RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-R01

Extracting Secrets from Locked Password Managers

Adrian Bednarek

Senior Security Analyst
Independent Security Evaluators (ISE)
@ISEsecurity

Agenda

- What is a password manager?
- Common terminology
- Security guarantees
- Threats
- Look at 1Password, LastPass, Dashlane, KeePass

Background

- Reverse Engineering
  - Software
  - Communications protocols
  - Obfuscated code
    - Challenging but higher likelihood of finding vulnerabilities
- Online Game Exploitation
  - Exploiting virtual economies


The Lord of the Rings Online


WILDSTAR


DarkFall
Unholy Wars


Ultima Online


Anarchy online


Asheron's Call 2
Fallen Kings


Dark Age of Camelot


RIFT


Age of Conan


FINAL FANTASY XIV
ONLINE


STAR WARS
THE


OLD REPUBLIC


SHADOWBANE


The Elder Scrolls
ONLINE


LINEAGE


WORLD OF WARCRAFT


Age of Wushu


FINAL FANTASY XI
ONLINE

Password Manager Research Timeline

August 2018

RESEARCH BEGINS

October 2018

WHITEPAPER DRAFT

December 2018

PUBLISH? 

More harm than good?
~60m Users

February 2019

BUGCROWD BAN

February 2019

PUBLISHED IN MEDIA

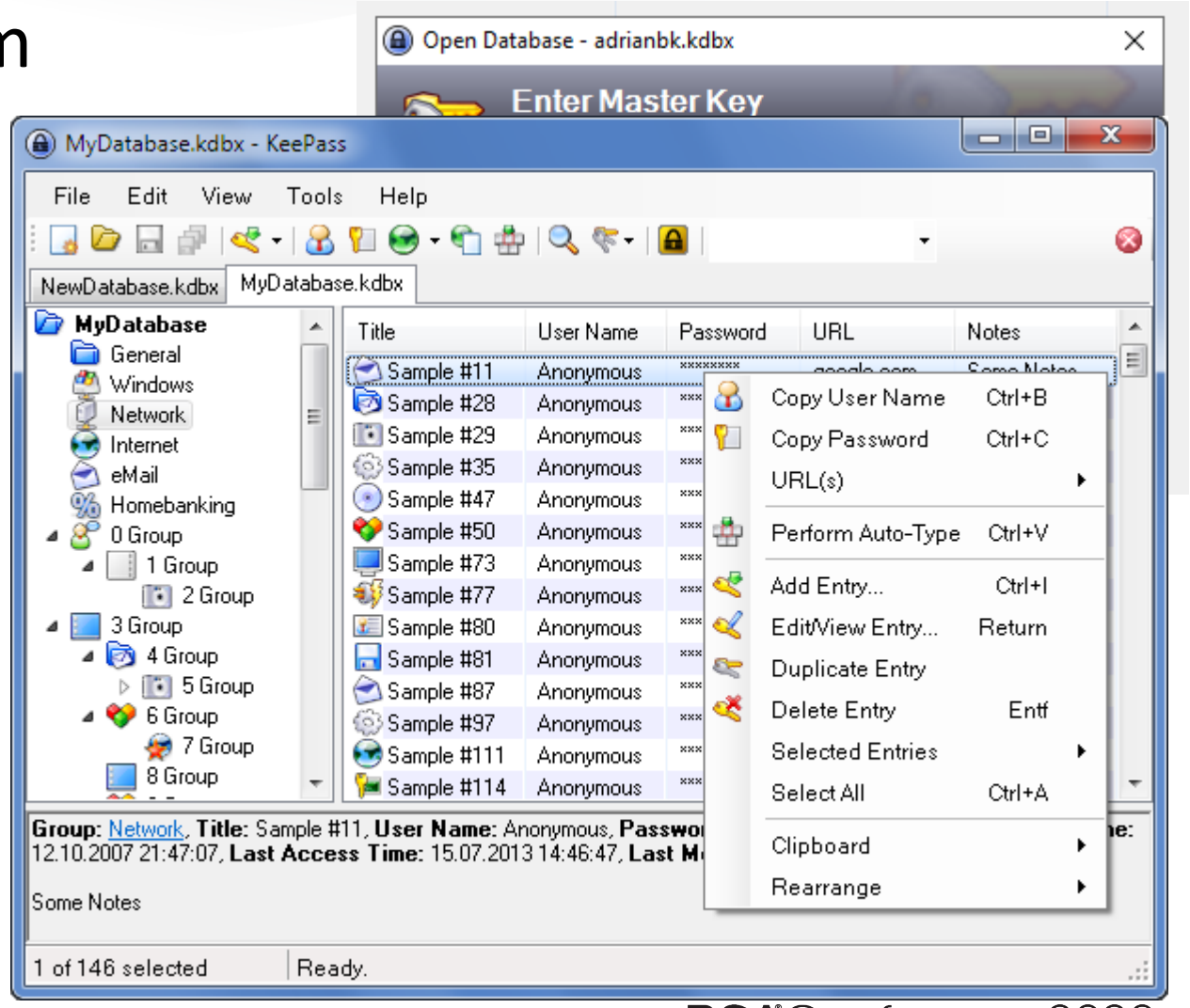
Washington Post
20+ outlets

RSAConference2020

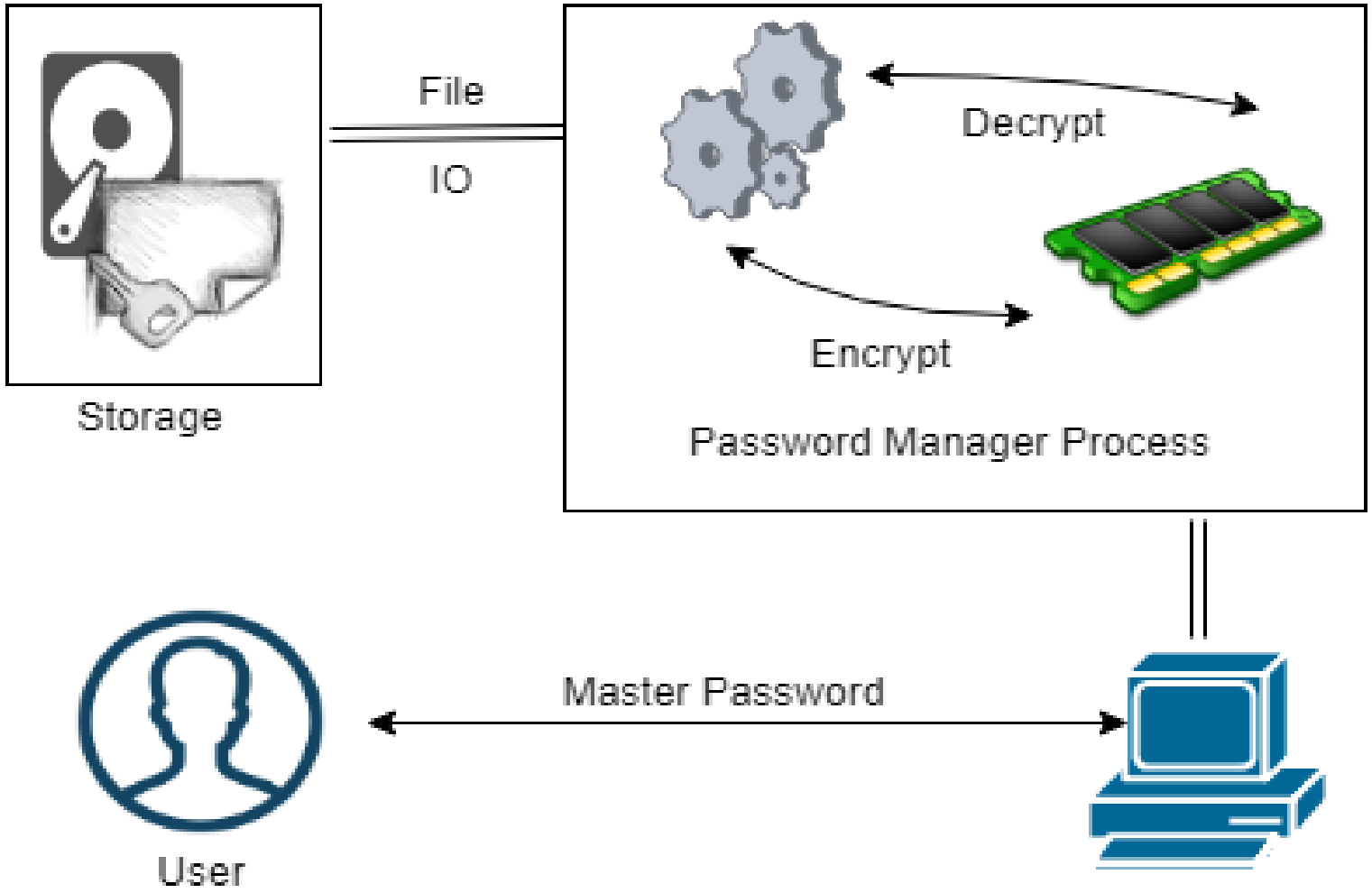
What is a password manager?

Anatomy of a Password Manager

- Credential management system
  - ~60m users
- Typical workflow
  - Enter a master password
  - Unlock access to all credentials
  - Lock password manager



Workflow Overview



RSAConference2020

Terminology

Password Manager Terminology

- Master password
  - A memorized secret that will grant access to all entries stored in a password manager
- Unlocked
  - The password manager has been unlocked by entering the master password and entries are viewable
- Locked
  - The password manager has been locked or ‘logged out’ from

Password Manager States

- Not Running
  - Password manager is not a running process. There should be no trace of the master password or entries on disk or in RAM
- Running: Unlocked State
  - Password manager has been unlocked by entering the correct master password
- Running: Locked State
  - The password manager is an active process
  - Entries are not viewable since it has been locked or ‘logged out’ from

RSAConference2020

Password Manager Security Guarantees

“Not Running” State Security Guarantees

- No secrets stored on disk that would reveal the master password or entries
- Credential database should be non-trivially encrypted
  - An attacker should not be able to find a flaw/break the encryption
- Credential database should not be brute forceable
  - Master password to decryption key workflow should be computationally intensive
  - Attacker should not be able to guess the master password at a rate of 1 million attempts per second for example

“Running:Unlocked” State Security Guarantees

- It should not be possible to extract the master password from memory
- Entries that have not been viewed should remain to be encrypted
  - E.g. If 1000 entries are present only the ones viewed or operated on should be present in memory
- It may be possible to extract cryptographic keys derived from the master password

“Running:Locked” State Security Guarantees

- All security guarantees of a “not running” should apply to a password manager that is in a locked state.
  - No master password extraction possible
  - No cryptographic key extraction possible
  - No entry extraction possible

Threat Scenarios

1: Running

2: Running: Locked* (pwm typically run in background)

3: Running: Unlocked

Attacks on “Not Running” Password Managers

- PBKDF2/Argon2 Password expansion
- All secrets are encrypted at rest

Password Manager	Key Expansion Algorithm	Iterations
1Password4	PBKDF2-SHA256	40,000 [15]
1Password7	PBKDF2-SHA256	100,000 [16]
Dashlane	Argon2	3 [17]
KeePass	AES-KDF	60,000 [18]
LastPass	PBKDF2-SHA256	100,100 [19]

Attacks on “Running:Locked” Password Managers

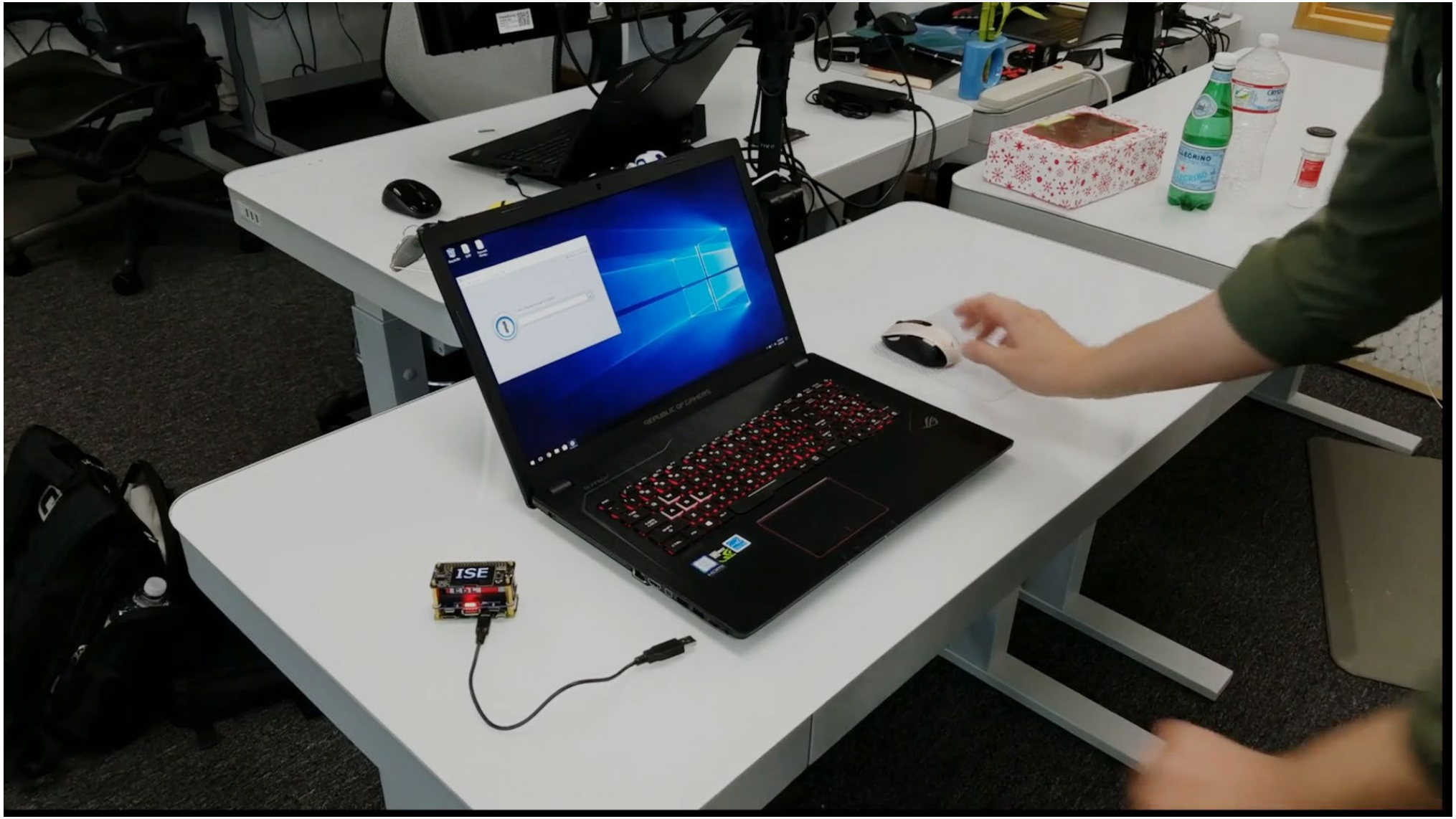
- Master password extraction ***should not*** be possible
- Cryptographic key extraction ***should not*** be possible
- Entry extraction ***should not*** be possible

