STEALTHbits Credential and Data Security Assessment

Executive Summary: Globex Corporation

STEALTHbits TECHNOLOGIES

PLEXEON

STEALTHbits’ Credential and Data Security Assessment (CDSA)

Regardless of an attacker’s entry point into an organization, they’re always after the same two things – credentials and data. In response, STEALTHbits works to remove inappropriate data access, secure the credentials attackers seek to compromise and exploit, and detect, prevent, and mitigate advanced threats at the endpoint, directory, and data layers of your environment.

To help shine a light on where you’re most vulnerable, STEALTHbits Technologies has engineered and conducted a comprehensive assessment of your Network File Share, Active Directory, and Windows Server infrastructure. The analysis detailed in the pages to follow will provide clear insight into the security stature of your credentials and data.

Assessment Scope

File Shares

Number of Hosts:

- 2

Number of Shares:

- 361

Number of Folders:

- 540,621

Number of Files:

- 39,006,138

Number of Permissions:

- 369,878,600

Storage Size Scanned:

- 7,250.35 GB

Active Directory

Number of Domains:

- 1

Number of Users:

- 7,750

Number of Groups:

- 4,364

Number of Computers:

- 13,230

Number of OUs:

- 109

Number of Permissions:

- 8,099,223

Systems

Number of Servers:

- 81

Number of Desktops/Laptops:

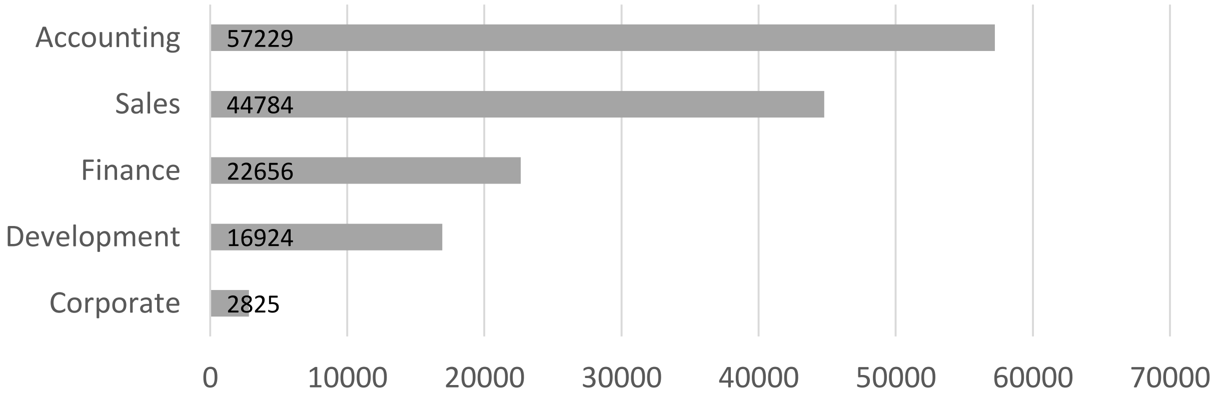
- 1

Operating Systems (Top 5):

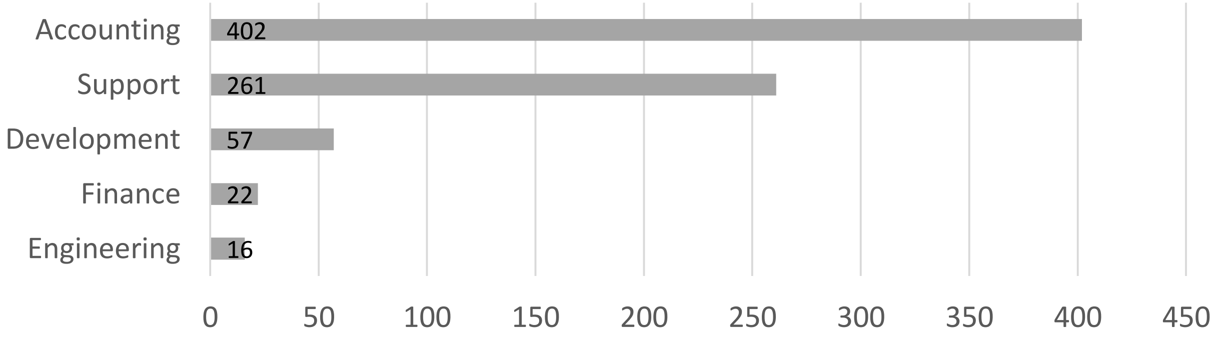
- Windows Server 2012 R2 Standard (80%)
- Windows Server 2008 R2 Standard (15%)
- Windows Server 2012 R2 Datacenter (2%)
- Windows 7 Professional (1%)
- Windows Web Server 2008 R2 (1%)

- **144,794** folders are openly accessible to all users (26%)
- **828** files containing sensitive data are exposed via open access

