



DIRECTDEFENSE

July 29, 2026

Halcyon Anti-Ransomware Platform Product Attestation

Prepared for:

Halcyon

Prepared and independently conducted by
DirectDefense, Inc



© 2026 DirectDefense Inc. All Rights Reserved. This document is unpublished material and contains trade secrets and other confidential information that are subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of DirectDefense, and may not be disclosed without written permission from DirectDefense, Inc. DirectDefense grants the client organization permission to copy this report for the purposes of disseminating information within its organization, or to any regulatory agencies.

CONFIDENTIALITY

This document contains company confidential information of a proprietary and sensitive nature. As such this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission.

DirectDefense treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission from the client organization.

ASSESSMENT PROJECT TEAM

The following DirectDefense personnel are involved in this engagement. Contact the appropriate personnel on this team to discuss the contents of this document or the work performed during this engagement.

Thomas Richards
Infrastructure Security Practice Manager
trichards@directdefense.com

Jenny Arvyn Soriano
Security Consultant
jsoriano@directdefense.com

Jesse Rodriguez
Principal Enterprise Security Consultant
jrodriguez@directdefense.com

Table of Contents

Table of Contents.....3

Executive Summary4

The Ransomware Imperative5

About the Evaluation5

Results.....6

Test Architecture & Methodology.....11

Analysis: What the Results Demonstrate18

Conclusion18

Appendix19

Executive Summary

Ransomware remains the most disruptive threat enterprises face. A single successful attack can take a business offline for days and cost millions to resume operations, let alone the costs incurred by a victim organization due to loss of sensitive data typically associated with the extortion phase of an attack. Due to this impact, knowing how effective your investments in Endpoint Detect and Repose and the quality of their protection mechanisms is important. Blocking one sample in a lab during a demo or proof of value demonstration proves very little. The real question is whether a product can stop ransomware consistently: across hundreds of unrelated samples that are showing up in breaches today and on systems that resemble what companies run in production. This whitepaper documents an independent evaluation that was built to answer that question.

Halcyon engaged DirectDefense, an independent cybersecurity consulting firm with more than two decades of experience, to evaluate its anti-ransomware platform. The goal was to measure how Halcyon performs at detection, prevention, and response against a large, representative set of live, in-the-wild ransomware, and to run those tests under conditions strict enough that the results would hold up to scrutiny.

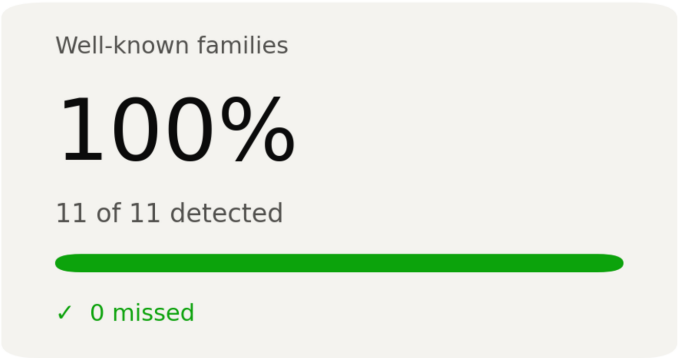
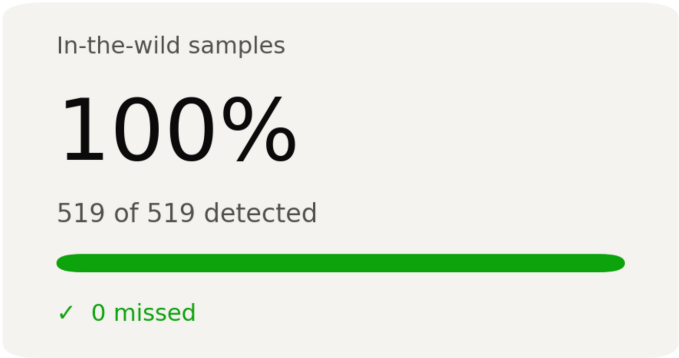
To ensure that every outcome could be traced back to Halcyon and nothing else, DirectDefense built a cloud-based detonation environment from the ground up. Each sample was run on its own Windows Server 2025 instance in AWS, provisioned immediately before the test and torn down immediately after. Network access was restricted to DirectDefense-controlled addresses, and Microsoft Defender was disabled before Halcyon was installed, which left Halcyon as the only endpoint defense in play.

In total, DirectDefense detonated 519 unique in-the-wild samples along with 11 well-known, high-impact families, including Akira, Play, WannaCry, LockBit, and Medusa, for 530 live payloads in all. Every one of them was blocked, a 100% block rate.

No sample encrypted a file, established persistence on the host, slipped past Halcyon's behavioral analytics, or executed its payload on a protected endpoint.

The bottom line

Measured under conditions that reflect a realistic production deployment, and validated by a fully independent assessor working under a rigorous methodology, Halcyon blocked 100% of the 530 ransomware payloads detonated against it. The results speak to how the platform performs as an enterprise anti-ransomware control in the real world.



Combined coverage: 530 of 530 test cases detected, 0 missed.

The Ransomware Imperative

Ransomware has evolved from opportunistic, single-host disruption into an industrialized criminal enterprise. Modern operators no longer simply encrypt files; they run structured intrusion campaigns that pursue several objectives in sequence, each of which a defensive control must be prepared to interrupt:

- **Pre-execution delivery and detonation** - the initial payload must be identified and stopped before it can run.
- **Defensive evasion** - attackers increasingly abuse vulnerable signed drivers and attempt to disable or blind endpoint detection and response (EDR) tooling before encrypting.
- **Tamper and shutdown of protective agents** - security software itself is targeted so that protection is removed at the decisive moment.
- **Data exfiltration for double and triple extortion** - data is stolen before encryption, so that even a clean restore does not remove the leverage held over the victim.

A credible anti-ransomware control should therefore be evaluated not against a handful of curated samples, but against the breadth of the live threat landscape and the specific techniques that modern families use to defeat traditional defenses. The evaluation documented here was designed around that principle. The aim was to maximize the volume and diversity of real payloads, reproduce the conditions of a genuine endpoint deployment, and remove every variable that could inflate or distort the platform's measured performance.

About the Evaluation

This assessment was conducted independently by DirectDefense. The engagement scope centered on a single, decisive question: when a live ransomware payload is executed on an endpoint protected only by Halcyon, what happens?

Engagement scope of work

The engagement assessed one primary threat vector through a single testing phase:

Ransomware Sample Detonation & Validation

DirectDefense established an independent testing environment consisting of a Windows Server endpoint instrumented with the Halcyon agent. Ransomware samples were selected and executed against the endpoint under controlled conditions. Throughout the engagement, DirectDefense documented the result of each detonation which included Halcyon's detection, prevention, and response performance across the full sample set.

Testing activities

TESTING ACTIVITY	SAMPLES TESTED	RESULT
Ransomware Simulation: Sample Malware	519	All samples blocked
Ransomware Simulation: Well-Known Malware	11	All samples blocked
Total	530	100% blocked

Results

Halcyon blocked every ransomware payload detonated against it. The test covered 519 in-the-wild samples and 11 well-known families, for 530 payloads in total. The platform achieved a 100% block rate, with zero successful encryptions, zero instances of persistence, and no evasion of its behavioral analytics.

In-the-wild ransomware samples

DirectDefense detonated **519 distinct in-the-wild ransomware variants**, each delivered as a unique executable and identified by its SHA-256 hash. **All 519 were detected and blocked.**



In-the-wild samples by detection outcome (519 samples).

Halcyon's Execution Protection classified each payload as a malicious executable and blocked it prior to execution, generating a corresponding alert. The sample corpus and the resulting block-level alerts are shown below.

Name
ffff8612adf342903e10a1e323c1af08c3a20300033fbcf670d730d5ddffff29.exe
ff7336fab385eceb6f3e63e8772f96ba6bdff14a6b9c5e38f7e9020ba7622612.exe
ff307b4303a9ed84395858f633c57d8c19416f2320e12014f7b5540368d1f766.exe
ff2ea862690bf3da6819b076e7768ee8890a85d2c637872bb6ffd9a935df1905.exe
ff2d32717e83c6320de88681a727377376ea2ff9382fd2659a5ca2ec23da1c2f.exe
fee6ec50e87e1efb94ec63eb9c139f741b599e9f23a8211b3f41e48bf3d27d27.exe
fedb4c3b0e080fb86796189ccc77f99b04adb105d322bdd3abfca2d5c5d43c8.exe
fe44beddd1cb0d0c503c54bc15439d7ad9821c6c2fa550128eb685c1d71796aa.exe
fe31a86fd9d99de76cc46b3f646b0e0330450fc035ac9a77c3006fae1875db34.exe
fe9fb9330c1f075715eab6dbc10d50baaeb26393f6dce10bb6aaa8f66faddc91.exe
fe1d95dfb4e593d2efca42093b6355d90de764179f2a1f5e14a0daf2cd61255d.exe
fde3aa2b3643f2fe88622e9bb727bcfc1bd4a2ff4a4ad6a0fa7b1b0e83275613.exe
fd8f1a04e8374004b13f58cb365b7c361552bb7cac1d4b0f279beb8ffa89f1.exe
fd3aaaedd7c9acd0a259580316f384636b866d2e07ce7bcd2eced844183a1bd.exe
fd1f206773f7a5c1c59245a9541d15e74fc5fd4f2e252ddf24e2f00a3521644e.exe
fcef7af7009917628116b0258e1186421a56e66b3b6ef1fbc19d25f99c07b528.exe
fce4540b185fafbb00902e447e499ad130b2f07b0ca61cea15c0563435383292.exe
fccfffbdd284aed28238fd27c3b19d40ddf22230d6713e2ed80a576809d781d9a.exe
fcaaa1432165a941e9fe4cbe3e40a7944282b73da6367577ae51b0ca0cda67ae.exe
fca304d629919fce152801bce6a277f759f3777a184a1f36af2a0a4a4d62f6d5.exe
fbf32d1055340cd0c110ed29e86f2bc6381b05f4deb3b9c591dc5e5f0dbf08ef.exe
fb949373d337cda67012c0734cdefde41f2b90b0397744d7155bddc784e8a51.exe

A sample of the in-the-wild ransomware corpus under test.

Alerts								
Columns		Filters						
Alert ID	Last Seen	First Seen	Events	Level	Assets	Type	Hash	Actions
f6d56498	07/03/2026 6:39:49 AM	07/03/2026 6:39:49 AM	1	Block	1	Malicious Executabl	1be07198	⋮
8dfaf491	07/03/2026 6:39:49 AM	07/03/2026 6:39:49 AM	1	Block	1	Malicious Executabl	111917fd	⋮
8f770a54	07/03/2026 6:34:15 AM	07/03/2026 6:34:15 AM	1	Block	1	Malicious Executabl	1bc54d25	⋮
84c6715f	07/03/2026 6:34:14 AM	07/03/2026 6:34:14 AM	1	Block	1	Malicious Executabl	11179a01	⋮
34149275	07/03/2026 6:28:37 AM	07/03/2026 6:28:37 AM	1	Block	1	Malicious Executabl	1bb211c8	⋮
820733d6	07/03/2026 6:28:37 AM	07/03/2026 6:28:37 AM	1	Block	1	Malicious Executabl	4f6865f1	⋮
9529df7d	07/03/2026 6:22:56 AM	07/03/2026 6:22:56 AM	1	Block	1	Malicious Executabl	109aaac6	⋮
1b17e19e	07/03/2026 6:22:55 AM	07/03/2026 6:22:55 AM	1	Block	1	Malicious Executabl	1bad553d	⋮
Total Rows: 100 of 107								

Halcyon alerts showing each sample blocked as a malicious executable.

