BROWSER STORED PASSWORD DISCOVERY TOOL FOR WINDOWS

Executive Summary

Prepared for Insurance Company

Scan Date 4/30/2017
Scan completed in 1 minute(s).

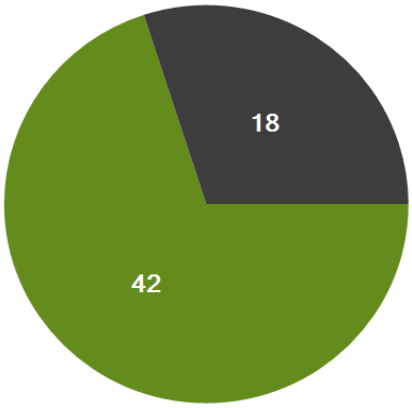
What happens if administrative credentials to sensitive systems are being stored in employee browsers?

Credentials stored in web browsers can pose a threat to both individual and domain security. These unregulated credentials have no expiration and are easily extractable from the user's machine. Often times these credentials are years old and have never been changed. With automated tools that can detect stored browser stored passwords across your domain, the process of finding and uprooting these long lived credentials has never been easier.

This scan has generated an excel file with a complete inventory of discovered browser stored passwords in your domain containing information such as the machine it is on, the windows user the credential belongs to, the URL of the credential, the date it was created, and the number of times it has been used.

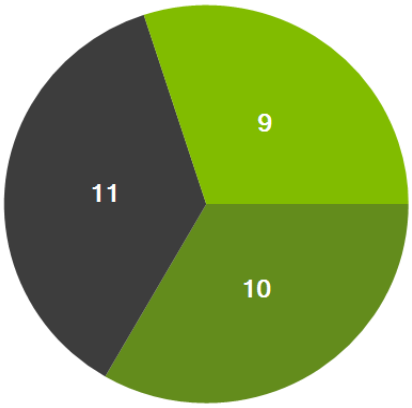
After reviewing the various reports, it is easy to see that improvements can be made to lock down browser stored passwords and greatly reduce your organization's risk to attack. Consider securing these credentials in Secret Server before they become compromised by attackers. Secure browser stored passwords in your domain!

Browser Stored Password Discovery Tool



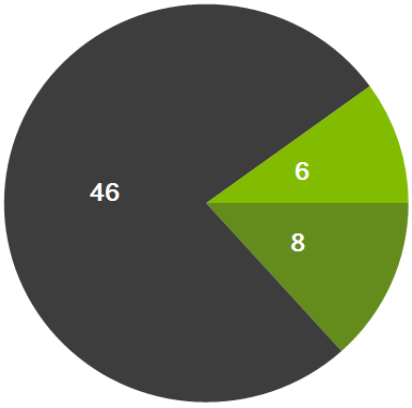
Distribution Of Browser (Firefox vs Chrome)

This is a break down of which browsers are storing passwords in your network. Extracting passwords from either browser can be effortless. Limit which browsers are allowed on your network!



Distribution Of Browser Stored Password Age

Here is the breakdown of browser stored passwords age, in years. Older passwords are more likely to have already been compromised, especially if the same password was involved in a different breach! Rotate passwords today!



