Uncle Sow: Dark Caracal in Latin America

eff.org/deeplinks/2023/02/uncle-sow-dark-caracal-latin-america

By Cooper Quintin	February 10, 2023

Español

In 2018, EFF along with researchers from Lookout Security published a report describing the Advanced Persistent Threat (APT) we dubbed "Dark Caracal." Now we have uncovered a new Dark Caracal campaign operating since March of 2022, with hundreds of infections across more than a dozen countries. In this report we will present evidence that the cyber mercenary group Dark Caracal is still active and continues to be focused on Latin America, as was reported last year. We have discovered that Dark Caracal, using the Bandook spyware, is currently infecting over 700 computers in Central and South America, primarily in The Dominican Republic and Venezuela.

In our original 2018 report, we described a campaign targeting thousands of Lebanese citizens with several different malware families, including a brand new mobile remote access trojan we named Pallas and a Windows remote access trojan called Bandook. Through our research we were able to shut down the malware campaign and notify a number of the victims. Our Operation Manul report established that the actors behind the campaign were working with the governments of Lebanon and Kazakhstan. The variety of targets and the apparent involvement of multiple governments throughout the campaigns lead us to believe that Dark Caracal is a cyber-mercenary or hack-for-hire group.

Since our original Dark Caracal report, there have been multiple reports on their continued activities. Checkpoint Research wrote about a campaign in 2020 and we have continued to follow the activities of Dark Caracal with our most recent report, also in 2020. Most recently, ESET wrote about Dark Caracal activities in Latin America in their report Bandidos at Large.

Dark Caracal is far from the only malware group currently targeting Latin America. The Quantum malware group targeted the Dominican Republic’s Ministry of Agriculture in 2022. The Dominican Republic is also a reported customer of NSO group.

Given Dark Caracal’s history of working with national governments — such as Kazakhstan and Lebanon — on politically motivated campaigns, it is possible that the new campaign described below is also at the behest of a government actor, but without more insight into who the infected computers belong to, we cannot draw any conclusions as to the motivation of these attacks.

Regardless, we call on lawmakers and regulators in South and Central America to be vigilant against Dark Caracal's spyware since it, and other spyware like it, has been used to commit gross human rights violations. Time and again, nation-states and cyber-mercenaries have used spyware to target activists, human rights defenders, and journalists whose actual work is to uncover governments' wrongdoing, speak truth to power and hold governments accountable. Such targeting has resulted in a growing list of extrajudicial killings of journalists and human rights defenders.

Governments should consider calling for a moratorium on the governmental use of these malware technologies, support computer security research, and human rights for all, including transparency, accountability and redress for victims.

Governments must recognize that government hostility to device security is dangerous for their people. If one government can use malware against civilians under a rival government there is nothing stopping the rival government from doing the same. Governments should be focusing on improving computer security and protecting their citizens rights to freedom of expression.

We hope this report will add to a body of work exposing cyber mercenaries and convince policymakers that cyber mercenaries and nation-state hacking are truly a global threat to human rights and civil society.

A new campaign appears

Recently we discovered a new version of the Bandook malware, which has been updated to have 148 unique commands it can send the infected computer, far more than the 120 available in previous samples. This sample and related samples seem to be part of a campaign that began in March 2022, utilizing a new command and control server (a remote computer which issues orders to the infected computers and receives data stolen from the infected computers) at the domain `deapproved[.]ru`.

In the “Bandidos at Large” report, ESET researchers detailed a mechanism within Bandook for downloading Windows DLLs (software libraries for Windows) from a domain secondary to the main command and control server to gain additional functionality. On analyzing the samples we obtained, we found that in this case the mechanism for downloading additional DLLs pointed to the domain `unclesow[.]com`. However, upon investigating, we realized that the unclesow.com domain had not yet been registered. We figured that this domain could provide information on Dark Caracal’s activities, so we registered it and set up a sinkhole (a server which hosts a domain that previously belonged to a malware campaign to protect infected computers and collect information.)

Unclesow[.]com is currently hosted by EFF. Since registering this domain, we have been collecting aggregate information on the victims of this malware campaign. Based on daily traffic logs, there appear to be between 600 and 800 infected machines at any time, mostly across Central and South America. Since every Bandook infection connects to the secondary domain multiple times per day, we are confident that we are seeing all infections for this current campaign. Because of our concern for the privacy of the victims of this malware campaign we have configured the server to delete logs after four weeks and collect the bare minimum of necessary information.

