STONESOFT

Network Security

Stonesoft

La Société

- Entreprise créée en 1990 spécialisée dans la sécurité et la haute disponibilité des infrastructures
- Présent à la bourse Helsinki NASDAQ OMX: SFT1V depuis 1999
- Pas de dette, moyens financiers importants
- Siège international à Helsinki, Finlande
- Siège USA à Atlanta

Focus clients

- Présent aux USA, EMEA et Asie
- Support global 24/7
- Clients dans plus de 90 pays avec des bureaux Stonesoft répartis dans 16 pays
- Focus sur les entreprises exigeant une forte sécurité des réseaux et des interconnexions en permanence opérationnelles

Innovation

- Solutions de sécurité intégrée et de continuité de services
- Centres R&D en France, Finlande & Pologne
- Nombreux brevets technologiques

Comment les Cybercriminels peuvent augmenter leur chance de réussir leurs attaques ciblées?

En les rendant plus simples.

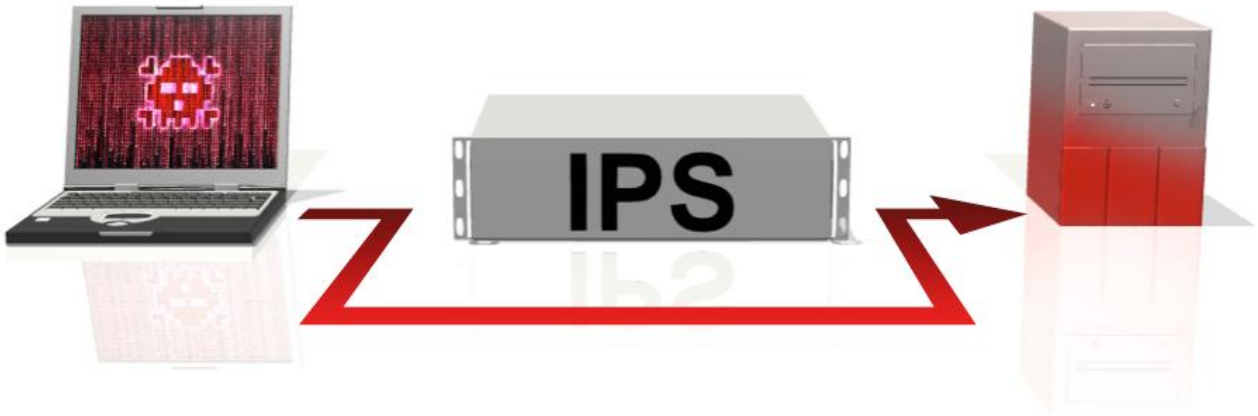
Advanced Evasion Techniques

Ænti evasion
BY: STONESOFT

Définition d’une ”Evasion”

Les techniques d’Evasion (contournement) sont des moyens **de camoufler** ou/et **de modifier** des cyber attaques classiques afin d’empêcher la détection et le blocage par les systèmes de sécurité informatiques.