Well-known ransomware families

DirectDefense additionally detonated **11 well-known, high-impact ransomware families**: akira, Black Basta, BlackCat, INC Ransomware, LockBit, Medusa, Money Message, Play, RagnarLocker, Royal, and WannaCry. **All 11 were detected and blocked.**

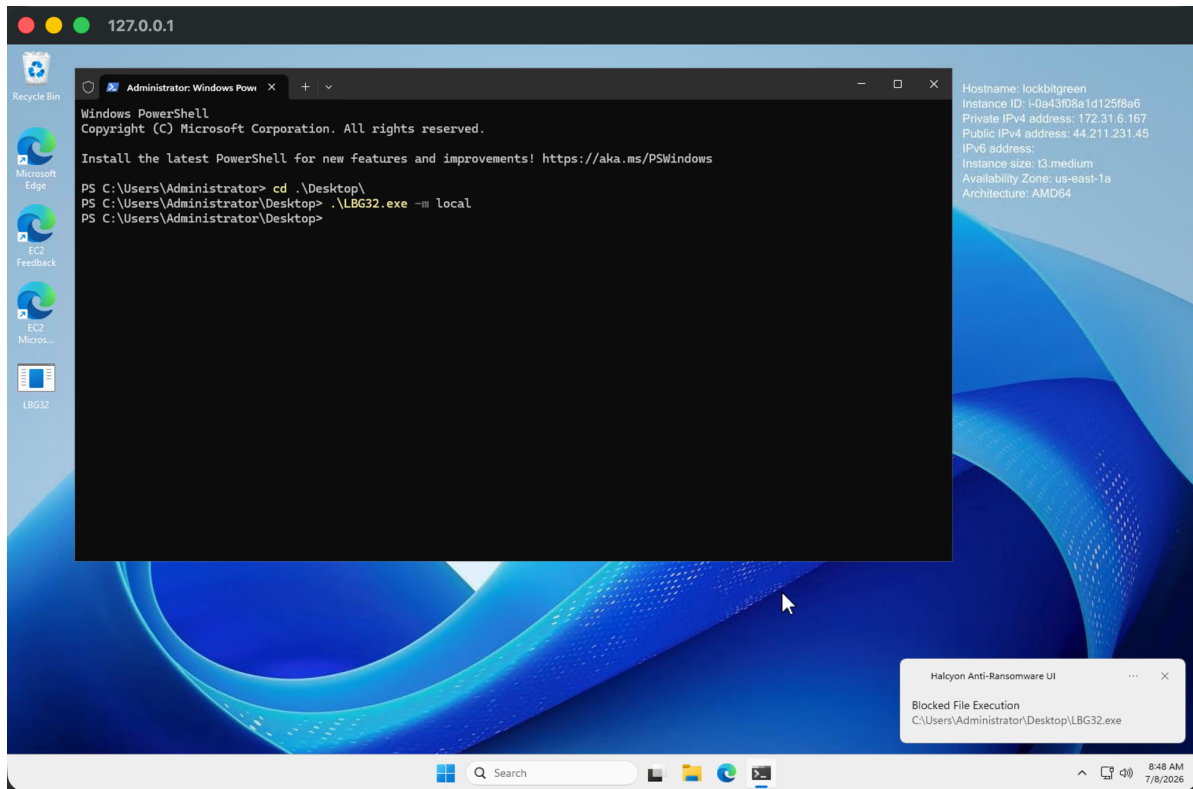


Well-known families by detection outcome (11 samples).

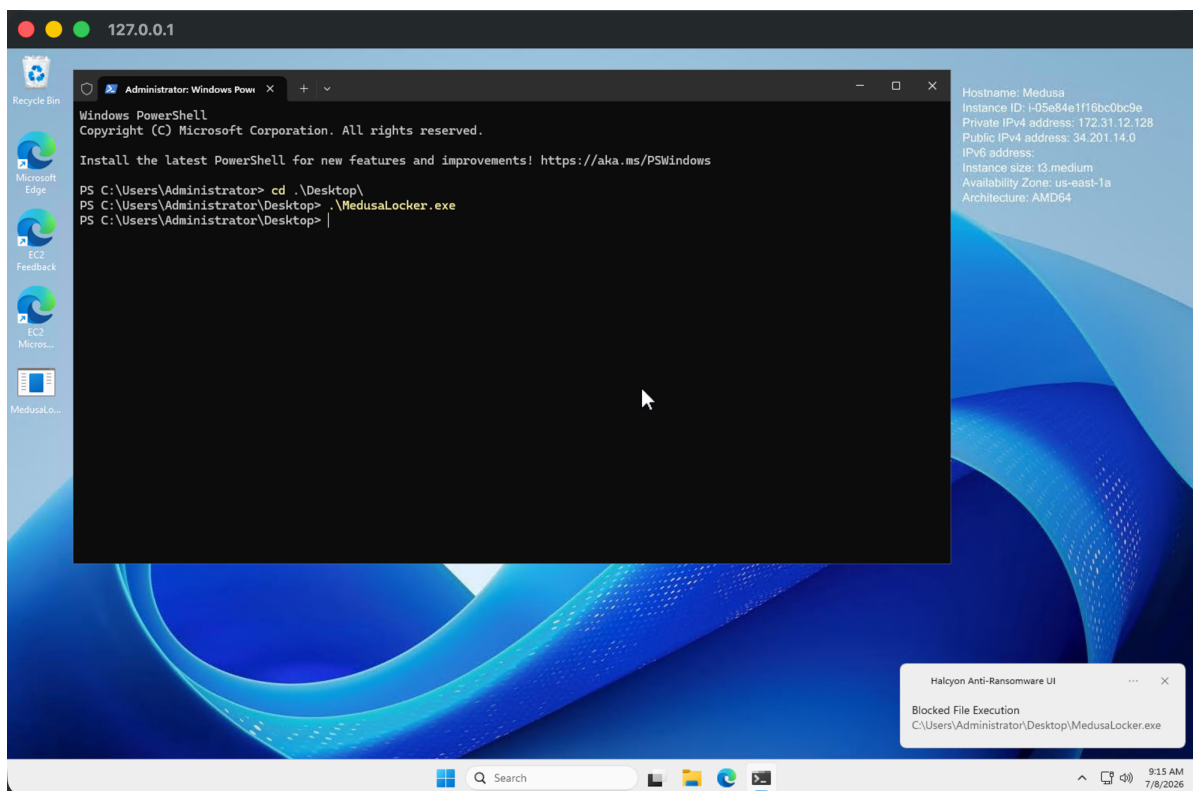
Name
> akira
> blackbasta
> blackcat
> INCRansomware
> lockbit
> medusa
> moneymessage
> play
> ragnarlocker
> royal
> wannacry

The well-known ransomware families included in the corpus.

Each family was executed directly on the protected endpoint. Halcyon blocked file execution at runtime and surfaced a clear anti-ransomware notification, as shown for LockBit and Medusa below.



LockBit detected and blocked at execution.



Medusa (MedusaLocker) detected and blocked at execution.

☐ Name	Policy	OS Name	Agent Version
☐  wannacry	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60
☐  royal	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60
☐  RagnarLocker	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60
☐  play	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60
☐  MoneyMessage	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60
☐  Medusa	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60
☐  ...	Prevention with File Resilience	Microsoft Windows Server 2025 Datacenter	2.0.2606.60

Console asset view confirming each family ran under the Prevention with File Resilience policy on Windows Server 2025.

Test Architecture & Methodology

The credibility of any efficacy claim rests on the rigor of the environment that produced it. DirectDefense built a cloud-based detonation harness that could provision isolated, single-use ransomware execution environments on demand. The design was governed by four principles that together protect the integrity of every result.

Isolated, single-use detonation environments

Each ransomware sample was detonated against a freshly created Windows Server 2025 endpoint. The endpoint was deployed in AWS from a custom Amazon Machine Image (AMI) that had been preloaded with the required test payloads, telemetry hooks, and endpoint instrumentation. Every environment was single-use, provisioned immediately before execution and destroyed on completion. As a result, no persistence mechanism, dropped artifact, registry modification, scheduled task, service creation, or lateral-movement primitive left behind by a prior sample could contaminate or bias a later trial.

Network-layer containment

Containment was enforced through tightly scoped AWS security groups that permitted inbound traffic exclusively to and from designated IP ranges. This was sufficient to enable secure operator control, sample delivery, and telemetry collection.

Isolating Halcyon as the sole control

To ensure that every detection, prevention, or response event could be attributed to the Halcyon platform alone, Microsoft Defender was fully disabled before the Halcyon agent was installed on each endpoint under test. This step removed any overlap with Windows' native protection stack and left Halcyon as the sole endpoint defensive control. The results therefore reflect Halcyon's standalone capability, without inflation or interference from adjacent controls.

Automated provisioning

DirectDefense used a purpose-built script to automate the creation of each EC2 test environment, which removed operator variability and allowed the tests to be run at scale. For each sample, the script carried out the following sequence:

- A custom Windows Server 2025 AMI preloaded with the test files was spawned, and network settings and security groups were applied to restrict all interaction to specific IP addresses.
- The host was renamed. For unnamed samples, the hostname was derived from the first 10 characters of the sample's SHA-256 hash; for known ransomware, the family name was used. The host was then rebooted, and the new hostname was verified to have taken effect.
- Windows Defender was disabled, and the malware executable was uploaded to the endpoint over SMB.
- The Halcyon agent was installed, and the sample was executed against the running protection.

Using this process, DirectDefense detonated all 519 in-the-wild samples and 11 well-known families against Halcyon in a reproducible way. The figures below trace a single sample through the automated pipeline.

```

---- [1] ----
hostname : 7eb2a629b5
filename : 7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe
fullpath : /root/projects/Halcyon/MALWARE/samples/unknown-ransomwares/7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe

[provision] launching a new instance (7eb2a629b5) from ami-0e7bbe4e7aedf6744...

[provision] launched i-0b4b9a87fd8a7b99a; waiting for it to reach 'running'...

[provision] instance i-0b4b9a87fd8a7b99a at 3.236.128.46

[provision] waiting for WinRM (5985) on 3.236.128.46...

[provision] WinRM is up

[provision] renaming host to 7eb2a629b5...
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [*] Windows 11 / Server 2025 Build 26100 (name:EC2AMAZ-6R2G8VJ) (domain:EC2AMAZ-6R2G8VJ)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [+] EC2AMAZ-6R2G8VJ\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [-] Execute command failed, error: HTTPConnectionPool(host='3.236.128.46', port=5985): Read timed out. (read timeout=30)

[provision] command did not report '[+] Executed command' (attempt 1/5); retrying...
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [*] Windows 11 / Server 2025 Build 26100 (name:EC2AMAZ-6R2G8VJ) (domain:EC2AMAZ-6R2G8VJ)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [+] EC2AMAZ-6R2G8VJ\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [+] Executed command (shell type: powershell)

[provision] rebooting to apply hostname...
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [*] Windows 11 / Server 2025 Build 26100 (name:EC2AMAZ-6R2G8VJ) (domain:EC2AMAZ-6R2G8VJ)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [+] EC2AMAZ-6R2G8VJ\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 EC2AMAZ-6R2G8VJ [+] Executed command (shell type: cmd)