Locked

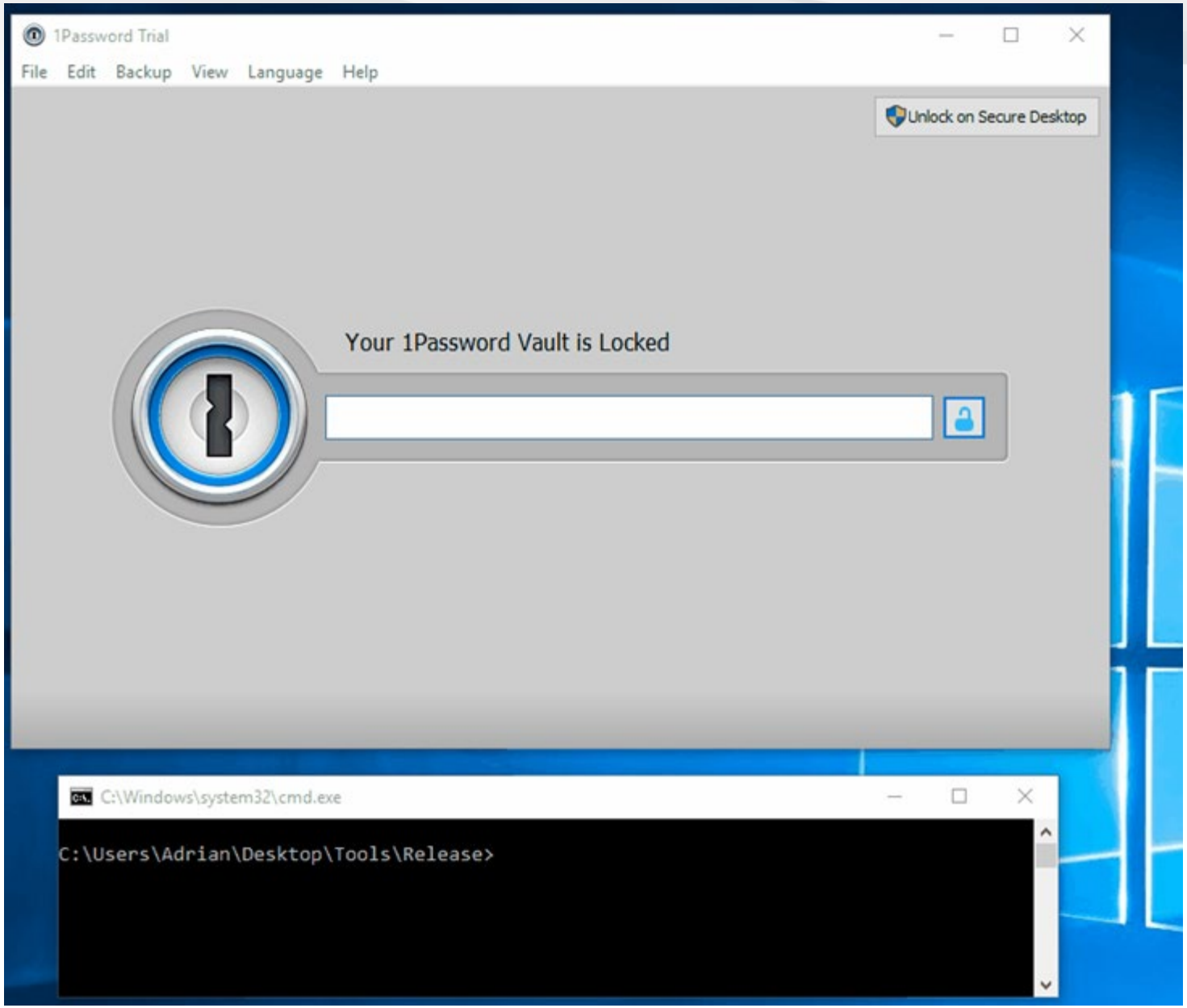
Unlocked

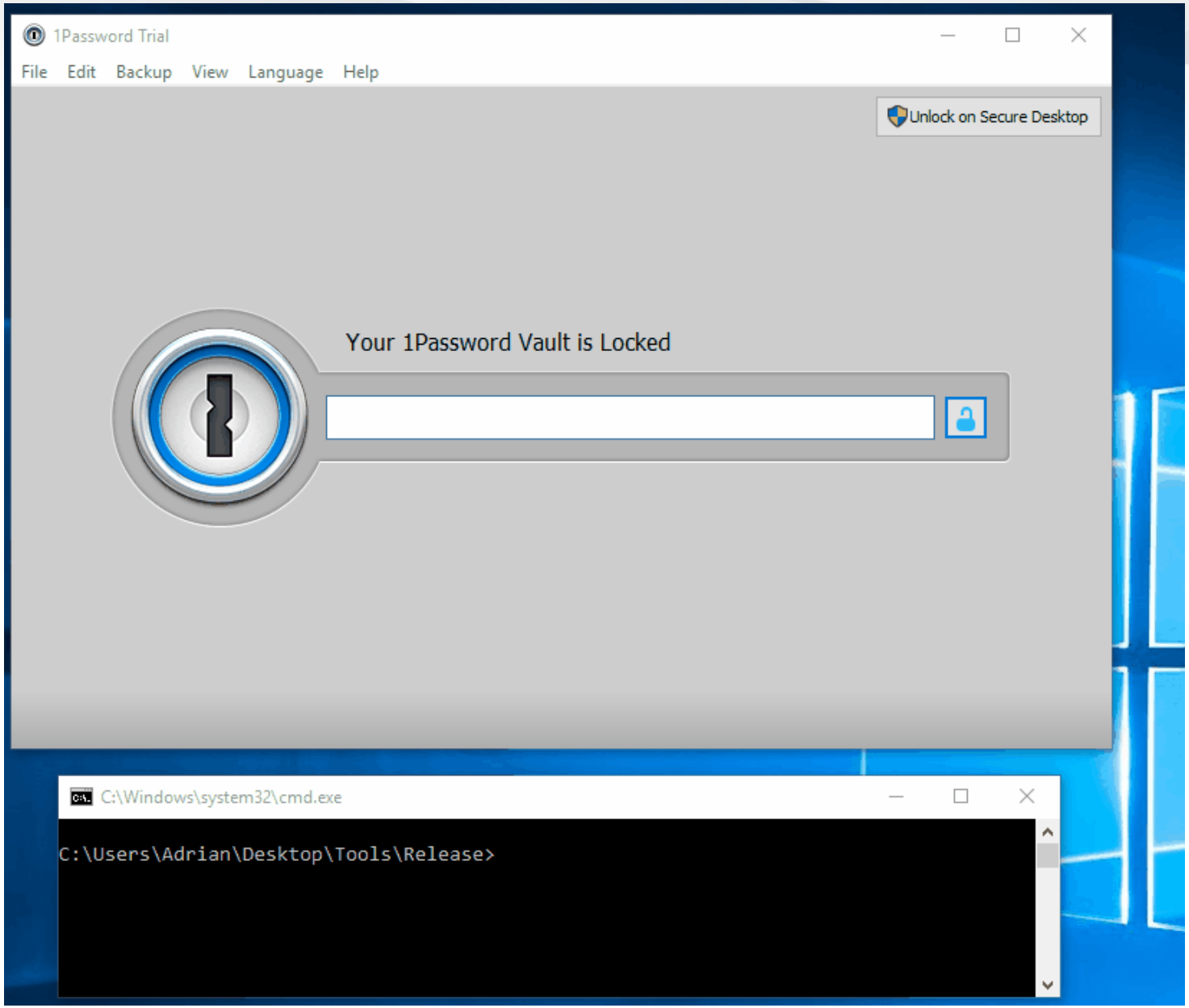
Running:Locked

