Новые техники защиты от старых угроз

- Обойти невозможно?

РУСКРИПТО

30.03.2012

STONESOFT

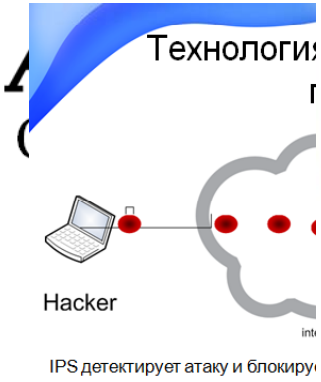
Содержание

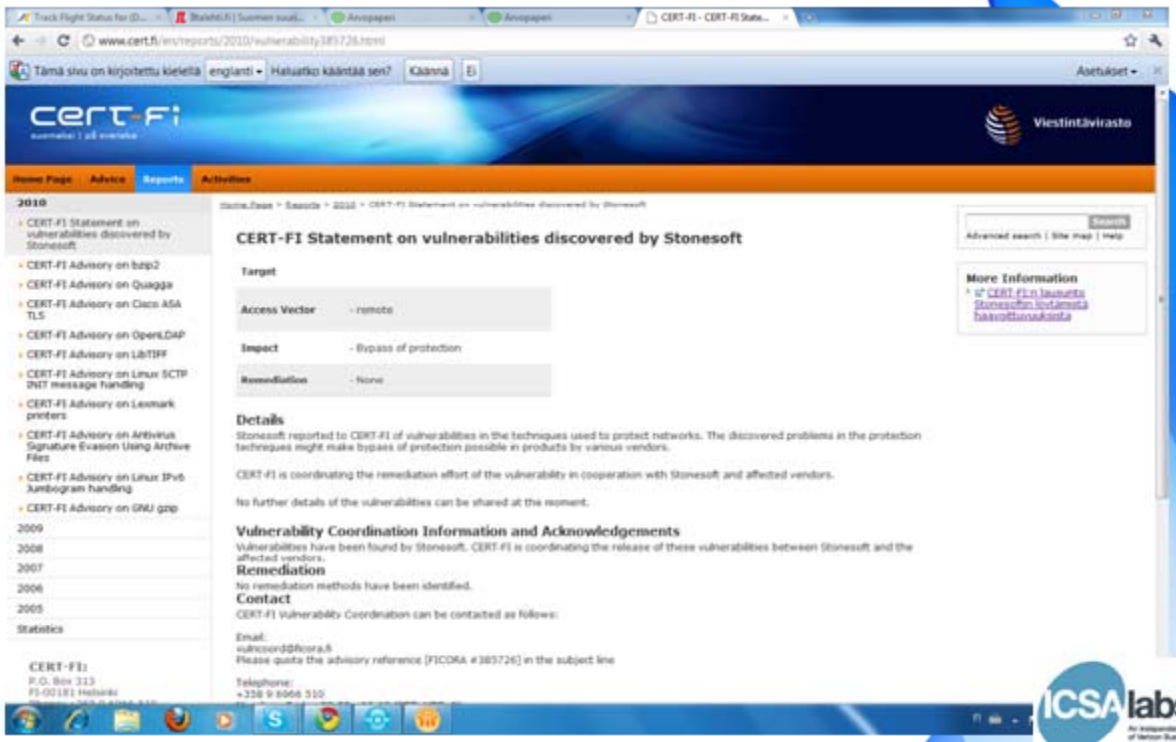
- РЕТРОСПЕКТИВА
- ТЕКУЩЕЕ СОСТОЯНИЕ ДЕЛ
- ЧТО ТАКОЕ ТЕХНИКИ ОБХОДА

STONESOFT

Ретроспектива (РусКрипто

Подтверждения со стороны - Cert





StoneSoft выявил новые спец
обхода (evasion techniques), к
использованы или скомбин
порядке, чтобы обойти
детектирования устройства

AET (Advanced evasio
динамические техни

...и новый виток гонки **ANTI-**
приемов нача

* - StoneSoft наверняка не единственная организация, которая это онаружила, что косвенно подтверждается необъяснимыми «мистическими» инцидентами

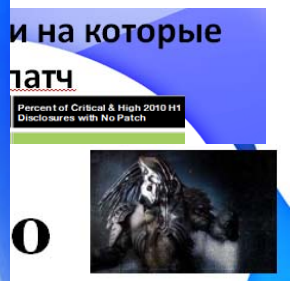
Æntievasion
BY: STONESOFT

Æntievasion
BY: STONESOFT

SMB fragmentation
MSRPC alter context
TCP TIME WAIT
IP random options

Обычно техники обхода не нарушают какой-либо стандартов RFC, например, поэтому модули разб протоколов их не распознают.

Æntievasion
BY: STONESOFT



- Способен одновременно использовать несколько случайно выбираемых техник обхода на разных уровнях

