XCSSET Mac Malware: Infects Xcode Projects, Uses 0Days

blog.trendmicro.com/trendlabs-security-intelligence/xcsset-mac-malware-infects-xcode-projects-performs-uxss-attack-on-safari-other-browsers-leverages-zero-day-exploits/

August 13, 2020

Exploits & Vulnerabilities

Further investigation led us to a developer's Xcode project that contained XCSSET source malware, which leads to a rabbit hole of malicious payloads. Most notable in our investigation is the discovery of two zero-day exploits.

By: Mac Threat Response, Mobile Research Team August 13, 2020 Read time: (words)

We have discovered an unusual infection related to Xcode developer projects. Upon further investigation, we discovered that a developer's Xcode project at large contained the source malware, which leads to a rabbit hole of malicious payloads. Most notable in our investigation is the discovery of two zero-day exploits: one is used to steal cookies via a flaw in the behavior of Data Vaults, another is used to abuse the development version of Safari.

This scenario is quite unusual; in this case, malicious code is injected into local Xcode projects so that when the project is built, the malicious code is run. This poses a risk for Xcode developers in particular. The threat escalates since we have identified affected developers who shared their projects on GitHub, leading to a supply-chain-like attack for users who rely on these repositories as dependencies in their own projects. We have also identified this threat in sources such as VirusTotal, which indicates this threat is at large.

This blog will summarize the findings of this threat, while its accompanying technical brief contains the full details of this attack. We detected the entry threat as TrojanSpy.MacOS.XCSSET.A and its command and control (C&C) related files as Backdoor.MacOS.XCSSET.A.

This threat primarily spreads via Xcode projects and maliciously modified applications created from the malware. It is not yet clear how the threat initially enters these systems. Presumably, these systems would be primarily used by developers. These Xcode projects have been modified such that upon building, these projects would run a malicious code. This eventually leads to the main XCSSET malware being dropped and run on the affected system. Infected users are also vulnerable to having their credentials, accounts, and other vital data stolen.

Once present on an affected system, XCSSET is capable of the following behavior:

- Using exploits, it abuses the existing the Safari and other installed browsers to steal user data. In particular, it
- Uses a vulnerability to read and dump Safari cookies
- Uses the Safari development version to inject JavaScript backdoors onto websites via a Universal Cross-site Scripting (UXSS) attack

- It steals information from the user’s Evernote, Notes, Skype, Telegram, QQ ,and WeChat apps
- It takes screenshots of the user’s current screen
- It uploads files from the affected machines to the attacker’s specified server
- It encrypts files and shows a ransom note, if commanded by the server

The UXSS attack is theoretically capable of modifying almost every part of the user’s browser experience as arbitrary JavaScript-injected code. These modifications include:

- Modifying displayed websites
- Modifying /replacing Bitcoin/cryptocurrency addresses
- Stealing amoCRM, Apple ID, Google, Paypal, SIPMarket, and Yandex credentials
- Stealing credit card information from the Apple Store
- Blocking the user from changing passwords but also stealing newly modified passwords
- Capturing screenshots of certain accessed sites

The method of distribution used can only be described as clever. Affected developers will unwittingly distribute the malicious trojan to their users in the form of the compromised Xcode projects, and methods to verify the distributed file (such as checking hashes) would not help as the developers would be unaware that they are distributing malicious files.

Further details of this attack may be found in its related technical brief.

Trend Micro Solutions

To protect systems from this type of threat, users should only download apps from official and legitimate marketplaces. Users can also consider multilayered security solutions such as Trend Micro Antivirus for Mac, which provides comprehensive security and multidevice protection against cyberthreats.

Enterprises can take advantage of Trend Micro’s Smart Protection Suites with XGen™ security, which infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity or endpoint.

Indicators of Compromise

SHA256	Filename	Detection
6fa938770e83ef2e177e8adf4a2ea3d2d5b26107c30f9d85c3d1a557db2aed41	main.scpt	TrojanSpy.MacOS.XCSSET.A
7e5343362fceeae3f44c7ca640571a1b148364c4ba296ab6f8d264fc2c62cb61	main.scpt	TrojanSpy.MacOS.XCSSET.A
857dc86528d0ec8f5938680e6f89d846541a41d62f71d003b74b0c55d645cda7	main.scpt	TrojanSpy.MacOS.XCSSET.A
6614978ab256f922d7b6dbd7cc15c6136819f4bcfb5a0fead480561f0df54ca6	xcassets	TrojanSpy.MacOS.XCSSET.A
ac3467a04eeb552d92651af1187bdc795100ea77a7a1ac755b4681c654b54692	xcassets	TrojanSpy.MacOS.XCSSET.A
d11a549e6bc913c78673f4e142e577f372311404766be8a3153792de9f00f6c1	xcassets	TrojanSpy.MacOS.XCSSET.A
532837d19b6446a64cb8b199c9406fd46aa94c3fe41111a373426b9ce59f56f9	speedd	Backdoor.MacOS.XCSSET.A
4f78afd616bfefaa780771e69a71915e67ee6dbcdc1bc98587e219e120f3ea0d	firefoxd	Backdoor.MacOS.XCSSET.A
819ba3c3ef77d00eae1afa8d2db055813190c3d133de2c2c837699a0988d6493	operad	Backdoor.MacOS.XCSSET.A
73f203b5e37cf34e51f7bf457b0db8e4d2524f81e41102da7a26f5590ab32cd9	yandexd	Backdoor.MacOS.XCSSET.A
ccc2e6de03c0f3315b9e8e05967fcc791d063a392277f063980d3a1b39db2079	edged	Backdoor.MacOS.XCSSET.A
6622887a849b503b120cfef8cd76cd2631a5d0978116444a9cb92b1493e42c29	braved	Backdoor.MacOS.XCSSET.A
32fa0cdb46f204fc370c86c3e93fa01e5f5cb5a460407333c24dc79953206443	agentd	Backdoor.MacOS.XCSSET.A
924a89866ea55ee932dabb304f851187d97806ab60865a04ccd91a0d1b992246	agentd-kill	Backdoor.MacOS.XCSSET.A
af3a2c0d14cc51cc8615da4d99f33110f95b7091111d20bdba40c91ef759b4d7	agentd-log	Backdoor.MacOS.XCSSET.A

534f453238cfc4bb13fda70ed2cda701f3fb52b5d81de9d8d00da74bc97ec7f6	dskwalp	Trojan.MacOS.XCSSET.A
172eb05a2f72cb89e38be3ac91fd13929ee536073d1fe576bc8b8d8d6ec6c262	chkdsk	Trojan.MacOS.XCSSET.A
a238ed8a801e48300169afae7d27b5e49a946661ed91fab4f792e99243fbc28d	Pods_shad	Trojan.MacOS.XCSSET.A

IP/Domain	Web Reputation Category
hxxps://adobestats.com/	C&C Server
hxxps://flixprice.com/	C&C Server
46.101.126.33	C&C Server