Distribution Of Browser Stored Password Usage

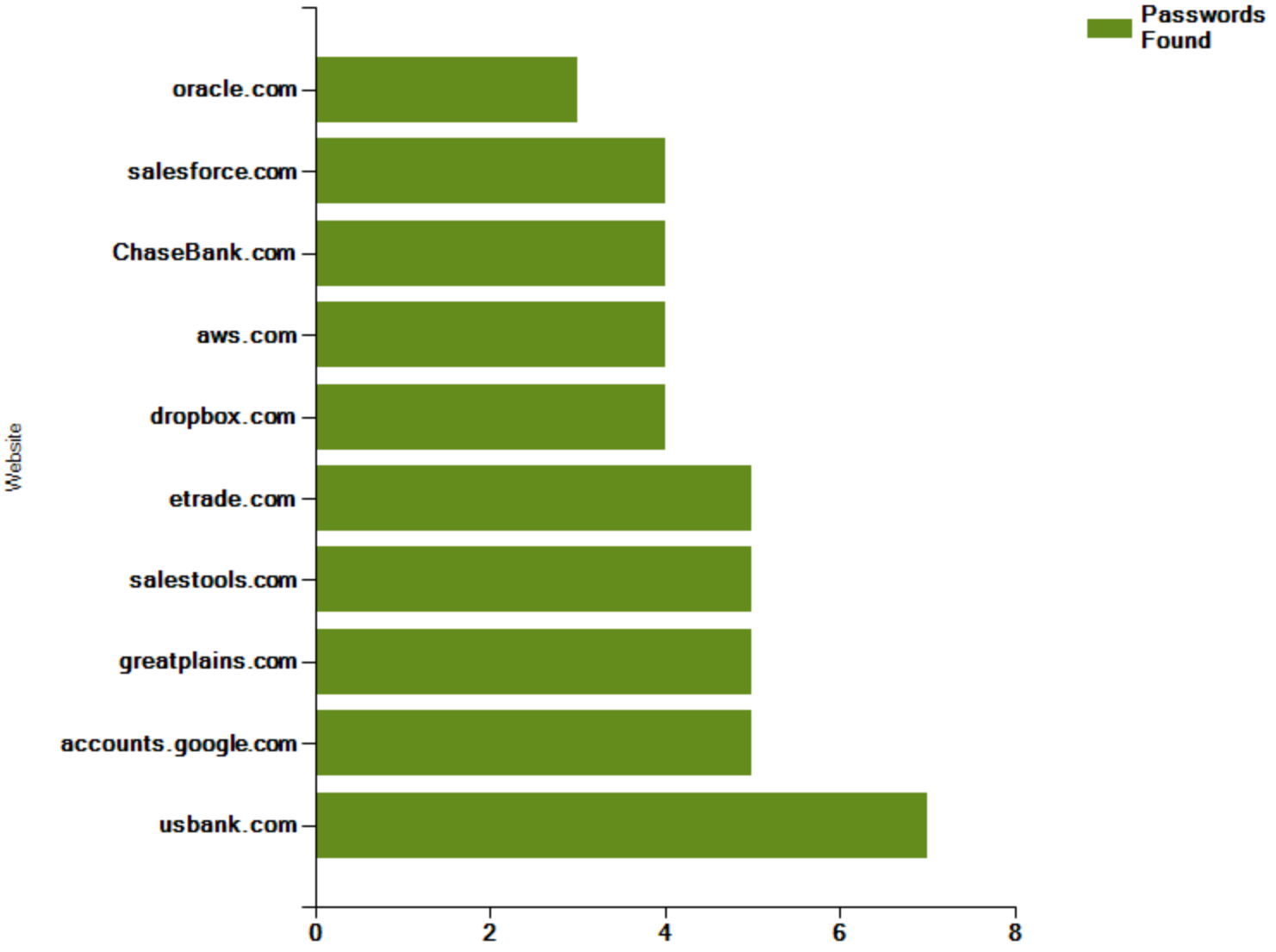
Here is the breakdown of how many times browser stored passwords have been used in your environment. Your most frequently used passwords should be managed by a central Privileged Account Management solution, especially if they are used to access critical sites or systems. Gain Better Control Of Passwords!

Browser Stored Password Discovery Tool

Top 10 Most Common Website Passwords Discovered

Careful! You should check if this list of websites contains any that pose a critical threat if the account is compromised. Those accounts should be stored, secured, and launched from Secret Server. Attackers look for stored passwords for banking websites, social media websites, and company infrastructure logins!

