Ætievasion

Современная защита от сетевых угроз – безопасность реальна?

РусКрипто’2011

STONESOFT

Secure Information Flow

Ландшафт современной киберпреступности

- Активная криминализация хакерской активности
- Атаки через социальные, сетевые сервисы
- Атаки на облачные технологии и из них:
  - Мультивекторные атаки
  - Террористические организации начали выдавать «гранты» на разработку методов проникновения …

Æntievasion
BY: STONESOFT

Эволюция атак ...

Атаки переходят на уровень приложений и делаются все более изощренными

Æntievasion
BY: STONESOFT

What's New

CIO 'Political' Cyberattacks Hit Half of Large Companies

InfoWorld OCTOBER 01, 2010 Zeus botnet thriving despite recent arrests

Хорошие новости: это не новый эксплоит или уязвимость.

Плохие новости: Кибер-террористы и хакеры увеличивают успешность своих атак.

Уже сейчас есть множество причин для волнений.

What's New

- Кибер преступники и изощренные хакеры **увеличивают свои «успешные достижения»** в части направленных атак путем применения современных техник. **Таких как техники обхода.**

CNN.com/US

HOME | ASIA | EUROPE | U.S. | WORLD | WORLD BUSINESS | TECHNOLOGY | ENTERTAINMENT | WORLD SPORT | TRAVEL

Hot Topics » Cheating Death - Money & Main St. - Latino in America - What If? - What Matters -

The Washington Post

Hot Topics Texas flag Chilean miners timeline 'Stone' Cliff Lee Kristi Noem Michelle Rhe

Waiting For Surgery: 5 Yea
In 5 Minutes You Can Save Him.

washingtonpost.com > Technology > Tech Policy

POST BUSINESS *Obama makes a villain out of Wall Street*

CLARIFICATION TO THIS ARTICLE
This article about Stuxnet, a computer worm designed to damage industrial control systems, said that a control-system malfunction in a natural gas pipeline resulted in the explosion and fire that killed eight people last month in San Bruno, Calif. Federal investigators say they have not yet established a link between the blast and the accidental malfunction, which an expert quoted in the article cited as an illustration of the kind of damage that could be done intentionally with Stuxnet.

U.S. power plants at risk of attack by computer worm like Stuxnet

By Lilon Nakashima
Washington Post Staff Writer
Friday, October 1, 2010; 2:49 PM

A sophisticated worm designed to infiltrate industrial control systems could be used as a blueprint to sabotage machines that are critical to U.S. power plants, electrical grids and other infrastructure, experts are warning.

The discovery of Stuxnet, which some analysts have called the "malware of the century" because of its ability to damage or possibly destroy sensitive control

An Iranian security man stands next to journalists outside the reactor building of the Russian-built Bushehr nuclear power plant in southern Iran on August 21, 2010. The Stuxnet computer worm has infected

Breaking news | Omar Reygadas, 56, who has 6 children, 14 grandchild grandchildren, is 17th of 33 miners rescued.

April 21, 2009 Updated 2042 GMT (0442 HKT)

Hackers stole data on Pentagon's newest fighter jet

From Mike Mount
CNN Senior Pentagon Producer

WASHINGTON (CNN) -- Thousands of confidential files on the U.S. military's most techn fighter aircraft have been compromised by unknown computer hackers over the past tw senior defense officials.

The Internet intruders were ab data related to the design and systems of the Joint Strike Fig computers of Pentagon contra designing and building the air the officials, who did not want because of the sensitivity of the

In addition to files relating to th gained entry into the Air Force's systems, according to the offici In, the Internet hackers were a information as the locations of

COMPUTERWORLD

Topics | News | In Depth | Reviews | Blogs | Opinion | Shark Tank

Security | App Security | Business Continuity | Cybercrime and Hacking | DRM an Privacy | Security Hardware and Software

View our resources | Connecting to the Cloud with F5 and VMware VMo

Home > Security

News

Cyberattacks raise e-banking security fears

Government, business groups urge banks to upgrade security controls as attacks grow

By Jaikumar Vijayan
March 10, 2010 07:35 AM ET | Comments (2) | Recommended (18) | Share

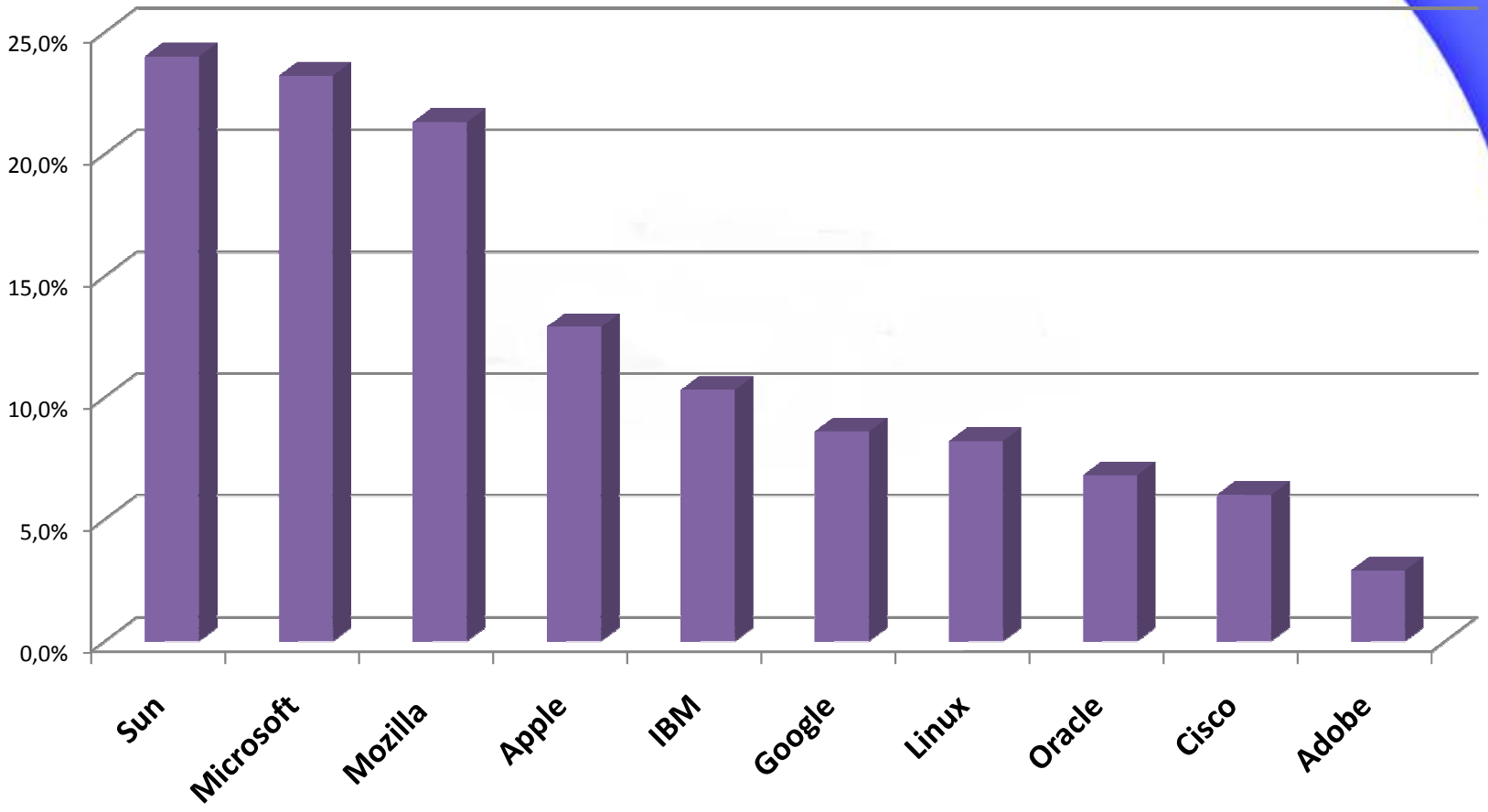
Computerworld - The unabated plundering of online bank accounts belonging to small and midsize businesses is raising significant questions about the authentication and fraud-detection mechanisms now used by financial institutions.

Such cyberthefts have led multiple businesses to file lawsuits against their banks and prompted government regulators to call on financial institutions to improve their security systems.

The FDIC recently disclosed that during the final 2009 quarter alone, cyberthieves stole more than $150 million from small and midsize business accounts.

