

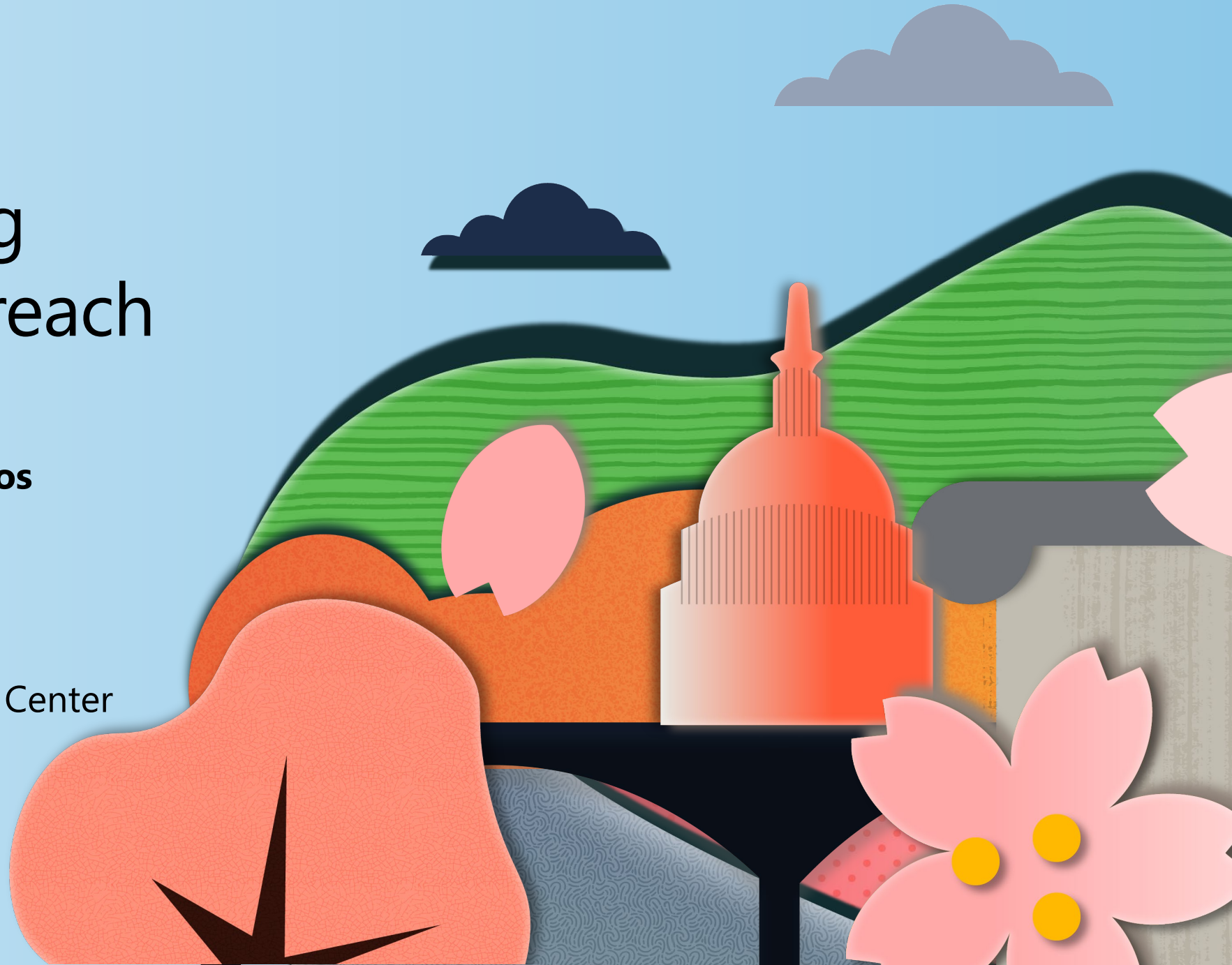


DC Engineering Academic Outreach

From TikTok to Flipper Zeros

Sartaj Singh Dhami
Sr. Security Investigator

Microsoft Security Response Center
Cyber Defense Ops Center
GovCloud / Sovereign Cloud



NATIONAL SECURITY

Microsoft says Chinese hackers breached email, including U.S. government agencies

UPDATED JULY 12, 2023 · 12:15 PM ET



Jenna McLaughlin



A signage of Microsoft is seen on March 13, 2020 in New York City. The U.S. government and Microsoft recently revealed that Chinese hackers broke in to online email systems and stole some unclassified information.

Jeenah Moon/Getty Images

Who Is Midnight Blizzard? Russian-Linked Group Has Repeatedly Targeted Microsoft, Company Says

James Farrell Former Staff

James Farrell is a breaking news reporter on the Forbes news team.



Mar 8, 2024, 04:25pm EST

Updated May 2, 2024, 11:59pm EDT

f **TOPLINE** Microsoft [says](#) that the Russian-linked group known as Midnight Blizzard or Nobelium has made repeated attempts to access Microsoft's systems in recent weeks, escalating its efforts against Microsoft since the company first disclosed in January that Midnight Blizzard had [accessed](#) some of its corporate email accounts.



⚠ Video unavailable

ADVERTISEMENT

← Ads by Google

[Send feedback](#)

[Why this ad? ▶](#)



News [Secure Future Initiative \(SFI\)](#) · 7 min read

Security above all else—expanding Microsoft’s Secure Future Initiative

By [Charlie Bell](#), Executive Vice President, Microsoft Security

May 3, 2024



Last November, we launched the [Secure Future Initiative](#) (SFI) to prepare for the increasing scale and high stakes of cyberattacks. SFI brings together every part of Microsoft to advance cybersecurity protection across our company and products.

Since then, the threat landscape has continued to rapidly evolve, and we have learned a lot. The recent findings by the Department of Homeland Security’s Cyber Safety Review Board (CSRB) regarding the Storm-0558 cyberattack from last July, and the Midnight Blizzard attack we reported in January, underscore the severity of the threats facing our company and our customers.

Lawmakers Question Microsoft's President About Its Presence in China

Brad Smith testified before a House committee a year after Chinese hackers infiltrated Microsoft's technology and penetrated government networks.

▶ Listen to this article · 5:44 min [Learn more](#)

📄 Share full article 🔄 📌



Microsoft's president, Brad Smith, told the House Committee on Homeland Security that his company's presence in China served American interests. Eric Lee/The New York Times



By **Karen Weise**

Karen Weise has covered Microsoft since 2018.

So Back to Research...

So it started with an email...

The screenshot shows an Outlook email window titled "Research opportunity with VT students - Message (HTML)". The interface includes a ribbon with various actions like Delete, Reply, Forward, and a Quick Steps pane. The email content is as follows:

Research opportunity with VT students

Husna Ali-Khan
To: Zac Rotsch; Iman Malik; Paul Muessig; Sartaj Dhani; Ben Hilburn; Alyce Babb

General

You replied to this message on 7/1/2022 2:40 PM.

VT Research.pdf
3 MB

Hello Hokies,

I hope you are looking forward to the long weekend!

