BlackBerry

Mobile Malware and APT Espionage

Prolific, Pervasive, and Cross-Platform

BLACKBERRY RESEARCH AND INSIGHTS TEAM

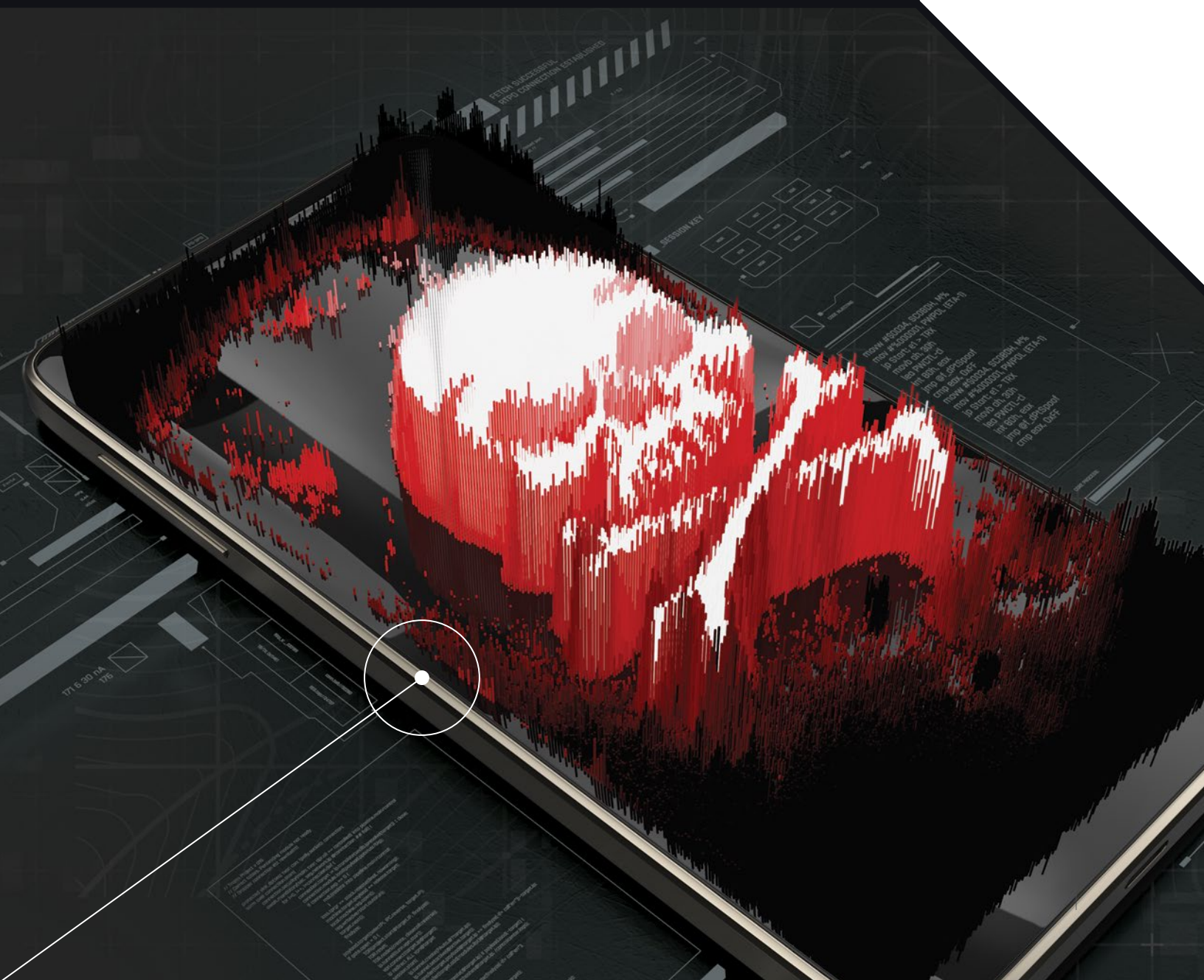


Table of Contents

Introduction

Mobile threats have been around nearly as long as the mobile phone, but they continue to increase in number and complexity as mobile devices become more embedded in, and critical to, our everyday lives. What started out as a somewhat limited attack surface more than a decade ago has grown into a vast landscape of devices utilizing the iOS and Android operating systems. These devices include mobile phones, tablets, televisions, medical devices, alarm systems, and point-of-sale credit card payment systems, among others.

Mobile platforms are primed for exploitation by governments engaged in espionage. They provide a quick, all-in-one means to acquire sensitive data from precisely chosen targets. Mobile phones today offer access to user location, contacts, email, texts and instant messaging, as well as encrypted communication applications and business files. Mobile devices also often bridge the gap between a target's professional and personal lives.

Targeted mobile espionage campaigns complement traditional computer network, human, and signals intelligence efforts and play to the advantage of governments stuck in an asymmetrical power imbalance with other nations. They also offer something traditional espionage means do not: plausible deniability and a lighter attack footprint.

Because of these advantages, the market for exploits targeting mobile devices has skyrocketed. As of this publication, the going rate for a zero-click exploit for the Android operating system has hit $2.5 million dollars, while zero-click iPhone exploits have dropped to $1 million dollars (Greenberg, 2019). These nosebleed prices are reflective of the increasing difficulty of producing reliable exploits given the significant financial and technological investments in security by smartphone manufacturers over the past several years. Yet, difficult does not mean impossible.

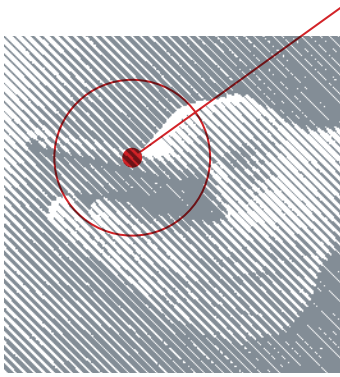
Indeed, the sheer scale of mobile malware that is in-use by state or state-sponsored APT groups that BlackBerry researchers observed in producing this report and the ease with which this mobile malware has been interwoven with desktop malware campaigns, shows definitively that at least several nation states have overcome that barrier.

Executive Summary

Mobile Malware and APT Espionage: Prolific, Pervasive, and Cross-Platform

Until now, the public's exposure to mobile phone malware has been dominated by news about the privately run "greyware" vendors who have made headlines for being purveyors of spyware tools. These commercial smartphone spyware tools reportedly end up in the hands of autocrats who use it to hamper free speech, quash dissent, or worse. Consumers of these news stories are often left with the impression that mobile malware is just something paranoid dictators purchase for use within their own borders in remote third world nations. It is not.

In this report, BlackBerry researchers reveal what the focus on those groups has overshadowed: several governments with well-established cyber capabilities have long ago adapted to and exploited the mobile threat landscape for a decade or more. In this context, mobile malware is not a new or niche effort, but a longstanding part of a cross-platform strategy integrated with traditional desktop malware in diverse ways across the geopolitical sphere.



This approach has allowed state and state-sponsored Advanced Persistent Threat (APT) groups to exploit a mobile dimension for espionage campaigns with impunity. Low threat detection rates and a false sense of security have made mobile users an easy target. Given an immature market, security solutions intended to block mobile malware are few in number, forensic access to smartphones remains relatively limited, and existing public research into the mobile malware threat posed by governments has been scattershot at best and maladroit at worst.

In the pages that follow, BlackBerry researchers expose several previously unknown attack campaigns conducted by APTs both familiar and newly identified. The research will also examine some already known, ongoing, targeted operations and reveal new intelligence and connections that fill in existing gaps in previously published research. This report also represents a broader survey of the strategic use of mobile malware by the Chinese, Iranians, Vietnamese, North Koreans, and two other unknown but likely state-sponsored groups targeting Pakistan's government and military.

Through this research, the researchers seek to redefine the meaning of "state-sponsored APT" in regard to threats targeting mobile devices and further define the notion of a *Golden Age of APT Mobile Malware* that dawned long ago with little notice, yet through persistence and pervasiveness continues to impact us all today.

This report provides a detailed survey of the strategic and tactical use of mobile malware by various governments. It attempts to fill in gaps in earlier research on the subject of mobile malware, and identifies and names new malware, new campaigns, and new threat actors — all of which yields a new and redefined understanding of nation-state APT operations. The conclusions drawn here are intelligence assessments representing judgments based on available data.

Key Findings

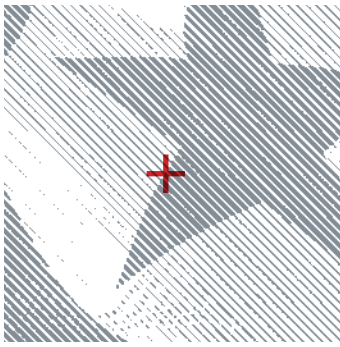
Strategic Intelligence Assessments:

- A collection of established state or state-sponsored APT groups acting in the interests of the Chinese, Vietnamese, North Korean, and Iranian governments have demonstrated the capability to develop native Android and/or iOS mobile malware. The malware is employed in both stand-alone campaigns targeting mobile devices as well as incorporated into cross-platform mobile/desktop espionage campaigns. This activity has been ongoing for a decade or more but has only recently garnered attention.
- Many of the government mobile espionage efforts examined had roots in campaigns designed to spy on targets of interest of some of the nations covered in this report for political purposes. Yet, we have also observed these APT groups pivot to traditional foreign intelligence and/or economic espionage targets. This suggests a more mature, un-siloed and collaborative effort inside different government entities where tools, infrastructure, and intelligence are being shared.
- The ability of state and state-sponsored APT groups to develop and deploy mobile surveillance campaigns within their existing cyber espionage efforts has outpaced the security industry's ability to detect and deter this malware on the endpoints.