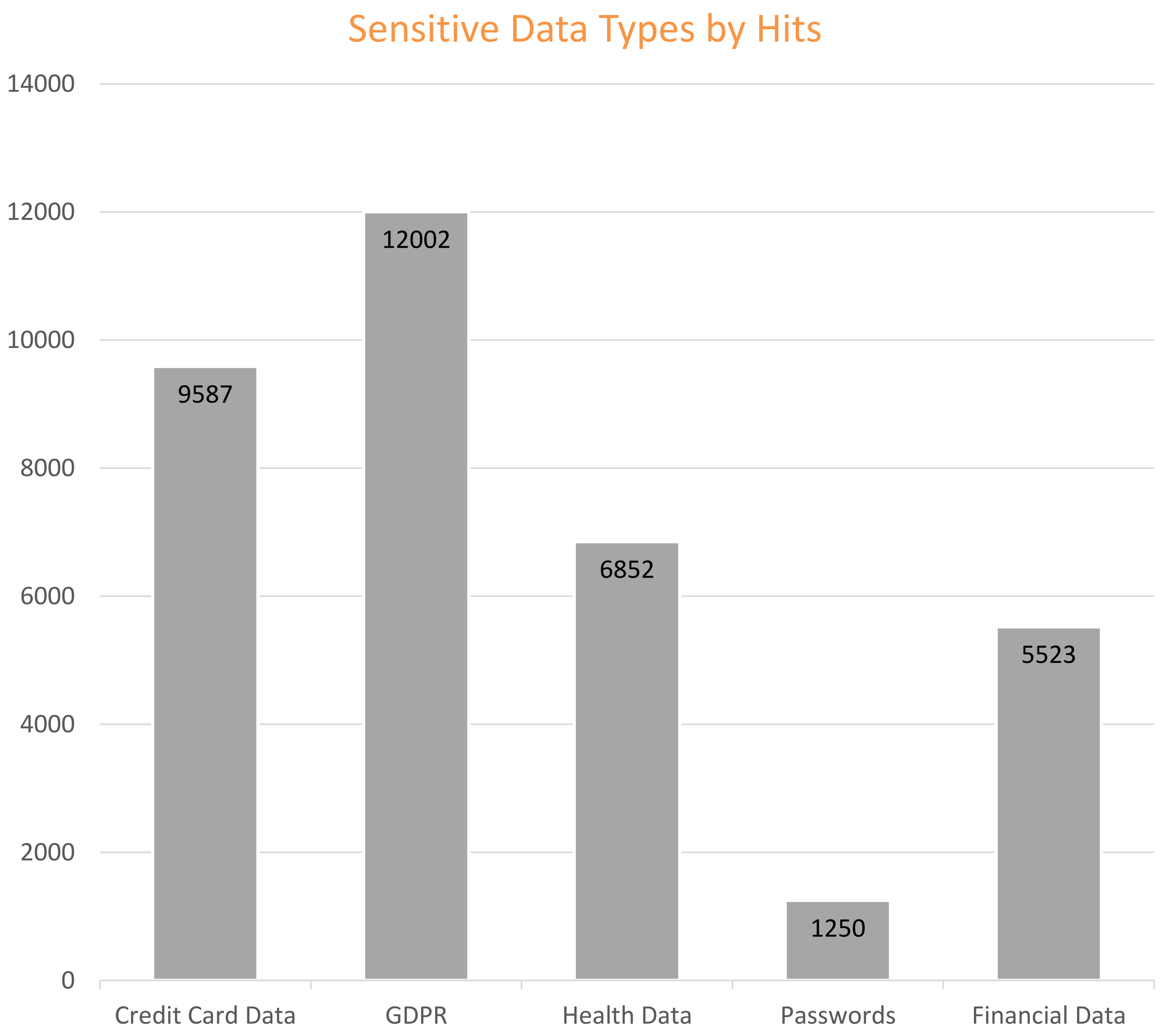
Top Shares with Open Access (by # of folders)