I'm contacting you based on your alumni status designation in the DC Engineering speaker's bureau. As part of our Academic Affiliate membership with the Hume Center at Virginia Tech, we have the opportunity to **engage with a multi-disciplinary student research team** in the upcoming school year. **Before reaching out to a wider audience, I thought I'd start with VT alumni to see if there is interest.** The program specifics are as follows:

- Fall and spring semester, approximately **5 students** on a team devoting **8-10 hours a week** to the project
- **1 hour/week** check-ins with a Microsoft mentor (**or rotating mentors**) to share progress
- Virtual, with possible in-person colloquium at the end of the year
- Students will be juniors and seniors come from one of the following programs: Computer Engineering, Computational Modeling and Data Analytics, Computer Science, Mechanical Engineering, Aerospace Engineering, and some other engineering and science departments. NON-STEM students (National Security and Foreign Affairs, Political Science) also possible.
- They are open to just about anything we'd like the students to work on, but we **would need to articulate a project by July 20th** and provide:
 - Research title/topic and a brief description of the project
 - Name of mentor(s)/advisor(s) for research topic
 - Desired Academic background of student group members – They will do their best to align students and their research interests with ours.

For past projects, students researched and designed a Cube Satellite then used a 3D printer to actually create it. Another team developed a working codebase for use on internal projects. A few of the projects simply researched different aspects of a topic via literature review and different software packages. (See pg. 3 and 4 of the **attached document** for more and check out the other companies involved)

I will reach back out next week to see if there is interest, and feel free to forward this to other colleagues. Happy to chat through any questions next week as well.

Best,

Husna

Husna Ali-Khan(she/her)
Director, Community Engagement & Partnerships
M 215.828.7577 | husnaalikhan@microsoft.com

DC Engineering Enabled My Curiosity, and Built out a Privacy Research Project

noosa yoghurt 
Sponsored · 



New noosa Fruit Smoothies. With the perfect blend of real fruit and creamy yoghurt, they'r... See More

Awes-yum. [Learn More](#) **Awes-yum.**

   18

4 Comments 2 Shares 




This photo is from a post. [View post](#)







Sartaj Singh Dhani 
November 1, 2020 · 

So the question is how did I start to get Noosa yogurt advertisements? More importantly how did Facebook know that I like this product? I didn't provide Noosa with my email or phone number. I haven't clicked on anything to like Noosa or their advertisements. Supreet buys Noosa for me at Giant Food Store. We both haven't clicked or liked anything associated with Giant. So how did this sorcery and madness start?

See those three dots in the upper right hand corner? I clicked on that to learn why I'm getting this ad on Facebook. [See less](#)

[Edit](#)

 Like  Comment  Share

 Write a comment...     



HUME CENTER FOR NATIONAL
SECURITY AND TECHNOLOGY
VIRGINIA TECH.

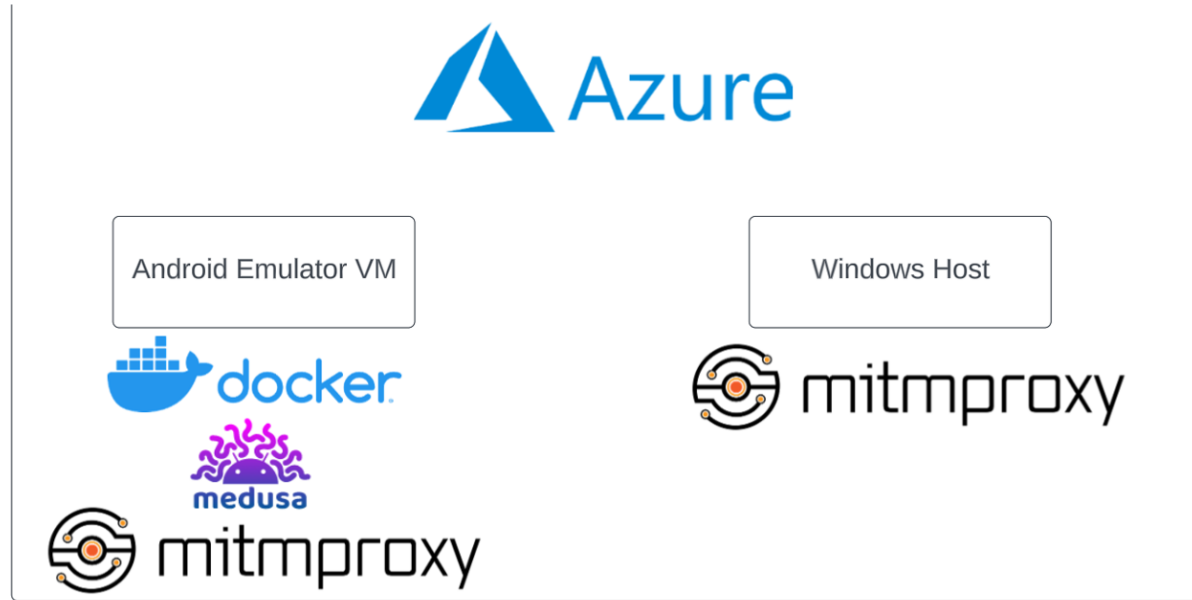
The National Security Risks of TikTok: A Comprehensive Assessment of Data Privacy and Collection

Cameron Alemand, Ian Rees, Kaitlyn Yoha, Benjamin Perry

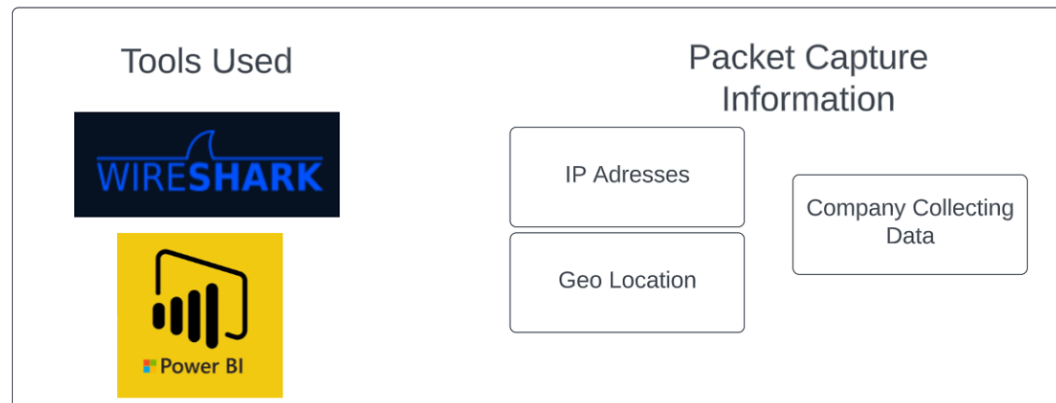
System Architecture



Data Capture →



↓ Data Processing



Creating The Virtual Machines



Microsoft Azure

Upgrade

Search resources, services, and docs (G+/)

Home >

Virtual machines

Virginia Tech (VirginiaTech.onmicrosoft.com)

+ Create ▾ ↺ Switch to classic ⌚ Reservations ▾ ⚙ Manage view ▾ ↻ Refresh ↓ Export to CSV 🔗 Open query | 🏷 Assign tags ▶ St...

Filter for any field...