Æntievasion
BY: STONESOFT

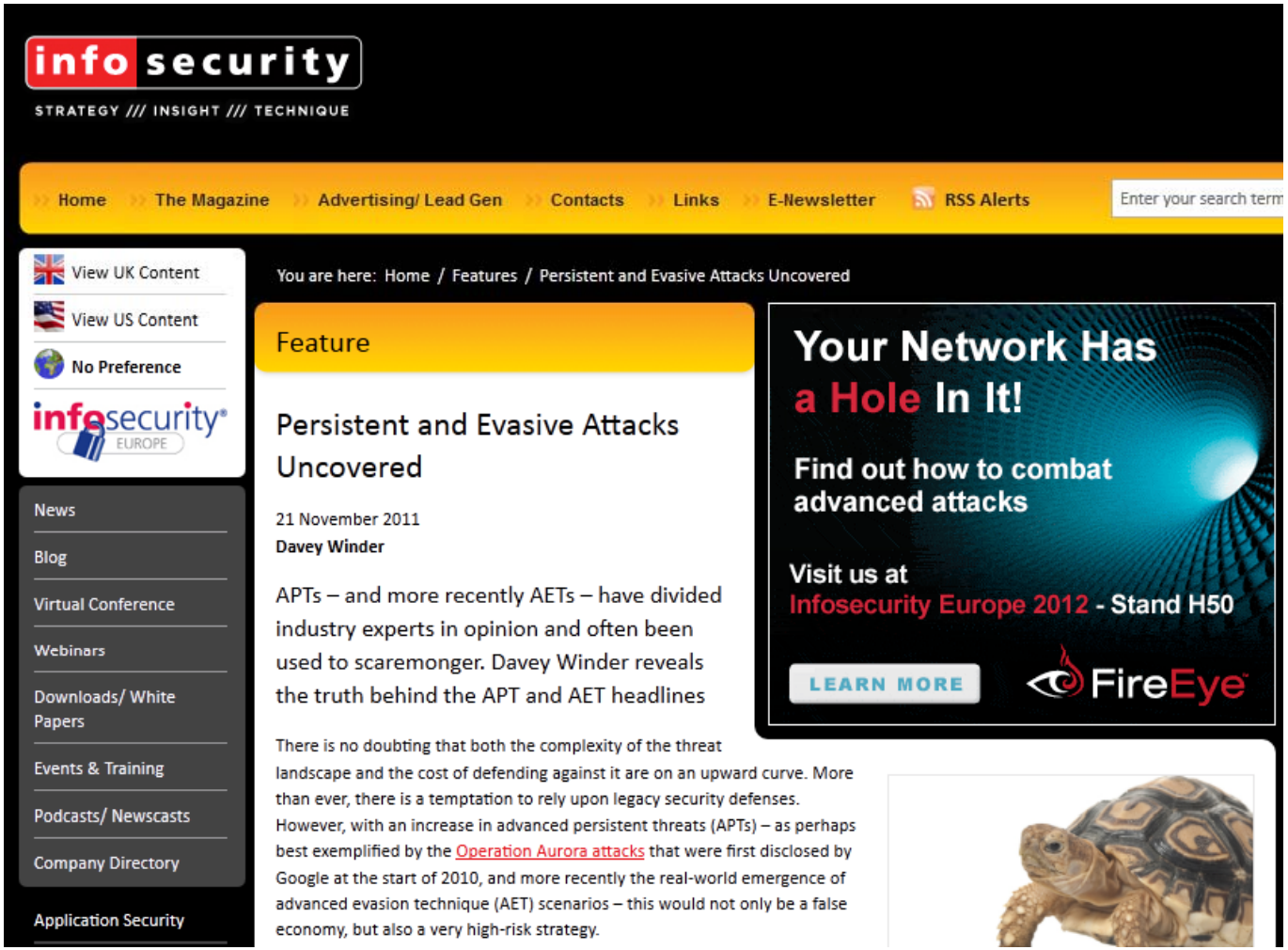
Æntievasion
BY: STONESOFT

STONESOFT

2011 временная шкала взломов

Атак больше на 45%
На 56% более дорогие

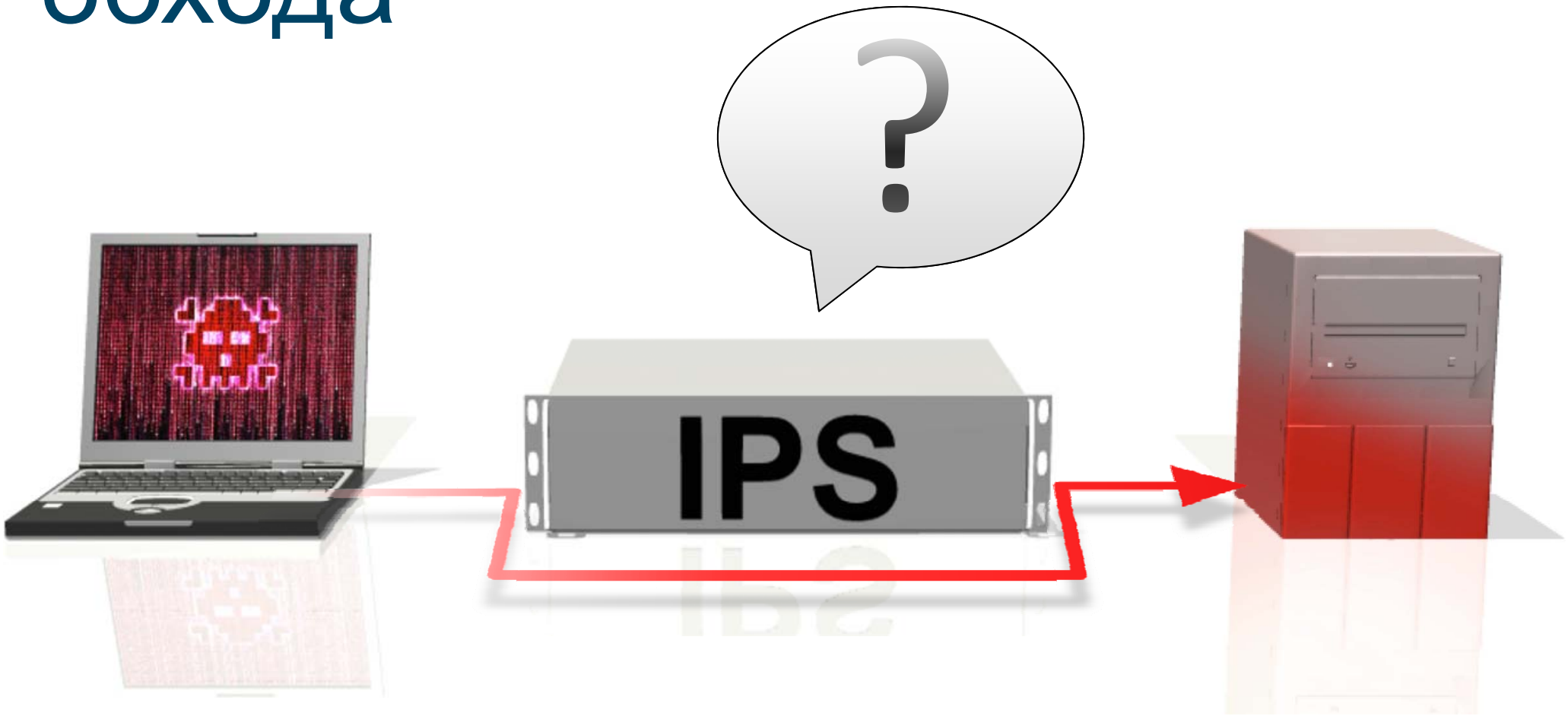
APT или AET?