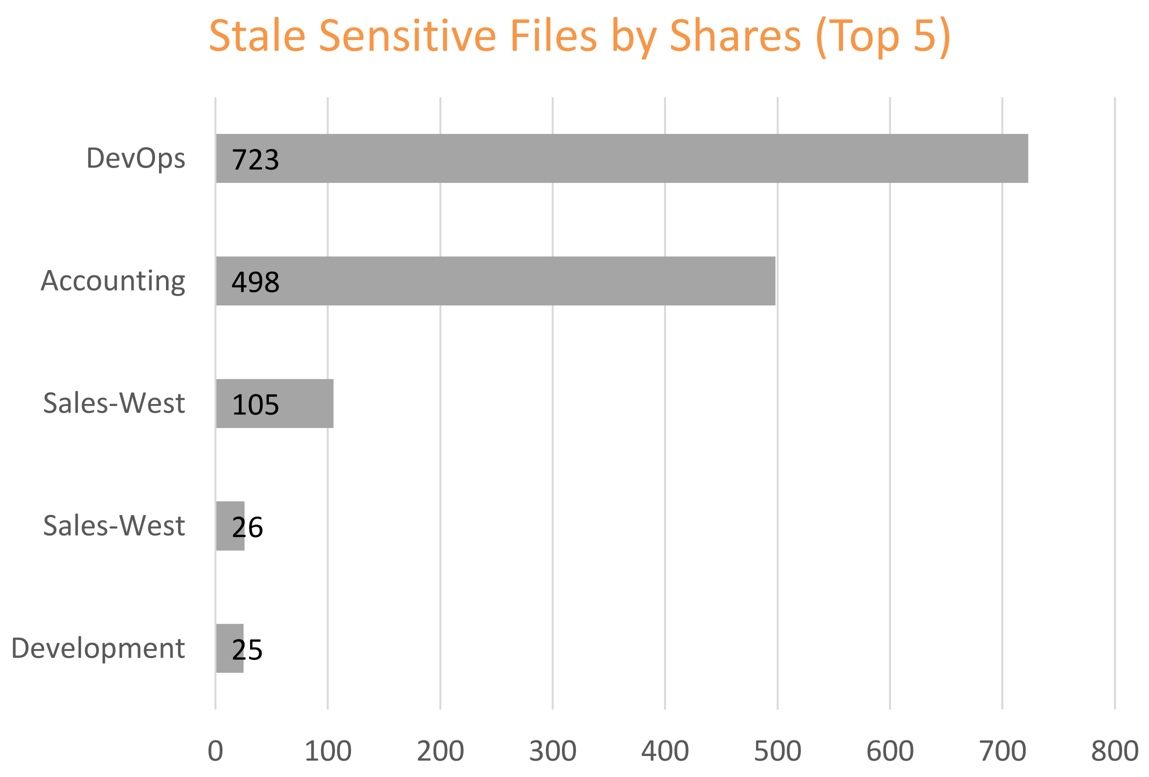
Top Shares with Open Access (by # of Sensitive Files)

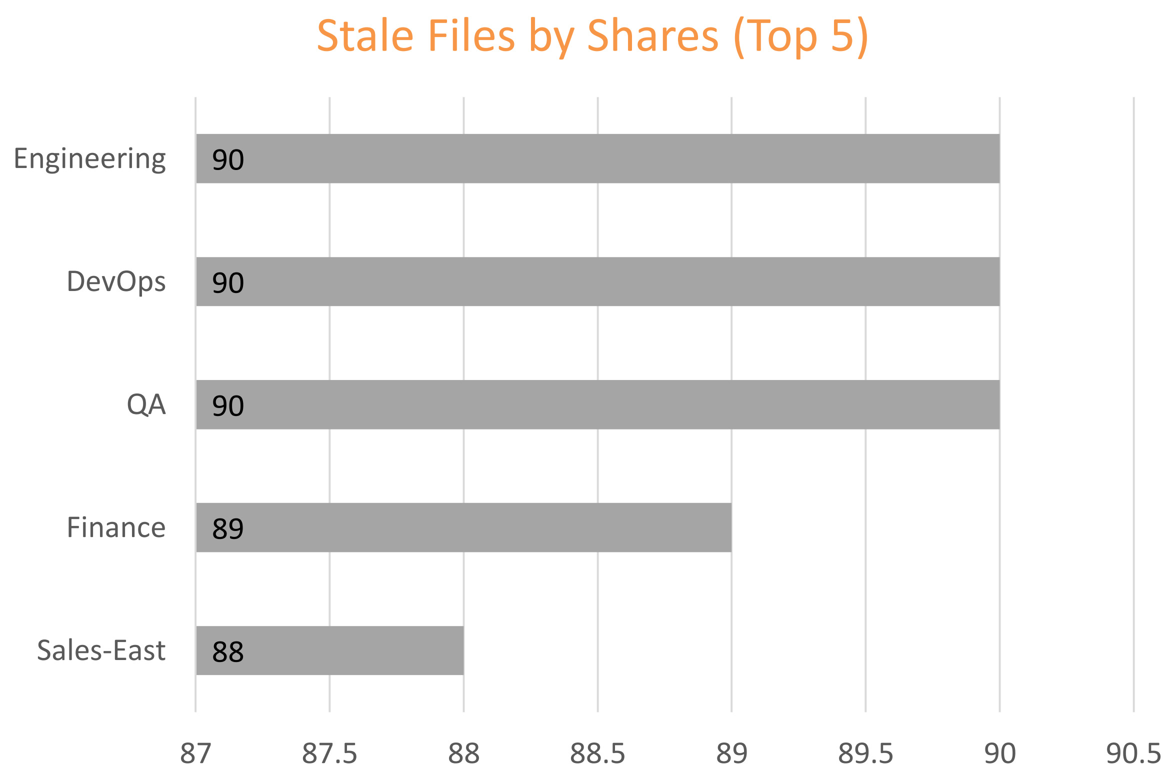


- **27,983** files have sensitive data
- **882** groups give access to sensitive data
- Sensitive data was found in **58%** of scanned file shares

