Dark Caracal: Good News and Bad News

BY GENNIE GEBHART | JANUARY 19, 2018

ENGLISH

Yesterday, EFF and Lookout announced a new report, Dark Caracal, that uncovers a new, global malware espionage campaign. One aspect of that campaign was the use of malicious, fake apps to impersonate legitimate popular apps like Signal and WhatsApp. Some readers had questions about what this means for them. This blog post is here to answer those questions and dive further into the Dark Caracal report.

Read the full Dark Caracal report here

First, the good news: **Dark Caracal does not mean that Signal or WhatsApp themselves are compromised in any way.** It only means that attackers found new, insidious ways to create and distribute fake Android versions of them. (iOS is not affected.) If you downloaded your apps from Google's official app store, Google Play, then you are almost certainly in the clear. The threat uncovered in the Dark Caracal report referred to "trojanized" apps, which are fake apps that pretend to look like real, trusted ones. These malicious spoofs often ask for excessive permissions and carry malware. Such spoofed versions of Signal and WhatsApp were involved in the Dark Caracal campaign.

The malicious actors behind Dark Caracal got these fake, malicious apps onto people's phones by spearphishing. Several types of phishing emails directed people—including military personnel, activists, journalists, and lawyers—to go to a fake app store-like page, where fake Android apps waited. There is even evidence that, in some cases, Dark Caracal used physical access to people's phones to install the fake apps. Again, if you downloaded your apps from the official app store, you can rest easy that this has likely not affected you.

And now the bad news: Dark Caracal has wide-reaching implications for how state-sponsored surveillance and malware works. Most people do not have to worry about this very specific threat. But for the small minority of users who may be directly targeted by nation-states or other skilled, motivated adversaries—and for the malware researchers who try to track those adversaries down—the Dark Caracal report uncovers a new infrastructure that makes it even harder to attribute attacks and malware campaigns to a particular nation or actor. More details are available in the report.

Dark Caracal is also a reminder that most modern hacking requires the unwitting participation of the user. The most dangerous thing in the online environment is not necessarily complex, headline-grabbing vulnerabilities, but well-crafted phishing messages and fake apps that trick users into handing over log-in credentials and granting excessive permissions. Keep an eye out for links, attachments, and apps pretending to be something they're not, and make sure your friends, neighbors, and others in your community are informed too.

RELATED ISSUES:

STATE-SPONSORED MALWARE

SECURITY EDUCATION

RELATED UPDATES

PRESS RELEASE | OCTOBER 22, 2019

EFF and Partners Urge U.S. Lawmakers to Support New DoH Protocol for a More Secure Internet

San Francisco—The Electronic Frontier Foundation (EFF) today called on Congress to support implementation of an Internet protocol that encrypts web traffic, a critical tool that will lead to dramatic improvements in user privacy and help impede the ability of governments to track and censor people.EFF, joined by Consumer Reports and...

DEEPLINKS BLOG BY COOPER QUINTIN, THREAT LAB | SEPTEMBER 9, 2019

Watering Holes and Million Dollar Dissidents: the Changing Economics of Digital Surveillance

Recently, Google's Project Zero published a report describing a newly-discovered campaign of surveillance using chains of zero day iOS exploits to spy on iPhones. This campaign employed multiple compromised websites in what is known as a "watering hole" attack. The compromised websites would automatically run the chain of exploits...

DEEPLINKS BLOG BY KATITZA RODRIGUEZ | DECEMBER 30, 2018

Where Governments Hack Their Own People and People Fight Back: 2018 in Review

Throughout 2018, new surveillance practices continued to erode the privacy of people in Latin America. Yet local and regional digital rights organizations continue to push back with strategic litigation, journalists and security researchers investigate to shed light on government use of malware, and local activists work tirelessly to fight overarching...

DEEPLINKS BLOG BY SYDNEY LI | MARCH 12, 2018

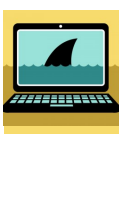
We Still Need More HTTPS: Government Middleboxes Caught Injecting Spyware, Ads, and Cryptocurrency Miners

Last week, researchers at Citizen Lab discovered that Sandvine's PacketLogic devices were being used to hijack users' unencrypted internet connections, making yet another case for encrypting the web with HTTPS. In Turkey and Syria, users who were trying to download legitimate applications were instead served malicious software...

PRESS RELEASE | JANUARY 18, 2018

EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World

San Francisco – The Electronic Frontier Foundation (EFF) and mobile security company Lookout have uncovered a new malware espionage campaign infecting thousands of people in more than 20 countries. Hundreds of gigabytes of data has been stolen, primarily through mobile devices compromised by fake secure messaging clients. The ...



DEEPLINKS BLOG BY EVA GALPERIN | DECEMBER 27, 2017

Nation-State Hacking: 2017 in Review

If 2016 was the year government hacking went mainstream, 2017 is the year government hacking played the Super Bowl halftime show. It's not Fancy Bear and Cozy Bear making headlines. This week, the Trump administration publicly attributed the WannaCry ransomware attack to the Lazarus Group, which allegedly works...

EFF IN THE NEWS

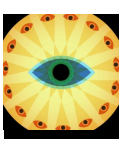
FBI allays some critics with first use of new mass-hacking warrant

The Electronic Frontier Foundation, for example, commended the feds for asking a judge to review exactly what data the FBI would and would not touch in victimized devices, which were located across the country. It was a "positive step" toward accountability and transparency in FBI computer break-ins, EFF staff attorney...

PRESS RELEASE | APRIL 13, 2017

EFF Urges Court to Roll Back Ruling Allowing Remote-Control Spying

Washington, D.C. – The Electronic Frontier Foundation (EFF) urged an appeals court today to review a dangerous decision by a three-judge panel that would allow foreign governments to spy on Americans on U.S. soil—just as long as they use technology instead of human agents. In *Kidane v. Ethiopia*...



DEEPLINKS BLOG BY NATE CARDOZO | MARCH 14, 2017

D.C. Circuit Court Issues Dangerous Decision for Cybersecurity: Ethiopia is Free to Spy on Americans in Their Own Homes

The United States Court of Appeals for the District of Columbia Circuit today held that foreign governments are free to spy on, injure, or even kill Americans in their own homes--so long as they do so by remote control. The decision comes in a case called ...

EFF IN THE NEWS

The secret world of vulnerability hunters

As with any tool designed for military and civilian uses, there are dangers of these hacking programs falling into the wrong hands. To be sure, the misuse of government-grade exploits unnerves many civil liberties groups. "Governments shouldn't be able to use them to crack down on free speech or dissidents,"...