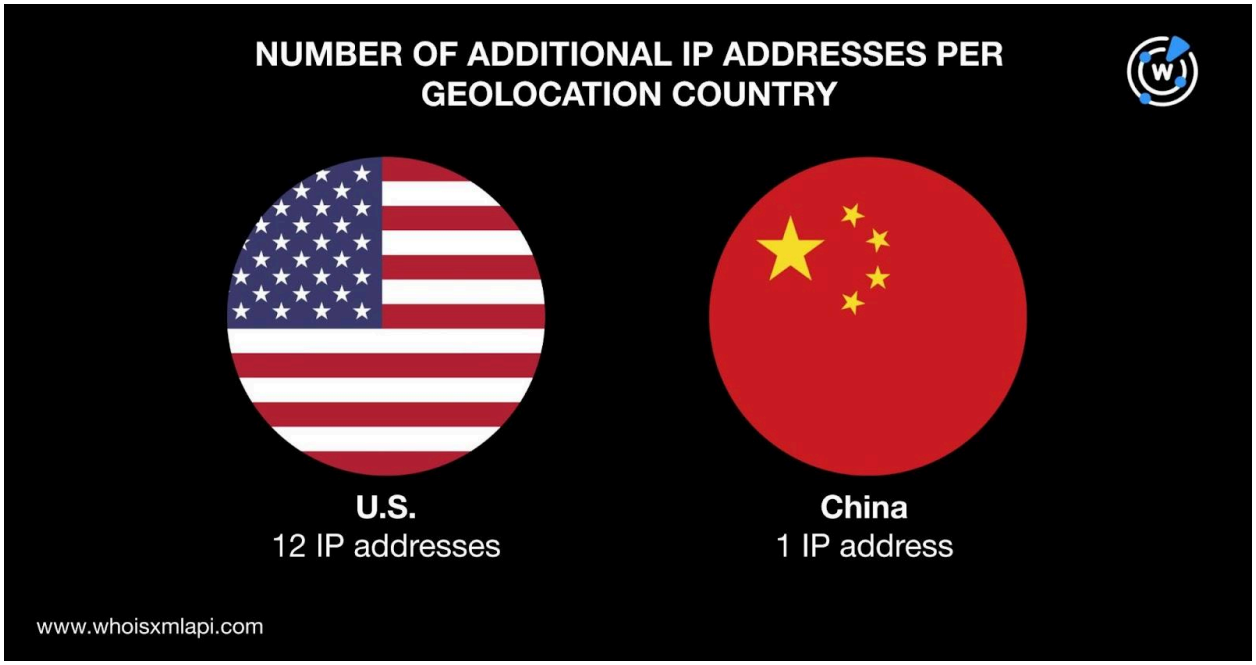
A Threat Intelligence API query for the 13 additional IP addresses showed that 11 have already been weaponized for cyber attacks. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]16[.]1	Attack Command and control (C&C) Generic threat Malware distribution Phishing Spamming Suspicious activity
104[.]21[.]48[.]1	Attack C&C Generic threat Malware distribution Phishing Spamming Suspicious activity
104[.]21[.]80[.]1	Attack C&C Generic threat Malware distribution Phishing Spamming

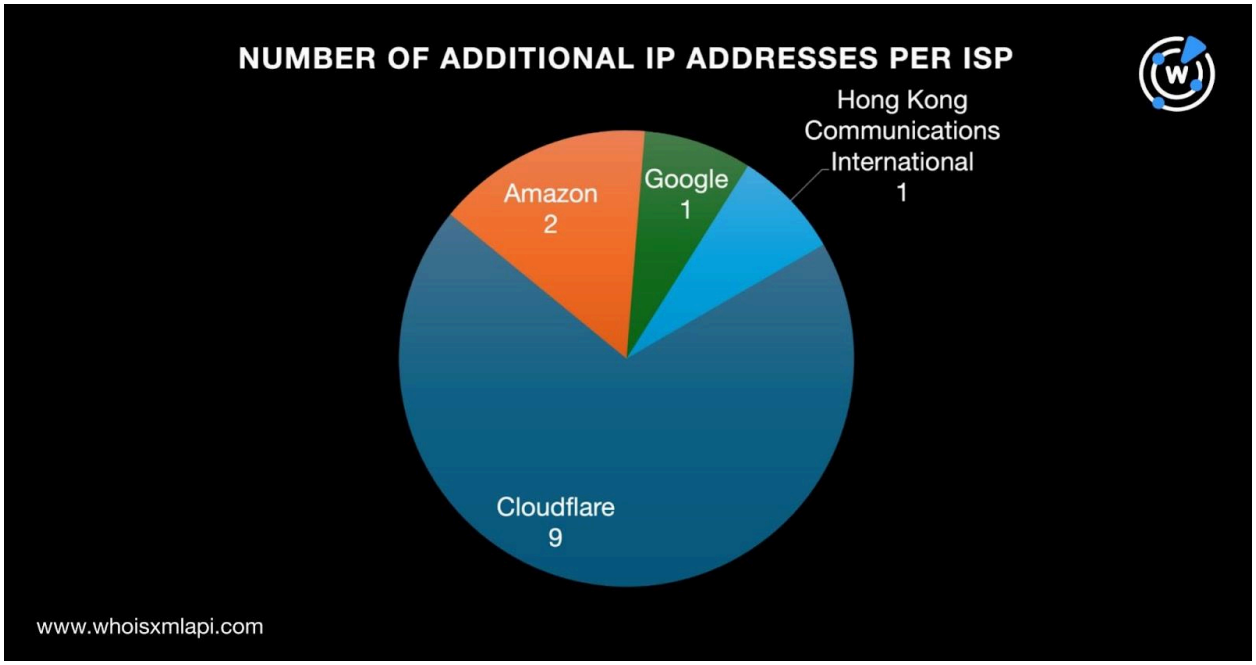
	Suspicious activity
104[.]21[.]96[.]1	Attack C&C Generic threat Malware distribution Phishing Spamming Suspicious activity
172[.]67[.]205[.]152	Malware distribution

