FIGHTING TARGETED MALWARE IN THE MOBILE ECOSYSTEM

Megan Ruthven  Andrew Blaich

Google  Lookout
Agenda

• Introductions
• Background on Chrysaor
• How it Works
• Hunting for Chrysaor
• Hunting beyond Chrysaor
• Conclusions / Special Thanks
• Questions
Who are we?

**Megan Ruthven** - Software Engineer on Google's Android Security Team, uses device and application data to combat malware on a global scale.

**Andrew Blaich, Ph.D.** - Security Researcher and Head of Device Intelligence at Lookout specializing in threat hunting and vulnerability research.
What is Chrysaor?

- Mobile espionage software believed to be created by NSO Group Technologies
- Believed to be related to the Pegasus spyware that was first identified on iOS and analyzed by Citizen Lab and Lookout.
Background

Pegasus for iOS
August 2016
Discovery: Citizen Lab & Lookout
Exploited: three zero-day vulns

Government Hackers Caught Using Unprecedented iPhone Spy Tool
LORENZO FRANCESCHI-BICCHIERAI
Aug 10, 2016, 4:57 AM

The malware was used to target a political dissident in the United Arab Emirates.

On the morning of August 10, Ahmed Mansoor, a 46-year-old human rights activist from the United Arab Emirates, received a strange text message from a number he did not recognize on his iPhone.

"New secrets about torture in state prisons," read the tantalizing message, which came accompanied by a link.

Mansoor, who had already been the victim of government hackers using commercial spyware products from Hacking Team and Pegasus, was suspicious and didn’t click on the link. Instead, he sent the message to Bill Marczak, a researcher at Citizen Lab, a digital rights watchdog at the University of Toronto’s Munk School of Global Affairs.
CHRYSAOR EXPLOIT CHAIN SEQUENCE
# Feature comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Hooking</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMS Command and Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Zero-Day Exploits</td>
<td>Yes</td>
<td>No (Not these samples)</td>
</tr>
<tr>
<td>Audio Surveillance</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Functionality without device compromise</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Standalone App</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Suicide Functionality</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Targets Popular Apps and built-in Device Features</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Disables System Updates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Screenshot Capture</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Searching for Chrysaor

Where do we start

• Did not exist in Google Play or any other Android app store
• Did not exist on VirusTotal
• Expected to have low prevalence because it’s distributed, used, and removed in highly targeted attacks
A massive dataset is key to solving mobile security

Expedites the identification of anomalies and malicious activity with scale & precision
Discovering Chrysaor - Starting

- Looked for *rare* Android apps based on:
  - Package information
  - Signer information
  - Uniqueness of app
Discovering Chrysaor - Correlating

• Leveraging **Pegasus for iOS** detections we linked together our rare apps with:
  • Account indicators
  • Country indicators
  • Behavior indicators
Discovering Chrysaor - Visualizing
Threat Intel Sharing

Lookout → Google

Apps of Interest:
- Package Names
- Signer Info
- Prevalence
- Locations
- Observed behavior
Intro to Google Play Protect (GPP)

• Our security service informs Play users of Potentially Harmful Apps (PHAs) installed or being installed

• Pseudo anonymous

• 1.5 billion 28 day actives

• Use logs to find other PHAs
Where do we start?

• First surfaced Lookout’s set of Chrysaor app & devices

• Checked for association with Chrysaor

• Only 0.000001% of Android devices affected by Chrysaor
How do we verify the complete needle?
Use data

• Leverage
  • The rareness of mobile espionage apps
  • Multiple apps with the same signing cert
  • Amount of GPP actives

• To find other apps & other devices
How to expand set of apps & devices

device1
- Installed Apps’ Certs
  - certA
  - certB
  - implant
  - certC
  - rareCertA

device2
- Installed Apps’ Certs
  - certB
  - certD
  - rareCertA
  - rareCertB
  - certE

device3
- Installed Apps’ Certs
  - certA
  - certC
  - certE
  - rareCertB
  - certF
Formalizing the method

- Filter-out common certs from set
- Group rare certs by device
- Connect co-installed certs
- Results: rare cert graph
- Can expand to any attribute
Automate & scale the process

Using the rare cert graph

1. Start with seed certs found from the initial investigation
2. Propagate to all connected certs
3. Verify apps are associated with group
4. Leverage code similarity to find more seeds
5. Repeat
Used before blocking Chrysaor apps

- Confident that only a couple dozen devices were affected
- Blocked Chrysaor apps
- Notified users
What’s next?
Expand apps over time
LIPIZZAN

• Found a separate set of espionage apps
  • 1 app was co-installed
  • Leading to finding the whole set
• Includes references to Equus Technologies
• Suspended 16 Play apps
• More information covered in blog post
Conclusions

• Using data to connect anomalous behavior together is effective in finding espionage apps
• Chrysaor devices continued to be protected from other espionage apps
• Keep your device up to date with the latest security patches
• Keep “unknown sources” disabled when not in use
Special thanks

The entire team(s) from both Lookout and Google including:

• **Lookout**: Adam Bauer, Michael Flossman, Jeremy Richards, Christoph Hebeisen, Danielle Kingsley, Stephen Edwards, Christina Olson, Kristy Edwards, and Mike Murray

• **Google**: Rich Cannings, Jason Woloz, Neel Mehta, Ken Bodzak, and Wentao Chang
Questions?

Megan Ruthven  
@maruthven  
maruthven@google.com

Andrew Blaich  
@ablaich  
andrew.blaich@lookout.com
Appendix A

• Blogs:
  • https://blog.lookout.com/pegasus-android

• Technical Analysis: