Cracking your AD P@sSw0rd$ is a GOOD THING!

Presented by Robert Reif

Grassr00tz 2022

Audit your passwords

Who am I?

Soc Analyst
Enthusiast Password Cracker
Avid Homelabber
General Tinker of things

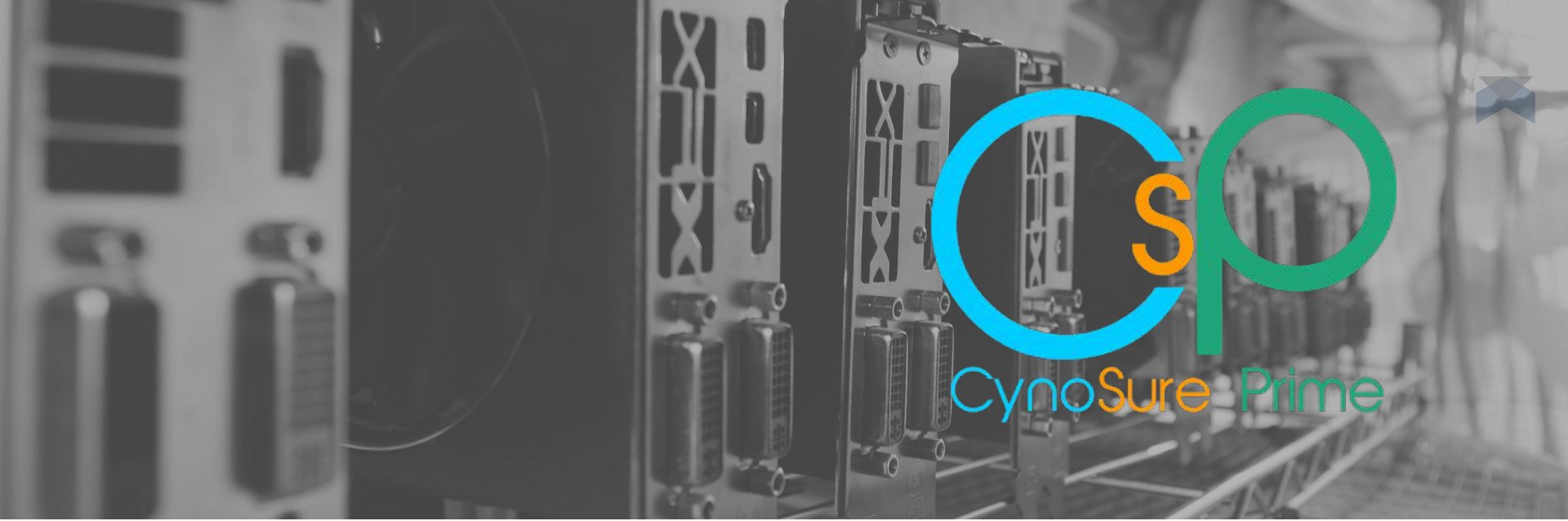
Twitter @winxp5421

<anything>@ProbablyNotAHacker.com

Keybase: keybase.io/winxp5421

Winxp5421

Audit your passwords



Password Research

We compete in all major hash cracking contests.

Release statistical analysis on data leaks that are made publicly available.

Twitter @cynoprime

cynosureprime.com

Audit your passwords

Overview

- Real world weekly password audit against a real world company!
  - With Pretty Graphs (Oooo, Ahhhh)
- Effectiveness of AD Policy changes
- Effectiveness of company policy changes
- Does policy change how people create passwords?
- End User Benefits how exactly?
- NIST to meet you…
  - NIST knowing you
- Audit your password environment.
  - No, really you should be doing this!

