Securing Domains against Registration Hijacking

SSAC | ICANN64 | March 2019

Introduction

Security and Stability Advisory Committee (SSAC)

Who We Are

- 39 Members
- Appointed by the ICANN Board

What We Do

Role: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- DNS & DNSSEC
- Registry & Registrar Operations
- ISP & Network Operations
- DNS Abuse & Cybercrime
- Internationalization
- ICANN Policy and Operations

How We Advise

104 Publications since 2002

Agenda

1 Introductions

2 Recent Domain Registration Hijacking

3 Securing your Organization's Domain Registrations

4 Conclusions

5 Relevant SSAC Publications

6 Panel Discussion

Presenters

- Tim April
- Rod Rasmussen
- Jay Daley

Recent Domain Registration Hijacking

Recent Domain Registration Hijacking

1. Attackers had the ability to modify registration records at the registry, typically by compromising login credentials
2. Attackers changed DNS delegations (NS) pointing the zones to the attackers' DNS servers. A and MX records also modified.
3. Once zones were redirected, attackers impersonated services hosted by the victims (e.g., e-mail, websites)
4. Attackers could Man-In-The-Middle (MITM) user traffic

Securing your Organization's Domain Registrations

A Review

This section contains advice on securing the registrant to registrar interface

For most of the audience this is going to be a review of things they already know

Credential Management

- Registrant credentials are critical for protecting zones
- Strong passwords are **very** important
- Multi-factor Authentication adds an additional layer(s) of protection, specifically helps against some MITM attacks etc
- The email address used for registrar communications should also have strong credentials as this path is used to reset registrar passwords and are targeted frequently
- Don’t forget credentials for email...

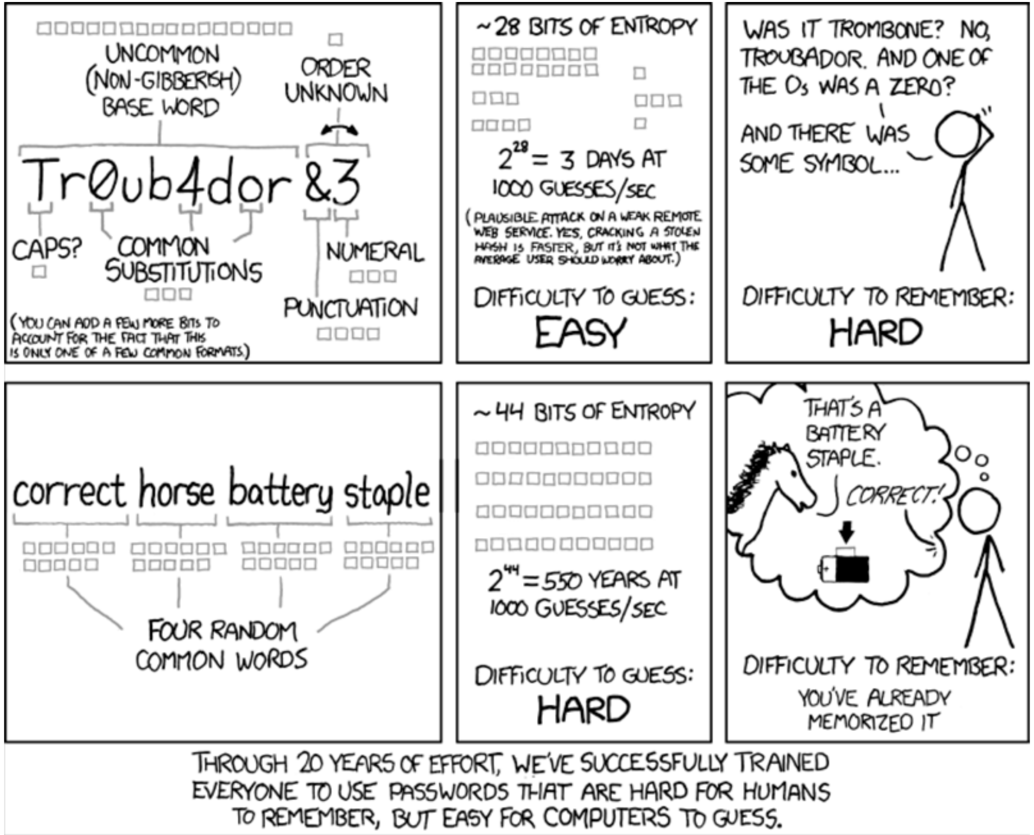
Credential Management: MFA

- Multi Factor Authentication(MFA) or 2-Factor Authentication(2FA)
- Use when offered, ask for it when it’s not
- Provides an additional layer of security over just using passwords

Credential Management: MFA

- Common MFA / 2FA types, roughly in order of preference
  - Universal 2nd Factor (U2F) *most preferred*
  - Time-based One-Time Password (TOTP)
  - HMAC-based One-Time Password (HOTP)
  - SMS Passcode
  - Phone Based Verification *least preferred*

Credential Management: Passwords



UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: https://xkcd.com/936/

Credential Management: Review

- Do:
  - Use strong unique passwords
  - Use a password manager
  - Use MFA
- Don’t:
  - Share passwords
  - Re-use passwords across multiple accounts

Email Security

- Email accounts, used for password resets, are often targets
- Senders: Use DMARC with SPF and/or DKIM
- Receivers: Enforce DMARC and SPF for mail, verify DKIM signatures
- Do not use a personal email address for critical domains (e.g., user@freemail.tld)
  - Use email address of a role in the organization (e.g., role@organization.tld)

Email Security (continued)

- Protect Email Access
  - Harden your email access to withstand MITM attacks
  - Require Transport Layer Security (TLS)
  - Use MFA for authentication
- Protect against phishing attacks
  - Conduct regular phishing training
  - Use spam filtering

Registry Locks

- Enable registry locks when available
- Registry locks must be disabled to make changes to records
- Not all registries or registrars support registry locks
  - Often comes at an extra charge
- Area for future work: registry lock process standardization

DNSSEC

- Sign your DNS zones
- Require users and services to use validating resolvers
- Will not protect from all types of attacks, but provides enhanced integrity protection
- DNSSEC Signed zones were less impacted than others in recent attacks
- DNSSEC Signed zones were like canaries in recent attacks

Be Careful What Nameservers You Use

- The security practices of your nameserver domain name and operators are just as important to the security of your own domain name

Monitoring

- Monitor your DNS infrastructure
- Monitor your DNS zones
- Monitor parent/registry for changes
- Monitor TLS certificate transparency logs
- Monitor for DNSSEC validation failures
- Monitor your nameserver records

Relevant SSAC Publications

Relevant SSAC Publications

- SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse
- SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts
- SAC049: SSAC Report on DNS Zone Risk Assessment and Management
- SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

Conclusions

Conclusions

- This is not the last time we will see these kinds of attacks
- Deploy security in-depth, there is no holy grail
  - Secure the credentials used to access your registrar
  - Use MFA where possible
  - Secure email addresses used for password reset
  - Deploy DNSSEC signing and validation
- Use Registry Locks
- Monitor your domains

Conclusions (Continued)

Most of us are already aware of this advice, but here we are saying it again.

Isn’t it time we have better industry security standards that all registrars are required to adopt?

Q&A

Thank you