WHAT YOU NEED TO KNOW ABOUT BRUTE FORCE ATTACKS

Brute Force Attacks – using automated tools to try one password after another until the correct one is found – are lately undergoing a resurgence. Here is what you need to know:

BRUTE FORCE ATTACKS ARE NOT ONLY A THREAT TO INTERNET FACING SYSTEMS

Often times, Brute Force Attacks are launched against internal servers:

- By malicious employees and contractors with legitimate access to the network
- By desktops and other systems within the corporate network that have been infected with malware
- By outside intruders that have obtained valid login credentials to the corporate network

NEW METHODS PROVIDE A MUCH HIGHER HIT RATE – WITH FAR FEWER ATTEMPTS

Automatically generated passwords created the old fashioned way (aaa, aab,aac….) can take a long time to produce a hit. The rise in organized criminal groups in cybercrime has led to newer, more efficient methods being deployed that provide a much higher hit rate, such as:

- Statistical analysis of large, stolen password databases to create ordered lists of the most often used passwords and word combinations. This technique provides hits with very few attempts across a limited range of logon IDs.
- Heuristic Password Generators applying rules of the local language against machine generated passwords to rule out any construct that does not constitute a proper word (such as more than two vowels in succession). This dramatically reduces the number of possible combinations.
- Using computer systems with multiple high-powered GPUs for statistical analysis and heuristic password generation.

IT'S ABOUT THE PASSWORD, NOT THE SYSTEM

Since users tend to use the same password across as many systems and applications as possible, attackers do not need to attack potentially well protected high-value systems. Instead they typically prefer to obtain a user's password from a lesser protected system – and then use that password for logging on to the high value target.

TARGET SERVICES WITH POOR LOGGING THAT TYPICALLY AREN'T MONITORED

FTP servers are the preferred target for Brute Force Attacks as most enterprises lack the tools for effective monitoring of FTP servers and most FTP software by default does not log failed login attempts etc.

Unlike many logins we face in our daily lives where a small number of logon failures results in a suspended user ID, most FTP servers lack any way to disable a user ID after a threshold number of failed logons. Attackers are free to try hundreds of thousands of times until they discover the right password.

FTP/SECURITY SUITE PROTECTS EFFECTIVELY AGAINST BRUTE FORCE ATTACKS

SAC's **FTP/Security Suite** detects Brute Force Attacks, automatically stops the attack, alerts IT staff and blocks the attacker from accessing the affected server and optionally all other servers in the enterprise – immediately.