XRAT Malware Tied to "Xsser/MRAT" Surveillance

By Lookout

Published: 2017-08-31 · Archived: 2026-04-02 10:55:47 UTC

Lookout researchers have identified a mobile trojan called xRAT with extensive data collection functionality and the ability to remotely run a suicide function to avoid detection. The malware is associated with the high-profile Xsser / mRAT malware, which made headlines after targeting both iOS and Android devices of pro-democracy Hong Kong activists in late 2014.

Lookout continues to regularly acquire new Android-variant samples of mRAT from multiple sources, and we have seen detections that show it has been live on Android devices in recent months. The frequency with which these samples are being deployed in the wild suggests that this family is still under continual development and actively used in various campaigns.

Lookout identified xRAT due to a combination of suspicious capabilities it uses, such as dynamically loading additional code, executing native libraries, using specific ciphers, and accessing sensitive user information. Samples from both mRAT and xRAT families have an almost identical code structure, make use of the same decryption key, share certain heuristics and naming conventions, and interestingly contain anti-debugging techniques that cause the a frequently-used malware researcher tool, the dex2jar decompiler, to crash. These many similarities strongly suggest that mRAT and xRAT have been developed by the same threat actor.

The command and control servers for xRAT are also linked to Windows malware, indicating that the malicious actors behind this threat are conducting multi-platform attacks against the PCs and mobile devices of targeted groups.

What it does

The discovery of xRAT and continued improvements to both xRAT and mRAT clearly demonstrate that threat actors are capable of deploying sophisticated tools to retrieve intelligence from mobile endpoints. Like mRAT, xRAT supports an impressive set of capabilities that include flexible reconnaissance and information gathering, detection evasion, specific checks for antivirus, app and file deletion functionality, and other functionality listed below. It also searches for data belonging to popular communications apps like QQ and WeChat. The threat actors themselves are able to remotely control much of its functionality in real time (e.g., which files to retrieve and what the settings of its automatic file retrieval module should be).

Listed below are the types of data gathered by xRAT and features that enable it to perform reconnaissance, run remote code, and exfiltrate data from Android devices:

- Browser history
- Device metadata (such as model, manufacturer, SIM number, and device ID)

- Text messages
- Contacts
- Call logs
- Data from QQ and WeChat
- Wifi access points a device has connected to and the associated passwords
- Email database and any email account username / passwords
- Device geolocation
- Installed apps, identifying both user and system applications
- SIM Card information
- Provide a remote attacker with a shell
- Download attacker specified files and save them to specified locations
- Delete attacker specified files or recursively delete specified directories
- Enable airplane mode
- List all files and directories on external storage
- List the contents of attacker specified directories
- Automatically retrieve files that are of an attacker specified type that are between a minimum and maximum size
- Search external storage for a file with a specific MD5 hash and, if identified, retrieve it
- Upload attacker specified files to C2 infrastructure
- Make a call out to an attacker specified number
- Record audio and write it directly to an already established command and control network socket
- Executes attacker specified command as the root user
- Instructs an infected device to repeatedly download, and then delete, large files - exhausting a user's mobile data.

xRAT runs a suicide function to avoid detection

xRAT also contains suicide functionality. When triggered, xRAT will clean out its installation directory before issuing a package manager command to uninstall itself. The developers behind xRAT created an alert system, flagging to the malware operator if any of the following antivirus applications are present on a compromised device.

- 管家 (housekeeper)
- 安全 (safety)
- 权限 (Authority)
- 卫士 (Guardian)