```

Provisioning a fresh EC2 instance and renaming the host.

```

[provision] waiting for WinRM (5985) on 3.236.128.46...

[provision] WinRM is up

[provision] verifying hostname is 7eb2a629b5...
WINRM 3.236.128.46 5985 7EB2A629B5 [*] Windows 11 / Server 2025 Build 26100 (name:7EB2A629B5) (domain:7eb2a629b5)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] 7eb2a629b5\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] Executed command (shell type: cmd)
WINRM 3.236.128.46 5985 7EB2A629B5 7eb2a629b5

[provision] configuring Windows Defender...
WINRM 3.236.128.46 5985 7EB2A629B5 [*] Windows 11 / Server 2025 Build 26100 (name:7EB2A629B5) (domain:7eb2a629b5)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] 7eb2a629b5\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] Executed command (shell type: powershell)

```

Verifying the hostname and disabling Windows Defender.

```

[provision] upload of 7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe not confirmed (attempt 2/5); retrying...
SMB 3.236.128.46 445 7EB2A629B5 [*] Windows 11 / Server 2025 Build 26100 x64 (name:7EB2A629B5) (domain:7eb2a629b5) (signing:False) (SMBv1:False)
SMB 3.236.128.46 445 7EB2A629B5 [+] 7eb2a629b5\Administrator:[REDACTED] (AdminPrivs)
SMB 3.236.128.46 445 7EB2A629B5 [*] Copying /root/projects/Halcyon/MALWARE/samples/unknown-ransomwares/7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe to \Users\Administrator\Desktop\7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe
SMB 3.236.128.46 445 7EB2A629B5 [+] Created file /root/projects/Halcyon/MALWARE/samples/unknown-ransomwares/7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe on \
\C$\Users\Administrator\Desktop\7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe

```

Uploading the ransomware sample to the endpoint over SMB.

```

[provision] installing Halcyon...
WINRM 3.236.128.46 5985 7EB2A629B5 [*] Windows 11 / Server 2025 Build 26100 (name:7EB2A629B5) (domain:7eb2a629b5)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] 7eb2a629b5\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] Executed command (shell type: cmd)

```

Installing the Halcyon agent on the target endpoint.

```

[provision] executing 7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759acffe3dc3bc0.exe over WinRM...
WINRM 3.236.128.46 5985 7EB2A629B5 [*] Windows 11 / Server 2025 Build 26100 (name:7EB2A629B5) (domain:7eb2a629b5)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0
.0.
arc4 = algorithms.ARC4(self._key)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] 7eb2a629b5\Administrator:[REDACTED] (AdminPrivs)
WINRM 3.236.128.46 5985 7EB2A629B5 [+] Executed command (shell type: cmd)

[provision] done. host=7eb2a629b5 ip=3.236.128.46 id=i-0b4b9a87fd8a7b99a

```

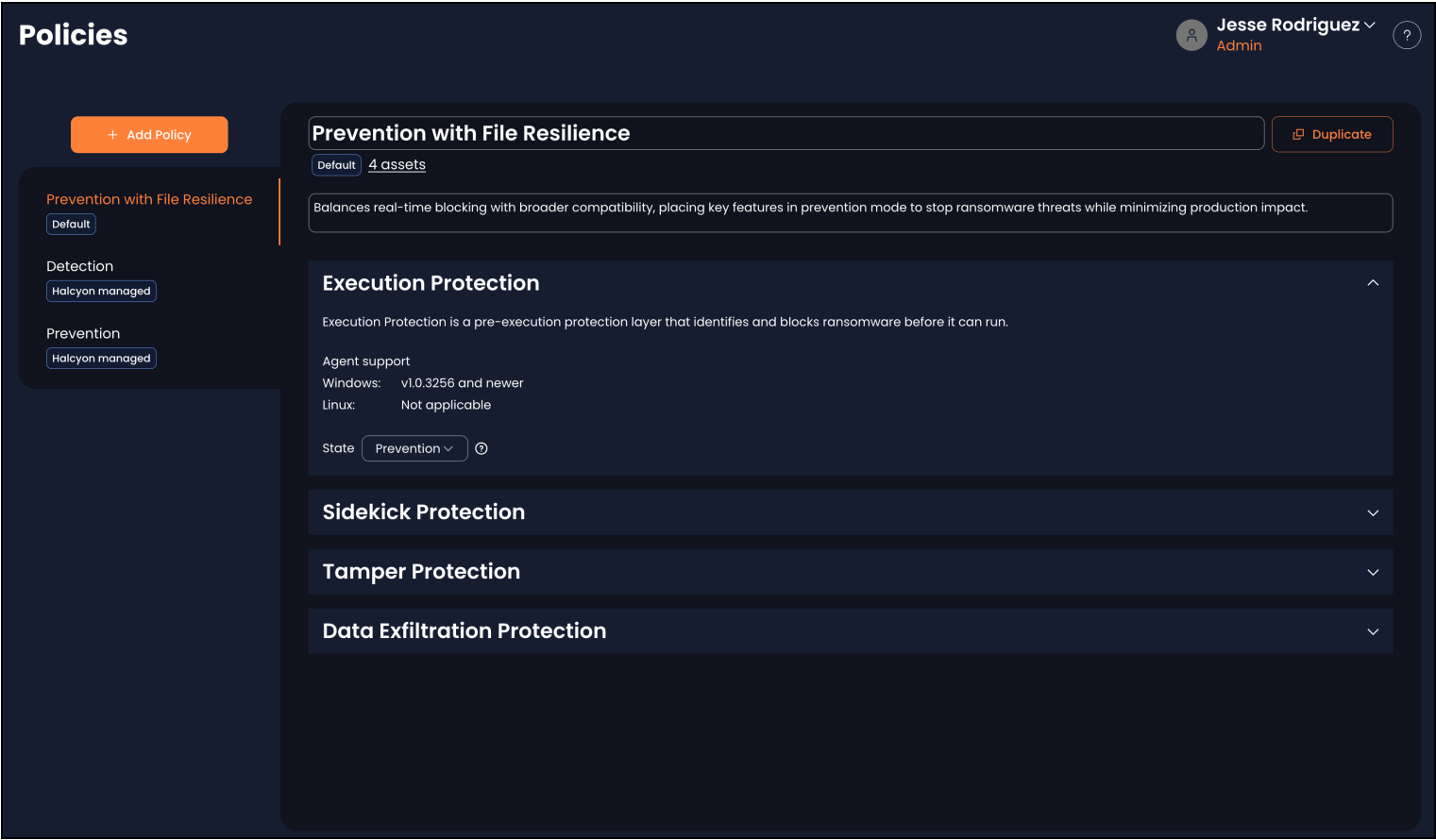
Executing the sample against the running Halcyon protection.

The Platform Under Test

Halcyon was evaluated as it would run in a production customer environment. Endpoints ran the Halcyon agent (v2.0.2606.60) under the default “Prevention with File Resilience” policy. The policy is organized into four coordinated protection layers.

Execution Protection

A pre-execution protection layer that identifies and blocks ransomware before it can run. This layer was configured in Prevention mode for the engagement.



Execution Protection configured in Prevention mode.

Sidekick Protection

A set of features ensuring that any supported EDR running alongside Halcyon remains fully operational and is not bypassed during a ransomware attack:

- **Kernel Guard** - protects against the use of vulnerable drivers that ransomware attackers exploit to evade and bypass EDR systems.
- **EDR Last Gasp** - a signaling feature that detects when supported third-party EDR software stops or shuts down, capturing the exit code and immediate context for deeper investigation.

Prevention with File Resilience

Default

Detection

Halcyon managed

Prevention

Halcyon managed

Default4 assets

Balances real-time blocking with broader compatibility, placing key features in prevention mode to stop ransomware threats while minimizing production impact.

Execution Protection

Sidekick Protection

Sidekick Protection is a set of features ensuring that any supported EDR running alongside Halcyon remains fully operational and is not bypassed during a ransomware attack.

Kernel Guard

Kernel Guard protects against the use of vulnerable drivers that ransomware attackers exploit to evade and bypass EDR systems.

Agent support

Windows: v1.0.4089 and newer

Linux: Not supported

StateDetection ⓘ

EDR Last Gasp

EDR Last Gasp is a signaling feature that detects when supported third-party EDR software stops or shuts down, providing the exit code and immediate context for deeper investigation.

Agent support

Windows: v1.0.3256 and newer

Linux: v2.0.2602 and newer

StateDetection ⓘ

Sidekick Protection: Kernel Guard and EDR Last Gasp.

Tamper Protection

A set of features that protect the Halcyon agent itself from unauthorized tampering and report when the agent stops providing ransomware protection:

- **Tamper Guard** - prevents unauthorized manipulation of the Halcyon agent's memory, processes, and file system.
- **Halcyon Last Gasp** - detects when the Halcyon agent stops or shuts down, providing the exit code and immediate context for deeper investigation.

+ Add Policy

Prevention with File Resilience

Default

Detection

Halcyon managed

Prevention

Halcyon managed

Prevention with File Resilience

Default4 assets

Duplicate

Balances real-time blocking with broader compatibility, placing key features in prevention mode to stop ransomware threats while minimizing production impact.

Execution Protection

Sidekick Protection

Tamper Protection

Tamper Protection is a set of features that protect the Halcyon agent from unauthorized tampering and reports when the agent stops providing ransomware protection.

Tamper Guard

Tamper Guard prevents unauthorized manipulation of the Halcyon agent's memory, processes, and file system.

Agent support

Windows: v1.0.3319 and newer

Linux: v1.0.4069 and newer

StatePrevention ⓘ

Halcyon Last Gasp

Halcyon Last Gasp is a signaling feature that detects when the Halcyon agent stops or shuts down, providing the exit code and immediate context for deeper investigation.

Agent support

Windows: v1.0.3319 and newer

Linux: v2.0.2508 and newer

StateDetection ⓘ

Tamper Protection: Tamper Guard and Halcyon Last Gasp.

15

Data Exfiltration Protection

An optional add-on that protects against ransomware-driven data-exfiltration attempts, providing protection against the double and triple extortion that can follow a successful attack:

- **Nefarious Peer Protection** - monitors for and detects communication attempts from protected devices to known ransomware data-exfiltration destinations.
- **Volumetric Protection** - monitors for and detects attempts to upload or transmit unusually large volumes of data within a 24-hour period.

Prevention with File Resilience

Default

Detection

Halcyon managed

Prevention

Halcyon managed

Balances real-time blocking with broader compatibility, placing key features in prevention mode to stop ransomware threats while minimizing production impact.

Execution Protection

Sidekick Protection

Tamper Protection

Data Exfiltration Protection

Data Exfiltration Protection is an optional add-on that protects against ransomware-driven data exfiltration attempts, providing protection against double and triple extortion that can follow a successful ransomware attack.

Nefarious Peer Protection

Nefarious Peer Protection monitors for and detects any communication attempts from protected devices to known ransomware data exfiltration destinations.

Agent support

Windows: v1.0.3256 and newer

Linux: v1.0.3292 and newer

State

Detection

Volumetric Protection

Volumetric Protection monitors for and detects attempts from protected devices to upload or transmit unusually large volumes of data within a 24-hour period.

Agent support

Windows: v1.0.3292 and newer

Linux: v1.0.3292 and newer

State

Detection

Upload Network Threshold (GB)

1

Data Exfiltration Protection: Nefarious Peer and Volumetric Protection.

16

Deployment

Agents were deployed from the Halcyon console using the current agent build (v2.0.2606.60) under a default deployment group configured for automatic updates.

Deploy

Jesse Rodriguez

Admin

Operating System	Version	
Windows	v2.0.2606.60 Latest Version	Download
Linux	v2.0.2606.60 Latest Version	Instructions Download

Installation Token

[Generate New Token](#)

Deployment Groups

Columns

Search...

