EVERY BREATH YOU TAKE

A CTI REVIEW OF STALKERWARE

@Ch33r10

*not speaking on behalf of my employers
“The opinions expressed in this presentation are those of the presenter, in their individual capacity, and not necessarily those of my employers.”
STALKERWARE

- WHAT IS IT?
- HOW DOES IT WORK?
- TARGETS/OPERATORS
- TRADECRAFT
- CTI HYPOTHESES
- CORPORATE AMERICA SOLUTIONS
STALKERWARE

WHAT IS IT?
STALKERWARE => SPY
STALKERWARE

Software used to “facilitate intimate partner violence, abuse, or harassment, including pernicious intrusions into the targeted person's life by way of physical or digital actions”

~The Citizen Lab

STALKERWARE | SPYWARE | DUAL-USE APPS | mRAT
INTIMATE PARTNER SURVEILLANCE TOOLS

- COMMODITY STALKERWARE/SPYWARE
- DUAL-USE APPS
- mRAT
- SHARED ACCOUNTS
- OSINT, SOCIAL MEDIA, PEOPLE, RECEIPTS, ETC
COMMODITY
STALKERWARE

BASIC Active & Passive Data Collection

- Texts
- Call Logs
- Some Chat Apps
- Pics & Videos
- Browser History
- GPS Location
<table>
<thead>
<tr>
<th>Record/Access/Monitor</th>
<th>Phone Calls</th>
<th>SMS</th>
<th>Chat Apps</th>
<th>Logs</th>
<th>Social Media</th>
<th>Stored Media</th>
<th>Web Traffic</th>
<th>Email</th>
<th>GPS</th>
<th>Contacts</th>
<th>Calendar</th>
<th>Keystrokes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerberus</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Highster Mobile</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Hoverwatch</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mobistealth</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>mSpy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>TeenSafe</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>TheTruthSpy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
STALKERWARE

Mobistealth
mSpy
FlexiSpy
Highster Mobile
Hoverwatch
Spyzie

TheTruthSpy
TeenSafe
Cerberus
Xnspy
WebWatcher

& More!!!
STALKERWARE

HOW DOES IT WORK?
COMMODITY

STALKERWARE

REQUIRED:

- PHYSICAL ACCESS TO DEVICE
- INTERNET ACCESS

INSTALL APPS FROM UNKNOWN SOURCES & DISABLE GOOGLE PLAY PROTECT

JAILBROKEN iPHONE (SPY W iCloud ACCT ACCESS)
RWDEICA, LHM Kill Chain, Commodity Stalkerware
COMMODITY

STALKERWARE

EASY TO USE, LEGAL-ISH*, CHEAP, READILY AVAILABLE, SIMILAR CAPABILITIES TO mRAT/SPYWARE, NO USER INTERACTION, NO TECHNICAL SKILL

DRAWBACK: PHYSICAL ACCESS TO DEVICE

*intercepting private communication is generally illegal (potential wiretapping crime) unless person doing it is a parent, employer, LE with warrant. Stalkerware vendors suggest getting consent.
mRAT

STALKERWARE

CHEAP-ISH, REMOTE INSTALLATION REQUIRES: SPECIFIC KNOWLEDGE TO OBTAIN, USER INTERACTION, TECHNICAL SKILL!!!

DRAWBACK: ILLEGAL
<table>
<thead>
<tr>
<th>TACTIC</th>
<th>TECHNIQUE</th>
<th>PROCEDURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>T1461: Lockscreen Bypass</td>
<td>Dental molding kit or playdough to lift fingerprints</td>
</tr>
<tr>
<td>Initial Access</td>
<td>T1475: Deliver Malicious App via Authorized App Store</td>
<td>Install spyware from Google Play Store</td>
</tr>
<tr>
<td>Collection, Credential Access</td>
<td>T1412: Capture SMS Messages</td>
<td>Use Spyware to receive SMS</td>
</tr>
<tr>
<td>Remote Service Effects</td>
<td>T1468: Remotely Track Device without Authorization</td>
<td>Use Spyware to Track User</td>
</tr>
</tbody>
</table>
EXISTING AV & ANTI-SPYWARE TOOLS INEFFECTIVE AT DETECTING & REMEDIATING STALKERWARE

