Multiyear Surveillance Campaigns Discovered Targeting Uyghurs

blog.lookout.com/multiyear-surveillance-campaigns-discovered-targeting-uyghurs

The Lookout Threat Intelligence team has discovered four Android surveillanceware tools, which we named SilkBean, DoubleAgent, CarbonSteal, and GoldenEagle. These four interconnected malware tools are elements of much larger mAPT (mobile advanced persistent threat) campaigns originating in China, and primarily targeting the Uyghur ethnic minority. Activity of these surveillance campaigns has been observed as far back as 2013. 1

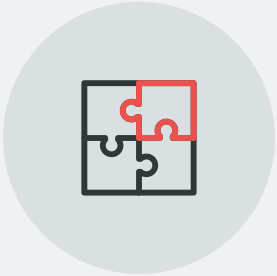
The primary aim of these apps is to gather and exfiltrate personal user data to attacker-operated command-and-control servers. Each malware tool has its own unique data gathering priorities and techniques, as detailed in our full report. Many samples of these malware tools were trojanized legitimate apps, i.e., the malware maintained complete functionality of the applications they were impersonating in addition to its hidden malicious capabilities.

Lookout has found evidence that the malware predominantly targeted Uyghurs, but also, to a lesser extent, Tibetans. These two groups are reportedly the main focus of China's "counter-terrorism" activity. 2 Titles and in-app functionality of samples, such as "Sarkuy" (Uyghur music service), "TIBBIYJAWHAR" (Uyghur pharmaceutical app) and "Tawarim" (Uyghur e-commerce site) show that the majority of this activity focused on Uyghurs.

SilkBean

Targeted focus on Turkic minority ethnic group, referencing Uyghur-relevant sites

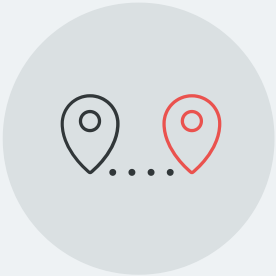
Trojanized apps for Uyghur/Arabic focused keyboards, alphabets, and plugins



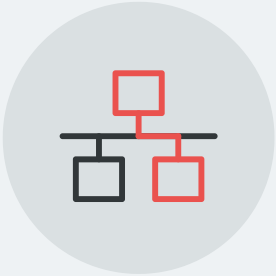
C2 connections with group also using DarthPusher, HenBox, PluginPhantom, and DoubleAgent

DoubleAgent

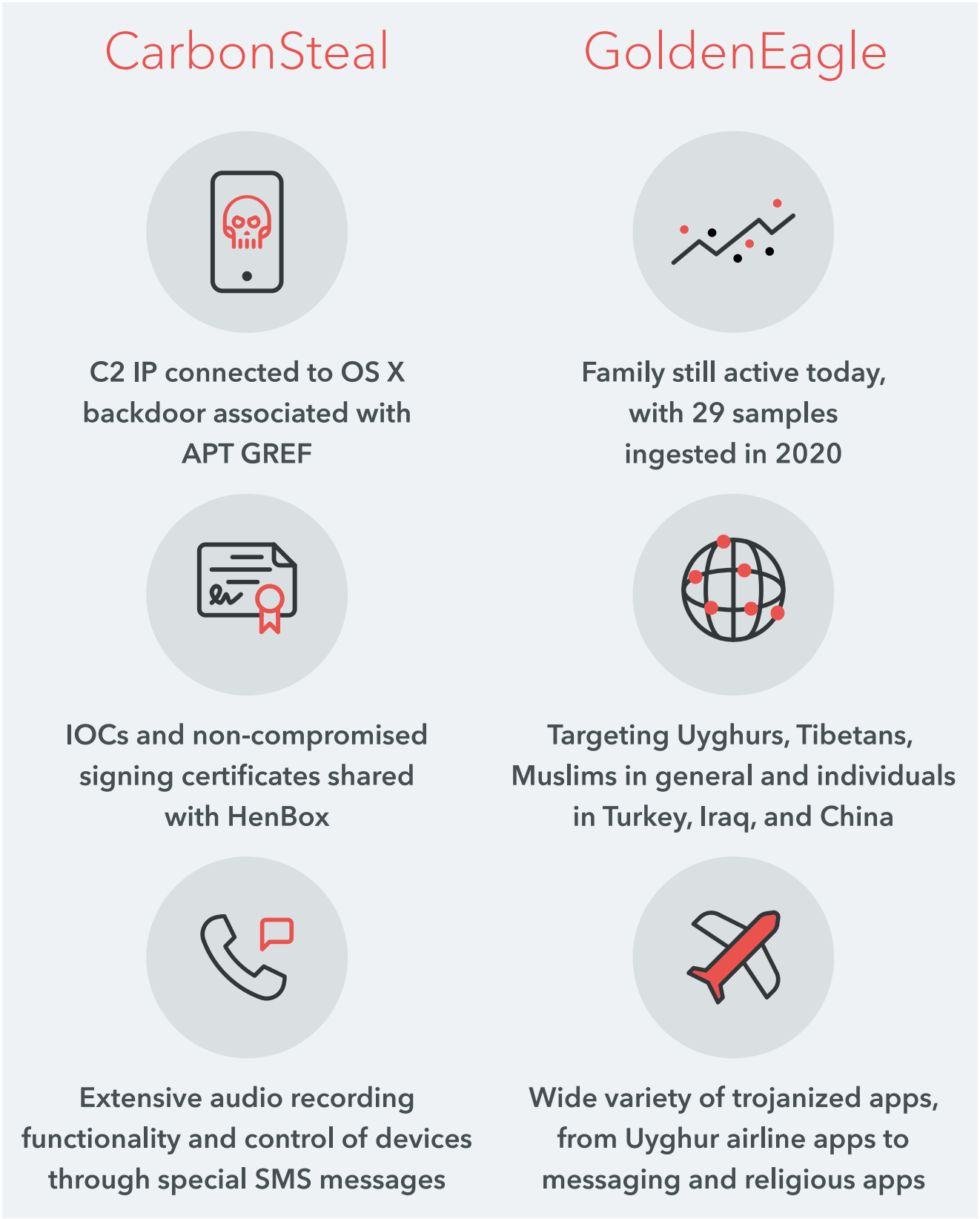
Trojanized Voxer, TalkBox, and Amaq News (official Daesh news app)



