The MOONSHINE Exploit Kit and the DarkNimbus Backdoor in the DNS Spotlight

Table of Contents

Executive Report

The Earth Minotaur threat group recently revived the MOONSHINE exploit kit, first discovered in 2019.

According to Trend Micro's in-depth analysis, MOONSHINE had more than 55 servers in 2024 and has been updated with more exploits and functions compared with its 2019 version. Apart from targeting vulnerable instant messaging apps on Android devices, it also affects Chromium-based browsers installed on Windows computers. DarkNimbus, the backdoor MOONSHINE delivered, also had two variants that affected both Android and Windows devices. These facts point to making the latest Earth Minotaur attack a multiplatform threat.

The researchers identified 53 indicators of compromise (IoCs) associated with the attack comprising 44 domains extracted from URLs and nine IP addresses. The WhoisXML API research team expanded the list of IoCs and uncovered additional threat artifacts, including:

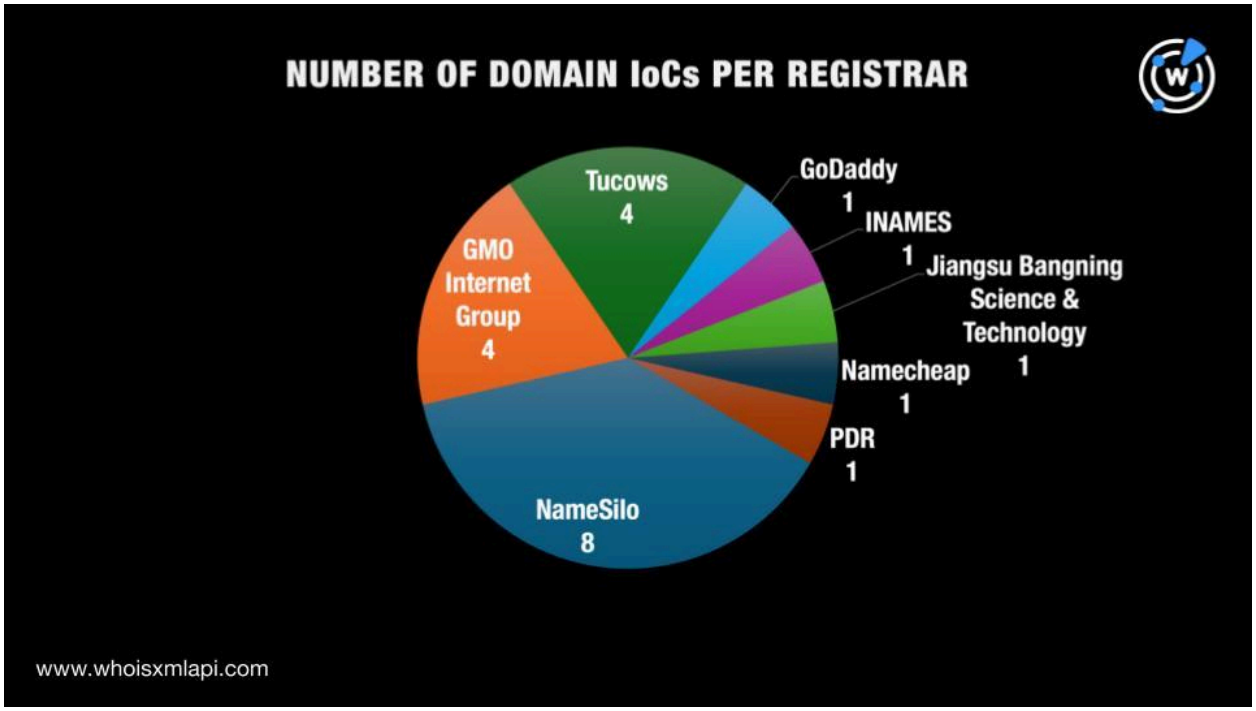
- 333 email-connected domains
- Eight additional IP addresses, all of which turned out to be malicious
- One IP-connected domain
- 121 string-connected domains