[+ Add Group](#)

Name	Description	Assets	Windows Versi...	Linux Version	Update Mode	Actions
Default Automatic	This group automatically deploys to the latest agent version. Assets will deploy once a...	0	Latest	Latest	Automatic	

Total Rows: 1

Halcyon agent versions and deployment configuration.

Analysis: What the Results Demonstrate

A 100% block rate is only meaningful in the context of how it was achieved. Three properties of this engagement make the result substantive rather than incidental.

Breadth

The corpus was not a small, curated set of convenient samples. It comprised 519 distinct in-the-wild variants alongside 11 of the most consequential families in the contemporary threat landscape. The consistency of the outcome across this volume and diversity indicates that Halcyon's protection generalizes across the modern ransomware population rather than succeeding narrowly against specific, known signatures.

Fidelity

Every sample was executed live on a production-representative Windows Server 2025 endpoint running the current Halcyon agent under its default policy.

Attribution

Because Microsoft Defender was disabled and each detonation occurred in a clean, network-contained, single-use environment, every blocked payload is attributable solely to Halcyon. No adjacent control, residual artifact, or cross-sample contamination could have contributed to or inflated the result.

Interpretation

Under a rigorously controlled, independently executed methodology, Halcyon prevented 100% of 530 live ransomware payloads from executing, persisting, or encrypting on a protected endpoint. The breadth of the corpus, the fidelity of the environment, and the clean attribution of every outcome together support a defensible conclusion: Halcyon delivers the depth, breadth, and consistency of protection required to defend enterprise Windows environments against the full spectrum of the modern known ransomware threat landscape.

Conclusion

The results of this independent, third-party assessment show that the Halcyon platform delivers enterprise-grade anti-ransomware protection under conditions that reflect a realistic production deployment. Across 530 live ransomware payloads, 519 in-the-wild samples and 11 well-known families, Halcyon achieved a 100% block rate. Not a single sample completed its encryption routine, achieved persistence, or evaded the platform's behavioral analytics.

The assessment was carried out by a fully independent assessor using a methodology that isolated Halcyon as the only endpoint control, and the results provide strong, defensible evidence of the platform's effectiveness in the real world. On the basis of this engagement, Halcyon meets the demands of modern ransomware defense, stopping threats consistently, at scale, and under the conditions that matter most.

Appendix

Environment summary

Protected platform	Microsoft Windows Server 2025 Datacenter
Cloud provider	Amazon Web Services (EC2)
Endpoint provisioning	Custom-hardened AMI, single-use per sample, automated via provision.sh
Halcyon agent version	v2.0.2606.60
Applied policy	Prevention with File Resilience (default)
Native AV state	Microsoft Defender disabled prior to Halcyon installation
Network containment	AWS security groups scoped to DirectDefense IP ranges
Total payloads detonated	530 (519 in-the-wild samples + 11 well-known families)
Overall result	100% blocked

Well-known ransomware families tested

Malware Family	SHA256 Hash
akira	82e4eec824567f08778d343f156cbce57ac11d4e7a695ce26db40daafdbb90a9
Black Basta	2558d0817586306d0dd7fbeadd371785cd0a0b7ed860ac62760dbbc92866008a
BlackCat	0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479
INC Ransomware	ade6be5d8c1fc999615cd2b5b17e93002ef28060f147ef51401d4677e0b2e351
LockBit	5c1c7a2a124c5122f8d83af55999f38c9fd41781cb9a154e97056ee2ada3c601
Medusa	57a7261dd4b434140bf2bc58c6dda3909bcb44ac1976b2ddcfd4f2b967d59526
Money Message	97abcf01deea74eb3771ddcef8bfc0906b46a55172588de8e2ad20f8d92b2de7
Play	306de9054425c7e29bd277f0405f54e7fd08e34e08b395a415caea436a12de87
RagnarLocker	041fd213326dd5c10a16caf88ff076bb98c68c052284430fba5f601023d39a14
Royal	d72eb7759c61464843fac05c7f99166341106c5802e253cca787587c3d1c11b7
WannaCry	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

In-the-wild ransomware samples tested

0000c55f7cddbada9bacba0e79637696f3bfeb95a5f71dfa0b398bc77a207eb41	003a12e223709514403a381ba979a13b18eb7dcf9cf070317b78ba301bcfd707
0085f13770b5b1ef96b1f5b57474c44fa21ae8befef06a17cd254f75a071ec2	00bea5d98ccdc9bf16139ab6446d5b523b3b37e822b48166aff903e93017c2b3
0179b97794bc30bcc3bcb70b7cef963d67fe8bc49f74b157648cd1afe89d324b	01fb3f059ce8e5a459fd1d93a22701a27901e844fd5c17148defaeb391921661
02a36418ff64b6c42a46b07ca3f93c73d65487839aabab6d1a3b0e6230f9f4c3	02aee694635ff0f73a5fb83b5cf589626f01913784af803a362dc33cf905cfbb
02fb57ab79d39ac99fa4ff86cf282b6d192b399ad3c038bb0c95c4a7b1ca4646	0305739fc252ccede178986da6a39c2d334c5870561123a998272141d7940f49
03112f3749615cbc48c10b553d90ac3b67469aa4d8faa7b4677c8ab4a81c8abd	043a4c5272e79b437fbb1d62b4eefc59da1e504b78d2da34bd32e45cfe68d1eb
046f03701a547406b31f2de5f17c4a3ffe71d241f90bee8c785627e9514bc503	04b3f73ed7f1396a140d62224def5ef07248fcda2951c8327b73dc5cc542c7b8
04e22ab46a8d5dc5fea6c41ea6fdc913b793a4e33df8f0bc1868b72b180c0e6e	0553d611f0e6c23bc01be1657d62215f6c0faeab7fbc1129d163d6f569a0a362
05b762354678004f8654e6da38122e6308adf3998ee956566b8f5d313dc0e029	05d8f0aad0cf86b9ca6267f09d3891635d65ea933bb602d7192131cc4fc8cbd1
061d0c2c1fd965f50cb1bd5ab22bb6841ef9aceabc7e8f9c6f121182fdbff9a8	066dc9a1134b1db77c1574a52002f53b28cc29d0a3769bd5156d1e0e0a51a91a
0675bc21605754db3bfd0cfff2f889ec95caa50f6a3fc7c5e163c13c45e5d0117	06778e13d7e43c57cc9570442cfa2a5fca1d46780705a403ddf2e482267d30c5
06d8fb44b94d8a5df183b369529c15d1e9cf609b8af4000931a5ebdb34cbd6	06e750ffa4fbdef95030a8b77d552af164bd74653aa1f2050c85db242cea9f72
0785f51844c31d854aeaa65fbf1745eb09657f14747c7dc8329bafb2aa54f558	09b0a9d2a838928d507773ea31c1065e05aba1b35acb34b344de5e41848c4c8e
09c5ff735d3d7b8c47b4df7de35e1c72b530b2c2566628bc29aaa54feb4d89f4	09e4882e100233acc717ab805398a9f630d302436e8b81f73eff633bf39ac3ac
09e7dc34dfc9b9e0c9d3106deb351c6e2eb3b064b3d61826b80068b925ef2198	09f70485e2480abf10d31ab127933eea9592f3034dc05da4a7aba81b8c4dfee5

0a2424c2714fe04ac66fb0b9c87c9d4d580a6720e0c13dbc6d6f0e7023943bca	0a5c0fad0de136e1355b4af0a123502b3632983d7de83173cee00a4198a889de
0a90e4f10dbcccecfdf5b8ef51b6b75dc867f2a701efbafbb411471b885a58cf6	0abb1b4d4b4c923748a3f52c4f9abdbbea8af71049c4a1f38d0251a8e239e89dc
0b268ed68bfb51f02cb58ac7696aa0573bc4a38d31d07c4785df75473d6620aa	0b2e5b6fc06419d8c10a32a47a55b47eba7822e4b80ea738e56d3ad59d2e5eb3
0bd2672eec977c8c06bc88f7af94bac435bcbc597a58c55deb504e515cd3db4f	0c9cd7505aa42e0eec321d31812843b79357a1e7e11e9eb9134e9425008648a2
0d060d75735d847bf55e5005262cf6ed04e5f3881880ccbfa6932543d1bdf741	0dab56d7e10a6dd1d7749c15daafdc6bcf8c4c7742abc9402f8751b30c49424f
0db9f914c0c514eabd418bd8894c6351fd46cdc1e384c1e561bec5e41b8d3461	0dcd9796499931866c82fd5883f547873f33a0545be5ab8ece5ae85f8170c974
0dee03c04c628ecfbeat1bd5acc48a43ff967649f7691911c57d05eea7c96d53	0e74bfece1a50bc0077cbac52b47ab70fce88b797ec50d82caa97f68b412c6e
0e8cdf50ceb754628b6a8fc8c13c6bf8eef52e5cf9f619197c52b7dc5d14a524	0ea7566cb7dafca986939a61f08f4ed3d06d3fb60e760f5bbb1676ac94fc510d
0ed273853d09146c7c1fd435354d7250d37dd4d128753e23e6684a4570a32f85	0ee7664a13412efa4ae3586ee4272e939b1b98889dd446752d7ef267389f2b63
0f02734cc4d81864067850bed0db593022dfb85a732ede700017c31abe8e2725	0fb7bfae5c2e10c4b752aa9af70aa0bc146e9c6ba22a330413bfc0aa3c581809
109287a22ab349544587f8342458923e761b45f86d2c6be394f9437b1dd2459d	109aaac64fe7ef5bbbed966000c4c56082e16900a68f5dbf1ab709f1d834a624a
10ca71f3f8e80e5ae8500a3b602e4fba131742392a151d2a795bd5aea4f277f7	11179a0188f13b38384708d490b9c434cb8cd38c61bccdf6c1f8d8e1db9b03dd
111917fd76e10fedb402c5656a7164fc2ab84b0df479269d932ac221c58d0c1f	1133e6fc3a7ef50688142f101507fcca2a7b9271a17466973263ae2f0ae30a11
114be72424c2451b6e0fd8dbb181a2da078a17780bdd3ffc8d490cf79246b9c8	11548cff900ca6bdd4a615926d8ace38c959cae6719d07567e186ce07be7f143
11811d48c3fee9b24fd182bb9fcc574d7eeb5f8c9501131829be54c2e7849bdc	11e59120875768e8f457a2b0fa07ba49c5d3449aee2e3ce5e9e5dc01717adb6d
1228d0f040f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2	12500aead32f0dc9181783f44f78ecfa8cc3978ac6c11af95cb668d87540602f
12d50254e587947a460141641e90195c90e713fe3c35f2d19ce692b4310da654	12ee150ac7298ce731e9dad69c59af79ea15852d3cd69ffaef95807c49335915
13044138fa9a4f5f2f6112de0f92fac4a1cfe41b83ae9fc3453bb203e20e0e37	13340a15664d413c710774fdb85962cbd8dd5cd28db32e0a20e40845b499e9e3
13652f32e8cf1b9f78ad8b6b827c9d996faf2a3be1e688859e49382b38a7069	139a7d6656feebe539b2cb94b0729602f6218f54fb5b7531b58cfe040f180548
13a46ba2643710b21458a4ea4293642b08947db9763a217809342a8f82009c0c	13c09019e8cf9b569d7c05326e6c548392c094b693812bcd18ccfe83ac991474
140ba6f6d6860d3653556ac11e82e2c1a9e3a934b9c5816610be4892a1081c17	144466c2584be7a84700bf80992e1d9de81c1367ed575b13e8dca5f7b8589a71
1493e324b7e54e85688045d03336b520f9ce739698b78f9ff603ace853363684	14be0fa1f4b703ee1ec218d4ae186e59a08f37c95c2518c938cfe9ddf6fbfbf38
14c4da236e87697bdd9191257f434f9eb515fbaf3c43ab5def241b6099c16f24	14de37b62b5b2f7696b7032a0bc8409a25c1d1fd900d02df40870998a8eaf1ab
152d562297516c01a35878e81920daa5ce558dda089e8c886f14d0b43b3d60c6	1550e3d8ed15db66cf39346033457d08b05ae4e7e62eb036a6471dc6359be241
1598a057f598749efd25a940f8a9bd9e353394ab4ad024338171d6065e96ea48	15a8f4ae1cebc1b011e5fae998ea3eece3f6bd65994e2f22daa27b830fce2fdd
15e5c681bf5888ff06f9f69870fca9f68a5ef2a00fcadaafc0c02113b543cad8	15fa65dcf5744a26a46aa51d1472c5aab03b7ebe59c416775199fc59691bf636
1631978bcbdc2afa4bc9563397768a8764c8e7a5617ee3374b36f044a8cf7dd9	16ec4a6beb0bb20f28fe2f9740575411e364acc976ee29b996e9ad1f1d7ae8
17cccaf7e3cd247b710527a158249ff5f20b1e479326bf53a1973592c5804461	1816775708b74a5c436172f5ba98308eaf0388b1db91a97db286abde37c752e3
186d49017645de9257f06f731b6830e0abfbad2339d865a45a90a468a710ec20	18c7f327fbf0c783e23dff0c32747ee828a6191efeeb6bbe1305070d70999d4d
18cee239efee80e28321ca153ebbd75836e926ce47f732678c8a1e91ae4a606c	197a76424435e56a5d2bff1261925248d0b7053d222bfee6c77ee1725761d646
19c0beb0aa9343159b4a5116be996869095e24b77673d7a4c7ff25dc7daa98bb	19f66d06ee76423b57159b6a72e2d00fcd6317b90e7bfac578214c5a3a4e3338
19f899dbd6301deeeeb1b856532504195cf5ed14e3e28a711995718b2c69e710	1a24ca4d08bfc68518434ace293d380dd52a80831882954ddfb4c9a2753e810
1a281397e0766151130a5473be660d194eaf5b596346d81fbde8b49d13f674ee	1a2a1080ff71fa51cee6b61934caa55106e114b3a872693d2e8fdc906ffde3cb
1a2ae527b7cd4367d914fbedf02ed960f1d28d10bb29d7689301b3b0305732c	1a2b4b90940a7f159e461825ef245a1b818823f4530669a49f5d4e93f64497e5
1a4a843fe14e6ef1ac563785286c57a72ae4b9eb455966c5ae82b38a3c6174ec	1a773441985e7682ff8e0cf885019d226e416ead1695ec188023777d5d4c9377
1b0b5d338d23ab7a6216d8d8e96e7b4f062c4740e8374072fd928fce563253ef	1bad553d11213b4a3f7f54f07f3ddb6d09dda297d59a2c70cf9e0d1d642926cc
1bb211c8370db7e8b620fd36f786e731654fef9731306bcaab982fa15b4b2ac9	1bc54d25fc39857be6b0c1d6940c471ed6d7698c16c9844095a5d6ea05948c53
1be07198c324c9732d4e2676945ec021eeacd78775aea2100f49ca0483d3f901	1c102ef66884c95dcaaf0dcc7e96fd6fc6da197a904de6a1d0895493c1a4cdb6
1c40b5c96d13580f1dfa38f59f177502349aa1c962ff95559e0ec805155eb983	1ce9de297787f619c15235435c693d319d4fc0d97e690f598a0eba1f5737ebbeb
1d1b880e752e4efcea941a7675d4c2bbf2d2bd63a57cd098a7044889a2274200	1d49c36ca884212a616a1302afd705c0800f022c16ed7a4160c5cd44c1d7720d
1d855937bcdef8637fa5b004f0fb4e15b39e92d1baa3b8f3482f2def184e760f	1df790dddb201f76bb687448b7c316d7eb0f3295aca4429f6cf696cd60b14ea4