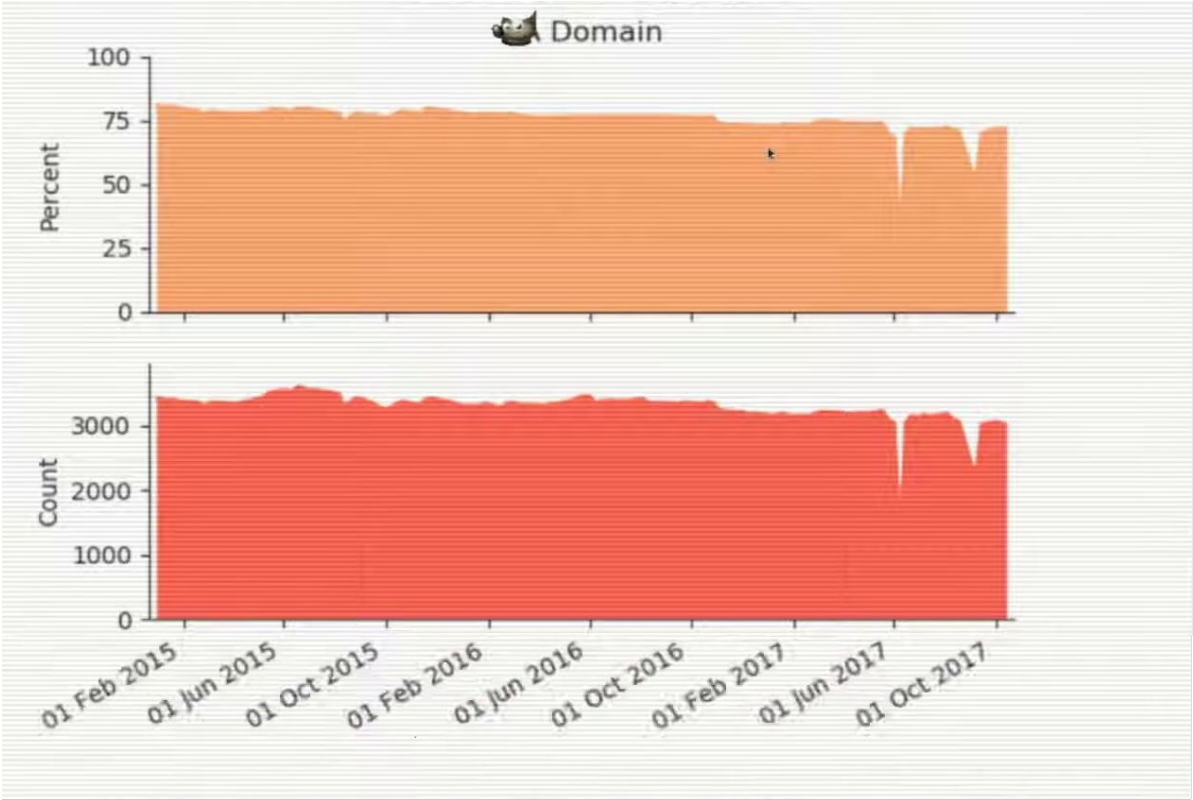
Audit your passwords

Password Audit?

- Dump NTDS.dit, SYSTEM, SECURITY Files from a Domain Controller
  - Yes, all the things! Plan your opsec accordingly
- Extract with DSInternals
  - First, Last, UPN, Privileged, Password hashes, Password history, Last Password Change
- Actually crack your AD User’s passwords!
- Quantify success and failure.
- Adapt and overcome.