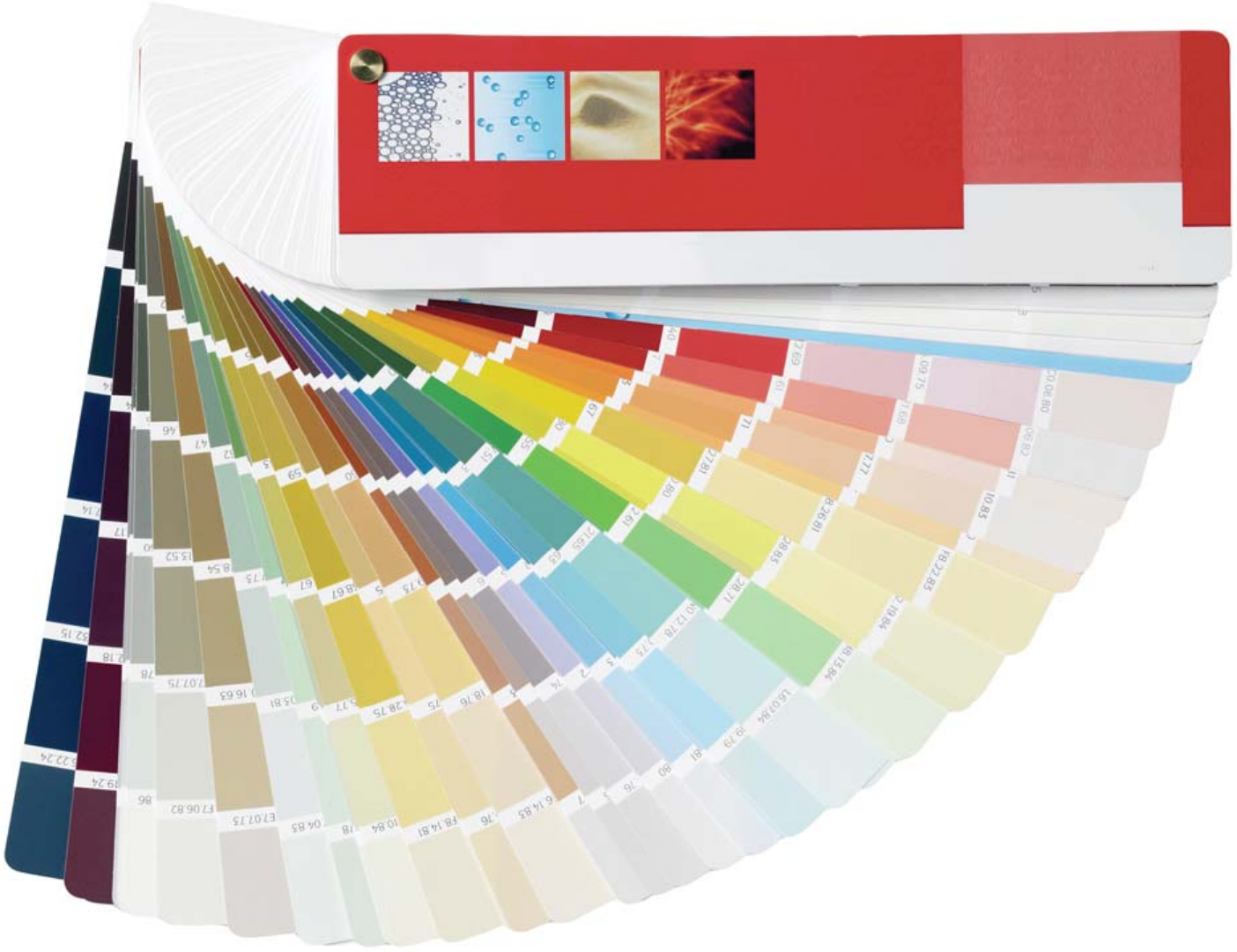
- несмотря на достаточно большое количество времени, прошедшее с момента анонса самих техник обхода, до сих пор многие вендоры предпочитают либо отрицать сам факт наличия угрозы (а значит, и проблемы с их продуктами), либо занижают его серьезность (по той же причине)

http://www.infosecurity-magazine.com/view/22156/persistent-and-evasive-attacks-uncovered-/

Принцип работы техники обхода

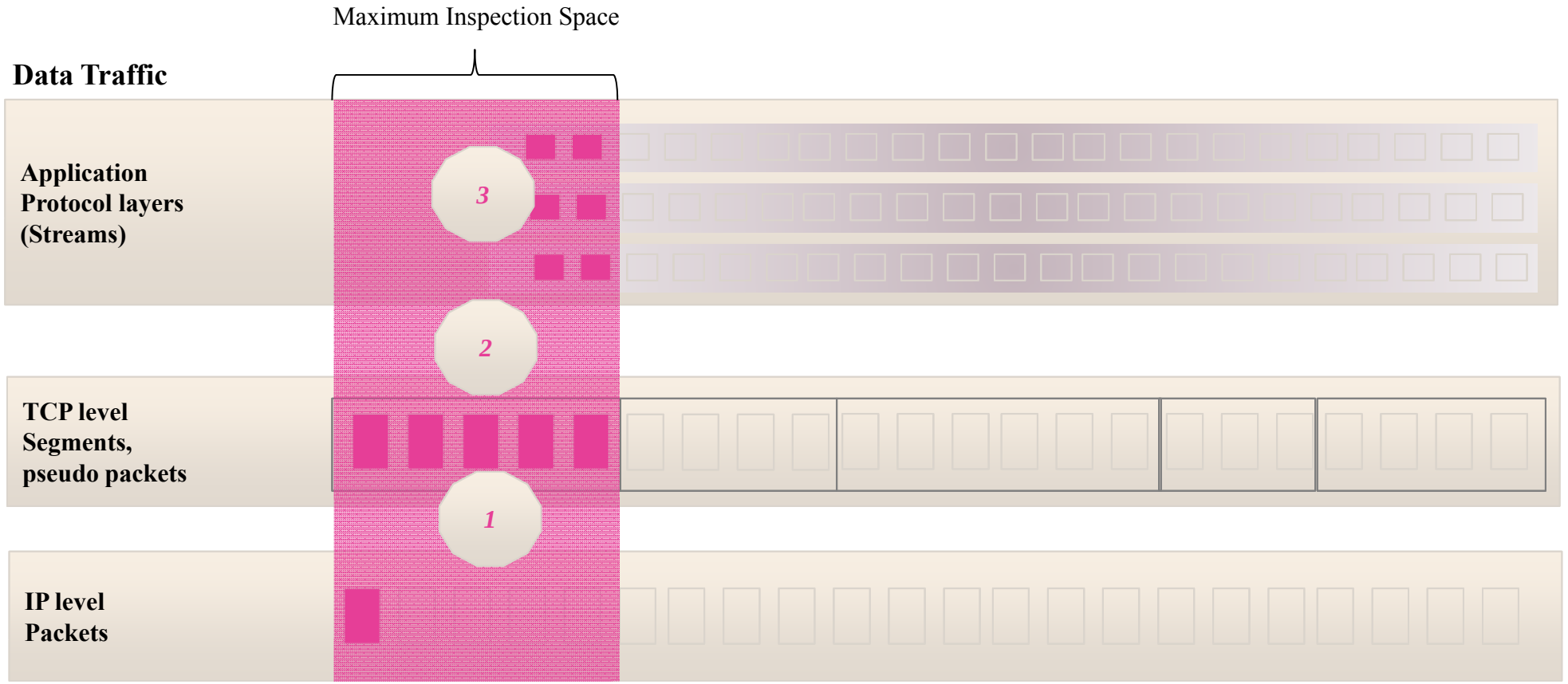


Принцип работы техники обхода



Вертикальная инспекция трафика данных

Пакеты, сегменты или псевдо-пакеты – инспекция на базе разных уровней



1 **Limited Protocol** decoding and inspection capability to gain speed.