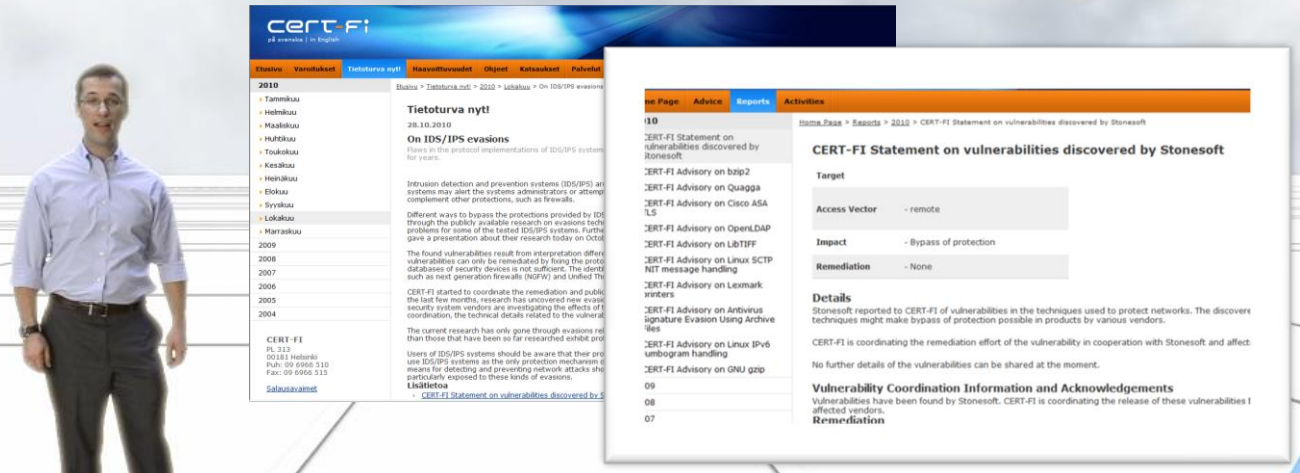
Les **Evasions** permettent aux cybercriminels hostiles et expérimentés d’injecter n’importe quels *contenus malicieux ou attaques* vers un système vulnérable **sans aucune détection** alors qu’ils devraient être normalement détectés et bloqués. Les systèmes sont alors **devenus inefficaces** contre ces types de technique d’Evasion.



Æntievasion
BY: STONESOFT

La R&D de Stonesoft a découvert et publié de nouvelles techniques de contournement qui peuvent être modifiées et combinées dans n'importe quel ordre afin de réduire à néant la détection des systèmes de sécurité

Advanced Evasion Techniques (AETs)



http://www.cert.fi/en/reports/2010/vulnerability385726.html

Ænti evasion
BY: STONESOFT

Cert 2010.1 set	23
Cert 2011.1 set	123
Cert 2011.2 set	163

Recherches sur les ”Evasions”...

Actuellement, 250+ Evasions que l’on peut combiner et cumuler sont en test dans les plateformes de recherche.

Le nombre de combinaisons d’Evasions est déjà pratiquement illimité!

