STONESOFT

Advanced Evasion Techniques (AET)

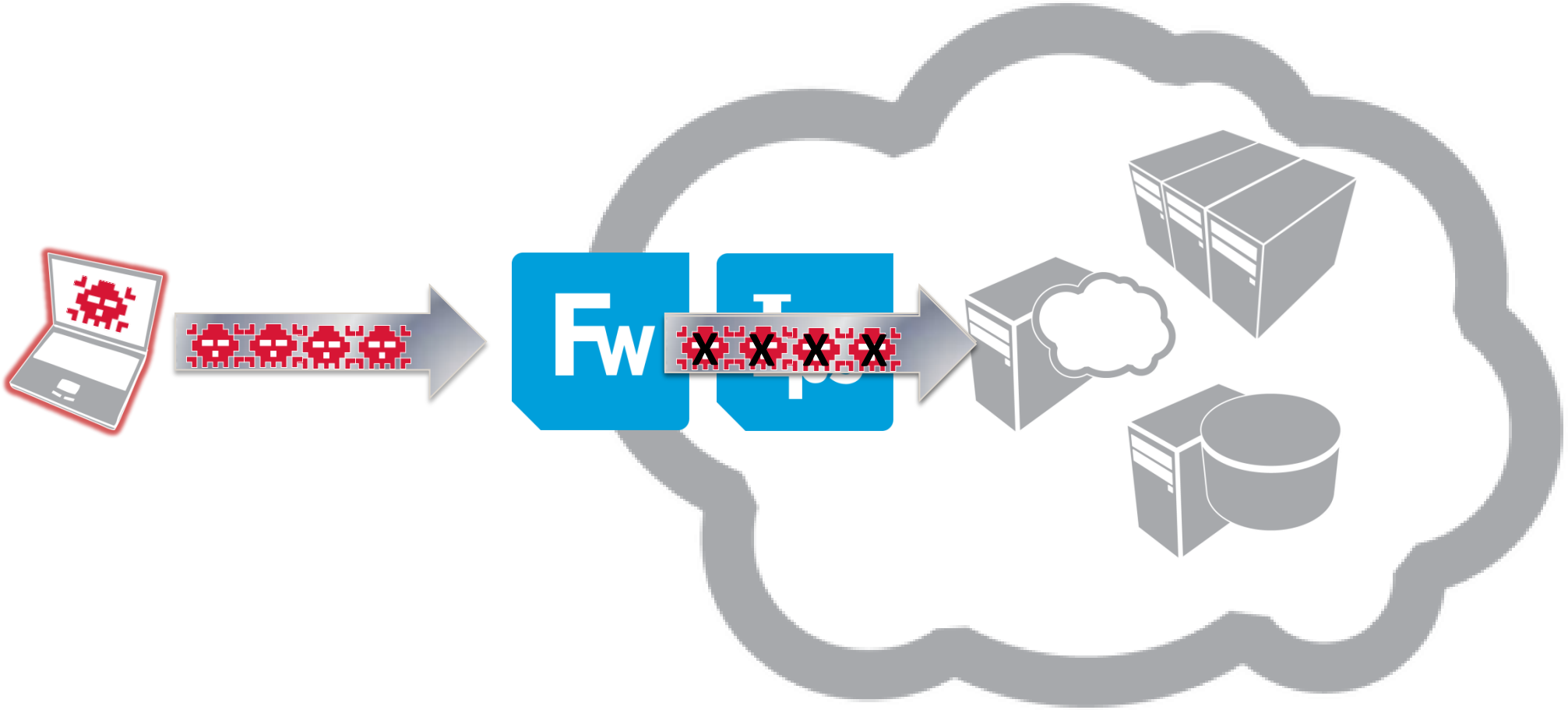
Are they being used to bypass your security?