Initially targeting Tibetan community, then pivot to Uygur focus



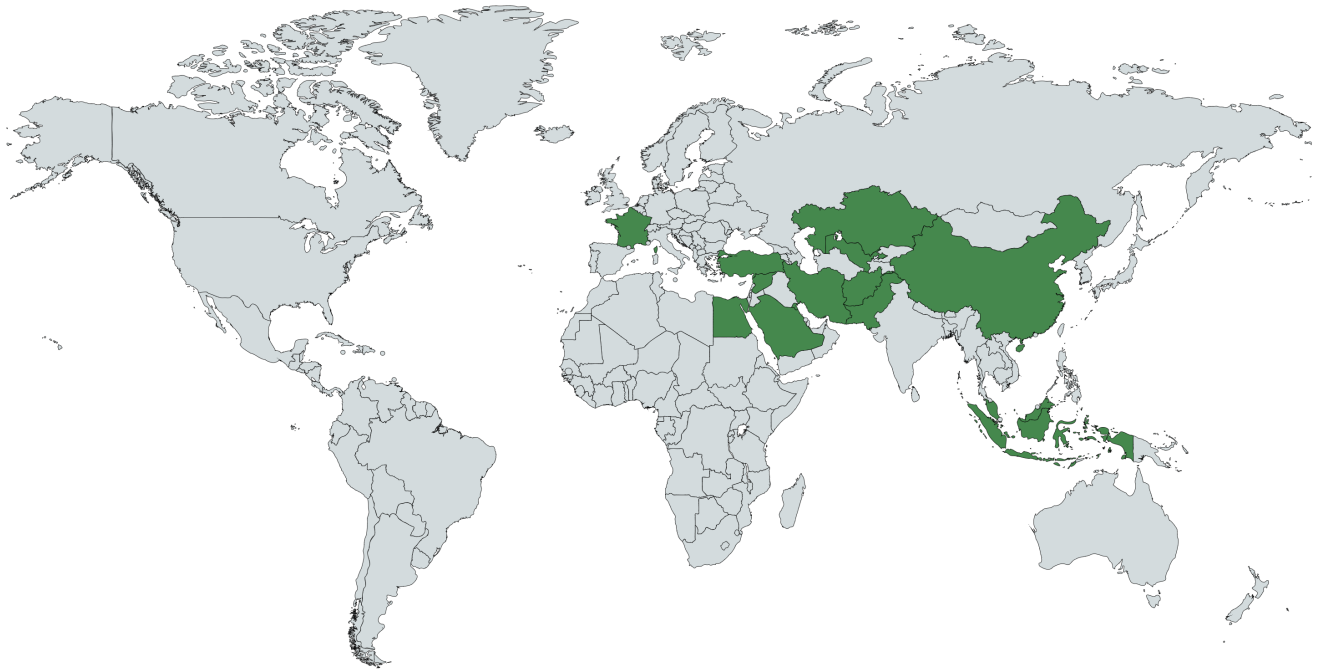
Overlap between DoubleAgent and SilkBean C2s when both families are active



The Chinese government's "Strike Hard Campaign against Violent Terrorism" (严厉打击暴力恐怖活动专项行动),which launched in mid-2014, led to the creation of the National Security Strategic Guidelines, the National Security Law and the Counterterrorism Law in 20153. We noticed that there was a dramatic increase in the number of samples we observed after these directives and initiatives were enacted.