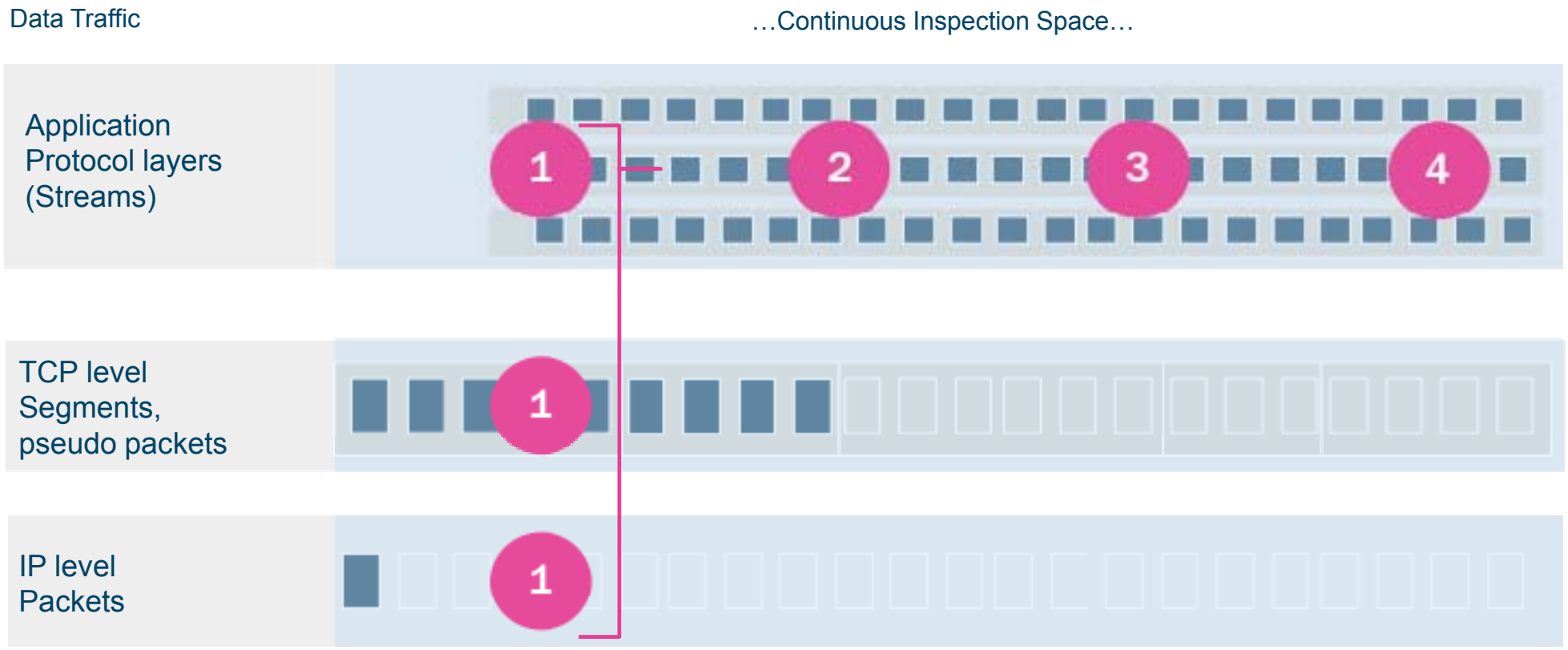
2 **Partial or No Evasion Removal** Majority of the traffic is left without evasion removal and inspected with limited context information available.

3 **Detect and Block Exploits** Unreliable or impossible exploit detection when evasion are not removed on all layers.

Технология борьбы с техниками обхода

Horizontal

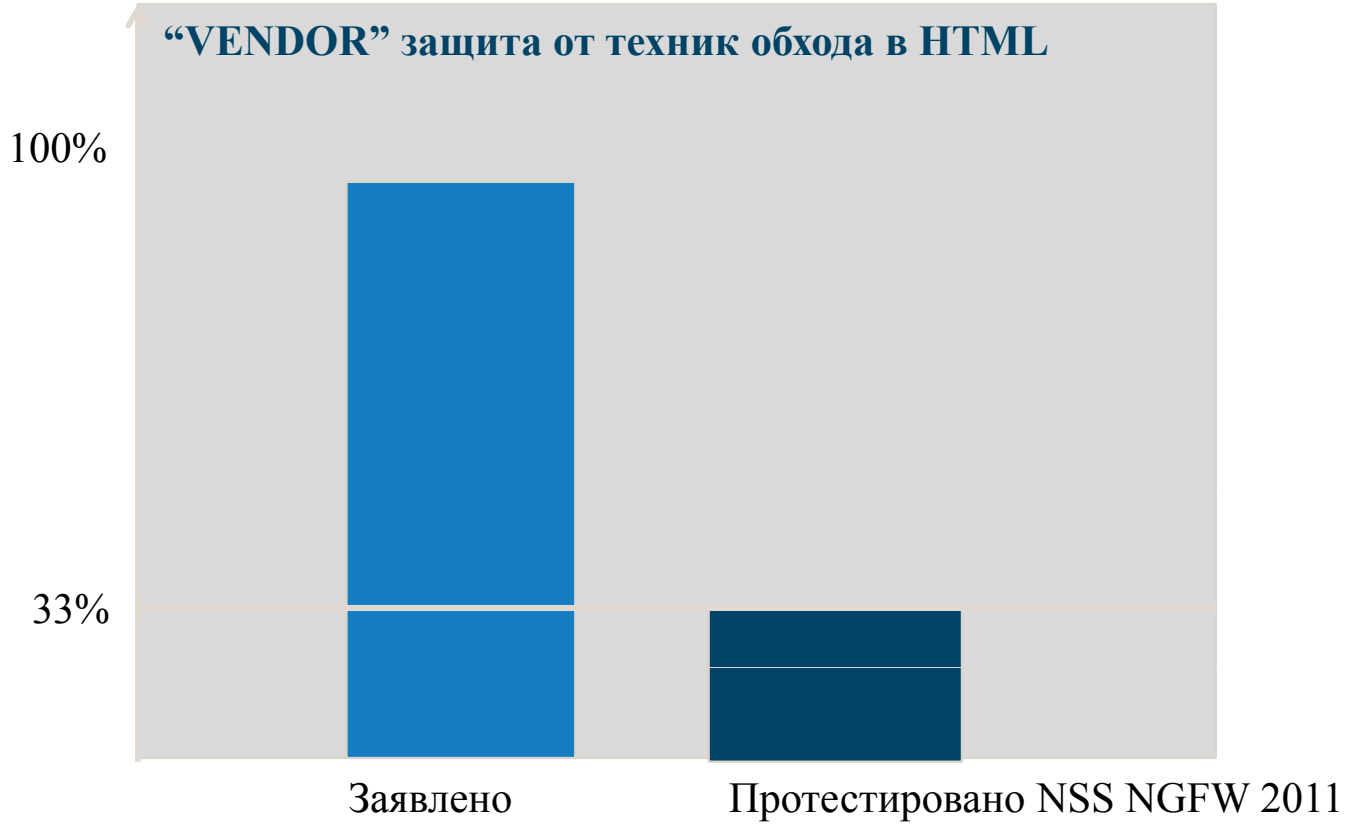
Data stream based, full Stack normalization and inspection process