Alan Cottom – Solutions Architect, Stonesoft

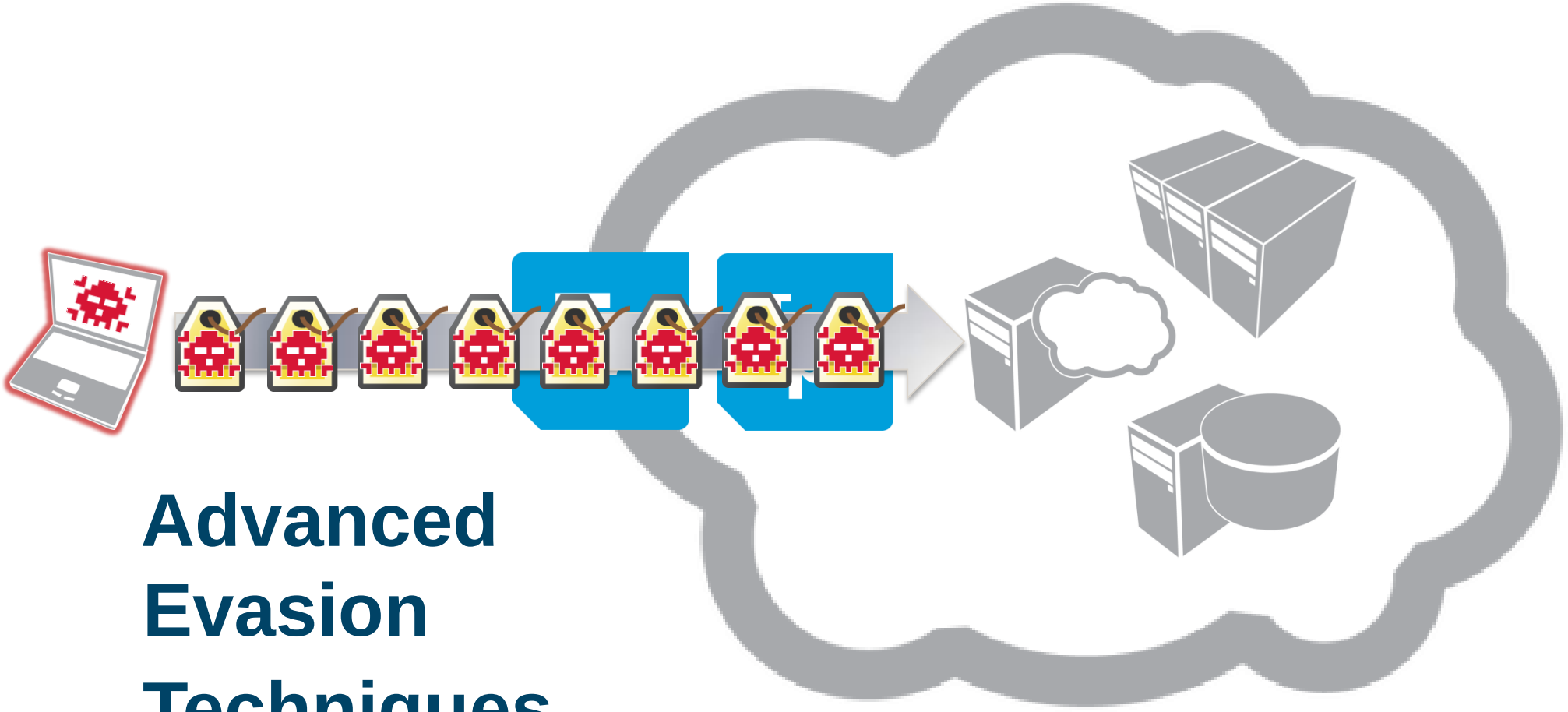
Stonesoft

Global Company	Customer Focus	Innovation
A Global Security Company, in business since 1990	Operations in USA, EMEA and Asia	Integrated network security and business continuity solutions
Listed in the Helsinki stock exchange (HEX)	Global 24/7 support Customers in more than 70 countries	R&D Teams in France, Finland & Poland
Corporate HQ in Helsinki, Finland	Focus on customers requiring advanced network security and always-on connectivity	Multiple Patents for core technologies

It’s OK, we’re protected.

