XLoader Disguises as Android Apps, Has FakeSpy Links

By By: Hara Hiroaki, Lilang Wu, Lorin Wu Apr 02, 2019 Read time: 6 min (1602 words)

Published: 2019-04-02 · Archived: 2026-04-05 14:04:56 UTC

In previous attacks, XLoader posed as Facebook, Chrome and other legitimate applications to trick users into downloading its malicious app. Trend Micro researchers found a new variant that uses a different way to lure users. This new XLoader variant poses as a security app for Android devices, and uses a malicious iOS profile to affect iPhone and iPad devices. Aside from a change in its deployment techniques, a few changes in its code set it apart from its previous versions. This newest variant has been labeled XLoader version 6.0 (detected as AndroidOS_XLoader.HRXD), following the last version discussed in a previous research on the malware family.

Infection chain

The threat actors behind this version used several fake websites as their host — copying that of a Japanese mobile phone operator's website in particular — to trick users into downloading the fake security Android application package (APK). Monitoring efforts on this new variant revealed that the malicious websites are spread through smishing. The infection has not spread very widely at the time of writing, but we've seen that many users have already received its SMS content.

Figure 1. Screenshot of a fake website that hosts XLoader

In the past, XLoader showed the ability to mine cryptocurrency on PCs and perform account phishing on iOS devices. This new wave also presents unique attack vectors based on the kind of device it has accessed.

In the case of Android devices, accessing the malicious website or pressing any of the buttons will prompt the download of the APK. However, successfully installing this malicious APK requires that the user has allowed the installation of such apps as controlled in the Unknown Sources settings. If users allow such apps to be installed, then it can be actively installed on the victim's device.

The infection chain is slightly more roundabout in the case of Apple devices. Accessing the same malicious site would redirect its user to another malicious website (hxxp://apple-icloud[.]qwq-japan[.]com or hxxp://apple-icloud[.]zqo-japan[.]com) that prompts the user to install a malicious iOS configuration profile to solve a network issue preventing the site to load. If the user installs the profile, the malicious website will open, revealing it to be an Apple phishing site, as seen in figure 2.

Figure 2. Screenshots of the malicious websites for iOS device user

Technical analysis

Most of this new attack's routines are similar to those of the previous XLoader versions. However, as mentioned earlier, an analysis of this new variant showed some changes in its code in line with its new deployment method. We discuss these changes and its effect on Android and Apple devices.

Malicious APK

Like its previous versions, XLoader 6.0 abuses social media user profiles to hide its real C&C addresses, but this time its threat actors chose the social media platform Twitter, which was never used in previous attacks. The real C&C address is encoded in the Twitter names, and can only be revealed once decoded. This adds an extra layer against detection. The code for this characteristic and the corresponding Twitter accounts can be seen in figures 3 and 4 respectively.

Figure 3. Code snippets showing XLoader 6.0 abusing twitter to hide the real C&C address

Figure 4. Malicious Twitter pages that hide the real C&C address

Version 6.0 also adds a command called “getPhoneState”, which collects unique identifiers of mobile devices such as IMSI, ICCID, Android ID, and device serial number. This addition is seen in Figure 5. Considering the other malicious behaviors of XLoader, this added operation could be very dangerous as threat actors can use it to perform targeted attacks.

Figure 5. Code snippets that show XLoader 6.0 adding a new C&C command, getPhoneState

Malicious iOS profile

In the case of Apple devices, the downloaded malicious iOS profile gathers the following:

- Unique device identifier (UDID)
- International Mobile Equipment Identity (IMEI)
- Integrated Circuit Card ID (ICCID)
- Mobile equipment identifier (MEID)
- Version number
- Product number

The profile installations differ depending on the iOS. For versions 11.0 and 11.4, the installation is straightforward. If a user visits the profile host website and allows the installer to download, the iOS system will go directly to the “Install Profile” page (which shows a verified safety certificate), and then request the users’ passcode for the last step of installation.

Figure 6. Installation process for iOS 11.0 and iOS 11.4

On later versions, specifically iOS 12.1.1 and iOS 12.2, the process is different. After the profile is downloaded, the iOS system will first ask users to review the profile in their settings if they want to install it. Users can see a “Profile Downloaded” added in their settings (this feature is in iOS 12.2, but not on iOS 12.1.1). This gives users a chance to see details and better understand any changes made. After the review, the process is the same as above.

Figure 7. Installation process for iOS 12.1.1 and iOS 12.2

After the profile is installed, the user will then be redirected to another Apple phishing site. The phishing site uses the gathered information as its GET parameter, allowing the attacker to access the stolen information.

Figure 8. Code snippet showing how the profile gathers information

Ongoing activity

While monitoring this particular threat, we found another XLoader variant posing as a pornography app aimed at South Korean users. The "porn kr sex" APK connects to a malicious website that runs XLoader in the background. The website uses a different fixed twitter account (https://twitter.com/fdgoer343). This attack, however, seems exclusive to Android users, as it does not have the code to attack iOS devices.

Figure 9. Screenshot of pornography website used by the new XLoader variant

Succeeding monitoring efforts revealed a newer variant that exploits the social media platforms Instagram and Tumblr instead of Twitter to hide its C&C address. We labeled this new variant XLoader version 7.0, because of the different deployment method and its use of the native code to load the payload and hide in Instagram and Tumblr profiles. These more recent developments indicate that XLoader is still evolving.

Adding connections to FakeSpy

We have been seeing activity from XLoader since 2018, and have since followed up our initial findings with a detailed research revealing a wealth of activity dating back to as early as January 2015, which outlined a major discovery—its connection to FakeSpy. The emergence of XLoader 6.0 does not only indicate that the threat actors behind it remain active; it also holds fresh evidence of its connection to FakeSpy.

