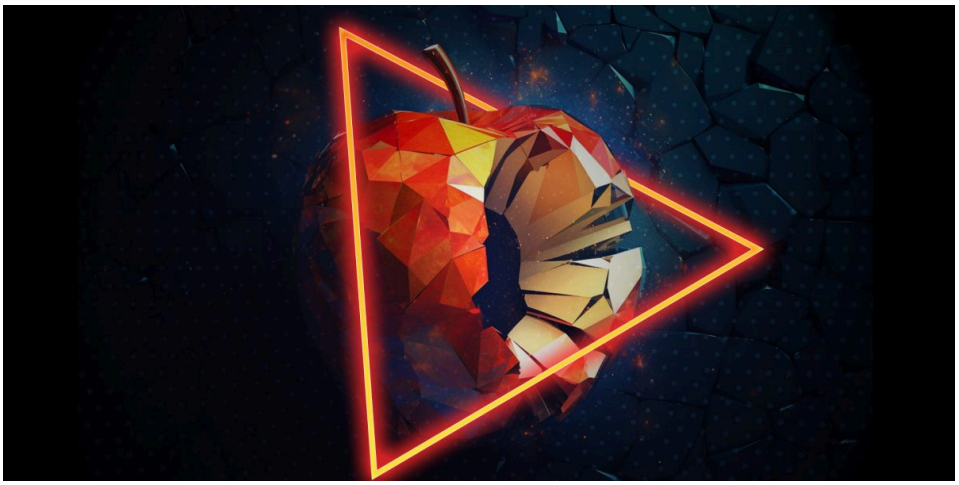
Operation Triangulation: iOS devices targeted with previously unknown malware

APT REPORTS 01 JUN 2023 5 minute read



// AUTHORS

IGOR KUZNETSOV | Expert VALENTIN PASHKOV | LEONID BEZVERSHENKO | GEORGY KUCHERIN

While monitoring the network traffic of our own corporate Wi-Fi network dedicated for mobile devices using the Kaspersky Unified Monitoring and Analysis Platform (KUMA), we noticed suspicious activity that originated from several iOS-based phones. Since it is

Table of Contents

impossible to inspect modern iOS devices from the inside, we created offline backups of the devices in question, inspected them using the Mobile Verification Toolkit's mvt-ios and discovered traces of compromise.
We are calling this campaign "Operation Triangulation", and all the related information we have on it will be collected on the Operation Triangulation page. If you have any additional details to share, please contact us: triangulation[at]kaspersky.com.

What we know so far

Mobile device backups contain a partial copy of the filesystem, including some of the user data and service databases. The timestamps of the files, folders and the database records allow to roughly reconstruct the events happening to the device. The mvt-ios utility produces a sorted timeline of events into a file called "timeline.csv", similar to a super-timeline used by conventional digital forensic tools.
Using this timeline, we were able to identify specific artifacts that indicate the compromise. This allowed to move the research forward, and to reconstruct the general infection sequence:

- The target iOS device receives a message via the iMessage service, with an attachment containing an exploit.
- Without any user interaction, the message triggers a vulnerability that leads to code execution.
- The code within the exploit downloads several subsequent stages from the C&C server, that include additional exploits for privilege escalation.
- After successful exploitation, a final payload is downloaded from the C&C server, that is a fully-featured APT platform.
- The initial message and the exploit in the attachment is deleted

The malicious toolset does not support persistence, most likely due to the limitations of the OS. The timelines of multiple devices indicate that they may be reinfected after rebooting. The oldest

traces of infection that we discovered happened in 2019. As of the time of writing in June 2023, the attack is ongoing, and the most recent version of the devices successfully targeted is iOS 15.7.
The analysis of the final payload is not finished yet. The code is run with root privileges, implements a set of commands for collecting system and user information, and can run arbitrary code downloaded as plugin modules from the C&C server.