1e2fc5ae75fed3c96401b319e6bed4d4188ddb15eb158bff58a86d4d11190ab	1e39baf3c100a1054c3819d43d42f7aa5d47aadd4da77535bd68711e69a483ff
1e3c5a0aa079f8dfcc49cdca82891ab78d016a919d9810120b79c5deb332f388	1e8128c37ed9ac36a7b850658b1ab7a183501cd9dbbaa02806e34e6b31bfb17d
1e868a8c838235fe7510cb3e244004ec73d866084810e9d9a477f83bf6d193c5	1ea89fdef77e7648bba68b21d31fe44d84cd0de17bef982aecb3e6c4418d8d49
1f252585420de8fb69015595e88ea068efc6a69ad2a626e291483abd04d75a0	1f4494f4bebf4c4ad0e779a9cbf9c42d98145358b06767688b12de687ee14d57
1fbe92fd6bfe90b69ca34637c2d22a78a3fabddc0fd6c1d58b1cefdd8d82a850	20447a8d908c2910585ceca2536f338b4e7a3a2907e4cee19b59267f4a68247e
20485dee1d04ab3d2b8f7de5db0b555d5bef8a7d4a88688405f7ef0944faa577	207555260a0a5fd048dc1deb72acea040d57f51bcae79a81fc9d63f0ed2ebe6f
20775b3bb6c72cb1391e484f9012bc5abf42e0fd588f79aff7ffd1ecb2a3681a	20ea5a86576371b9b1e12838b4c0cc16060980210a44c3f100144ce57d08e7bc
20eaae7e23b85e42915307ef478635fc8a17528fdd5026258b78749f3bfe01f4	213e716f45542547f33173d609de4c3382901bb2a6f3da042c513d010df0270e
21500278a094e6e4d5e3613ad2d0ed1ad795f7a54fd643398578b80fa1fb773d	21695a69a6309b605b42878781baf59eec9c8890943403685a405017f1acd684
217e7059c3096776ca6639411c2ea351a3a0ce6eaa83c48735e8c8ebcc00f3b9	21cd9ae5f690448f4170132171269e4bc79253b2e55d8ebb74ef4c7410398494
2203c4bedcf50fefec0b3ef51fd60bf7875fe8c343da8219498981b03f9b178e	2210baa7b596879b413965c17f9f33dbf698ac183b2b82329d397c73dee5fc3d
2312fb3d9174830e02b9636c8117a0d4059936c32ac3fd0535a19dbaf839121f	23159995210062562a9a84bcb8cad96001c9fdb8025da26bde05def0cd85868f
232de704644cbdc83456c00202e4ee5f3acfb6435ceace92dae549af4d99e50a	236065889a55e5b73072fb87f349505c7c863f68718a0f9ebfb8273463b7ad03
23c3c226820faeac5c29763e58bb3ee8c680fe1f438d1ec538023adc58a20bc8	23c54ab630b9a1b03cc6522fff3d1a4030a8a3713b69684ae8848ad4571438c7
242aebd465074b295b6b6ad77607d0a8340886ef0fd8d1b8a32686cb320f46f9	2452a341ed8bca9dd380e6b97b0270b75c042b49fa4b7c769e2effa1cf778b57
24a480e9fc105dbd9bacb9a2e24a0a08d3c140103472e43c8d4a484df744edef	24fde15b911a1682ea65d365b66277100175ff33b3a08bd1f26008ace9a02187
25bfec0c3c81ab55cf85a57367c14cc6803a03e2e9b4afd72e7bbca9420fe7c5	25dd99ebe321f3711e5e7be0c67d899e2395df0cc6f91e9381ae4c650920af2e
262358c0caacf2ae846f2868c40fd8556ee52a9fdec33323f823d5b7e826f361	26a5683251f87bf6b27e7ff21984a052ecd5363c53dc1c5912c068394ecfc02a
26f55b42952d42b25d0a076fb6e8d93ae5ff8c5e9002757f0457d7054cddb1eb	270900314dafa388586a51c73a7e66d99d9ac0fe3bdbbe840028ba99bef604e7
27b68cf11941b87535232b09a8db698a32fa28d2449e83f2d082c00eba65bddd	2827e992b12d787fe257201313a910a98a6d765883d0966a5305bd742ecc6d31
284b294160d8af073b668443204ea9f49d93f12d3ea1e030106eb43c1ae2b1ab	288d6ff8ffa70bd740dc87b973a2620ffadedd4541c787f995dbc4965ff93745
28e83ccfc6069bb00c4ad2645e6acead34373061d13968feb0bef742943b98c9	28f627abac4980aea326f8298309ca3c60164458c447c4a366f712bdbaf5e38
2905585dc0356d27383bbc9b7c7161eb3cdf3c2409c7ed6a4d3865499fb8b811	2a38671288f2206d1955b7724c5c89c625ab2ffcd1677228252c2283fd3e4127
2a40a6605cf1c2691776bb4bb4c2ca31eba2f8d90d42d2a4a8aca3502779adee	2a4e31d65225ab3297ea1d767f42ccb400c8afbfa42b1310eba5ed6fc19f394c
2b2172da57a4c5633bc40dd772b80b5b1101378de987adf315639add264208ba	2bd9ee9ade08c0bd876ec816f399b1e0b96a60cc9c76ddb8e2470476a84757b3
2bf8e882c057c2d48a50b0e46c906108681d718245c2ec50097eb570c6ae7c7b	2c78e8904031d5684c8538c81402a68d20ce4f28ab584e829968e91149c41355
2ca7539d2d65e887e3673f39fb7216780b43c2ced6a09c9e09752d533e9efe91	2cfd6fb05252605b41f017247e53de0154880fc64be63847f93c251c1b69f74b
2ddbf3888b8db02323cb2ad66c2866b60da93d18b2979229e68f1d36def479a2	2dec51241207a1774f34cb623432822e8d4757b80ea730816b32685b9ebd7cca
2e464ef682ab399beb83c05fb83eb76b32601f1a4bff7e56621803036a5d44a4	2e501211ff6816ea024db150d41615345f6259568d5e15db67d30b34f060252f
2e754ecb1b064998849c1726f2b21e9ab9ee35b94b40e38e755e63c4874d4efd	2e7ddeea92385b0acef13e1167926fbb9fb90e15ce2d30da6b397515587f3074
2eb49b3ecb235a85789a2265e281182d9f7ef3fda0af610435157b8cd3b9d495	2ec160cab1a29dde59883a4ab192800f1edb38b8af6a4a4db97928771c61664f
2ee6ac6270c386b42a3f1d9adccda744c49dde944d8ba79fe6d780c4a09e98b0	2f022dacd013c10da72759a20cf7392637460f983d59631ebf636328d0f977ee
2f3032891c5f4801eae5bc44eab58f5438d07dcc3159d699095727e5f8c8c1c4	2f44b100f69534a796c0fa3db6930d18fe2e8359551035a346f77b6763cf6f9f
2f91555af84698ee0c7c793dd8287bdc48e6fa27e3c90fb61f74fb92c92166e5	2f9dd6c576897b8bae9e4c723d6ae3cab8e3f03075c2186aab4b4c84380f1875
3015f3af233ec911920e3e6611f1cb0a6c857b8ef961f6965db5b544f6043d63	30e73d31ad9ae201ca5221bc5ae364989f8658cfa98142e4d90089e2d0989883
30ec7f2230073a6a9c44e5d8be55c918846b410532790ec6a4d64f569a33936e	30fc76fa9ab29effd9ead257facdbceb320823890f8d9771c91493918fdb4c4e
310043170798e8be728b202bd30d0b695b0afb862df647e3079b21f438b0e68f	312431691c096bda9f959dfb64264d29e1d3da06d09bc252e4e045d14585cea0
312ed67e1dc83ee5931aed99fa2b90c219a951c607bb06c9cfc613f625cb39de	31485a7ce7e5b4ae39ee06c8c425fe9090d1520b062b4941ad37233cc4851fe6
31927b09242dcee836edb23c23e02fae8c223ce7ba19bfc021ba3536b75e6f4a	31ec3ca73892f1116e74fef120e7816d7eca42ba2b147f0947b0be1ded7de64b
3203ff10754a7d9f30a7931b2076c03a42c607934d45a2b1050bc5472e5f7429	3231a27209d6d84b5649af307dcd720bd68377d75c9fb7650b717b5b5b3e16d
325493ca0b549e0bafdd509ec25f624df4e56ec70219ae9077b266bc973b906f	325c5d1fd2f772e7de77fff854a9259bedb253e9aa0a53db3d9fc66792eb4ae1