Tactical Intelligence Assessments:

- A recent mobile espionage campaign against targets of interest can be traced back to the Chinese state-sponsored APT group known under the umbrella term WINNTI, known for desktop malware campaigns targeting global gaming companies, pharmaceutical giants, industrial manufacturing, chemical companies, and the United States defense industrial base.
- The earliest documented mobile campaign against targets of interest is connected to desktop espionage campaigns by a Chinese state or state-sponsored APT BlackBerry researchers refer to as BBCY-TA1 (a.k.a. IRON HUSKY). This group's targets also include the Russian military and ongoing surveillance of the Mongolian government.
- Another early mobile campaign against targets of interest can be attributed to the Chinese state or state-sponsored APT known as REAVER (a.k.a. SUTR), whose previously observed campaigns involve desktop malware and a range of Western economic and government espionage targets. Several other well-known Chinese APT groups, including LOTUS BLOSSOM and SCARLET MIMIC, are also linked to this activity.
- Targets of interest are the focus of a cross-platform (mobile and desktop malware) espionage campaign utilizing newly identified malware families for Android and Windows that BlackBerry researchers dubbed PWNDROID3 and PWNWIN1. This is the work of a newly identified Chinese state or state-sponsored APT group BlackBerry researchers have dubbed BBCY-TA2 conducting a newly identified campaign BlackBerry researchers dubbed OPERATION DUALCRYPTOEX. The group shares infrastructure with another newly identified Chinese state or state-sponsored APT group BlackBerry researchers have dubbed BBCY-TA3 which is engaged in economic espionage and whose targets include a range of Western and South Asian commercial enterprises in telecommunications and chemical manufacturing in nearly every major chemical manufacturing company in the world outside China, with particular interest in companies based in Germany, the U.S., and Canada.

- In fewer than three years, the Iranian effort to add mobile surveillance capabilities underwent drastic improvement in terms of the quality and complexity of its Android malware, the sophistication of its socially engineered delivery mechanisms, the ability to pivot between domestic and foreign target sets, and the implantation of a cross-platform strategy that integrates mobile and desktop malware.
- North Korea (DPRK) has at least two APT groups, LAZARUS and SCARCRUFT, engaged in espionage campaigns with a mobile dimension. In one campaign, it appears that SCARCRUFT inexplicably engaged in false-flag activity designed to implicate LAZARUS.
- Vietnam's OCEANLOTUS (a.k.a. APT32) has been conducting isolated mobile operations since at least early 2014, predating the identification and examination of the group.
- A newly identified OCEANLOTUS espionage campaign BlackBerry researchers have dubbed OPERATION OCEANMOBILE has both a mobile and a desktop dimension. The newly identified mobile malware family, which BlackBerry researchers have dubbed PWNDROID1, is obfuscated to escape detection and is propagated via fake apps made available on legitimate app stores by way of elaborately concocted cover stories as well as through well-known third-party app stores.
- The Pakistani government is the target of a newly identified and ongoing espionage campaign BlackBerry researchers have dubbed OPERATION DUALPAK which is employing newly identified malware BlackBerry researchers have dubbed PWNDROID2. BlackBerry researchers determined the campaign to be the work of a likely state-sponsored APT group known as BITTER. The malware was propagated via fake apps and elaborate phishing schemes that mimic real entities including *Pornhub Premium* and the *Ansar Foundation*.
- The Pakistani military, other government agencies and their officials were also the subject of a concurrent espionage campaign employing both mobile and desktop components BlackBerry researchers have dubbed OPERATION DUALPAK2 which utilizes newly identified Windows malware family BlackBerry researchers have dubbed PWNWIN2. BlackBerry researchers determined this effort to be the work of another state-sponsored APT group known as CONFUCIUS.

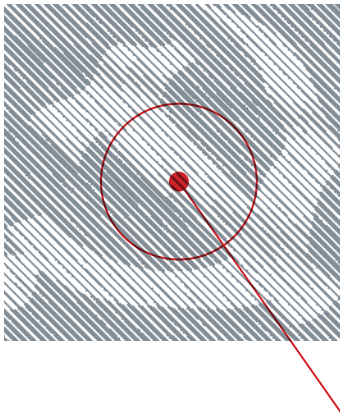


China

THREAT REPORT

China

The earliest publicly available security research detailing the use of mobile malware by a nation-state APT focused on China. The most frequent focus of Chinese mobile malware are targets of interest perceived to be a potential threat to the power of the Chinese Communist Party (CCP).



Analysts point out that, in attempts to influence how China is perceived both at home and abroad and solidify The Party's authority, the CCP has for many years prioritized efforts to "win over" (or undermine) groups critical of official national narratives put forward by Beijing. That imperative brought about something of a "whole of government" response involving different agencies, each of which is tasked with distinct but overlapping missions which eventually dovetail on similar policy issues. These efforts come from different angles, but all feature some form of domestic espionage (Bowe, 2018).

Chinese state-run organizations dedicated to this effort include the overt and purportedly civilian United Front Work Department, the Ministry of State Security (an intelligence agency) that runs covert operations both at home and abroad, and a section of the Chinese military engaged in both overt and covert warfare that until recently was known as the *Liaison Department* of the *PLA's General Political Department*. After a 2016 reorganization of the Chinese military, it is now likely called the *Central Military Commission's Political Work Department* (Bowe, 2018).

The *Political Work Department* and its predecessor have a long and fascinating history dating back to the 1930s and the start of World War II.

Analysts have noted that much of its work was borrowed or heavily influenced by the former Soviet Union's "active measures" playbook. This branch of the Chinese military is understood to engage in work that "operates at the nexus of politics, finance, military operations, and intelligence to amplify or attenuate the political effect of the military instrument of national power," (Stokes & Hsiao, 2013).

CHINA'S COMBINED THREAT: EXAMPLE 1 — RECENT TARGETING OF POLITICAL TARGETS BY WINNTI

The mobile malware campaign efforts BlackBerry researchers observed against Chinese targets of interest can be understood as a single covert stage in a larger active measures influence operation and strategy. The question becomes: who was and is currently behind these attacks? Might the *Political Work Department* have a cyber capability and field activity groups?

BlackBerry researchers examined the most recent mobile malware case to come to public attention: campaigns against targets of interest *in diaspora* via iOS and Android malware as described by Volexity (Case, Meltzer, & Adair, 2019) and Google's Project Zero (Beer, 2019). Google did not specifically mention who was targeted, but they detailed the iOS exploits and implants employed in great depth. In this campaign, mobile malware was distributed via a number of popular websites of interest to or only accessible to the targets of interest and their supporters outside of China.

BlackBerry researchers found, after investigating these two reports, that the attack group behind the campaign was likely not a previously unknown Chinese APT group — one who might represent the hidden cyber wing of the *Political Work Department*. Instead we found these recent espionage attacks to be linked to a very familiar Chinese APT group known as WINNTI, particularly as described in its later iteration as BURNING UMBRELLA (Hegel, 2018).

WINNTI has been categorized within the security community as something of a conglomerate utility player working in support of the Chinese government with various, disparate targets in desktop malware campaigns, including global gaming companies, pharmaceutical giants, industrial manufacturing, chemical companies, and the United States defense industrial base.

While WINNTI has been known to target multiple desktop platforms, including Linux, BlackBerry research reveals for the first time here that WINNTI also engages in mobile espionage campaigns. Here's a brief description of how the connection was made:

- The IP address "142.4.50[.]213" mentioned in the Volexity report had "d.scanvpn[.]com" resolve to it beginning in November of 2014. We found an additional subdomain "mail.scanvpn[.]com" which resolved to "133.130.89[.]39" in October of 2018. The domain "mail.openmd5[.]com" also resolved to this IP address beginning in June of 2018. The "openmd5[.]com" domain was first registered with the email address "rooterit@outlook[.]com". This email address was used to register the following domains:

- aboluewang[.]com
- classifyonline[.]com
- freesss[.]net
- gistal[.]com
- huixunnews[.]com
- lycostal[.]com
- openmd5[.]com
- openncheckmail[.]com
- openother[.]com
- rooter[.]tk
- siddiq1ar[.]com

- "rooter[.]tk" and was previously documented by several different organizations.
- ThreatConnect observed the domains used to directly target and infect targets of interest in 2013 as well as being used in the strategic compromise of the legitimate websites to deliver malware (ThreatConnect Research Team, 2013).
- Palo Alto's Unit42 noticed the domains were used as command-and-control servers for several "FFRAT" samples in 2015 (Flacone, Scott, & Cortes, 2015).
- Citizen Lab found the same domains were linked to an operation used to target several Chinese language news sites in 2017 (Dalek, Alexander, & Brooks, 2017).
- "rooterit@outlook.com" more recently appeared in a larger report titled BURNING UMBRELLA (Hegel, 2018) providing a direct link to the WINNTI umbrella.

As demonstrated above, many different security companies had a snapshot in time of one small piece of the WINNTI elephant, but none possessed a complete picture. Given this APT's consistent focus on targets of interest, it should come as no surprise that this group is also continuing to pursue China's interests in monitoring targets of interest living abroad.

The most recent effort compliments a domestic campaign that also features a mobile dimension. For several years, the Chinese government has compelled those entering the Xinjiang region in China to install Android applications on their smartphones (AFP, 2017), some of which have been found to have atrociously bad security (Cox, 2018), raising suspicions that they are really meant as backdoors focused on certain targets of interest.

The connection between the political espionage campaign and a threat actor best known for military and economic espionage on other platforms was surprising. Analysts have written about the crossover between China's active measures effort and its wider intelligence apparatus since before APT1 was named and shamed. In 2013, Mark Stokes and Russell Hsiao wrote about the converging interests of the then *PLA's General Political Department* or *GPD (*now the *CMC's Political Work Department)* and the *Ministry of State Security (MSS)*. "Given common roots tracing back to the 1930s," they wrote, "GPD liaison work and MSS operations may sometimes be indistinguishable," (Stokes & Hsiao, 2013).

Indeed, Stokes and Hsiao suggest that China's political warfare unit was (and is) likely also a consumer of intelligence from other units of the Chinese military, including signals and foreign intelligence. The crossover is understandable, as certain targets of interest are not just the focus of the government for domestic issues, but also for alleged counterterrorism reasons. China considers elements of some targets of interest an extremist threat to its government both at home and abroad.

CHINA'S COMBINED THREAT: EXAMPLE 2 — BBCY-TA1

BlackBerry researchers found that the domestic/foreign intelligence crossover is not limited to the one example presented above.

The connections between China's mobile attack campaigns aimed at specific targets of interest and traditional desktop campaigns aimed elsewhere go back to the earliest public security research detailing China's mobile surveillance.

One report, published by Kaspersky Lab in March of 2013, was the first to document Android attacks against targets of interest. The attacks followed the compromise of an email account belonging to a high-profile target of interest. This email account was subsequently used to send spear-phishing emails to the target's contacts. One of the payloads sent in these emails was written for Android, and the subject of the email itself purported to be related to a high profile target of interest group (Baumartner, Raiu, & Maslennikov, 2013).

The Android malware did not automatically send harvested information from infected phones, but instead waited until a specially crafted text message was received. Another piece of Android malware (known as an APK file), also identified by Kaspersky, referenced the disputed Senkaku Islands/ Diaoyu Islands in the East China Sea, which continue to be a geopolitical flashpoint between China and Japan to this day.

