Gartner Research

Publication Date: 29 November 2010 ID Number: G00209087

Advanced Evasion Techniques: Weapon of Mass Destruction or Absolute Dud?

Bob Walder

Researchers working for the Finnish security company Stonesoft claim to have discovered new techniques that bypass current security systems and that cybercriminals could use to gain access to internal protected assets of many companies.

Key Findings

- Evasion techniques are applicable to passive network scanning (intrusion detection systems or IDSs) and in-line protection only (intrusion prevention systems or IPSs, and next-generation firewalls or NGFWs).
- Evasion techniques are well-known and have been a constant threat for more than a decade.
- In creating advanced evasion techniques (AETs), traditional evasion techniques have been extended and combined to create evasions we have not yet seen available in commercial testing tools, although the techniques themselves have been in use in the security testing industry for several years.
- Some IPS/IDS/NGFW vendors are no better at handling evasions today than they were when they released their original products. This is demonstrated in independent tests.
- It has been determined via independent testing that some of the new combinations discovered are capable of evading certain market-leading IPS devices, thus increasing the risk of compromise for users of those devices.

Recommendations

- Although the evasion threat is very real, panic is unwarranted, despite the hype surrounding the "discovery."
- Use independent test reports to determine which vendors are capable of handling evasion techniques effectively.
- Ask questions of the vendors of products you have already deployed or are considering for your next NGFW/IPS/IDS, insisting that they prove they have effective anti-evasion techniques in their products.

- Determine which anti-evasion techniques are available on devices in your network, and then activate them, despite any potential performance impact.
- Be vigilant with patching processes. A functioning exploit is required in order to take advantage of evasion techniques, and if the target system is patched against the vulnerability, no amount of evasion will help.

WHAT YOU NEED TO KNOW

So-called AETs represent nothing more than an evolution in existing and well-known evasion techniques. This is not to say that they are not a threat — organizations should ensure that their in-line and passive detection devices are capable of effectively normalizing network traffic prior to inspection in order to neutralize evasion attempts.

EVENT

Event Facts

On 18 October 2010, researchers working for the Finnish security company Stonesoft announced the discovery of what they referred to as "advanced evasion techniques" (AETs). By extending and layering known evasion techniques, they have created combinations that have not previously been seen in commercially available test tools, although many of the techniques have been in use for several years in the security testing community via custom-designed tools. It has been determined that some of the new combinations discovered are capable of evading certain market-leading IPS devices, thus increasing the risk of compromise for users of those devices.

At present, Stonesoft is proceeding with a responsible disclosure process, having already notified the Finnish Computer Emergency Response Team (CERT-FI), the affected vendors and other vendors of in-line security devices.

Analysis

Gartner believes the danger of AETs has been overhyped, although the danger of evasion techniques in general needs to be addressed by enterprise intrusion prevention programs.

AETs exist, although they are an extension of an existing threat category, rather than a brand-new one. The issue faced by users is that many in-line security devices — IPSs in particular — have demonstrated consistently in independent tests that they are incapable of handling effectively the traditional forms of evasion that have been known since 1997/1998. The evolution of evasion techniques at this time is only going to enlarge the "threatscape," and Gartner believes that some security vendors will evolve their products to deal with new evasion approaches, and some will not. The key is making sure enterprise defenses evolve appropriately.

For casual hacking by nontechnical attackers using toolkits and prepackaged attack tools, evasion techniques are not widely used (although a number of the more-advanced/expensive "blackware" tools include evasion techniques). For those involved in targeted attacks, however, the techniques have been in common use for several years.

Evasion techniques are not, in and of themselves, exploits. Any attacker would need a functioning exploit that is already proven to work against the target host. If the host is unpatched and the in-line defenses (IPS/NGFW) have no appropriate signature, the exploit will be successful. If the IPS/NGFW has a signature covering the exploit, then it will be blocked.

This is the point where sophisticated attackers will begin to consider the use of evasion techniques. Having noted that the exploit was blocked, the attacker will then begin to use the same exploit, coupled with one or more evasion techniques, to disguise the exploit and render it invisible to the IPS/NGFW inspection engine. Such an attack will often be successful, since so many IPS engines fare badly against even the most basic evasion techniques. Gartner clients are advised to examine independent test reports from security testing organizations, such as ICSA

Labs or NSS Labs to identify those systems that are currently ineffective against evasion techniques.

Note that, if the target host has been patched against the exploit, then no amount of evasion will help. This is the key differentiator — evasion techniques are only effective as a "cloaking" mechanism to effect the delivery of an exploit through an NGFW or IPS to the intended target. Once that host system is patched against a particular vulnerability, however, it is safe.

Note that all evasion techniques are applicable to passive network devices (IDS) and in-line protection (IPS/NGFW) only, and do not help bypass more-rigorous endpoint protection systems.

It is important to recognize that users of in-line perimeter security products are at no increased disadvantage now than they were before the "discovery" of AETs. Devices that fared poorly in anti-evasion tests before will still fail against AETs. Some of the new layering techniques may cause problems for devices that could previously handle individual techniques, but Gartner expects this issue to be corrected rapidly by those vendors that have traditionally taken anti-evasion seriously.

Gartner clients are advised to review current deployments and planned refresh of in-line and passive network-based security devices such as IDS, IPS and NGFW. Ask vendors tough questions about their ability to handle evasions, and about AETs in particular. Insist they prove they have effective measures in place, in your own network, under your control, or in an independent test lab under the control of a trusted third party, but NOT in the vendor's own test labs.

Evasion techniques are a meaningful threat, and Gartner advises enterprises to use the publicity surrounding AETs to demand that security vendors begin taking evasion testing more seriously than they have in the past.

RECOMMENDED READING

"50 Ways to Defeat Your Intrusion Detection System," Fred Cohen, 1997

"Insertion, Evasion,and Denial of Service: Eluding Network Intrusion Detection," Thomas H. Ptacek and Timothy H. Newsham, January 1998

"Defeating Sniffers and Intrusion Detection Systems," horizon, Phrack Magazine, December 1998

Gartner

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner