

Anti-evasion

Background

As part of daily research and development work, Stonesoft vulnerability experts were experimenting with the latest and most advanced network security threats in StoneLab. One of them is the threat of evasion techniques. Deep packet inspection, traffic normalization and evasion detection are already standard functions of network security systems and testing procedures. Current research and testing methods for evasion techniques are based primarily on publicly known evasion tools (e.g. Metasploit, CORE IMPACT®, CANVAS®). Evasion techniques have been considered a very difficult and time consuming area of R&D. Since clear, tangible evidence of evasion techniques in the real-world has been lacking, it has also been challenging to explain the threat in a meaningful way. Part of the reason for this difficulty is that current security technologies offer a very low level of detection and visibility.

These challenges gave Stonesoft reasons to investigate evasions further. Our experts challenged all the dominant rules, principles and thinking in order to generate more insightful knowledge of evasions. It is likely that many will try to ignore evasions, saying this threat is only theoretical and not real. Unfortunately those who choose this route run the risk of becoming a target. Or are already a victim.

Evasion

Evasion techniques are a means to disguise and/or modify cyber attacks to avoid detection and blocking by information security systems. Evasions enable advanced and hostile cyber criminals to deliver any malicious content, exploit or attack to a vulnerable system without detection, that would normally be detected and stopped. The security systems are rendered ineffective against such evasion techniques, in the same way a stealth fighter can attack without detection by radar and other defensive systems.

Use of evasions

If someone really wants to execute a targeted cyber attack knowing that the networks are well protected, they need evasion techniques to improve the success rate. Evasion techniques work like a master key to anywhere, and offer time to find an exploit that works. In the case of highly advanced attacks, a working evasion technique offers good insurance against getting detected and caught. So it pays off if the stakes are high, as in the case of financial or business data, warfare, terrorism, or political attacks. Unexplained and mysterious data losses, system crashes and financial data thefts occurring without any detection or explanation given by the security devices are clear candidates for evidence of evasion techniques. That makes it an even more severe threat because if you cannot detect, you cannot protect.

By knowing all the benefits of using evasion techniques it is a bit naïve to think that advanced cyber criminals and hackers are not using evasions or that they are using only publicly known techniques or tools.

Research breakthrough

We made a decision to invest time, money and effort to research evasions. We took a radical approach and challenged:

- Use of the operating system's TCP/IP stack
- Conservative sending & liberal receiving rule (RFC 791)
- Using evasion techniques only one at a time
- Considering the lower levels of the TCP/IP stack static and thus well protected against evasion techniques

After developing a test environment and needed research tools we had a breakthrough. Stonesoft vulnerability experts discovered a new species of advanced evasion techniques (AETs). These AETs have been demonstrated as real, and are considered serious by independent security experts and test labs. This discovery has been reported by Stonesoft to security authorities (CERT-FI, US-CERT and CERT/CC) and through their coordination to all affected vendors. There is hard evidence, live demonstrations and experimental research data that these AETs work in reality and can bypass 99% of current security devices without leaving any traces. That makes the threat worth everybody's full attention.

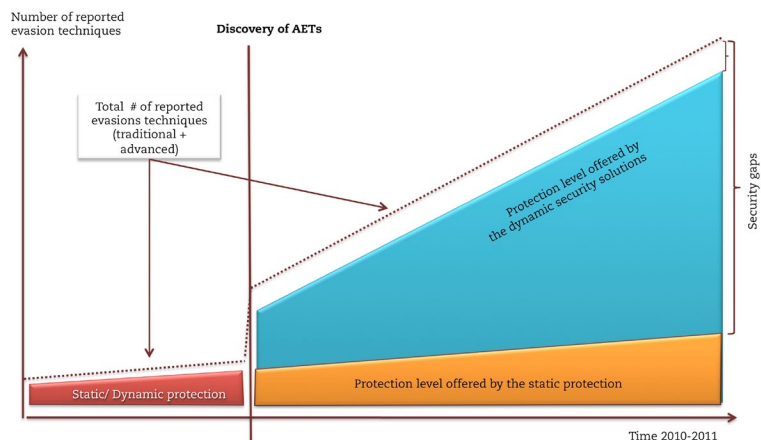
Implications

- Digital assets are unprotected.
- Everyday operations and businesses may well be at risk without knowing it.
- The false perception of being safe makes organizations an easy target.
- The vast majority (99%) of current security appliances are unprepared and unable to give appropriate protection.

Can we strike back?

The immediate course of action is to increase the knowledge about AETs at www.anti-evasion.com, and then evaluate/audit all the critical digital assets (data and operational systems) and servers that are hosting those assets. After that, organizations need to protect critical servers with anti-evasion ready security solutions that are designed, built and tested from the ground up to provide dynamic protection against traditional and advanced evasion techniques. Migration to dynamic security becomes relevant as the need and speed of updates against AETs increases exponentially.

Estimated increase of reported evasions and protection levels (dynamic vs. static)



Advanced Evasion Techniques (AET)

What is new? Advanced evasion techniques can be altered or combined in any order to avoid detection by security systems. AETs are, by their nature, dynamic, unconventional, virtually limitless in quantity, and unrecognizable by conventional detection methods.

They can work on all levels of the TCP/IP stack and work across many protocols or protocol combinations.

The amount of new AETs is growing exponentially, and thus they create an everlasting and ever-changing challenge for the information security industry and organizations around the world.

Anti-evasion ready

Anti-evasion ready solutions are software-based, and can be updated automatically, remotely and effortlessly from a central management center. Anti-evasion ready appliances need to be capable of receiving current AET patches and security updates continuously. Such solutions must have the capability in their core functionality to detect, flag and report evasions via a central management client.