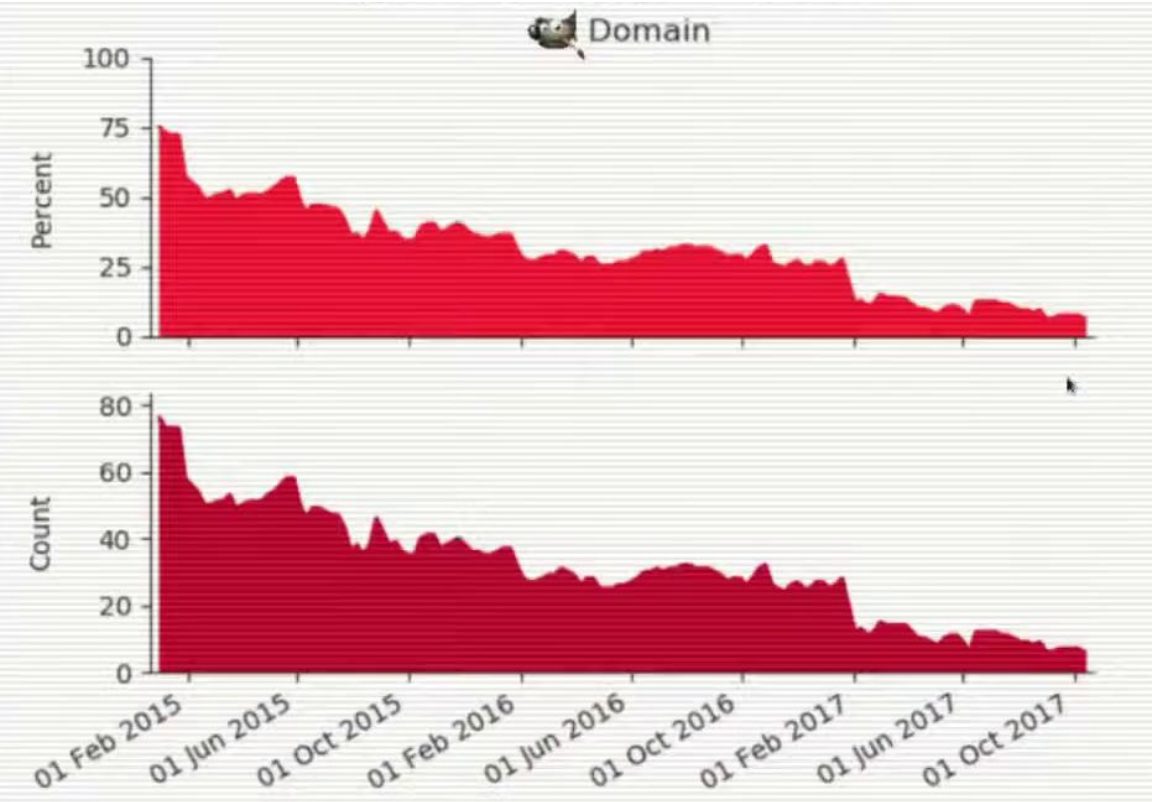
Let’s we have a look at what information we can gather from this!