Forensic methodology

It is important to note, that, although the malware includes portions of code dedicated specifically to clear the traces of compromise, it is possible to reliably identify if the device was compromised. Furthermore, if a new device was set up by migrating user data from an older device, the iTunes backup of that device will contain the traces of compromise that happened to both devices, with correct timestamps.

Preparation

All potential target devices must be backed up, either using iTunes, or an open-source utility idevicebackup2 (from the package libimobiledevice). The latter is shipped as a pre-built package with the most popular Linux distributions, or can be built from the source code for MacOS/Linux.
To create a backup with idevicebackup2, run the following command:

```
idevicebackup2 backup --full $backup_directory
```

You may need to enter the security code of the device several times, and the process may take several hours, depending on the amount of user data stored in it.

Install MVT

Once the backup is ready, it has to be processed by the Mobile Verification Toolkit. If Python 3 is installed in the system, run the

following command:

```
pip install mvt
```

A more comprehensive installation manual is available the MVT homepage.

Optional: decrypt the backup

If the owner of the device has set up encryption for the backup previously, the backup copy will be encrypted. In that case, the backup copy has to be decrypted before running the checks:

```
mvt-ios decrypt-backup -d
$decrypted_backup_directory $backup_directory
```

Parse the backup using MVT

```
mvt-ios check-backup -o $mvt_output_directory
$decrypted_backup_directory
```

This command will run all the checks by MVT, and the output directory will contain several JSON and CSV files. For the methodology described in this blogpost, you will need the file called timeline.csv.

Check timeline.csv for indicators

1. The single most reliable indicator that we discovered is the presence of data usage lines mentioning the process named "BackupAgent". This is a deprecated binary that should not appear in the timeline during regular usage of the device. However, it is important to note that there is also a binary named "BackupAgent2", and that is not an indicator of compromise. In many cases, BackupAgent is preceded by the process "IMTransferAgent", that downloads the attachment that happens to be an exploit, and this leads to modification of the timestamps of multiple directories in the "Library/SMS/Attachments". The attachment is then deleted, leaving only modified directories,

without actual files inside them:

```
2022-09-13 10:04:11.890351Z Datausage
IMTransferAgent/com.apple.datausage.messages
(Bundle ID: com.apple.datausage.messages, ID:
127) WIFI IN: 0.0, WIFI OUT: 0.0 - WWAN IN:
76281896.0, WWAN OUT: 100956502.0
2022-09-13 10:04:54.000000Z Manifest
Library/SMS/Attachments/65/05 - MediaDomain
2022-09-13 10:05:14.744570Z Datausage BackupAgent
(Bundle ID: , ID: 710) WIFI IN: 0.0, WIFI OUT:
0.0 - WWAN IN: 734459.0, WWAN OUT: 287912.0
```

2. There are also less reliable indicators, that may be treated as IOCs if several of them happened within a timeframe of minutes:

   - Modification of one or several files: *com.apple.ImageIO.plist*, *com.apple.locationd.StatusBarIconManager.plist*, *com.apple.imservice.ids.FaceTime.plist*
   - Data usage information of the services *com.apple.WebKit.WebContent*, *powerd/com.apple.datausage.diagnostics*, *lockdownd/com.apple.datausage.security*

   Example:

```
2021-10-30 16:35:24.923368Z Datausage
IMTransferAgent/com.apple.MobileSMS (Bundle ID:
com.apple.MobileSMS, ID: 945) WIFI IN: 0.0, WIFI
OUT: 0.0 - WWAN IN: 31933.0, WWAN OUT: 104150.0
2021-10-30 16:35:24.928030Z Datausage
IMTransferAgent/com.apple.MobileSMS (Bundle ID:
com.apple.MobileSMS, ID: 945)
2021-10-30 16:35:24.935920Z Datausage
IMTransferAgent/com.apple.datausage.messages
(Bundle ID: com.apple.datausage.messages, ID:
946) WIFI IN: 0.0, WIFI OUT: 0.0 - WWAN IN:
47743.0, WWAN OUT: 6502.0
2021-10-30 16:35:24.937976Z Datausage
IMTransferAgent/com.apple.datausage.messages
(Bundle ID: com.apple.datausage.messages, ID:
946)
2021-10-30 16:36:51.000000Z Manifest
Library/Preferences/com.apple.locationd.StatusBar
IconManager.plist - HomeDomain
2021-10-30 16:36:51.000000Z Manifest
Library/Preferences/com.apple.ImageIO.plist -
RootDomain
```

