Testbericht zum Remediation-Vergleich

Der Vergleichstest wurde im Auftrag der Enigma Software Group von AV-TEST GmbH durchgeführt
Bericht vom: 10. Mai 2017, aktualisiert am 24. Mai 2017

Zusammenfassung

Im März hat 2017 hat AV-TEST in einem Vergleichstest die Remediation-Funktionen und -Fähigkeiten von SpyHunter geprüft, ein Produkt der Enigma Software Group. Durchgeführt wurde der Test auf einem sauberen Windows 7-System (SP1, 64 Bit) und das gleiche Disk Image wurde auf mehreren baugleichen Rechnern verwendet.

Der Malware-Korpus für den Remediation-Test umfasste 21 Schädlinge und der Testablauf wurde in zwei Phasen unterteilt. In der ersten Testphase wurde zunächst das Image mit einem Malware-Sample infiziert und im nächsten Schritt der Versuch unternommen, das Sicherheitsprodukt zu installieren, den Rechner zu scannen und die erkannte Bedrohung zu entfernen. In der zweiten Testphase wurde die Antiviren-Lösung deaktiviert, damit das System infiziert werden konnte. Daraufhin wurde die AV-Lösung wieder aktiviert und das System neu gestartet um sicherzustellen, dass sämtliche Komponenten der Sicherheitslösung einwandfrei funktionieren. Im letzten Schritt wurde versucht, das System zu säubern und einen zusätzlichen Systemscan durchzuführen.

SpyHunter erzielte in der ersten Testphase mit 98 % ein fast perfektes Ergebnis und war in der Lage, alle aktiven Komponenten der Malware zu entfernen. Nur in einem Fall verblieb die von einer Malware erzeugte Anwendung im System. Die nächsten drei getesteten Produkte, Emsisoft Anti-Malware, Malwarebytes Free und Malwarebytes Premium, haben diesen Testteil ebenfalls mit Erfolg absolviert und Ergebnisse von 92-93 % erreicht, während Spybot Search & Destroy und IObit Malware Fighter weit abgeschlagen bei jeweils 40 % und 10 % landeten.

Nach der Auswertung der zweiten Testphase ergab sich bei der Produktbewertung ein ganz ähnliches Bild zum ersten Testteil: Mit 97 % erzielte SpyHunter wiederum ein sehr gutes Ergebnis, indem das Programm alle aktiven Komponenten der Malware neutralisierte und nur ein Start-Eintrag in der Registry sowie die erzeugten Anwendungen im System verblieben. Emsisoft Anti-Malware, Malwarebytes Free und Malwarebytes Premium erhielten gleichermaßen gute Wertungen von 92-93 %. Schlusslichter waren erneut Spybot Search & Destroy und IObit mit Ergebnissen in einer Größenordnung von 40 % und 10%.

Übersicht

Angesichts der stetig steigenden Anzahl an Bedrohungen, die mittlerweile entwickelt und über das Internet verbreitet werden, steigt auch das Risiko, dass Systeme infiziert werden. Während noch vor wenigen Jahren neue Bedrohungen alle paar Tage veröffentlicht wurden, muss im heutigen Bedrohungsszenario mit mehreren tausend neuen Schadprogrammen pro Stunde gerechnet werden.