In revisiting Kaspersky's early work, BlackBerry researchers were able to connect those earliest attacks to a threat group active today in targeted desktop attacks aimed at the Mongolian government. BlackBerry researchers refer to this group as BBCY-TA1. Kaspersky was the first to identify this group (which they called IRON HUSKY) a few years ago and documented prior desktop campaigns targeting the Mongolian government as well as the Russian government and military, but they appear not to have made the connection to the early mobile campaign against targets of interest, and indeed have only published limited information on IRON HUSKY since.

Here is how BlackBerry researchers identified this new connection:

- Both of the Android backdoors mentioned in the 2013 Kaspersky report communicated with the IP address "64.78.161[.]133," which was subsequently used by another malicious domain "www.mol-government[.]com" in July of 2014.
- This domain was linked to multiple China-affiliated attacks on the Mongolian government and the email address "hlemonk@163[.]com" (Fagerland, 2012).
- One of the domains associated with that email address has remained operationalized to this day and continues to be used in isolated, targeted attacks against the Mongolian government by BBCY-TA1.

What's notable about this connection is that it suggests either that two Chinese APT groups with different targets and different missions are sharing infrastructure, or that a single APT group has expanded its targeting portfolio well beyond its initial scope. Both possibilities have implications which are addressed below.

A COMBINED THREAT: EXAMPLE 3 — REAVER

In the month following the Kaspersky research on the mobile malware campaign, in April of 2013, Citizen Lab published research that showed a different mobile campaign had been deployed nearly five months prior, in December of 2012, focusing on targets of interest with trojanized Android applications. In this case, the attacker's use of command-and-control infrastructure was considerably more complex and used encoded web comments to issue commands to the infected devices.

After further investigating the Citizen Lab report, BlackBerry researchers connected the 2012 mobile attacks on activists to several well-known, traditional desktop APT espionage groups including REAVER (aka SUTR), SCARLET MIMIC, and LOTUSBLOSSOM, whose tools notably do not typically include mobile malware. Instead, REAVER and LOTUSBLOSSOM are better known for Windows-based espionage campaigns linked to recent attacks on the automotive industry, the defense industry, the European Union, and the United Nations.

BlackBerry researchers previously wrote about similar crossover with targets of interest (BlackBerry Cylance Threat Intelligence Team, 2019). BlackBerry researchers made the new connection as follows:

- The domain "android.uyghur.dnsd[.]me" first resolved to the IP address "184.82.123[.]143" nearly seven months prior in May of 2012 and changed to IP address "216.176.190[.]44" in September of 2012, which would strongly indicate that it was likely used before December.
- The domain "internet.3-a[.]net" also resolved to both IP addresses around the same timeframe and was later directly attributed to SUTR by Citizen Lab. In the same vein another dynamic DNS domain was also connected to this one "ios.dnsd[.]info" which would indicate that iOS devices were likely targeted around the same timeframe.
- Several other dynamic DNS domains linked to this early attack continued to resolve into the present and connect to REAVER/SUTR, SCARLET MIMIC, and even LOTUSBLOSSOM.

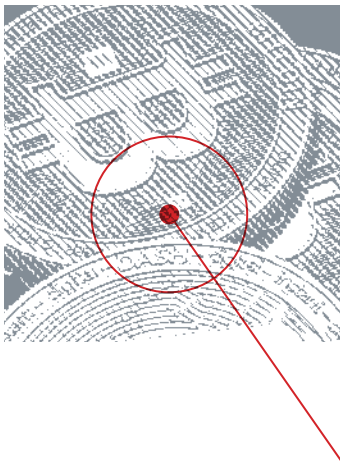
This would again indicate either shared infrastructure among different APT groups with vastly different targeting priorities, which in the BlackBerry researcher's estimation is rare, or a single APT group with a wildly disparate target set over time, which would also be anomalous. Both possibilities present significant challenges to the conventional wisdom surrounding Chinese APT groups.

CHINA'S COMBINED THREAT: EXAMPLE 4 — BBCY-TA2 AND BBCY-TA3

In retracing the history of the first publicly available reports on Chinese mobile malware campaigns, BlackBerry researchers found one campaign could be traced from the earliest reported activity straight through to the present day. It should come as no surprise that it was aimed at other political targets of interest making headlines. BlackBerry researchers observed a resurgence in the group's activity whenever domestic unrest began to arise in specific regions of the country.

BlackBerry researchers dubbed this newly identified campaign OPERATION DUALCRYPTOEX. The researchers also identified new malware families that target both Android and Windows, which BlackBerry researchers dubbed PWNDROID3 and PWNWIN1, respectively. The effort is the work of a newly identified Chinese APT group BlackBerry researchers dubbed BBCY-TA2.

BBCY-TA2's malware is distributed via mobile applications that mimic a popular peer-to-peer marketplace called "localbitcoins[.]com" designed to convert Bitcoin to cash at the regional level. China has seen a sharp rise in cryptocurrency adoption and demand following the ongoing unrest because certain targets of interest rely on Bitcoin for operational security and concerns over local currency instability. Numerous local retailers have begun to accept various cryptocurrencies while Bitcoin Cash is becoming a near de-facto standard among certain Chinese targets of interest (Redman, 2019), (Hamacher, 2019). But to be truly useful, crypto cash must often become hard cash in the local currency. And that is what sites like *Local Bitcoins* offer.



BBCY-TA2 has taken note and taken advantage. PWNDROID3 offered a wide range of capabilities including geolocation tracking, call monitoring, screen monitoring, and a host of other functions. Perhaps the most intriguing feature was a function that holds a list of specific locations or addresses and sends BBCY-TA2 geofencing alerts when they are visited. Here is a brief overview of the technical connections between BBCY-TA2 and the 2014 campaigns, as well as a quick tour of OPERATION DUALCRYPTOEX:

- The 2014 mobile campaigns, which came in September of that year, involved the "Occupy Central with Love and Peace" movement. Reporting at the time was often conflicting; however, given access to better data sources now, the majority of these mobile campaigns were all closely related and most likely deployed by the same set of operators, BBCY-TA2.
- The first campaign mimicked Code4HK, a group of developers. A message, "Check out this Android app designed by Code4HK for the coordination of Occupy Central!" was sent to a number of targets of interest and contained a trojan which communicated back to the domains "www.xsser[.]com" and "mm.v1lady[.]com" (Boehler & Sam, 2014). The Code4HK malware was also signed with the email address "STREAM@V1LADY[.]COM" on July 7, 2014.
- Shortly thereafter Lacoon Mobile Security (now Check Point) discovered what they called Xsser iOS mRAT (Bublil, Brodie, & Bashan, 2014). mRAT also communicated to "www.xsser[.]com" and was one of the first targeted iOS threats to be found in the wild. However, it would have only been able to infect already jailbroken devices. Conveniently, according to research at the time, roughly 14% of the nearly 60 million iOS devices in China had been jailbroken to support Chinese keyboard applications.
- The domain "mm.v1lady[.]com" resolved to "112.124.47[.]157" beginning on September 17, 2014. This IP would be a lynchpin for the group for nearly three years and link to both "mm.bbmouseme[.]com" and "mm.outputinfo[.]com". Lookout found the same operators had created a new Android RAT they termed xRAT in 2017 (Flossman, 2017), and newer undisclosed variants continue to infect users even in 2019.

Regarding OPERATION DUALCRYPTOEX:

- "63c9a6108c056cfd3962c2608d262384d65ac199d5ec480f6e8779e470915df8" is one recent sample signed on July 11, 2018 which communicates to BBCY-TA2's C2, "huaian.bbmouseme[.]com", and portends to be related to "localbitcoins[.]com".
- The sample utilized the "javax.crypto.Cipher" DES implementation to encode sensitive strings in the APK with the secret key "i_want_you_and_i_need_you". This key appears in some of BBCY-TA2's Windows backdoors as well. The author(s) may not have fully understood the mobile implementation, though, as only the first 8-bytes of the previous string would be used in the encryption and decryption process.

OPERATION DUALCRYPTOEX marks the fourth example BlackBerry researchers identified in this report where there was established crossover in infrastructure with another APT group's activity.

In this case BBCY-TA2's infrastructure crosses into the activity of another desktop-malware-focused APT group, though it too appears to be new. BlackBerry researchers have dubbed this newly identified yet traditional cyber espionage APT group BBCY-TA3.

BlackBerry researchers observed this group most recently targeting telecommunications providers across the countries that ring the South China Sea for espionage purposes. In addition, BlackBerry researchers observed extensive campaigns throughout 2018 and 2019 in which BBCY-TA3 pursued nearly every major chemical manufacturing company in the world outside China, with particular interest in companies based in Germany, the U.S., and Canada.

Conclusions on Chinese Activity

After an historic retrospective look at China's mobile surveillance, it is clear the majority of it was consistently domestic in focus. During this introspection BlackBerry researchers uncovered unexpected connections to a range of additional APT groups whose targets run the gamut of verticals from government to military to commercial, and which crisscross the globe.

These connections are significant because they challenge an assessment some China analysts have made about the government's ability to integrate horizontally and coordinate across a vast bureaucracy rife with its own problems of dysfunction, corruption and stove-piping, as represented in the seminal Chinese Industrial Espionage (Hannas, Mulvenon, & Puglisi, 2013).

If Chinese APT groups are coordinating efforts and/or sharing tools, they become more difficult to defend against. The shared tool sets also pose a challenge for organizations whose risk profile relies on blacklisting domains or looking only for certain types malware, and who might mistakenly allow access on the basis of the belief that they are outside of China's target profile.

Our perception of the Chinese APT groups must expand to include both mobile and desktop threats, domestic and foreign organizations, and domestic/economic/government/military target profiles. It's also worth expanding our notion of the typical target of the Chinese government: malware meant for targets of interest *in diaspora* for domestic reasons may very well end up inside a Western business that proves an attractive target for someone else.

Iran

THREAT REPORT

Iran

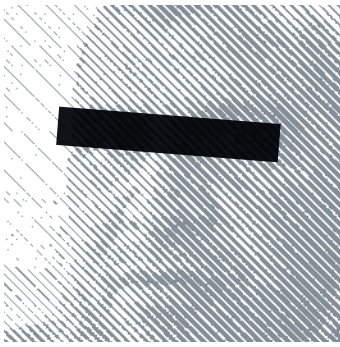
Iran's mobile surveillance capability has historically been primarily focused inward to target various people of interest to the Iranian government. While some of the first documented cases involved journalists and activists abroad, the motivation behind the attacks appeared to be domestically driven.