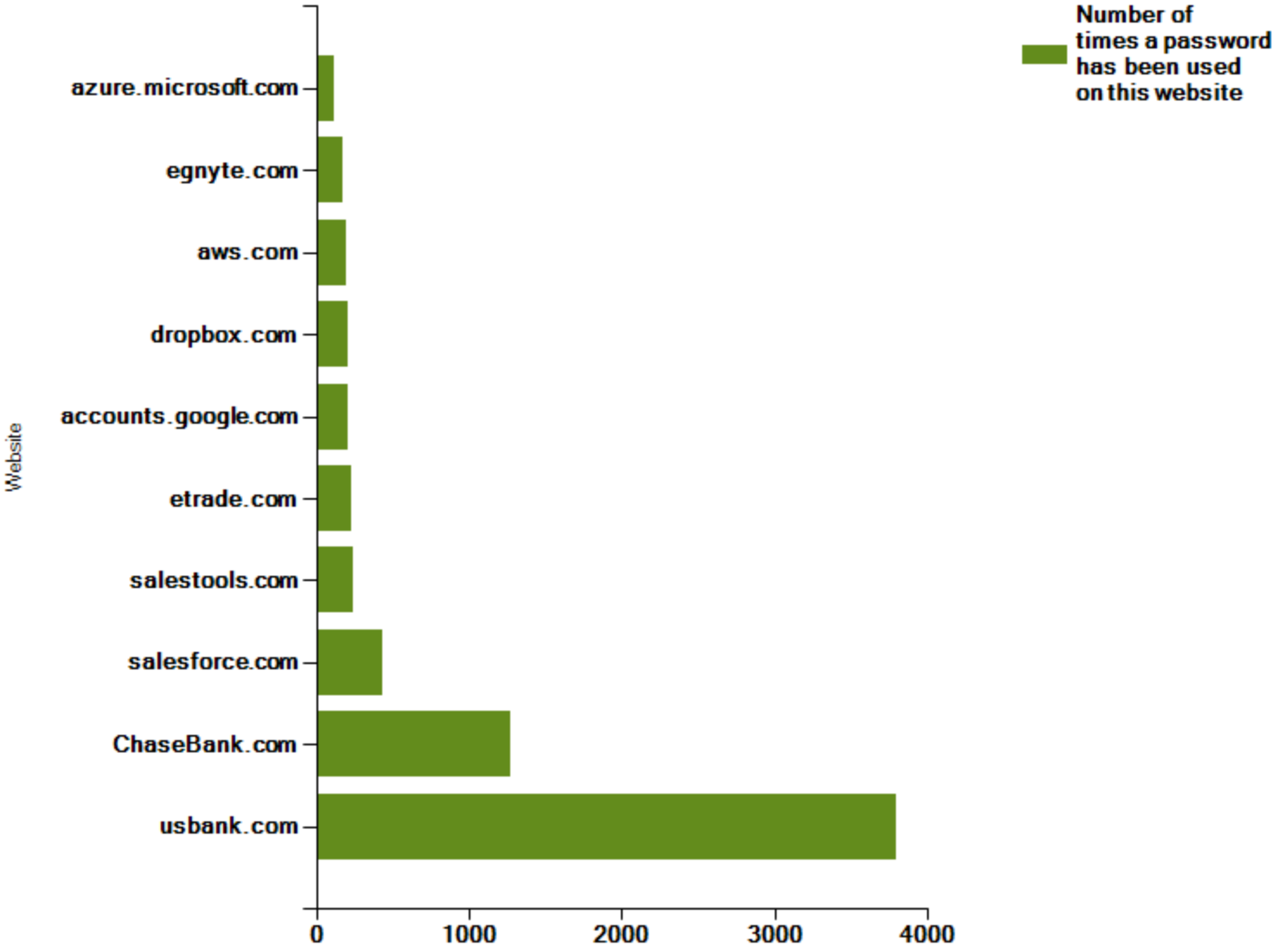
Protect the accounts that provide access!