STONESOFT

Network Security

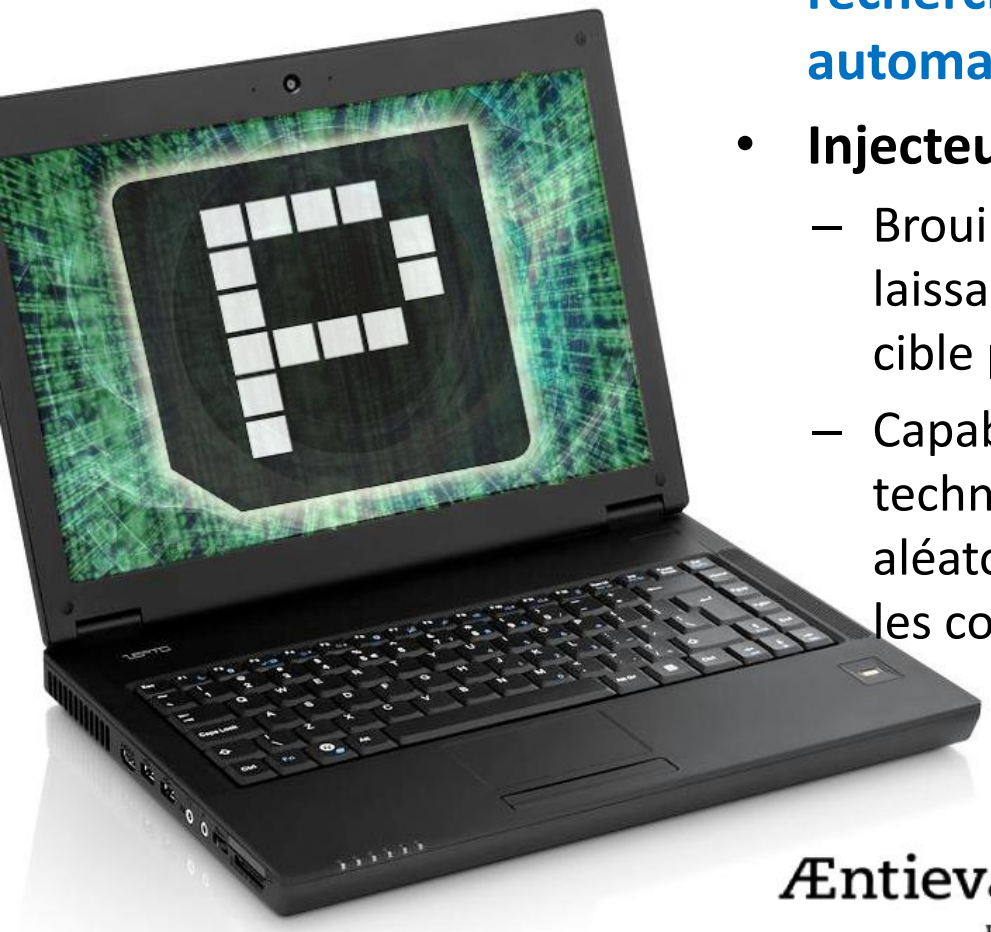
STONESOFT

Network Security

2^{250}

STONESOFT
Network Security

Predator 4.1



- Equipement de sécurité afin de concevoir un **environnement de recherche** pour des tests **automatisés**
- **Injecteur d'Evasion**
  - Brouille les protocoles tout en laissant le payload intact tel que la cible pourrait l'interpréter.
  - Capable d'utiliser de multiples techniques d'Evasion de manière aléatoire et simultanément sur toutes les couches.

Æntievasion
BY: STONESOFT

Conclusion de recherche

1. Impossible de se protéger contre toutes les combinaisons.
2. Sans modèle de tests automatisés, les éditeurs sont incapables de développer des produits efficaces contre les évasion
3. La question est : Qui peut offrir un haut niveau de protection tout en proposant des mises à jour dynamiques et efficaces contre les Evasions ?
4. A l'avenir, IPv6 offrira un univers de combinaisons encore plus vaste

Commentaires sur les AET

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 a real and credible – not to mention growing –and 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.

University of Glamorgan
Prifysgol Morgannwg

We believe AETs pose a serious threat to network security and have already seen evidence of hackers using them in the wild. It is also very promising to see that Stonesoft is taking the threat posed by evasions seriously as they have been overlooked by many in the past

-Andrew Blyth, Professor of Glamorgan University

STONESOFT
Network Security

Implications

- Les données critiques perdent leur protection, peu importe l'efficacité de détection de l'équipement de sécurité.
- On devient aveugle sur la tentative ou réussite d'une attaque si l'équipement échoue sur son traitement anti-évasion
- La fausse impression de protection crée des cibles faciles
- Augmente le taux de réussite des attaques réseaux.
- Etablit une nouvelle menace pour les organisations offrant un large gain (financier, stratégique, politique, technique) pour les cybercriminels expérimentés.
- L'amélioration de la gestion de patches et une mise à jour constante des protection contres les Evasions sont impératives

Connues

- IP fragmentation with manipulated fragment size and order
- TCP segmentation with manipulated segment size and order
- SMB fragmentation
- SMP transaction write method
- MSRPC multibind (bind to multiple “unnecessary or non-existent” contexts + the vulnerable context)
- MSRPC fragmentation
- MSRPC encryption

Pas si connues

- IP random options
- TCP TIME_WAIT
- TCP urgent pointer
- SMB write/read padding
- SMB transaction method fragmentation
- SMB session mixing
- MSRPC alter context
- MSRPC object reference
- MSRPC endian manipulation

Urgent!