<table>
<thead>
<tr>
<th>Product</th>
<th>Filename</th>
<th>APK Version</th>
<th>Positive Count</th>
<th>Engines Used</th>
<th>% Positives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerberus</td>
<td>Cerberus_disguised.apk</td>
<td>3.5.2</td>
<td>6</td>
<td>63</td>
<td>9.5%</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>flexisy_5002_3.0.1.apk</td>
<td>3.0.1</td>
<td>34</td>
<td>63</td>
<td>54.0%</td>
</tr>
<tr>
<td>Hoverwatch</td>
<td>hoverwatch-setup-fovfm.apk</td>
<td>6.3.260</td>
<td>22</td>
<td>59</td>
<td>37.3%</td>
</tr>
<tr>
<td>mSpy</td>
<td>mspy_android.apk</td>
<td>5.3.0</td>
<td>20</td>
<td>63</td>
<td>31.7%</td>
</tr>
<tr>
<td>TheTruthSpy</td>
<td>TheTruthSpy.apk</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>TheTruthSpy</td>
<td>TheTruthSpy-2.apk</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td><strong>Mean</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>22.1%</strong></td>
</tr>
</tbody>
</table>

THE CITIZEN LAB | THE PREDATOR IN YOUR POCKET P 40 https://citizenlab.ca/docs/stalkerware-holistic.pdf
STALKERWARE

TARGETS

“THE VICTIMS ARE EVERYDAY PEOPLE”
~Morgan Marquis-Boire
RELATIONSHIPS
SIMILAR SURVEILLANCE CAPABILITIES AS STALKERWARE TARGETS
CHILDREN
EMPLOYEES
JOURNALISTS
WASHINGTON POST
REPORTER
ASSASSINATED
JAMAL KHASHOGGI

ABDULAZIZ | PEGASUS
DISSIDENTS
ACTIVISTS  BLM
CITIZENS  WeChat
RELIGIOUS LEADERS  Tibetans | Dalai Lama
TERRORISTS

WHATSAPP- "YOU'VE BEEN HACKED"
EUROPEAN LE- OOOPSY
MILITARY TikTok=BAN
GOVERNMENTS
GOV OFFICIALS
LAW ENFORCEMENT

LOOKOUT | STEALTH MANGO | MIDDLE EAST | INDIRECT COMPROMISE USA/UK/AUS/IRAN
STALKERWARE

OPERATORS
RELATIONSHIPS
STALKERWARE VENDOR BREACHES

FlexiSpy: Metropolitan Police

Mobistealth: Military, FBI, ICE, DHS, TSA
SIMILAR SURVEILLANCE CAPABILITIES AS STALKERWARE OPERATORS
CYBERCRIME
HACKTIVISTS
STALKERWARE

HOSTILE ACTOR TRADECRAFT
KIMBER

SHARED ACCTS | DUAL-USE APPS | UNILATERAL MANIPULATE FRIENDS/FAMILY EMOTIONAL & PSYCHOLOGICAL ABUSE
ELECTRA

mRAT | TECHNICAL | SOCIAL ENGINEERING
EMOTIONAL & PSYCHOLOGICAL ABUSE
POISON HYDRA

PHYSICAL THREATS/ABUSE TO GAIN ACCESS
EMOTIONAL & PSYCHOLOGICAL ABUSE
STALKERWARE

CTI HYPOTHESES

NORMAL USE OF COMMODITY STALKERWARE
RTFM

CORPORATE AMERICA
CORPORATE

MOBILE DEVICE MANAGEMENT/

BYOD
CORPORATE

STALKERWARE VENDORS

- POOR SECURITY PRACTICES
- MISCONFIGS SPYFONE S3/API
- BREACHES
- UNENCRYPTED TRANSMISSION/MITM?
STALKERWARE VENDOR BREACHES

Retina-X (2x)  TheTruthSpy
Flexispy       Family Orbit
Mobistealth    mSpy
Spy Master Pro Copy9
SpyHuman       Xnore
Spyfone        Mobiispy
HelloSpy       WtSpy
CORPORATE

HOW MANY EMPLOYEES IMPACTED BY STALKERWARE?

