Dark Caracal: You Missed a Spot

eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot

By Cooper Quintin and Eva Galperin December 10, 2020

Security researchers at EFF have tracked APTs (Advanced Persistent Threats) targeting civil society for many years now. And while in many cases, the “advanced” appellation is debatable, “persistent” is not. Since 2015, EFF has tracked the cyber-mercenaries known as Dark Caracal, a threat actor who has carried out digital surveillance campaigns on behalf of government interests in Kazakhstan and Lebanon.

Recent activity seems to indicate that this actor is active once again. In November of 2019 the group Malware Hunter Team discovered new samples of the Bandook malware which is associated with Dark Caracal. This time with legitimate signing certificates for Windows (issued by the "Certum" certificate authority,) which would allow them to be run without a warning to the user on any Windows computer. Tipped off by the emergence of new variants of the Bandook Trojan, researchers at Checkpoint found three new variants of Bandook: some expanded (120 commands), some slimmed down (11 commands), and all signed with Certum certificates. The Checkpoint researchers also discovered several new command and control domains in use by Dark Caracal.

In previous campaigns, this actor has displayed impressively lax operational security, enabling researchers to download terabytes of data from their command and control servers. The latest campaign exhibits a somewhat higher level of opsec. Checkpoint reports that targets included "Government, financial, energy, food industry, healthcare, education, IT and legal institutions" in the following countries: Singapore, Cyprus, Chile, Italy, USA, Turkey, Switzerland, Indonesia and Germany.

Recommended Mitigations against Dark Caracal

The Dark Caracal threat actors still seem to primarily use phishing and Office-based macros as their primary method of infection. Because of this, the best step one can take to protect against Dark Caracal is to disable Office macros on your personal devices or that of your entire organization. This is additionally a good basic security hygiene practice. Standard methods to avoid phishing attacks are also good practice. Readers may also take some comfort in the fact that Bandook is currently detected by many, if not most, antivirus products.

The Bandook Trojan

One of the primary signatures of the Dark Caracal threat group is their use of the Bandook Trojan, which is described in the Checkpoint report as follows:

> The final payload in this infection chain is a variant of an old full-featured RAT named Bandook. Written in both Delphi and C++, Bandook has a long history, starting in 2007 as a commercially available RAT that was developed by a Lebanese individual nicknamed PrinceAli.
>
> Bandook's execution flow starts with a loader, written in Delphi, that uses the Process Hollowing technique to create a new instance of an Internet Explorer process and inject a malicious payload into it. The payload contacts the C&C server, sends basic information about the infected machine, and waits for additional commands from the server.

These findings are consistent with what EFF previously published in our Dark Caracal and Operation Manul reports.

We were surprised to see the Checkpoint report when it was released on Thanksgiving as we had been tracking Dark Caracal again as well. Building on Checkpoint's work, we are publishing additional indicators of compromise we have observed that may be of interest to other security professionals and malware researchers.

Additional Dark Caracal Indicators of Compromise

Hashes:
09187675a604ffe69388014f07dde2ee0a58a9f7b060bff064ce00354fedc091
0c5735e066bfbc774906942e97a6ffc95f36f88b9960c4dd6555247b3dd2cdb0
2106e0eabc23d44bd08332cf0c34f69df36b9e84a360722a7fd4d62c325531d1
211f1638041aa08762a90c15b1aff699d47e4da21429c22b56f8a3103d13b496
27306de878f7ab58462b6b9436474e85c3935a5b285afec93f4b59a62c30dd32
2b54f945f5e3d226d3a09cdfcc41e311b039ceadf277310697672c8c706aa912
2f9ba191689e69e9a4f79b96d66c0fee9626fbd0ea11e89c0129e5d13afe6d76
3c8ad8264d7ce9c681c633265b531abb4cf9b64c2e1a3befadc64e66e1b5632e
4175c7f8854e2152462058a3e2f23a9026477f9b8001923e2c59b195949070f5
4f2ebe6f4fc345041643d5d7045886956fe121272fa70af08498a27135a72d97
520ead3a863d4ea139f93bbad4d149a37ca766b38af0567f1f31a9205613b824
614d0bece286af47db5a9f17d24778b16e30fea10ab8d4c7f0739246b83d8366
6e79e2a567013cbeea1d13f3e6c883e56e66ab36de88802eb1313736c25293ec
76f9615ce6ce6d20a9404b29649a4987a315c6b6fc703fa289da0aae37d39bce
a5b1ba27edee6953fa30771090387a5aca3e4d4541973df9b2e2b535444db5c3
b8c1cb11108d62611ac8035701eea8bb90b55faff2d0a28c23e2dcced176a52f
c4cba54bf57b3bc3bc8f1d71a7d78fcf25eae18d1d96ba4a4fa5eb8d6fb05e08
c852ebf981daa4d17216a569425b6128f5f7f56d746d4aa03ffecef53fb2829b
c8cbded2f6a5792c147a3362a4deb01a54a13fe9b5636367f2bb39084ed6e13a
cdf6413b56618cd641f93c2ca7fa000c486f7f2455daa3e25459e0d1e72ecf45
d50696eec5288f29994aa68b8f38c920f388a934f23855fb516fa94223c29ecc
d6de67f2187d2fad2d88ca3561aa9f9bf3cecf2e303916df0fc892ed97d94ff5
f08cbc1c5bca190bc34f7da3ad022d915758f5eb2c0902b13c44d50129763cf1
f3b54507a82a17f4056baaa3cb24972a2dfa439fa9b04493db100edb191a239f
fe18568eb574d8fa6c7d9bd7d8afa60d39aae0e582aff17c5986f9bab326ec8a

