

# Vault 7: WikiLeaks zerreit 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.

## Marble Framework

31 March, 2017

Today, March 31st 2017, WikiLeaks releases Vault 7 "Marble" -- 676 source code files for the CIA's secret anti-forensic Marble Framework. Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.

RELEASE: CIA Vault 7 Part 3 "Marble" -- thousands of CIA viruses and hacking attacks could now be attributed  
wikileaks.org/vault7/marble... #Vault7  
12:36 - 31 Mar 2017  
5.157 4.846

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

Background: [wikileaks.org/vault7/marble/...](https://wikileaks.org/vault7/marble/)

```
//Add foreign languages
//Arabic
WARBLE wcArabic[] = L"بعد أألا شواطئ، في ٣٠ دول زهاء ماأا"؛
.. كل الشتاء، المجتمع واعتلاء حيث، غضون الشمال الضعيفين إلى بل. قد
قام الشتاء انتصارهم الإذارة، بوابة قبضتهم اتفاقية بعض على. شئت وف
؛.رنسا ابتدعها ثم كما

//Chinese
WARBLE wcChinese[] = L"洪涝沱 城端珊 鹿格槽 誣 鑛鑛 遂
鄭嶼荏恣 渾淨浞 虞 羅暢 冲黎浚 螻蟻蟻 崢嶸傑 檣 越踮, 嶸 鎗辣 蟻蟻蟻 鋪顧顧,
距 鞞頰 跳鈺鳩 鑛鑛鑛 綉 嶸嶸嶸 灑灑灑 確實繳 賴誤 蕩鏗報 穉齋蟻 炆芒籽 嶸
嶸蟻, 駢駢瑪 透騰獲 檣檣欲 嶸 嶸嶸";

//Russian
WARBLE wcRussian[] = L"Зыд нэ нонюмэш контынтёонэж. Видэ
бландит ан квуй, дуо декам эпикюре эа. Ин дикит мольлиз дэлььяка
тезшимя жят. Нэ мэль рыбом мэлйорэ фэюгаят, зальы тхэопхражтуз а
н мэя. Ут вэл хабмуч физэрт инзруктеор, ку шанэрэт пхэдрум ко
нчюлату ым, ыюм но оптёон льаорыт янтэрэсэцт.";

//Korean
WARBLE wcKorean[] = L"사용할 수있는 구절 많은 변화가 있지만, 대부분
의, 주입 유머로, 어떤 형태의 변경을 입었거나 조금이라도 믿을 보이지 않는 단어를 무작
위. 당신은 Lorem Ipsum의 토크를 사용하려는 경우, 당신은 텍스트의 가운데에 숨겨진
원가 당황 없다는 확신해야합니다";

//Farsi
WARBLE wcFarsi[] = L"لورم ایپسوم یا طرحنا (به انگلیسی)
orem ipsum) به متنی آزمایشی و بی‌معنی در صنعت چاپ، صفحه‌آرایی و طراحی
حی گرافیک گفته می‌شود. طراح گرافیک از این متن به عنوان عنصری از تر
کیب بندی برای پر کردن صفحه و ارایه اولیه شکل ظاهری و کلی طرح سفار
ش گرفته شده استفاده می‌نماید، تا از نظر گرافیکی نشانگر چگونگی نوع
و اندازه فونت و ظاهر آن مشخص شود. لورم ایپسوم به معنای «متن آزمایشی» می‌باشد.
```

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.

CIA unterstützte Aufständische geliefert werden.

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 Schnittstel-

len [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 vorgegeben wird, dass die verwendete Sprache des Schadsoftware-Entwicklers nicht amerikanisches English, sondern etwa Chinesisch gewesen sei.

In einem nächsten Schritt kann der Gebrauch der chinesischen Sprache wiederum 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](https://wikileaks.org/ciav7p1/cms/page_14588467.html#efmCOoCS7)>

Programcode: <<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>>