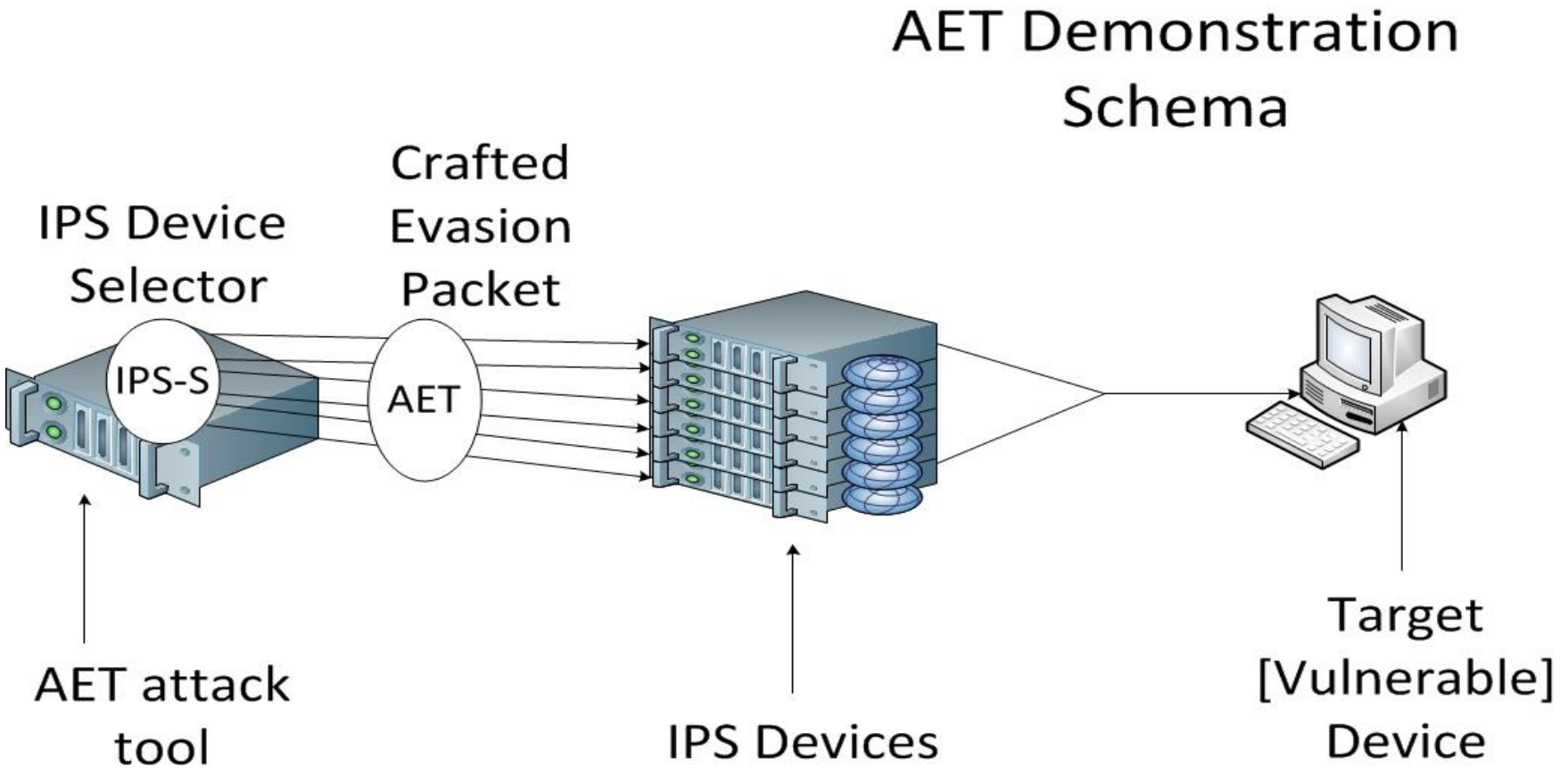


Are you sure?