Passwords Recovered Domain Wide



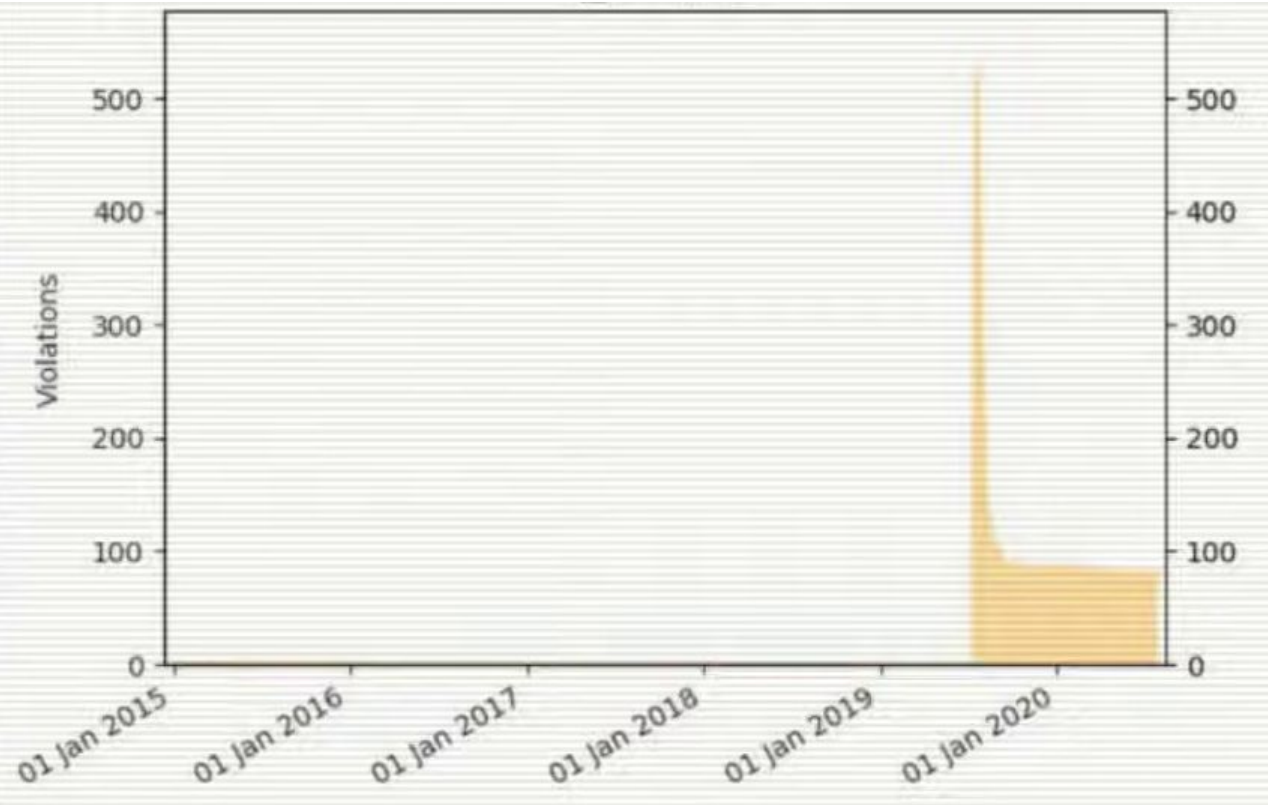
Audit your passwords

Recovered Admin Accounts



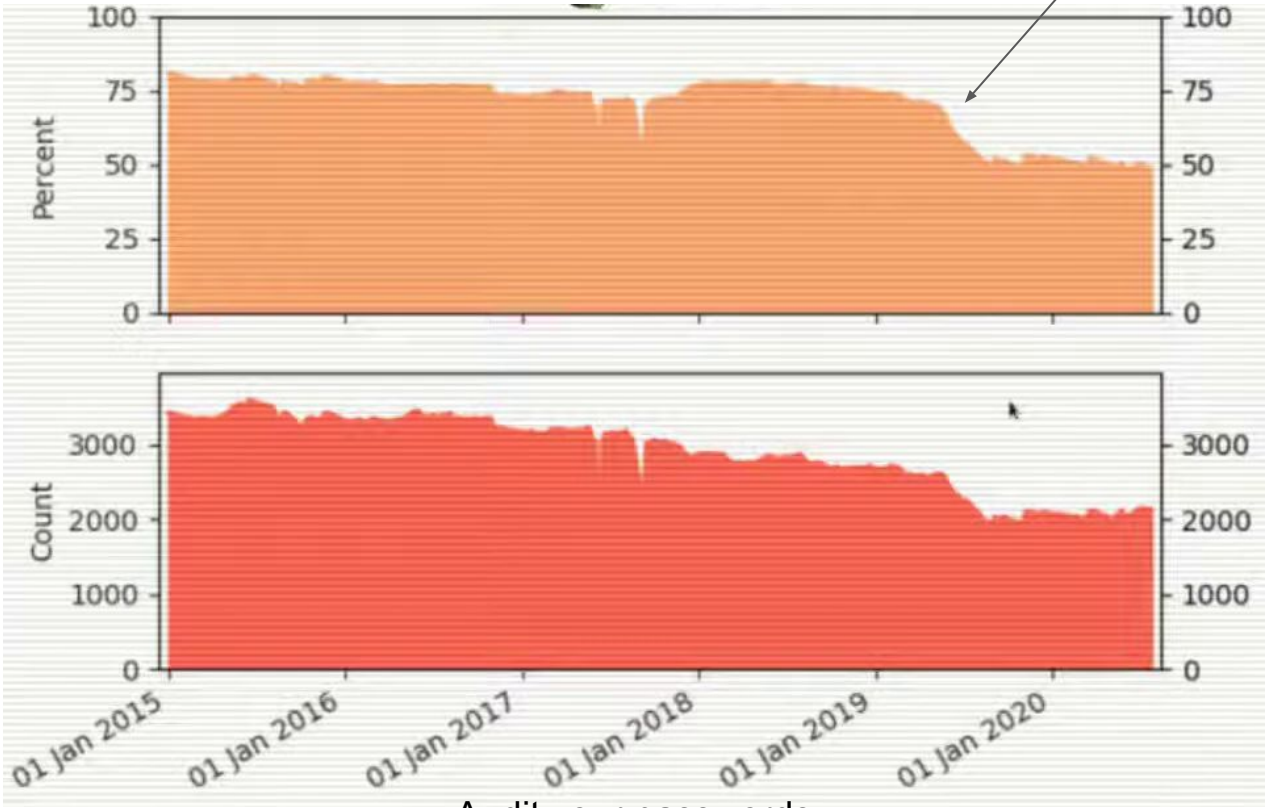
Audit your passwords

Policy Violations



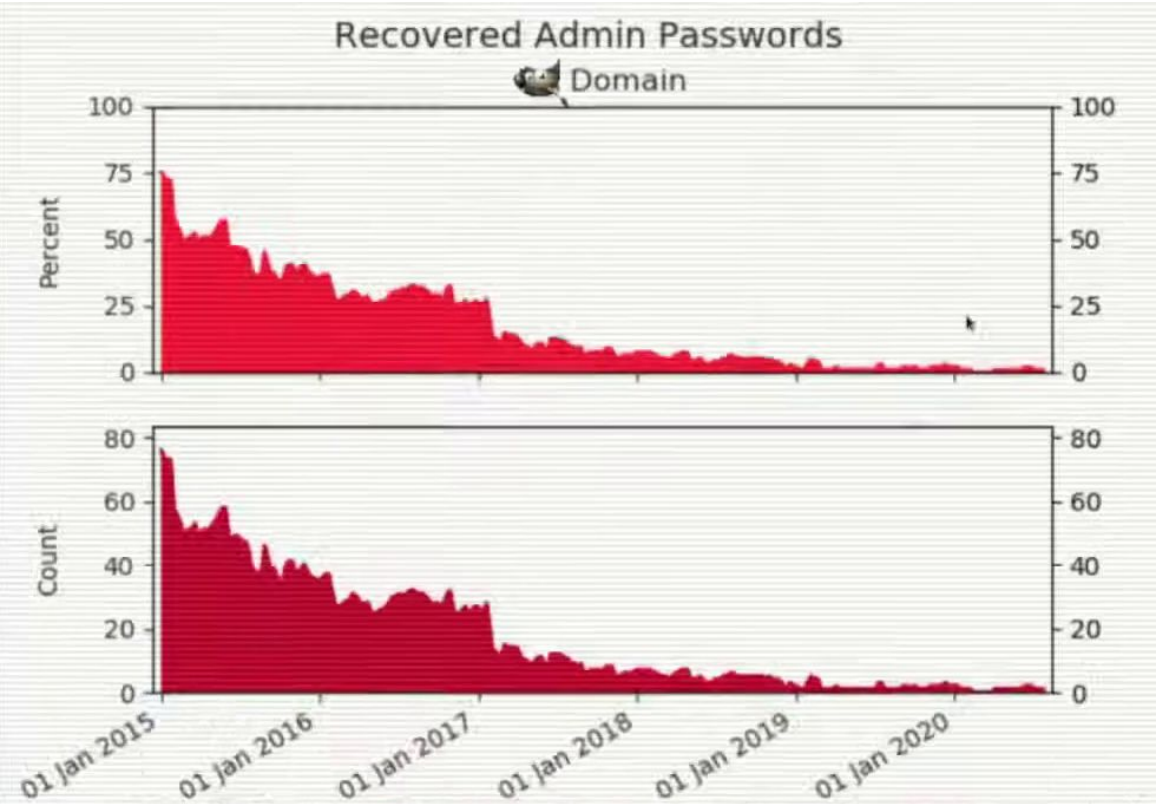
Audit your passwords

Passwords Recovered Domain Wide



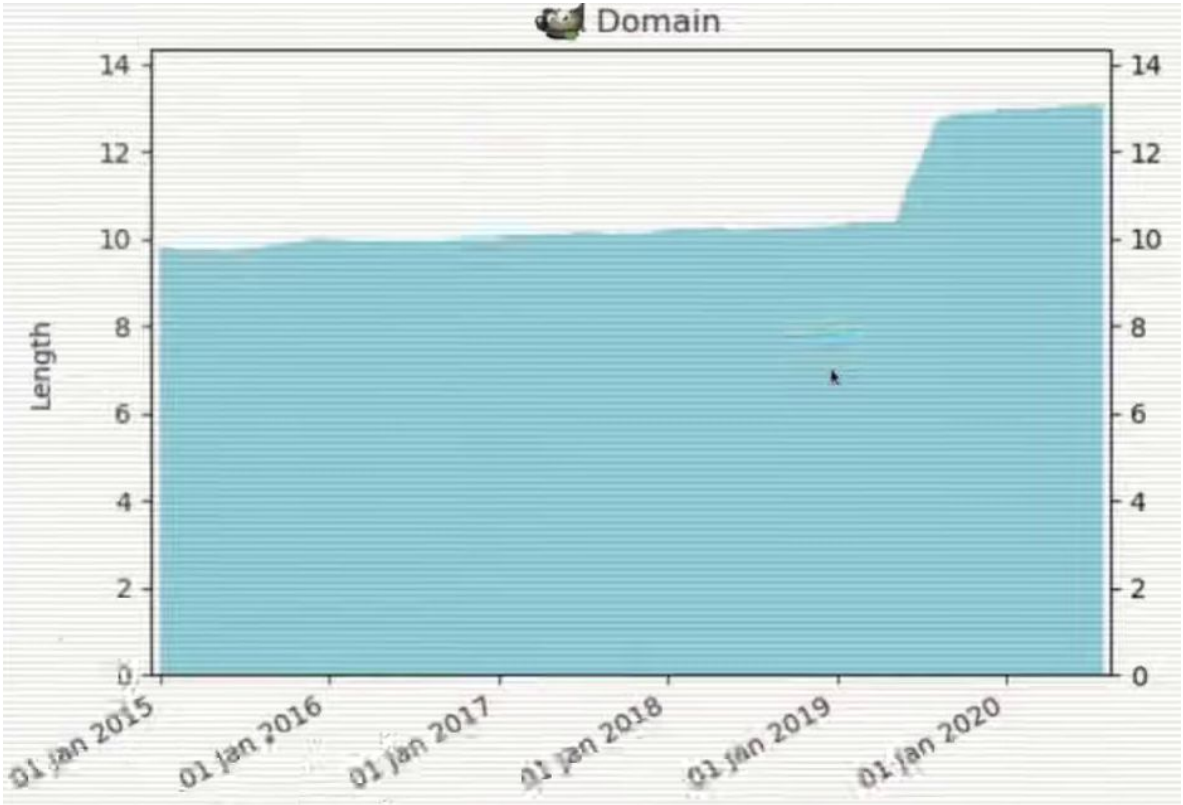
Audit your passwords

Recovered Admin Passwords



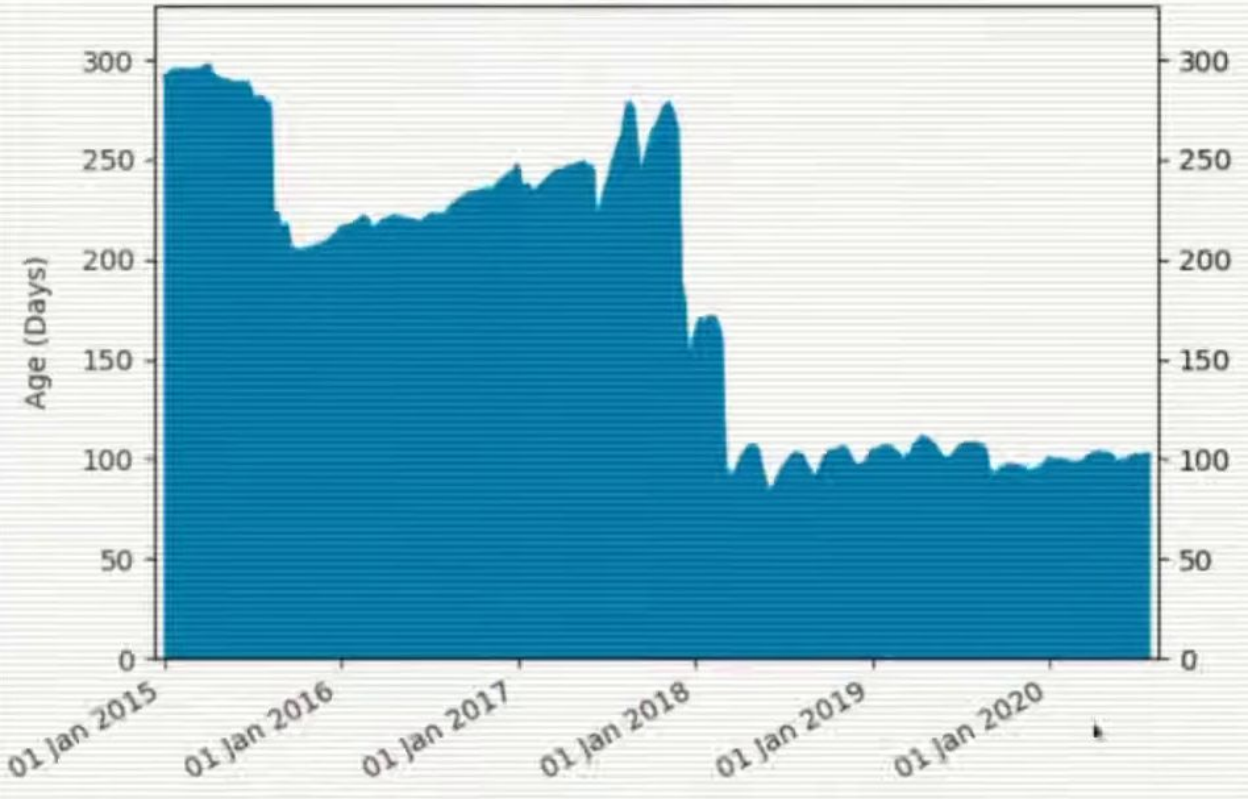
Audit your passwords

Average Password Length Over Time



Audit your passwords

Password Age Over Time



Audit your passwords

Pwd Patterns and Changes