- Insérer un octet dans le flux TCP
- Le serveur décide d'utiliser ou d'ignorer cet octet supplémentaire
- Un IPS peut être contourné par une interprétation du pointeur urgent

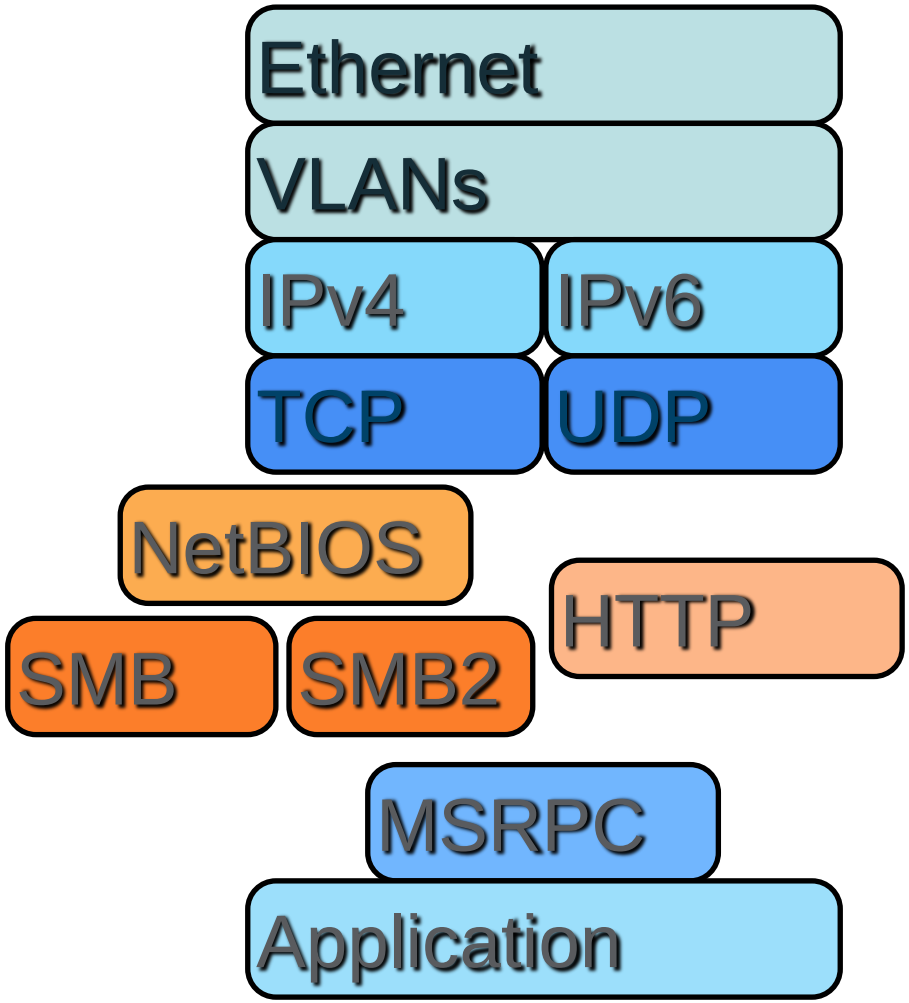
```
TCP:      \xff  P S M B

IPS:      \xff  P S M B

OS:       \xff S M B
```

Ænti evasion
BY: STONESOFT

Prenons l'exemple de MSRPC



IP fragmentation

- fragment IP payload
- random_order: send frags in random order
- out_of_order: send one frag out of order
- fwd_overwrite: perform forward overwriting with fragments
- last_first: send last fragment first
- one_duplicate: send one duplicate fragment

IP evasion

- random_options: send random IP options

TCP fragmentation

- split TCP payload into smaller segments

TCP evasion

- time_wait: open a decoy connection and attack from same IP:port while in TIME_WAIT
- urgent_ptr: insert meaningless data into 1 byte urgent segments

SMB fragmentation

- fragment SMB payload

SMB evasion

- andx_connect: negotiate SMB session and connect to a tree, connect an AndX message
- decoy_trees: open decoy SMB tree connects in the same TCP stream as the attack
- read_offset: use random offsets in SMB read operations
- pad_write_random: pad SMB write commands with a random sized block of random data
- pad_write_static: pad SMB write commands with a static sized block of random data
- random_write_method: use a random SMB write method (TRANSACT / WRITE)
- write_offset: use random offsets in SMB write operation