A Closer Look at the IoCs

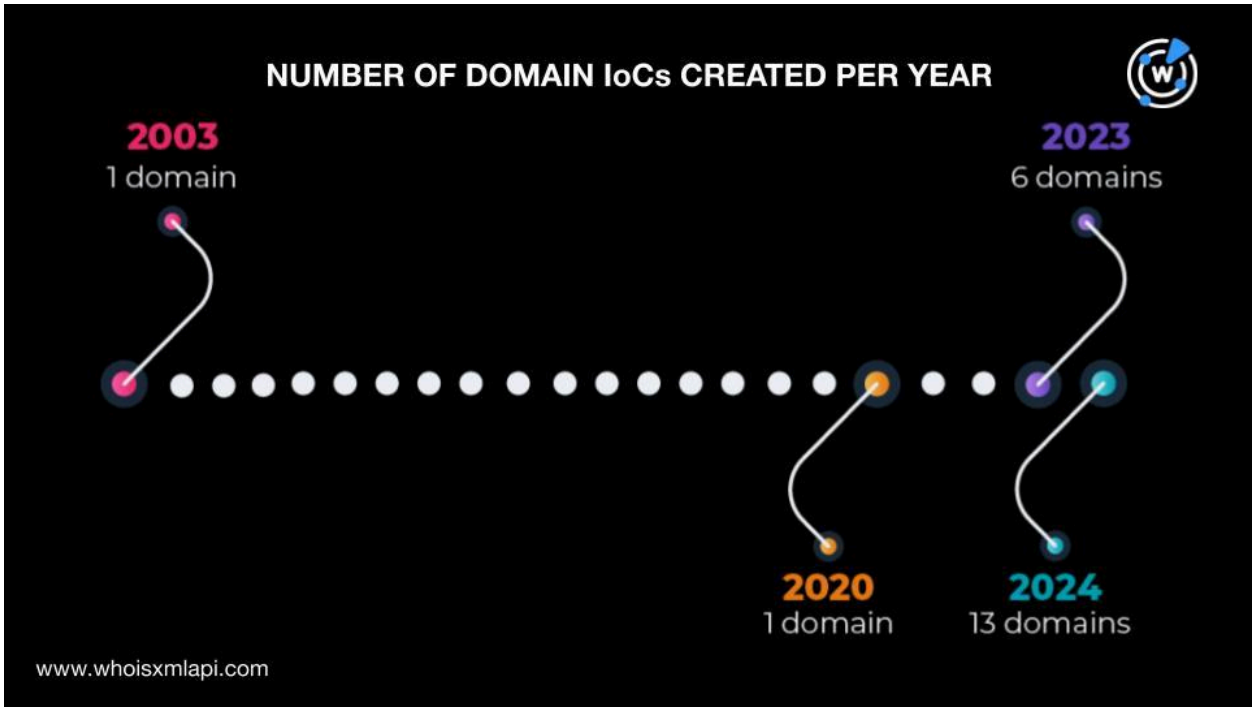
As our usual first step, we queried the 44 domains tagged as IoCs on WHOIS API and found that only 21 had current WHOIS records. Here's a breakdown of their record details.

- They were administered by eight registrars led by NameSilo, which accounted for eight domains. GMO Internet Group and Tucows tied in second place with four domains