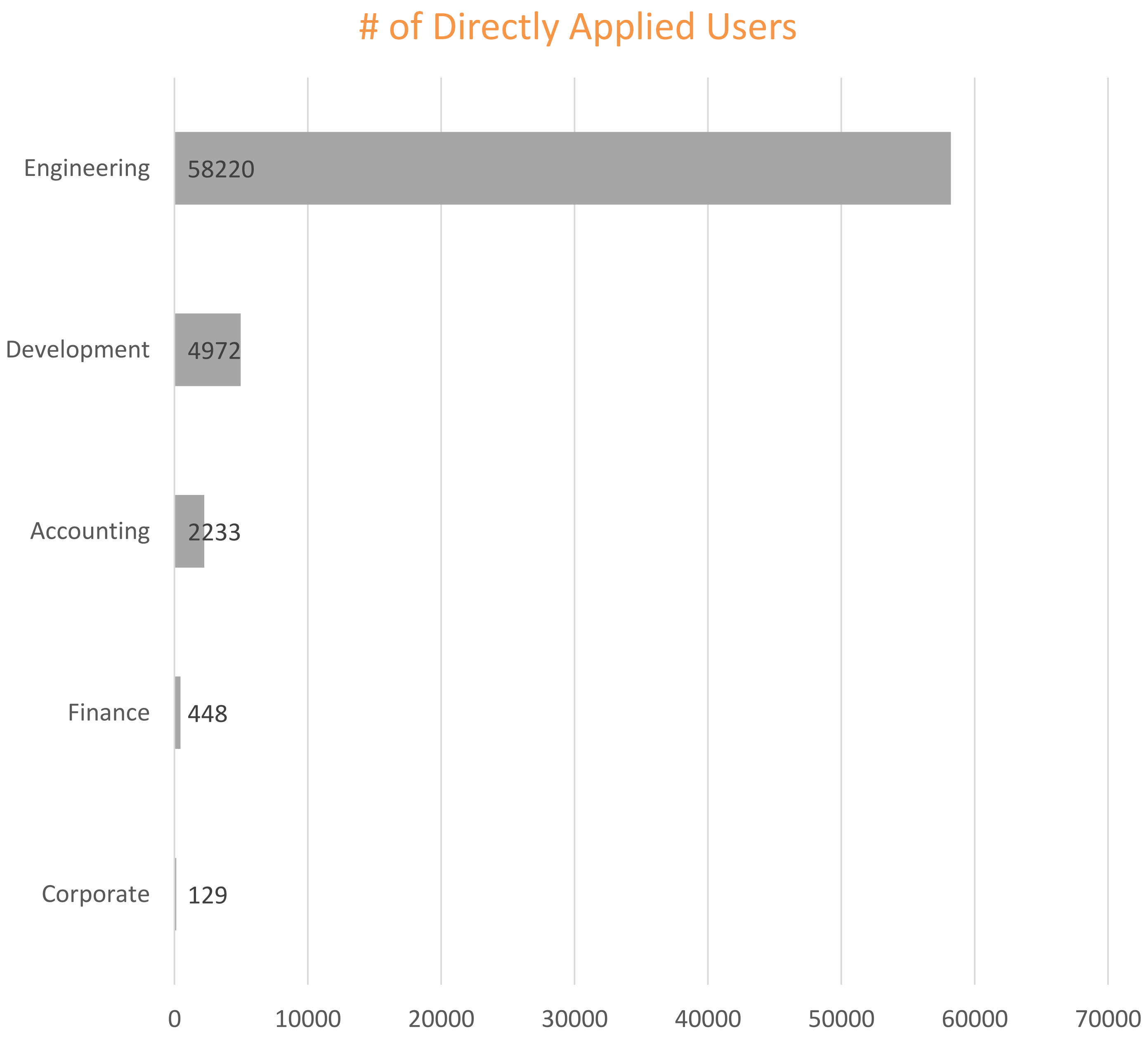


62.8% of all files examined are stale





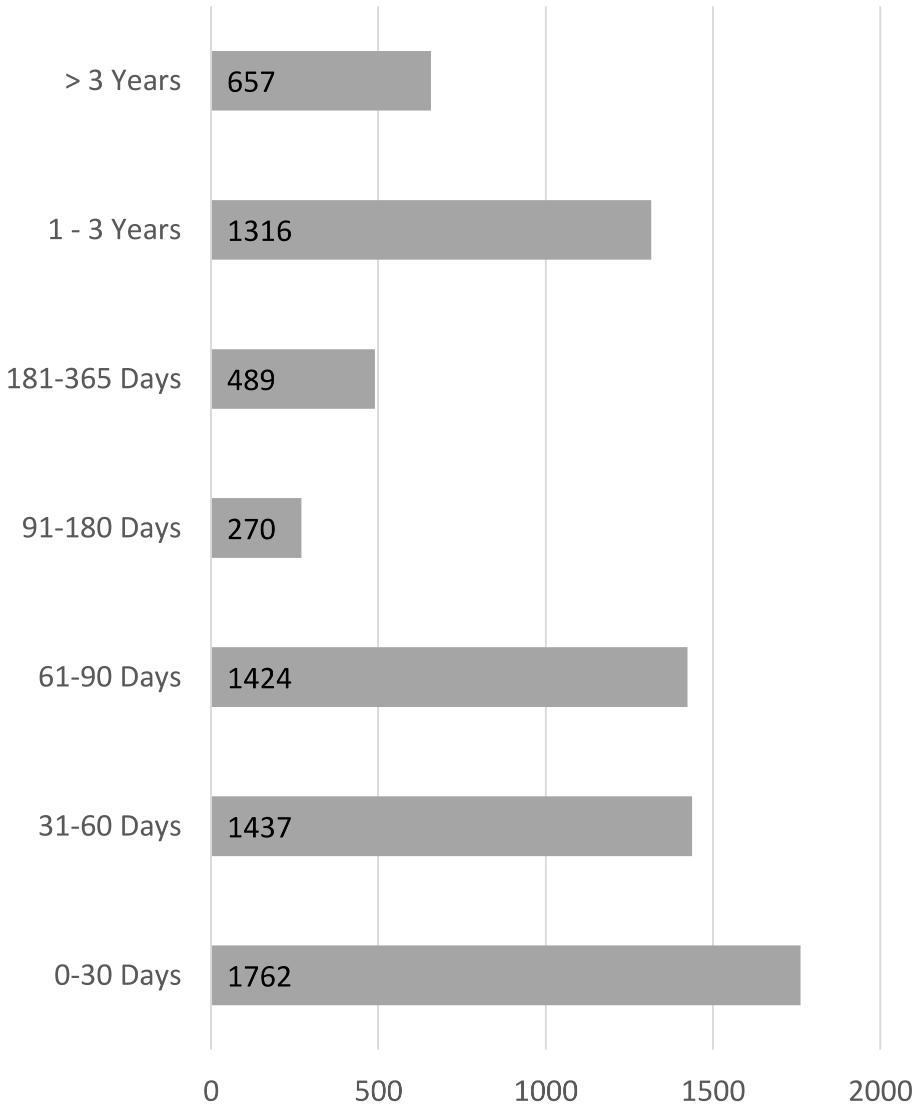
- **58,435** high risk permissions
- **259,426** direct user permissions
- **26,804** unresolved SIDs
- **193,491** folders with broken inheritance
- **0** historical SIDs



Key Discoveries – Weak Passwords

- **944** users with weak passwords (12.18%)
- **312** users with weak historical passwords (4.02%)
- **594** instances of password re-use (7.66%)
- **304** passwords never expire (3.92 %)
- **7257** passwords are stored with weak or reversible encryption (93.64%)
- **2** plaintext passwords found in Group Policy Preferences

