Rising usage of Apple Developer Certificates for signing Windows malware

Author: Piotr Mazurkiewicz
No of pages: 10
Read time: 7 min

Contents

1 Introduction

This research has been inspired by latest MagicSword article "Apple iOS Distribution Certificate Used to Sign Windows Malware". As we dive deeper into the world of leaked Apple Developer Certificates, we discovered a widespread pattern of misuse of them to sign malicious Windows PE.

Several websites and repositories on the internet circulate leaked or unauthorized iOS Enterprise Developer Certificates or Apple Developer Certificates. These sources typically claim host certificates that can be used to sign iOS apps outside the App Store. From a security perspective, this is significant because such certificates are commonly abused for:

- Malware distribution on iOS
- Bypassing Apple's app review and security controls
- Installing untrusted apps on user devices
- **Serve up the Windows PE binary as signed to bypass some security controls or to look more like a legitimate app since it's signed**

One example often referenced in discussions about certificate abuse is a GitHub repository claiming to host "the latest iOS Enterprise Development Certificates" and offering programmatic access to them. This is emblematic of the broader trend of leaked enterprise certificates circulating publicly.
Additionally, various public webpages aggregate similar certificate collections or offer sign-your-binary "services". These websites typically function as hubs where users can obtain or apply enterprise certificates for sideloading purposes, again, often outside legitimate usage.

Example sites:

- hxxps://beacons.ai/orion_sideloading/certificates
- hxxps://beacons.ai/ziolexy/certificates
- hxxps://linktr.ee/tutelboy
- hxxps://esignhub.bio.link/
- hxxps://jorkthepork.com/

Figure 1 A screenshot of OrionSideloading webpage offering various types of Apple Developer Certificates for download and malicious use

There's also a GitHub repository with massive number of certificates accessible here: hxxps://github.com/loyahdev/certificates

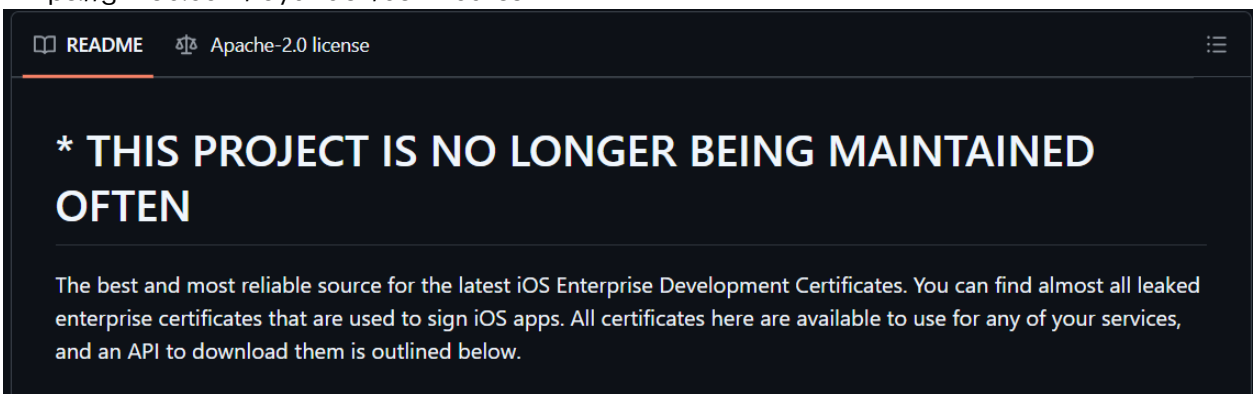

Figure 2 Screenshot of github repo containing an impresive collection of iOS Developer Certificates

Almost all of the sites offer very similar list of available certificates, with most offer certificates created for organizations (according to the certificate name) like:

- Sunshine Insurance Group Co., Ltd
- China CITIC Bank Corporation Limited
- Rizhao Sunday Power Generation Co., Ltd.
- Sun Life Everbright Life Insurance Co.,Ltd
- Bank of Chongqing Co.,Ltd.
- Sunshine Insurance Group Co., Ltd.
- Ministere de l Emploi de la Protection Sociale
- Mylan INC
- Bank of Chongqing Co.,Ltd.