Æntievasion
BY: STONESOFT

MSRPC fragmentation

- fragment MSRPC payload

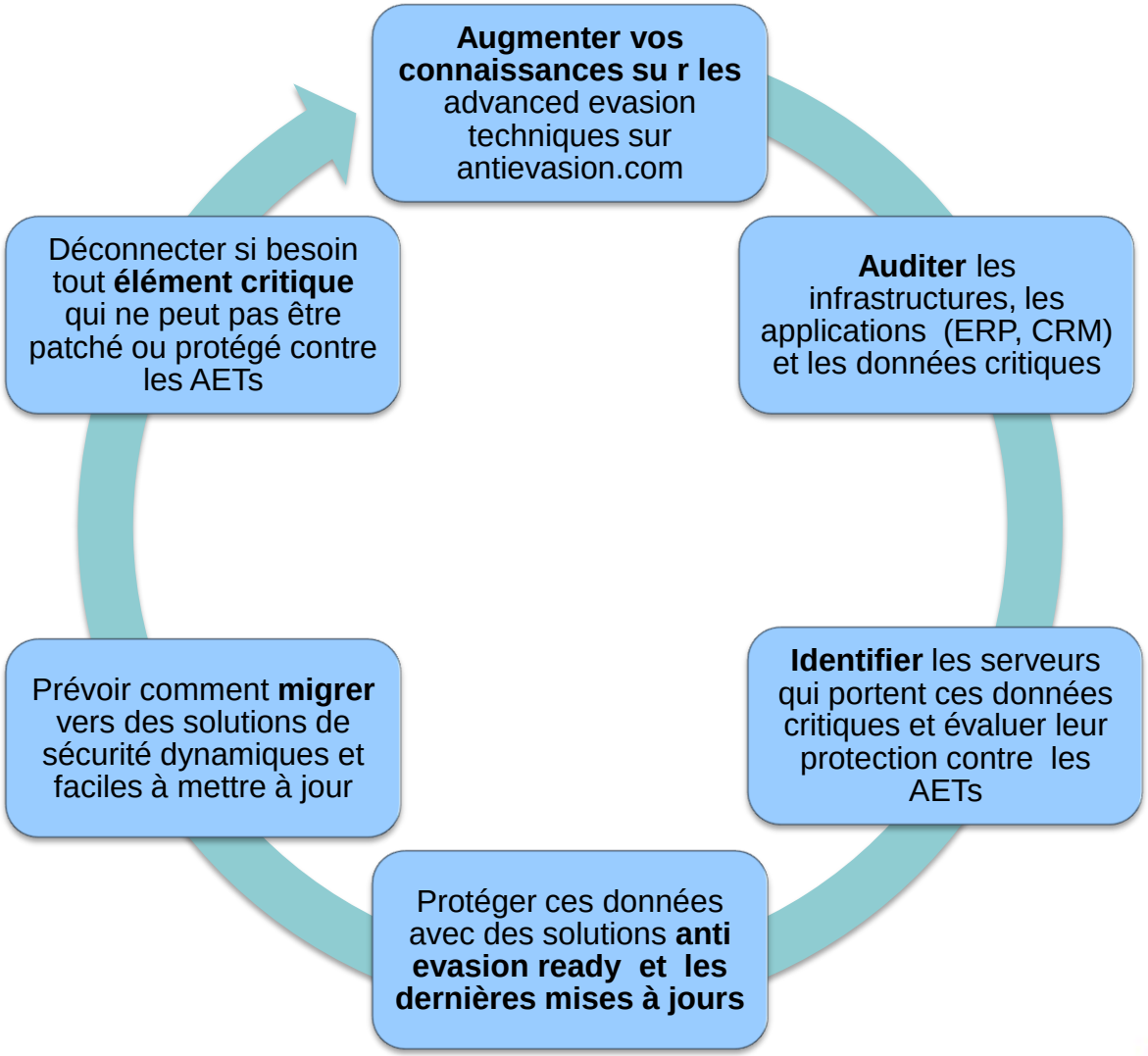
MSRPC evasion

- big_endian: communicate in big endian format
- random_object: add a random object reference to the MSRPC request
- alter_context: bind to a random context and then alter to the correct