The Iranian APT strategy for adoption of the mobile dimension is thus in line with that of the Chinese attack groups, whose earliest mobile campaigns were similarly motivated by an imperative to keep track of certain individuals both in and out of country who challenged the authority of the government.

DOMESTIC KITTENS?

Public research on Iranian mobile attacks was first published in 2016 and revealed a state-sponsored effort still in the initial stages of development, where threat actors deployed a relatively immature and simplistic toolset which included variants of "DroidJack" and Android Metasploit payloads (Guarnieri & Anderson, 2016). Following this early activity, it was clear the Iranian government took on significant development efforts, as revealed in the exposure of several subsequent and more sophisticated mobile campaigns such as Check Point's DOMESTIC KITTEN report last year (Check Point Research, 2018).

In their report, Check Point detailed how a more advanced set of Android malware was quickly leveraged in a prolonged campaign of Iranian government espionage that was focused on Kurdish and Turkish natives, as well as ISIS supporters. At first glance this would suggest an outward-facing mobile espionage effort driven by counterterrorist and foreign policy concerns. None of that would be particularly surprising given that all these groups are in play in the Syrian conflict where Iran supports the Assad regime.



However, Check Point assessed that the targets were in fact all Iranian citizens. What we still do not know, based on Check Point's analysis, is whether this domestic campaign was motivated by a larger, politically driven influence operation strategy as with the Chinese, or if it represents one facet of a larger political security strategy, or both. In a follow up post, Check Point added

more insight and clarified that "despite the heavy targeting of Iranians, there were also Kurdish and Urdu natives, ISIS supporters and even Yemeni citizens among the victims," (Check Point Research, 2018).

While only a limited number of indicators of compromise (IoCs) were shared in Check Point's initial report, BlackBerry researchers used the IoCs provided to find a much larger list of hashes as well as command-and-control infrastructure detailed in the Appendix. BlackBerry researchers expanded on the intelligence for the public to better understand and assess this threat.

In Check Point's follow-up post published a month later and referred to above, a number of additional details were released regarding DOMESTIC KITTEN, including the name of one of the more complex Android samples BlackBerry researchers observed: "com.eracomteck/example.badoo".

This Android malware is relatively unique, and BlackBerry researchers used it along with other forensic indicators to draw a clear connection to a different campaign written about in a June 2019 report by TrendMicro called "Bouncing Golf" (Xu & Guo, 2019). TrendMicro noticed the connection to DOMESTIC KITTEN but did not adhere to it conclusively. In our view, "Bouncing Golf" was very clearly a continuation of DOMESTIC KITTEN's activities.

What's significant about that connection is that it represents a dramatic shift in targeting from domestic to foreign espionage. The majority of the data TrendMicro was able to identify in the most recent campaigns was related to stolen military documents and images, all taken primarily from other Middle Eastern countries. This is also indicative of a concurrent shift in motivation behind the espionage, from domestic to military.

In a relatively short amount of time, Iran can be seen to have followed an implementation strategy first employed by other non-democratic countries like China in honing a capability initially on domestic targets of interest before turning it outward for other espionage purposes. Iran has previously been observed following this course in the development and implementation of its traditional desktop cyber operations strategy (Anderson & Sadjadpour, 2018).

MUDDYWATER GOES MOBILE

BlackBerry researchers uncovered how DOMESTIC KITTEN, an Iranian APT group that uses mobile malware, has expanded its portfolio from domestic target to include foreign espionage targets in a short amount of time. Let's consider another example, this time with another Iranian APT group that has been traditionally focused on foreign espionage using desktop malware, but which has recently been observed adding a mobile component to its campaigns — MUDDYWATER.

In June of 2019, TrendMicro pointed out that the MUDDYWATER group had started deploying Android payloads. In their report, TrendMicro explained how a number of pieces of Android malware reached their targets, detailing an SMS phishing campaign that sent messages in Turkish with a link which, if clicked, took victims to a website which they identified as a "legitimate website belonging to a non-profit research organization in Turkey." They wrote, "most likely, the organization's website was compromised, which is not surprising as its website was hosted on WordPress, a platform MuddyWater is fond of targeting," (Lunghi & Horejsi, New MuddyWater Activities Uncovered, 2019).

Here is a technical explanation of how TrendMicro made that connection:

- TrendMicro was able to identify four unique android payloads based upon a common command and control server "78.128.139[.]131". The following Six unique Android APK's were available in a common malware repository:

  02f54da6c6f2f87ff7b713d46e058dedac1cedabd693643bb7f6dfe994b2105d

  26de4265303491bed1424d85b263481ac153c2b3513f9ee48ffb42c12312ac43

  3bfec096c4837d1e6485fe0ae0ea6f1c0b44edc611d4f2204cc9cf73c985cbc2

  6b4d271a48d118843aee3dee4481fa2930732ed7075db3241a8991418f00d92b

  9af8a93519d22ed04ffb9ccf6861c9df1b77dc5d22e0aeaff4a582dbf8660ba6

  dff2e39b2e008ea89a3d6b36dcd9b8c927fb501d60c1ad5a52ed1ffe225da2e2

- One variant, e9617764411603ddd4e7f39603a4bdaf602e20126608b3717b1f6fcae60981f2, was slightly different from the six above but still contained a reference to a unique image hosted at the URL:

  "http://airplanesandmore[.]com/prodimages/largeSpace%20Shuttle%20Endeavour.jpg".

- The SMS spreading function also still linked to a malicious APK hosted from the URL: "http://setav[.]org/wp-includes/APK/SetaNews.apk", which served the SHA256 hash be9fb556a3c7aef0329e768d7f903e7dd42a821abc663e11fb637ce33b007087.

Indeed, the website in question, "setav[.]org, is the website for SETA, which in English is *The Foundation for Political, Economic and Social Research*, a political policy think tank based in Ankara, Turkey. TrendMicro did not discuss that although the think tank describes itself as "independent, nonprofit, and nonpartisan," a German news organization uncovered evidence that it is more than that.

Deutsche Welle, a German broadcast media company published a news item claiming that "the foundation is run by [Turkish Prime Minister] Erdogan loyalists and headed by Serhat Albayrak, the elder brother of Erdogan's son-in-law, Finance Minister Berat Albayrak. He is also Chairman of the Board of the largest government-related media group in Turkey. Virtually all of SETA's senior management is active in an advisory capacity for Erdogan," (Mumay, 2019).

Deutsche Welle also provided evidence that the supposed non-profit was used in information and influence operations beneficial to the Turkish government. BlackBerry researchers assess that MUDDYWATER was aware of this connection, and that the SETA domain was chosen precisely because of its relationship with the Turkish government, given the likelihood that it would be implicitly trusted by government officials targeted by the SMS text messages.

Iran is continuing to conduct mobile surveillance on its own citizens, minority ethnic groups, and neighboring countries involved in strategic regional conflicts. BlackBerry researchers suspect the increased interest in countries like Turkey is due to recently forged military ties with Russia.

In fewer than three years, Iran has drastically improved the quality and complexity of its Android malware, the sophistication of its socially engineered delivery mechanisms, the ability to pivot between domestic and foreign target sets, and the implantation of a cross-platform strategy that integrates mobile and desktop malware.

The DPRK

THREAT REPORT

The Democratic People's Republic of Korea (DPRK)

North Korean APT groups have historically focused on traditional South Korean espionage targets. A dramatic shift occurred in 2014 with the high profile and highly damaging attack against Sony Pictures Entertainment. Following this attack North Korea gained a significant amount of attention from western researchers who attempted to lift the fog surrounding North Korea's larger cyber strategy. Research efforts, like Novetta's "Operation Blockbuster" did a phenomenal job of detailing LAZARUS' known malware at the time (Novetta, 2016).

That effort expanded to include North Korea's mobile malware strategy. Following Novetta's landmark publication, both Palo Alto and McAfee published research about LAZARUS' known Android malware in 2017 (Kasza, Cortes, & Yates, 2017), (Han, 2017). With this connection made, North Korea joined the league of government APT groups with an operational mobile surveillance element in their offensive cyber strategy.

What's worth noting about the research into North Korean mobile malware is that LAZARUS' initial set of Android malware was markedly different than that of other nation-state APT group's early work.

Instead of writing malware in Java, the language of the Android operating system and its apps, LAZARUS elected instead to create native executable (ELF ARM) binaries to perform the malicious functionality.

This strategy indicates one of the following:

- LAZARUS was either not comfortable enough with the Android platform to write for it, or else they were simply accustomed to coding for Linux; or
- LAZARUS deliberately chose to avoid writing malware in Java for Android in order to attempt to evade detection.

Whether intentional or not, LAZARUS' mobile malware did in fact escape detection for a period of time, but eventually this unique characteristic made their samples relatively easy to reliably detect as well.

Most of the observed North Korean mobile malware has been trained on a range of targets in South Korea, which seems to bear the brunt of most of their desktop malware attacks as well.

As a result of the Korean language barrier and the inherent interest of the South Korean government to exaggerate the North Korean threat, much of the cutting-edge intelligence on the mobile threat remains foggy. And even when BlackBerry researchers examined the Korean language research and lifted one layer of that fog, another took its place, as detailed in the next example.

SCARCRUFT — THE FOG OF FALSE FLAGS

While LAZARUS, which the US government also calls HIDDEN COBRA (US-CERT, 2017), has earned the most media attention, it is worth remembering that is not the only North Korean state-sponsored APT group in action. Another group, which Kaspersky first named SCARCRUFT (a.k.a. APT37, GEUMSEONG121) is engaged in mobile malware campaigns that are the subject of recent research from South Korean antivirus firm Alyac (Alyac, 2019).

Alyac described how SCARCRUFT began leveraging cloud provider services like DropBox and Yandex to download additional malicious files and upload stolen data. One of the more recent Android samples Alyac wrote about, from August 2019, carries the hash value "8863dc53aba8dbaa7a76ab4653d54a4a7412dc9bb986b8fe1d3d8350bbb730f1." In examining this piece of Android malware, Alyac observed a direct crossover with similar desktop malware being served from the same Dropbox account.

> This crossover is significant because it provides evidence that multiple North Korean APT groups have implemented a cross-platform strategy that combines the simultaneous use of mobile and desktop malware on the same target.

Interestingly, McAfee also documented the use of cloud providers by yet another likely North Korean state-sponsored APT group called SUN TEAM in a blog post about the mobile monitoring of North Korean defectors, which may expand the list to three such groups with this cross-platform surveillance capability (Min, 2018).