Password Age Distribution



Key Discoveries – Critical Active Directory Rights

Non-administrators that can perform sensitive AD actions

66

Reset Passwords

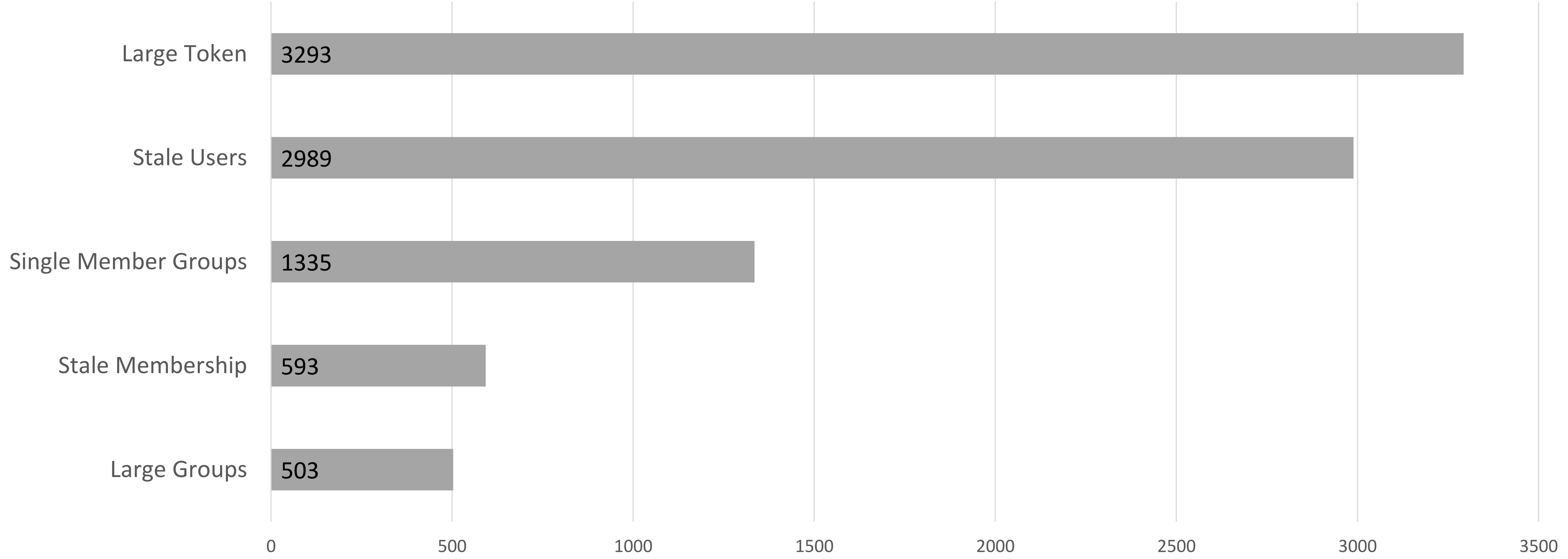
3

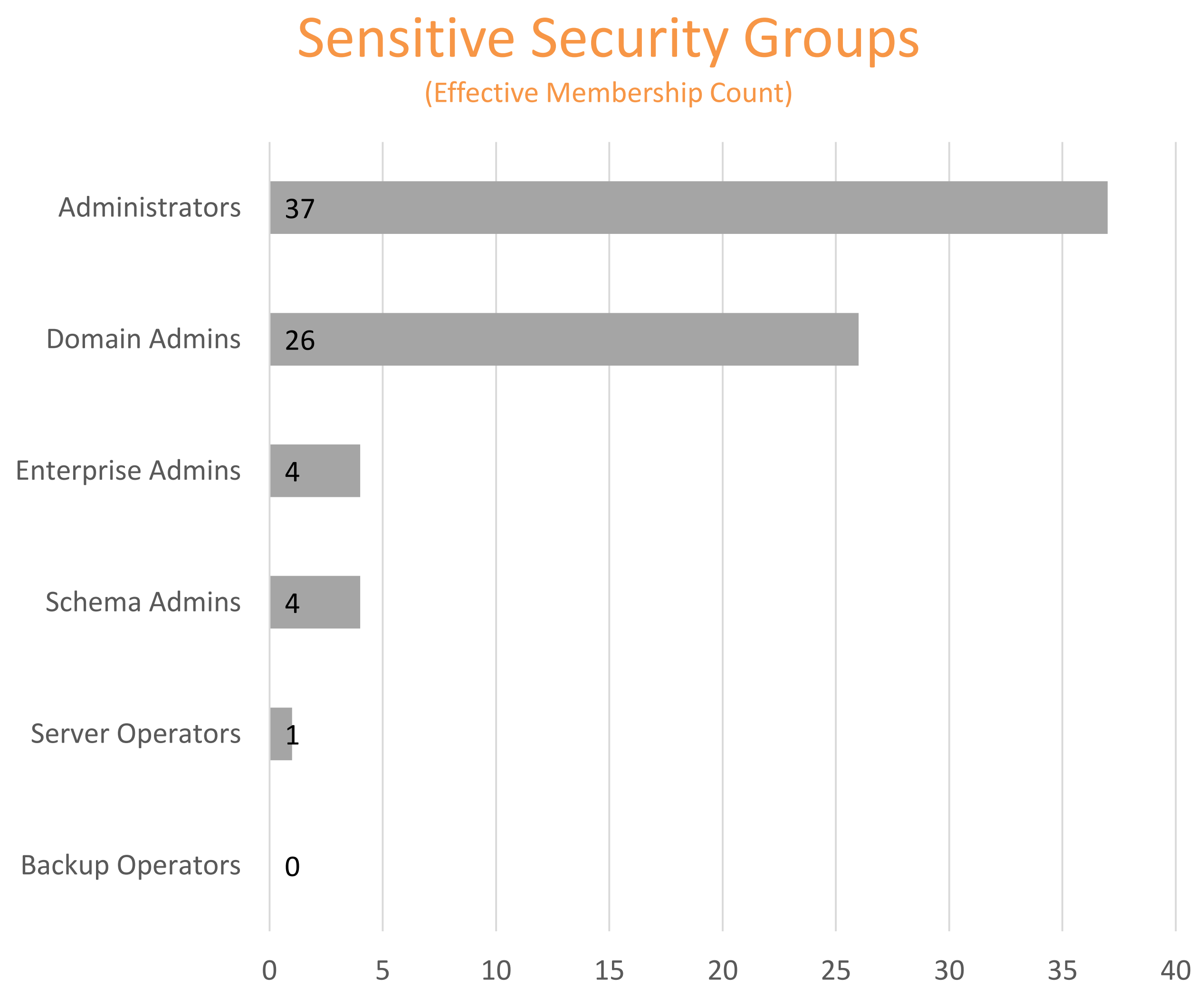
Replicate Password Data

66

Change Group Membership

Principal Count by Issue

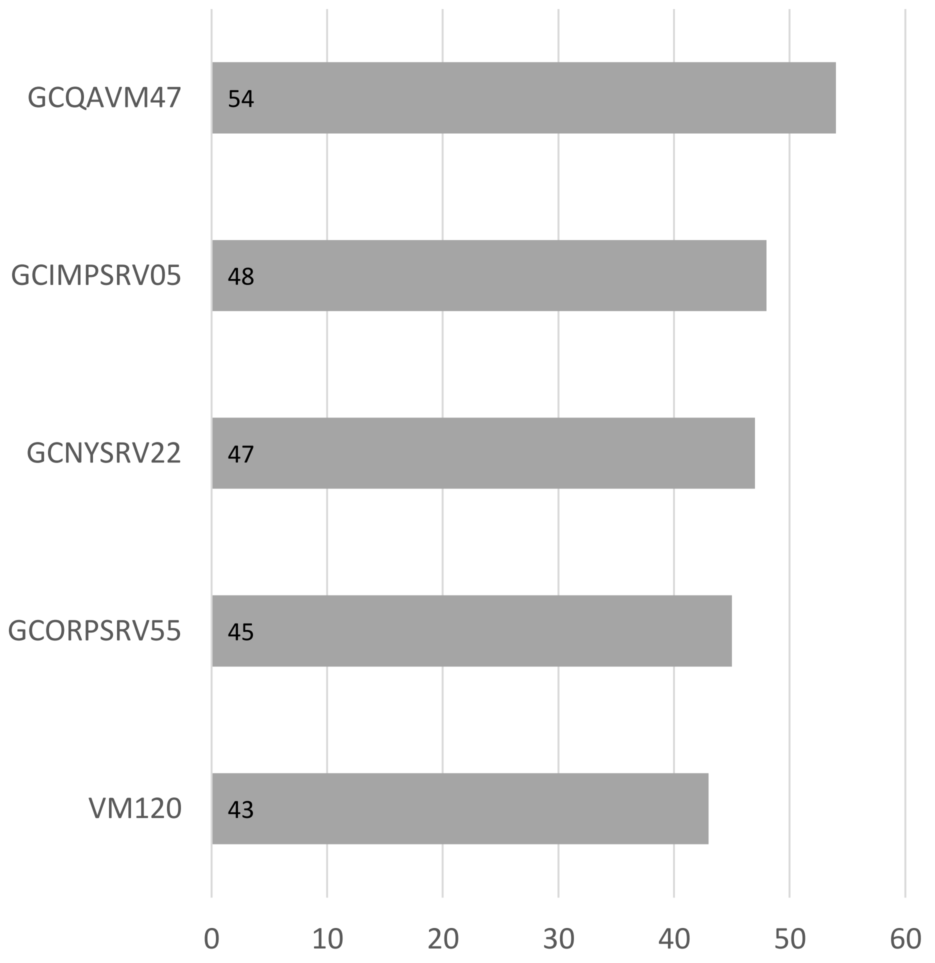


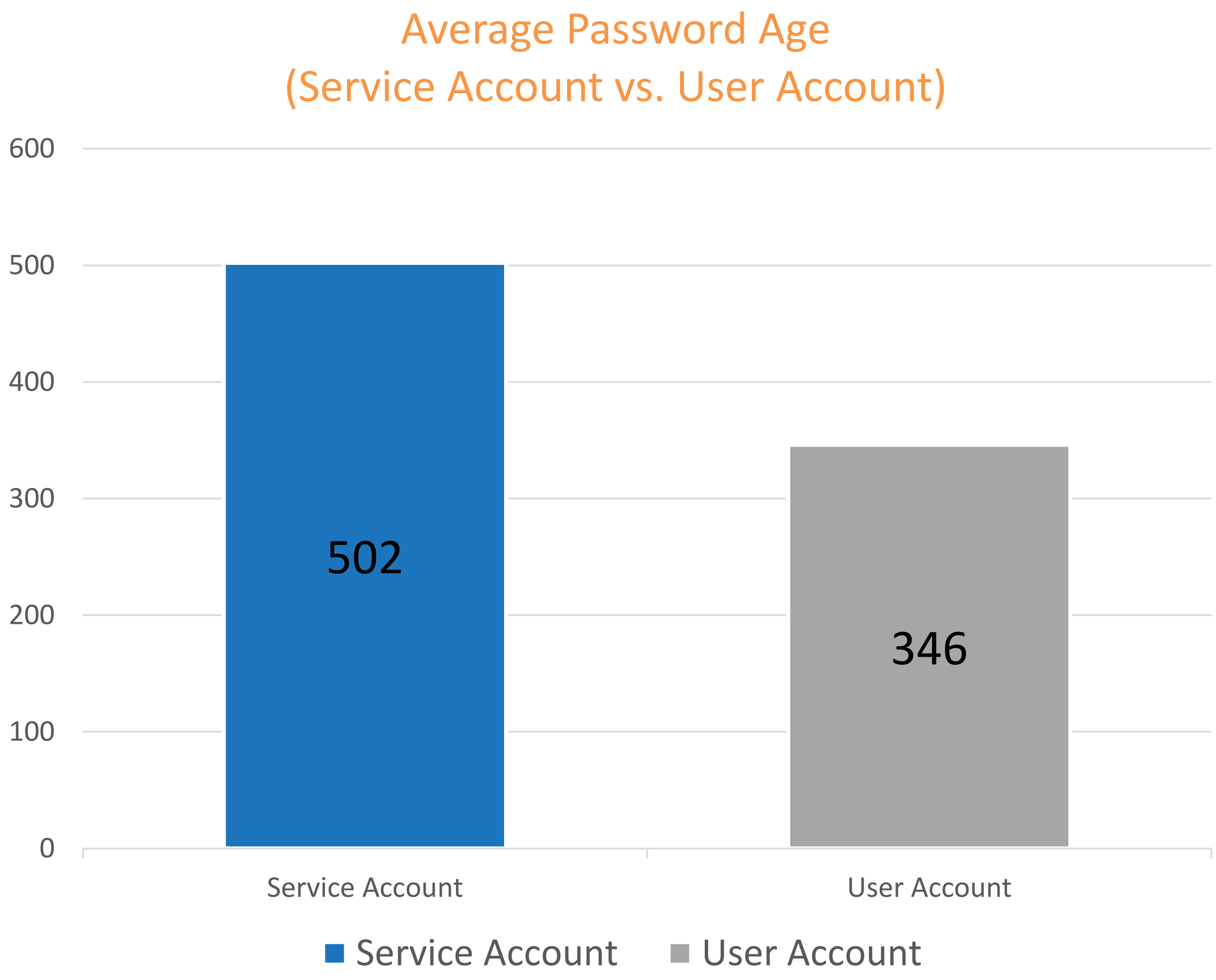


- Total Number of Administrators