- 清理 (Cleanup)
- 杀毒 (Antivirus)
- Defender
- Security

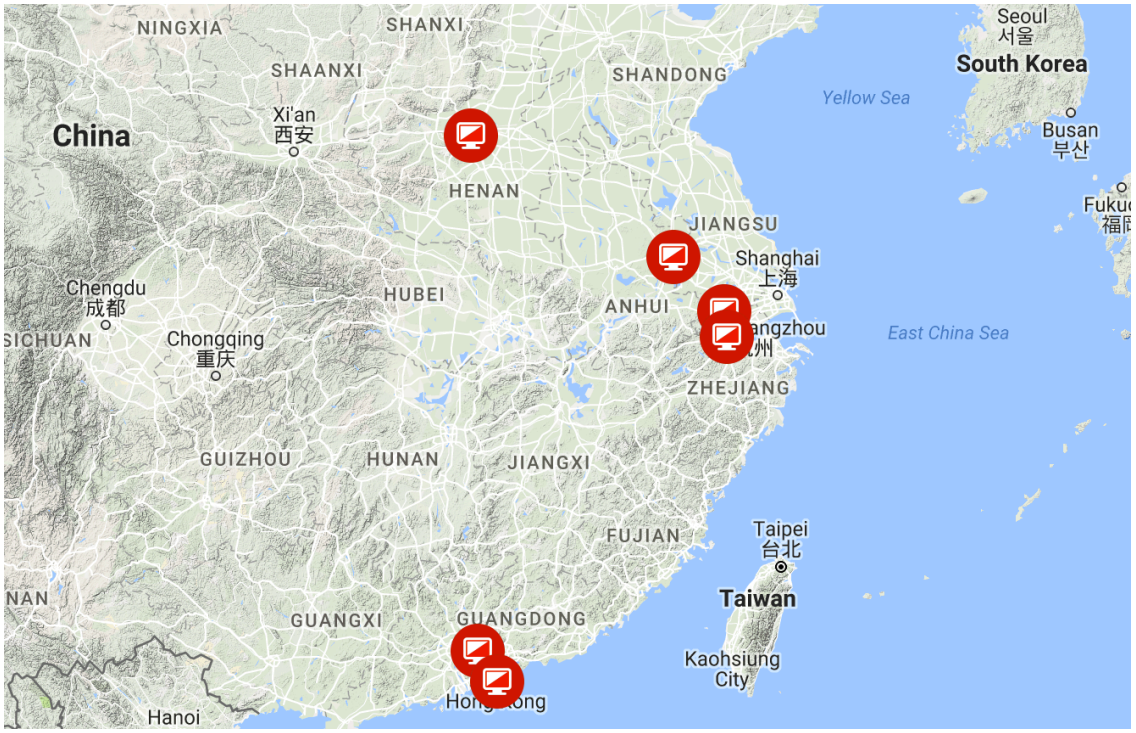
Our analysis found xRAT contains a robust file deletion module, capable of removing large portions of a device or attacker-specified files. xRAT can be remotely instructed to perform the following deletion operations:

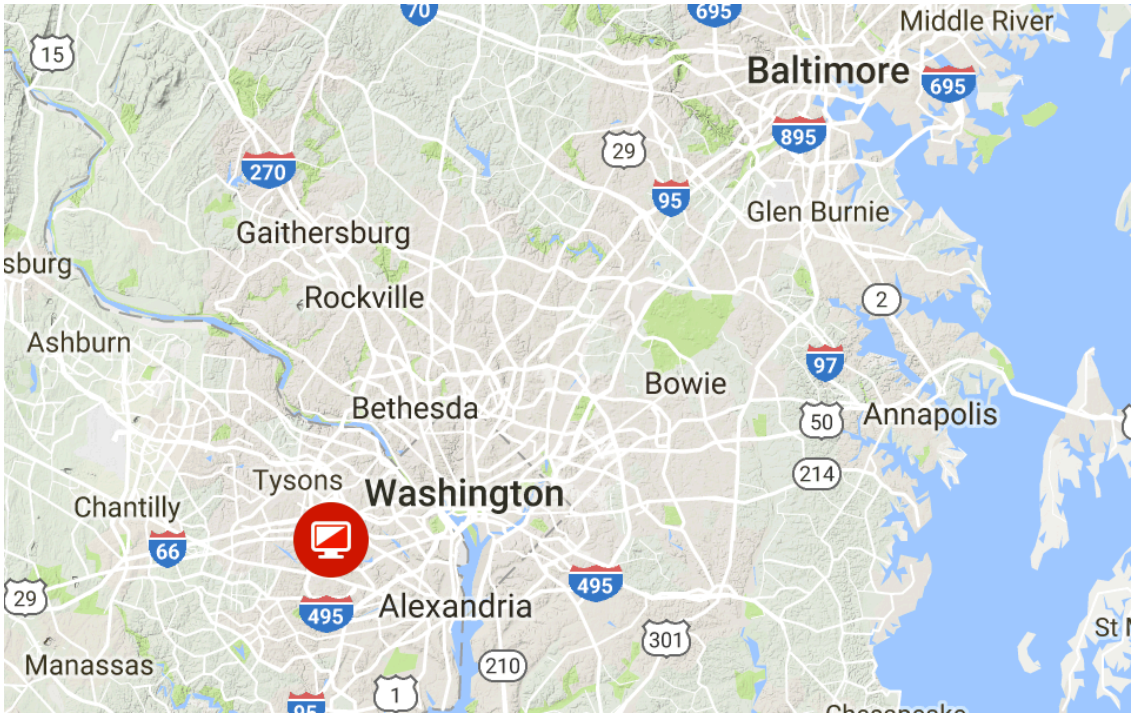
- Remove images from certain directories on the SDCard
- Remove audio files from certain directories on the SDCard
- Wipe a device, removing large portions; including all files from the SDCard, all apps and data that exists under the path /data/data/, and all system apps installed under the path /system/app/.
- Remove specific input method editors (IME). This includes
- com.htc.android.htcime,
- HTC_IME.apk, com.samsung.inputmethod,
- SamsungChineseIME.apk,
- com.tencent.qqpinyin,
- com.sohu.inputmethod.sogou,
- com.iflytek.inputmethod,
- com.google.android.inputmethod.pinyin, com.tencent.qqpinyin-1.apk,
- com.sohu.inputmethod.sogou-1.apk,
- com.google.android.inputmethod.pinyin-1.app,
- com.iflytek.inputmethod-1.apk, and
- other generic instances of IME apps.
- Removes messaging applications from a compromised device. This includes
- com.tencent.mm,
- im.yixin, com.tencent.mobileqq,
- com.whatsapp, and
- other messaging applications that may have a similar package name.

