Vulnerability, Malware and Risk

Background

Information Assurance is crucial to functioning of any organization. The ability to assure availability, confidentiality and Integrity of information is critically dependent on the health of every system connected to the organization. A typical enterprise consists of a complex network of computers. Such network of computers is prone to risk from any of the end point system connecting to the network. A vulnerable system connecting to the enterprise network potentially puts the entire organisation to risk by being easy targets of cyber-attacks.

Most attacks use vulnerabilities in systems. These vulnerabilities are flawed pieces of code in the software that can, in principle, allow a malicious user to gain unauthorised access to a system. Given the complexity of software some of these vulnerabilities escape the most stringent QA scrutiny. Users and volunteer groups with constant vigilance detect and report these vulnerabilities.

An interesting question that arises is: How long does it take a vulnerable computer connected to the internet to be infected with malicious software? The answer depends on the OS the computer is running. In any case, it is matter of minutes to a few hours, with Unix systems typically holding out longer than Windows operating system. (https://isc.sans.edu/survivaltime.html).

Many service providers scan the network and provide a comprehensive report of the vulnerabilities existing in the end point systems. However, most of them do not take the next step of removing these vulnerabilities.

In this paper we talk about how to ensure the health of all the systems that connect to the network by removing any known vulnerability in them. Saner makes this process very simple, intuitive and fast. This keeps enterprises safe from many known attacks.

How Most Attackers Gain Access to a System

Providing Information Assurance invariably depends on preventing unauthorized access to the end point systems. Unauthorized access to the system and controlling the system is exactly what an attacker accomplishes by exploiting vulnerabilities in the system. This makes every system in a network a potential entry point for an attack.

Many complex applications run on end user computers. These software applications have vulnerabilities, weaknesses that allow potential attackers to use them to gain access to the system or cause unpredictable behaviour in the system. In this sense Vulnerabilities are the root cause for most malware attacks. It stands to reason that the systems with fewer vulnerabilities are more dependable. Every day, on an average about 30 new vulnerabilities are uncovered and published in the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search). The time between the publication of a Vulnerability and an attack using the vulnerability is a matter of days (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf). According to Center for Strategic and International Studies, “75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching” (http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf). For most of these vulnerabilities the application vendor provides a “Patch” – an update to the software that removes the vulnerability. By keeping the systems up to date with the latest software most of these vulnerabilities may be removed.

Anti-Virus Software and Residual Risk

Anti-virus (AV) software have been fairly successful in containing attacks. AV software use signature based detection of malware. They depend on the availability of the signatures or patterns that identify the virus as malicious code. While the dictionary of signatures is growing exponentially, attackers have devised clever ways of disguising their attacks to escape detection. Polymorphic codes that mutate when they execute in a host can potentially avoid detection. This can render AV software ineffective in detecting and blocking all malware attacks.

More importantly, AV software is designed to detect and act on an on-going attack and prevent them. They are also effective in removing the offending piece of code after the attack. But they are not designed to do effective prevention. Thus leaving unmitigated risks in the systems.

Patch – Remove the Vulnerabilities Before they can be Exploited

A software patch is a piece of code designed to correct a known problem in the Software. In response to uncovered vulnerabilities, software vendors correct the offending code and release an update in the form of a patch. When the software is updated the vulnerability is removed. Sometimes patching applications as soon as a patch is made available becomes important. This is especially important when critical patches are released by a software vendor. The availability of a patch can provide the information that attackers may use to write an exploit. This could shorten the time to attack after a vulnerability is uncovered and a patch is available. The safest way to mitigate the risk of an attack is to patch the system immediately.

Challenges of SW Patching

Patching and keeping applications up to date is unquestionably important. However, the fact is that a significant percentage of computers are running unpatched OS and applications. Most successful cyber-attacks target unpatched systems in the network. Why then are so many systems still unpatched? Individuals may not be equipped with the knowledge or skills to accomplish effective patching. However, the patching process in an enterprise may be quite complex.

