Detects new Xcode malware targeting iOS developers

International cybersecurity experts have broadcast an urgent message about a malicious Xcode project called XcodeSpy. The malware is currently targeting iOS software developers in a supply-chain attack.

The ultimate goal is to install a backdoor on a developer's macOS computer for later malicious activity.

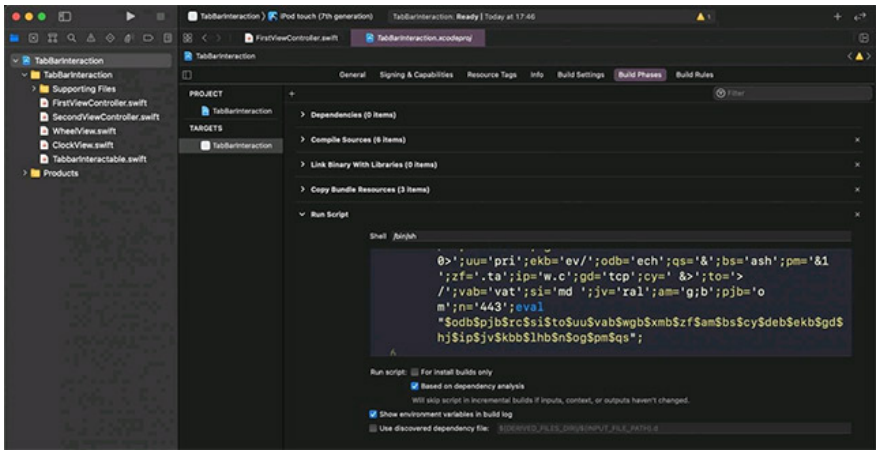
If you do not know, Xcode is a free application development environment created by Apple and built into the Mac operating system. Xcode allows developers to create apps that run on macOS, iOS, tvOS, and watchOS.

Like many other application development environments, developers on Xcode often create specialized projects to perform specific functions. These projects can then be shared online so other developers can contribute or leverage to create their own products.

Taking advantage of this fact, attackers are increasingly actively creating malicious, fake projects, in the hope that they can be incorporated into other developers' applications. When those apps are compiled, the malicious component infects the developer's computer in a typical supply chain attack.

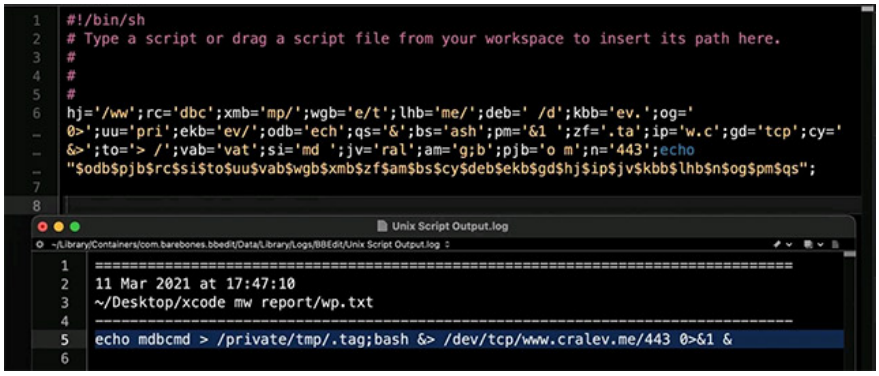
Researchers from cybersecurity company SentinelOne have discovered a malicious version of the legitimate iOS project TabBarInteraction Xcode, currently being spread during a supply chain attack.

As part of the attack, the attacker cloned the legitimate TabBarInteraction project and added a cryptic malicious 'Run Script' script to the project, as shown below. This malicious version of TabBarInteraction has been dubbed '**XcodeSpy** ' by SentinelOne .



Once the project is built, Xcode will automatically execute the Run Script to open a remote shell back to the attacker's server. This server is called **cralev.me** .

' *The script will create a hidden file named .tag in the / tmp directory, containing a single command: mdbcmd. It will then be routed through a shell, sent back to the attackers' C2 server* , "explained SentinelOne security expert Phil Stokes in a new report.



By the time SentinelOne discovered this malicious project, the C2 server was no longer available, so it is not clear what actions were taken through this back-interacting shell.

However, researchers have discovered two malware samples uploaded to VirusTotal containing the same string " **/private/tmp/.tag** ". That may indicate that they are part of this attack.

' *By the time the malicious Xcode project was discovered, the C2* ***cralev [.] Me*** *server was offline. Therefore it is not possible to determine the result of the* ***mdbcmd*** *command* ***directly*** *. Fortunately, however, there are two EggShell backdoor templates on VirusTotal that contain the Telltale XcodeSpy* ***/private/tmp/.tag*** *' string .*

The Backdoor EggShell allows threat agents to upload and download files, execute commands, and snoop on the victim's microphone, camera, and keyboard.

Currently, it is not clear how this malicious Xcode project was distributed.