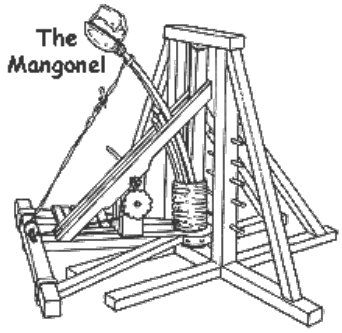
When the Data Center is Under Siege Don’t Forget to Watch Under the Floor

Lori MacVittie, 2011-22-06

Don't get so focused on the trebuchets, mangonels and siege towers that you forget about the sappers.



We often compare data center security to castles and medieval defenses. If we're going to do that, we ought to also consider the nature of attacks in light of the military tactics used to perpetrate such attacks, namely siege warfare.

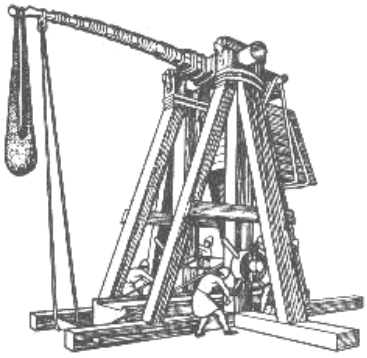
It's likely more apropos today than it was when the analogy was first made because today organizations are definitely under siege from a variety of attack methods. Most of them are obvious if you have someone on the walls (monitoring traffic). You can see the ammunition being fired from the trebuchets and mangonels and feel the walls shaking as they are pounding, again and again, by the large rocks (network layer attacks) hurled with great force. You might even notice a siege tower or two being hauled closer and closer to the walls in an attempt to get atop the walls, take out the archers that are waiting, and penetrate deeper into the keep's defenses – ultimately hoping to loot the keep (applications) and steal the treasure (data). In medieval times siege warfare could last weeks, months and even years. In the data center, attacks may not last as long but the impact of the modern digital siege - measured in downtime and dollars – can be just as devastating.

Interestingly, siege warfare became more interesting – and dangerous – with the introduction of mining. Mining was the process of digging tunnels underneath the walls surrounding the keep with the intention of weakening – or in later years destroying – its supports, thus bringing down the primary obstacle between the attackers and their intended target. In later years the men who were at first called simply miners became known as sappers and would eventually take on broader engineering tasks unsuitable for the typical siege warfare combatant. The trick for the defenders was to figure out where the sappers might mine the walls and prevent it - often by collapsing the tunnel before the attackers could do damage to the supports or walls.

In many sieges, the sappers were the primary means of breaching the walls. The rest of the attacks – the big stones, flaming pitch, and arrows coming from the main body of the army – were merely a distraction. A method of tying up the defender's resources while the real attack went (hopefully) unnoticed underneath the walls.

Modern attacks leverage much the same style of attack against the data center: the network and infrastructure-focused attacks are siege weapons, designed to detract you from the real attack that's going on at other layers of the stack.

BEWARE the APPLICATION LAYER SAPPERS



Now, the sappers today aren't actually attacking "under the floor" but like ancient sappers they are more focused in their attack and are definitely more dangerous to the health and well-being of the application. While the network is besieged by a variety of network-layer attacks, the sappers are going after the applications, using more modern and infinitely more difficult to detect methods of bringing it down. They're turning the application protocols against the application, using fewer resources to accomplish the same results.

The problem is that you can't ignore the siege and focus solely on the sappers, and neither can you can ignore the sappers and focus wholly on the siege. There needs to be protections up and down and across the data center that can detect and/or prevent such attacks from having an impact on the availability of applications and their supporting infrastructure. The wall does work, as long as it is strong enough and has enough resources (and intelligence) to be able to stand despite the barrage of attacks it experiences. We need to extend the wall up and down, to cover applications in a way that also makes them able to stand against attacks that would sap resources – regardless of how quickly that may occur. The motte and bailey, moat and keep, is no longer enough. You need to put into place protections at the application layer, as well, recognizing that it's not just about data theft but about resource theft. And while the former is more easily detected through the use of a web application firewall, the latter is more subtle and may go undetected. Protection from such attacks are necessary to prevent the rapid reduction in capacity that ultimately leads to outages.

Solutions capable of shielding the application from the impact of slow, transport and application layer attacks is just as necessary as being able to deflect network layer attacks. Multi-layer security is not a nice to have these days, it is a must have if one is to properly protect the data center from the increasingly hostile hordes attempting to bring down, take out and steal data from applications in the data center.

The term "sapper" is wholly fit to be applied to the application layer attackers today because what they're trying to do is "sap" the resources of an application and bring it down by slowly but surely consuming those resources, all the while undetected by the operators manning the data center walls. It's time to re-evaluate your siege plans and if necessary put into place those protections that not only deflect the attacks of modern siege weapons, but prevent the sappers from sneaking under the data center walls and taking out the application directly.

- The Many Faces of DDoS: Variations on a Theme or Two
- Spanish police website hit by Anonymous hackers (June 2011)
- What We Learned from Anonymous: DDoS is now 3DoS
- Custom Code for Targeted Attacks
- Defense in Depth in Context
- The Big Attacks are Back…Not That They Ever Stopped
- (IP) Identity Theft in Cloud Computing Environments
- If Security in the Cloud Were Handled Like Car Accidents
- F5 Friday: Multi-Layer Security for Multi-Layer Attacks
- Challenging the Firewall Data Center Dogma
- The "True Security Company" Red Herring

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com