The same day that we set up DNS entries for unclesow[.]com, several other domains that had been previously registered had their DNS suddenly pointed at the same server that hosted unclesow. There were 6 domains pointed automatically at our server:

```
setsizee[.]com
seconsave[.]com
scanlostt[.]com
sanesity[.]biz
Email-securlink[.]com
goadaaddy[.]com
```

Based on the timing and apparent phishing-related nature of these domains, we suspect this was an automatic process, possibly set up by the same people running the Dark Caracal campaign. A few days later, several of the domains were pointed at a new IP address not under our control. However, three of the domains (seconsave[.]com scanlostt[.]com and sensity[.]biz) still point to our sinkhole server. We were able to identify several other related domains which were hosted on other servers at the same time as these domains (when they were not pointing to our sinkhole.)

The connection of these domains to the current Dark Caracal campaign is unclear. They may be for a different campaign or another purpose The tactics and tools and procedures used don't match up, with the above domains being hosted on DigitalOcean registered with NameCheap and not mentioned in the Bandook samples, whereas the domains mentioned in the Bandook samples are hosted with the bulletproof hosting provider OvO [ovo.sc], and registered with a company called 1984 [1984.is]. Additionally, we observed no interesting traffic or traffic indicative of a Bandook infection to any of the domains pointed at our sinkhole other than unclesow[.]com. The only connection to this campaign for these domains is the fact that they were pointed at our sinkhole automatically when we set it up. For now it remains a mystery.

Since we registered the unclesow[.]com domain, the attackers have changed the command and control domain twice, first to cudenpower.co and then to bomes[.]ru. However, in both cases and still to this day, they have not changed the secondary infection domain from unclesow[.]com, thus our sinkhole continues to function even for new samples of malware. It is unclear whether the malware operators realize that their secondary domain is controlled by us at this time.

Bandook Continues Evolving

The versions of Bandook this campaign uses appear to be newer than the ones used in the last campaigns reported on by ESET. The first stage of the malware has switched from using GOST for encryption of the payload to using DES for encryption of its second stage payload. The key for decryption is derived from a passphrase by hashing it with the RIPEMD-128 algorithm.

Additionally the malware contains 148 possible commands it can send the infected computer from the command and control server instead of the previous 132 in the samples analyzed by ESET. The commands include capabilities such as: turning on the webcam, adding or removing files from the computer, taking control of the mouse, recording the screen, starting a remote desktop session, and downloading other libraries for additional functionality (see appendix for more.)

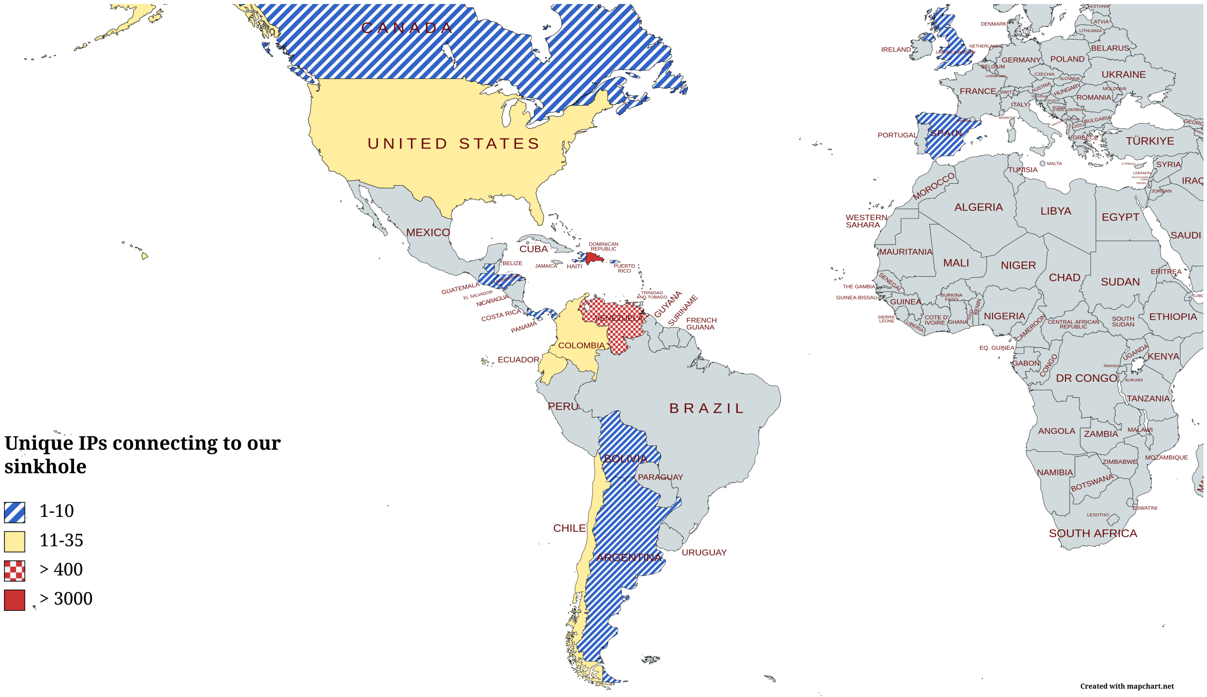
These changes indicate a deep nexus to the Dark Caracal group as the source code for Bandook is not public and the malware is not for sale as far as we know.

