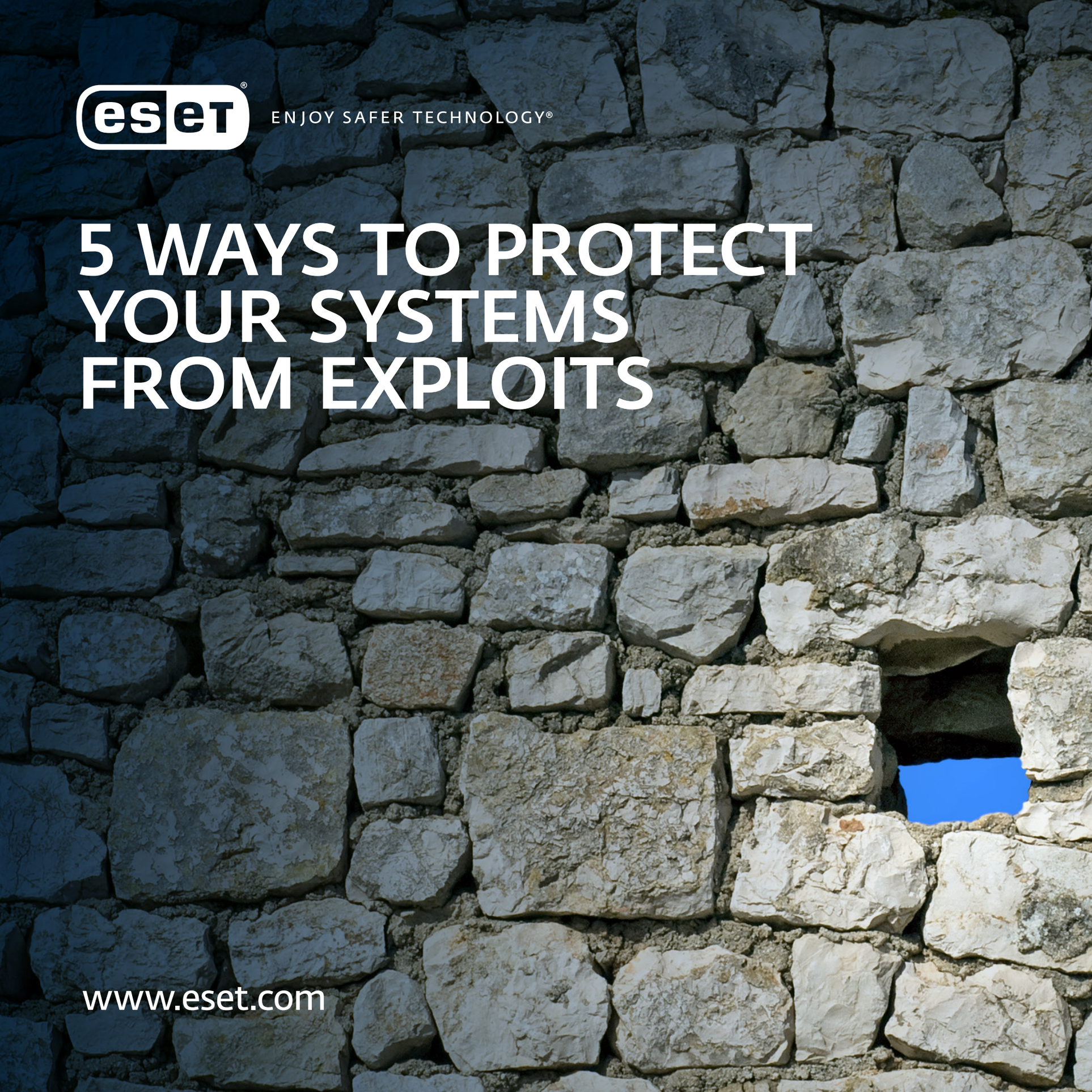
ENJOY SAFER TECHNOLOGY®

# 5 WAYS TO PROTECT YOUR SYSTEMS FROM EXPLOITS



www.eset.com

# 5 ways to protect your systems from exploits

By Michael Aguilar, Business Product Technical Lead, ESET North America

With the rising tides of ransomware eating up much of the newsfeeds, we are also being reintroduced to an accompanying friend of malware: exploits. While they are different, the two can seemingly go hand in hand depending on the threat you may have just incurred or behaviors you may be seeing on your system. An exploited machine may not be infected, but it can be leveraged to affect or infect every machine in your environment if the vulnerabilities in the network are not properly controlled.

## What is an exploit?

An exploit is a weakness in an underlying application, application implementation, OS, or other aspect of the machine itself that can affect the system and make it vulnerable. In short, it is a weakness that is leveraged against you. The following should help align where these items fit in the topography of an attack:



- A vulnerability is a weakness in a piece of your computing infrastructure.
- Risk is what is incurred due to the vulnerability existing, and it can be mitigated, accepted, or ignored depending on the feasibility that it will be exploited.
- An exploit is taking advantage of a vulnerability, and thusly causes the business to suffer from exposure due to the exploit being utilized.