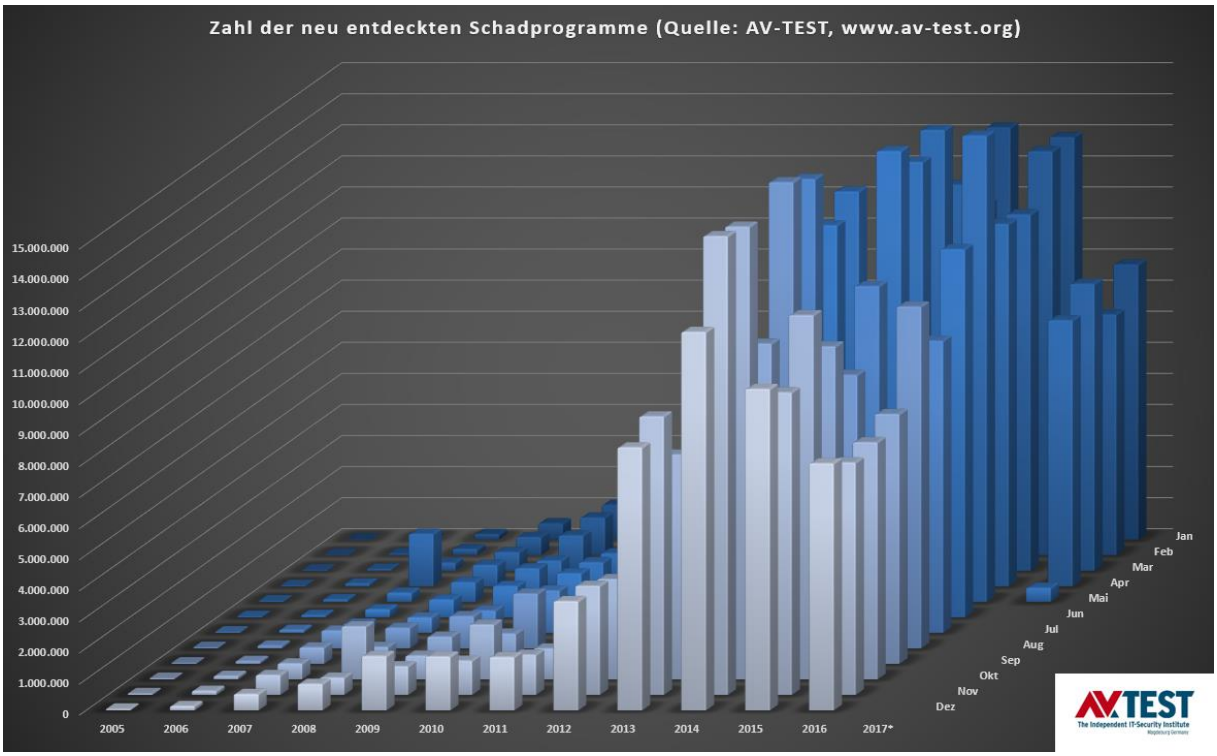

Abbildung 1: Neue Malware-Samples pro Jahr

Während AV-TEST in 2000 noch über 170.000 neue Malware-Samples sammelte, war die Anzahl an Schädlingen bis 2013 bereits auf über 80 Millionen gestiegen. Der Blick auf die Zahlen in Abb. 1 zeigt, dass sich der Anstieg auch in 2016 fortgesetzt hat. Derzeit befinden sich mehr als 630 Millionen Malware-Samples in der AV-TEST-Datenbank.

Hersteller von Sicherheitssoftware müssen beim Schutz ihrer Kunden eine ungeheure Menge an neuen Schädlingen bewältigen. Diese Menge kann zu Problemen führen, denn es ist nicht in jedem Fall möglich, einen Rechner rechtzeitig vor Bedrohungen zu schützen. Selbst wenn eine aktualisierte Antiviren-Software auf dem Rechner installiert ist, kann dieser trotzdem infiziert werden, wenn mehrere Stunden von der Entdeckung eines neuen Schädlings bis zur Bereitstellung passender Signaturen vergehen. In einigen Fällen kann es dann schon zu spät sein. Infektionen können wirtschaftlichen Schaden verursachen, beispielsweise wenn vertrauliche Daten gestohlen werden oder der Rechner nicht mehr effektiv genutzt werden kann, bis der Schädling vollständig aus dem System entfernt worden ist.

Vor diesem Hintergrund gewinnen Remediation-Techniken zunehmend an Bedeutung, wenn ein infizierter Rechner schnell wieder einsatzbereit sein muss. Es ist jedoch zwingend erforderlich, dass der Reinigungsprozess beim Einsatz dieser Technik in zwei Punkten zuverlässig abläuft:

1. Der Schädling und sämtliche Schädlingskomponenten müssen entfernt und verseuchte Systeme wiederhergestellt werden.
2. Saubere Programme sowie das System selbst dürfen im Laufe des Reinigungsprozesses nicht in Mitleidenschaft gezogen werden.

Getestetes Produkt

Der Test wurde im März 2017 durchgeführt und AV-TEST hat die zum Testzeitpunkt verfügbare aktuellste Software-Version verwendet:

- SpyHunter von Enigma Software Group

Testmethodik und Bewertung

Plattform

Alle Tests wurden auf baugleichen Rechnern mit folgender Hardware durchgeführt:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB RAM
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

Als Betriebssystem wurde Windows 7 (SP1, 64 Bit) inklusive der in der Version installierten Hotfixes und am 3. Januar 2017 verfügbaren Patches eingesetzt.

Testmethodik

Der Remediation-Test wurde in zehn Schritten unter Beachtung der folgenden Methodik durchgeführt:

1. **Sauberes System für jede Malware**. Die Testsysteme wurden jeweils gereinigt und wiederhergestellt, bevor sie mit einem einzelnen Malware-Sample infiziert wurden.
2. **Physische Rechner**. Für den Testablauf wurden ausschließlich physische Rechner genutzt, während virtuelle Umgebungen nicht zum Einsatz kamen.
3. **Internetzugang**. Es bestand zu jeder Zeit vollständiger Internetzugriff für die Rechner, um bei Bedarf während des Tests in der Cloud nachzufragen.
4. **Produktkonfiguration**. Bei sämtlichen Produkten und den dazugehörigen Remediation-Tools oder bootfähigen Rettungs-Tools wurden die Standardeinstellungen verwendet, entsprechend der Konfiguration bei Auslieferung.
5. **Infektion der Test-Rechner**. Ein natives System wurde mit einem Schädling infiziert und dann neu gestartet. Es musste sichergestellt werden, dass der Schädling vollständig lauffähig war.

6. **Schädlingsfamilien und Schadsoftware (Payloads)**. Bei den Testsamples wurde darauf geachtet, dass sie nicht aus der gleichen Schädlingsfamilie stammten oder die gleiche Schadsoftware nutzten.
7. **Remediation unter Einsatz sämtlicher verfügbarer Produktfunktionen**.
    a. Es soll versucht werden, das Sicherheitsprodukt mit den Standardeinstellungen zu installieren. Die Produktangaben für die Entfernung von Malware müssen vollständig befolgt werden.
    b. Sollte a. nicht durchführbar sein, sollte man es mit einem ***stand-alone Fix-Tool bzw. einem Rettung-Tool*** versuchen (sofern verfügbar).
    c. Sollte b. nicht möglich sein, sollte zur Eliminierung der Bedrohung eine stand-alone ***Boot-Lösung*** eingesetzt werden (sofern verfügbar).
8. **Prüfung der Malware-Entfernung.** Die Überprüfung des Rechners erfolgte manuell, kontrolliert wurde die vollständige Entfernung und der Verbleib von Dateiresten.
9. **Bewertung der Performance bei der Malware-Entfernung.** Die Performanceleistung des Tools und der gesamten Sicherheitslösung wurde unter Verwendung eines vereinbarten Punktesystems bewertet.

10. **Übermäßige Remediation-Auswirkungen.** In dem Test wurde ebenfalls geprüft, inwieweit eine Sicherheitslösung aggressive Methoden bei der Säuberung des Systems einsetzt. So gibt es beispielsweise Produkte, die Hosts-Dateien oder sogar ganze Verzeichnisse komplett entfernen, obwohl dies nicht für einen erfolgreichen Remediationsablauf erforderlich ist. Sollten solche Methoden eingesetzt werden, führt dies zu Punktabzügen bei der Bewertung.

