Recent Identity Threats and Trends: Lessons to Improve Identity Security

Martín Gallo

Sr. Director of Research, SecureAuth

JUNE 2021 | #identiverse

Who?

Identity Security Without Compromise

Lead Innovation Labs at SecureAuth

Offensive security background, moved into identity security
Former PdM/PO, Penetration Tester, IT&InfoSec Consultant

Community and knowledge sharing advocate

What?

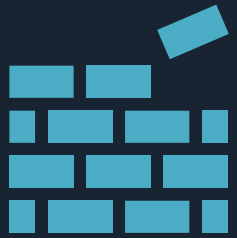
Recent Threat Cases

Recent Trends

Lessons for Identity Security

Recent Threat Cases

Identity-related operations,
tactics and techniques



Fundamentals

Leveraging improved known tactics and techniques

Detours

Bypassing or rendering identity security measures ineffective

Rising

Trend-setting with novel procedures and methods

Fundamentals

85%

Human

61%

Credentials

Incidence on breaches reported in
Verizon's 2021 Data Breach Investigation Report

Password spraying
[T1110.003]

Single password + large number of users, target common passwords

Credential stuffing
[T1110.004]

Breach dumps, target password reuse

Low and slow

Larger time periods between attempts, larger attack duration

Fast IP rotation

Larger pool of distributed IP addresses, quick addition of new ones

STRONTIUM

Tracked and reported by Microsoft Threat Intelligence Center (MSTIC) and Microsoft Identity Security.

Targeted **+200 organizations** and **+10.000 accounts** only between Sep 2019 and June 2020.

STRONTIUM: Detecting new patterns in credential harvesting

Canada suffers cyberattack used to steal COVID-19 relief payments

Canadian online portal suffered credential stuffing attack around August 2020.

From a total of **12M accounts**, **+9K** were successfully breached due to password reuse.

GCKey

Detours

Got mobile-based MFA?

SMS, Authenticator app, push notification, +

Cerberus

Initially reported by Threat Fabric in February 2020.

Malicious application abusing Android's **Accessibility Services** to provide RAT functionality.

Among others, **targeted Authenticators** and **MFA-enabled** banking, finance and crypto applications to steal OTP codes.

MFA stealing malware

Mobile malware targeting Authenticators and MFA-enabled apps.

Input Prompt [T1411], Input Capture [T1417], Input Injection [T1516]

Hijacking 2FA – A look at Mobile Malware Through an Identity Lens

Got IP binding and Device Recognition?

Commonly used mechanism to perform unmanaged device recognition and limit abuses

Genesis/Richlogs

Reported late 2019, active during 2020 and now defunct.

Pay-per-bot stores that provided **access** to compromised devices by means of phishing or stolen credentials.

Monetized digital **fingerprints** and **proxy access** to bypass MFA and other detection mechanisms in considerable secure sites.

Access black markets

Black market for access proxies & digital fingerprints that bypass protection and recognition mechanisms

Use Alternate Authentication Material: Web Session Cookie [T1550.004], Proxy Through Victim [T1604]

Why Browser Fingerprinting is Creating Challenges for Identity Security

Rising

Abusing Established Trust

Leverage established trust in identity security measures to retain access

Golden SAML

Forge Web Credentials: SAML Token [T1606.002]

As **post-exploitation** steps in **supply-chain attacks**, threat actors compromised **SAML certificates** or **bypassed MFA solutions** to forge access to third-party services.

Detection is challenging, as the circumvented identity security solutions are **trusted**

Abusing user awareness

Exploiting user’s behavior against them

Application-based Phishing

Use Alternate Authentication Material: Application Access Token [T1550.001]

High-profile attacks targeting multiple organizations, increasing since 2019.

Leverage **OAuth Consent** to perform targeted phishing and access victim's data in the service provider.

Abuses the fact that **email links** and **phishing sites** are 100% **valid and secure**.

Coinbase, Microsoft's Office 365, Google's GMail, AWS, +

Malicious Office 365 Apps Are the Ultimate Insiders

Recent Trends

Observing threats direction

Recent Trends

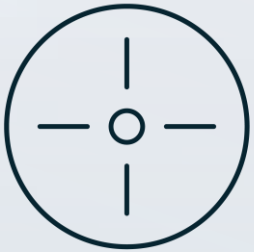
and their directions

Monetization

Actors are monetizing breach data and compromises easily

Feedback loops

Identity-based attacks nurturing both entry and post-exploitation vectors



Targeted and expanded

Social engineering and phishing beyond email

Lessons for Identity Security

Obtaining insights

Lessons

Keep adapting

2020 showed us that the context can quickly change, and we need to be ready

Back to basics, renewed

Account management, access control, least privilege, security awareness

The basics are the same, we need to renew methods

Stay threat-aware

Threat landscape is continuously changing, stay aware and ready to adapt

Thank you!

@martingalloar
mgallo@secureauth.com