As described in our report, the past activity of this mAPT is connected to previously reported desktop APT activity in China4, which is linked to GREF, a China-based threat actor also known as APT15, Ke3chang, Mirage, Vixen Panda and Playful Dragon.

We noticed that campaigns by this mAPT are also active outside of China, based on the languages and services targeted by the malware samples. For example, titles such as “Turkey Navigation”, “A2Z Kuwait FM Radio”, ” اخبار سوريا” (“Syria(n) News”) may suggest targets in Turkey, Kuwait and Syria respectively. Our research found that at least 14 different countries may be affected by the campaigns. 12 of these are on the Chinese government’s official list of “26 Sensitive Countries,” which according to public reporting5, are used by authorities as targeting criteria.



There are at least four other Android tools in the same mAPT actor’s mobile surveillance arsenal. They are publicly known as HenBox 6, PluginPhantom 7, Spywaller 8, and DarthPusher 9, which have been previously observed targeting Chinese-speaking individuals and those of the Uyghur ethnic minority.

The surveillance apps of these campaigns were likely distributed through a combination of targeted phishing and fake third-party app stores. They are not available on Google Play. Users of the Lookout mobile security products are protected from these threats.

1. https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/
2. https://www.ohchr.org/Documents/Issues/Terrorism/SR/OL_CHN_18_2019.pdf
3. https://www.uscc.gov/sites/default/files/Research/Chinas-Response-to-Terrorism-CNA061616.pdf
4. https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

5. https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs
6. https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/
7. https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/
8. https://blog.lookout.com/spywaller-mobile-threat
9. https://thehackernews.com/2015/03/Xiaomi-Mi-4-malware.html

Lookout Threat Advisory customers are given regular updates and analyses on threat research such as this one. Visit our Threat Advisory Services page to find out more.

The Lookout Threat Intelligence team has discovered four Android surveillanceware tools, which we named SilkBean, DoubleAgent, CarbonSteal, and GoldenEagle. These four interconnected malware tools are elements of much larger mAPT (mobile advanced persistent threat) campaigns originating in China, and primarily targeting the Uyghur ethnic minority. Activity of these surveillance campaigns has been observed as far back as 2013. 1

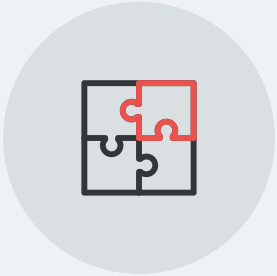
The primary aim of these apps is to gather and exfiltrate personal user data to attacker-operated command-and-control servers. Each malware tool has its own unique data gathering priorities and techniques, as detailed in our full report. Many samples of these malware tools were trojanized legitimate apps, i.e., the malware maintained complete functionality of the applications they were impersonating in addition to its hidden malicious capabilities.

Lookout has found evidence that the malware predominantly targeted Uyghurs, but also, to a lesser extent, Tibetans. These two groups are reportedly the main focus of China's "counter-terrorism" activity. 2 Titles and in-app functionality of samples, such as "Sarkuy" (Uyghur music service), "TIBBIYJAWHAR" (Uyghur pharmaceutical app) and "Tawarim" (Uyghur e-commerce site) show that the majority of this activity focused on Uyghurs.

SilkBean

Targeted focus on Turkic minority ethnic group, referencing Uyghur-relevant sites

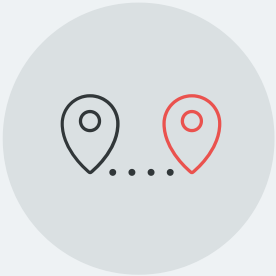
Trojanized apps for Uyghur/Arabic focused keyboards, alphabets, and plugins



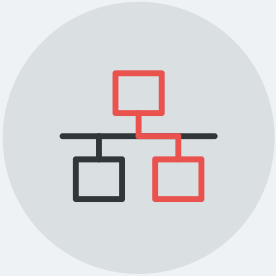
C2 connections with group also using DarthPusher, HenBox, PluginPhantom, and DoubleAgent

DoubleAgent

Trojanized Voxer, TalkBox, and Amaq News (official Daesh news app)



