**Why knock on the front-door and be noticed?**

Firewalls have now become the most basic protection small and large organizations deploy on their perimeter. Personal firewalls have also made it to mobile computing devices and are now available in Windows operating systems. IDS/IPS agents are deployed on end-points to detect and prevent intrusions. There is software now available which ingests activity data from such agents and there is smart analytics and AI available to monitor malicious activities. Most matured companies are already doing this as this is now table steaks. Attackers are not standing still and have found other ways on how to get steal data or cause chaos. Attacks via exploring vulnerabilities in open source software which in the last decade makes up a majority an executable is also has gotten on the radar of enterprise though there is not an easy solution yet to upgrade to the latest version of the library because of various technical challenges that development teams phase. Another form of attack which was in the news recently was related to crypto currency mining <<reference it here>>. With the adoption of open source and free software attackers are exploiting vulnerabilities in software and processes and looking at insiders to serve their purpose. Recall stuckten which shut down the reactors in Iran? That was not an attack which came through the front door but from inside by someone sticking a USB into a computer.

Hence, the next threat coming from software that users are able to install by bypassing Privileged Access Manager. To counter this threat, companies have taken away the admin privileges from users and only allow software be installed via an approval process by raising a ticket with IT Help Desk. However, the problem still exists because open source and commercial companies have started to provide software as zip files instead of installers to eliminate the friction faced by users not having to call helpdesk to install software. Unless the software updates the windows registry or privileged files on linux, users can simply unzip software they downloaded in their directory and start to use it. Even if security is scanning file names on disk, that can be easily bypassed by changing the name of the file so most scanners look for filenames on disk or process names in memory.

In today’s world, developers like to have freedom on what they want, when they want since they want speed to test their ideas or just to play with the next shining object. When you talk to developers they understand the risk but then expect security to solve the problem. Security has to be a partnership between development and security organization to mutually understand the risks and work out a balance which provides development teams the freedom to explore new software while keeping companies data and systems secure.

Maybe the pendulum has swung too far to the right where developers want freedom and expect security to find ways of mitigating the risks. To thwart the attempts by attackers to take advantage of this divide, technology and security need to work closely together.

There are options available to solve this problem such as allowing developers to have segregated sand boxes which are not connected to company network so that they can install and play with new software and innovate. Only when a technology has matured and risk mitigations are in place, software should be brought into the enterprise. The other is to have a list of approved software that companies publish which are well known to users from which they can select from. This will at least stop the likelihood of an honest user downloading software and bringing in a Trojan horse inside the company and becoming an insider threat. This will not stop a person with malicious intentions to install the software anyway. For that scanners need to evolve and search engines like google and bing can play a role.

Enterprise which store data such as people personal information, financial information or provide critical services such utilities, election devices, medical services etc which can threaten people livelihood, affect lives and cause chaos and affect political outcomes must start to consider third party software threats as attackers are not looking to knock on the front door to get in, they are findings ways to leverage people and systems which are already inside the company and baiting them to be their Trojan horse.