Bewertung der Wirksamkeit

Nach dem folgenden System wurden für jedes getestete Malware-Sample Punkte vergeben:

a. Malware wurde vollständig entfernt (3 Punkte)
b. Malware wurde erkannt und entfernt, es blieben nur inaktive Dateireste zurück (2 Punkte)
c. Es wurde etwas entdeckt und teilweise entfernt, Reste der Schadsoftware waren jedoch noch aktiv (1 Punkt)
d. Die Malware wurde nicht entdeckt und somit nicht entfernt (0 Punkte)

Bei der Punktevergabe wurde nicht berücksichtigt, welche der verfügbaren Techniken zur Entfernung der Malware benötigt wurden. Es sollte jedoch jede Technik zum Einsatz kommen. Wenn ein Produkt die Einträge in der Hosts-Datei entfernt, die zu dem entsprechenden Produkt gehören, dabei einen sauberen Rechner zurücklässt, und die Funktionalität sowie die Aktualisierbarkeit des Produkts gewährleistet bleibt, sollte das Produkt für seine Remediationsleistung die volle Punktzahl erhalten, selbst wenn Einträge anderer Sicherheitssoftware-Anbieter in der Hosts-Datei zurückbleiben.

Samples

Das Testset umfasste 21 Schadprogramme, mit denen Windows 7 (SP1, 64 Bit) infiziert werden konnte.

Testergebnisse

SpyHunter schnitt mit 123 von 126 möglichen Punkte am besten in diesem Vergleichstest ab, gefolgt von den beiden Malwarebytes-Produkten, die mit 118 Punkten ein gutes Ergebnis erzielten und sich den zweiten Platz sicherten. Emsisoft Anti-Malware lag mit 116 Punkte und somit einer ebenfalls guten Wertung nur knapp dahinter. Mit insgesamt 50 Punkten kam Spybot Search & Destroy nur auf ein mageres Ergebnis, während IObit Malware mit gerade einmal 12 von 126 möglichen Punkten denkbar schlecht abschnitt.