At the time of this report, unpacked versions of malware were detected by 41 out of 70 antivirus products in VirusTotal whereas a representative sample of the packed malware was detected by 35 out of 71 antivirus products.

The command and control servers are more locked-down than we have seen in the past, with the only open services being SSH and the command and control service listening on port 2222. There is no web administration interface as has been seen in the past.

Victimology

From connections to our sinkhole we have observed victims in several Central and South American countries. Approximately 75% of infected computers are located in The Dominican Republic and 20% in Venezuela.

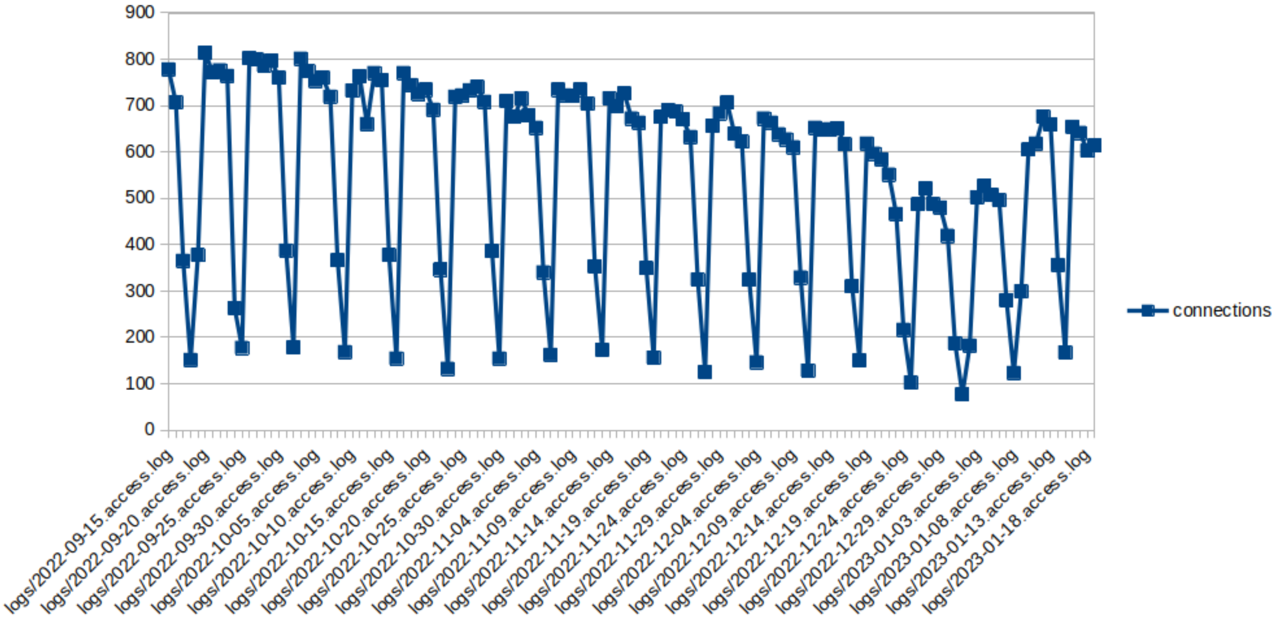


A map of Bandook infections based on Shodan Data.

