REAL WORLD ENTERPRISE SECURITY EXPLOIT PREVENTION TEST 2014

by MRG Effitas

WHY THIS TEST IS RELEVANT TO ENTERPRISE CUSTOMERS?

This test focuses on how effectively corporate endpoint security products can protect against exploits delivered via drive-by download techniques that are commonly used in Advanced Persistent Threat (APT) attacks.

Traditional protection techniques are not always able to protect against these threats. This is especially true of zero-day vulnerabilities – newly discovered flaws in popular software which do not have a ready solution. Signature-based methods rarely enable security vendors to spot exploits which target these 'unknown' loopholes. Complex exploits also have a large arsenal of techniques which can bypass or overcome proactive protection technologies. And if just one exploit slips through the layers of traditional defenses, the consequences could be enormously damaging. So it's vital to protect the enterprise against attack by deploying an exploit-specific layer of security.

SOME EXPLOIT TECHNIQUES

Drive-by download exploits carry an extra risk; no user interaction is required to run the malware on the victim machine. Test results confirm that individual machine security can be readily compromised when visiting even legitimate websites or web resources, which may have been deliberately infected to target the specific enterprise. This type of attack can also be combined with spear-phishing to form a so-called 'watering-hole' attack (read more here).

Today, exploiting vulnerabilities in legitimate programs is one of the most widespread methods of infecting computers. Java-based exploits are especially popular among organized criminals, because traditional protection methods based on memory corruption are not effective against Java exploits. Outdated Java runtime environments are very common in enterprise organizations because enterprise-level Java applications may be not compatible with the latest JRE versions, so can't be upgraded to new versions which would plug known vulnerabilities (read more vulnerabilities statistics in securelist.com here).

Another trend is to attack using ready-made 'exploit packs' greatly increasing the probability of penetrating the target system by fielding multiple exploits that simultaneously attack vulnerabilities in different popular applications, (more information can be found here).

WHAT WAS THE GOAL OF THE TEST?

Endpoint security solutions are usually considered the ultimate barrier against these attacks, so effectiveness of their technologies in protecting against exploits is important. For this reason, the MRG Effitas test organization tested the ability of enterprise-class endpoint security products to prevent drive-by exploits when installed on a Windows endpoint.

WHICH PRODUCTS WERE TESTED?

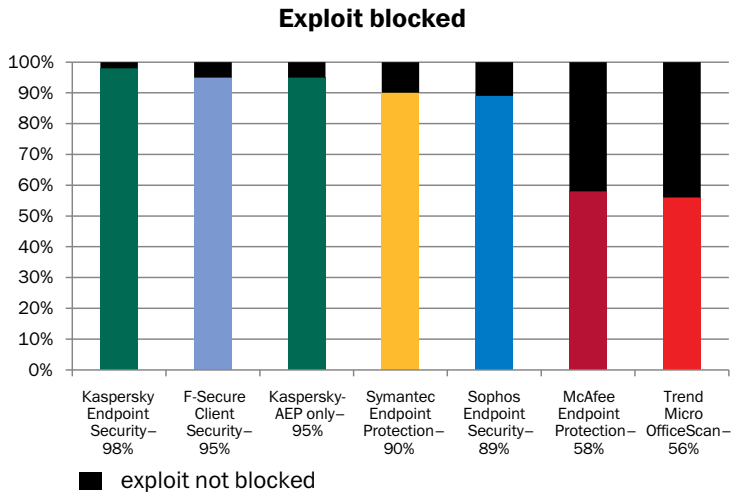
In total, six products were tested:

- Kaspersky Endpoint Security, in 2 configurations:
  - full featured as standard
  - with only Automatic Exploit Prevention enabled
- F-Secure Client Security
- Symantec Endpoint Protection
- Sophos Endpoint Security
- McAfee Endpoint Protection
- Trend Micro OfficeScan

Please consult the report for configuration and version details.

KASPERSKY LAB PRODUCT PERFORMANCE

The top score for any product was a theoretical 100% of exploits blocked. Kaspersky Endpoint Security was able to come very close to this. With full functionality deployed, Kaspersky Endpoint Security blocked 98% of exploits. Kaspersky Automatic Exploit Prevention, enabled in isolation, blocked 95% – confirming the value of this specialized module in combating these threats.



WHAT DOES THIS SCORE REALLY MEAN?

The results presented in this report confirm that Kaspersky Endpoint Security offers the efficient protection against variations of the most dangerous exploits commonly targeting enterprises. Kaspersky Lab's Automatic Exploit Prevention technology significantly reduces the risk of sophisticated targeted attacks that exploit vulnerabilities.

TEST SOURCE

The report is available here.

WHERE CAN I FIND MORE INFORMATION ABOUT AUTOMATIC EXPLOIT PREVENTION?

More information about Automatic Exploit Prevention technology can be found here.

WHAT IS THE MRG EFFITAS TEST ORGANIZATION?

MRG Effitas is a UK-based independent IT security research organization which focuses on providing cutting edge efficacy assessment and assurance services. MRG Effitas began when the "Malware Research Group" was formed in 2009 and rapidly gained a reputation for being the leading efficacy assessor in the browser and online banking space due to increasing demand for its services.

For more information about how to purchase Kaspersky Security of Business solutions including Automatic Exploit Prevention, please contact to your reseller.

KASPERSKY lab