Subscription equals all

Type equals all

Resource group equals all ✕

Location equals all ✕

+ Add filter

<input type="checkbox"/> Name ↑↓	Type ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/> mitmproxy	Virtual machine	Azure subscription 1	mitmproxy_group	East US
<input type="checkbox"/> mitmproxyASIA	Virtual machine	Azure subscription 1	mitmproxyASIA_group_11...	East Asia
<input type="checkbox"/> mitmproxyCANADA	Virtual machine	Azure subscription 1	mitmproxyCANADA_group	Canada Central
<input type="checkbox"/> mitmproxyUK	Virtual machine	Azure subscription 1	mitmproxyUK_group	UK South


```
azureuser@temp1: ~
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lauriekirk>ssh -L 5555:127.0.0.1:5555 azureuser@20.3.129.248
azureuser@20.3.129.248's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1031-azure aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Feb  1 22:22:59 UTC 2023

System load:  0.01          Processes:            212
Usage of /:   13.1% of 28.9GB Users logged in:          1
Memory usage: 13%          IPv4 address for docker0: 172.17.0.1
Swap usage:   0%           IPv4 address for eth0:   10.10.0.4

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how Microsoft
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

22 updates can be applied immediately.
19 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Wed Feb  1 21:52:00 2023 from 131.107.1.241
azureuser@temp1:~$
```


redroid11_arm64
10:30


Log in to TikTok

Manage your account, check notifications, comment on videos, and more.

 Use phone / email / username

 Continue with Facebook

 Continue with Google

 Continue with Twitter

By continuing, you agree to our [Terms of Service](#) and acknowledge that you have read our [Privacy Policy](#) to learn how we collect, use, and share your data.

Don't have an account? [Sign up](#)



Sartaj Singh Dhami

Laurie Kirk

Joe Mansour

Luis Fernandez (M...)

Perry, Benjamin

Ian Re...

Yoha, ...

Kevin

Path	Method	Status	Size	Time
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.6kb	17ms
https://bsync.us.tiktokv.com/v%2f2pipeline/device_id...	POST	200	1.1kb	48ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.7kb	18ms
http://example.com/	GET	200	648b	6ms
http://example.com/favicon.ico	GET	404	648b	3ms
http://0.0.0.0:8081/	GET	200	426b	5ms
http://0.0.0.0:8081/static/vendor.css	GET	200	25.7kb	7ms
http://0.0.0.0:8081/static/app.css	GET	200	4.7kb	52ms
http://0.0.0.0:8081/static/app.js	GET	200	196.6kb	53ms
http://0.0.0.0:8081/updates	WS	101	115.7mb	5min
http://0.0.0.0:8081/static/fonts/fontawesome-webfont...	GET	200	75.4kb	5ms
http://0.0.0.0:8081/state	GET	200	416b	18ms
http://0.0.0.0:8081/flows	GET	200	233.5kb	304ms
http://0.0.0.0:8081/events	GET	200	4.3kb	23ms
http://0.0.0.0:8081/static/images/favicon.ico	GET	200	356.6kb	25ms
http://0.0.0.0:8081/options	GET	200	4.5kb	29ms
http://0.0.0.0:8081/static/images/chrome-devtools/res...	GET	200	295b	11ms
http://0.0.0.0:8081/static/images/resourceimageicon.p...	GET	200	976b	12ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.6kb	26ms
https://webcast16-normal-useast5.us.tiktokv.com/ies/s...	GET	200	15b	146ms
https://api16-core-useast5.us.tiktokv.com/ies/speed/7a...	GET	200	11b	336ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	2.0kb	102ms
https://api16-normal-useast5.us.tiktokv.com/ies/speed...	GET	200	11b	151ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.8kb	39ms
https://gecko16-platform-useast5.us.tiktokv.com/geck...	POST	200	9.9kb	219ms
https://gecko16-platform-useast5.us.tiktokv.com/geck...	POST	200	9.9kb	45ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.8kb	42ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.1kb	47ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.1kb	60ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.4kb	60ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.7kb	76ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.5kb	78ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.6kb	123ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.7kb	91ms
https://log16-applog-useast5.us.tiktokv.com/service/2/...	POST	200	1.6kb	92ms

```

GET https://1f16-geckocdn.tiktokcdn-us.com/obj/ies-fe-gecko-tx/d137780efa02
9d788f448e10c7d6f951_rstd?iid=7215324383328732971&device_id=721532385482960
2358&ac=mobile&channel=googleplay&aid=1233&app_name=musical_ly&version_code
=280605&version_name=28.6.5&device_platform=android&ab_version=28.6.5&smix
=as&device_type=redroid11_arm64&device_brand=redroid&language=en&os_api=30&
x-vc-bdturing-sdk-version 2.2.1.i18n
x-tt-trace-id 00-740b277c464316-d14-05462-110421-240b277c464316-01

```

```

user-agent com.zhiliaoapp.musically/2022806050 (Linux; U; Android 11; en_US;
redroid11_arm64; Build/RD2A.211001.002; Cronet/T1NetVersion:d23bd114 2023-01-
13 QuicVersion:5f23035d 2022-11-23)
accept-encoding gzip, deflate, br

```

```

x-
argus: HpxURJv6VgtExFHUn2weseRuSHPqiPsz1004iNET3QYSR85+hOEQFggGVMxSSN6zhgk
kRtcd8N/Ccu2BzLC2RwHvsJshuTkmXvp+icFjkNqzmbuJ7qg+Exc80vD/6Aizjb/QxLDLxZuw
Z+uE0+5FRXcPqLnYSYvvp5/kGfYsQuicDD0YvPJTQVcY3/Vicv68zhM8TCJIDH3bMIU/c9kVa
x-gorgon: 840430bd0000669457b006eb6554c5b5e5d2f7d4dda744d0adda
x-khronos: 1679950577
x-ladon: c91xEPSprfghQ2tY4uPi4fXrKNjTYAskL7yoxRpFnSscg1z

```

```

Query
id: 7215324383328732971
device_id: 7215323854829602350
ac: mobile
channel: googleplay
aid: 1233
app_name: musical_ly
version_code: 280605
version_name: 28.6.5
device_platform: android
ab_version: 28.6.5
ssmix: a
device_type: redroid11_arm64
device_brand: redroid
language: en
os_api: 30
os_version: 11
openudid: d601a4b559a62b7b
manifest_version_code: 2022806050
resolution: 720*1184
dpi: 320
update_version_code: 2022806050
_rticket: 1679950577899
current_region: US
app_type: normal
sys_region: US
timezone_name: GMT
residence: US
app_language: en
ac2: unknown
uoo: 1
op_region: US
timezone_offset: 0
build_number: 28.6.5
host_abi: arm64-v8a
locale: en

```

```

chain POSTROUTING (policy ACCEPT)
target prot opt source destination
completedProcess(args='adb -s 127.0.0.1:5555 shell iptables -t nat -L', returncode=0)
argo> exit
checking the working directory for leftovers...
all good!
bye !!
mitproxy@mitproxyV2:~/medusa-0.1.0$ wget -e https_proxy=127.0.0.1:8080 --ca-certificate ~/mitproxy/mitproxy-ca-cer
get: missing URL
usage: wget [OPTION]... [URL]...

try 'wget --help' for more options.
mitproxy@mitproxyV2:~/medusa-0.1.0$ wget -e https_proxy=127.0.0.1:8080 --ca-certificate ~/mitproxy/mitproxy-ca-cer
2023-03-27 20:59:49~ https://example.com/
connecting to 127.0.0.1:8080... connected.
ERROR: cannot verify example.com's certificate, issued by 'O=mitproxy,O=mitproxy':
Unable to locally verify the issuer's authority.
To connect to example.com insecurely, use '--no-check-certificate'.
mitproxy@mitproxyV2:~/medusa-0.1.0$ wget -e https_proxy=127.0.0.1:8080 --ca-certificate ~/mitproxy/mitproxy-ca-cer
2023-03-27 21:00:24~ https://example.com/
connecting to 127.0.0.1:8080... connected.
ERROR: cannot verify example.com's certificate, issued by 'O=mitproxy,O=mitproxy':
Unable to locally verify the issuer's authority.
To connect to example.com insecurely, use '--no-check-certificate'.
mitproxy@mitproxyV2:~/medusa-0.1.0$

```

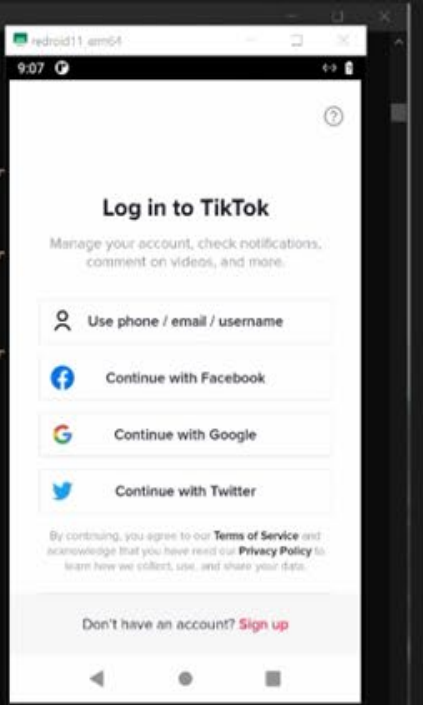
```

Select mitproxy@mitproxyV2:
** System restart required ***
Last login: Mon Mar 27 19:55:30 2023 from 73.171.42.239
mitproxy@mitproxyV2:~$ adb devices
List of devices attached
07.0.0.1:5555 device

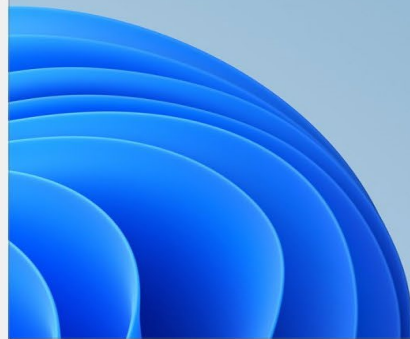
mitproxy@mitproxyV2:~$ docker run --rm -it --net-host mitproxy/mitproxy mitweb --web-host 0.0.0.0
docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Post "http://x2Fvar%2Frun%2Fdocker.sock/v1.24/containers/create": dial unix /var/run/docker.sock: connect: permission denied.
See 'docker run --help'.

mitproxy@mitproxyV2:~$ sudo docker run --rm -it --net-host mitproxy/mitproxy mitweb --web-host 0.0.0.0
[sudo] password for mitproxy:
00:46:37.112] HTTP(S) proxy listening at *:8080.
00:46:37.113] Web server listening at http://0.0.0.0:8081/
00:46:37.969] No web browser found. Please open a browser and point it to http://0.0.0.0:8081/
00:50:55.441] [172.17.0.2:42296] client connect
00:50:55.444] [172.17.0.2:42312] client connect
00:50:55.445] [172.17.0.2:42318] client connect
00:50:55.826] [172.17.0.2:42312] server connect api16-normal-useast5.us.tiktokv.com:443 (23.222.12.16:443)
00:50:55.864] [172.17.0.2:42296] server connect api16-core-useast5.us.tiktokv.com:443 (23.45.233.26:443)
00:50:55.710] [172.17.0.2:42318] server connect webcast16-normal-useast5.us.tiktokv.com:443 (184.25.127.142:443)

```




```
Administrator: Command Prompt - BruteSharkCli.exe --input-dir privacy-project\tiktok\tiktok-capture\pcap --output temp --modules DNS
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.170.210
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.179.143
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.178.102
Found: DNS Mapping: pull-hls-f77-va01.tiktokcdn.com -> 1928505594.rsc.cdn77.org
Found: DNS Mapping: pull-hls-f77-va01.tiktokcdn.com -> 143.244.58.93
Found: DNS Mapping: pull-f5-tt01.tiktokcdn.com -> 209.177.91.122
Found: DNS Mapping: pull-f5-tt01.tiktokcdn.com -> 209.177.91.102
Found: DNS Mapping: pull-f5-tt01.tiktokcdn.com -> 23.251.117.117
Found: DNS Mapping: pull-flv-l77-va01.tiktokcdn.com -> 1394501235.rsc.cdn77.org
Found: DNS Mapping: pull-flv-l77-va01.tiktokcdn.com -> 37.19.206.98
Found: DNS Mapping: pull-cmaf-l16-sg01.tiktokcdn.com -> pull-cmaf-l16-sg01.tiktokcdn.com.akamaized.net
Found: DNS Mapping: pull-cmaf-l16-sg01.tiktokcdn.com -> a1736.z.akamai.net
Found: DNS Mapping: pull-cmaf-l16-sg01.tiktokcdn.com -> 23.60.159.208
Found: DNS Mapping: pull-cmaf-l16-sg01.tiktokcdn.com -> 23.60.159.185
Found: DNS Mapping: pull-w5-va01.tiktokcdn.com -> pull-w5-va01.tiktokcdn.com.c.worldfcdn.com
Found: DNS Mapping: pull-w5-va01.tiktokcdn.com -> pull-oversea-total.s.worldfcdn.com
Found: DNS Mapping: pull-w5-va01.tiktokcdn.com -> pull-fcdn-overseae2.s.worldfcdn.com
Found: DNS Mapping: pull-w5-va01.tiktokcdn.com -> 107.151.171.147
Found: DNS Mapping: pull-cmaf-f16-sg01.tiktokcdn.com -> pull-cmaf-f16-sg01.tiktokcdn.com.akamaized.net
Found: DNS Mapping: pull-cmaf-f16-sg01.tiktokcdn.com -> a1857.z.akamai.net
Found: DNS Mapping: pull-cmaf-f16-sg01.tiktokcdn.com -> 23.60.159.137
Found: DNS Mapping: pull-cmaf-f16-sg01.tiktokcdn.com -> 23.60.159.169
Found: DNS Mapping: pull-f5-tt02-infra.fcdn.us.tiktokv.com -> pull-f5-tt02-infra.fcdn.us.tiktokv.com.c.worldfcdn2.com
Found: DNS Mapping: pull-f5-tt02-infra.fcdn.us.tiktokv.com -> pull-f5-tt02-infra.fcdn.us.gts.ttoverseaus.net
Found: DNS Mapping: pull-f5-tt02-infra.fcdn.us.tiktokv.com -> 147.160.181.32
Found: DNS Mapping: pull-flv-f77-tt02.fcdn.us.tiktokv.com -> 1561539925.rsc.cdn77.org
Found: DNS Mapping: pull-flv-f77-tt02.fcdn.us.tiktokv.com -> 37.19.206.98
Found: DNS Mapping: pull-cmaf-f16-tt01.tiktokcdn.com -> pull-cmaf-f16-tt01.tiktokcdn.com.akamaized.net
Found: DNS Mapping: pull-cmaf-f16-tt01.tiktokcdn.com -> a507.z.akamai.net
Found: DNS Mapping: pull-cmaf-f16-tt01.tiktokcdn.com -> 23.60.159.195
Found: DNS Mapping: pull-cmaf-f16-tt01.tiktokcdn.com -> 23.60.159.186
Found: DNS Mapping: push-rtmp-f5-tt01.fcdn.us.tiktokv.com -> push-rtmp-f5-tt01.fcdn.us.tiktokv.com.c.worldfcdn2.com
Found: DNS Mapping: push-rtmp-f5-tt01.fcdn.us.tiktokv.com -> push-rtmp-f5-tt01.tiktokcdn.com.c.bytetcdn.com
Found: DNS Mapping: push-rtmp-f5-tt01.fcdn.us.tiktokv.com -> push-fcdn-self-oversea.s.bytetcdn.com
Found: DNS Mapping: push-rtmp-f5-tt01.fcdn.us.tiktokv.com -> 172.96.112.195
Found: DNS Mapping: push-rtmp-f5-tt01.fcdn.us.tiktokv.com -> 23.251.115.8
Found: DNS Mapping: push-rtmp-f5-tt01.fcdn.us.tiktokv.com -> 23.251.115.6
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> pull-flv-l16-tt01.tiktokcdn-us.com.atomile.com
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 138.113.19.16
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 138.113.158.123
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.169.229
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.156.117
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.158.194
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 138.113.159.11
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 138.113.158.121
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.145.81
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.178.214
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.180.20
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.170.210
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.179.143
Found: DNS Mapping: pull-flv-l16-tt01.tiktokcdn-us.com -> 157.185.178.102
Found: DNS Mapping: pull-hls-f77-va01.tiktokcdn.com -> 1928505594.rsc.cdn77.org
Found: DNS Mapping: pull-hls-f77-va01.tiktokcdn.com -> 143.244.58.93
Found: DNS Mapping: pull-cmaf-l10-sg01.tiktokcdn.com -> pull-cmaf-l10-sg01.tiktokcdn.com.rocket-cdn.com
Found: DNS Mapping: pull-cmaf-l10-sg01.tiktokcdn.com -> hcdnl.pulldyin.ovc.gslb.rocket-cdn.com
Found: DNS Mapping: pull-cmaf-l10-sg01.tiktokcdn.com -> 156.59.151.145
Found: DNS Mapping: pull-cmaf-l10-sg01.tiktokcdn.com -> 156.59.151.17
Found: DNS Mapping: pull-cmaf-l10-sg01.tiktokcdn.com -> 156.59.151.16
```