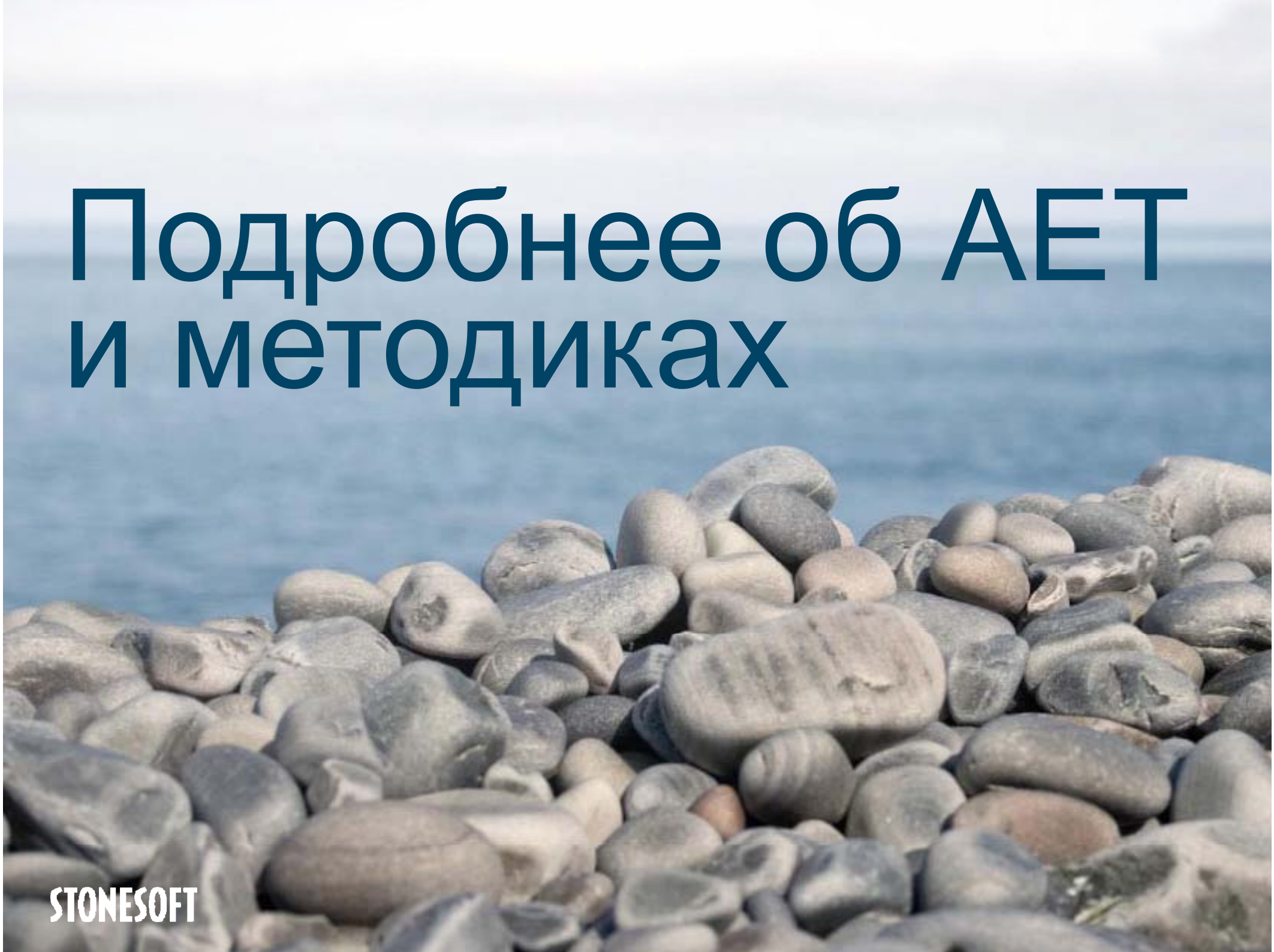
1. Normalize traffic on all protocol layers as a continious process.
2. Advanced Evasion removal process makes the traffic evasion free and exploits detectable.
3. Detect exploits from the fully evasion free data stream.
4. Alert and report Evasion attacks through management system.

На самом деле...

Примечание:
В данном тесте использовались только простые, известные и хорошо документированые техники обхода. А что случится, если будут использоваться динамические?



Подробнее об AET и методиках



STONESOFT

Почему АЕТ работают?

- Тяжело реализовать стек TCP/IP на промежуточном устройстве
- Реализация детектирования техник обхода и нормализация сложны и влияют на производительность!
- Обнаружение техник обхода по принципу «аномалий» ведет к ложным срабатываниям
- Простой, но скоростной поиск по регулярным выражениям по пакетам данных будет пропускать атаки с техниками обхода
- Корректный разбор TCP/IP, который неуязвим к TCP техникам обхода, требует много памяти

Тестирование от AET?