WOMEN ((20K*50%)*33%) = 3,333
MEN ((20K*50%)*16%) = 1,667

5K (25%) Employees experience IPV sometime in their lifetime
x 54% IPV Survivors Tracked w Stalkerware =
2.7K (13.5%) Employees impacted by stalkerware at one point in their lives
13.5%*

EMPLOYEES IMPACTED BY STALKERWARE AT SOME POINT IN THEIR LIVES

*FIGURE APPROXIMATE BASED UPON IPV/IPS STATISTICS & SIMULATED COMPANY F/M RATIOS & WORKFORCE SIZE
CORPORATE INSIDER THREAT
CORPORATE

EXECUTIVES

EMPLOYEES
CORPORATE

COMPETITORS
CORPORATE INDUSTRIAL ESPIONAGE
STALKERWARE
CORPORATE AMERICA SOLUTIONS
### Corporate CTI

**The Citizen Lab**

**The Predator in Your Pocket P 37-38**

[https://citizenlab.ca/docs/stalkerware-holistic.pdf](https://citizenlab.ca/docs/stalkerware-holistic.pdf)

<table>
<thead>
<tr>
<th>App</th>
<th>Domain</th>
<th>IP</th>
<th>Country</th>
<th>ASN Name</th>
<th>ASN #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerberus</td>
<td><a href="http://www.cerberusapp.com">www.cerberusapp.com</a></td>
<td>66.228.35.203</td>
<td>United States</td>
<td>Linode, LLC</td>
<td>63949</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>admin.flexispy.com</td>
<td>104.25.91.115</td>
<td>United States</td>
<td>Cloudflare, Inc.</td>
<td>13335</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>admin.flexispy.com</td>
<td>104.25.92.115</td>
<td>United States</td>
<td>Cloudflare, Inc.</td>
<td>13335</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>api.flexispy.com</td>
<td>180.150.144.84</td>
<td>Hong Kong</td>
<td>Rackspace IT Hosting AS IT Hosting Provider Hong Kong</td>
<td>45187</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>blog.flexispy.com</td>
<td>104.25.92.115</td>
<td>United States</td>
<td>Cloudflare, Inc.</td>
<td>13335</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>blog.flexispy.com</td>
<td>104.25.91.115</td>
<td>United States</td>
<td>Cloudflare, Inc.</td>
<td>13335</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>client.mobilefonex.com</td>
<td>180.150.156.198</td>
<td>Hong Kong</td>
<td>Rackspace IT Hosting AS IT Hosting Provider Hong Kong</td>
<td>45187</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>community.flexispy.com</td>
<td>104.25.91.115</td>
<td>United States</td>
<td>Cloudflare, Inc.</td>
<td>13335</td>
</tr>
<tr>
<td>FlexiSPY</td>
<td>community.flexispy.com</td>
<td>104.25.92.115</td>
<td>United States</td>
<td>Cloudflare, Inc.</td>
<td>13335</td>
</tr>
</tbody>
</table>
CORPORATE TABLE TOP

MONETIZE | TAKE-DOWN
STALKERWARE

- Stalkerware, Spyware, mRAT, Dual-use Apps
- Data Access varies by vendor/type
- Target/Operators: Relationships
- Sub-optimal AV detection
- Org Specific Threat Modeling
ABOUT ME

- MBA IT Management
- D.Sc. Cybersecurity Student at Marymount University
- GSEC, GCIH, GCFE, GMON, GDAT, GPEN

@ch33r10
RESEARCH

https://www.ft.com/content/263133ac-a28b-11e9-974c-ad1c6ab5efd1
https://havron.dev/pubs/clinalsec.pdf
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618
http://damonmccoy.com/papers/Creepware_SP.pdf
https://citizenlab.ca/docs/stalkerware-legal.pdf
https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html