File Explorer window showing the contents of the 'tiktok-capture\pcap' directory. The table lists files with their modification dates, types, and sizes.

date modified	Type	Size
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,766 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,766 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,766 KB
1/10/2023 4:29 AM	Wireshark capture...	9,768 KB
1/10/2023 4:29 AM	Wireshark capture...	9,766 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB
1/10/2023 4:29 AM	Wireshark capture...	9,766 KB
1/10/2023 4:29 AM	Wireshark capture...	9,767 KB


```

"142.251.40.138","Warren Township","United States","Google LLC"
"142.251.40.170","Warren Township","United States","Google LLC"
"142.251.40.202","Warren Township","United States","Google LLC"
"142.251.40.206","Warren Township","United States","Google LLC"
"142.251.40.234","Warren Township","United States","Google LLC"
"142.251.41.10","Warren Township","United States","Google LLC"
"143.244.58.93","Prague","Czechia","Datacamp Limited"
"185.152.65.76","Prague","Czechia","Datacamp Limited"
"146.75.38.73","Reston","United States","Fastly Inc"
"147.160.177.32","Palo Alto","United States","Bytedance Inc."
"147.160.177.37","Palo Alto","United States","Bytedance Inc."
"147.160.177.42","Palo Alto","United States","Bytedance Inc."
"147.160.178.32","Portland","United States","Bytedance Inc."
"147.160.178.35","Portland","United States","Bytedance Inc."
"147.160.178.36","Portland","United States","Bytedance Inc."
"147.160.178.39","Portland","United States","Bytedance Inc."
"147.160.179.32","Chicago","United States","Bytedance Inc."
"147.160.179.35","Chicago","United States","Bytedance Inc."
"147.160.179.37","Chicago","United States","Bytedance Inc."
"147.160.180.32","Johnstown","United States","Bytedance Inc"
"147.160.180.42","Johnstown","United States","Bytedance Inc"
"147.160.180.43","Johnstown","United States","Bytedance Inc"
"147.160.180.45","Johnstown","United States","Bytedance Inc"
"147.160.181.32","New York","United States","Bytedance Inc."
"147.160.181.33","New York","United States","Bytedance Inc."
"147.160.181.34","New York","United States","Bytedance Inc."
"147.160.181.35","New York","United States","Bytedance Inc."
"147.160.181.36","New York","United States","Bytedance Inc."
"147.160.181.37","New York","United States","Bytedance Inc."
"147.160.181.65","New York","United States","Bytedance Inc."
"147.160.182.32","Johnstown","United States","Bytedance Inc."
"147.160.182.36","Johnstown","United States","Bytedance Inc."
"147.160.182.41","Johnstown","United States","Bytedance Inc."
"147.160.182.42","Johnstown","United States","Bytedance Inc."
"185.152.65.38","Prague","Czechia","Datacamp Limited"
"195.181.163.74","Miami","United States","Datacamp Limited"
"156.59.151.144","Singapore","Singapore","Zenlayer Inc"
"156.59.151.145","Singapore","Singapore","Zenlayer Inc"
"156.59.151.16","Singapore","Singapore","Zenlayer Inc"
"156.59.151.17","Singapore","Singapore","Zenlayer Inc"
"143.244.60.108","Chicago","United States","DataCamp Limited"
"157.185.145.81","Portland","United States","Quantil Networks Inc"
"157.185.156.117","San Jose","United States","Quantil Networks Inc"
"157.185.156.120","San Jose","United States","Quantil Networks Inc"
"157.185.158.171","Miami","United States","Quantil Networks Inc"
"157.185.158.192","Miami","United States","Quantil Networks Inc"
"157.185.158.194","Miami","United States","Quantil Networks Inc"
"157.185.158.195","Miami","United States","Quantil Networks Inc"
"157.185.163.159","Monrovia","United States","Quantil Networks Inc"
"157.185.163.161","Monrovia","United States","Quantil Networks Inc"
"157.185.163.96","Monrovia","United States","Quantil Networks Inc"
"157.185.163.98","Monrovia","United States","Quantil Networks Inc"
"157.185.169.224","Monrovia","United States","Quantil Networks Inc"
"157.185.169.229","Monrovia","United States","Quantil Networks Inc"
"157.185.169.230","Monrovia","United States","Quantil Networks Inc"

```

File Home Insert Modeling View Help Format Data / Drill

Paste Cut Copy Format painter Clipboard

Get data Excel workbook Data hub SQL Server Enter data Datasource Recent sources

Transform data Refresh data Queries

New visual Text box More visuals Insert

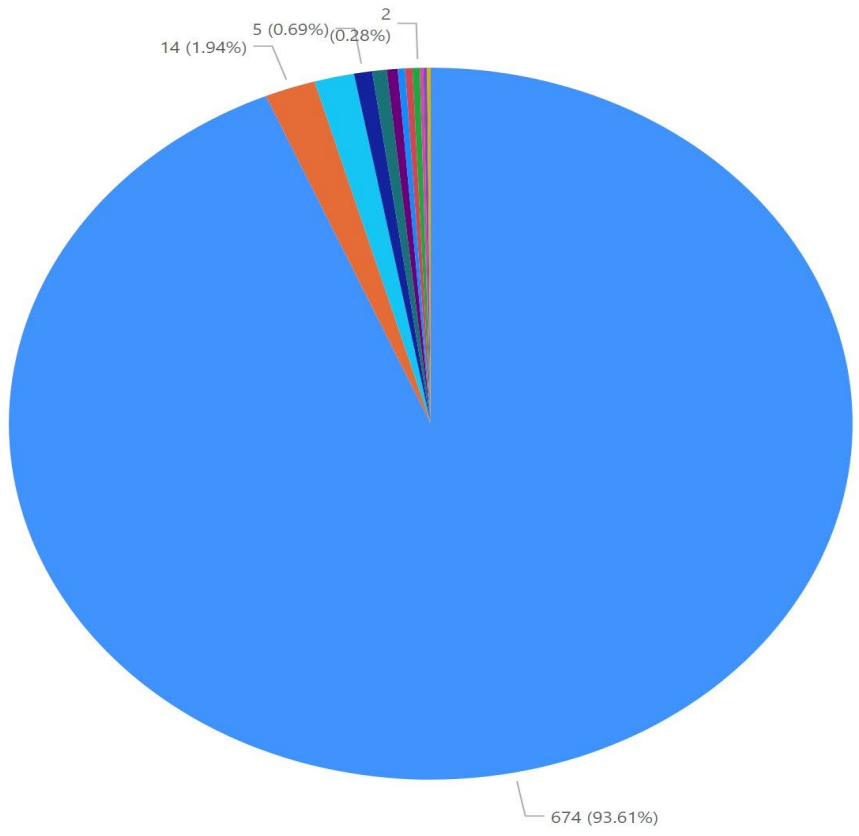
New measure Quick measure Calculations

Sensitivity Sensitivity

Publish Share

Back to report

COUNT OF COUNTRY BY COUNTRY



- Country**
- United States
 - Czechia
 - Singapore
 - Canada
 - Mexico
 - France
 - Luxembourg
 - Philippines
 - Germany
 - Ireland
 - Japan

Filters

Search

Filters on this visual

- Count of Country is (All)
- Country is (All)

Add data fields here

Filters on this page

Add data fields here

Filters on all pages

Add data fields here

Visualizations

Build visual

Legend

Country

Values

Count of Country

Details

Add data fields here

Tooltips

Add data fields here

Drill through

Cross-report Off

Keep all filters On

Add drill-through fields here

Fields

Search

IP_GeoLocation

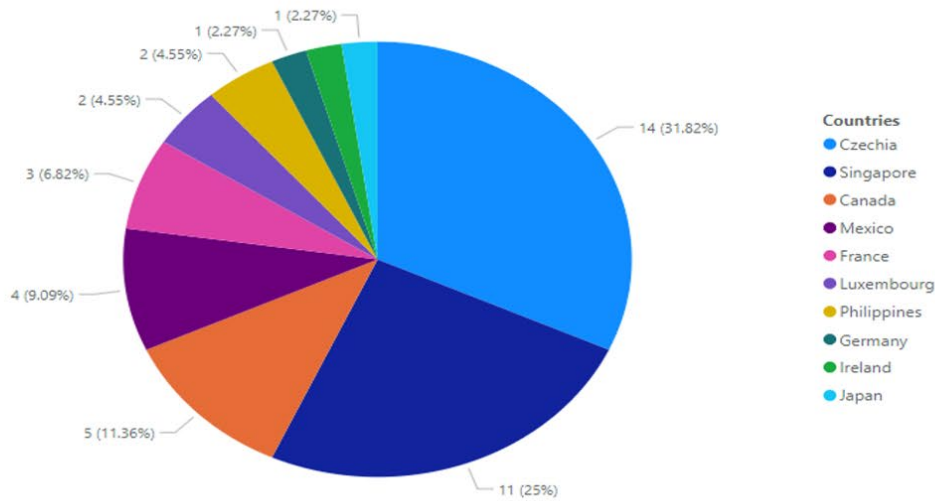
- City
- Country
- IP
- Isp

IP Connections Going Abroad

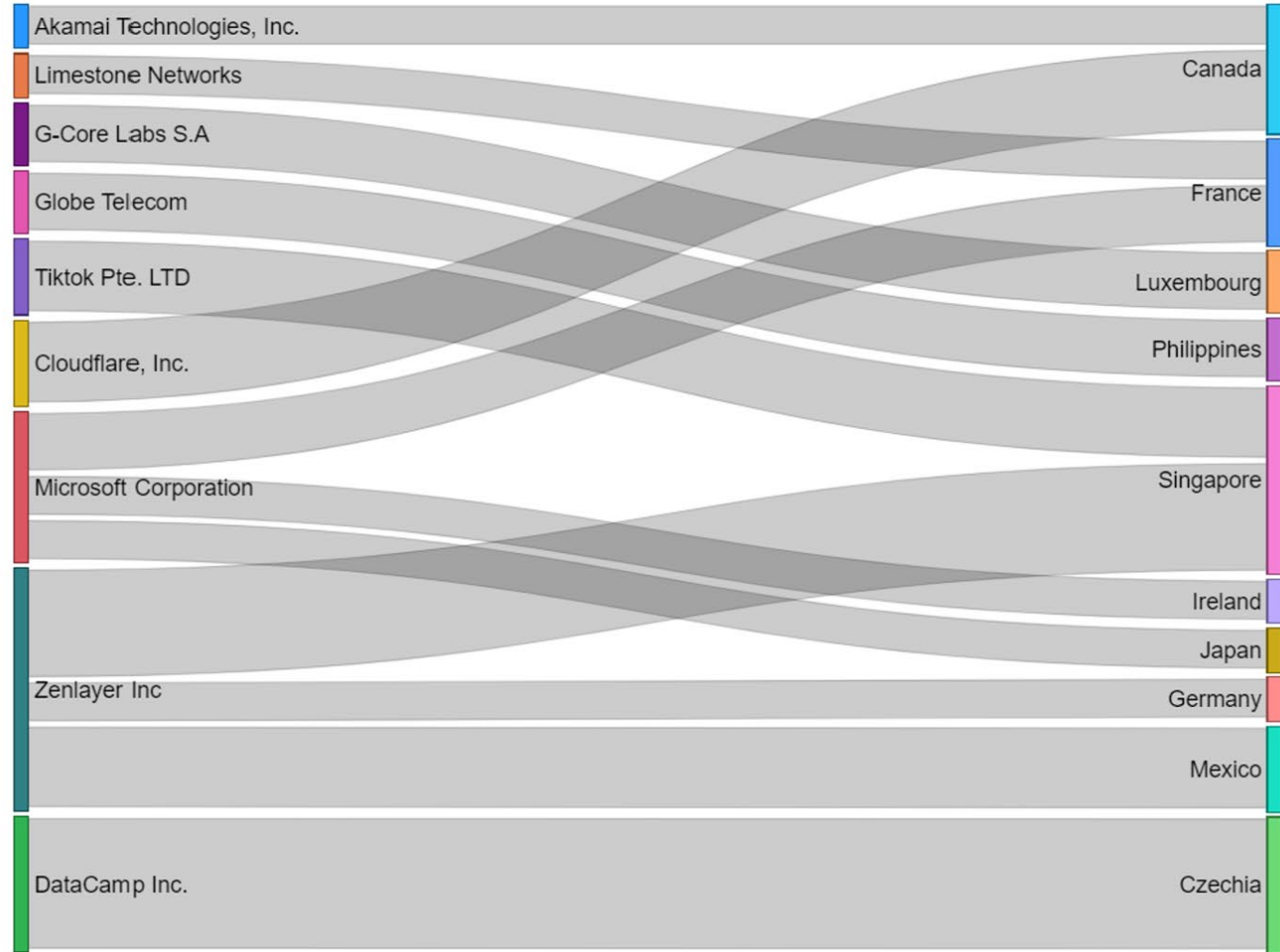


- 45 total foreign IP connections
- 10 foreign countries
- IPs registered to 17 publicly listed corporations – and a few unlisted
- 10 foreign countries