Unpacked bandook sample:
fabce973a9edff2c62ccb6fdd5b14c422bc215284f952f6b31cc2c7d98856d57

Bandook user-agent:
User-Agent: Mozilla/4.0 (compatible; ALI)
User-Agent: Uploador

Command and Control URLs:

hxxp://blancomed.com/newnjususus1/post.php
hxxp://blancomed.com/newnjususus2/post.php
hxxp://blancomed.com/newnjususus4/post.php
hxxp://blancomed.com/newnjususus5/post.php
hxxp://blombic.com/OSPSPSPS2222292929nnnxnxnxnxnx/add.php
hxxp://blombic.com/uioncby281229hcbc2728hsha11kjddhwqqqqc/add.php
hxxp://www.opwalls.com/tunnel2015/add.php
hxxps://blancomed.com/newnjususus1/post.php
hxxps://blancomed.com/newnjususus2/post.php
hxxps://blancomed.com/newnjususus3/post.php
hxxps://blancomed.com/newnjususus4/post.php
hxxps://blancomed.com/newnjususus5/post.php
hxxps://pronews.icu/aqecva/
hxxps://pronews.icu/aqecva/add.php
hxxps://pronews.icu/raxpafsd/images
hxxps://pronews.icu/phpmyadmin
hxxps://pronews.icu/cgi-bin

hxxp://wbtogm.com
/hc1/
/hc2/
/hc3/
/hc4/
/hc5/
/hc1/images/
/hc1/temp/
/hc1/vk/
/hc1/vk/19160/
/hc1/index.php
/hc1/search.php
/hc1/view.php
/hc1/tv.php
/hc1/test.php
/hc1/log.php
/hc1/get.php
/hc1/config.php
/hc1/cm.php
/hc1/auth.php
/hc1/chrome.php
/hc1/panel.php
/hc1/validate.php
/hc1/pws.php

/hc1/vk.php
/91SD8391AC/cap.abc
/91SD8391AC/pws.abc
/91SD8391AC/extra.abc
/91SD8391AC/tv.abc
/hc4/get.php?action=check
/91SD8391AC/ammyy.abc
/91SD8391AC/89911111111012

Command and Control Domains:
megadeb[.]com
blancomed[.]com
opwalls[.]com
blombic[.]com
wbtogm[.]com

Related Issues

State-Sponsored Malware

Tags

threat lab

Join EFF Lists

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Thanks, you're awesome! Please check your email for a confirmation link.

Oops something is broken right now, please try again later.

Related Updates

Deeplinks Blog by Karen Gullo | April 28, 2022

EFF Statement on the Declaration for the Future of the Internet

The White House announced today that sixty one countries have signed the Declaration for the Future of the Internet. The high-level vision and principles expressed in the Declaration—to have a single, global network that is truly open, fosters competition, respects privacy and inclusion, and protects human rights and fundamental...

Deeplinks Blog by Bill Budington | April 4, 2022

Anatomy of an Android Malware Dropper

Recently at EFF's Threat Lab, we've been focusing a lot on the Android malware ecosystem and providing tools for its analysis. We've noticed lot of samples of Android malware in the tor-hydra family have surfaced, masquerading as banking apps to lure unsuspecting customers into installing them. In this...