Another example: modification of an SMS attachment directory (but no attachment filename), followed by data usage of com.apple.WebKit.WebContent, followed by modification of com.apple.locationd.StatusBarIconManager.plist. All the events happened within a 1-3 minute timeframe, indicating the result of a successful zero-click compromise via an iMessage attachment, followed by the traces of exploitation and malicious

FROM THE SAME AUTHORS

SAS CTF and the many ways to persist a kernel shellcode on Windows 7

How to catch a wild triangle

The outstanding stealth of Operation Triangulation

activity.

```
2022-09-11 19:52:56.000000Z Manifest
Library/SMS/Attachments/98 - MediaDomain
2022-09-11 19:52:56.000000Z Manifest
Library/SMS/Attachments/98/08 - MediaDomain
2022-09-11 19:53:10.000000Z Manifest
Library/SMS/Attachments/98/08 - MediaDomain
2022-09-11 19:54:51.698609Z OSAnalyticsADDaily
com.apple.WebKit.WebContent WIFI IN: 77234150.0,
WIFI OUT: 747603971.0 - WWAN IN: 55385088.0, WWAN
OUT: 425312575.0
2022-09-11 19:54:51.702269Z Datausage
com.apple.WebKit.WebContent (Bundle ID: , ID:
1125)
2022-09-11 19:54:53.000000Z Manifest
Library/Preferences/com.apple.locationd.StatusBar
IconManager.plist - HomeDomain
2022-06-26 18:21:36.000000Z Manifest
Library/SMS/Attachments/ad/13 - MediaDomain
2022-06-26 18:21:36.000000Z Manifest
Library/SMS/Attachments/ad - MediaDomain
2022-06-26 18:21:50.000000Z Manifest
Library/SMS/Attachments/ad/13 - MediaDomain
2022-06-26 18:22:03.412817Z OSAnalyticsADDaily
com.apple.WebKit.WebContent WIFI IN: 19488889.0,
WIFI OUT: 406382282.0 - WWAN IN: 66954930.0, WWAN
OUT: 1521212526.0
2022-06-26 18:22:16.000000Z Manifest
Library/Preferences/com.apple.ImageIO.plist -
RootDomain
2022-06-26 18:22:16.000000Z Manifest
Library/Preferences/com.apple.locationd.StatusBar
IconManager.plist - HomeDomain
2022-03-21 21:37:55.000000Z Manifest
Library/SMS/Attachments/fc - MediaDomain
2022-03-21 21:37:55.000000Z Manifest
Library/SMS/Attachments/fc/12 - MediaDomain
2022-03-21 21:38:08.000000Z Manifest
Library/SMS/Attachments/fc/12 - MediaDomain
2022-03-21 21:38:23.901243Z OSAnalyticsADDaily
com.apple.WebKit.WebContent WIFI IN: 551604.0,
WIFI OUT: 6054253.0 - WWAN IN: 0.0, WWAN OUT: 0.0
2022-03-21 21:38:24.000000Z Manifest
Library/Preferences/com.apple.locationd.StatusBar
IconManager.plist - HomeDomain
```

3 An even less implicit indicator of compromise is inability to install iOS updates. We discovered malicious code that modifies one

Free Download Manager backdoored – a possible supply chain attack on Linux machines

Dissecting TriangleDB, a Triangulation spyware implant

of the system settings file named *com.apple.softwareupdateservicesd.plist*. We observed update attempts to end with an error message “Software Update Failed. An error ocurred downloading iOS”.