From 2017: Most common topologies:

?u?l?l?l?l?l?d?d	Austin20	1.36% of cracks (CAP Append 2 Digits)
?u?l?l?l?l?l?l?d?d	Arizona20	1.26% of cracks (CAP Append 2 Digits)
?u?l?l?l?l?l?l?l?d?d	Carolina20	1.17% of cracks (CAP Append 2 Digits)
?u?l?l?l?l?l?l?d	Arizona2	1.14% of cracks (CAP Append 1 Digit)
?u?l?l?l?l?l?d?d?s	Austin20!	0.98% of cracks (CAP Append 2 Digits + Spec)

From 2020 After 12+ password policy went into place:

?u?l?l?l?l?l?l?d?d?d?d?s	Arizona2020!	2.10% of cracks (CAP Append 4 Digits + 1 Spec)
?u?l?l?l?l?l?l?l?l?l?d?s	California2!	1.04% of cracks (CAP Append 1 Digit + 1 Spec)
?u?l?l?l?l?l?l?l?d?d?d?d?s	Carolina2020!	1.01% of cracks (CAP Append 4 Digits + 1 Spec)
?u?l?l?l?l?l?l?l?l?d?d?s	Wisconsin20!	0.92% of cracks (CAP Append 2 Digits + 1 Spec)
?u?l?l?l?l?l?l?l?l?l?d?d?d?d?s	California2020!	0.78% of cracks (CAP Append 4 Digits + 1 Spec)
?u?l?l?l?l?l?d?d?d?d?s?s	Austin2020!!	0.74% of cracks (CAP Append 4 Digits + 2 Spec)

Notice: Passwords got longer, Users are choosing longer words

Audit your passwords

Pwd Patterns and Changes

Client Name:	Was 2.64%	Now 2.24%	
Seasons:	Was 2.05%	Now 6.66%	Why more? Season are long words
Months:	Was 1.06%	Now 1.46%	Why more? Months are long
Years:	Was 0.51%	Now 8.65%	Why more? Easy way to increase length

The use of common strings by users is still a massive security risk.
Especially with "password spraying" attacks.

Adapt and Overcome

To prevent "password spraying" attacks:

- Black list common passwords - Password1, Password2020 (duh)
- IDS/NIDS to detect attacks (duh)
- Learn what your users are doing with passwords / common strings (NEW)
  - Audit your passwords
- Train your users not to create basic passwords - using REAL data (NEW)
  - Audit your passwords
- Block Months/Years/Season/Client Name (NEW)
- Eradicate that “one” password… You know the one.