With computers, there are system-level and application-level exploits that can be used against a machine. For example, a system-level exploit could overtake the RPCSS service via a buffer overflow attack with machines running English Windows 2K, Windows 2003, and Windows NT 4.0 SP3-6a. Meaning machines running these OS versions, the RPCSS service has a weakness that allows commands to exceed the memory allocation for that process and insert commands to run in other memory space.

With application exploits, weak code is discovered by checking the source code for vulnerable libraries or through the use of techniques such as ***fuzzing***. Fuzzing is the semi-automated or automated testing technique that takes random or invalid data and runs it through the input of an application, checking the application for unexpected crashes or possible memory leak

and buffer overflow vulnerabilities. A few recent attacks have targeted Java applications. Every time an "update Java" prompt is clicked to ignore, you open yourself up to have the Java application exploited by unknown attackers. Many advanced attacks pertaining to exploit kits rely on this method. Clicking on a site that is affected by an EK, like the *EC Council Site* was, relays the information regarding your down-level Java to their servers, allowing them to send an encrypted package to the machine. This in turn will bypass Java's security feature, handing the keys of your computer to an attacker.

So, in short, an exploit is a hole in your armor that is used against you. The vulnerability is the hole, and the risk is that it is exposed. So, what do you do now?

## How do you protect yourself from exploits?

Just install one application and you are SET! If only it were that easy. Much of the prevention of these kinds of attacks exploiting your systems is knowing your environment and controlling it. There are many technical controls that can be applied to your systems to help prevent them from getting exploited due to vulnerabilities:



1 **Patch management**—The easiest way to fill a security hole is to take the hole away. Knowing what you are patching is key, as you do not want to take down the entire network. So plan appropriately.

   A *Applying patches regularly helps prevent issues and reduce exposure risk by removing the vulnerabilities that can lead to exploitation. Items like Java, Flash, Adobe, and Microsoft applications, including the operating system, need to be updated regularly. This can be handled via Windows Update Services from an MS server or another third-party application. For UNIX/Linux systems, you can use Chef, Puppet, or a third-party tool like Lumension.*

2 **Rate your patching by how critical it is to the business and operations.**

   A *If an item cannot be patched, then the business must accept the risk to exploitation.*

   B *Have a reversion plan in case a patch breaks something. You will always sleep better if an action can be undone in your environment.*

3 **Decommissioning older legacy systems**—I know some still have that one legacy application that NEEDS the Windows 2000 server to run; however, even having an OS that vulnerable in the infrastructure is not great, especially if you re-use passwords (as many do). Getting access to this machine can wreak havoc, as passwords can be dumped and file-system access can be used if there are any mapped drives.

4 **Review created/homemade/specialty applications**—Depending on your business, you may use in-house self-created applications OR have a vendor create applications for you. If this is the case, please ensure that the code used is solid and not able to be exploited. This is where having someone who can interpret the code or create the application in-house would be best. They can then review the code structure to ensure that the application cannot be exploited due to the use of vulnerable components found in the C programming library, such as **strlen()** (string length) or **strcopy()** (string copy).

   A *If running Windows Server, review and apply the items located in this Microsoft article pertaining to baseline hardening of the Windows Server OS:* *https://technet.microsoft.com/en-us/library/cc526440.asp*

   B *If using Unix/Linux, you can follow this SANS guide to hardening the Linux/Unix OS:* *https://www.sans.org/media/score/checklists/linuxchecklist.pdf*

C *If predominantly using an OS X site, these few resources, one provided by Apple, though it pertains to the 10.6 builds, can still be followed to apply to newer builds: https://www.apple.com/support/security/guides/*

**5 Install security applications on endpoints to protect against network and system level exploitation.**

A *A security product with an IDS/IPS solution will prevent traffic from being exploited like in a MITM (man in the middle) attack or DNS redirect.*

B *Having any type of antivirus application normally will stop many attempts at application exploitation via malicious executable code, scanning the obfuscated code or identifying it once the code is exposed at runtime.*

Preventing your systems from being exploited requires planning and configuration to ensure that the patching will go smoothly and not accidentally bring down aspects of the environment. Using ESET security systems or any system like ours that has an exploit blocker included is one giant recommendation that I would make. The *Exploit Blocker* technology in the ESET applications monitors existing applications and Microsoft components, ensuring that no malicious behaviors take place. If a detection is triggered due to an application acting suspicious, the threat is blocked immediately with information sent to our Live Grid systems to possibly stop the attack on other systems across the world.

**Evaluating endpoint security solutions?** Learn what to consider, including independent testing firms' recommendations, the cost of false positives, usability and more, in this *tech brief*.

*Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via Coursera.org. He is currently responsible for working with large-scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.*

*For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.*

ENJOY SAFER TECHNOLOGY®