Advanced Evasion Techniques

AETs in action



AETs in action…

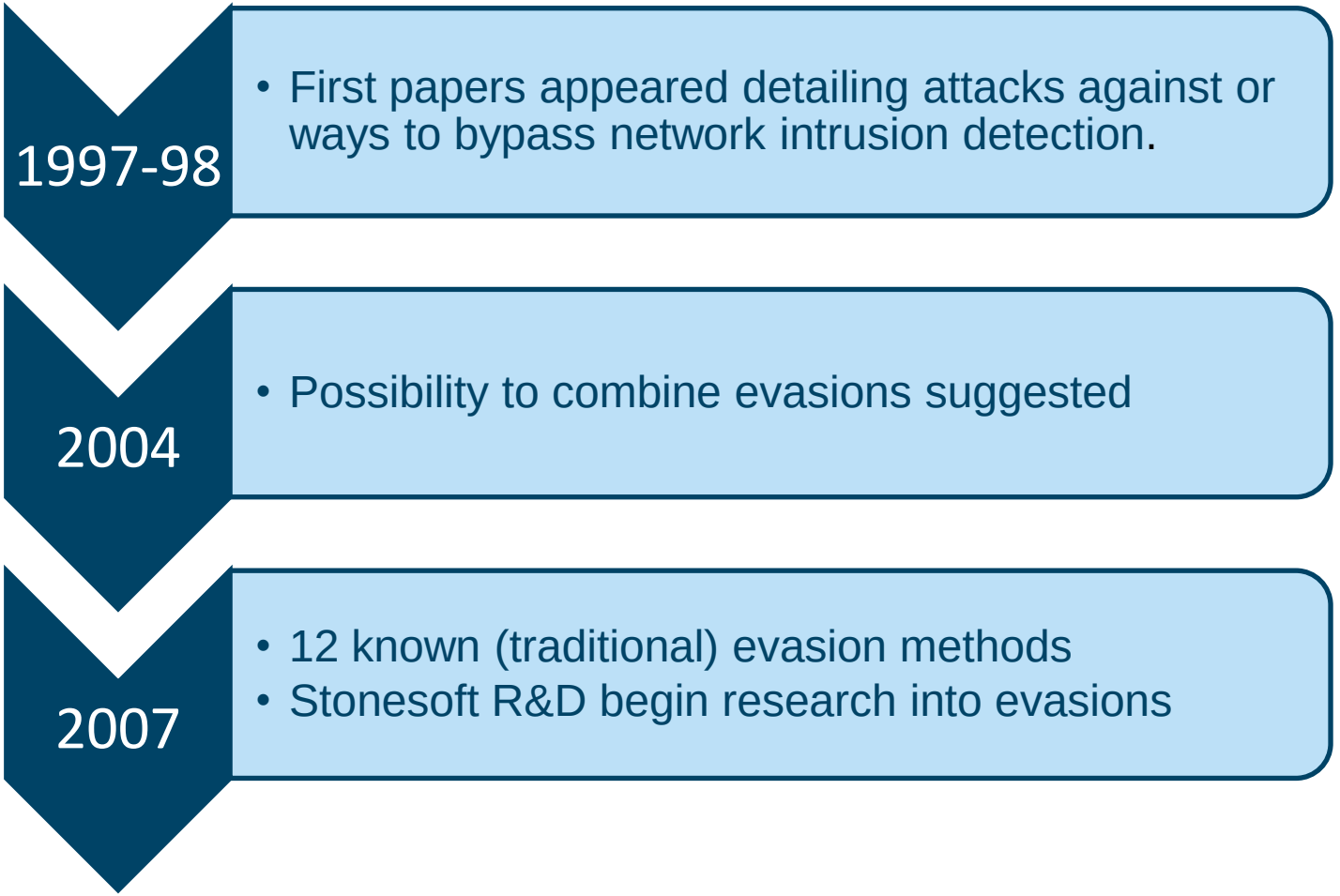
AETs vs Next Gen FW

Evasion (*definition*)

