Dark Caracal

Cyber-espionage at a Global Scale

Executive Summary

As the modern threat landscape has evolved, so have the actors. The barrier to entry for cyber-warfare has continued to decrease, which means new nation states – previously without significant offensive capabilities[1] – are now able to build and deploy widespread multi-platform cyber-espionage campaigns.

This report uncovers a prolific actor with nation-state level advanced persistent threat (APT) capabilities, who is exploiting targets globally across multiple platforms. The actor has been observed making use of desktop tooling, but has prioritized mobile devices as the primary attack vector. This is one of the first publicly documented mobile APT actors known to execute espionage on a global scale.

Lookout and Electronic Frontier Foundation (EFF) have discovered Dark Caracal[2], a persistent and prolific actor, who at the time of writing is believed to be administered out of a building belonging to the Lebanese General Security Directorate in Beirut. At present, we have knowledge of hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information. We are releasing more than 90 indicators of compromise (IOC) associated with Dark Caracal including 11 different Android malware IOCs; 26 desktop malware IOCs across Windows, Mac, and Linux; and 60 domain/IP based IOCs.

Dark Caracal targets include individuals and entities that a nation state might typically attack, including governments, military targets, utilities, financial institutions, manufacturing companies, and defense contractors. We specifically uncovered data associated with military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions during this investigation. Types of data include documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data.

The joint Lookout-EFF investigation began after EFF released its Operation Manul report, highlighting a multi-platform espionage campaign targeted at journalists, activists, lawyers, and dissidents who were critical of President Nursultan Nazarbayev's regime in Kazakhstan. The report describes malware and tactics targeting desktop machines, with references to a possible Android component. After investigating related infrastructure and connections to Operation Manul, the team concluded that the same infrastructure is likely shared by multiple actors and is being used in a new set of campaigns.

The diversity of seemingly unrelated campaigns that have been carried out from this infrastructure suggests it is being used simultaneously by multiple groups. Operation Manul clearly targeted persons of interest to Kazakhstan, while Dark Caracal has given no indication of an interest in these targets or their associates. This suggests that Dark Caracal either uses or manages the infrastructure found to be hosting a number of widespread, global cyber-espionage campaigns.

Since 2007, Lookout has investigated and tracked mobile security events across hundreds of millions of devices around the world. This mobile espionage campaign is one of the most prolific we have seen to date. Additionally, we have reason to believe the activity Lookout and EFF have directly observed represents only a small fraction of the cyber-espionage that has been conducted using this infrastructure.

[1] https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

[2] In keeping with traditional APT naming, we chose the name "Caracal" (pronounced [kar-uh-kal]) because the feline is native to Lebanon and because this group has remained hidden for so long. From the Wikipedia entry "the caracal is highly secretive and difficult to observe" and "is often confused with [other breeds of cat]." The naming further builds on EFF's "Operation Manul," another feline reference. We like cats.

Key Findings

Lookout and EFF researchers have identified a new threat actor, Dark Caracal.

- Our research shows that Dark Caracal may be administering its tooling out of the headquarters of the General Directorate of General Security (GDGS) in Beirut, Lebanon.
- The GDGS gathers intelligence for national security purposes and for its offensive cyber capabilities according to previous reports.
- We have identified four Dark Caracal personas with overlapping TTP (tools, techniques, and procedures).
- Dark Caracal is using the same infrastructure as was previously seen in the Operation Manul campaign, which targeted journalists, lawyers, and dissidents critical of the government of Kazakhstan.

Dark Caracal has been conducting a multi-platform, APT-level surveillance operation targeting individuals and institutions globally.

- Dark Caracal has successfully run numerous campaigns in parallel and we know that the data we have observed is only a small fraction of the total activity.
- We have identified hundreds of gigabytes of data exfiltrated from thousands of victims, spanning 21+ countries in North America, Europe, the Middle East, and Asia.
- The mobile component of this APT is one of the first we've seen executing espionage on a global scale.
- Analysis shows Dark Caracal successfully compromised the devices of military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions.
- Dark Caracal targets also include governments, militaries, utilities, financial institutions, manufacturing companies, and defense contractors.
- Types of exfiltrated data include documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data.
- Dark Caracal follows the typical attack chain for cyber-espionage. They rely primarily on social media, phishing, and in some cases physical access to compromise target systems, devices, and accounts.