Because the infected computers connect to the sinkhole server and make an http GET request for the path `` `/flras/get.php?huln=nevi` `` approximately every three hours we can reliably estimate the number of infected machines. At its peak we suspect more than 800 computers were infected in this malware campaign. However, this number may be lower if some machines are changing their IP addresses in the middle of the day due to moving to a new network or a dynamic IP address changing. Since all connections initiated by Bandook use a standard user agent (see Appendix) we do not have a way to keep track of individual machines when they change IP addresses.

Because Bandook malware samples have only ever been observed for Windows, we assume that the infected machines are all Windows computers. According to Shodan data, many of the IP addresses belong to commodity routers on consumer ISP networks. It is our assumption that those routers have dynamic IP addresses that frequently change, thus increasing the number of unique IPs connecting to our sinkhole.

Infections drop off on Saturdays and especially Sundays, leading us to believe that most infected machines are located at places of business. This hypothesis is also supported by the number of connections from infected machines dropping on major public holidays such as Christmas Eve, Christmas, and New Year's Day.



Number of infected computers connecting to our sinkhole per day

Though we haven't been able to contact any of the victims of this current campaign, their location opens the possibility that it is a continuation of the campaign outlined in the Bandidos at Large Report. Because of Dark Caracal's history of working on behalf of governments, we can't discount that possibility here either, though the client's identity remains a mystery for now.

Thanks to ESET, Martjin Grooten, Jeremy Kennely, Bill Marczak, and VirusTotal, for assistance with this research.

Appendix - Indicators of Compromise

Command and Control domains:

deapproved[.]ru
cudenpower[.]co
bomes[.]ru
cumumberpro[.]org
unclesow[.]com - SINKHOLED

Possibly Related Domains
setsizee[.]com
seconsave[.]com
scanlostt[.]com
sanesity[.]biz
Email-securlink[.]com
Blackshok[.]com
Scannost[.]biz
sedsource[.]com
snappcost[.]com
scicuredsit[.]com
secredserv[.]com
savesomme[.]com
secursnd[.]com
Serversend[.]biz
Surfarr[.]com
subnettr[.]com
nertsecure[.]com
sendgriide[.]com
sso-siigninn[.]com

Bandook malware indicators
User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/2010010146b Firefox/55.0
Path connected to on sinkhole: /flras/get.php?huln=nevi

Selection of Bandook Commands
CaptureScreen
ClearCred
GetCamlist
SendCam
StopCam
Uninstall
CompressArchive
GenerateReports
GetWifi
StartShell
GetSound
SplitMyFile
GetAutoFTP
SendStartup

```
getkey
SendMTPList
SendMTPList2
GrabFileFromDevice
PutFileOnDevice
DeleteFileFromDevice
CopyMTP
ChromeInject
DisableChrome
RarFolder
SendUSBList
SignoutSkype
StealUSB
StartFileMonitor
SendFileMonLog
GetUSBMONLIST
GetFileMONLIST
StopUSBMonitor
SearchMain
StopSearch
StopFileMonitor
SendinfoList
EnableAndLoadCapList
DisableMouseCapture
AddAutoFTPToDB
DeleteAutoFTPFromDB
ExecuteTV
ExecuteAMMY
DDOSON
ExecuteTVNew
InstallMac
UnzipFile
GenerateOfflineDB
GetDDSize
RECSCREEN
StartLive
PREEW
```

Unpacked bandook samples

```
1a2ff4a809b5a3757eaa05dc362acb2b227a7d02cb13d74c17d850d44181cf04
```