Shortly before that McAfee blog post, Alyac identified another interesting find in a second piece of Korean-language research: strong evidence suggesting that SCARCRUFT attempted to plant false flags in one of their extremely targeted operations against South Korea (Alyac, 2019). What was even more interesting was the false flag pointed to LAZARUS. While it's not entirely clear why one North Korean APT group would wish to lead investigators and/or its target to believe that another North Korean APT group was responsible, the implication is clear: a dense haze still lingers over the internal workings of the North Korean government.

Vietnam

THREAT REPORT

Vietnam

BlackBerry researchers established that the only reported state or state-sponsored APT group in Vietnam, first identified by Chinese security company 360Safe and dubbed OCEANLOTUS (a.k.a. APT32), has integrated mobile and desktop malware vertically in the same campaigns since the very beginning of its observed activity. BlackBerry researchers delved into more of the mobile aspects of OCEANLOTUS' campaigns.

That OCEANLOTUS was even a player in the mobile malware arena had gone undetected until just recently, when in August of 2019 an obscure Chinese antivirus company wrote about a small number of different mobile operations conducted through 2017 (Antiy PTA Team, 2019). BlackBerry researchers reviewed these findings and discovered additional IoCs associated with this past activity which included evidence that OCEANLOTUS has been a player in the mobile malware arena since at least early 2014, predating the identification and naming of the group itself which occurred in May of 2015.

BlackBerry researchers assessed with a high degree of confidence that the mobile malware campaigns identified are under the control of OCEANLOTUS, primarily due to code similarity to known OCEANLOTUS desktop campaigns as well as simultaneous use of command-and-control infrastructure for both these new mobile campaigns and separate novel desktop campaigns associated with the group. What's more, as alluded to above,

BlackBerry researchers observed OCEANLOTUS engaged in cross-platform attacks that involved both mobile and desktop malware simultaneously in use on the same target in the same campaign.

A NEW MOBILE CAMPAIGN: OPERATION OCEANMOBILE

In the newly identified operation BlackBerry researchers dubbed OPERATION OCEANMOBILE, they observed OCEANLOTUS initiate a mobile espionage campaign delivered via a sophisticated trio of fake apps for Android. One of these apps supposedly provided support for high-resolution graphics on the phone (e.g. for use in games), while another purported to block ads on your phone, and a third presented itself as a browser and cache cleaner. The apps were distributed through phishing, but also to a wider set of targets via third-party app stores as well as the official Google Play Store.

It is worth noting that OCEANLOTUS distributed its apps in part via phishing, which connotes a specific target. They also chose to seed the apps in several stores for anyone to download anywhere, which suggests the net may have in fact been much wider, or perhaps entirely indiscriminate.

For now, one question raised by the campaign caught our attention — namely exactly how it was that the apps laden with malware made it into the Google Play Store itself? What BlackBerry researchers discovered was that OCEANLOTUS went to the trouble of establishing an entire fake backstory to give its malicious apps an air of legitimacy. They created modified GitHub repositories that theoretically showed evidence of the developers' code for each app, complete with public facing "contact us" email addresses to answer any questions that might arise about their "products." They even went to lengths to concoct entire privacy policies for their apps, which few people tend to actually read, but nevertheless was ironic, given that OCEANLOTUS' entire premise was to spy on its targets.

The newly discovered malware family these apps delivered, which BlackBerry researchers dubbed PWNDROID1, was first identified by Russian antivirus company Dr. Web in 2019, though they did not name it, nor were they able to attribute it to a specific group (Dr. Web Antivirus, 2019).

In reverse engineering the malware, it was particularly intriguing to observe that OCEANLOTUS applied a technique commonly seen in desktop malware campaigns to help it escape detection by scanning. They created an otherwise benign looking application which when analyzed in detail would in fact load and execute an additional encrypted payload. This helped ensure that the apps would pass muster with Google and App Store administrators and fly under the radar of other antivirus companies.

Further technical information regarding the PWNDROID1 backdoors used in this newly revealed operation that BlackBerry researchers dubbed OPERATION OCEANMOBILE is as follows:

- Fake OpenGL ES Updater:
  Initial Campaign: June 6, 2019
  Policy: https://gist.github.com/lijustharma/1771c2852eb687a1f193ff58a10d5dd2
  SHA256: 669f21afd98391abd0d1d72af57aa5d57b9b3f93f379773e5696e5495f27f1e2
  SHA256: c8e78a4fbc26c78110259dd1e1d7330443935a406731a38715e5e84ec613e3cd

- Fake Ad Blocking Program:
  Initial Campaign: June 6, 2019
  Policy: https://gist.github.com/agcondiefoun/806b89fbb683f55f3f6cae275f8902cb
  SHA256: a2d75b3bca022d4439fc5abbd43c8d0a6adda08548691b05c7ba6ac17e9cc815
  SHA256: c1aa3b0e24958547765c90659021c9a2cd65d9bec532b1d93d46ceeaacb33a32

- Fake Browser Cleaner:

  Initial Campaign: June 6, 2019

  Policy: https://gist.github.com/rhenchesttija/ef404116cda4e7c1bfda5ebf179d4fc0

  SHA256: 99eba5020158332510da7732473142492010ce7a3ae2f0e4749212764f9f4528

- "c1aa3b0e24958547765c90659021c9a2cd65d9bec532b1d93d46ceeaacb33a32", the most recent sample, was only identified by four antivirus vendors at the time it was submitted to a commonly used malware repository. BlackBerry researchers ascribed this to the fact that the embedded payload (assets/libcore), which performed all of the malicious functionality, was AES-encrypted within the APK.
- The username "agcondiefoun" was used to post the fake ad blocking app to various places. A profile matching the username was identified on GitHub: "https://gist.github.com/agcondiefoun" and contained the following gist: the file was dated May 10, 2019, although the gist was created on June 6, 2019, which indicates the actors were likely planning the attack for some time prior to distribution. The gist contained an additional email address "adsgroup@gmail[.]com". A matching document was posted to Pastebin anonymously on June 17, 2019; it's not clear if this activity is related to the group or was just someone republishing the information elsewhere. However, the APK's first started to appear in numerous third-party app stores on that date as well.
- OCEANLOTUS used a similar process with the fake OpenGL updater app, leveraging the username "lijustharma" to post the application to various app stores.
- A related GitHub page was identified here: "https://gist.github.com/lijustharma/1771c2852eb687a1f193ff58a10d5dd2"
- The page was created on June 6, 2019, and contained another email address of interest "plugin.support@hotmail[.]com". An identical post was also created on Pastebin on June 17, 2019, at the following URL: "https://pastebin.com/mBMHevsh".
- BlackBerry researchers were then able to identify another associated GitHub account: "https://gist.github.com/rhenchesttija/ef404116cda4e7c1bfda5ebf179d4fc0", Pastebin URL: "https://pastebin.com/EdmjAbFX", and another malicious APK. The gist was dated May 6, 2019 but was created on June 6, 2019. BlackBerry researchers were able to identify one additional GitHub account likely associated with the actor, but it does not appear to have been operationalized yet: "https://gist.github.com/hoenihahav/9b3e64fc03568a4c4f2f8b5e3da3c72d".

OCEANLOTUS has been a constant threat to Vietnamese targets of interest, regional players in South Asia and farther afield, and will continue to exploit new avenues of surveillance as they become available. They have readily adapted their malware to alternative platforms including macOS, so it is not surprising to discover continuing operations in the Android space.

BlackBerry researchers are still analyzing the full extent of OCEANLOTUS' mobile campaigns to better understand its scale, scope, and targets, and retrieved some statistics relating to a different piece of OCEANLOTUS malware used in a past campaign in 2018 (one that presented itself as a codec library but was clearly not). The website AppBrain calculates and disseminates data on apps distributed via the Google Play Store. In this case, OCEANLOTUS' malware-laden app was installed at least 5,000 times before it became unavailable in February of 2019 as seen in the image below:

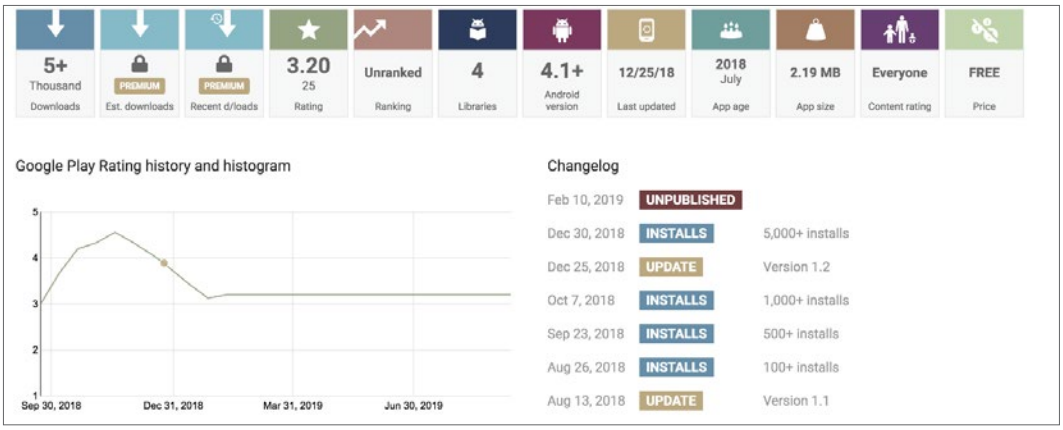


Figure 1: Details from AppBrain About One OCEANLOTUS Mobile Application

It's not entirely clear just how wide-reaching OCEANLOTUS' mobile operations truly are, but they are undoubtedly significantly larger than what's been discovered and published to date.

Target: Pakistan

In early August of 2019, India stripped the disputed Kashmir region of its autonomy, re-igniting a decades-long row with its neighbor, Pakistan, who also claims authority over parts of the region. There were thousands of arrests, a build-up of military forces and, for a period of nearly a month, direct armed conflict between two nuclear-armed countries seemed imminent.

In light of episodes like this, in addition to the constant churn of Pakistan's often violent brand of politics and its overnight celebrity as the conduit for China's major Belt and Road Initiative, Pakistan has remained one of the world's most sought after espionage targets.

Nearly all the governments with a developed cyber capability have an interest in, and ability to spy on the Pakistani government and its influential military. Even APT groups with unattributed state backing have had a go at it. BlackBerry researchers have written extensively about one such group, THE WHITE COMPANY, previously (Livelli, Smith, & Gross, 2018).

It should come as no surprise that the collective APT espionage effort targeting Pakistan has been cross-platform and includes mobile malware, but evidence proving the assumption is nevertheless sporadic and sparse. BlackBerry researchers identified two such campaigns and will discuss their mobile dimension below. They each involve two, known, unattributed but likely state-backed APT groups, BITTER and CONFUCIUS. While the latter group has been reported to have used mobile malware before, the former has not.