Browser Stored Password Discovery Tool

Top 10 Most Frequently Used Passwords

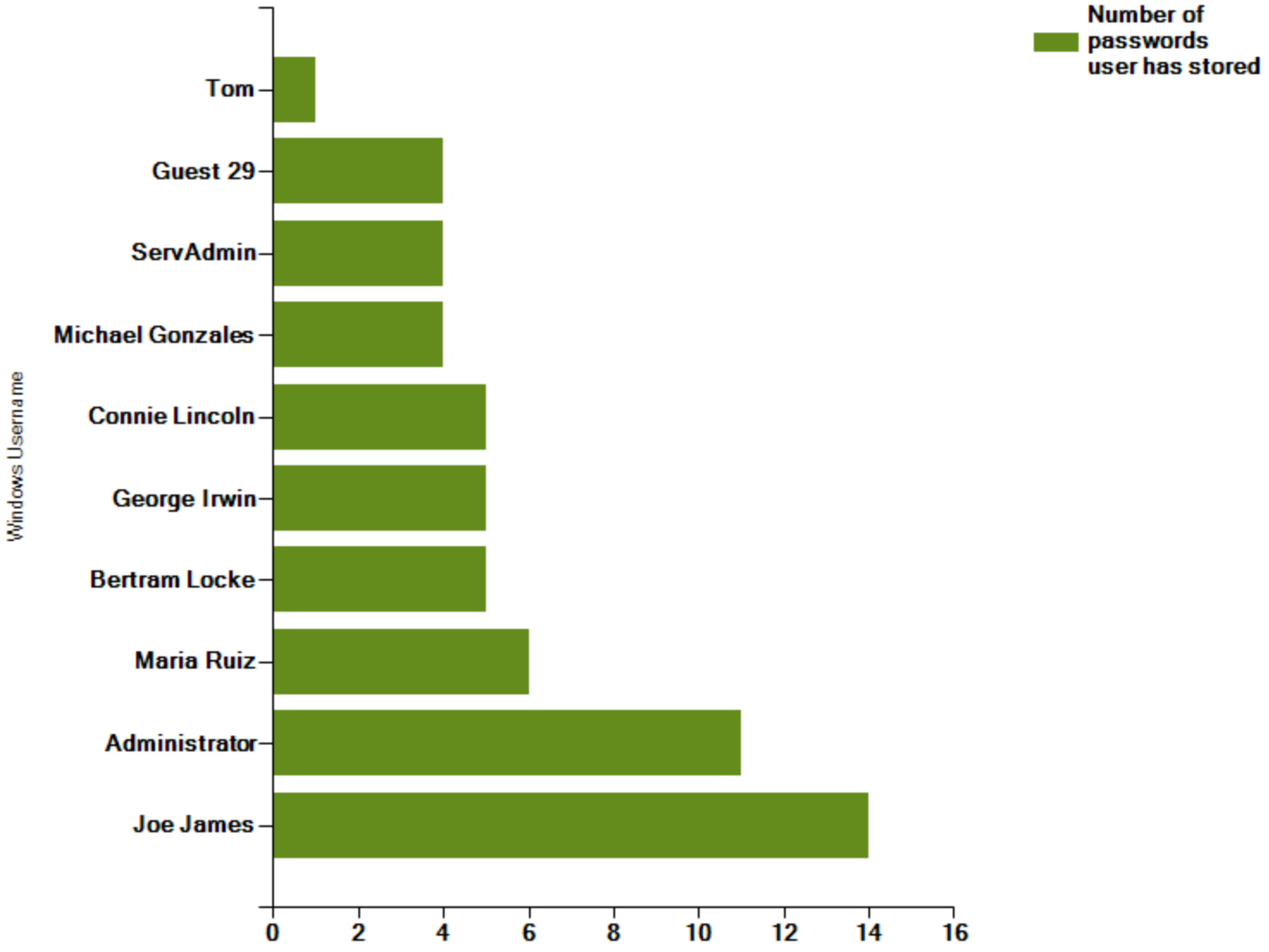
Look Out! These most frequently used passwords are likely to be important in day to day operations and are stored insecurely. Secure your most frequently used passwords!



Browser Stored Password Discovery Tool

Top 10 Most Common Users With Stored Passwords

Caution! These users love to store their passwords in their browsers! Make sure they aren't storing anything critical or sensitive to your organization. Store these passwords in a central vault!



Browser Stored Password Discovery Tool

Top 10 Most Common Machines With Stored Passwords

Watch it! These machines have the most browser stored passwords on them, and are most vulnerable to having these passwords stolen! Secure passwords and the access they provide!