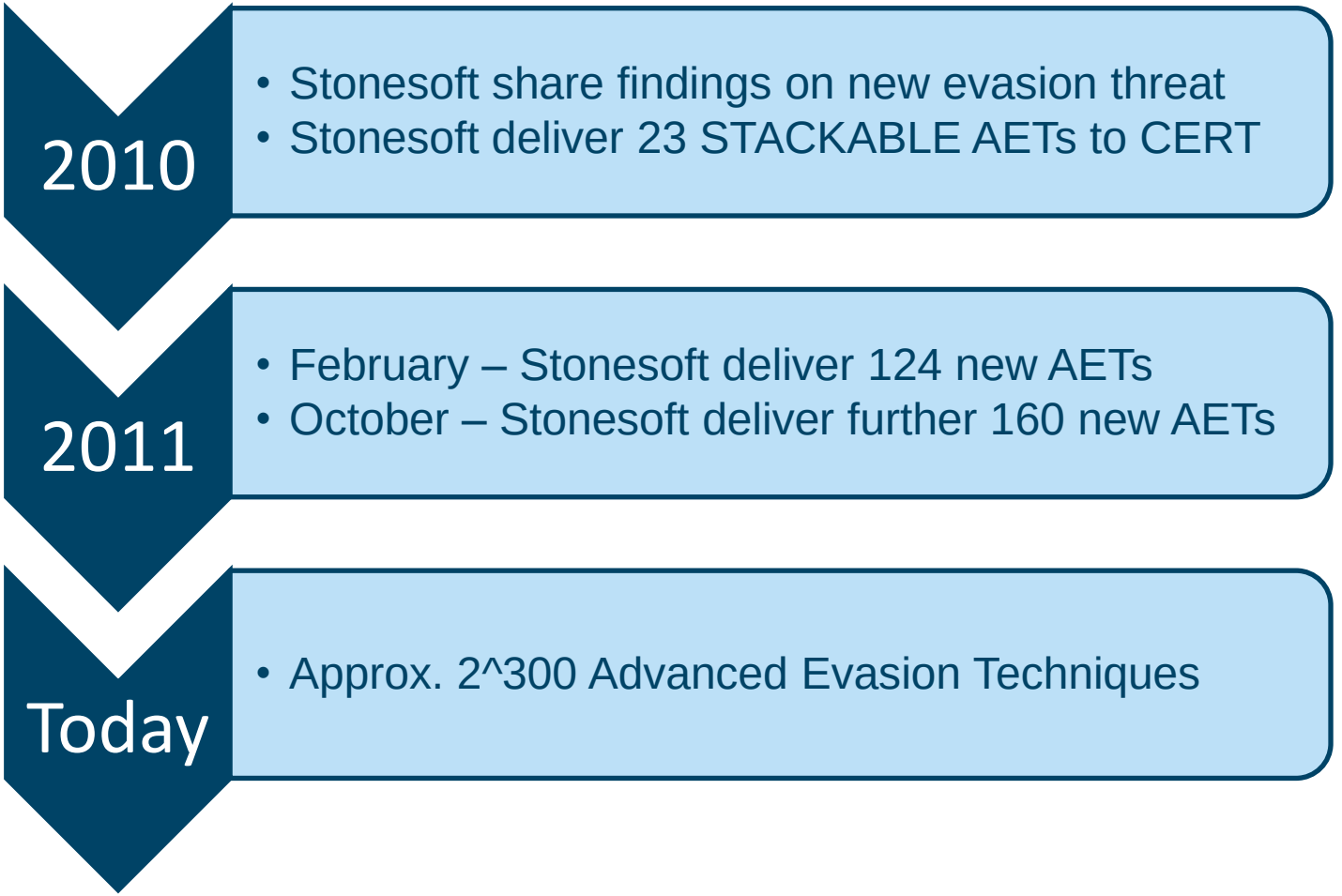
Evasion techniques are a means to **disguise** and/or **modify** cyber attacks to avoid detection and blocking by information security systems. Evasions enable advanced and hostile cyber criminals to deliver ***any malicious*** content, exploit or attack to a vulnerable system **without** *detection*, that would normally be detected and stopped.