In "Guide to Enterprise Patch Management Technologies", (http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf), NIST lists a few of these challenges:

- SW Inventory management – Having an up to date inventory, with complete information about the installed version of all the software in each of the systems connected to the enterprise is important. But it is a challenging task.
- Resource Overload – Software vendors release patches either bundled with many issues resolved in one, or if the issue is critical and likely to have a major impact they may release one off patch. In either case, the network bandwidth is likely to be choked with many systems downloading the required patches.
- Installation Side Effects - The applied patches may alter some security configurations. Organizations should be able to identify these and remedy them for effective vulnerability management.
- Effectiveness of Patching – Patches often require that the patched software be re-started or the entire system be re-started. They are ineffective unless this step is completed. Knowing that the applied patch has been effective is crucial and needs to be ascertained.

In addition there are a few other points that can complicate the patching process in an enterprise

- Risk assessment and prioritization – Not all vulnerabilities pose the same level of risk. Given that the patching process in an enterprise can be elaborate, a judicious choice of patches will be necessary for optimal operations. This prioritization It is important to know vulnerabilities and the risk posed by these vulnerabilities to an organization which helps prioritizing what patches to apply, how critical they are.
- Knowing what patch to apply - Once the risks are identified and prioritized, the task of identifying the appropriate patches to apply can be time consuming.

How Saner Accomplishes Vulnerability Mitigation

At SecPod we believe that a stitch in time saves nine. While Malware detection and cure products are still an important tool in an enterprise, they can only do a partial job. Saner identifies and removes vulnerabilities before they are exploited by attackers. With continuously updated vulnerability data the repository helps us ensure that all known vulnerabilities are detected and a patch is available to specifically address the vulnerability.

How Saner Addresses Common Challenges

Saner runs an agent on each of the end point systems. This helps track all the applications running on any end point system. With this architecture Saner does not need to have a central repository of all systems and the software running on them. Saner takes care of applying the patches to any known vulnerable software on the system. This overcomes the Inventory Management problem alluded to earlier.

When a patch is required, every end point system will need to download the patch from either the internet or the intranet. Connecting to the internet to download patches can mean choking of the enterprise band width. Saner overcomes this by allowing enterprises to have an in house deployment. This allows the server to download the required patch once and allow the end users to get the required patch from this in-house server. This avoids multiple downloads. The individual systems will still use the intranet bandwidth to download patches. However, the intranet bandwidth is usually high enough to withstand this amount of network traffic.

Another potential problem faced by enterprises is the alteration in configuration values introduced by new patches. This is handled by Saner by checking for misconfigurations. For example, if an application is set to start automatically by default, but the enterprise policy is to prevent auto start. Saner ensures that if any alterations violates the organisation policy it is detected and fixed. Such checks are made after a remediation is done to ensure that no misconfigurations exist in the system.

After applying a patch, some applications require either a restart of the application or the OS. If the system is not restarted the patch is not effectively applied. Saner performs a scan immediately after the remediation (patching) is done. If the patch is not properly applied it shows up in the console as a vulnerability.

In an enterprise, it may not always be practical to remediate all the vulnerabilities. Saner identifies vulnerabilities and provides information on the risk that they pose. The IT manager can make a determination of the threat posed by examining the severity of the vulnerabilities. Decisions on applying the patch can be made, armed with this information, available in Saner dashboard.

Identifying the appropriate patch to apply is automated in Saner. This ensures that no extra time is required to identify the correct patch to apply; choosing which patch to apply is a matter of a few mouse clicks.

Conclusion

Anti-virus software provides a means of identifying threats in an enterprise, but they are not 100 % effective on their own. Often they are unable to detect the malware before the damage has been done. In that case, Anti-Virus software can help in containing the virus and minimising the damage caused. To a large extent Anti-Virus software is a reactive approach.

At SecPod we believe that prevention is better than cure. Our conviction that if vulnerabilities are removed from the system – we will be able to prevent the attack from happening. This can go a long way to provide confidence in the Confidentiality, Integrity and Availability of the information in an enterprise. We do not claim that Saner is replacement for Anti-Virus software. Robust security necessitates many layers of defence. While saner is the first line of defence, preventing the exploitation of vulnerabilities, Anti-virus software will act as a second line of defence. In such cases, Anti-Virus software will be effective.

A large number of attacks can be prevented by using Saner. Saner in combination with enterprise Anti-Virus software is a much more effective solution to prevent damages from Cyber-Attacks, than using an Anti-Virus Software alone.