Number of Foreign Country Connections



Scale of IP Connections Associated by Company to each Country



Flipper Zero: Microsoft Project-Based Learning Program

Apply by March 22, 2024

CCI is partnering with Microsoft in a Project-Based Learning Program for an experiential learning experience involving the **Flipper Zero, a portable multi-tool device**. The project will run from June 3 to Aug. 2, 2024.



APPLY TO THE FLIPPER ZERO PROGRAM

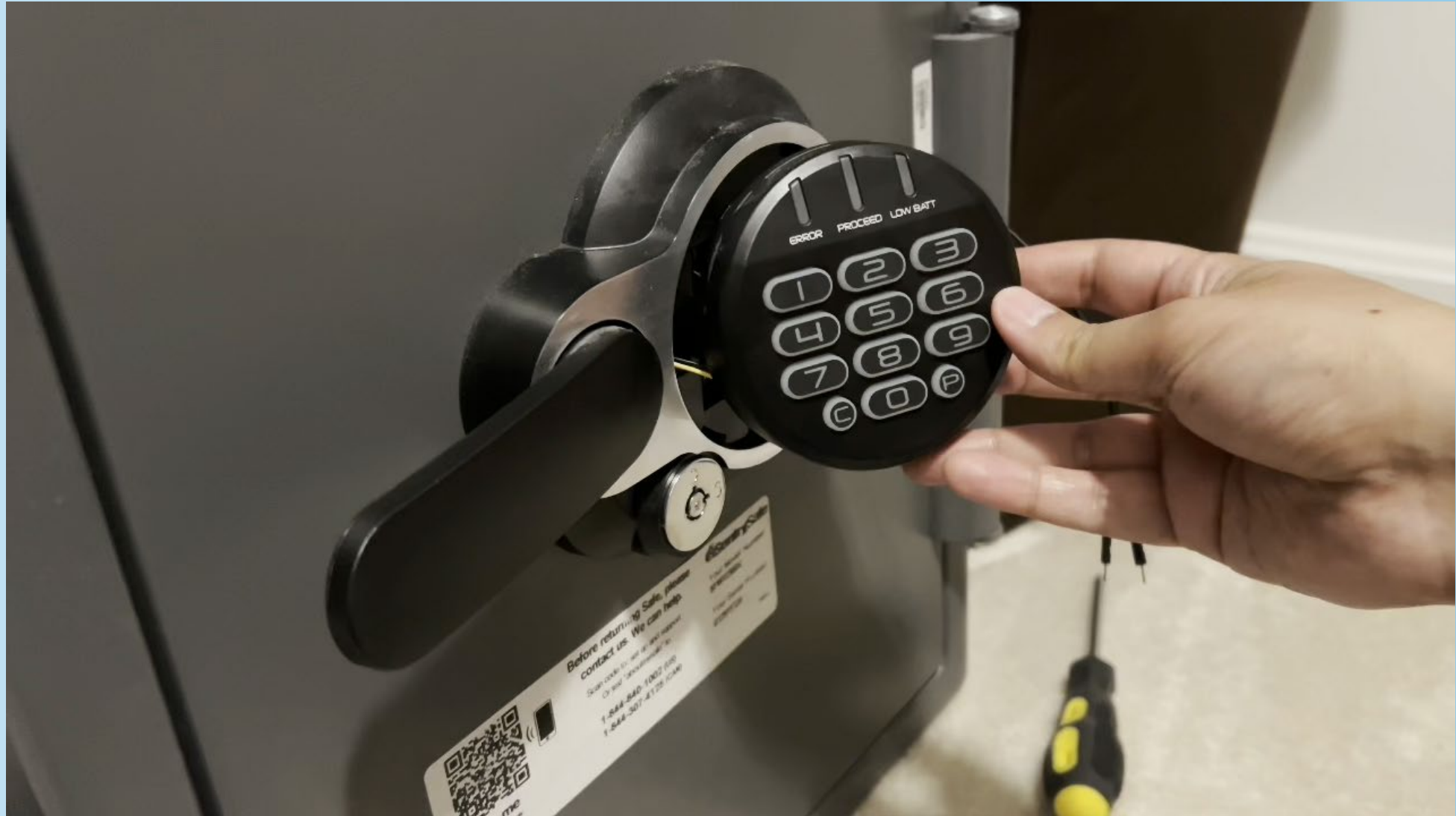
LLM from Telemetry?

- Get Clearance Ready
- Project-Based Learning Program
- Internship & Job Fair 2023
- CCI Education and Experiential Learning Programs
- Partnership with CACI
- Cybersecurity Education in Virginia
- Virginia's Centers of Academic Excellence

Bluetooth Low Energy Attack



SentrySafe Physical Attack



Our Microsoft Flipper Zero Mentors



Joe Mansour
Sr. Security Researcher

Reston



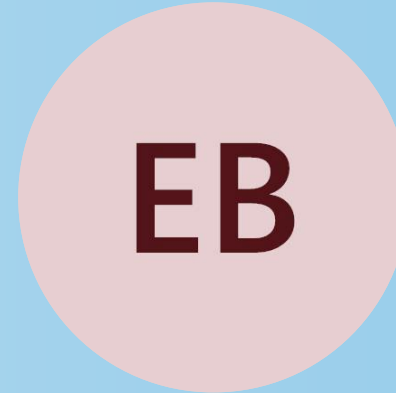
Scott Gee
Sr. Security Incident
Responder

Reston



Sartaj Singh Dhani
Sr. Security Investigator

Reston



Ed Bolton
Sr. Security Detection
Engineer

Reston



Luis Fernandez
Security Investigator II

Redmond

Participant avatars and names:

- FX: Xu, Frederi...
- JW: Jackson Wa...
- Joe Mansour
- Sajan Ronv...
- DS: Danyaal Shaoza...
- EA: Ethan Agye...
- SG: Scott Gee

Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. Learn more

Meeting chat

Xu, Frederick (External) Monday 5:01 PM

yeah i can access the CLI on windows I don't think the current version supports the BLE spam attack logs though unfortunately

Monday 5:01 PM

[Command-line interface - Flipper Zero - Documentation](#)

Learn how to access... docs.flipper.net

1

Zhong, Christopher (External) Monday 5:15 PM

<https://ieeexplore.ieee.org/document/10041465>

2

<https://arxiv.org/>

Chris Gaal Monday 5:29 PM

need to drop for another call. Great work all!