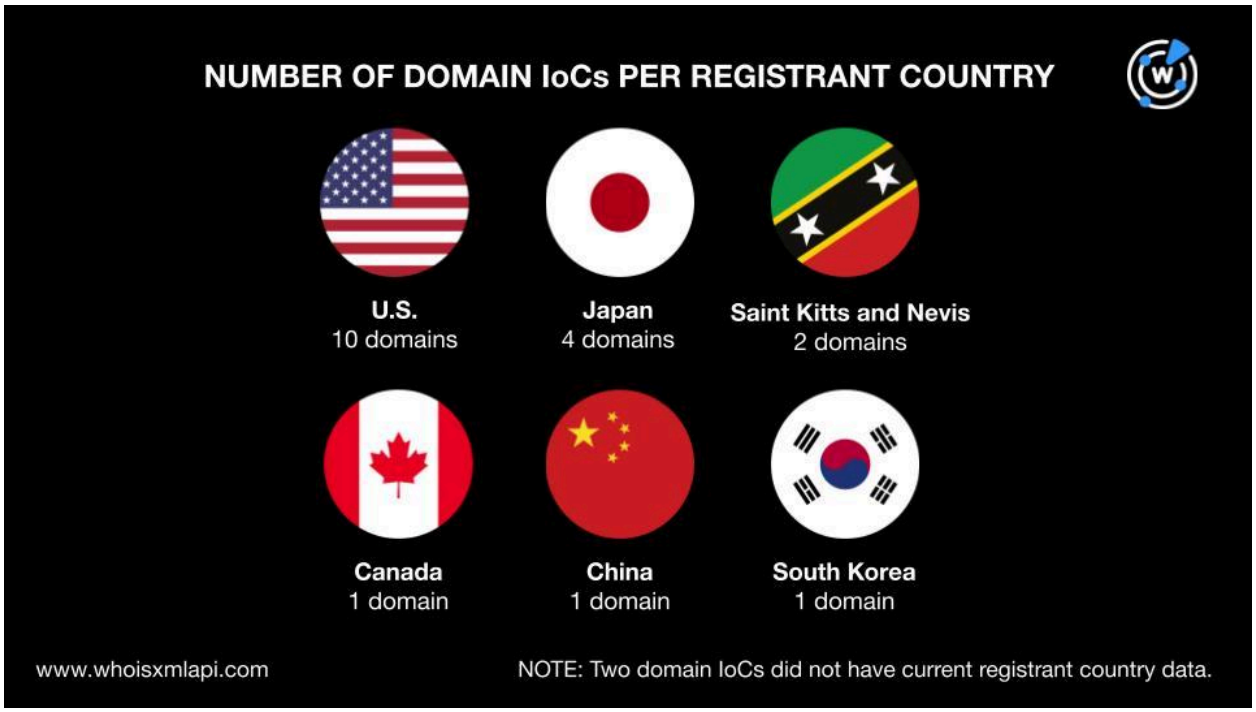
each. Finally, GoDaddy, INAMES, Jiangsu Bangning Science & Technology, Namecheap, and PDR accounted for one domain each.



- They were created between 2003 and 2024. Specifically, one domain each was created in 2003 and 2020, six in 2023, and 13 in 2024.



- Only 19 domains had registrant countries. Ten were registered in the U.S., four in Japan, two in Saint Kitts and Nevis, and one each in Canada, China, and South Korea.