These features further highlight the considerable amount of control xRAT operators have over a compromised phone, allowing it to evade detection by covering its tracks and deleting entire sections of a device.

Command and control infrastructure

The majority of command and control servers used by xRAT in the past have been based in China with some appearing in Hong Kong. After analyzing recently acquired samples, we further identified attacker infrastructure on the East Coast of the United States. This may indicate an expansion in deployment from the actor behind this family as they've previously used servers geographically close to regions where their tooling is being deployed.





Interestingly, the adversary infrastructure has Windows malware associated to it. One particular malicious executable is named MyExam, indicating that the actors behind this family may be continuing to target students, similar to how attackers used mRAT during the protests in 2014.

Associated xRAT Domain / IP	Port
sj.bbmouseme.com	1430, 8888
www.lyserver.com	1440
www.99chi.com	1430
apk.servicses.com	1430
114.215.70.24	1440, 8888
119.23.216.132	1440, 1444
223.255.151.41	1440
222.89.235.56	1330, 1430, 1431, 1440
121.42.188.201	1440
223.255.151.39	1440
221.226.6.58	1433, 1440, 6778
223.255.151.52	1499
61.36.11.75	1430
20.20.20.109	1430
119.147.137.96	1430
119.252.255.9	-

Data compromise via xRAT highlights valuable data on mobile devices

xRAT appears to specifically target political groups, but it's also a good example of how much data can be compromised via a mobile device.

Enterprises must be prepared for these types of threats that compromise contacts, messaging app conversations, email, Wi-Fi passwords, SIM card information, audio, and text messages. Data compromise via mobile presents a significant risk to company-confidential data, and can risk an enterprise's compliance standing, potentially resulting in hefty fines.

This is particularly concerning for businesses who will be subject to GDPR come May 2018, which demands enterprises protect personal information for anyone it interacts with or sends to the European Union. Enterprises should invest in a mobile threat detection solution to complement EMM/MDM technologies, providing invaluable visibility into threats and risks to enterprise data via mobile devices.

Lookout is continuing to investigate the actor behind xRAT, its supporting infrastructure, and the evolving capabilities of the surveillanceware itself.

Interested in learning more about our Threat Intelligence service or how a threat like xRAT could impact your enterprise? Contact us today.

SHA-1s

- 0a58d677ad5fc1562b6ceb6395cfb7b819cc511f
- 20e9b876c2d4253ce61bff01ae364c06b7fa61f4
- 655599f68ec019d3ad8c2d66283958e2dd1e3b9d
- cd20dcd07278714083c757aa07db3a6f663a0b36
- 9e71b0d6bc2b6ffe6f5774b5218de710cee7fe7a
- 701fe85b177b9eba92e1c7e99e64381d950a7b62
- cd1f88caeb30e3f4b0467093175c952fbd433872
- e9fc56c772a70002358c78bc65ba0c0cc0f70447
- 585fc6502ed786db13a7afff8ba61e2eed8e26b9
- 979da00fe2986a0cbc12b60a9419232ab1bf7218
- 2125c20ffd03eff2be2c46dfdd8a2092b73e5766
- 35eb14fca9dd8f95c0b8c416d2d4191388d40e01
- 26325f1e6066e1069d88ca570116bb8bac311a23
- 0aed0f17af2998593b08dad254d3c01dfc6d4d8e
- 6836826b47fcc0c0128ed35c8e546d7c1f7076bd
- dac7a2baa45e47e251ffe5446228914141edd077
- eea40659209a2df7fb4106e9040fe4931c1da3cc
- aaaab3bed79ce615de0e22576e6118cd2d5f624d
- fc583449a9da921995a909bb78a29c794af2fa37
- f006fb13d238a7f39e7cf7fe4521a79664cf8a4a

Michael Flossman

Head of Threat Intelligence

Michael is Head of Threat Intelligence at Lookout where he works on reverse engineering sophisticated mobile threats while tracking their evolution, the campaigns they are used in, and the actors behind them. He has hands-on experience in vulnerability research, incident response, security assessments, pen-testing, reverse engineering and the prototyping of automated analysis solutions. When not analysing malware there's a good chance he's off snowboarding, diving, or looking for flaws in popular mobile apps.

Source: https://www.lookout.com/blog/xrat-mobile-threat