- Сама по себе процедура очень сложна:
  - Требует утилит, но большинство из доступных содержат только несколько техник обхода.
  - IPS устройства имеют тенденцию к обнаружению некоторых из тех техник обхода, которые доступны в публичных утилитах.
  - IPS устройства зачастую пропускают атаки, которые содержат техники обхода, которые не реализованы в доступных тестовых утилитах.

Как происходило раскрытие информации об АЕТ

- 2010
  - 23 техники были раскрыты вендорам через FI-CERT
  - В 2010 было протестировано 7 IPS/NGFW устройств с последними версиями ПО и правил инспекции
    - Все уязвимы!
  - В феврале 2011, ни один из вендоров не был способен блокировать все атаки с помощью техник обхода, раскрытых в 2010
    - И более того, большинство раскрытых атак, как оказалось, были публично изучены еще за 4 года до этого…

…Как происходило раскрытие информации об AET

- В феврале 2011, было раскрыто 124 образца техник обхода вендорам через FI-CERT
  - Все протестированные продукты были уязвимы к ним
    - Наихудший продукт был уязвим к 66 техникам обхода
    - До сих пор нет полноценных исправлений
- В октябре 2011, было раскрыто 163 образца
  - IPv4/IPv6, TCP, smb, http

АЕТ – что же это?

- Комбинация методов обхода на нескольких уровнях работы протоколов одновременно:
  - Например, транспортный и прикладной
- Изменение техник обхода в середине соединения в одном из или нескольких уровнях работы протоколов
  - Не применяют техники к соединению в целом, но только к конкретным данным, которые воздействуют на уязвимость

Комбинация техник обхода…

- Не существует публично доступной утилиты, которая
  - Спроектирована использовать несколько техник обхода на разных уровнях от IP до прикладного одновременно
  - Способна контролировать размер и порядок отправки каждого пакета/датаграммы
  - Способна менять техники обхода «на лету», к каждому пакету или любому протоколу, имеет несколько методик обхода или их комбинаций
  - Спроектировано для тестирование обработки протоколов и методов декодирования устройствами защиты
  - Реализует самые известные исследования в техниках обхода и имеет интерфейсы для автоматизированного тестирования
- Почему?
  - Такая утилита требует нестандартного TCP/IP стека, который спроектирован для тестирования устройств защиты и применения техник обхода

Представляем Predator

- Утилита для тестирования сетевых устройств
  - Содержит несколько эксплоитов, которые должны обнаруживаться и блокироваться сетевыми устройствами
- Реализует почти все известные техники обхода и спроектирован для их изучения и автоматизированного тестирования
- Способен комбинировать техники обхода на одном или нескольких уровнях работы протоколов
- Способен менять техники обхода на лету и в одном или нескольких уровнях
- Evasion Fuzzer
  - Случайным образом модифицирует «транспортный» протокол, но оставляет неизменной полезную нагрузку
  - Использует несколько техник обхода, выбранных случайным образом, одновременно и на разных уровнях
    - Передает одну и туже полезную нагрузку, пока не добьется успеха

Представляет Predator

- Не использует TCP/IP стек ОС
  - Содержит модифицированный TCP/IP стек, который совершенно не зависит от стека TCP/IP системы
    - Спроектирован для тестирования сетевых приложений на разных уровнях
    - Использует принципы RFC себе на пользу
      - Подход RFC: быть строгим с форматом того, что отправляется, но принимать все
      - Подход утилиты: пробовать все и смотреть, что получается

Исследования AET

- Исследования начались в 2007
  - Было 12 различных техник, которые не “стекировались”
- В 2009
  - 32 техники обхода, которые можно было комбинировать
- в 2010

  180 техник обхода, которые можно комбинировать
- в 2011

  Сотни техник обхода (больше подсчет не ведется)

Количество комбинаций

- 2007: 12
- 2009: 2^32 =

  4 294 967 296
- 2010: 2^180 =
  1532495540865888858358347027150309183618739122183602176

- Невозможно протестировать все комбинации!


Реакция вендоров
на AET
STONESOFT

Суть ответа

- *Now, think about that. That does not make sense!*

В ответ на Predator/AET

- Детектирование Shellbanner

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

В ответ на Predator/AET

- Детектирование shellcode payload
  - shellcode используется как триггер в payload-е для блокировки соединения
- Предотвращение доступа к уязвимому интерфейсу (RPC)
  - Даже если нет реальной атаки/эксплоита == ложное срабатывание!

В ответ на Predator/AET

- Предотвращение TCP сегментации
  - Для MSRPC, терминировать TCP соединение если размер сегмента <20 байт
- Блокировать кодировку Bigendian в MSRPC
  - Если обнаруживается Bigendian → просто блокировать

В ответ на Predator/AET

- Если IPS/NGFW обнаруживает и идентифицирует атаку без техник обхода, он(а) должна обнаруживать туже самую атаку, когда используются техники обхода
  - Но большинство устройств на это не способны
  - Если используются техники обхода, большинство устройств детектируют только «аномалии», связанные с техниками обхода, что приводит к ложным срабатываниям
  - Если же отключить детектирование аномалий, то вообще не происходит обнаружения

В ответ на Predator/AET

- Когда IPForge/Predator был портирован с ruby на C++
  - Без модификации самих атак
- Некоторые из устройств конкурентов начали пропускать атаку, запускаемую с помощью версии на c++
- Тогда как «старая» версия на ruby все еще обнаруживалась