Packed Bandook Samples

```
051495d208bad010334f14c162600b66c7ef437ae3f6bd037e39bbfc4ccdb415
05ebf95d8f31364facffaba40b4e2d3d7a1ef7183211dc491608577de240dd7e
0928bba82e3399a66d9ec7fb0dfd7321f325ddad95f087452bbafc5c1b1f37fa
0965c040b7459d6d413c810876d8dfb9830da6182e5badfd6fdb57a5a6edf262
0ba40163751d3d93981e8628f82223225fdc3d273a9ea88769414c4fa56c1717
0f746d029fa569f8f940c3a0e63351e3e6e89874197f32d6d201a4ead4a770f0
13163ef0ff1027e664b29fc3b67967d44aa4b84dc762310a5e1567a8fa5e9225
1b66391808a6d74efb0d64095dcb2a6477d92fe243d8651ef1bed9c89df86ad1
1c36c4baf5d2e3cf42ff3a9088dc554e33f620dc09fabf60d899075dd28bc025
```

```
1dff1a28d786690661abc41f0e71c05d80a73b0b6f8899fb88101b2a5c3b091f
2009b5e99ffe57bec2440ef3eecab14f076ad1786007b2f2d3750f1df5e7c36f
21e75eff0a9499f4c41491821eb6429e450a83ee7659052417276ddaae6c0cba
2593acc084419e0f7b249fc6e1bd626e0782e3466f6b143fd2543b28b4bfb622
28f61daa127cd988b8615fc924d67b0e645b66bb185bd72e326417480bd23de3
2aab3b73337dd50d8cbab955db6e0e1345ae0a8e24dbcb3440fdd0189a31d80b
2c0d1f7a3d2186b31b36f99e7091d622f10d0ed5b6e54bafe0b116f5a6fab5ab
2cd1f9c3348eb8ae6e3975c0e5449ac8a780d2adfccbddac568f1f5fef2b2d8b
2e738d147f9816366ba47daeee9194c69bc9106c9bc582b81eca19692ba811e2
3a31234da1745a9861f3ae780e222ad18e81844abe0f13e068f4b532af1c209a
41bc659baba8cb340cafa2217c39b5d1e31fe1a3e7f143ccc2315ed32430f4d5
48f0fe5523ab829e6ed4d9c8d001e257430de823ff42bf087883180118c4cb35
4a5a794a33c30694fbb5ddde47fce30eece544739bba3e91e83bd2b1bb895989
4b52781e2aad22679a91a65700b638d58b529c3a67ee81a1d8a466760bc43926
4e0a7e0ed2b44214760ba6638b3eb70cbb8d4a229a5539d6ac26f38e0b7df549
4ee8dee9ab57ddb049969a4602e7e058898d7a8fe762e43ec65ca7a6684bbae5
503f9c9fd3fcec0a26bb75ecac77209ce7081792fdd6837c83a3a120d8def3e4
54772c69367903fbf64322733f6b2f7425fdef169e42dd6f33da1bad4f973f51
64d1f9539a9c3dd6c93a0bd2a2ab1b9650b3cc18a13d0f2536e035357899d7eb
75f4ea3d11cf9dc790c188f9ad63376f799de03983df1df1c2455d763b62c522
7c01580972c59fde937eef7d038edf34ae4217a62a104d75536494b69b8247c4
7d1bd29643f949007fd093030d3274e3467267048bdf008e0191947a67edef01
89b7696c2ad55743c22dae4b28f5588571f27d695000ac7d634f6aaabe52b390
9afd4654b3d0b09392b4c884740efe455ae393ed3b6aef18150f6504970390e6
9cd898cc6682a4fdc7618585715890cdf812c9e28f78bdc44a065afc05865071
9ee48b8992988aa82fd9f3db98429c5f6a8066cccecb98db961ef121bdabb942
a074383dc5f22f659f9c1de66831b520cd0a307ef6a5b01ffc53997df7aa718b
a0d63cb3d6a9087b9a71abc8ce31d5d80774c0edb35ce56a371de4151e9b2f5a
a44be2bfb30bbdcc04fc33339abd60d4cdeded1a46542fc9b1394928229cc18a
ac4ebcf88525c6ea966b4fe8d183cb2261d0419b75640e67cbfc3a2ae9ddc739
b079f2c81638d23c59c0c04c9e2b6caf02e8bac37746d1cded77b4638bd025be
b3ac90ce7995ac2c70c310cc369ceaf70e29ab5e7d098a363b6431ae306949f3
b5404a3c626150c7224cf37bffa68f6bd1b9040ba7cf0ca3a3cc9aa40a6a1df9
b8cbbcc44782202a04475244bdd862ff2ccb80855cc157eb562beffebe417c33
bb42e80c74a1671ce1159806436c9c0ffb78078050676a5b63b3d3c40948f38a