OPERATION DUALPAK — TARGET: PAKISTANI GOVERNMENT

A newly identified espionage campaign BlackBerry researchers dubbed OPERATION DUALPAK targets members of the Pakistani government. We assess that it is the work of a state-backed APT group known as BITTER. This threat actor was first identified by Chinese security firm 360 in 2016.

BITTER is known for its relentless espionage campaigns targeting Pakistan. To a lesser degree, it has also been observed targeting China, India and other countries in South Asia, as well as Saudi Arabia. While their traditional desktop malware campaigns are well documented, we believe OPERATION DUALPAK to be the first publicly documented instance in which newly identified BITTER mobile malware that BlackBerry researchers dubbed PWNDROID2 has been used. In addition, this operation also featured an unusually extensive, traditional desktop malware campaign in parallel.

Like other APT groups discussed in this report, e.g. OCEANLOTUS, the chosen method of malware distribution was fake apps, in this case distributed via SMS, WhatsApp, and various social media platforms in June and July of 2019. What intrigued us was the choice of subject matter BITTER selected for the malware-laden apps, which were designed to appeal to both low-brow and high-brow elements of the Pakistani government.

First, the low brow: One of the applications purported had an adult entertainment theme, calling itself *Pornhub Premium*. Technical details regarding this phase of the operation are here:

All of the identified mobile malware samples communicated to the dynamic DNS domain "newsbroadcastlive.ddns[.]net" which currently resolves to the IP address "188.215.229[.]220".

- Based upon our initial investigation it appears that the applications were spread via various platforms as discussed above in June and July of 2019. The URL shortener "tinyurl[.]com" was employed in at least one phishing instance.
- The following shortened address: "http://tinyurl[.]com/y485gdjo" expanded to:
- "http://intlopenpipeservice[.]net/HBL/PornhubPremium.mp4.apk"
- An additional URL was identified which also served up the exact same APK, "http://spiceworld.rf[.]gd/Premium.php" with a different filename "P-Hub Premium.apk".
- "intlopenpipeservice[.]net" above resolved to "162.222.215[.]183" from January 2019 until July 2019. Another domain of interest appeared on this IP address in July "rnail.googlle.conn.pk.intlopenpipeservice[.]net" and was likely used to phish Gmail account credentials.

Following that trail, our research led us out of the gutter and toward a series of new malware samples which, in turn, connected us to the high-brow method of delivery.

Perhaps the most interesting of those was a fake app purporting to bear association with the *Ansar Foundation*. Ansar is a real UK-based NGO which has been operating in Pakistan for more than a decade. Ansar is the Arabic word for "helper," and according to its website the foundation has conducted relief work for those affected by flood and earthquakes as well as victims caught in military operations conducted in Northern Pakistan.

Although the evidence BlackBerry researchers uncovered in relation to the fake *Ansar*-related malware did not indicate precise targeting, it did roughly coincide with the time a number of other NGOs were kicked out of Pakistan.

One of the domains BITTER used in OPERATION DUALPAK, "wdibitmapservice[.]net", overlapped with multiple other unique IP addresses with a common set of related dynamic DNS domains belonging to the same actor. This allowed BlackBerry researchers to conclude that this recent Android campaign is highly likely to be associated with ongoing Windows targeting related to BITTER.

OPERATION DUALPAK2 — TARGET: PAKISTAN MILITARY AND GOVERNMENT

BlackBerry researchers uncovered a second newly identified campaign dubbed OPERATION DUALPAK2, which also targeted various Pakistani government departments as well as military officials. The campaign features the well-integrated use of cross-platform malware aimed at both mobile devices and desktop computers. Based on our research, OPERATION DUALPAK2 is the work of another, well-known and likely state-sponsored APT called CONFUCIUS.

CONFUCIUS has historically targeted Pakistan for espionage and was first identified and named by Palo Alto in 2016 (Lancaster & Yates, 2016). Following that report, TrendMicro has published several additional papers and updates on the group.

Recently, researchers gave a talk in which they attempted to link several seemingly disparate APT groups targeting Pakistan into a singular connected nexus (Lunghi & Jaromir, Linking Cyberespionage Groups Targeting Victims in South Asia, 2019). They also alluded to the fact that Phronesis, an Indian cybersecurity firm founded by former Indian military officers, is likely involved with one or more of the activity sets which include APT groups known as PATCHWORK, CONFUCIUS, URPAGE, HANGOVER, DONOT/EHDEVEL, and SNAKE IN THE GRASS. Whether this ambitious assessment holds up over time remains to be seen.

For now, BlackBerry researchers delineate additional historic and recent mobile campaigns conducted by CONFUCIUS. This is not the first time CONFUCIUS' mobile operations were exposed; in February of 2018, TrendMicro documented the use of fake chat apps that were created to conduct mobile surveillance of isolated targets (Lunghi & Horejsi, Deciphering Confucius' Cyberespionage Operations, 2018).

Following that disclosure by TrendMicro, CONFUCIUS adopted several new domains and concurrently switched their other existing mobile operations to new IP addresses. But in their retooling, they adopted a particularly interesting tactic to ensure that their mobile malware was delivered only to desired targets — inserting a human element.

Never before had BlackBerry researchers encountered an opportunity to interact with the human face of an APT group live during an ongoing espionage operation. This presented a unique opportunity.

CONFUCIUS embedded a chat program on one of the websites used to distribute "dating/romance" chat apps that really enabled CONFUCIUS to surveil its targets.

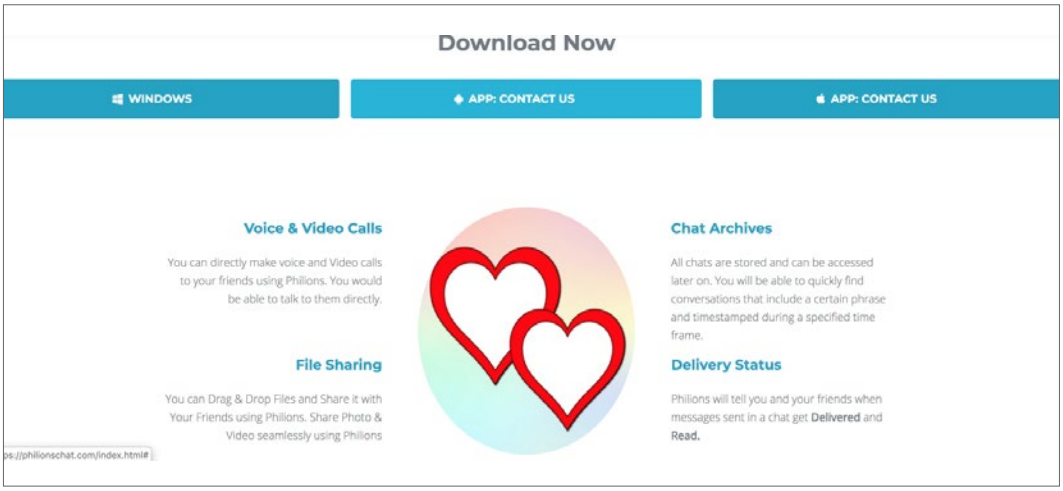


Figure 2: Screenshot of Phillionschat.com

As clearly demonstrated in the figure above, in order to receive the (malicious) iOS or Android application one must click to initiate a conversation with the administrator. This was done through an embedded JavaScript version of the *RocketChat* application which used the subdomain "web.philionschat[.]com." BlackBerry researchers were able to find an associated "web" subdomain for each actively used domain involved in mobile distribution.

A newly identified Windows payload Blackberry researchers dubbed PWNWIN2 could easily be downloaded from each individual site without any additional interaction and closely imitated one of the previous operations (TweetyChat).

BlackBerry researchers attempted to initiate a conversation with CONFUCIUS but were shut down pretty quickly, as seen in the figure below. Obviously, the time zone difference didn't help, but it also seemed CONFUCIUS did not want to provide the Android payload to us, or to chat:

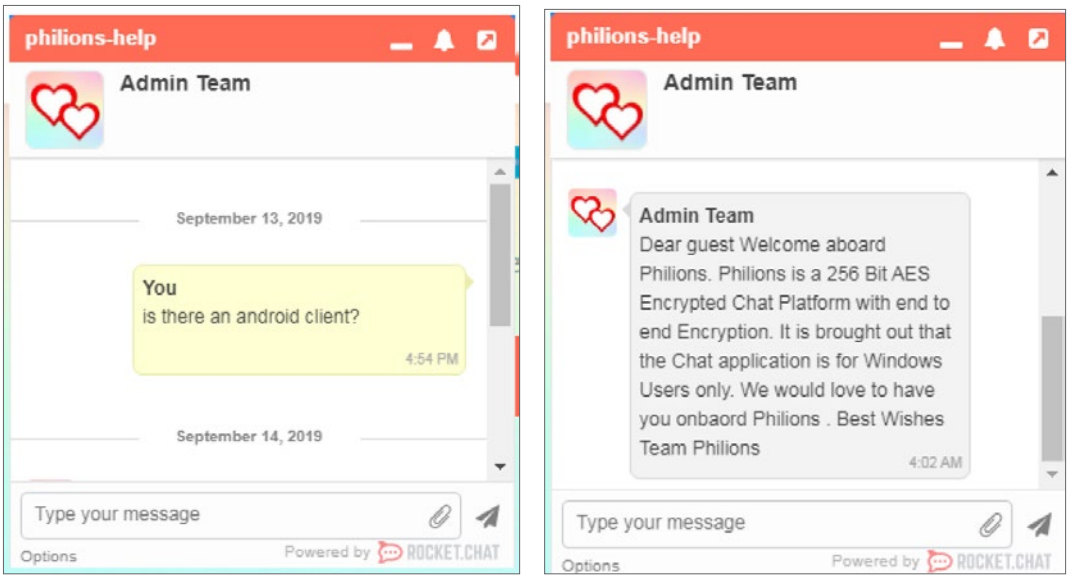


Figure 3: BlackBerry Gets Rejected by CONFUCIUS

Other fake apps distributed by CONFUCIUS in this campaign carried a more serious tone, including one that promised news about the crisis in Kashmir referenced above in the beginning of this section.