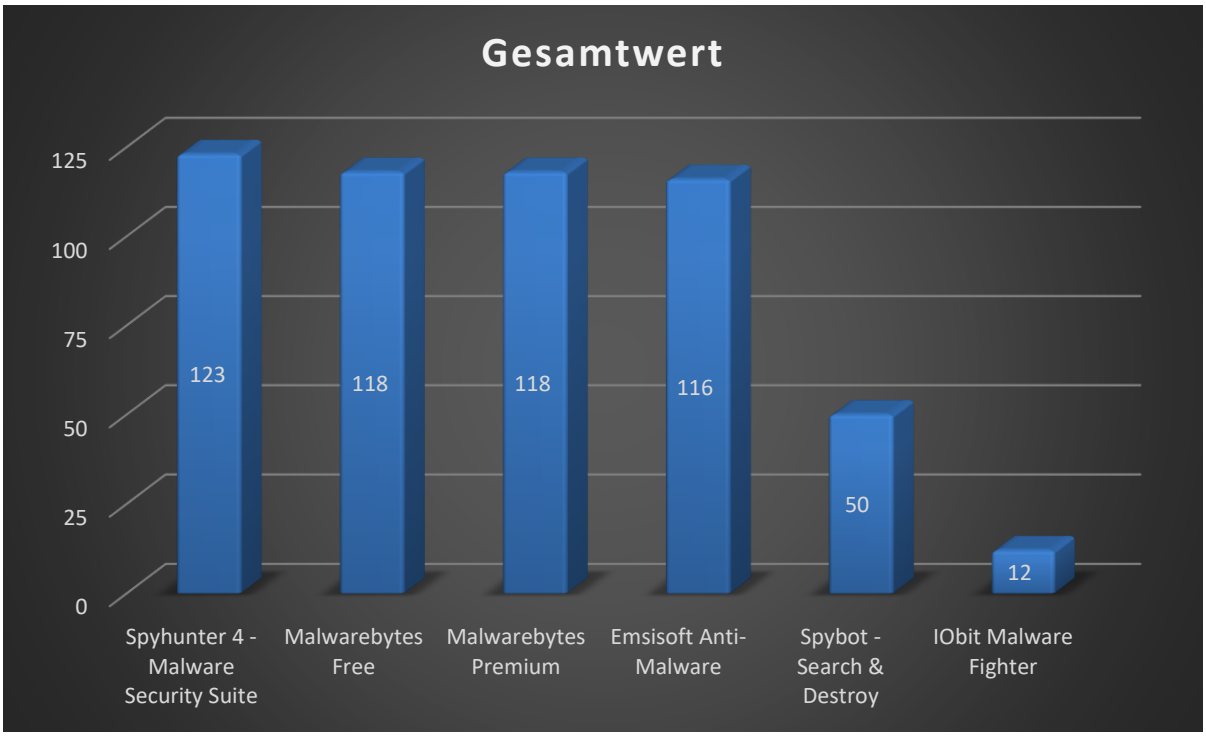

Abbildung 2: Remediation-Gesamtergebnis - Testphasen 1.1 und 1.2

Grafiktext: Gesamtergebnis
x-Achse (korrigieren): SpyHunter Spybot Search & Destroy

In den Abbildungen 3 und 4 lässt sich klar erkennen, dass die Ergebnisse der Testphasen 1 und 2 fast identisch sind. Die maximal erreichbare Punktzahl lag in den beiden Testabschnitten jeweils bei 63 Punkten.

SpyHunter erreichte in der ersten und zweiten Testphase 62 bzw. 61 Punkte und damit ein exzellentes Ergebnis. Das Programm ließ in beiden Tests jeweils eine Anwendung im System und in Testphase 2 einen Eintrag in der Registry zurück.

Mit 59 Punkten pro Test konnten beide Versionen von Malwarebytes ein gutes Gesamtergebnis vorweisen, auch wenn es ihnen in einem Fall nicht gelang, die Malware zu entfernen, und aktive Komponenten der Malware im System verblieben. Emsisoft Anti-Malware sicherte sich mit 58 Punkten pro Test den 3. Platz, indem das Programm alle aktiven Komponenten der 21 Testsamples löschte und nur eine Anwendung und Registry-Einträge im System zurück ließ.

Spybot Search & Destroy konnte weniger als die Hälfte der getesteten Malware-Samples entfernen und erhielt deshalb nur jeweils 25 Punkte in Testphase 1 und 2.

Mit nur 6 erreichten Punkten pro Test schnitt IObit am schlechtesten ab: das Programm war nicht in der Lage, 18 der 21 Malware-Samples zu löschen.