Network activity during exploitation

On the network level, a successful exploitation attempt can be identified by a sequence of several HTTPS connection events. These can be discovered in netflow data enriched with DNS/TLS host information, or PCAP dumps:

- Legitimate network interaction with the iMessage service, usually using the domain names *.ess.apple.com
- Download of the iMessage attachment, using the domain names .icloud-content.com, content.icloud.com
- Multiple connections to the C&C domains, usually 2 different domains (the list of known domains follows). Typical netflow data for the C&C sessions will show network sessions with significant amount of outgoing traffic.

Network exploitation sequence, Wireshark dump

The iMessage attachment is encrypted and downloaded over HTTPS, the only implicit indicator that can be used is the amount of downloaded data that is about 242 Kb.

Encrypted iMessage attachment, Wireshark dump

C&C domains

Using the forensic artifacts, it was possible to identify the set of domain name used by the exploits and further malicious stages. They can be used to check the DNS logs for historical information, and to identify the devices currently running the malware:

addatamarket[.]net
backuprabbit[.]com
businessvideonews[.]com
cloudsponcer[.]com
datamarketplace[.]net
mobilegamerstats[.]com
snoweeanalytics[.]com
tagclick-cdn[.]com
topographyupdates[.]com
unlimitedteacup[.]com

virtuallaughing[.]com
web-trackers[.]com
growthtransport[.]com
anstv[.]net
ans7tv[.]net

APPLE IOS | CYBER ESPIONAGE | DATA THEFT | DIGITAL FORENSICS | MOBILE MALWARE | TARGETED ATTACKS | TRIANGULATION | VULNERABILITIES AND EXPLOITS

Operation Triangulation: iOS devices targeted with previously unknown malware

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

BIL
Posted on June 1, 2023. 2:41 pm

iOS 16.x not affected?

Reply

SECURELIST
Posted on June 2, 2023. 11:10 am

Hi Bil!

We identified that the latest version of iOS that was targeted by Triangulation is 15.7. However, given the sophistication of the cyberespionage campaign and the complexity of analysis of iOS platform, we can't guarantee that other versions of iOS are not affected.

Reply

SEDRIC LOUISSAINT
Posted on June 2, 2023. 11:07 am

Very well written! Thank you for sharing and being transparent!

Reply

JANE DOE
Posted on June 2, 2023. 3:19 pm

For clarity, this forensic examination is about the novel malware (the payload delivery mechanism could be Pegasus or Graphite) and not the built-in Apple backdoor as evident by the Wireshark dump and the supplied C&C domains. However, make no mistake about this, yes, the device manufacturer (Apple) could be compelled to work with the IC (intelligence community) and we would never know (network traffic could appear as routine Apple service). For now, on Apple's merit, the device iCloud synchronization and back-ups are end-to-end encrypted (if enabled) without Apple having the key. The question is if there is mechanism to recover the one's private key (e.g. similar to how the macOS FileVault FDE key could be "stored" with Apple for convenience).

Reply

WAQAS
Posted on June 2, 2023. 7:28 pm

It's unfortunate to see Kaspersky, a long-standing company, facing targeting from both the US and Russian intelligence agencies.

Reply

JJ
Posted on June 3, 2023. 7:20 am

You state: " Without any user interaction, the message triggers a vulnerability that leads to code execution."
Is this vulnerability reported to apple and what is their reaction.

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of the SideWinder APT group

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Interpreting your great report, a bug fix from apple and a reboot should fix the attack?

Reply

SECURELIST
Posted on June 5, 2023. 2:38 pm

Hi JJ

Yes. We have shared information with the Apple Security Research team.

As of time of writing we were able to identify one of many vulnerabilities that were exploited that is most likely CVE-2022-46690. This vulnerability was fixed in iOS 16.2. However, given the sophistication of the cyberespionage campaign and the complexity of analysis of the iOS platform, further research will surely reveal more details on the matter. We will update the community about new findings once they emerge.