2 A bit more info about Apple Developer Certificates

2.1 Purpose behind the certificates

To develop and distribute applications for macOS, you must enroll in the Apple Developer Program. Membership provides access to an Apple Developer Certificate, which allows you to digitally sign your applications. Code signing is a core part of Apple's security model and a prerequisite for seamless deployment.

Technically, unsigned applications can still be executed on macOS. In practice, however, doing so introduces conflicts and often requires elevated user privileges. This is due to Gatekeeper, Apple's built-in security mechanism designed to ensure that only trusted software runs on a system.

When a user attempts to open an unsigned app, Gatekeeper blocks it by default. To proceed, the user must take additional steps, such as:

- Manually approving the app via System Settings → Privacy & Security → "Open Anyway"
- Removing the quarantine attribute using command-line tools
- Temporarily adjusting security policies per macho file

These steps are manageable for technical users, but they create unnecessary complexity in corporate environments. They also require a higher level of system access, which is typically restricted in managed enterprise setups.

In contrast, applications signed with a valid Apple Developer Certificate are recognized as coming from an identified developer. As a result, they can be launched immediately without additional prompts, creating smoother and more professional user experience.

For organizations operating primarily within the macOS ecosystem - particularly those distributing proprietary tools internally - having a proper signing certificate is essential. Apple provides a dedicated enrollment option, the Apple Developer Enterprise Program, specifically for this purpose. This program allows companies to sign and distribute in-house applications directly to employees without publishing them on the public App Store.

It is important to note, that Enterprise-signed applications are strictly limited to internal distribution. Deploying them externally, whether to customers, partners, or the general public, constitutes a violation of Apple's Enterprise Program Terms of Service.

In short, while it is technically possible to operate without a developer certificate, doing so introduces avoidable friction, security prompts, and administrative overhead. For any serious macOS development effort, especially in a corporate setting, proper enrollment in Apple's developer ecosystem is not just recommended, but practically must-have.

2.2 Impact on Windows OS and its users

The abuse of legitimately issued code-signing certificates by threat actors is a sophisticated technique designed to subvert the fundamental "chain of trust" that operating systems rely on. While Apple Developer Certificates are natively used for macOS and iOS, threat actors frequently leverage them to sign Windows PE files to bypass security solutions that treat validly signed binaries, even from different ecosystems, as lower risk.

Overview of Certificate Abuse

Adversaries obtain these certificates through several methods:

- Direct Purchase/Resellers: Certificates are sometimes bought by third-party resellers who do not perform adequate due diligence on their customers.
- Theft and Compromise: Legitimate companies, such as those listed, may have their development environments or certificate store compromised, allowing attackers to export the private key and sign malicious payloads.
- Fraudulent Enrollment: Actors use stolen identity documents or shell companies to enroll in the Apple Developer Program.

2.3 Most popular certificates used to sign Windows malware

In addition to the certificate described in MagicSword research ("Jafar Sakhar" (UID: J4FUC525X9), we managed to identify many more, less popular, certificates used to sign Windows malware.

Several other Apple Developer certificates show notable, but substantially lower, levels of malicious usage. These include:

- Mylan Inc. (UID: 68SXA5MV6R) – 27 malicious PE files
- GAC Toyota Motor Co., Ltd. (UID: 6L3J23729R) – 18 malicious PE files
- Shanghai Foreign Aviation Service Co., Ltd. (UID: 827L6D9F6E) – 14 malicious PE files
- Ministère de l'Emploi et de la Protection Sociale (UID: 9Y5MZH2469) – 12 malicious PE files
- Kotak Mahindra Bank Ltd. (UID: 2JL8954UQK) – 11 malicious PE files

Most of the certificates are registered for companies geolocated in Asia.

Overall, the "Jafar Sakhar" certificate exhibits an order of magnitude higher malicious usage than any other certificate in the dataset, suggesting it played a central role in a large-scale or long-running malware-signing operation. The remaining certificates, while also abused, appear far less frequently and represent smaller clusters of misuse.