Normalisation

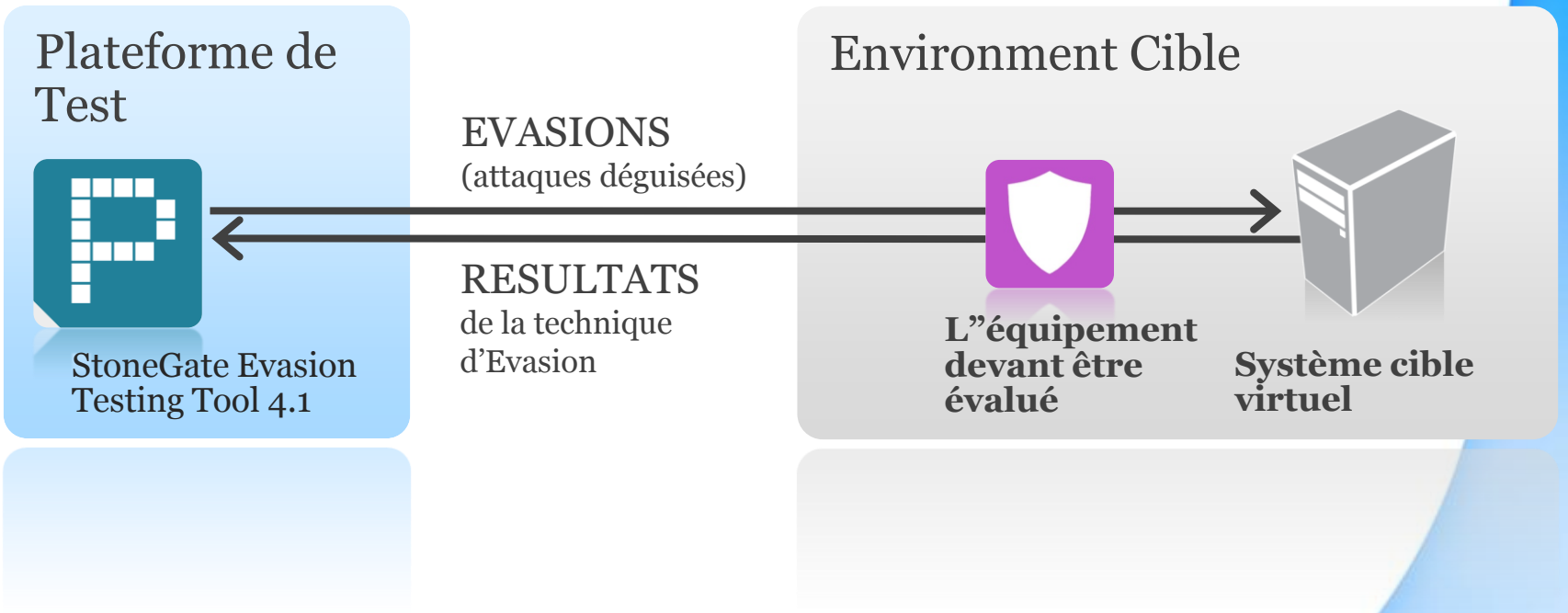
- La normalisation protocolaire est un moyen de combattre les techniques d'évasion
- La capacité d'Anti Evasion dépend de l'efficacité d'un système à normaliser un trafic sur toutes les couches.
- Cela signifie que toute analyse protocolaire est normalisée afin de pouvoir détecter les attaques par une signature. Il n'y a que la signature de l'attaque qui doit être utilisée.

Processus pour réagir face aux AETs



Æntievasion
BY: STONESOFT

Audit type ÆRT



Æntievasion
BY: STONESOFT

STONESOFT

Vidéo de Démo

STONESOFT

Network Security