325e68d260f998d766a958aedfab6d3d6a68464ec739e210f6d9213a16b4cd71	327d7323c0e2058bca4d346af1773b9dc75de7300bc335baffc988d927477521
328e47ae4eb2041cb27bdaf555ed818959155f62748935556697983c06075580	32a790c34dfb26d8c64ebe78cea4e6e4d76a4aae5ac08eac6c5628f0e207f077
32df834aa1a6d2d2ce1f6fb4d761148baec042f9483a1e17831572d56bef5951b	32f02e1e6d9104a070f260bca9ccbccb0add32c0a7f7dca0653dec41c35803d6
33611fbde2eca82c40b9805042b7eb52eecac7175989a9c583ffa99e35013b82	33639ecf0125d32de1cb8b25955e05cb7c25daba559baae507a1b2c4e23d1170
3377c186d074f39b9c6bd99fcddb01b36dbd0e0e3a0f5f99d07c033c6889d359	33afa2f1d53d5279b6fc87ce6834193fdd7e16e4b44e895aae4b9da00be0c502
34716b6fb4a4c4f2389621af31f9c352157e6902b739d933396c6ee97a943ee2	349c8c4c06c53e0c9912b74283c9e5bc5dd512e5676d8fa42e03c8f917b502cd
34a166acedbfb7f55713dee7b7caa5a057d40c4663b6ae540a1a93cccdff8b43	351286709c2ee33698ea561657f5b0c1644cc946084d24be931d96ec29fc5e7b
352cf240e8410e2d4a57d8eb6224d2f04d78288bbd7bb8781840b7c259eaf410	355784fa1c77e09c0de0fcd277bfc9edb3920933f2003d2d1d1b84822f25697b
3587c89d94c6ba87968bc64dc5fa5456abac1d58a1cbbfe4b2395265fba5ee9a	35e19682553b56a2518e1f6c3df2f42bffb40a0ea755b6908efd0d04723c12f
35e1b615af8d3ee2c7c240d84bbd7e2c033b817c66a26064614fa47f263d61e0	3641759c232dba3b8c1858cdeefce2e6c7676543e1ee582928acaaf65d46d141
36484100d6624806a3dbb88636d466bf4fc18a7ed099400f1fead7b1ddd3a967	369887bf9c111747938f5608e4bd2d098aa9046cd44891816c84da5b39a1602c
36d942498516e926984e45c546e28e6c73e246051ff321f74f018396610d98a1	36e2a66a2b5412fd2006a9b43329d5c9d5befeadd22143bfaf68ebb68ccc125cc
37364bf6ff165fc73d9fee57f43b4094873606e1bc1c78490eca8b790f333ec	37720f30bc6ad0dc8654fd20936845b1b02135db50c2cb1e2013baad099c75c4
37899d9950cc64437687c0ab2bdcaaa81b01e56aebef7845fff9565dbe889365	3791154be3c1a9fca812f58ed622a817dff81ad86a34d60db5f662c11a8b916
37d11c6e7d54d852a438bbd7ee5586879bc286f6e5107c4b30fd1aaf6f7fadc0	3829d01bbbbb8a0187ca4d01271b2d61aa294780590e049e5175c182a0ed4f788
384ff84aea37f4279947e733d13693fde79fb08583f16510bcf37bf079ce8d18	3894db0978e2a07b65c1dd9b1f6a9b7d9e51c12158f44e9df3bd02ec820eba51
394cd8f681ea933fe48b69dd75a9017f32559a338ecceffba8fdcd23bbc519f9	39c7f21764aba05f06053c0b07983e8ad4e40ab65acd82e23d22d6ad42ddc7bf
3a0cf7f824cd82b039a64c54bd7484308d03f70c7598611e399457843b0f1342	3a7de348ce59bbeada267b854fb97f77c50e086157223cdcb609072ecb7b60d8
3a88f907b0079312df6333fec1a267cf8c9e43419c70298337224c7c44753540	3ac6c88e9519d343db742b452cf74854abaaee8316d5eadd0621ffa5d09e5faa
3afe8147d5c028609701fc60e89b384c467f103f9c8a92b88f16545ff31e1575	3b1d975e17ec74b820ffbd792fd067b84444c2b02337a7a401fb434ed5aa0bc9
3b1f3dcc0e70e0f99db67a6804670ae9e9605fe5a58433c56c85ac4d6c0b1103	3b4e0f9f4f4592e715e649f4cdbc6427e6479ca5f46bd560365aeaf0de313595
3b6fce7df86670b2a0f83869ee051ec74176deac192e77ad22b8669894722a0b	3b7f3fcb1b8a5c40a05c2915e7042b151ccd9aab4f01a7ef4f0c24e6a6fa7519
3b95034236f25eaccb14f2639c9ea01abe77888bdd1018ae85f1a1997c1691f7	3bc38cbfd1143c5e2411dade6df8ff28a09b8a63397d86cd7f3b3316ae36ad67
3be0b6b1b975d63746056d743d1da2fba8066bb3937ae7d2d3a9e88e53a352d1	3c07ab463ec63ad60d1a51d2ada47fc8d593722eab238f1e6e1c78e6670badf7
3cb4c1946982747df6f94fb6d4702ed0f2b318f38f8612cfeceda2abde831367	3d0e22e2216aeed6321fa9ae214ca21fddb604247677787199e3e8b788e8f8a8
3dbb35b9c2752d9caa038cc3372af2f7c7bee90d3ce921ce959ada9734243a870	3e035f2d7d30869ce53171ef5a0f761bf9c14d94d9fe6da385e20b8d96dc2fb
3e08dc086be5a6582b7d4fbfe586d8b903ebf679c22e903e21c7938e2253ddb7	3e16929d3f56b20a623a7a0c9a5ad862897ea0c758c7adadb8b941cc3200c397
3e3d8f54eb911b086875d48e2e95a5326e975023e086e9992104b8efc9e9411a	3ec4ef04617041a5b700b817abd993cb6b8f50dceb3143755e9f5e5aaa1f77d0
3f1a997a19e863bd10e08aa9ce3766339ca4ecd962e606dece9c9109a09e8989	3f7a31b72a67efe03906eb97a0aa279e288260884f6564745f6b0eed264c499b
3f96ae5bc6bf3d0f098caab482620b98ba1f4574b03698c55b177a85e7dd9087	400b5a2f6cbf803a9626a300e1acdd663a6a46b6ef9051243358ec0ace2f73a2
40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6eccdda67a747e17	40de140251dae960c3555d50bcb8705ea8c7251fb7786943afbdd78fc85406f
40e7bfe8c2e763c546a894d3326ed3871fc0f6c7b8b691e40df5d8e03d336313	411cff7686e071c4142309236bb975fa75a8cc84c886368d43a936ad36504f0
416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e	41716c618af5ac07214e5ca4ff0c7538dc5ab7fd0b3462213cb19c2d41c6f282
41bce3e382cee06aa65fbee15fd38f7187fb090d5da78d868f57c84197689287	41c87a6e4515b1a1f767636c455d484dae6659fb00bdf78dad7aa4d70583caef
422b0f7e47a49ef31d59e70584faba55b14fb713eeef51dceaaff3b80142fb333	42496a3d1b15909aa621713b4b36b1bcb30bf423af5c3ad4946553abf3df424a
42f7ef7956c43e3efafd261c65d405bcf6fb728bc798bf5461165d78ea156f67	4337d7b8a3405e245ec8c607fcdfbaba717c6c299569ca000960e99742a6dbf5
4393d4d1272d39a93a02818c92b3fb89f5c30c0732191bfda76755269b56f24c	43b20ecf7f88a5594709cfde684f509b34b768421a283fca2a670648a0a8162c
43df71d99d724fd01dc77717750338e68605af1cb20b10ab54b724a1fe579b4	4429b765338367d304e98635c7f2df30473edb0e4d90eb739015d726853c7fb0
44844a0dd1beab144365289ccb6904d3f4fc41bb10fde687f1c54f233517f9c5	44b4687563edba8978551ed2d32ed8b7bf1440cdd645e93e20fde9da60e449a
452040edeca638724280063218afc5c9698b16f8bc1700c2b147f687e887545f	45dc9bb023598cd0bcfd4a795a304ec18167e28d1cb6dfa46e129727a392d0b7
4653c92bda89dbd012629642f9eddd08cfae69c22152a253e1e464b220a7df5d	46f1acfa2bc20df79923e8610c2eb70d44b9b0261431750b8368215836c29aac