  - **38**
- Non-Expiring Admin Passwords
  - **22**
- Oldest Password
  - **7,518** days

- **213** unique accounts have Local Admin rights
- **268** unique users have logon rights
- The Average Password Age of users with Local Admin rights is **502** days
- The Oldest Password identified for an account with Local Admin rights is **7,518** days

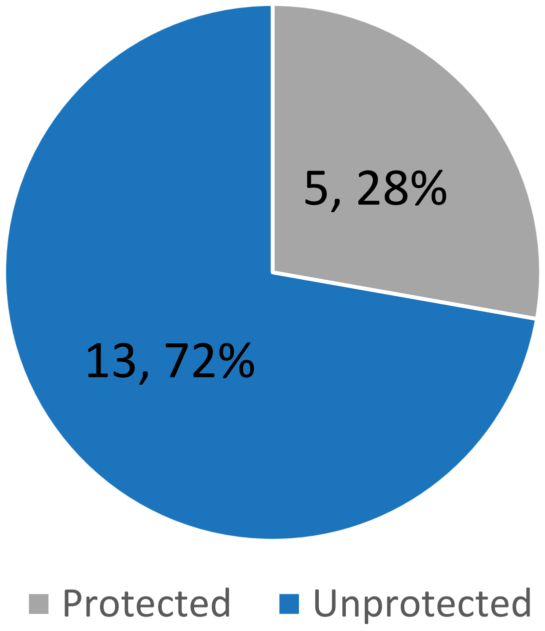
Top Servers by Local Admin Count