As to rebooting, Triangulation blocks the opportunity to update iOS which means that even if the device is rebooted it still has an opportunity to re-infect it. A factory reset combined with the immediate system update would solve the problem.

Reply

ANNIE
Posted on June 12, 2024. 3:59 am

Hi, is iOS 16.1 still the latest version this malware has been seen on as of now?

Reply

SECURELIST
Posted on June 13, 2024. 8:52 am

Hi Annie,

We haven't seen Triangulation deployments happening after we published information about the attack.

Reply

ARTUR
Posted on June 3, 2023. 8:41 am

What about iOS 16.x is it not affected by „default" or via „Lockdown Mode" ?

Reply

SECURELIST

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities

Posted on June 5, 2023. 2:43 pm

Hi Artur!

Kaspersky cybersecurity experts identified that the latest version of iOS that was targeted by Triangulation is 15.7. However, given the sophistication of the cyberespionage campaign and the complexity of analysis of iOS platform, the further research may reveal more details on the matter. We will update the community about new findings once they emerge.

Reply

SECURELIST
Posted on June 5, 2023. 5:10 pm

Most probably, Lockdown Mode can help protecting against this attack.

Reply

TIMOTHY AVELE
Posted on June 4, 2023. 5:51 am

Thank you for this thourough and in-depth analysis. But could this exploit be used on Android perhaps using a different name?

Reply

SECURELIST
Posted on June 5, 2023. 2:58 pm

During the research we have not observed exploits for Android.

Reply

FORRAI TIBOR
Posted on June 4, 2023. 8:56 pm

Dear KL analysts,
Could you share Triangulation malware file SHA-1 or SHA-256 checksums, besides the already published spear-phishing domain names?
Thanks in advance!

Reply

SECURELIST
Posted on June 5, 2023. 3:18 pm

Our investigation of this attack is ongoing. All the related information will be posted on the Operation Triangulation page soon: https://securelist.com/trng-2023/

Reply

MOHAMED ARAFA
Posted on June 7, 2023. 12:15 am

First thank you Kasper Team for this great summary. actually include all what happen by easy way that really very simplify my problem that i was not understood since 4 months ago till last few hours , although contacted Apple team many times ,

unfortunately the problems still at ios 16 for sure as you advised due to wrong backup or recovery as we never guess that apple ID may be hacked ,

we are kindly ask you to advised us if there Kasper tool or support team can explore who is hacking us ? or is there exeperts can help us by provide them the analytic data ? what ever it`s cost , we trust kasper team as always will support

Reply

JW
Posted on June 11, 2023. 3:31 am

Doesn't the malicious message with an attachment trigger an alert if you have them enabled? I am wondering how this is 0-click without user interaction, if the device shows an alert and/or vibrates when a message comes in

Reply

SECURELIST
Posted on June 13, 2023. 11:13 am

The malicious message is malformed and does not trigger any alerts or notifications for user

Reply

TIBOR FORRAI
Posted on June 20, 2023. 9:09 am

Hello, how come there is no further information after almost 3weeks?

Reply

JILL COBB
Posted on August 6, 2023. 6:42 pm

This is currently in my phone and I've tried to report to the police but they shunned me off. I think i can date it too at least May 22. How can i help?

Reply

LJK
Posted on October 27, 2023. 10:26 am

Let's hope for better zero click detection by apple

Reply

LJK
Posted on October 27, 2023. 10:28 am

There are many more infection chains!
Companies and private individuals who have been abusing their abilities the last 3-4 years.
Phones are not secure. Some attacks seem to be made possible on purpose.
I hope Kaspersky starts offering analysis of app privacy and backup logs.

Thank your for doing this

Reply

PAULINHO
Posted on June 25, 2024. 6:41 am

Just curious how long it takes your team to analyse the whole exploit chain

Reply

// LATEST POSTS

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS,
ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023

Privacy Policy | License Agreement | Cookies