47351390e09cdc867f8188d0821ccdedc54031d103806e2a27072721ae87c7ab	476541925e50c623930249d4f8e0a7f02357a3e4e3384864564653b23bdd74a2
479c0646a806b4d5839e4f1380d6e23ec1a6f29782f5eea53791acae7e0ed1a3	47d16fcecec0cea3d7b25f274f61c014019e9ba0d764ac270beeb211af2f0e1
483a4b303ceac929286b0f7ae41909b8779a79bed8184fd4512a83fe722514b5	4895307b795ab409411f248042e08ad054a7988e4a43e9f7c82b13daaa72854c
490f2dfcdd55f858e4318daabb0a25acab365f1c9f2d4b76fa7f413e4bde493a	494d4a23d91e4f9c6174f38b786ec7073e16b8fe4995aaf57a465b580694c5ab
4a3a1e917586b6f131cb8dbc787a53954e0c50ce3a379d0654a25161c8775dba	4a3cfe78a7b07b3f3a82087a1a0e90d1d428a83c38d1cc0ca6ac21fcf87eb1f0
4a4af2cf8a2814dd9ee4b7b2f3deb0fec6acbf32dd8256d2e81b0aa591950149	4a4fbe6c26090071c17d34ef4bb9f91b4f9dac653950c27d950e383526a9f1d2
4a5b04cf77636aa824f4e5f52b3d0584e223a587d1b3a83d0e1f3531f51a75a2	4a6fcb18081307deb956ac4e065d33b2a7b9f4680abee240d8494bc1e31c4ba6
4ac794d727500189bb35ace4ef2b39bd026a3b3fede6c77fcf45b8948dbdb23	4af1d309b5e9b581053bf720734ce1275ff1ac4d146b7b6675be5ed05b8a5e6a
4b0389d9fd2f57f33081424e4f6fd70119cbac965572af7c10ebca247efb596d	4b9a45a6cb42426431b1e7088c89a5d9c5d8b1d52e30887a11eca6b2f27ef545
4bddf1d83aff1b4ee5d43ae80eb781e67c5d8c2bfaea5f0f2baa0d9fc5b8f582	4be415c196067f67e61a9ce6502186281b1c6296fbce722b585e2d401277fe42
4bfcf460670fa5b692433648d043c99b7709e3061c2092ecce31ab7101e433be	4c0694437066093c8c0af2f5c69232613a4223c7c2fe0c9a95f9b996cabd2ba6
4c4f1d2fc750fb1718f42974c943b887f77849e63564d8a836797a68f5e978010	4c4f2e4334abc83202641a73219b4fdc7b78965bb5f950cb605cbf4909b99bc6
4c789a42fa936d7f5455c475d0a324dc17b4c261096e6195fd5a24da58ddbc4e	4c8a396a41a5dbf3f3a9156f02953a3dde6463792c1df37cfac8a78bf2da225
4c91274c018d2e578afd75c6a91efbebf279364224e5fa6afa8152ee6d4b151	4da5b52c7cf1080acb7a6948909489d3e1bd85639d316e5f5d41cd25e94b164d
4e0f201ceafe25e91a45bb2efdd5b279c542739ffa573c516cc1fd4338689e79	4e430435fe79c4cfcae5a15db87b469c7b8ed684b2fea5ab680ccc304553f02
4e78271ab70710d11a455e89ad769b4dbff0cdec21c31b6f0279942361e353b	4eddf9b4678049dd5955d9dd4bf35470280666fd636d9401095bc5ce78def9d9
4f9400d87ff7894a8eae85bb9d3ff58b207848549bd8bb37974d26d80d7b8e04	4fb72d02bbc8450256a7517791c0fe47478fd876ea393d5676cf0b8b213dfbae
504c55eb05c663b9777ef3d834204e75304d5c39879fc36ebb2b6a8bf86a1ef9	5118487605fbae8a280b74697a80987c06781259c8526b02394946208dd58374
5142b54ddc44f6bd5705db6a6c6b63625b2a09c79f7f4a6e37091fe4d6472ece	519f192848d09c27bdf94fc7647826a0f371ed54af3a4511c133cc72e2be75c
51ccc3d9300fb6bcd9f6d33474a436079c24a4b005d5e0a56acf5d6173eb3883	51ffa033018d9343049305061dcde77cb5f26f5ec48d1be42669f368b1f5705
527c42ae884fc5a0ac7cd62136b3237986cf8e96c03c4bd44a84ce49a9ad0014	529d26d33394df465e075facc994c925b5c11aa3be6bc453d3cb65d224540221
52d75adcda87f702bb1ff9c1bb747620c8d1929ad73e741816c65b5f0390ec72	5306423470df1ea746ca5c9405e4a205692bb26b714c94b5728774b67dc3acac
53383d0a1768598d25a87112ac69008dc69bd8cb01fb25b10caf3f0b22f88243	5345af8f49c750ee4425d60f521851484ac8e07305b96458c2658b7c774c6285
53473454925c3d75c4eea8c2d884ed49ca961d82d2e02cfd3809bdd14f482234	5363fb7a76901024e9caf60862d27516028140a644625afb74851efe472be68e
538835903a4043ea7e3bdfa95314d9cc873d49aedbe031a46d1256e513f2f731	5389240ce3717e5591c00dc50fa7d40699242a7a152bd63451a37ee5d93f98bf
539050939433011f2a6658f1a2d39c8a80145747e973a6a7f595aa8f3896a273	53c6e0030c7d7de37a2e989b9df9b9bee7bd31f6d9bbcb3d65187bee79daf7c1
5440747755660765b7ef60c274f4e89c4fefb0692b5b0a08fe0e3cd641b8897a	546d31edf80dad3347e5f416ced251655230e80a440f272dad07dea815b49792
54b9ce57e8e9852094aa866a488a289f90ecdb6475b8a5587cacc0f32dc88663	54dd24f92df70209c3e5b8b244a420ab208a7cd3380d446671289694bac2b654
54fc16dd92df7fceff3e99f85ff9afcb6778a5c38c2ff05e6ced0b0469c89efd	557c250826ae74a9561df683151504a327f8453302fd1447e59df9af148b25e7
5592fcc5e6dfc129c89a9b518e2a283964d683aba10e2605dac44312477045b7	55dd7d5ff2fcbfcca3a3c2a4a0b6028a6e447952e171ee34e26982d5e08a8d04
55faa4f42d54bb163789d2211f6faf188d10ae134dcbb8fc2fc455e69dd000d8	55fff8cf6a28b7d5481eca7ef351a6d6ccb7a8a126e12f3feabf4983ddc9aedd
563a23d7915aa65b64570089700c1b8436ea65f88f984db19088534b0a79d6a5	56726f8fb86ff5a866acf2de33dd2ca493040895119c60e76aa7abdf618d16ec
572cbaf82c340e44f8eb3ef9f696a4c04692a8d695c79c855b244e11ea43d867	573317dd4ea92fd509ff2879d4f0e6a60a452595019438a5c814f94055d4bdd4
573adb05d0ab04bf0cadef998d84ef3291be38cb88a60f999815b5b9629d2776	57a6781a924cb9f292c26cbc3f1334d9940622210975d7d31a25dccfa340b3f6
583e600ad8121162f8b1123ad0976984f88792a9fa3f8de94018d504d78528cd	58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6
589f9777faeb13669a435a62db9f7bbaa0f57c4d78769b0702248b04e1dbef3b	58ad733b6abcf3793248cfb24aa8e75709b58982a11b86800a81f65287747f24
58c25228491ea7a4b6b9c842188eb5fa36da4102e88c16c0b39bef964d143053	58c763b64f4d0ec776f4d464568aac93ab8f7a86d6204bbe7aba29056d7d1160
5911c73e47354b5c884e5e9e85ae44634e284d04a0d21be8473462a46bd79dbf	5943cc84945744720c51e05d5b85c62d55dd1b3f6d8a163d2cebfbf14ace5ce0
59a42267b9e392fb7b5c3b5f4ccc28bd7ff3fcc1fe5d95539e36bedfdb0440	59abee968c2453dc88fddb6b64cb18ab7c0a024579e52087c9f73c7868c274ef
5a025e90322a0561cd844a97cbee426eea06ebc63f2073eb99fda5c5c448aa3	5a085858957683731b23b139fe2a728c0d4a97503e9ce6f28c4d0f4464c721c4
5a0f393c6f12bc60d70ea6293b16bd3fb46699102882e534333466b186aeceb7	5a1617a4566520e1cde85da7d832ef0402cd62a4f76d16f8d74f14dc025dccf7

5a596fb1e2cf5949b576e63eb4f8c9c0674ee82b716a8d124f47bbfee60e9e5	5a62166caa6b71dab4f2f25fd3c95f5e532d700d13d9063ea92d8393f0737845
5af44619bcc7a5ec5d5c91d4a3e2e3934cef504eea5b83f46d11f11118de0b05	5b0edcc8eb9e6855b236e4e60173d365e64a75e4330484136857fedd0c15b34b
5b17977681dda9f411c488562cce08aaef7c75d34bff08ed937f072d4ca1d0e7	5be1357a2a7c11c607eca8de1085e06e495005ba91b2e1738b9832f6750d20c7
5bf3c79c215baa02b56ea179c08281a01ca2e862f054b4d7619a106a0bbdddf1	5c2f8738655ca508e97984ff552171d11003953a931b50a3fe53044acba59bbb
5c735d8e0a9df181b234c2523571740a00a1b9b7309ad1ced290273713a51c4a	5c90c818852b5e3b9f6922d6d3d79b536b3a493772f2a6195129d018b1e3125e
5cb47a20841fb1fbe14e147634b45b7a2ae6ffcf2881fa87d0160d8cbab662ac	5cbc3d3a9b8052f358598bf0599725b733e7cb4d45cc2d927103d9247fab8f58
5ccaa2a253d1d83e97188114e83bc6a26b6d8ffaf07dce2d1f81d30024e2ebc0	5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552
5cd068773b7dd9cc44c0a69c66470029ce1a40414e2f8e91c1c74703c1302c65	5ce036d79fbfbc9e4466d8e5e22dc1a7f355a27045b0c5eb36ce7f7ec59b9623
5cf90d4621b68b375089c82de13d8464bc99fff62b5656ec9ab3f16809e68218	5d40615701c48a122e44f831e7c8643d07765629a83b15d090587f469c77693d
5d55e5b70480d492d78d5c9aadf2f24576b8e94997b9191997182f5673622a0e	5d7ff3c74b97445d1957ec444de2b373e90e35187e3f994541112df7ac70db94
5db02cbaaa84847cf875ee07bb23311d35fa37764ddfed6acdefdb2653e00a8	5e4c85160e04892eb694971de69a817f39c4787c22cc0d2ff0df659cc2cabafd
5e6a07a362cbf91b37ef9158dd154c3b463428e3e7f7d707e3a68776d6d8bf7f	5eb237569d5a8acbef04d8f5601986c1b025e0c91790303c1cf03a951bf29f44
5f70d23114051e0b4084437612c7e445d2c2d4bccaed6aeea58d4033fe4dc7d	5ff4b223e5ec450ec7f0d1a5c839c1b9e51c60424eb9125d6642f50284a2b04a
601ff3e0ec0a2037f5e119a4d8b068e99512aef63374daba45350cdbc7c2b2a1	612aabbcb72685cfe1ce2af351f95bda6840c6b6c303328900b748066f4717cc
6154405c5dc97fc6bc9db44661f6923529688ccac96b2851645aed8528658dd2	61699227582ab5ed3d99b5bb24fb653084c6701629bf9bdbccce116969bed182
616b29246552573a424166a79823bb99f55b195be363d6d7003f26f26f81c389	6182431e8567d174c8020a6f28de7ef7888b309ac7c95f2ac38d6911a33970b5
6234d00256f43c39bb30b1b9faa236aa0a0fde0629397ebd5d1c6830103e1ad7	6247f283d916b1cf0c284f4c31ef659096536fe05b8b9d668edab1e1b9068762
624f751deaa1cf08ec586557bf0ab7ad60b9a7c9cb414b478b09c9aabcfe97a1	625ba2e8988a996ef843e66481f1cd381ac413f8e1a7dab8b1f9ee31432446e7
62acb6f37e4eefe9096d4decdd83b16c024f1f791ae88977d77c5f1bd0a5ea45	62c372ada766d7f49e3bdf3389348712a3dceda4069c8a95ff6df20d936322f7
62e1dd66052f5cf5c362cc0979ff18bb11a24566ef66663f954ba88d789721ae	62f7d91100920eeca8a240776e0e62e3de22d11963491a9160b3f798f6c569d
6341f19450cfd5830fa71dcd8739f1cfa36b5b4712f5bfa937aed92eb5f10af3	635959d247bd2b616237805302b5156079f082edf3d3d3ac3582d0568f97341d
6370ea3f82d274ffcc1937ecd421418bd512913bdfecca083efebd126a369f6	638db45fe0172ad4d260b02edde4517b7bbdbb587235d32a8f4f7e9fdd54f4d9
6401f8eb56a6e5319a35d741afd06064d7d1dc0fa1de14c0d3535143cca81c03	6433c5e49905216fe33d5e9fc633069e44708ac6797054f85188f9a9f8b15358
64495b3aeeee0ec9136e2329b07ec988996f2df366b6b2f0c3c74754d7d2d486	64630939b939b964ee8a603360b02fe54d02d8dd2e3809f0193f279b3b8ccfb2
651623541fd9ee3ce400aa0881c215f3798c5741f222e18679baeb6da8e69eb7	652ee1a2587e3ed937a885245032e04201f4b3a104f5c1607aee5588c4fabcb3
65b9d8a9886b3e0fccc492209eb345f37bc6258eb84fc66001bf328691a34c89	664e65f58fb8b110ef5564af4f059c1526715f2e902feec90313310c455ffd5d
6651aa86da06753d616db714bba0c92d5dcffe4cedafc722df4fe383c6f9d615	6654d431d74b68523ef97acab92059ba09473c9e07d3e6d6cf4579562ad21877
66643bd66df2390e170132f2d915821f4022a9a69f9b50c8dd11236e213062a9	66cf3687425ccaab9b8387a594d558b5e2f83d03d913c99ae81c86bdb3c4eb21
67169cd76c8d4224c5b4279b243d3a023655e60f8dcf2bad0cd454ae615b67f5	671f9f804856cf9fe225ff05966d8288a92f829d1e25dd6e3977564f0a974ef3
67346dd2a97ee744e4b969840f205402a9aa7a1e0dc211eb9e42be4b55e7744b	6749adaa000433a56955faf6b096cf9f5a8b2484286c3ea22fd61252aaef1998
67988e834be64ed307670ecc3f4d61f34e700860c842f236bda5d3224d9bf643	67b5f2fb0320196d1d646a679cb489c901bca6526ee5692f6cd3d5d387afb956
67e90753dbd59ac0d8ca19b210bc90d84df68df54c48984d72e9dbdc99dc8a1e	67eff154c6269df76601edd9b849015904bb417aec3522e392744fab23b709c2
6836a300059972b62ef5a8aeb4c72c9a577409a2e6e414779930cf76986c1356	687b66a5cdcb02564155e1aaef60fd44da9b42e659f97ab037675c7267c8d142
68872cc22fbdf0c2f69c32ac878ba9a7b7cf61fe5dd0e3da200131b8b23438e7	68df8c70b8cd62098c88877ae39b72b355d6e5e26c8c73704ecd0a4d8465a970
68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccc2bc0d8	6900f64ee0544502a5214526a1565e9424cf47177640db004e282dceba126855
690d8ff83716986653f22539e0b5a1fc9cf9b6eeff0f6d3131eff6265a888617	6943bc818f6b9e2e86cde492d090cf45e2874ac3d2f9a35f314e9e381fc7d1dc
695247684c88a6ffff0ec6c567841f49c6e5d3725062aa5704044c405e82c337	6966e7294a5883b7879d8cffd2076baae4b3270f381a9995dec9aa7632d6d34
6a3e68b023acbb3e95ad6912daede8119111219a6d3a08036003bf5e198311ef	6a4902019df0fd2f246548bfae5473eb965c12371294394fabef291d647e4544
6aadcb9c5ed22bd8e24d7d49ee768c9bbfba9e8b3b8c6e222b2582b4b566d2c	6c53c18d22e0dff92493f48d297ff655bf5b942ccaacdf3720b7da23dabfe5c
6c6221b5770e11d0576b4b2c09bf54013b344de28b05d1edf22e377040dfbef9	6c6653ae2ebd362e9d61916aa31a12166a943b514ecd5493c163dc93bbb91603
6c6a30ed95f62fc2a9f20b399ff33439e9a6866535af16bd3538c21ab478a2fb	6d36da1517a22b8cf3e0fffa8a97dd6c78dd249cb00ca494753813a98383f5da