One such immediately apparent connection was the similar deployment technique used by both XLoader 6.0 and FakeSpy. It had again cloned a different legitimate Japanese website to host its malicious app, similar to what FakeSpy had also done before. Their similarity is made more apparent by looking at their naming method for downloadable files, domain structure of fake websites and other details of their deployment techniques, exemplified in figure 10.

Figure 10. Source code for malicious websites used by XLoader (left) and FakeSpy (right)

XLoader 6.0 also mirrors the way FakeSpy hides its real C&C server. When before it had used several different social media platforms, it now uses the Twitter platform, something FakeSpy has done in its past attacks. Analysis of the malicious iOS profile also revealed further connections, as the profile can also be downloaded from a website that FakeSpy deployed early this year.

Conclusion and security recommendations

The continued monitoring of XLoader showed how its operators continuously changed its features, such as its attack vector deployment infrastructure and deployment techniques. This newest entry seems to indicate that these changes won't be stopping soon. Being aware of this fact can help create defensive strategies, as well as prepare for upcoming attacks.

In addition, just as uncovering new characteristics is important, finding ones we've also seen in a different malware family like FakeSpy also provides valuable insight. Links between XLoader and FakeSpy can give clues to the much broader inner workings of the threat actors behind them.

Perhaps more information on XLoader will be known in the future. For now, users can make the best of the knowledge they have now to significantly reduce the effectivity of such malware. Users of iOS can remove the malicious profile using the Apple Configurator 2open on a new tab, Apple's official iOS helper app for managing Apple devices. Following simple best practicesnews article, like strictly downloading applications or any files from trusted sources and being wary of unsolicited messages, can also prevent similar attacks from compromising devices.

Trend Micro Solutions

Users can take advantage of Trend Micro™ Mobile Security for Android™products (available on Google Playopen on a new tab) to block malicious apps that may exploit this vulnerability. End users and enterprises can also benefit from its multilayered security capabilities that secure the device's data and privacy, and safeguard them from ransomware, fraudulent websites, and identity theft. For organizations, Trend Micro™ Mobile Security for Enterpriseproducts provides device, compliance and application management, data protection, and configuration provisioning. It also protects devices from attacks that leverage vulnerabilities, prevents unauthorized access to apps, and detects and blocks malware and access to fraudulent websites.

Indicators of Compromise

SHA256	Package	App label
332e68d865009d627343b89a5744843e3fde4ae870193f36b82980363439a425	ufD.wykyx.vlhvh	SEX kr porn
403401aa71df1830d294b78de0e5e867ee3738568369c48ffafe1b15f3145588	ufD.wyjyx.vahvh	佐川急便
466dafa82a4460dcad722d2ad9b8ca332e9a896fc59f06e16ebe981ad3838a6b	com.dhp.ozqh	Facebook
5022495104c280286e65184e3164f3f248356d065ad76acef48ee2ce244ffdc8	ufD.wyjyx.vahvh	Anshin Scan
a0f3df39d20c4eaa410a61a527507dbc6b17c7f974f76e13181e98225bda0511	com.aqyh.xolo	佐川急便
cb412b9a26c1e51ece7a0e6f98f085e1c27aa0251172bf0a361eb5d1165307f7	jp.co.sagawa.SagawaOfficialApp	佐川急便

Malicious URLs:
hxxp://38[.]27[.]99[.]11/xvideo/
hxxp://apple-icloud[.]qwe-japan[.]com
hxxp://apple-icloud[.]qwq-japan[.]com/
hxxp://apple-icloud[.]zqo-japan[.]com/
hxxp://files.spamo[.]jp/佐川急便.apk
hxxp://mailsa-qae[.]com
hxxp://mailsa-qaf[.]com

hxxp://mailsa-qau[.]com
hxxp://mailsa-qaw[.]com
hxxp://mailsa-wqe[.]com
hxxp://mailsa-wqo[.]com
hxxp://mailsa-wqp[.]com
hxxp://mailsa-wqq[.]com
hxxp://mailsa-wqu[.]com
hxxp://mailsa-wqw[.]com
hxxp://nttdocomo-qae[.]com
hxxp://nttdocomo-qaq[.]com
hxxp://nttdocomo-qaq[.]com/aa
hxxp://nttdocomo-qar[.]com
hxxp://nttdocomo-qat[.]com
hxxp://nttdocomo-qaw[.]com
hxxp://sagawa-reg[.]com/
hxxp://www[.]711231[.]com
hxxp://www[.]759383[.]com
hxxp://www[.]923525[.]com
hxxp://www[.]923915[.]com
hxxp://www[.]975685[.]com
Malicious Twitter accounts:
https://twitter.com/lucky88755
https://twitter.com/lucky98745
https://twitter.com/lucky876543
https://twitter.com/luckyone1232
https://twitter.com/sadwqewqeqw
https://twitter.com/gyugyu87418490
https://twitter.com/fdgoer343
https://twitter.com/sdfghuio342
https://twitter.com/asdqweqweqeqw

https://twitter.com/ukenivor3
Malicious Instagram account:
https://www.instagram.com/freedomguidepeople1830/
Malicious Tumblr accounts:
https://mainsheetgyam.tumblr.com/
https://hormonaljgrj.tumblr.com/
https://globalanab.tumblr.com/
C&C addresses:
104[.]160[.]191[.]190:8822
61[.]230[.]204[.]87:28833
61[.]230[.]204[.]87:28844
61[.]230[.]204[.]87:28855
61[.]230[.]205[.]122:28833
61[.]230[.]205[.]122:28844
61[.]230[.]205[.]122:28855
61[.]230[.]205[.]132:28833
61[.]230[.]205[.]132:28844
61[.]230[.]205[.]132:28855

Source: https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/