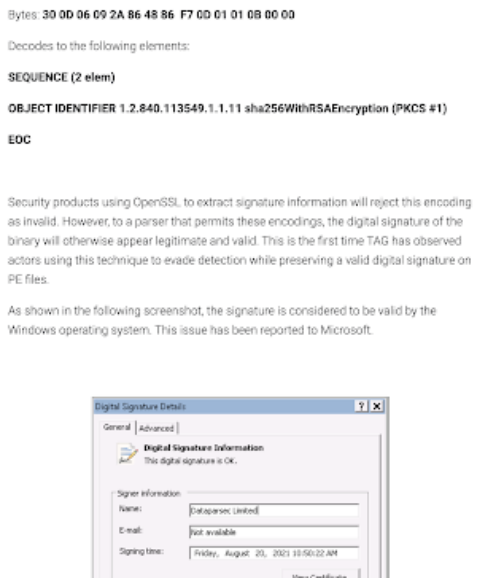
Financially motivated actor breaks certificate parsing to avoid detection

blog.google/threat-analysis-group/financially-motivated-actor-breaks-certificate-parsing-avoid-detection/

Neel Mehta September 23, 2021



Threat Analysis Group

Introduction

Google's Threat Analysis Group tracks actors involved in disinformation campaigns, government backed hacking, and financially motivated abuse. Understanding the techniques used by attackers helps us counter these threats effectively. This blog post is intended to highlight a new evasion technique we identified, which is currently being used by a financially motivated threat actor to avoid detection.

Attackers often rely on varying behaviors between different systems to gain access. For instance, attacker's may bypass filtering by convincing a mail gateway that a document is benign so the computer treats it as an executable program. In the case of the attack outlined below, we see that attackers created malformed code signatures that are treated as valid by Windows but are not able to be decoded or checked by OpenSSL code — which is used in a number of security scanning products. We believe this is a technique the attacker is using to evade detection rules.

Technical Details

Code signatures on Windows executables provide guarantees about the integrity of a signed executable, as well as information about the identity of the signer. Attackers who are able to obscure their identity in signatures without affecting the integrity of the signature can avoid detection longer and extend the lifetime of their code-signing certificates to infect more systems.

OpenSUpdater, a known family of unwanted software which violates our policies and is harmful to the user experience, is used to download and install other suspicious programs.The actor behind OpenSUpdater tries to infect as many users as possible and while they do not have specific targeting, most targets appear to be within the United States and prone to downloading game cracks and grey-area software.

Groups of OpenSUpdater samples are often signed with the same code-signing certificate, obtained from a legitimate certificate authority. Since mid-August, OpenSUpdater samples have carried an invalid signature, and further investigation showed this was a deliberate attempt to evade detection. In these new samples, the signature was edited

such that an End of Content (EOC) marker replaced a NULL tag for the 'parameters' element of the SignatureAlgorithm signing the leaf X.509 certificate.

EOC markers terminate indefinite-length encodings, but in this case an EOC is used within a definite-length encoding (l= 13).

Bytes: **30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 00 00**

Decodes to the following elements:

SEQUENCE (2 elem)

OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)

EOC

Security products using OpenSSL to extract signature information will reject this encoding as invalid. However, to a parser that permits these encodings, the digital signature of the binary will otherwise appear legitimate and valid. This is the first time TAG has observed actors using this technique to evade detection while preserving a valid digital signature on PE files.

As shown in the following screenshot, the signature is considered to be valid by the Windows operating system. This issue has been reported to Microsoft.

Since first discovering this activity, OpenSUpdater's authors have tried other variations on invalid encodings to further evade detection.

The following are samples using this evasion:

https://www.virustotal.com/gui/file/5094028a0afb4d4a3d8fa82b613c0e59d31450d6c75ed96ded02be1e9db8104f/detection

New variant:

https://www.virustotal.com/gui/file/5c0ff7b23457078c9d0cbe186f1d05bfd573eb555baa1bf4a45e1b79c8c575db/detection

Our team is working in collaboration with Google Safe Browsing to protect users from downloading and executing this family of unwanted software. Users are encouraged to only download and install software from reputable and trustworthy sources.

POSTED IN:

Threat Analysis Group