6d570005503121205ee2d2bd962c3a1081fa719d313e5d5bf5327508bbeec40d	6e05345ff2c04cd8bf045ba30c2e64f168dc2b9c94863f9f884500e7487c5d22
6e9c9b72d1bdb993184c7aa05d961e706a57b3becf151ca4f883a80a07fdd955	6edbe66b81f7168fa9d4b087c28409d6dfc98d560760369da4ed4ca2262abd33
6f20d88b0fca845de6f031af4f5ddc13e35eee5456987465631dcd0429b6a0cc	6ff970f1502347acd2d00e7746e40fba48995abbe26271d13102753c55694078
704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f945c85f4320	70cf0314cd62c34c463fea3f5d4ff509887fc1a8e6075ae9e28e7055e64cd972
70f8b5f670cd9a3e4c04c0ca81a64d780b7173adef497dcd31a27b40b7fc796	7129f8932aa90f1e8b3b88805d9aba446fec716d264dbae9ce66844346985e29
713b4f8bed05eacc11436ea5d279e9d65ab51ce594dcfb85cf291283a816c9e1	7198b9b8ee09944d3c4aeb4dff2e7c2430c045db128f3d55dff9f2a2e5462788
71a7c326ae125db5b637a28f12c9979911983b5251a825135ca7ac96cfe9f98a	71aa336353d147a6ce268c0f687b75e882c2def18f76e38bf885874ff632b3bc
71cdbf2a808a454a06dea146d25781c27ae095ea99d7b1680143a8594df40a92	71e3fce98a6436cf6a771732e9556106a071d86236f752d4540f669bef058f9c
72005393754e624b85c5124a2ccc3cfcf9064dd91793ab80de3e735b7de38e9b	7261c59aea05d1c1e6c37ebcd79e1c58ad361a08fd602405ab055596bcb700de
7278c810ca56dc9b3170ba206fe7bec4baa5006b1769ac95698e758c5a0a991e	72b84c97d8c0f5e23847609f0b55d000c0ad42d04b0cf9e7bc325ed2bfa111a
72f890e5ada836bbf7eb51fb3d9804a33dd066fc4bfc6af69d1c2eef2f2a809	732b48669b7b394a74938ac3468809c4dddc3e76ae54e196e3e55d54df84a6e2
734341e9ef7cb666a184261f0debe9946be330ee2b4ca9b6d1663020ea0192bd	735ba06531859c76c5d656fd40bd7aa691598bd62f20b26bed29d1c79fb134a9
738c30fe1fd86b2cdcae10bb847be8d5e3ff5fa504f6513e517b65f4261c28e34	73c6e9c64f6cbcc197631c109c2e41e0de3827096a7435bff7a0f1939e547673
742c30cb2e9da1c31ba72d8594912412e7ee2f391a45fe4a33e2a9d41a3ddb6c	7439135129b3d44c311a183f5c5886e976b8710ee58bdf7a864262aa284726e
7465fb96a930489b1720be2333e661029fee6f1081147528e9b11998268d1cc4	749f27547a34bd062fd4dbec7e530a6226de1c6272fafd478dab074d55600bb94
74bd61a9400bb6ab8debaea2d3f3227541d99145c8da4d2dee3f5ad1fffd16bc	74c1104e12627e6f11c97a23f2b70974d5778fc5700c2f6e0f5226b1636db8e4
74dbe14c91f78d3558e4fa99fc964e0aaa64653997a631a12f3b0a50e6e4b9a	7638a51b6d1ef1f84a3c184cbfb33b2d3a90ee269fdb580f423cc3201d5d9a0
768d3ffd942d8aea0f5def0c113d1a4e86bf9f78732b49c4222fa94bae3cf71	76f635861c3ed485327063f1e8b34f045b4e45c589c0f1c74501bc512e04c648
76fab1fb6fafa786432c7a0cee1234990f83401b5740f01260cc46cb1d0b8312	7705bd4b90d0fae9fdb4a44ebb50cc848716bff6cccb59ff636cd5264333873
77127c45c1b0fb1937184403d1a440c8edba90ba7c07116129cf4f81030843e9	773218009d83c2da08986fb456ea8ab233fbc04a7de491666f1d264c4b3ccd7f
774d10e680e922fcac0a846f41b0aef156b0566694ba54a7c763cbf01ed4b5e9	779ba0b54aaddc6bc6d11232684f5a364cfac47dba957d92fef15dec15d214a
77abbf73fb981dc9005d5acd01ebee1af5447117728a07c801fb4613cd0e492e	77b06dac5918b7e3a16a47bdad2ac28661dd3aac255f496407cfe59959a8c889
77c69e116d6faa6d15b63aaafa6567eff09b61e9af29f39401aab7f555a6eab	7856b234ee6d3de00ce42d0c8b743185ea157a19a423ce20c54ccea06353c7dd
7871e7e4dbb6bf1b7cc238d46da929d6e268cb8edbf774a9e64a08c5f52b16b	788a40438bb841134198f014bd81c88dbf992ba52298b03b20caccf39585ef5c
79260520787e2ccd0304f289c880d73ddcde2db9cf1f355ca5a1be4d5f66f401	792918078d885cfbd5efc48e908ce6c629deb5cca942dfa76f92a2a2e6a1b421
792e0504865aad5db81a49b0083e7282657d16ae0dee63309af5e9790f0ea48	7934cdb1ab66ecb9c4353eaf56856bff4d5bbc54da5f89160b71d4dee4ee798b
793e9b14ca4f3484fe5035738676359d44d4bc44ef098cbe42e310e15f06c2c2	794167f8a60fd33fccd48ac4e2b74d1f57fe9e7dced542e5e531614ea893a8e1
79a4c04639a0a9983467370b38de262641da79ccd51a0cdcd53aba20158f1b3a	79ae77b4c1b2f944355d87bd2396d671dd6783f3b238c66064de4a7b8ef57b6b
79eaea7f4ba37ec676489f24e3f9f45c164d5ae463e532f41aa55134adb24469	79eea747ac7672aa293d09038498c9b2a43f6f1a24adeff166dad71cf7cc8efa
7a138c5528e4671a0cc3295d8ba510aa0cfc01996d1d5ad445cbe58a505e185f	7a4f6796357a1415c382a611f2c863558a15308f84b983ba7ee302211ff570e9
7aca6898549dbb4fc53dca770c99ae9bc2ff4042721295adfa947038e8e3b887	7adbe411926ffed9deb6c7a7f85ffd579452613bd5729694601fba88bbda10a0
7b231588e91bb88b46e3bf94e975fb8a4f121fcfcaa124519d9bb9922706308c	7c73f64214983a95f2cd9b2f2b494862758f23ad2043aea03d8ff09934f0a0da
7c95313c1b19ad464ba9759d1bdc794da23f3c2209a27a1014bcde5a282f99f	7c99afcc3d415f52a613084c9990854e0e8103fdd755e8d6cb9cd6d91794e19d
7cbda3ff0347c933c2d9f5ed93a946c20ddb38eaac57a2a8b8cfd127bffbbe5c	7cc43f029259c53df8248af61b97983ab93c4de126a793deecc98365857ef0e8
7d50e2e9363228c42379f9c75639401b5c2c0fbe63b15d9165b390cef4cd8a03	7d9c97a133997396b0625a5d2b762fb8b33f5152d4dd893c7a463cc41372ab5
7da69e9d728567cde830124dcb3ac6fd8e3d4ace146ab97069bb0854ca093132	7dbb87519d86cc06c86dd2a0cc7c6e8d9c1ac61eec41d8d4567555075578015a
7e47e5283bfea7390f7409ba8c7df95795fb8d4cca511aaeb13781e0fb1fe31	7e8e386de3d41008e7de9e8221f05949262c0c000f1751bfded4c5284f89910c7
7eb090049922ff83d3dd5f2e3aad48975dfe31f46389d074aa1279c7147c7451	7eb2a629b5dbbe9e3ebb8e05af2f9bdd62f58d7e7f846572c759accfe3dc3bc0
7ef2f26e3432980b41e02e1adbfd5f61a3b735d1ddb1b065c3dabc23cc6a4232	7ef6352f29723ff4f3702fd5e6d041695ccda89105d47b6aff5bf87521fe2345
7f270ed5ea5d8ee2802a0cb39609b87aa0b7b5050e4b44a58c2e6ac400ecc544	