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)*

Evasion timeline



Evasion timeline



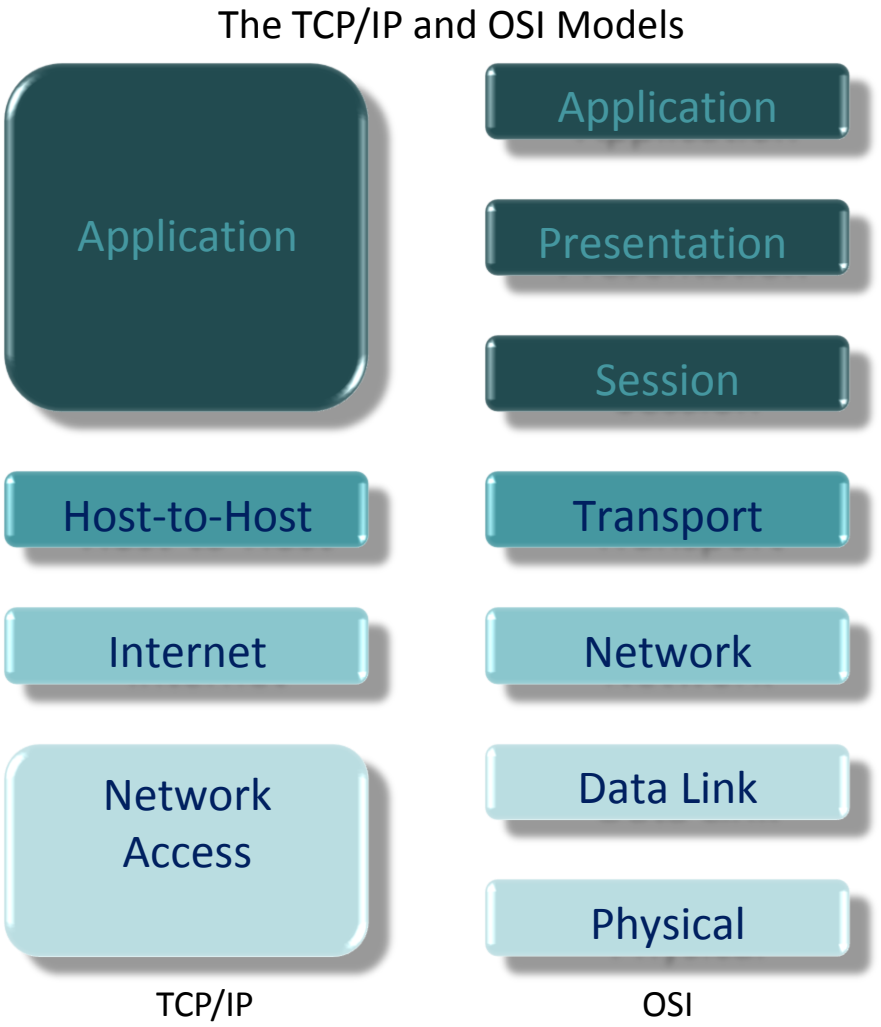
Why AETs are different

In order to understand what an advanced evasion is we must refer back to the rules surrounding network communications and specifically TCP/IP.

Known evasions target specific layers of the TCP/IP protocol stack. This makes them relatively easy to detect and stop.

Advanced evasions target multiple layers of the protocol stack and combine multiple evasion methods.

They do not conform to the rules. Making them virtually impossible to detect.



AET Example – TCP Evasion

Open and close a TCP connection. Open a new TCP-connection to the same service using the same TCP-source port.

> According the TCP RFC, the TCP client MUST wait ”TIME-Wait Delay” amount of seconds before reusing a source port.

If the attacker uses his their own TCP/IP Stack, they can open and close a TCP-connection and immediately open a new TCP connection using the same source port.

> The IPS stack should handle new connections as new connections regardless of the TIME-Wait-Delay

AET Example – MSRPC Evasion

The client may change the current context using the Alter Context method. All subsequent requests then go to the new context.

Example: The client binds to non vulnerable context and then changes into a vulnerable context and sends the exploit.

Surely my current IPS/IDS/NGFW can stop them?

It is possible to effortlessly evade most market-leading security solutions by using one or more advanced evasion techniques (AETs).

NOTE! Tests include all of the **highest ranked** security devices from the **Gartner Magic Quadrant**

All products are running the latest versions and updates.

StoneGate products were originally vulnerable but now include comprehensive protection against AETs as standard.

How can I defend against AETs?

Cover the basics (Patch, permissions etc.)

Know your assets (Who, What, When & Where)

Be vigilant (Monitor)

Deploy Advanced Evasion ready network security (Scalable, responsive)

Review (Don’t be complacent)

AETs - Comment

ICSA labs
An Independent Division of Verizon Business

"Advanced Evasion Techniques can evade many network security systems. We were able to validate Stonesoft's research and believe that these Advanced Evasion Techniques can result in lost corporate assets with potentially serious consequences for breached organizations."

– Jack Walsh, Program Manager

NSS Labs
Security. Certified.

"If the network security system misses any type of evasion it means a hacker can use an entire class of exploits to circumvent security products, rendering them virtually useless. Advanced Evasion Techniques increase the potential of evasion success against the IPS, which creates a serious concern for today's networks."

– Rick Moy, President

Gartner

"Recent research indicates that Advanced Evasion Techniques are real and credible – not to mention growing –a growing threat against the network security infrastructure that protects governments, commerce and information-sharing worldwide. Network security vendors need to devote the research and resources to finding a solution."

– Bob Walder, Research Director

Summary

- AETs are real
- AETs are NOT exploits
- Most vendors are severely lacking in this area
- AETs will not just go away
- You CAN defend against AETs

alan.cottom@stonesoft.com

www.stonesoft.com