Vault 7: WikiLeaks zerreißt CIA-Tarnkappe

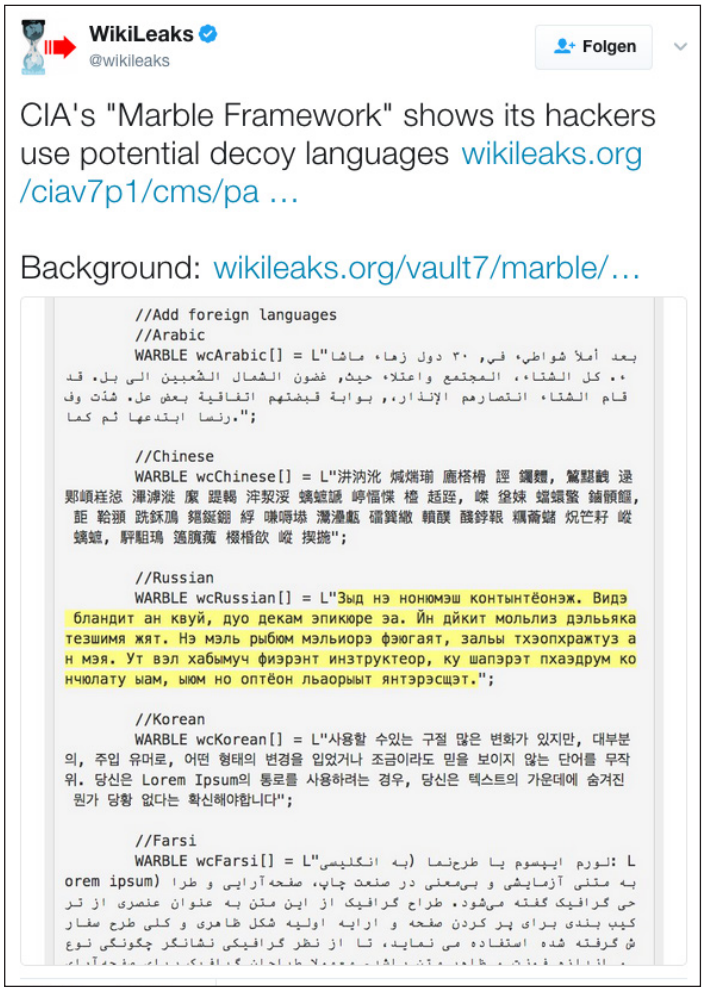
Die Enthüllungsplattform WikiLeaks hat am 31. März 2017 unter dem Namen Vault 7 „Marble“ neue Dokumente zu den Hacking-Aktivitäten des US-Geheimdienstes CIA veröffentlicht. Demnach können nun tausende CIA-Viren und Hacking-Attacken nachvollzogen werden. Die Hacker-Tools sind brandaktuell, noch im letzten Jahr wurden sie genutzt.

von RT deutsch

Die enthüllten Dokumente tragen den Namen „Marble“ und enthalten nach Informationen der Enthüllungsplattform 676 Quellcodes des anti-forensischen und geheimen CIA Marble Framework. Dieses werde dazu genutzt, um forensische Ermittler daran zu hindern, von der CIA genutzte Viren, Trojaner, aber auch Hackerangriffe nachvollziehen und rückverfolgen zu können.

Mit anderen Worten: Die CIA entwickelte eine Software, die ihre Hacker-Aktivitäten mit einer Tarnkappe umgibt. Dabei verschleiert Marble Textfragmente, die in von der CIA genutzter Schadsoftware eingesetzt werden. Auf diese Weise sind die Hacker-Werkzeuge der CIA nicht mehr identifizierbar.

WikiLeaks vergleicht den technischen Vorgang mit der herkömmlichen analogen Praxis, seine Signaturen von konventionellen Waffen zu entfernen, bevor man sie an Söldner im Ausland schickt. Marble sei „das digitale Äquivalent“ eines speziellen CIA-Instruments, um englische Texte auf von den USA produzierten Waffensystemen zu tarnen, bevor diese an insgeheim von der CIA unterstützte Aufständische geliefert werden.



Twitter-Veröffentlichung von Wikileaks vom 31. März 2017 mit einem Ausschnitt aus dem Programm-Code der Test-Routinen von „Marble“, der belegt, wie digitale „Spuren“ verwischt oder absichtlich verfälscht werden können.

Marble gehört zur anti-forensischen CIA-Methodik und deren Schlüssel-Programmbibliothek für Schadsoftware-Codes.

Es wurde entwickelt, um eine einfache und flexible Verschleierung zu ermöglichen, da String-Verschleierungs-Algorithmen (insbesondere die spezifischen), oft eingesetzt werden, um Schadsoftware mit einem speziellen Entwickler oder Entwickler-Unternehmen in Verbindung zu bringen.

Bei der CIA „core-library“ handelt es sich demnach, um eine Sammlung all jener Schnittstellen [interfaces] die von den AED-Programmbibliotheken (Applied Engineering Devision) genutzt werden.

Der Marble-Quellcode beinhaltet ebenso einen Rück-Verschleierer [deobfuscator] um CIA-Textverschleierungen wieder rückgängig machen zu können. In Kombination mit den enthüllten Verschleierungs-Techniken, entsteht ein Muster oder eine Signatur, die forensischen Ermittlern die Möglichkeit gibt, vorangegangene Hacking-Attacken und Viren der CIA zuordnen zu können. Marble wurde durch die CIA im Jahr 2016 genutzt.

Der Quellcode offenbart, dass Marble über Test-Beispiele nicht nur auf English, sondern auch auf Chinesisch, Russisch, Koreanisch, Arabisch und Farsi verfügt. Dies erlaubt ein forensisches Doppelspiel, indem beispielsweise vorgeben wird, dass die verwendete Sprache des Schadsoftware-Entwicklers nicht amerikanisches Englisch, sondern etwa Chinesisch gewesen sei.

In einem nächsten Schritt kann der Gebrauch der chinesischen Sprache widerum verschleiert werden – ganz so, als ob der Autor seine Urheberschaft zu vertuschen versuche. Dies führe dazu, dass die digitalen Forensiker weiter in die Irre geleitet werden.

Quellen:

Marble Frame Work home: *<https://wikileaks.org/ciav7p1/cms/page_14588467.html#efmCOoCS7>*

Programmcode: *<https://wikileaks.org/vault7/document/Marble/Marble.zip>*

Marble Framework Breifing Slides: *<https://wikileaks.org/ciav7p1/cms/files/Marble%20Framework.pptx>*

Dieser Text wurde zuerst am 31.3.2017 auf den RTdeutsch unter der URL ‹https://deutsch.rt.com/nordamerika/48512-vault-7-wikileaks-zerreisst-cia-hacking/› veröffentlicht. (Lizenz: RTdeutsch)

‹http://www.free21.org/?p=27082›