Основные выводы

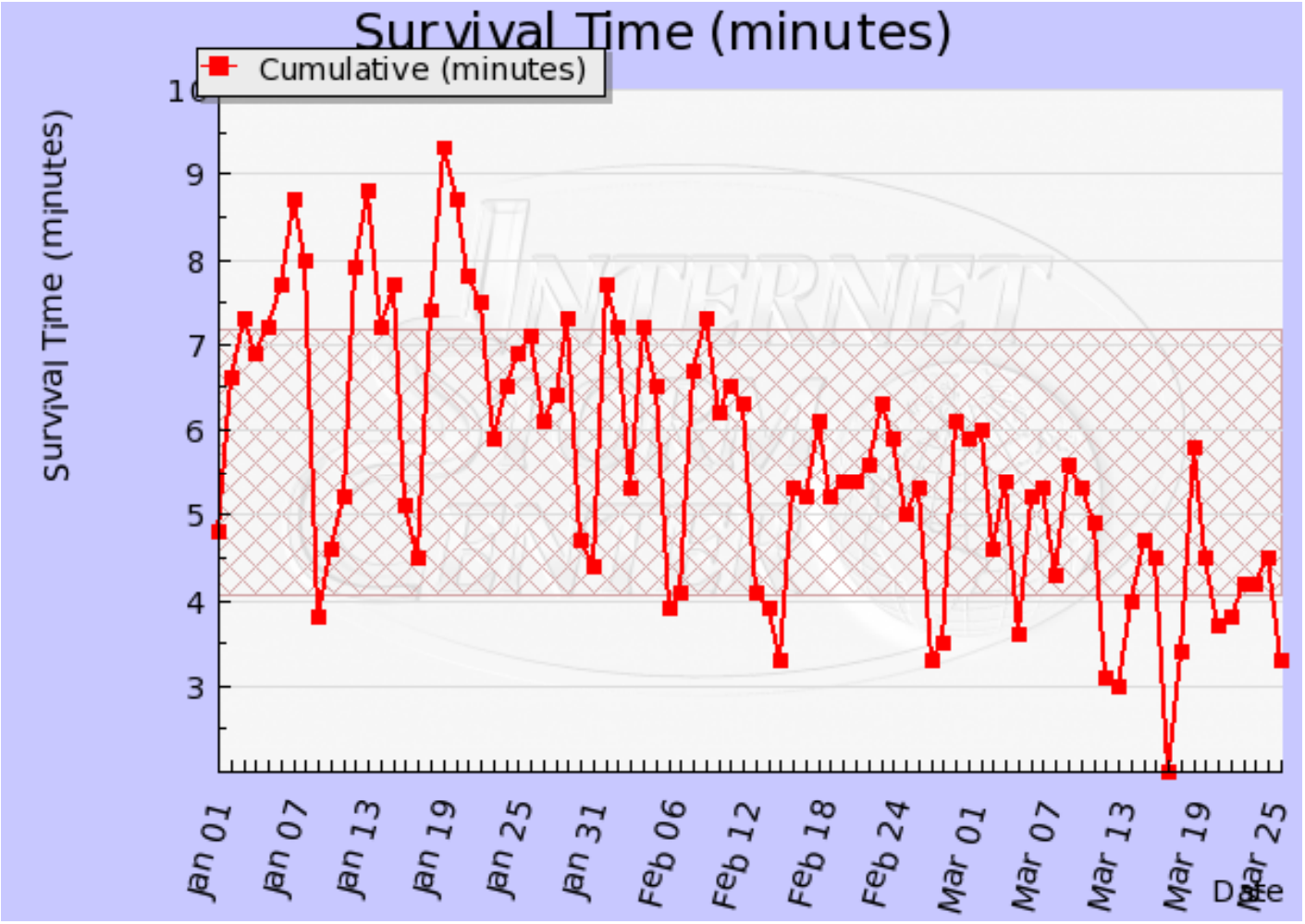
- Большинство (все?) устройства безопасности конкурентов
  - Используют для поиска атак «packet based pattern matchers»
    - Атака на границе пакета приведет к успешному уклонению от детектирования
  - Не выполняют полный разбор TCP/IP
  - Не используют подход на основе защиты от уязвимостей, а применяют обнаружение эксплоитов
    - Можно легко обойти, модифицировав полезную нагрузку в эксплоите, при этом собственно техники обхода даже не нужны!

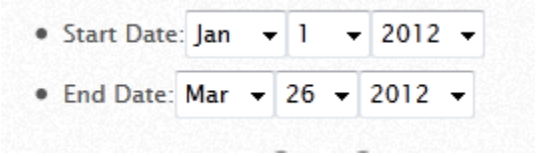
Конкретный пример

4 октября 2010г.	**опубликована информация в CERT-FI: CERT-FI Advisory on IDS/IPS device vulnerabilities that may circumvent protections**
28 октября 2010г.	Cisco опубликовала свой ответ (отсутствие подробного описания проблемы, сославшись на процедуры, принятые в PSIRT
1 ноября 2010г.	CERT добавил описание конкретных работающих 23 техник обхода
15 декабря 2010г.	публичное раскрытие информации CERT
12 января 2011г.	Checkpoint, HP TippingPoint, TrendMicro добавили информацию относительно своих продуктов
1 марта 2011г.	Top Layer Security добавил информацию о своих продуктах

При этом CERT заявляет, что опасность «налицо» - http://www.cert.fi/tietoturvanyt/2010/10/ttn201010281217.html

Выжить в Интернет



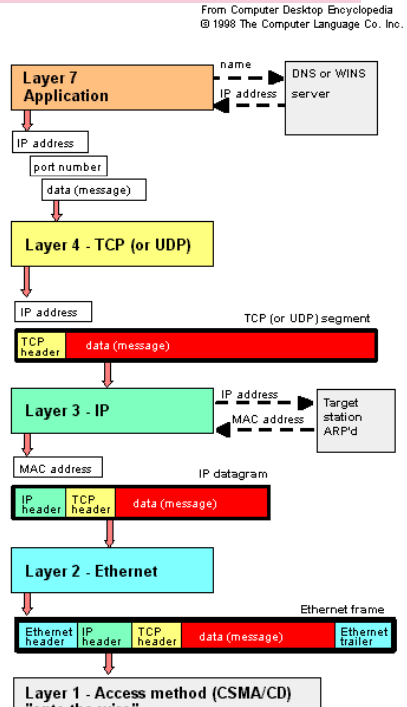


https://isc.sans.edu/survivaltime.html

Реакция вендоров

Checkpoint*	Создан 14.12.2010 Изменен 03.03.2011	Признала, что проблемы существуют, оперативно выпустили сигнатуры, все имеют рейтинг High
HP Tipping Point Top Layer	Н/П	«открестились», не узявимы
TrendMicro		Признали, выпустили обновления
SourceFire IBM ISS		Как будто не проявили внимания (см. далее)

- * - несмотря на бюллетень, Checkpoint утверждает, что ее решения неуязвимы как минимум на сетевом и транспортном уровнях... RPC и SMB – исключения из правила!!!



Реакция в публичных блогах

VRT

WE ARE THE SOURCEFIRE VULNERABILITY RESEARCH TEAM. WE ARE LEGION. RESISTANCE IS FUTILE.

FRIDAY, OCTOBER 22, 2010

Some Facts About Advanced Evasion Techniques

Chances are you've heard the recent "news" about Advanced Evasion Techniques (AETs) from Finnish IPS vendor Stonesoft. Originally announced in an October 4 press release, the good folks at Stonesoft reported the IDS/IPS evasion techniques mentioned in their release to CERT-FI, which promptly issued a public statement. CERT-FI also gave Sourcefire full details on the evasion techniques, allowing us to evaluate their impact on Snort and the Sourcefire 3D system.