Though espionage campaigns that do not bear the identity of the threat actor frequently do not interest the press, operations like the two described above are arguably more disconcerting. BITTER and CONFUCIUS bear all the hallmarks of government-sponsored resources and targeting priorities. Their operations reveal a mature skillset that fluently interweaves both desktop and mobile malware, as well as infrastructure and delivery methods for each. CONFUCIUS took the extra step to develop realistic web pages and supporting applications to provide an additional level of deception.

In stark contrast to nearly every other government-related APT mobile campaign discussed in this overview, this one bore no overt political motivation. Instead what BlackBerry researchers found was conventional yet sophisticated espionage targeting the nation's military and government.

Conclusion

Conclusion

This report is intended to provide a detailed survey of the strategic and tactical use of mobile malware by various governments. It attempts to fill in gaps from earlier research on the subject of mobile malware to offer a new and redefined understanding of nation-state APT operations. The conclusions drawn here are intelligence assessments representing judgments based on available data.

Taken together, this report provides an examination of the complex nature of mobile espionage campaigns deployed by different governments, revealing that previously held perceptions were both shallow and incomplete. When the term APT comes to mind, everyone naturally tends to explore what's familiar: Windows, Mac, Linux, or the occasional odd industrial control system.

But as this report shows, the mobile space was already under attack for some time. In many regards, mobile surveillance has always been an ingredient of individual nation-state's APT operations. Attacks on Android and iOS will undoubtedly become more prevalent and blended into traditional desktop-centric operations.

The evidence is all around just waiting to be uncovered. Even so, the security solutions, antivirus software, and incident response services that might have detected these operations are only now starting to appear in a significant way. Mobile security is definitely an area that needs to be more fully addressed, but we are already a decade behind.

The public-facing security research on targeted mobile threats has pioneered a new way forward. Good mobile research was sporadically published in the past and, in many cases, presented as a niche phenomenon — another subdiscipline for specialization. Research that examines threats holistically is hard to come by.

BlackBerry hopes this report conveys a deeper appreciation for how the Chinese, Vietnamese, Iranians, North Koreans and other state-backed groups view, implement and execute upon their mobile strategies. Although considerably different, those strategies had a common denominatora — they all approached the mobile facet in a way that ran counter to how the overwhelming majority of the security industry treats it. All the APT groups BlackBerry surveyed purposefully interwove mobile malware into their espionage operations not as a niche effort, but as a holistic one.

Looking ahead, businesses and other organizations that are grappling with how to build resilience against a relentless onslaught of cyber espionage campaigns would do well to adjust their strategy to incorporate mobile defense, both for company-issued smartphones as well as those permitted for use in a "bring your own device" plan.

Governments and policy experts hard at work defining deterrence strategies, cyber norms and red lines in the international community will be challenged by what the findings reveal and portend regarding the incorporation of mobile threats into the broader espionage picture. There is considerably more than is covered in this comprehensive report to reveal and comprehend.

Works Cited

AFP. (2017, July 14). *China Orders Xinjiang's Android Users to Install App That Deletes 'Terrorist' Content.* Retrieved from Radio Free Asia: https://www.rfa.org/english/news/china/china-orders-xinjiangs-android-users-to-install-app-that-deletes-terrorist-content-07142017102032.html

Alyac. (2019, August 5). 금성121 APT 조직, 스테가노그래피 기법과 스마트폰 노린 퓨전 공격 수행 출처. Retrieved from Alyac Blog: https://blog.alyac.co.kr/2452

Alyac. (2019, August 3). 금성121 조직, 라자루스로 위장한 APT '이미테이션 게임' 등장 출처. Retrieved from ESTsecurity: https://blog.alyac.co.kr/2453

Anderson, C., & Sadjadpour, K. (2018, January 4). *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

Antiy PTA Team. (2019, August 1). *Analysis of the Attack of Mobile Devices by OceanLotus.* Retrieved from Antiy Labs: https://www.antiy.net/p/analysis-of-the-attack-of-mobile-devices-by-oceanlotus/

Baumartner, K., Raiu, C., & Maslennikov, D. (2013, March 26). *Android Trojan Found in Targeted Attack*. Retrieved from Kaspersky SecureList: https://securelist.com/android-trojan-found-in-targeted-attack-58/35552/

Beer, I. (2019, August 29). *A very deep dive into iOS Exploit chains found in the wild.* Retrieved from Google Project Zero: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

BlackBerry Threat Intelligence Team. (2019, May 14). *Reaver: Mapping Connections Between Disparate Chinese APT Groups. Retrieved from :* https://threatvector..com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

Boehler, P., & Sam, C. (2014, September 17). *Fake Occupy Central app targets activists' smartphones with spyware.* Retrieved from South China Morning Post: https://www.scmp.com/news/hong-kong/article/1594667/fake-occupy-central-app-targets-activists-smartphones

Bowe, A. (2018, August 24). *China's Overseas United Front Work — Background and Implications for US.* Retrieved from US-China Economic and Security Review Commission: https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf

Bublil, S., Brodie, D., & Bashan, A. (2014, September 30). *Lacoon Discovers Xsser mRAT, the First Advanced Chinese iOS Trojan.* Retrieved from Check Point Blog: https://blog.checkpoint.com/2014/09/30/lacoon-discovers-xsser-mrat-first-advanced-ios-trojan/

Case, A., Meltzer, M., & Adair, S. (2019, September 2). *Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs.* Retrieved from Volexity: https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

Check Point Research. (2018, September 7). *Domestic Kitten: An Iranian Surveillance Operation.* Retrieved from Check Point Research: https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/

Check Point Research. (2018, October 23). *Zooming In On "Domestic Kitten"*. Retrieved from Check Point Research: https://research.checkpoint.com/zooming-in-on-domestic-kitten/

Cox, J. (2018, April 9). *Chinese Government Forces Residents To Install Surveillance App With Awful Security.* Retrieved from Motherboard: https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang

Dalek, J., Alexander, G. C.-N., & Brooks, M. (2017, July 5). *An intrusion campaign targeting Chinese language news sites.* Retrieved from Citizen Lab: https://citizenlab.ca/2017/07/insider-information-an-intrusion-campaign-targeting-chinese-language-news-sites/

Dr. Web Antivirus. (2019, July 12). *Android.Backdoor.736.origin.* Retrieved from Dr. Web: https://vms.drweb.com/virus/?i=18042563&lng=en

Fagerland, S. (2012, August 18). *The Chinese Malware Complexes: The Maudi Surveillance Operation.* Retrieved from SeeBug: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2012/NormanShark-MaudiOperation.pdf

Flacone, R., Scott, M., & Cortes, J. (2015, November 24). *Attack Campaign on the Government of Thailand Delivers Bookworm Trojan.* Retrieved from PaloAlto Networks Unit42: https://unit42.paloaltonetworks.com/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/

Flossman, M. (2017, August 31). *Lookout discovers sophisticated xRAT malware tied to 2014 "Xsser / mRAT" surveillance campaign against Hong Kong protesters.* Retrieved from Lookout Blog: https://blog.lookout.com/xrat-mobile-threat

Greenberg, A. (2019, September 3). *Why 'Zero Day' Android Hacking Now Costs More Than iOS Attacks.* Retrieved from WIRED: https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/

Guarnieri, C., & Anderson, C. (2016, August 24). *Increased Use of Android Malware Targeting Journalists.* Retrieved from Iran Threats: https://iranthreats.github.io/resources/android-malware/

Hamacher, A. (2019, September 2). *Hong Kong Protests Are Accelerating Bitcoin Adoption.* Retrieved from Yahoo! Finance: https://finance.yahoo.com/news/hong-kong-protests-accelerating-bitcoin-184623552.html

Han, I. (2017, November 20). *Android Malware Appears Linked to Lazarus Cybercrime Group.* Retrieved from McAfee: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/

Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). *Chinese Industrial Espionage: Technology acquisition and military modernization.* Abingdon: Routledge.

Hegel, T. ". (2018, May 3). *Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers.* Retrieved from 401TRG: https://401trg.com/burning-umbrella/

Kasza, A., Cortes, J., & Yates, M. (2017, November 20). *Operation Blockbuster Goes Mobile.* Retrieved from PaloAlto Networks Unit 42: https://unit42.paloaltonetworks.com/unit42-operation-blockbuster-goes-mobile/

Lancaster, T., & Yates, M. (2016, September 28). *Confucius Says…Malware Families Get Further By Abusing Legitimate Websites.* Retrieved from PaloAlto Networks Unit42: https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

Livelli, K., Smith, R., & Gross, J. (2018, November 12). *The White Company: Operation Shaheen.* Retrieved from : https://www..com/content/dam/-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf

Lunghi, D., & Horejsi, J. (2018, February 13). *Deciphering Confucius' Cyberespionage Operations.* Retrieved from TrendMicro Blog: https://documents.trendmicro.com/assets/research-deciphering-confucius-cyberespionage-operations.pdf

Lunghi, D., & Horejsi, J. (2019, June 10). *New MuddyWater Activities Uncovered.* Retrieved from TrendMicro Research: https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

Lunghi, D., & Jaromir, H. (2019, January 22). *Linking Cyberespionage Groups Targeting Victims in South Asia.* Retrieved from First: https://www.first.org/resources/papers/tallinn2019/Linking_South_Asian_cyber_espionnage_groups-to-publish.pdf

Min, J. (2018, May 17). *Malware on Google Play Targets North Korean Defectors.* Retrieved from Mcafee Blog: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malware-on-google-play-targets-north-korean-defectors/

Mumay, B. (2019, July 11). *Opinion: What's next for journalism in the Erdogan era?* Retrieved from Deutsche Welle: https://www.dw.com/en/opinion-whats-next-for-journalism-in-the-erdogan-era/a-49554127-0

Novetta. (2016, February 24). *Operation Blockbuster.* Retrieved from *Operation Blockbuster*: https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Redman, J. (2019, June 16). *Bitcoin Trades for a Premium in Hong Kong During Protests.* Retrieved from Bitcoin.com: https://news.bitcoin.com/bitcoin-trades-for-a-premium-in-hong-kong-during-protests/

Smith, B. (2017, December 19). *Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats.* Retrieved from Microsoft Blog: https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/

Stokes, M., & Hsiao, R. (2013, October 14). *The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics.* Retrieved from Project 2049: https://project2049.net/2013/10/14/the-peoples-liberation-army-general-political-department-political-warfare-with-chinese-characteristics/

ThreatConnect Research Team. (2013, December 20). *ThreatConnect Gets to the Root of Targeted Exploitation Campaign.* Retrieved from TheatConnect Blog: https://threatconnect.com/blog/threatconnect-gets-root-targeted-exploitation-campaigns/

US-CERT. (2017). *HIDDEN COBRA — North Korean Malicious Cyber Activity.* Retrieved from US-CERT: https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity

Xu, E., & Guo, G. (2019, June 18). *Mobile Cyberespionage Campaign 'Bouncing Golf' Affects Middle East.* Retrieved from TrendMicro Blog: https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

Appendix:

Threat Actor #2 Details:
Domains:
huaian.bbmouseme[.]com
SHA256 Hashes:
63c9a6108c056cfd3962c2608d262384d65ac199d5ec480f6e8779e470915df8

DOMESTIC KITTEN Details:
Domains:
systemdriverupdate[.]com
ydownyload[.]net
ynewnow[.]net

IP Addresses:
46.4.143[.]130
62.112.8[.]37
62.112.8[.]174
89.38.98[.]49
137.74.157[.]150
162.248.247[.]172
178.32.113[.]166
178.162.203[.]102
178.162.203[.]178
185.81.98[.]43
185.81.98[.]44
185.81.98[.]45
190.2.144[.]140
190.2.145[.]145
195.248.243[.]65
198.50.220[.]44
212.8.249[.]107

SHA256 Hashes:
02d6ca25b2057f181af96d2837486b26231eaa496defdf39785b5222014ef209
039fc34ace1012eff687f864369540b9085b167f0d66023f3b94f280a7fdf8b7
0decfca211fa63010a36ed42cad54d6f262f9fe52123cf684b6b9400b91e275a
19e25eab993c71321576e22ff89f8f6cddf2cd2bc88f6a182834dd75b97f9892
3547224113e8a2f5e8eedbc46494769adf750962507a5a2cf153ebfe391b1350
35de26b494a99d7373e992bf6e5c11fc8236a4efa67adc61584e85f9ffecab43
3bfc116ed396e232dbc99e12a94ee2f7bfe3171d819a26fe345907ef3fc98e24
3d41830f943c31f69eb6ed7804cc18b289ba2172d258bd118a8503d120318d63
45ab522d313f52e5521c8675a8427e7671f096a6296a73a877d709049e4ed074
53e00f1e8d2d6aa2d8a0eda2bf2d924fbc6f67db12ac3238d7c4b4520de7fadc
54479fbb2f3c8c16714e526925537e738b1b586310c8d15ce10f33327392e879
5787723b2221464337e6bbe4200aab912f1f711447224e4e6c4c96c451ff41bf
6b59582a4b24a411aa922abb667dd99a8d76a75fd644eaa8c15830141a536be9
6bdefb392a2613ced97297efe6994f0dbfa1e085d80da9a6d82f8ce56980dd11
7f603216a0a7bae2c8cec65a800608ac22cfff8cd98c699677e44d36267a9798
8324266e25d6a8dbc6e561e035b9e713c3bd339ba9bb5e5b9d4f0821a0262510
9156f5bd322306c9038a3bc830e53e7b13c272e121fb70b3b8d7d9968fb97e4f
a96e07116a965c92cf3254837689bab58d65e5d954cc180d5ae7018a3ff1d29e
b1df569ad4686e16ec0c661733d56778f59cdb78207a3c2ad66df9b9828c84ab
ca730b8b355e44919629a958d940e77eb1b4cd0c1bbe2ab94a963222f2723f57

ccef7ca705b899fe337eda462d38216c414c0cfe41052dec102c8f6d8876ad8a
d90168d1f3568b5909d2e14288300ede298f6c663b51e883e7eb5d8d70277423
e32fb3d0f54126e192c9d39c8ef31ac04c868f0cdbbe9a19d7b2ce66a4732aa2
e391dac157812061803c3c4d8873a31ab395d2f0b95c00d2b707e7f5e8fd6086
f1728125f37ca8738b19b418a3fe896e9bdcde5aed6559db3eea55f4e17602c4
fb22508e5d5224711fe2c23858b90b710f3cd2728a24deb309bc4cd77641e608

OCEANLOTUS Mobile Infrastructure Details:
Historic Domains:
aki.viperse[.]com
ckoen.dmkatti[.]com
game2015[.]net
gameandroid.taiphanmemfacebookmoi[.]info
itpk.mostmkru[.]com
jang.goongnam[.]com
ming.chujong[.]com
mokkha.goongnam[.]com
nhaccuatui.android.zyngacdn[.]com
quam.viperse[.]com
sadma.knrowz[.]com
taiphanmemfacebookmoi[.]info
ulse.chujong[.]com

Historic IP Addresses:
46.183.221[.]188
46.183.221[.]189
46.183.221[.]190
185.29.8[.]24

Current Domains:
science.tayenthflores[.]com
fp.rentwoylas[.]com
heal.lancebarkerwa[.]com
wand.gasharontomholt[.]com
term.ursulapaulet[.]com
inc.graceneufville[.]com
video.viodger[.]com
cloud.anofrio[.]com
traits.senapusmireault[.]com
status.elizongham[.]com
art.yfieldrainasch[.]com
doc.rainaschiffer[.]com

Current IP Addresses:
45.9.239[.]34
45.9.239[.]45
45.9.239[.]77
45.9.239[.]110
82.112.184[.]197
176.107.181[.]128

There was one additional IP address which matched unique attributes of the other C2 servers and resided in the same Class C network: “45.9.239[.]139”; however, BlackBerry researchers were unable to locate any samples which communicated to this address.

BITTER:

Based upon SSL certificate similarities and other unique command-and-control attributes the following domains and IP addresses are also active and connected to this actor's mobile malware infrastructure:

Android C2 Domains:
activemobistore.ddns[.]net
cbyxhuxo663.ddns[.]net
flashnewsservice[.]org
wdibitmapservice[.]net

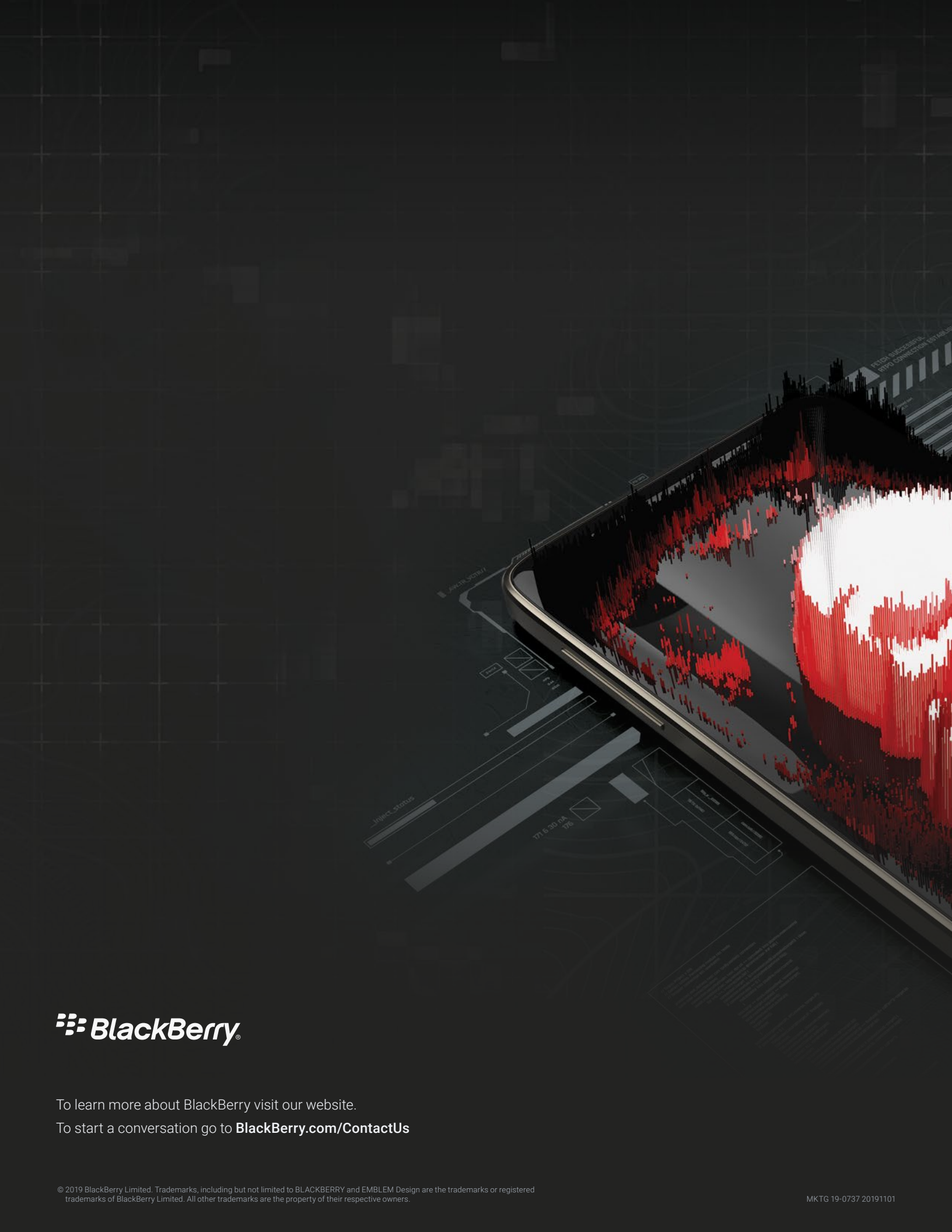
Android C2 IP Addresses:
172.81.132[.]172
172.81.132[.]102
172.81.132[.]49
89.249.65[.]150
108.62.118[.]219

PWNDROID2 SHA256 Hashes:
450e99d8516ff6f2f40afbf8fb8622d0f4b5c0af6311806a9500d8d298a56876
ac0e417c793215b6c0bcfefedd4aff6d374276475eea7aca58ce463f4d6dcf67
b2adc519cf1a8f8d429fd776d2d99aa2163cfa24f0c935c0ec075393805f9490

CONFUCIUS
Historic Mobile Domains:
nowhatsapp[.]com
web.nowhatsapp[.]com
myrocketchat[.]com
tweetychat[.]com
secretchatpoint[.]com
simplechatpoint.ddns[.]net

Current Mobile Domains:
android-helper[.]info
chatit[.]club
chaton[.]life
chaton[.]live
kahmir-n[.]com
kashmir-n[.]com
philionschat[.]com
sync.chatit[.]club

Hashes:
SHA256:
cdd03568a2672f65380f179a6412fd9a24a8198d4059a2990024431d7cbfb76c
(myrocketchat[.]com)



BlackBerry

To learn more about BlackBerry visit our website.

To start a conversation go to **BlackBerry.com/ContactUs**

MKTG 19-0737 20191101