Legal Case

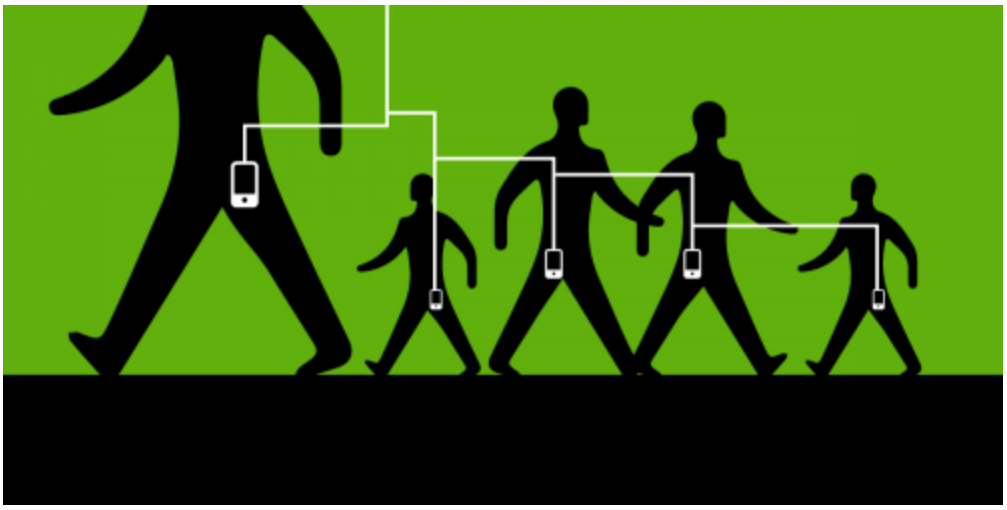
AlHathloul v. DarkMatter Group

EFF is representing prominent Saudi human rights activist Loujain AlHathloul in a lawsuit against spying software maker DarkMatter Group and three of its former executives for illegally hacking her iPhone to secretly track her communications and whereabouts.AlHathloul is among the victims of an illegal spying program created and run by...

Press Release | December 9, 2021

Saudi Human Rights Activist, Represented by EFF, Sues Spyware Maker DarkMatter For Violating U.S. Anti-Hacking and International Human Rights Laws

EFF filed a lawsuit today on behalf of prominent Saudi human rights activist Loujain AlHathloul against spying software maker DarkMatter Group and three of its former executives for illegally hacking her iPhone to secretly track her communications and whereabouts.



Deeplinks Blog by Cindy Cohn | July 20, 2021

Pegasus Project Shows the Need for Real Device Security, Accountability, and Redress for Those Facing State-Sponsored Malware

EFF has warned for years of the danger of the misuse of powerful state-sponsored malware. Until governments around the world get out of the way and actually support security for all of us, including accountability and redress for victims, these outrages will continue.

Deeplinks Blog by Bill Budington | May 13, 2021

FAQ: DarkSide Ransomware Group and Colonial Pipeline

With the attack on Colonial Pipeline by a ransomware group causing panic buying and shortages of gasoline on the US East Coast, many are left with more questions than answers to what exactly is going on. We have provided a short FAQ to the most common technical questions that are...

Deeplinks Blog by Cooper Quintin | September 25, 2020

Introducing "YAYA", a New Threat Hunting Tool From EFF Threat Lab

At the EFF Threat Lab we spend a lot of time hunting for malware that targets vulnerable populations, but we also spend time trying to classify malware samples that we have come across. One of the tools we use for this is YARA. YARA is described as "The Pattern...

Press Release | July 24, 2020

EFF to Court: Trump Appointee's Removal of Open Technology Fund Leadership Is Unlawful

San Francisco—The Electronic Frontier Foundation (EFF) today joined a group of 17 leading U.S.-based Internet freedom organizations in telling a federal appeals court that Trump administration appointee Michael Pack has no legal authority to purge leadership at the Open Technology Fund (OTF), a private, independent nonprofit that helps hundreds...

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, Mona Wang | 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...

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Thanks, you're awesome! Please check your email for a confirmation link.

Oops something is broken right now, please try again later.

Related Issues

State-Sponsored Malware

Related Tags

threat lab