Per our standard vulnerability handling guidelines, Sourcefire is awaiting CERT-FI's release of details to the public - currently planned for November 23 - before discussing the technical nitty-gritty with the world at large. Having conducted in-house testing with the data provided to CERT-FI by Stonesoft, we've found that Snort handles all of the reported AETs nicely, and absent any evidence that large-scale attacks using these techniques are underway, we're toeing the responsible disclosure line and giving other vendors a chance to assess and update their products as necessary.

Stonesoft, meanwhile, apparently decided to shift gears out of responsible disclosure mode. While their first release generated some local press in Finland, the issue was largely under the international radar, as you would expect for an unverified set of evasions that were currently under investigation by the vendors in question. This past Monday, they issued a second press release. Put out in conjunction with a press release from ICSA Labs which purported to confirm Stonesoft's AET findings, the issue suddenly sprung to international prominence, with a number of articles heralding the end of IDS/IPS systems' ability to detect even the most mundane attacks. At the same time as this second release, Stonesoft also erected www.antievasion.com, a site full of pretty graphics and hype about AETs.

SEARCH THE BLOG

Search

BLOG ARCHIVE

- ► 2012 (12)
- ► 2011 (24)
- ▼ 2010 (94)
  - ► December (4)
  - ► November (2)
  - ▼ October (4)
    - Rule Release for Today, Thursday October 28th, 201...
    - Rule Release for Today, Tuesday October 26th, 2010...
    - Some Facts About Advanced Evasion Techniques

STONESOFT

Более того…

- VRT (в статье от 22.10.2010) утверждает что SourceFire прошел тест NSS Labs 2009 года, однако:

METHODOLOGY VERSION: 6.0
DECEMBER 2009

Product Line	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	FTP Evasion	TOTAL
[redacted]	✓	✓	✓	✓	✓	PASS
[redacted]	✓	✓	✓	✓	✓	PASS
Sourcefire	✓	✓		✓	✓	FAIL

Более того...

Product Line	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	FTP Evasion	TOTAL
[redacted]	√	√	√	√	√	PASS
[redacted]	√	√	√	√	√	PASS
Sourcefire	√	√	√	√	√	PASS
[redacted]	√	√				FAIL
[redacted]	√				√	FAIL
[redacted]			√			FAIL
[redacted]						FAIL

RESISTANCE TO EVASION*

* Although the Sourcefire 3D 4500 failed to detect an RPC Fragmentation evasion attempt in our Q4 2009 test, a fix to the product resolving this issue was subsequently validated by us on February 10, 2010.

- Интересно, что от 10.02.2010 есть «новый официальный», «исправленный» отчет.
- Но почему бы не сказать это открыто?

В декабре 2010 NSS Group изменила методику тестирования, добавив дополнительные проверки по Evasion-техникам (версия 6.1 – см. подробнее отчет о тестировании)

Новые бюллетени, старые песн

http://www.cert.fi/haavoittuvuudet/2011/haavoittuvuus-2011-071.html

С языка: финский На: английский Перевести

06/14/2011

IDS / IPS systems of protection provided by-pass methods

Location:	- Active network equipment	For more information
Attack Method:	- Remote Access	For more information
Abuse:	- Security Override	For more information
Solution:	- Amending Software	For more information

Stonesoft has reported to CERT-FI technologies, which can be used to bypass intrusion detection and prevention systems (IDS / IPS). The vulnerabilities associated with difficulties in the interpretation of the TCP protocol and MSRPC case. Changes in protocol packets can create a situation in which the IDS / IPS does not interpret the traffic correctly, but the receiving device to keep it accurate. Some of the techniques require multiple edits combination of several series of packets.

Using the techniques that an attacker can use the known attacks without the IDS / IPS systems are capable of detecting or preventing them. CERT-FI to keep vulnerabilities of these technologies, because they help to bypass the network protections. Stonesoft reported to CERT-FI for 124 different examples of by-pass methods, which can be roughly divided into eight different categories.

The vulnerability Co-ordination:

CERT-FI vulnerability remediation will be undertaken to coordinate cooperation with Stonesoft and manufacturer partners. CERT-FI has discussed the case of a large number of manufacturers.

Vulnerable software:

Checkpoint

- Check Point has verified That All versions of the Check Point IPS blade properly block and report a These evasion techniques. Well or IPS update patches are required. For details please read the Following

(MS-RPC over CIFS Fragmentation)

Top Layer Security

- Top Layer Security has Evaluated the IPS 5500 E-Series against These evasion techniques, and verified That they are not in Successful bypassing IPS protection. Please visit www.toplayer.com for more details.

SOLUTION AND LIMITATION OF OPPORTUNITIES:

Update the vulnerable software manufacturer's instructions. Attack detection and response systems, users should consider complementary methods cyber attacks and to prevent observation.

Официальные ответы вендоров на AET

AET vulnerabilities reported through global CERT vulnerability coordination process to all vendors

1. Набор из 24 AET в июне 2010
2. Набор из 124 AET в феврале 2011
3.Набор из 180 AET в марте 2011

Производитель	Комментарии вендоров (источник: http://www.cert.fi/en/reports/2010/vulnerability385726.html) от 26 марта 2012
Checkpoint	Checkpoint has released an advisory. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_dogoviewsolutiondetails=&solutionid=sk59468
Palo Alto NW	No comments about remediation
Juniper	No comments about remediation
McAfee	No comments about remediation
Fortinet	No comments about remediation
Cisco	Cisco PSIRT is aware of the issues reported by StoneSoft and is actively investigating what impact these vulnerabilities may have on Cisco products. PSIRT will disclose any security vulnerabilities discovered in compliance with Cisco's security vulnerability policy: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
HP/ Tipping Point	HP DVLabs has tested the evasion techniques against the TippingPoint IPS and found that all of the evasion techniques were NOT successful. TippingPoint customers are not impacted and no further updates are necessary. Customers may contact the TAC for more information.
Top Player	Top Layer Security has evaluated the IPS 5500 E-Series against these evasion techniques, and verified that they are not successful in bypassing IPS protection. Please visit www.toplayer.com for more details.
Sourcefire	No comments about remediation
Trend Micro	Trend Micro has completed its investigation into these issues and found that Deep Security version 7.5 and later fully protects against these issues. Customers are encouraged to upgrade to the latest version of Deep Security.

Вопросы?

Контакты:
info.russia (at) stonesoft.com

STONESOFT