Secunia
Stay Secure

Cybercriminals do not need administrative users

Stefan Frei
Secunia Research Analyst Director

07-04-2011

For years the software industry has promoted reduced privileges for user accounts as a key security best practice to prevent misuse and successful exploitation of end-point systems. There are two main rationales/assumptions that back up this strategy: A) malware requires administrative access to successfully exploit and compromise a system, and B) users without administrative access are prevented from bypassing the organisation's security policy as they cannot install and run unauthorised programs on their own.

Problem

Unfortunately, user accounts with reduced privileges do not provide protection from attack, misuse, or compromise. Reduced privileges for end-users can only be regarded as one part of an effective security strategy that should not be solely relied on. Organisations should know the limitations of this approach to prevent them from getting a false sense of security and under-investing in complementary security layers. This paper discusses the limitations of security by denying users administrative access to their systems, and highlights how cybercriminals can achieve their goals without administrative access.

In any organisation, staffs work on their end-points to carry out daily tasks. By definition, and irrespective of the privileges they are granted on their systems, they need and have access to all business relevant data and internal networks required to get the job done. Thus, even when working with reduced privileges, any program or process running with the same set of privileges also has full access to all of this data. This very fact highlights that the valuable information which cybercriminals are eager to "acquire" is present regardless of users' privileges and justifies cybercriminals' interest and investment in finding ways to compromise end-users' systems.

Attack Surface

In every organisation, the number and complexity of pre-installed programs and plug-ins found on typical end-points alone provide plenty of opportunities for attack and compromise. Running as a non-admin user mainly helps to limit what a user can install and configure on the system, it does not prevent an attacker from gaining control of the user's account. A single exploitable vulnerability in one of the many installed programs (or plug-ins) is all cybercriminals need to run their malware in the context of the local user. Furthermore, as the user has access to the internal network, the malware can use the user's account to relay attacks against other systems.

Recent research shows that the number of vulnerabilities affecting typical end-points (with Microsoft Windows XP and the Top-50 most prevalent programs installed) increased from 225 in 2007 to 729 in 2010. From 2009 to 2010 alone a more than 70% increase in the number of vulnerabilities affecting typical end-

points was recorded[1]. This represents an enormous opportunity for cybercriminals and also helps explain why up to 9% of the end-points in large enterprises were found to be bot infected, despite the implementation of best of breed security policies and perimeter protection[2].

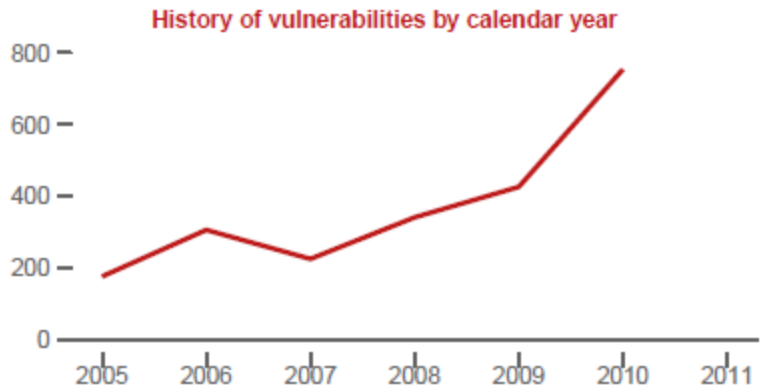

Figure 1. The number of vulnerabilities affecting a typical end-point with Windows XP and the Top 50 most prevalent programs increased from 225 in 2007 to 729 in 2010, or by 71% in the last year

Furthermore, many of the vulnerabilities are of the "Privilege Escalation" type that allows the attacker to gain elevated privileges, thereby nullifying the protection sought in restrictive user permissions. In 2010, about 14% of the vulnerabilities affecting a representative end-point with Windows XP and the 50 most prevalent programs installed were of this type. Exploiting this type of vulnerability allows an attacker to escape the stringent permissions of the user and execute its code with administrator or system privileges.

No Installation Required

The fact that many programs do not need to be installed or require administrative privileges to be run on an end-point is often overlooked. For example, there is a growing list of so-called "Portable Applications"; programs that do not require installation. The user simply starts the program after

No need to install …

An increasing number of programs can be **executed without prior installation**. The majority of 200+ programs offered on PortableApps.com do **not require administrative users** to run.

[1] Secunia Yearly Report 2010 - http://secunia.com/company/yearly_report
[2] Damballa on Darkreading - http://bit.ly/EntBot

downloading it from a USB stick or a Flash drive. PortableApps.com for example, features more than 200 types of programs (productivity, networking, instant messaging, file sharing, graphics, games, etc.) that can be executed without requiring any installation. Most of these programs do not even require administrative rights to run. Furthermore, there are many tricks that allow users to bypass restrictive user rights to run and install programs on their own. There is a rich body of step-by-step instructions on the Internet that shows users how to bypass user restrictions to run their own programs.

End-Point Exploitation

Over recent years, and in the face of more restricted environments, cybercriminals have developed successful technologies and strategies to make exploitation and system compromise independent of administrative access on end-points. An increasing number of recent exploits and malware does not require modifying a system file or the registry; just running in memory is sufficient to access and steal sensitive information or infect other internal systems. For example, hijacking browser traffic or communicating with an external host for data exfiltration does not require administrative access. Malware does not even need to be persistent and survive a reboot. A couple of minutes on the end-point are enough for malware to identify and steal most of the sensitive data, and for it to spread further. Additionally, today's end-points are typically left powered on for extended periods of time between reboots, thereby decreasing the need of the malware to take extensive action and privileges to stay persistent. Zeus or Carberp are good examples of recent and prevalent malware that are able to compromise a host without administrative rights[3]. .

Conclusion

Limiting users' privileges on end-points is a recommended and effective means to reduce the risk of host exploitation and limits the capabilities of malware upon successful compromise. However, it should not be seen as a replacement for vulnerability management and expedited patching of software, nor is it a replacement for anti-virus or other protection technologies.

These days, cybercriminals systematically obfuscate malware to bypass anti-virus and other defence technologies with increasing success by creating a large number of obfuscated serial variants[4]. Limiting user privileges on end-points is a best practice to complement, not replace, additional layers of security. A

[3] Damballa on Darkreading - http://bit.ly/EntBot

[4] NSS Anti-Malware Group Test Report 2010/Q3 - http://www.nsslabs.com/research/endpoint-security/anti-malware/consumer-anti-malware-products:-group-test-report-q3-2010.html

process to identify vulnerable programs, including programs not authorised by the organisation, paired with effective patch management is an absolute must to reduce the window of exposure and eliminate the root cause of potential compromise.