We queried the 13 additional IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in two countries. Specifically, 12 IP addresses were geolocated in the U.S. while one pointed to China as its origin.



- They were administered by four ISPs led by Cloudflare, which accounted for nine IP addresses. Amazon took the second spot with two IP addresses. Finally, one IP address each was administered by Google and Hong Kong Communications International.



After the last step, we now had 25 IP addresses for further analysis. That said, we queried the IP addresses on Reverse IP API and found that 16 of them currently hosted domains and three of them could be dedicated hosts. In particular, the three possibly dedicated IP addresses hosted 67 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 67 IP-connected domains showed that three have already figured in cyber attacks. An example would be bing-server[.]com, which was associated with malware distribution.

Lastly, we scoured the DNS for domains with the same text strings as the 13 domains identified as IoCs. We used Domains & Subdomains Discovery and found 199 string-connected domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out. In particular, they started with these eight strings:

- bootstrapcdn.
- c1oudf1are.
- chmobank.
- ciscocdn.
- huionepay.
- samsungcdn.
- telegrams.
- windowstimes.

Notice that the text strings also resemble various popular brand names, such as Cloudflare, Samsung, and Windows.

A Threat Intelligence API query for the 199 string-connected domains revealed that seven of them were already considered malicious. Take a look at three examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
bootstrapcdn[.]cfd	Malware distribution
bootstrapcdn[.]codes	Malware distribution
bootstrapcdn[.]site	Malware distribution

—

Our DNS deep dive into the IoCs for the latest UNC5174 attack leveraging VShell led to the discovery of one alleged victim IP record and 287 potentially connected artifacts. We specifically collated eight email-connected domains, 13 additional IP addresses, 67 IP-connected domains, and 199 string-connected domains. Several of the artifacts, particularly 11 IP addresses and 10 domains have already been weaponized for various cyber attacks.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Email-Connected Domains

- 027zr[.]com
- conf-edu[.]org
- placdn[.]com
- whcx118[.]com
- yaoyao-ei[.]org
- ztecdn[.]com

Sample Additional IP Addresses

- 104[.]21[.]112[.]1
- 13[.]248[.]213[.]45
- 172[.]67[.]205[.]152
- 198[.]176[.]59[.]221
- 76[.]223[.]67[.]189
- 8[.]8[.]8[.]8

Sample IP-Connected Domains

- 6a867b0b-f156-4d91-a342-09d2c1cce7b4[.]random[.]sex666vr[.]com
- account[.]gooogleasia[.]com
- aliyun-cloud[.]com
- ap[.]gooogleasia[.]com
- bing-server[.]com
- btt[.]sex666vr[.]com
- cdn-vr[.]sex[.]sex666vr[.]com
- cdn-vr[.]sex666vr[.]com
- cdn[.]gooogleasia[.]com
- evil[.]gooogleasia[.]com
- front[.]japanslr[.]sex666vr[.]com
- front[.]sex666vr[.]com
- front[.]tw-slr[.]sex666vr[.]com
- gooogleasia[.]com
- k8[.]sex666vr[.]com
- kf159[.]www[.]sex666vr[.]com
- ld[.]ldplus7[.]ws
- ldplus[.]sex666vr[.]com
- ldplus7[.]ws
- m[.]ldplus7[.]ws
- microsoft[.]gooogleasia[.]com
- plus[.]ldplus7[.]ws
- vr[.]sex666vr[.]com
- website[.]ldplus7[.]ws
- www[.]666[.]sex666vr[.]com
- www[.]aliyun-cloud[.]com

Sample String-Connected Domains

- bootstrapcdn[.]biz
- bootstrapcdn[.]center
- bootstrapcdn[.]cf
- c1oudf1are[.]io
- c1oudf1are[.]link
- chmobank[.]online
- chmobank[.]ru
- ciscocdn[.]net
- huionepay[.]biz
- huionepay[.]cc
- huionepay[.]cn
- samsungcdn[.]net
- telegrams[.]agency
- telegrams[.]app
- telegrams[.]asia
- windowstimes[.]cf
- windowstimes[.]com
- windowstimes[.]me