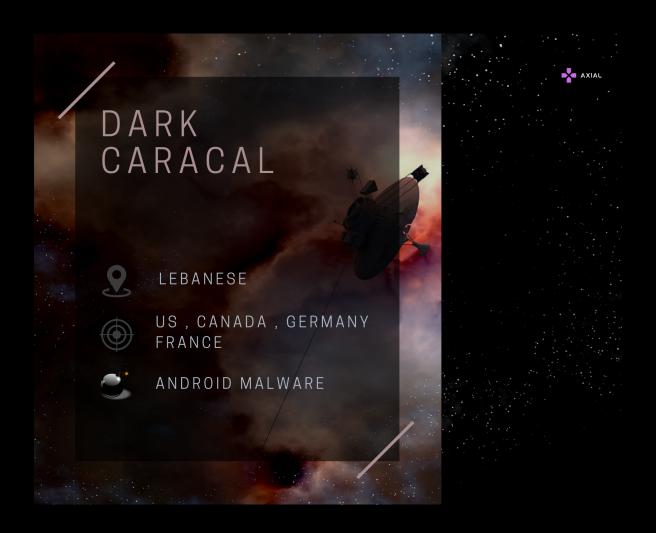
DARK GARACAL







A SURVEY ON DARK CARACAL: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

The Dark Caracal is an APT group associated with the Lebanese General Directorate of General, in recent attacks it employed a new version of a 13-year-old backdoor Trojan dubbed Bandook.

II. TARGETS

The different targeted sectors include:Government, financial, energy, food industry, healthcare, education, IT and legal institutions.

III. METHODS USED

Previous campaign: has mainly used phishing attacks (and in some cases physical access to victims systems[2]) in order to install malicious Android applications, including ones that imitate the look and feel of popular instant messaging applications, on victims systems to gain full control over the devices.

Latest campaings: The first stage leverages a lure Microsoft Word document (e.g. "Certified documents.docx") delivered inside a ZIP file. Upon opening the archive, malicious macros are downloaded, which subsequently proceeds to drop and execute a second-stage PowerShell script encrypted inside the original Word document.

In the last phase of the attack, the PowerShell script downloads encoded executable parts from legitimate cloud storage services like Dropbox or Bitbucket then assemble the Bandook loader, which injects the RAT into a new Internet Explorer process. The Bandook RAT is available on the underground market since 2007, it supports common backdoor commands, including capturing screenshots and carrying out various file-related operations.

IV. CAMPAIGNS

- Lookout first gained visibility into attacker infrastructure in July 2017, millions of requests being made to it from infected devices. This demonstrates that Dark Caracal is likely running upwards of six distinct campaigns in parallel, some of which have been operational since January 2012. Dark Caracal targets a broad range of victims." states the analysis. "Thus far, Lookout have identified members of the military, government officials, medical practitioners, education professionals, academics, civilians from numerous other fields, and commercial enterprises as targets. The data allegedly stolen includes documents, call records, text messages, audio recordings, secure messaging client content, browsing history, contact information, photos, location data, and other information that allows the group to identify their targets and have a look at their personal lives
- 2020: Check Point Research recently observed a new wave of campaigns against various targets worldwide that utilizes a strain of a 13-year old backdoor Trojan named Bandook.Bandook, which had almost disappeared from the threat landscape, was featured in 2015 and 2017 campaigns, dubbed "Operation Manul" and "Dark Caracal", respectively. These campaigns were presumed to be carried out by the Kazakh and the Lebanese governments, as uncovered by the Electronic Frontier Foundation (EFF) and Lookout.During this past year, dozens of digitally signed variants of this once commodity malware started to reappear in the threat landscape, reigniting interest in this old malware family.



V. IOCS

MD5 Hashes

- 27f8d8bbbeeda5fc439ee18d9d4da 343
- 44584c8d010242fddb44afe5ce8608
 72
- a6501c62b3a6ffa8d028a88138fe50
- 7c15ee5b9a12dacaace8fb62271f12f
 1
- 4e9e12c98cfbc5f3aa3c1345bd063fa
 0
- 1a3889ded73044f8ba0a00c2f089a3 bd
- 70ff19341dee7973ea6dd8e15c6ba8
 6f
- d6e524514e0d112015c841b62377 d648
- 3f310215a70d748f9335c767e61a2a h4
- d1600f45005aa8b8fcbb446f34f7b9f
 5
- 4d7e67ed02713c789336f8804231b
 1ca
- 9bcf889b14968c61df95961a161719 ba
- 54ad403349831b175a98a429f818f 02a

C2's /Domains

ancmax[.]com planethdx[.]com mecodata[.]com globalmic[.]net kaliex[.]net axroot[.]com sabisint[.]com megadeb[.]com roxsoft[.]net flexberry[.]com opwalls[.]coms1[.]megawoc[.]com executable. accountslogin[.]services adobeinstall[.]com adobeflashviewer.accountslogin[.]services dropboxonline[.]com

iceteapeach[.]com

nvidiaupdate[.]com

skypeupdate[.]com

paktest.ddns[.]net

2ndprog[.]monster

p2020[.]xyz

watermelon2017[.]com

TTP's

Dark Caracal's version of Bandook communicates with their server over a TCP port using HTTP payloads Base64 encoded and suffixed with the string "&&&".

Dark Caracal has used macros in Word documents that would download a second stage if executed. Dark Caracal leveraged a watering hole to serve up malicious code.

Dark Caracal leveraged a compiled HTML file that contained a command to download and run an executable.

Dark Caracal controls implants using standard HTTP communication.

VI. REFRENCES / SOURCES

https://research.checkpoint.com/2020/bandook-signed-delivered/
https://securityaffairs.co/wordpress/111617/apt/dark-caracal-still-active.html
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_DarkCaracal_srr_20180118_us_v.1.0.pdf
https://research.checkpoint.com/2020/bandook-signed-delivered/