c2cefbd20085e81a87ad49fb661f808bc937700b894f4bf4937ae32b0a3d37a2
c9bedb88c60aa6723e4d6d9894cdd484df4ecedbf653da8348d9675da22dcc35
ca67528ba276f8f3c85a40fdbb8db182f85fe36d7eb6088041e16c547f381be0
cc3284a5512916f736dda51fe76e6b0a35f97efbe18d55385120338776854c55
d27d0748b818b6d443e175c506284b3b33e2379dc20a38bad61e9b6b940048e4
d819faa902e7cd74680a334ab7bcd156df8c9d99078bd62ecdf98d364804712c
d8775fce1a11f8a891675ab591170aba7338ce17340de24332e146267e3f4f3e
db147eb3e95d70e1a4bb246bef7a02dd16eb706e587ef263e05b083afe8f61b4
db9ec59e23d8848bf3dee499edc1eeea8060fa359478ebbcd8172c5900d9e48a
dbfb45bd9a3f2dd649fa657a190b542e3dfbcb253612216e484bccbd91fdccab
e63a5fb04d995a6835b925fc240635323464de07fd4cae76324e7f03e13d8080
e6af856627d8796abbdbd1380b4441759be609fa36235a703ad069710ac3dba5
ea720e0eb9c65489938dc899237e298c0f13b43b8f1e16478b23cc0a5eabd02d
f2cc4d82e5019783286ac9722dc39047d9128ff5175208a01bfee06c8023487b
f39087c5ee2e1c592732eb870157e0cb4473b9b70e45eb0bd8244e52c23c5668
4d50d9c16c5fd8220f4b120ef947d0d7f90d04ae23ca163778dde615f19cabb4
d1031a8e6e33a27016a3d80862585328a69f5ae74e5d16ad844182c189e513e2
```

```
0e6f5c6bcc2bea274b600ea0f3608185369d657d2750da7c63a8b36538c3c6ba
7ca1beb6ebe4d00b6e129713b95d898f984da6277e5fbfbb8f4a8d59076c9fa2
5e5324dbf854b9eb9b6d52ff5949e8a8f9d8054ad7391456ab7520b03932e456
5c4833a0cce81a96416e01a861506364b64070bc33106a18b444f5b7b5bb4296
F742a398eb7d3f6af2dc30e67e9d163224e98d437bdf91fb15bb76d40bf36956
D1031a8e6e33a27016a3d80862585328a69f5ae74e5d16ad844182c189e513e2
0e6f5c6bcc2bea274b600ea0f3608185369d657d2750da7c63a8b36538c3c6ba
5e5324dbf854b9eb9b6d52ff5949e8a8f9d8054ad7391456ab7520b03932e456
5c4833a0cce81a96416e01a861506364b64070bc33106a18b444f5b7b5bb4296
f075ce4c940411bb36da70f18b8dc5d1db94350abc029979d435385ce753e785
4375b6a9de977b7c56bacee03f435052e772789022b1dc759bf6d7e28953b683
E1778d20e7cfc282e73740ae884dc4dccdb439b46558cb96d1d015f8a8807719
6ed505600f4963a0fe2a11fed1a6526be1dcf40bf7563f3641a49688ecba249c
86a076ba12148527863fd9ea78f0d146a15d13f8d35d9d77a738c221f5b0e9f6
F07d90d7f9306a00ba979fc4ebc3dcbf9149cdd9cc86ad9caf3036a19019189b
B1cbd4105b4f90a557ab17684e4cb34961e467228c738777a4daf170ef343d97
F44243f05cc74db860ff7389635754d2cacbc5b0689131d8049d38987e2b0ce3
bb1d607a2b7b9c9ba7af03cfa6dfb5237c021154130ae71bf271b640b8773146
```

```
353dcc4479725da180b0c12fdc433d46fddefdced3a967e7fe528d030a61a791
8a17dd089005204473ae8e1f298a5caf210db82961ef600da3653e4c3afbf314
Dd031eb32ea22e1ac6d3cacec042a2641878cc67e3b4b8482f32dc20e53e348d
```

```
013e252190aaa4b43bcb5ffe13d7b664873ddde38f8df29980d6599c89cb1c78
347de6ac8612bc2b291ceedba11356b5dd8b4b0d6b68357f6903cc676146fbd7
86d0e2434757f8fe71770b7d43b0112e780e420b7c9edeb527d1fd0cd02c0c61
9c540d911f6d17033e59fe3bb09181675cb7123b725f2b4ca1089f9351abc3df
cfd84f553f34d635bbb6ea04375b8090324e653b40e26b17731c5ead7c38406e
fbc8faeaddacba22fb306021c849608a26250e5ff464ed7c630675e87f1c3d16
```

Tags

threat lab

Related Updates

Deeplinks Blog by Bill Budington, Cooper Quintin | December 24, 2022

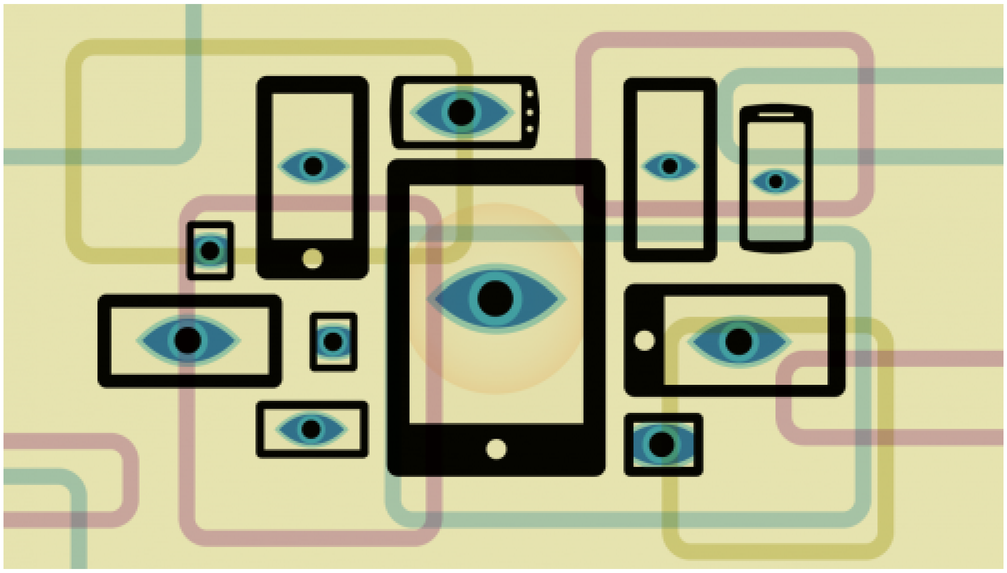
EFF’s Threat Lab Sharpens Its Knives: 2022 in Review

EFF’s Threat Lab is dedicated to deep-dive investigations that examine technology-enforced power imbalances in society. In 2022 we’ve sharpened our knives and honed our skills in an effort to bring down the stalkerware industry, taken aim at invasive surveillance by police, raised red flags around the security and privacy...

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

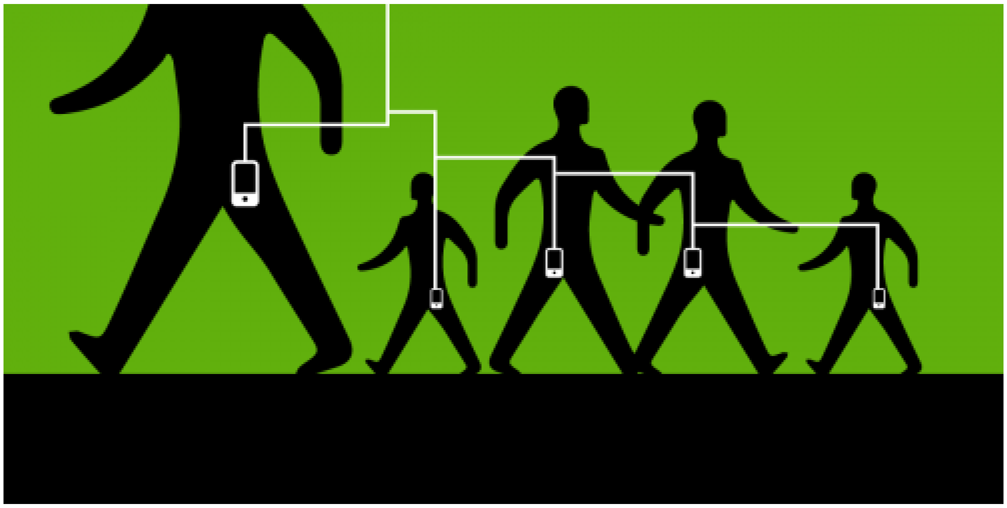
AlHathloul v. DarkMatter Group

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, Eva Galperin | December 10, 2020

Dark Caracal: You Missed a Spot

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...

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...