Dark Caracal Activity Timeline

Jan. 2012 — First mobile surveillance campaign, oldb, launched

Nov. 2012 — op13@mail[.]com registers phishing domain arablivenews[.]com

Mar. 2014 — Custom FinFisher mobile sample created

Nov. 2014 — arablivenews[.]com expires and is decommissioned

Dec. 2015 — op13@mail[.]com registers arabpublishershlb[.]com domain

Jun. 2015 — Operation Manul phishing emails first seen

Jun. 2016 — gmailservices[.]org and twiterservices[.]org WHOIS details registered as Hadi Mazeh and op13@mail[.]com

Aug. 2016 — EFF releases "Operation Manul" report

Oct. 2016 — op13@mail[.]com registered arablivenews[.]com. Threat Connect report[3] suggests domain may be related to "APT 28"

Dec. 2016 — secureandroid[.]info watering hole goes live.

Dec. 2016 — Second mobile surveillance campaign, wp7, launched

[3] "https://www.threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/"

Dark Caracal uses tools across mobile and desktop platforms.

- Dark Caracal uses mobile as a primary attack platform.
- Dark Caracal purchases or borrows mobile and desktop tools from actors on the dark web.
- Lookout discovered Dark Caracal's custom-developed mobile surveillanceware (that we call Pallas) in May 2017. Pallas is found in trojanized Android apps.
- Dark Caracal has also used FinFisher, a tool created by a "lawful intercept" company that is regularly abused by other nation-state actors.
- Dark Caracal makes extensive use of Windows malware called Bandook RAT. Dark Caracal also uses a previously unknown, multi-platform tool that Lookout and EFF have named CrossRAT, which is able to target Windows, OSX, and Linux.

Dark Caracal uses a constantly evolving, global infrastructure.

- Lookout and EFF researchers have identified parts of Dark Caracal's infrastructure, providing us with unique insight into its global operations.
- The infrastructure operators prefer to use Windows and XAMPP software on their C2 servers rather than a traditional LAMP stack, which provides a unique fingerprint when searching for related infrastructure.
- Lookout and EFF have identified infrastructure shared by Operation Manul and Dark Caracal as well as other actors.
- Attributing Dark Caracal was difficult as the actor employs multiple types of malware, and our analysis suggests the infrastructure is also being used by other groups.

Lookout and EFF are releasing more than 90 indicators of compromise (IOC):

- 11 Android malware IOCs
- 26 desktop malware IOCs
- 60 domains, IP Addresses, and WHOIS information

Dark Caracal Activity Timeline (cont.)

Mar. 2017	Third mobile surveillance campaign, wp8, launched
Apr. 2017	Fourth mobile surveillance campaign, wp9, launched
Jun. 2017	Fifth and sixth mobile surveillance campaigns, wp10 and wp10s, launched
Jul. 2017	wp8 campaign ceases collecting data
Jul. 2017	adobeair[.]net taken down for several dayss
Jul. 2017	adobeair[.]net resumes operations
Aug. 2017	wp9, wp10, and wp10s campaigns cease collecting data
Aug. 2017	adobeair[.]net WHOIS details changed to Nancy Razzouk, op13@mail[.]com, Lebanon
Aug. 2017	oldb campaign ceases collecting data
Sep. 2017	wp7 campaign ceases collecting data
Sep. 2017	adobeair[.]net changes hosting and is secured against data leaks
Dec. 2017	Secureanroid[.]info's domain name expires
Jan. 2018	Dark Caracal made public

About Lookout

Lookout is a cybersecurity company for a world run by apps. Powered by the largest dataset of mobile code in existence, Lookout is the security platform of record for mobile device integrity and data access. Lookout is trusted by hundreds of millions of individuals, hundreds of enterprises and government agencies, and such ecosystem partners as AT&T, Deutsche Telekom, and Microsoft. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

Lookout Website
www.lookout.com

Blog
blog.lookout.com

Email
threatintel@lookout.com

Twitter
@lookout

About EFF

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

EFF Website
www.eff.org

Blog
www.eff.org/deeplinks

Email
press@eff.org

Twitter
@eff

Contributors

Andrew Blaich, Lookout
Apurva Kumar, Lookout
Jeremy Richards, Lookout
Michael Flossman, Lookout

Cooper Quintin, EFF
Eva Galperin, EFF

Special thanks to the many others in our organization, and to our partners, who contributed significantly to this work.