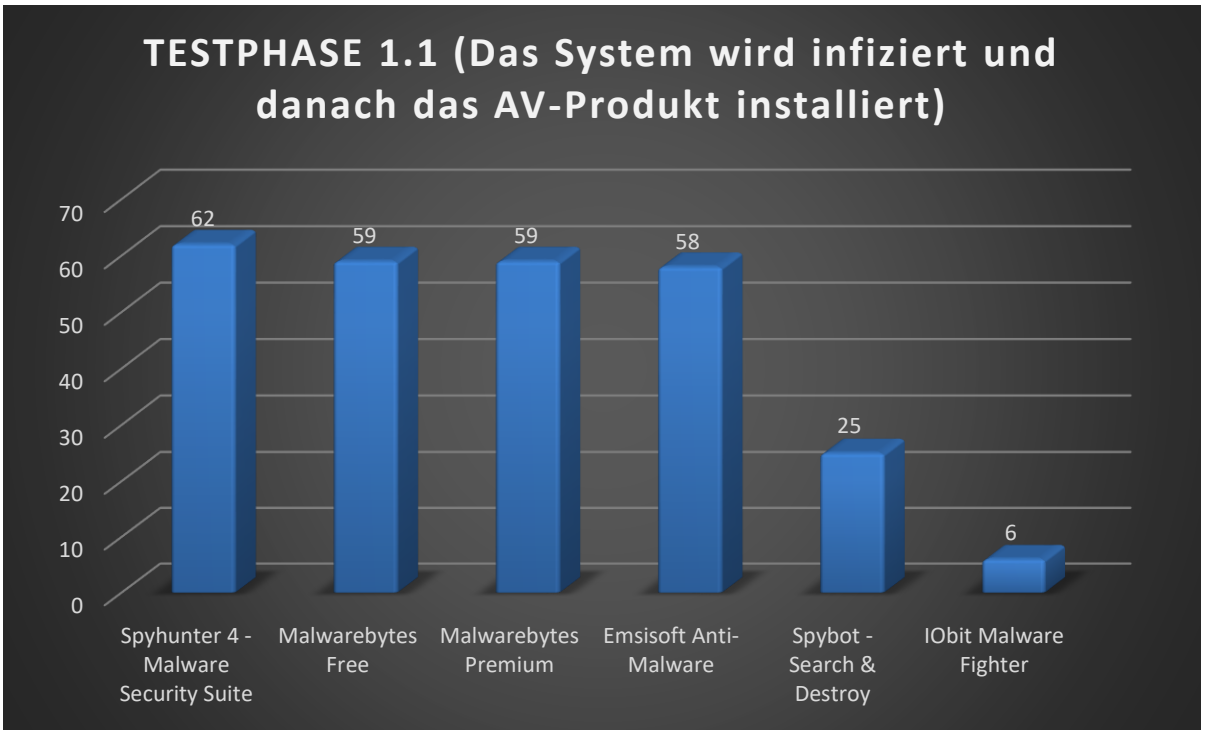

Abbildung 3: Remediation-Ergebnis - Testphasen 1.1 und 1.2

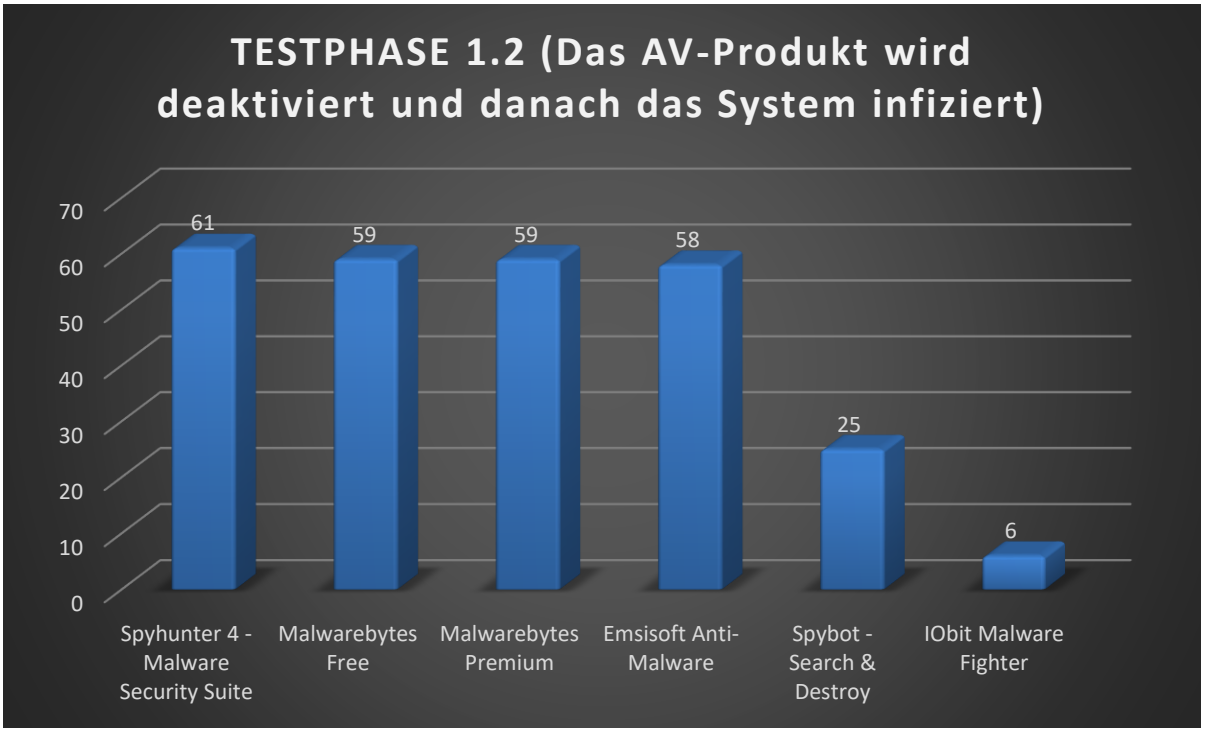

Abbildung 4: Remediation-Ergebnis - Testphasen 1.2 und 1.2

Grafiktext: Testphase 1.2 (das AV-Produkt wird deaktiviert und danach das System infiziert)
x-Achse (korrigieren): SpyHunter Spybot Search & Destroy

Anhang

Information zur getesteten Softwareversion

Entwickler, Hersteller	Produktbezeichnung	Programmversion	Engine/Signaturversion
Emsisoft	Anti-Malware	2017.2.1.7260	4.0.1.856/20170324
Enigma Software Group	SpyHunter 4	4.24.3.4750	2017.01.17v01
IObit	Malware Fighter	4.5.0.3457	1634
Malwarebytes	Malwarebytes Free	3.0.6.1469	n/a
Malwarebytes	Malwarebytes Premium	3.0.6.1469	n/a
Safer Networking	Spybot Search & Destroy	1.6.2.46	n/a

Liste der im Remediation-Test verwendeten Malware-Samples

(SHA256)
* 0x0101d4a72a3685aaf8a7baa4408223914ba7f1c8d193628fabbe98cd377536cd
* 0x01168762ca9a57ffe5b69371b85d7d60339a3a95091554e87750715fc146313d
* 0x0bf7ab1fd378c78ea8206c84dfa780c472d84c5357238d78df369881f762ad99
* 0x246082bd340133a0b634ef874a20f9823336fc3e65baddaddc57c3af5588a35a