CN	UID	Sum
iPhone Distribution: Mylan Inc.	68SXA5MV6R	27
iPhone Distribution: GAC TOYOTA MOTOR CO.\,LTD	6L3J23729R	18
iPhone Distribution: Shanghai Foreign Aviation Service Co.\, Ltd.	827L6D9F6E	14

iPhone Distribution: Ministere de l Emploi de la Protection Sociale	9Y5MZH2469	12
iPhone Distribution: Kotak Mahindra Bank Ltd	2JL8954UQK	11
iPhone Distribution: VNG SINGAPORE PTE LTD (5DTU4K85Q7)	5DTU4K85Q7	8
iPhone Distribution: Gac Trumpchi Car Sales Co.\, Ltd.	SRQNM733R4	7
iPhone Distribution: Thu Phung Phuong (V3G76YR455)	V3G76YR455	6
iPhone Distribution: BEIJING TIANYUAN NEW ENERGY TECHNOLOGY CO.\,LTD.	UX47YY36D4	5
iPhone Distribution: TCL household Appliance Marketing Co.\, LTD	2GM7ZL62GN	5
iPhone Distribution: ANBANG INSURANCE LTD.	H5SM6ZV38F	5
iPhone Distribution: Flavilet De Guzman (LYK9LJG4PQ)	LYK9LJG4PQ	4
iPhone Distribution: China Mobile Group Jiangsu Company Limited	852BN2UPEC	4
iPhone Distribution: mei liu (BXK4A984CH)	BXK4A984CH	3
iPhone Distribution: Bank of Jiangsu Co.\, Ltd.	P6C8BKXGNH	2
iPhone Distribution: China Mobile Group Shandong Co.\, Ltd.	773Z3KSBGR	2
iPhone Distribution: Googdood CO.\, LTD. (B22BQCU3RZ)	B22BQCU3RZ	2
iPhone Distribution: Sunshine Insurance Group Co.\, Ltd.	LH28XA7T22	2
iPhone Distribution: HDFC Life Insurance Company Limited	CDX79FRC6X	2
iPhone Distribution: Kiran Manzoor (PW69H46354)	PW69H46354	2
iPhone Distribution: BANK NEGARA INDONESIA (PERSERO)\, PT TBK	LYN9JKT395	2
iPhone Distribution: China Mobile Group Shandong Co.\, Ltd.	773Z3KSBGR	2
iPhone Distribution: Emre Sabri Aktay (HH3NU426A8)	HH3NU426A8	2
iPhone Distribution: HDFC Life Insurance Company Limited	CDX79FRC6X	2
iPhone Distribution: Henan Provincial Communications Planning Survey & Design Institute Co.\,Ltd.	W94WHMS6HF	2
iPhone Distribution: FPT Software Company Limited	854MF4G8EF	2
iPhone Distribution: Aldo Group Inc	MB36D7323X	1
iPhone Distribution: JiaJia Qiu	JT6T3GY5F5	1
iPhone Distribution: Quantum Hi-technology Trade Co.\,Ltd	258LMP5L4A	1
iPhone Distribution: BMW Brilliance Automotive Ltd.	4YR932H55S	1
iPhone Distribution: saed aleutaybi (C2R96QBQDD)	C2R96QBQDD	1
iPhone Distribution: Capinfo Company Limited	Z33AYFK3S6	1

iPhone Distribution: China Mobile Communications Corporation	L28Y5F2E2C	1
iPhone Distribution: GLOBAL TAKEOFF\, INC	VTM793CVGA	1
iPhone Distribution: ONCE (4ZQ76CHKAT)	4ZQ76CHKAT	1
iPhone Distribution: SANY Group Co.\,Ltd	BW96G9Z5R7	1
iPhone Distribution: Sunshine Insurance Group Co.\, Ltd.	LH28XA7T22	1
iPhone Distribution: Volentix Labs Inc (RX3AT725L2)	RX3AT725L2	1

2.4 Threat Hunting for similar malware in your organization

Microsoft Defender for Endpoint simple KQL can be used for hunting:

```
DeviceFileCertificateInfo
| where Issuer == "Apple Worldwide Developer Relations Certification Authority"
| where Signer startswith "iPhone Distribution"
```

For Sysmon hunting, you can look for specific Signer inside of Event ID 7, however this event is disabled by default and needs to be configured before.

About Atos Group

Atos Group is a global leader in digital transformation with c. 56,000 employees and annual revenue of c. €7.2 billion (pro forma for the disposal of Advanced Computing activities), operating in 61 countries under two brands – Atos for services and Eviden for products and systems. European number one in cybersecurity and cloud, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us

atos.net
atos.net/career