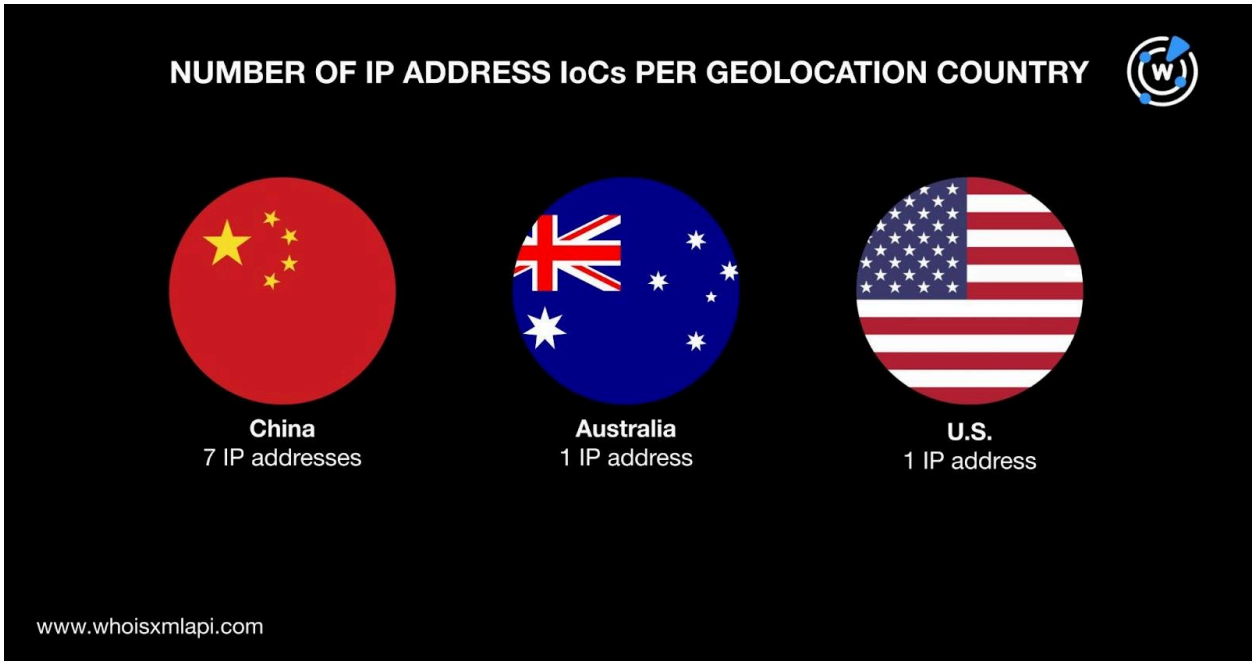


A DNS Chronicle API query for the 44 domains tagged as IoCs revealed that only 32 had historical IP resolutions. Altogether, they posted 371 IP resolutions over time. The IoC tibetonline[.]info recorded the earliest IP resolution date—13 October 2019. The following table shows the total number of IP resolutions and first and last IP resolution start dates for five other domain IoCs.

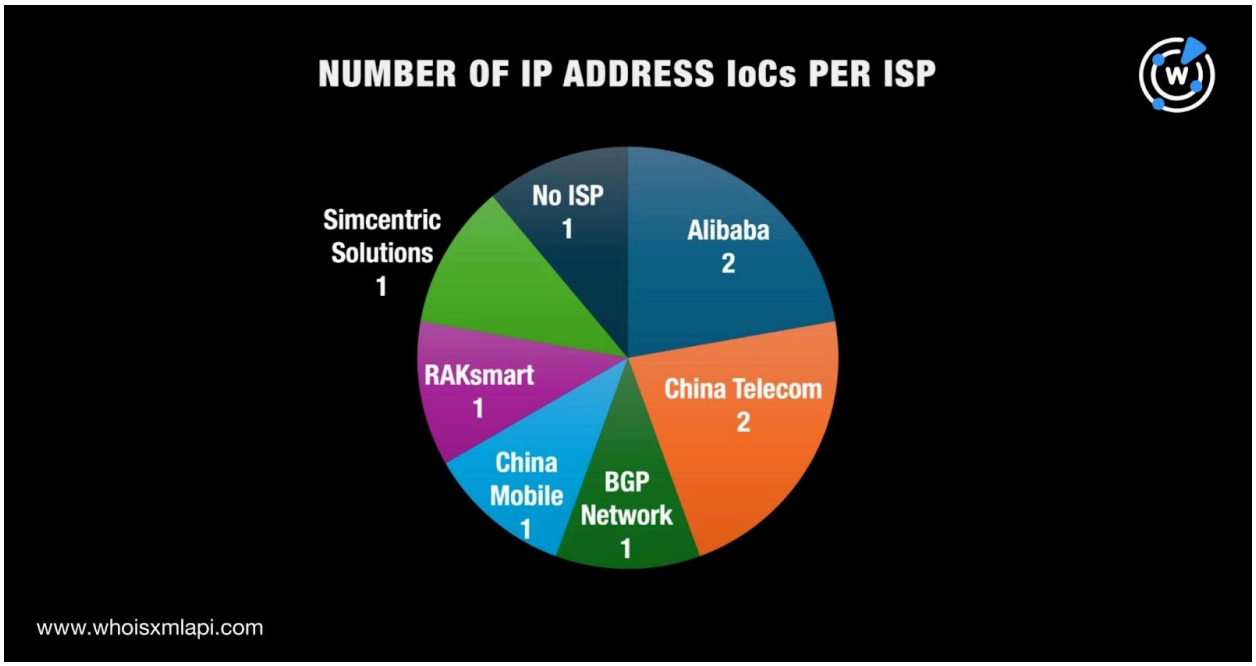
DOMAIN IoC	TOTAL NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION START DATE	LAST IP RESOLUTION START DATE
ansec[.]com	43	18 October 2019	3 December 2024
cloudvn[.]info	38	29 August 2020	19 December 2024
symantke[.]com	29	8 May 2022	15 August 2024
lodepot[.]com	27	29 September 2021	12 December 2024
ammffggo[.]com	24	19 November 2021	2 June 2023