* 0x369fab397bbc2ca10601c3ca89f77b24eecf485b080f07d820daf8a6487554a2
* 0x3b56fcb59462dac54bee27b85bc8e29af286d0349909aa9a313868e8be5c96bd
* 0x453442bc8fd9e0fec64febb1c7c81cc1daecc151faa0aa30041b25296b906423
* 0x454ecf8d9846abae025fa57f097fa6bc11b3ac7bd68b9a1c2eb55bc6861b3d4c
* 0x4b91c4e2f69697a888b56147f69d4c96ca13095a2aaf640a48e68994c7228565
* 0x4da0d3e569ceeced62b7128ed35c55cfb48236be628ba64411f066a9a38a5aff
* 0x4e59b6263b5b3a5ce4ea5054dc48cca37945ca930ad1a5aa300029539d8042a3
* 0x6a9936983ee1bc49d5fff7e2ae6435462667c7f62547a710297b8f9c86a36873
* 0x7021df3d38a24a1de948ef5c820b60d8e61c95ed3409c255680eba79e4221123
* 0x7a1e9db7fe1bc6341b1e1a002c19ca6f32224aa0c4eb6582d984d66bb44f339e
* 0x8f995f37b1aee61018742c35ab410820b02982fe2ac0b9a2554d02909f2590a2
* 0x9643447291f6e468611c8acb6e58f8e3b3c40a3394e4f7d5c20489a9af0e0750
* 0xc0d110efbd58448c8fed7e249a3e5503185cd3f2fc4a13339874646256877f9e
* 0xda3458870afb6487c435129bd1ac4c8b994c2133d3790ca505949cc2644293bf
* 0xee7e9a572dd14739aaf6cc16f1d52e66b62347f1902a2c93a9145ab9c0f29d83
* 0xf6c186da15892176e8f8cd31e9dd637024a4e4e08510315011d6d735a32f2c93