Demo Attack – Running:Locked (1Password4)



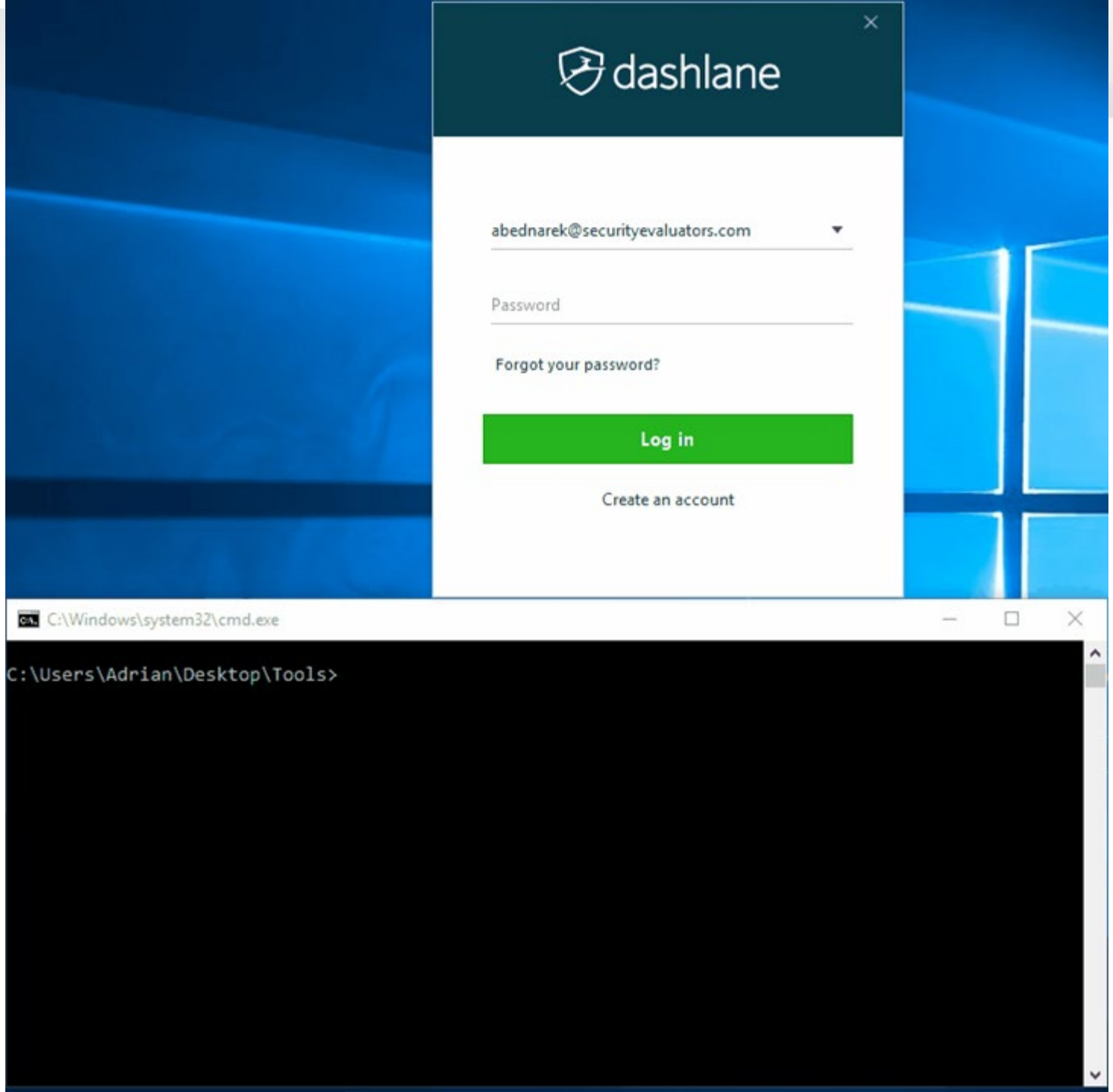
Again without cuts:

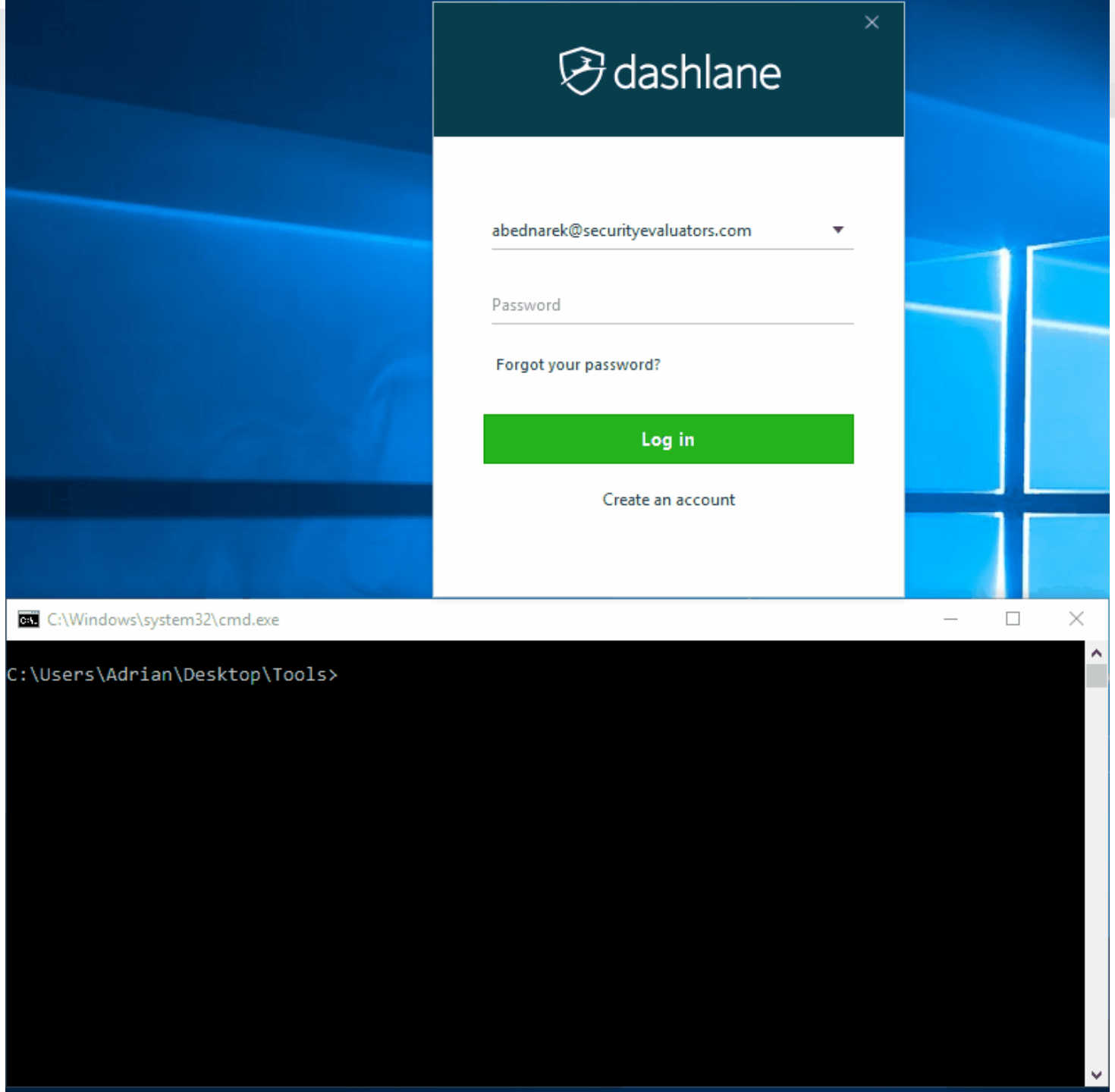

1Password Trial
File Edit Backup View Language Help
Unlock on Secure Desktop
Your 1Password Vault is Locked
C:\Windows\system32\cmd.exe
C:\Users\Adrian\Desktop\Tools\Release>


1Password Trial
File Edit Backup View Language Help
Unlock on Secure Desktop
Your 1Password Vault is Locked
C:\Windows\system32\cmd.exe
C:\Users\Adrian\Desktop\Tools\Release>

Running:Locked

- Dashlane
  - Master password is not recoverable
  - Entries are recoverable
- KeePass 2
  - Master password is not recoverable
  - Interacted with entries are recoverable
- LastPass
  - Master password persists in plaintext
  - Interacted with entries are recoverable
- 1Password 7
  - Master password persists in plaintext
  - Entries are recoverable


dashlane
abednarek@securityevaluators.com
Password
Forgot your password?
Log in
Create an account
C:\Windows\system32\cmd.exe
C:\Users\Adrian\Desktop\Tools>


dashlane
abednarek@securityevaluators.com
Password
Forgot your password?
Log in
Create an account
C:\Windows\system32\cmd.exe
C:\Users\Adrian\Desktop\Tools>

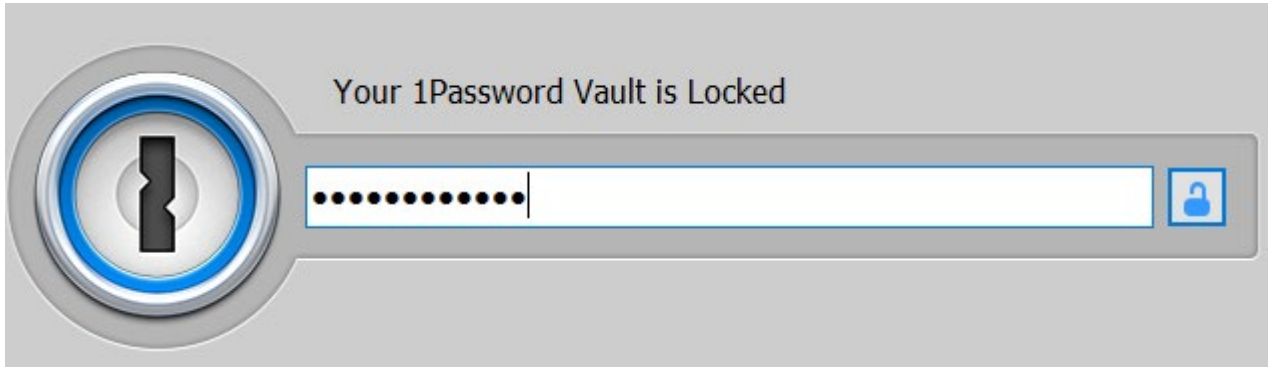
RSAConference2020

A Windows Bug Appears!

A side-quest led to an interesting 20+ (?) year old windows bug

Windows Bug Discovery

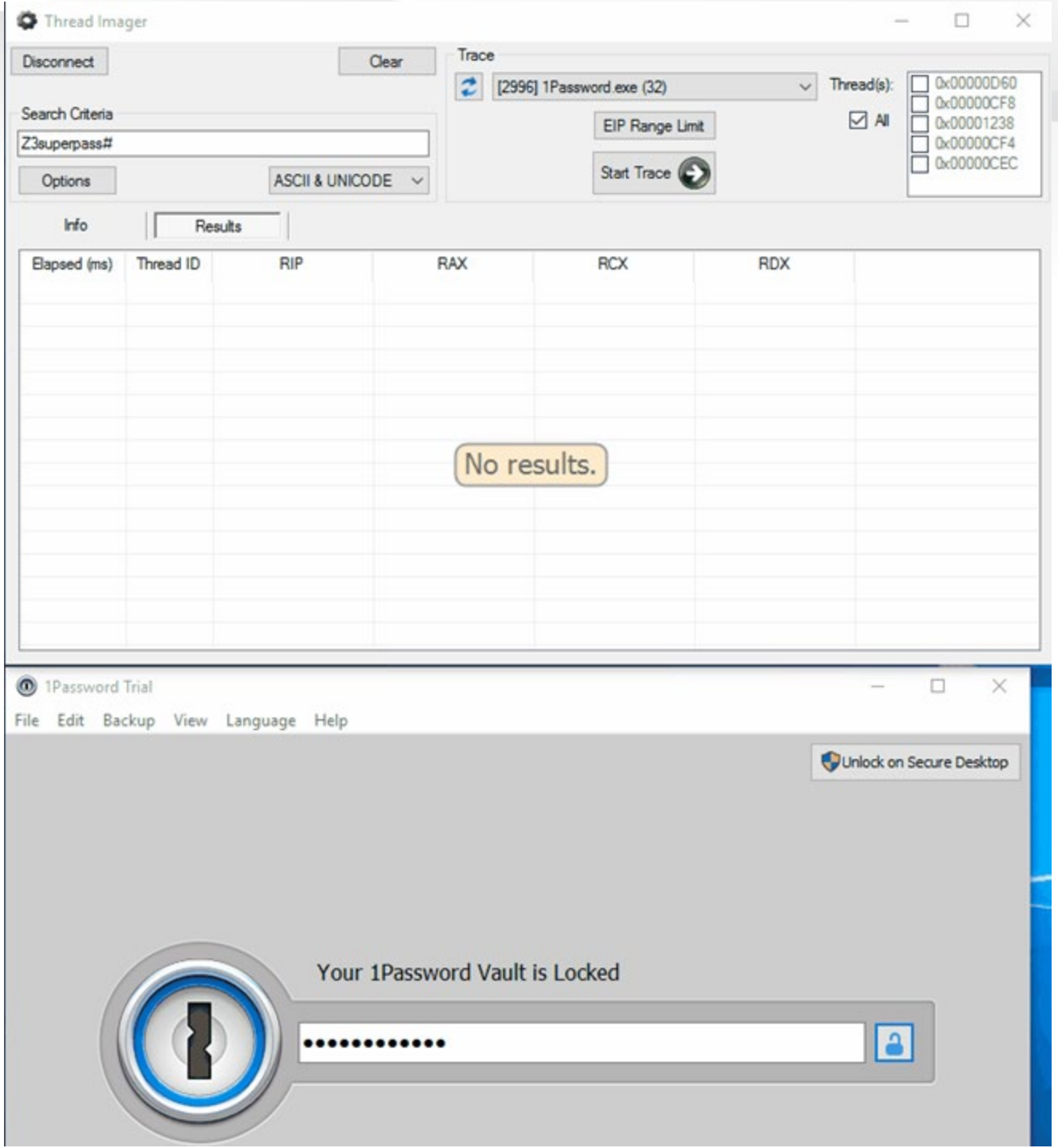
- Original Test
  - Locked password manager
  - Master password typed in:

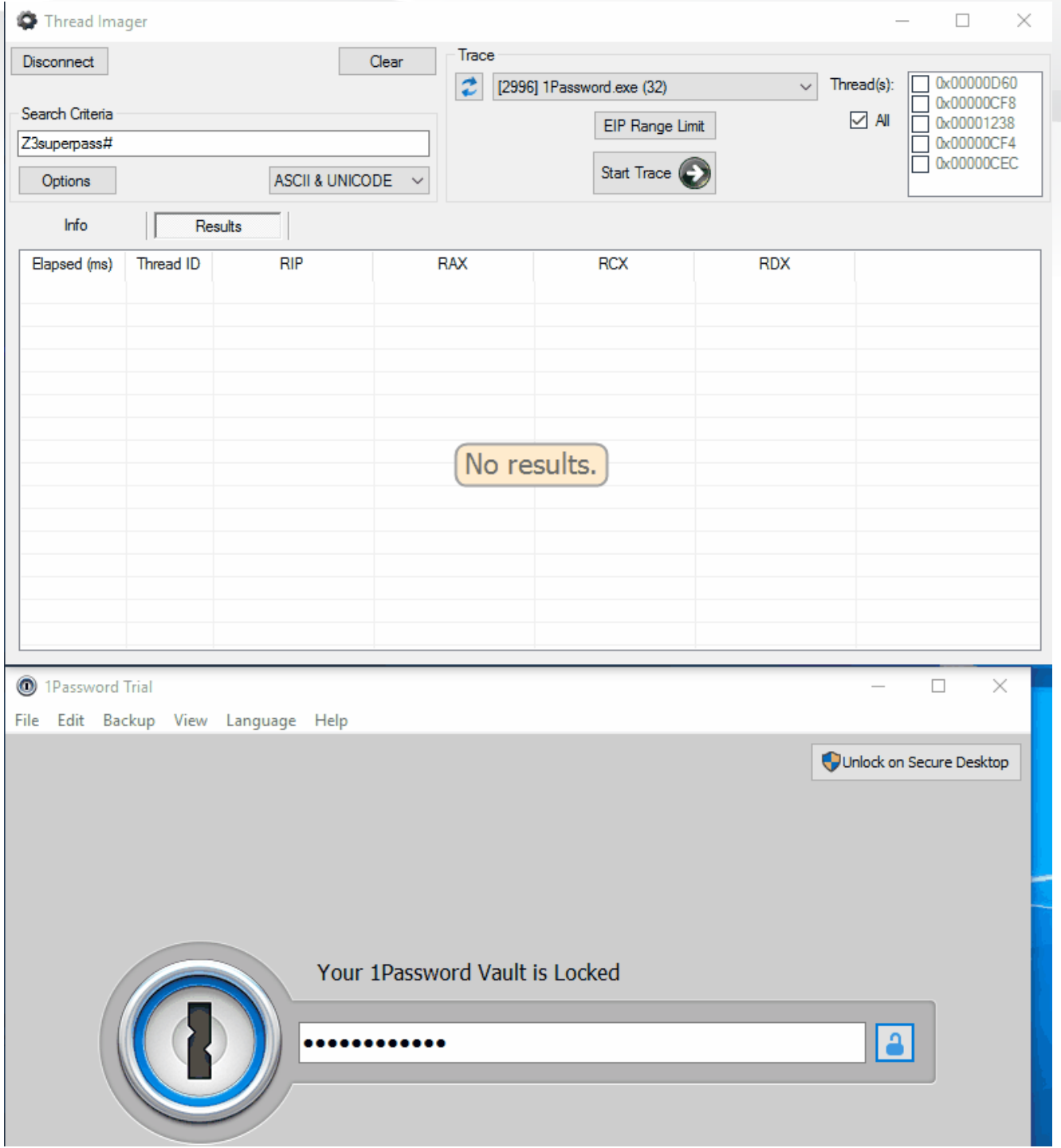


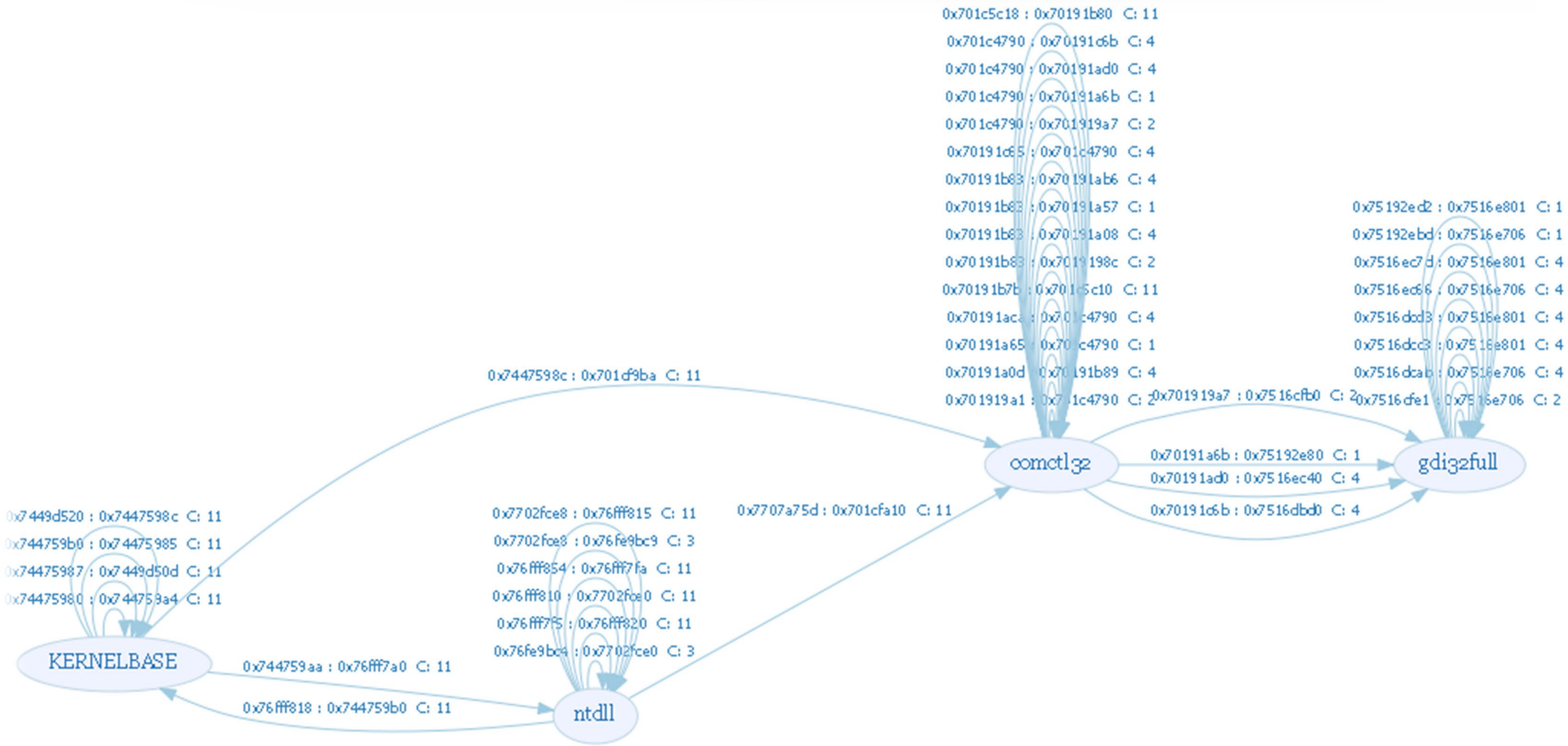
  - Where is the master password?
    - Doesn't exist in a readable state :

1Password.exe (8216)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000000000000	000000000000 – 00000000FFFF																
000000010000	00	00	00	00	00	00	00	00	B3	D3	B0	B2	10	CF	00	01	.....³Ó°².Ï..
000000010010	EE	FF	EE	FF	01	00	00	00	20	01	01	00	00	00	00	00	îÿîÿ.... .....
000000010020	20	01	01	00	00	00	00	00	00	00	01	00	00	00	00	00	.....
000000010030	00	00	01	00	00	00	00	00	10	00	00	00	00	00	00	00	.....
000000010040	20	07	01	00	00	00	00	00	00	00	02	00	00	00	00	00	.....
000000010050	0F	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	.....
000000010060	E0	0F	01	00	00	00	00	00	E0	0F	01	00	00	00	00	00	à.....à.....
000000010070	60	80	00	40	60	00	00	40	00	00	00	00	00	00	10	00	`.@`..@.....
000000010080	00	00	00	00	00	00	00	00	C1	D3	B1	C1	10	CF	00	00	.....ÁÓ±Á.Ï..


Thread Imager
Disconnect
Clear
Trace
[2996] 1Password.exe (32)
Thread(s):
0x00000D60
0x00000CF8
0x00001238
0x00000CF4
0x00000CEC
All
EIP Range Limit
Search Criteria
Z3superpass#
Start Trace
Options
ASCII & UNICODE
Info
Results
Elapsed (ms)
Thread ID
RIP
RAX
RCX
RDX
No results.
1Password Trial
File
Edit
Backup
View
Language
Help
Unlock on Secure Desktop
Your 1Password Vault is Locked


Thread Imager
Disconnect
Clear
Trace
[2996] 1Password.exe (32)
Thread(s):
0x00000D60
0x00000CF8
0x00001238
0x00000CF4
0x00000CEC
All
EIP Range Limit
Search Criteria
Z3superpass#
Start Trace
Options
ASCII & UNICODE
Info
Results
Elapsed (ms)
Thread ID
RIP
RAX
RCX
RDX
No results.
1Password Trial
File
Edit
Backup
View
Language
Help
Unlock on Secure Desktop
Your 1Password Vault is Locked