Audit your passwords

NIST - A Rant

- Bill Burr
  - Choose alphanumeric passwords sprinkled with capitals and special characters. (2003)
    - Trivial for a computer to do
  - Force user to change password often
    - Forcing a user to iterate
  - “*It just drives people bananas and they don’t pick good passwords no matter what you do.*” -Bill Burr
    - No, we have forced people to “give up”
  - “Unfortunately, we do not have much data on the passwords users choose under particular rules, and much of what we do know is found empirically by “cracking” passwords…” -NIST 800-63 v1.0.2

Audit your passwords

NIST - A Rant

- NIST - 2020
  - Do NOT force users to rotate passwords.
    - Are we really sure about this?
      - Sure, maybe if they are uncrackable
  - Do NOT force users to have complex passwords
    - Yes, to better support Pass-Phrases and Pass-Sentences
      - Currently an extreme minority
  - Blacklist passwords in known public dumps
    - Maybe meant to say audit your passwords? :)
    - HIBP does not cover all the things!

Audit your passwords

Adapt and Overcome

- Direct targeted and specific end-user password training
  - Group individuals doing the same bad password habits
  - Run a specific training on why <XYZ> is bad
  - Show them their own passwords as examples of what not to do.
- How can we make better passwords that are easier to remember!
- Relaxing requirements!

Audit your passwords

Fin

Twitter: @winxp5421

Twitter: @cynoprime

cynosureprime.com

Audit your passwords

Bonus Slides

For the Password Crackers

-m 1000 -a 3 ?a?a?a?a?a?a?a?a?a

4x RTX 2080 TI == 380GH/s Keyspace == 95^9

95^9 / 380 x 10^9 == 1,658,551 Seconds

1,658,551 Seconds / 86,400 (Seconds in one day) == 19.2 Days

Summary: Longer than your engagement scope.

Bonus Slides

For the Password Crackers

- Hashcat Utilizes per character Markov Chains in all bruteforce operations
  - Most probable characters based on the characters around other characters first
  - These tables are on the fly tunable
  - Let’s use this to our advantage

Bonus Slides

For the Password Crackers

-m 1000 -a 3 ?a?a?a?a?a?a?a?a?a

4x RTX 2080 TI == 380GH/s Keyspace == 95^9

95^9 / 380 x 10^9 == 1,658,551 Seconds

1,658,551 Seconds / 86,400 (Seconds in one day) == 19.2 Days

Summary: Longer than your engagement scope.

Bonus Slides

For the Password Crackers

-m 1000 -a 3 ?a?a?a?a?a?a?a?a

Hashrate	X	Seconds	==	Number of Guesses in 8 hours
380 x 10^9	X	29,280	==	11,126,400,000000000

# of Guesses	^	(	1	/	Length	)	==	char
11,126,400,000,000,000	^	(	1	/	9	)	==	60

Uses only the top most probable 60 char for each char position
Instead of all 95 characters

-m 1000 -a 3 ?a?a?a?a?a?a?a?a?a -t 60

Audit your passwords

Bonus Slides

For the Password Crackers

- Chain Rules ‘hashcat -m <ht> ./hl.txt ./dict.txt -r best64.rule -r best64.rule’
  - More GPU Ram = More better!

- Use CeWL scrape the organizations webpage for industry terms, names, etc.

- Purple Rain
  - ‘shuf dict.txt | pp64.bin --pw-min=8 | hashcat -a 0 -m <ht> ./hl.txt -g 300000’
  - PRobability INfinite Chained Elements
  - Infinite Monkeys + Infinite Keyboards = Profit
  - Randomly Generate 300k rules
    - Bonus Points: --debug-mode=4 --debug-file=success_purplerain.rules

Credits

Shapes & Icons

Vectorial Shapes in this Template were created by **Free Google Slides Templates** and downloaded from **pexels.com** and **unsplash.com**.

Icons in this Template are part of Google® Material Icons and **1001freedownloads.com**.

Backgrounds

The backgrounds were created by **Free Google Slides Templates**.

Images

Photos in this template were downloaded from **pixabay.com**. Attribution is located in each slide notes and the Credits slide.

Fonts

The fonts used in this template are taken from **Google** fonts. (Muli)
You can download the fonts from the following url: https://www.google.com/fonts/

Color Palette

The Template provides a theme with four basic colors:

#4e6e9aff	#4e6e9acc
#5477a7cc	#eeeeeeff

Trademarks

Microsoft® and PowerPoint® are trademarks or registered trademarks of Microsoft Corporation.

Google Drive® is a registered trademark of Google Inc.