3

Monday 5:31 PM

oof. forgot i have another

Type a message

Reaction icons: Copy, Smile, Link, Pin, Plus, Send

LibreOffice Impress presentation slide:

Slide 4 of 7

11.38 / 1.68 0.00 x 0.00 English (USA) 140%



Home > storageflipper Storage account

Upload Open in Explorer Delete Move Refresh Open in mobile CLI / PS Feedback

Essentials

Resource group (move)	: rg-flipper	Performance	: Standard
Location	: eastus	Replication	: Locally-redundant storage (LRS)
Subscription (move)	: JWalker Flipper Project	Account kind	: StorageV2 (general purpose v2)
Subscription ID	: da56d0a8-9811-4ce9-a9ff-df3f97b829f1	Provisioning state	: Succeeded
Disk state	: Available	Created	: 6/29/2024, 12:50:13 AM

Tags (edit) : Add tags

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Key metrics

See all metrics

Show data for last: 1 day Show data for: Account

Total egress

Total ingress

Average latency

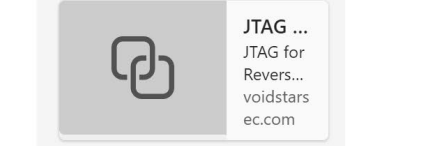
Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. Learn more

Meeting chat

2

Joe Mansour 4:42 PM

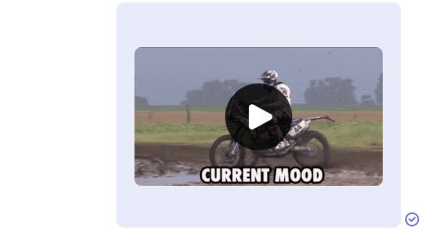
JTAG Hacking with a Raspberry Pi - Introducing the PiFex (voidstarsec.com)



Danyaal you could also start very small and say you want to implement an IDCODE scan and then move on to other more complicated JTAG features

and enumeration

4:48 PM



Xu, Frederick (External) 4:49 PM

wow

Type a message

Participant avatars: FX (Xu, Frederick), CZ (Zhong, Christopher), Luis Fernandez (M365), PT (TUNISON, PATRICK), and another participant.

Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. Learn more

Meeting chat

Xu, Frederick (External)

Last read

Danyaal Shaozab (External) 5:00 PM

DS Xu, Frederick, you can connect to the Flipper CLI pretty easily, it's in /dev as ttyACM0 (Linux, not sure for Windows), and you can run: screen /dev/ttyACM0



Just make sure you are in the 'dialout' group

Xu, Frederick (External) 5:01 PM

FX yeah I can access the CLI on windows I don't think the current version supports the BLE spam attack logs though unfortunately

5:01 PM

[Command-line interface - Flipper Zero - Documentation](#)



Type a message

Exposed IoT Access Points

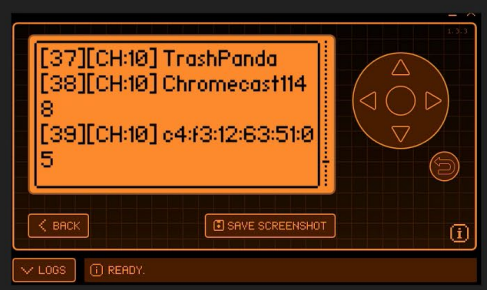
MY NETWORKS

- FlipperTesting

OTHER NETWORKS

- [dishwasher]_E30A-JT9003326Y
- TrashPanda
- Other...

Samsung Dishwasher



Chromecast

88:57:1D:E9:60:35 Samsung-Range.Ian (192.168.1.162) -69/-95 dBm 11.0 Mbit/s, 20 MHz 43.3 Mbit/s, 20 MHz, MCS 4, Short GI

Oven

Good targets

Meeting participants:

- FX** Xu, Frederick (External)
- DS** Danyaal Shaozab (External)
- Luis Fernandez** (M365)
- PT** TUNISON, PATRICK (External)

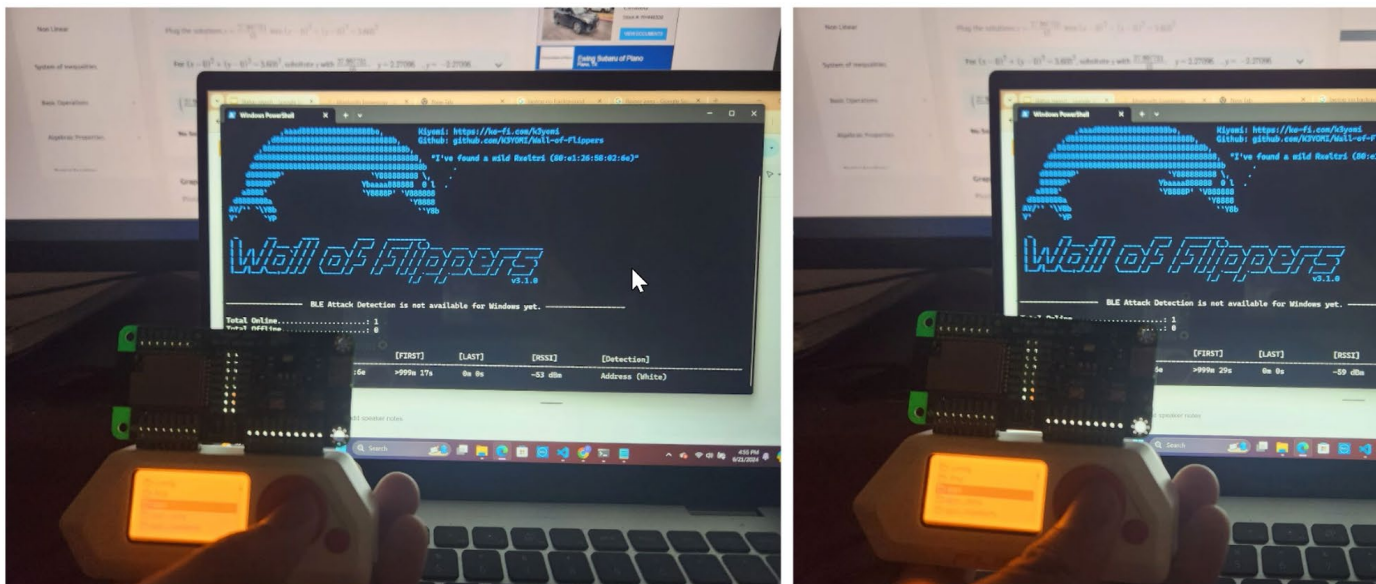
Some Unmute (Ctrl+Shift+M) ide your org. It's possible they have message-related policies that will apply to the chat. Learn more

Meeting chat

- Jackson Walker (External) Monday 5:35 PM
 - JW Yes I am available on August 5th
- Joe Mansour Monday 5:36 PM
 - I'll be at Blackhat that week but I will definitely check out the recording 😊
 - 👍 4
- Monday 5:38 PM Meeting ended: 1h 13m 4s
 - Open in Loop workspace
 - Attendance
- Today
- 4:23 PM Meeting started
- Last read
- Zhong, Christopher (External) 4:33 PM
 - CZ RIP
 - 👍 4
- 4:36 PM
 - please limit your update talks to eight minutes. this will allow for two minutes of questions/discussion/guidance.
 - 👍 4

Drawback 1

- RSSI is not accurate at >1 meter
- Oscillation is too high
- "Kalman Filter" or "Particle Filter"
- Walls do in fact make the flipper BLE suck



Type a message

🔗 😊 🗨️ 📌 + ➤

What About You?



DC Engineering

Missions that matter