We then queried the nine IP addresses tagged as IoCs on Bulk IP Geolocation Lookup and found that:

- They were geolocated in three countries led by China, which accounted for seven IP addresses. One IP address each was geolocated in Australia and the U.S.



- Only eight had ISPs on record. They were administered by six ISPs led by Alibaba and China Telecom, which accounted for two IP addresses each. The four remaining IoCs were administered by BGP Network, China Mobile, RAKsmart, and Simcentric Solutions.



Our DNS Chronicle API query for the nine IP addresses tagged as IoCs revealed that only three had historical domain resolutions. Altogether, they posted 78 domain resolutions over time. The IP address 103[.]255[.]179[.]186 recorded the first domain resolution date—7 October 2019. The IoC 125[.]65[.]40[.]163, meanwhile, recorded a single first domain resolution date—11 November 2019.

IoC List Expansion Analysis Findings

We began our search for connected threat artifacts by querying the 44 domains tagged as IoCs on WHOIS History API and found that 35 of them had 64 email addresses in their historical WHOIS records. Nineteen were public email addresses.

A Reverse WHOIS API query for the 19 public email addresses showed that three could belong to domainers, while nine did not have other domain connections. The seven remaining public email addresses appeared in the current WHOIS records of 333 other domains after duplicates and those already identified as IoCs were filtered out.

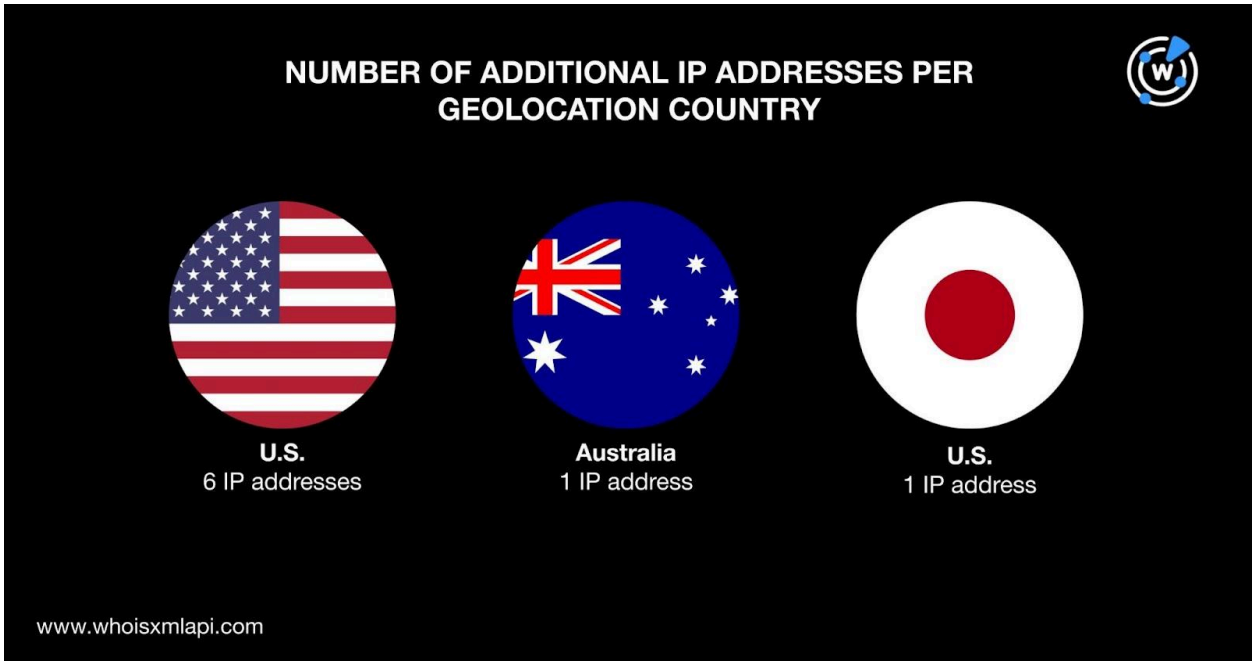
Next, we queried the 44 domains tagged as IoCs on DNS Lookup API and found that seven actively resolved to eight IP addresses after duplicates and those already identified as IoCs were filtered out.

Threat Intelligence API queries for the eight additional IP addresses revealed that they were all malicious. Take a look at three examples below.

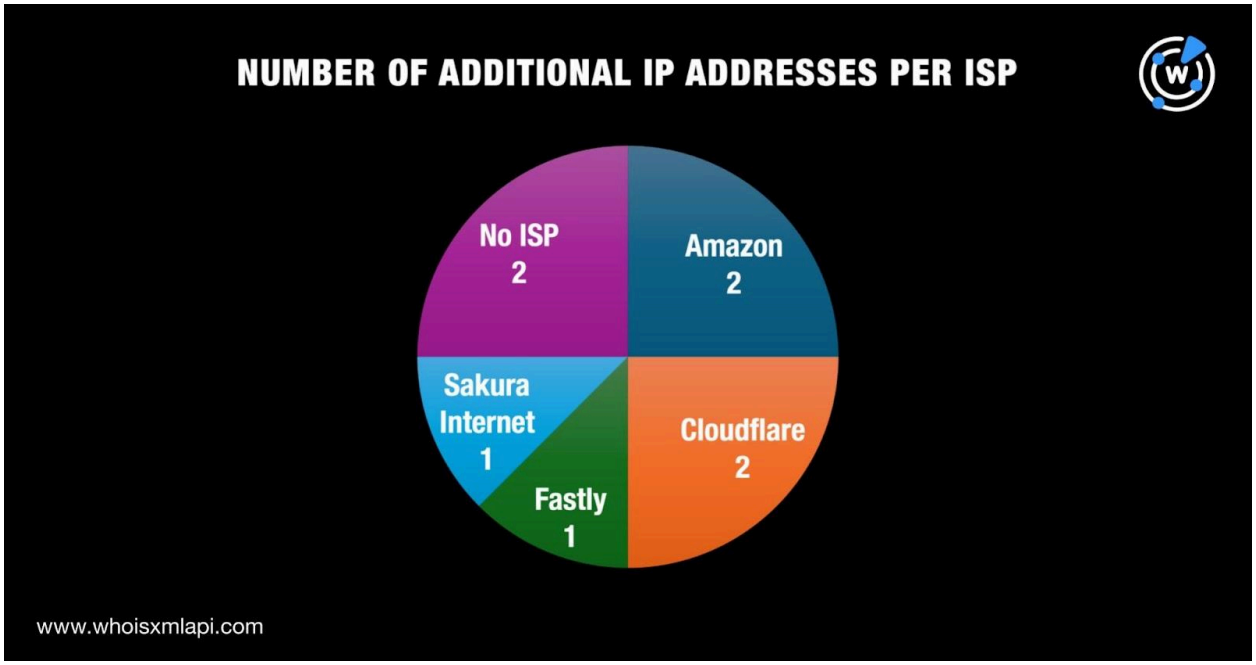
MALICIOUS IP ADDRESS	ASSOCIATED THREATS
103[.]224[.]212[.]217	Attack Command and control (C&C) Generic threat Malware Phishing Suspicious activity
199[.]36[.]158[.]100	Attack Generic threat Malware Phishing Suspicious activity
52[.]223[.]13[.]41	Attack C&C Generic threat Malware Phishing Suspicious activity

A bulk IP geolocation lookup for the eight additional IP addresses showed that:

- They were geolocated in three countries led by the U.S., which accounted for six of the additional IP addresses. One IP address each was geolocated in Australia and Japan.