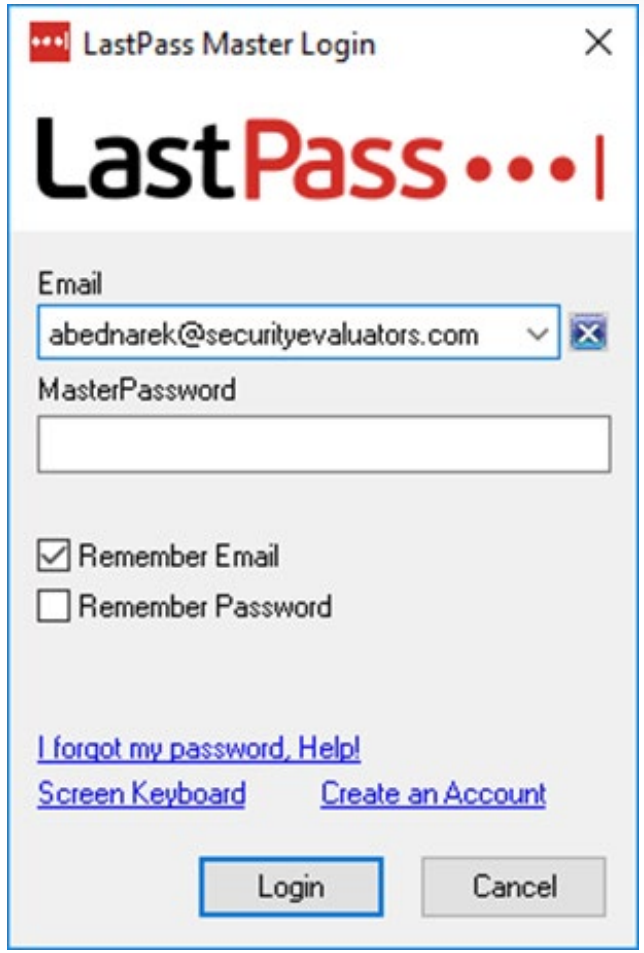

0x701c5c18 : 0x70191b80 C: 11
0x701c4790 : 0x70191c6b C: 4
0x701c4790 : 0x70191ad0 C: 4
0x701c4790 : 0x70191a6b C: 1
0x701c4790 : 0x701919a7 C: 2
0x70191c85 : 0x701c4790 C: 4
0x70191b83 : 0x70191ab6 C: 4
0x70191b83 : 0x70191a57 C: 1
0x70191b83 : 0x70191a08 C: 4
0x70191b83 : 0x7019198c C: 2
0x70191b7b : 0x701c5c10 C: 11
0x70191ac : 0x701c4790 C: 4
0x70191a65 : 0x701c4790 C: 1
0x70191a0d : 0x70191b89 C: 4
0x701919a1 : 0x701c4790 C: 2
0x75192ed2 : 0x7516e801 C: 1
0x75192ebd : 0x7516e706 C: 1
0x7516ec7d : 0x7516e801 C: 4
0x7516ec66 : 0x7516e706 C: 4
0x7516dcd3 : 0x7516e801 C: 4
0x7516dcc3 : 0x7516e801 C: 4
0x7516dcab : 0x7516e706 C: 4
0x7516cfe1 : 0x7516e706 C: 2
0x7447598c : 0x701cf9ba C: 11
0x701919a7 : 0x7516cfb0 C: 2
comctl32
0x70191a6b : 0x75192e80 C: 1
0x70191ad0 : 0x7516ec40 C: 4
0x70191c6b : 0x7516dbd0 C: 4
gdi32full
0x7449d520 : 0x7447598c C: 11
0x744759b0 : 0x74475985 C: 11
0x74475987 : 0x7449d50d C: 11
0x74475980 : 0x744759a4 C: 11
KERNELBASE
0x7702fce8 : 0x76fff815 C: 11
0x7702fce8 : 0x76fe9bc9 C: 3
0x76fff854 : 0x76fff7fa C: 11
0x76fff810 : 0x7702fce0 C: 11
0x76fff7f5 : 0x76fff820 C: 11
0x76fe9bc4 : 0x7702fce0 C: 3
0x7707a75d : 0x701cfa10 C: 11
0x744759aa : 0x76fff7a0 C: 11
0x76fff818 : 0x744759b0 C: 11
ntdll

RSAConference2020

The Bug!

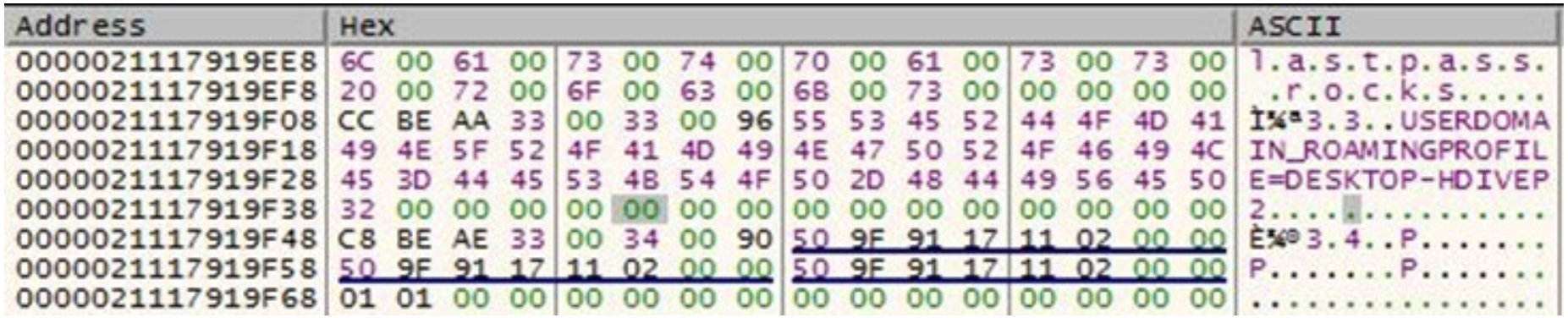
LastPass (Windows bug mitigation)

- Locked:



LastPass (Windows bug mitigation)

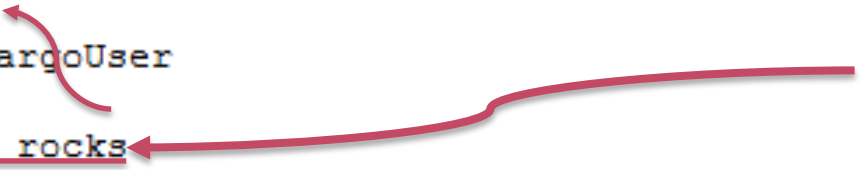
- Master Password?:



Address	Hex	ASCII
0000021117919EE8	6C 00 61 00 73 00 74 00 70 00 61 00 73 00 73 00	l.a.s.t.p.a.s.s.
0000021117919EF8	20 00 72 00 6F 00 63 00 6B 00 73 00 00 00 00 00	.r.o.c.k.s.....
0000021117919F08	CC BE AA 33 00 33 00 96 55 53 45 52 44 4F 4D 41	Ì¾ª3.3..USERDOMA
0000021117919F18	49 4E 5F 52 4F 41 4D 49 4E 47 50 52 4F 46 49 4C	IN_ROAMINGPROFIL
0000021117919F28	45 3D 44 45 53 4B 54 4F 50 2D 48 44 49 56 45 50	E=DESKTOP-HDIVEP
0000021117919F38	32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	2.....
0000021117919F48	C8 BE AE 33 00 34 00 90 50 9F 91 17 11 02 00 00	È¾®3.4..P.....
0000021117919F58	50 9F 91 17 11 02 00 00 50 9F 91 17 11 02 00 00	P.......P.....
0000021117919F68	01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Mitigation is helpful (for us)

```
xn--rht27z
FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
USERDOMAIN_ROAMINGPROFILE=DESKTOP-HDIVEP2
/9gb
astPass
rage]
xn--mkru45i
abcd123!
kawellsfargoUser
AHSM
lastpass_rocks
ected_storage]
ected_storage]
xn--nit225k
xn--ntsq17g
xn--pssu33l
```



Attacks on “Running:Unlocked” Password Managers

- Master password extraction ***should not*** be possible
- Cryptographic key extraction ***may*** be possible*
- Entry extraction ***should*** be possible for interacted entries

Attacks on “Running:Unlocked” Summary

- 1Password4
  - Master Password: Recoverable* (with difficulty)
  - Entries: Last interacted with entry
- 1Password7
  - Master Password: Recoverable
  - Entries: All are recoverable
- Dashlane
  - Master Password: Not recoverable
  - Entries: All are recoverable
- KeePass 2
  - Master Password: Not recoverable
  - Entries: Interacted with are recoverable

Attacks on “Running:Unlocked” Summary

- LastPass
  - Master Password: Recoverable
  - Entries: Recoverable

RSAConference2020

Summary

In a nutshell…

- Password managers are not perfect, but you should still use them!
- https://www.ise.io/casestudies/password-manager-hacking/

	KDF	Iterations	Unlocked State Secrets	Master Password	Locked State Secrets	Master Password	Keylogger	Clipboard sniffing
1Password 7	PBKDF2	100K	All Records	Present	All Records	YES	YES	YES
1Password 4	PBKDF2	40K	Last Active	Present	NO	YES	YES	YES
Dashlane	Argon2	3	All Records	Encrypted	All Records	NO	YES	YES
KeePass	AES-KDF	60k	Interacted	Scrubbed	Interacted	NO	YES	YES
LastPass	PBKDF2	5k	Interacted	Present	Interacted	YES	YES	YES

Apply What You Have Learned Today/Going Forward

- Things to keep in mind:
  - Consider the risk you are undertaking by using or not using a password manager
  - Think of various threat scenarios and understand the consequences (e.g. lost powered on laptop, laptop imaged in a running state at a border crossing for example)
- In the short run:
  - Develop contingencies for threat scenarios
  - Plan for mitigations around password managers that are not inline with your appetite for security
- In the long run:
  - Be on the lookout for emerging zero knowledge solutions
  - Understand and anticipate emerging threats against password managers!

RSAConference2020

Thank You!

https://www.ise.io/

https://www.linkedin.com/in/adrianbksd/