Initially targeting Tibetan community, then pivot to Uygur focus

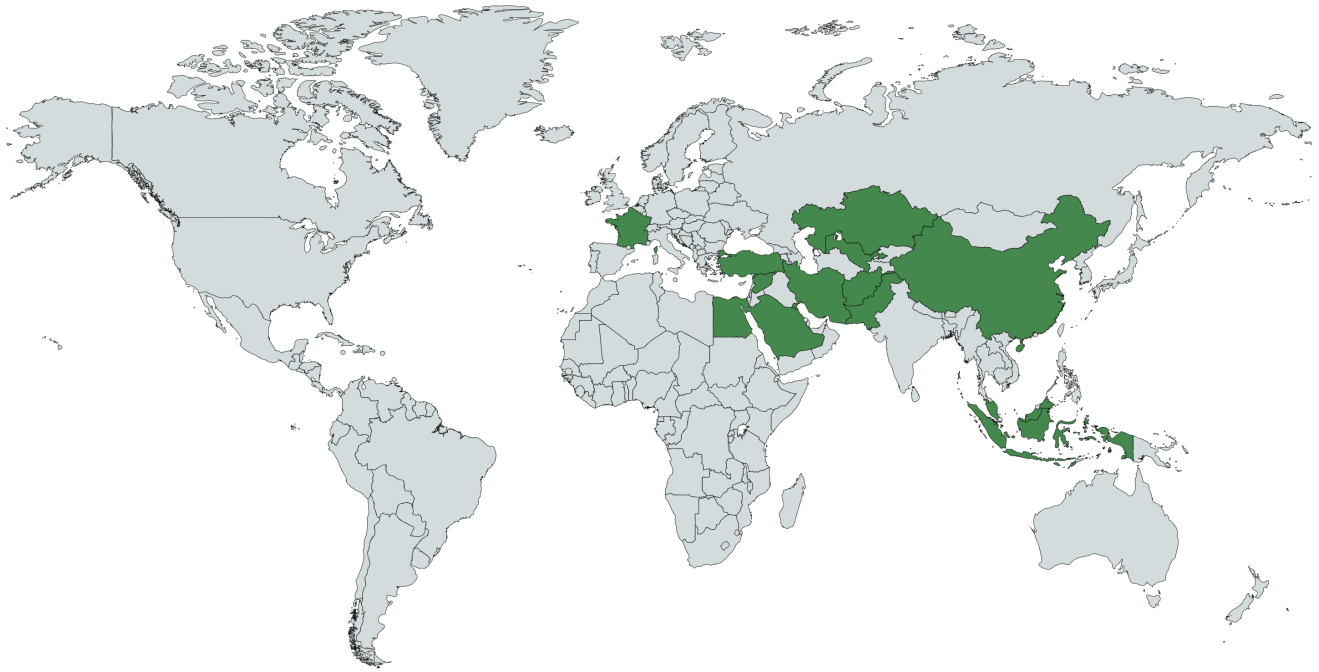


Overlap between DoubleAgent and SilkBean C2s when both families are active

The Chinese government's "Strike Hard Campaign against Violent Terrorism" (严厉打击暴力恐怖活动专项行动),which launched in mid-2014, led to the creation of the National Security Strategic Guidelines, the National Security Law and the Counterterrorism Law in 20153. We noticed that there was a dramatic increase in the number of samples we observed after these directives and initiatives were enacted.

As described in our report, the past activity of this mAPT is connected to previously reported desktop APT activity in China4, which is linked to GREF, a China-based threat actor also known as APT15, Ke3chang, Mirage, Vixen Panda and Playful Dragon.

We noticed that campaigns by this mAPT are also active outside of China, based on the languages and services targeted by the malware samples. For example, titles such as “Turkey Navigation”, “A2Z Kuwait FM Radio”, ” اخبار سوريا” (“Syria(n) News”) may suggest targets in Turkey, Kuwait and Syria respectively. Our research found that at least 14 different countries may be affected by the campaigns. 12 of these are on the Chinese government’s official list of “26 Sensitive Countries,” which according to public reporting5, are used by authorities as targeting criteria.



There are at least four other Android tools in the same mAPT actor’s mobile surveillance arsenal. They are publicly known as HenBox 6, PluginPhantom 7, Spywaller 8, and DarthPusher 9, which have been previously observed targeting Chinese-speaking individuals and those of the Uyghur ethnic minority.

The surveillance apps of these campaigns were likely distributed through a combination of targeted phishing and fake third-party app stores. They are not available on Google Play. Users of the Lookout mobile security products are protected from these threats.

1. https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/
2. https://www.ohchr.org/Documents/Issues/Terrorism/SR/OL_CHN_18_2019.pdf
3. https://www.uscc.gov/sites/default/files/Research/Chinas-Response-to-Terrorism-CNA061616.pdf
4. https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

5. https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs
6. https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/
7. https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/
8. https://blog.lookout.com/spywaller-mobile-threat
9. https://thehackernews.com/2015/03/Xiaomi-Mi-4-malware.html

Lookout Threat Advisory customers are given regular updates and analyses on threat research such as this one. Visit our Threat Advisory Services page to find out more.

July 1, 2020

Download Case Study
{{consumer="/components/cta/consumer"}}

TAGS:

|

Threat Intelligence
|

Surveillanceware