- Only six of them had ISPs on record. Amazon and Cloudflare accounted for two IP addresses each. Fastly and Sakura Internet, meanwhile, administered one IP address each.



We then queried the 17 IP addresses—nine tagged as IoCs and eight additional—on Reverse IP API and discovered that while eight of them hosted other domains, only one could be a dedicated host.

The IP address 103[.]255[.]179[.]186 hosted one domain—gateoptical[.]com—after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

To cap off our analysis, we searched for other domains that contained the same text strings as those identified as IoCs using Domains & Subdomains Discovery. Only 18 of the 44 text strings appeared in other domains. They were:

- ahamar.
- ansec.
- api1-meta.
- bstram.
- chatonlineapp.
- cloudvn.
- esetinc.
- leak-news.
- lodepot.
- newsdomain.
- newwechat.
- onlinewechat.
- onlineweixin.
- onlinewxapp.
- serverwechat.
- tibetonline.
- weetogether.
- wetransfering.

The strings appeared in 121 other domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

—

Our analysis of the 53 MOONSHINE and DarkNimbus IoCs led to the discovery of 463 connected artifacts comprising 333 email-connected domains, eight additional IP addresses, one IP-connected domain, and 121 string-connected domains. Eight of these artifacts have already figured in malicious campaigns so far.

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

- 189map[.]cn
- 3sixtyfive[.]com
- 4crazy[.]com
- 51andorid[.]com
- admincloud[.]cn
- agbank[.]com[.]cn
- aircloud[.]cn
- aircloud[.]com[.]cn
- akiro[.]com
- alcobra[.]com
- allcloud[.]cn
- allcloud[.]com[.]cn
- aodigou[.]com
- aovi[.]com[.]cn
- arifan[.]com
- asuscloud[.]cn
- atcloud[.]cn
- axbank[.]com[.]cn
- azbank[.]cn
- bankcloud[.]com[.]cn
- bbpower[.]com
- beidoutuan[.]com
- birthsmart[.]com
- bnyun[.]cn
- boooz[.]com
- bqbank[.]cn
- braggie[.]com
- braspa[.]com
- buy2sell[.]com
- caddyhome[.]com
- carboman[.]com
- chainbank[.]com[.]cn
- chen-chuan[.]cn
- chinaacademyofart[.]cn
- chuangweike[.]com
- classcloud[.]cn
- clicktv[.]net
- cloudair[.]cn
- cloudair[.]com[.]cn
- cloudauto[.]cn
- cloudband[.]cn
- cloudblue[.]cn
- cloudcity[.]cn
- cloudcity[.]com[.]cn
- cloudcross[.]cn
- cloudcross[.]com[.]cn
- clouddoctor[.]cn
- cloudframe[.]cn
- cloudgolf[.]cn
- cloudhome[.]com[.]cn

Sample Additional IP Addresses

- 1[.]2[.]3[.]4
- 103[.]224[.]212[.]217
- 104[.]21[.]31[.]195
- 160[.]16[.]200[.]77

Sample String-Connected Domains

- ahamar[.]loan
- ansec[.]ae
- ansec[.]be
- ansec[.]ca
- api1-meta[.]ws
- bstram[.]xyz
- chatonlineapp[.]fun
- cloudvn[.]asia

- cloudvn[.]click
- cloudvn[.]club
- esetinc[.]ir
- leak-news[.]com[.]ua
- lodepot[.]com[.]au
- newsdomain[.]club
- newsdomain[.]co[.]uk
- newsdomain[.]com
- newwechat[.]cn
- onlinewechat[.]cn
- onlinewechat[.]fun
- onlinewechat[.]online
- onlineweixin[.]com
- onlinewxapp[.]ws
- serverwechat[.]ph
- tibetonline[.]asia
- tibetonline[.]be
- tibetonline[.]ch
- weetogether[.]com
- wetransfering[.]cf