- Total Number of Service Accounts
  - **18**
- Oldest Service Account Password
  - **2,084** days
- Average Password Age
  - **502** days

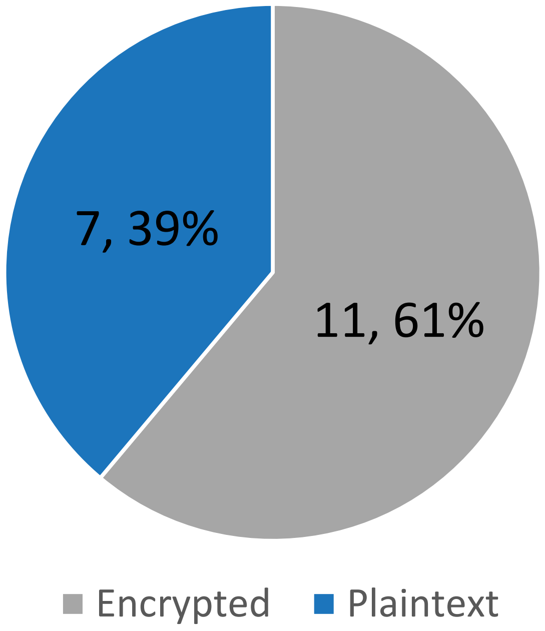
Systems with Protected Credentials (LSA)



Systems with Suspicious PowerShell Commands

0

Systems with Plaintext Credentials (WDigest)



STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.

STEALTHbits TECHNOLOGIES | PLEXEON