Ænti evasion
BY: STONESOFT

Топ 10 вендоров с непатченными уязвимостями в 1 квартале 2010



IBM-X-Force-Vulnerability-Threats-1H2010

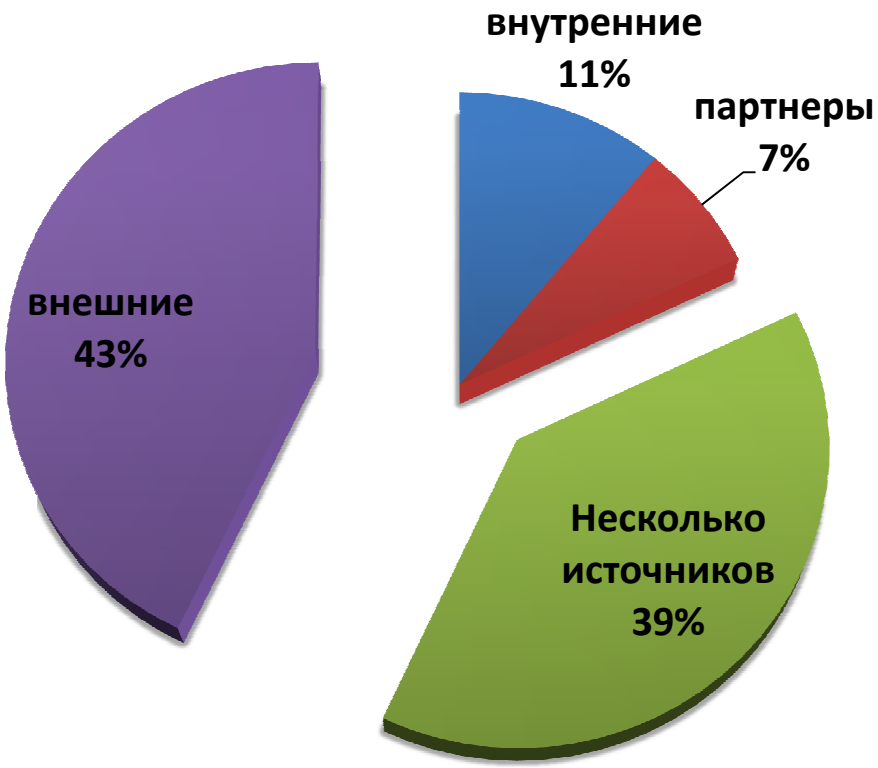
Критичные уязвимости на которые не выпущен патч

Vendor	Percent of 2010 H1 Disclosures with No Patch	Percent of Critical & High 2010 H1 Disclosures with No Patch
All Vendors - 2010 H1 Average	55%	71%
Sun	24%	9%
Microsoft	23%	11%
Mozilla	21%	4%
Apple	13%	0%
IBM	10%	29%
Google	9%	33%
Linux	8%	20%
Oracle	7%	22%
HP	7%	5%
Cisco	6%	2%
Novell	5%	10%
Adobe	3%	2%

IBM-X-Force-Vulnerability-Threats-1H2010

Атаки на ресурсы

До 82% инцидентов, являются результатом атак извне системы



Æntievasion
BY: STONESOFT

"2009 Data Breach Investigations Report", Verizon Buziness

Некоторые проблемы распространения патчей у популярных вендоров

- Корпорация Microsoft, выпустившая недавно очередную порцию патчей ***столкнулась с трудностями при распространении заплаток***.
- Представители компании Symantec, заявили, что в состав октябрьских заплаток вошли патчи для дыр, эксплойты для которых уже циркулируют в интернете.

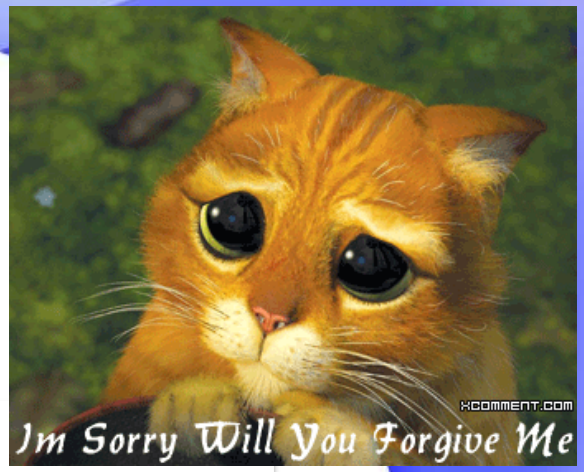
- В январе-феврале 2009 эпидемия червя Conflicker стала возможной только благодаря тому, что во многих компаниях не были установлены обновления безопасности, опубликованные в октябре 2007 г.

- **Администраторы просто не успевают устанавливать патчи!**
  - **Иногда для установки патча надо потратить до 30 дней (!!!) (US Air Force)**

- **Появляются статьи победного содержания**
  - ***«Уфф. Сегодня патчи можно не ставить»***
  - *«Виртуальный патч спасет от атак»*
  - *И др.*

Ænтievasion
BY: STONESOFT

Печально признавать, но…



Информационные ресурсы **незащищены.**

Ежедневные операции и бизнес подвергаются риску .

Ложное чувство защищенности делает организации легкой мишенью.

Большинство (>90%) современных устройств безопасности **не подготовлены и не могут** обеспечить защиту.

Ætievasion
BY: STONESOFT

Исследования

StoneSoft выявил новые специфичные техники обхода (evasion techniques), которые могут быть использованы или скомбинированы в любом порядке, чтобы обойти возможность детектирования устройствами безопасности.

AET (Advanced evasion techniques, динамические техники обхода)*

…и новый виток гонки **ANTI-EVASION** техник и приемов начался!

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

Æntievasion
BY: STONESOFT

Техника обхода (Evasion)

Определение

Техники обхода являются средством **сокрытия** и/или **изменения** атак с целью избежать обнаружения и блокирования средствами защиты. Техники обхода позволяют искушенным злоумышленникам доставлять *любой вредоносный* контент, эксплоит или атаку до уязвимой системы **без** ее *обнаружения*, хотя обычно воздействие было бы обнаружено и остановлено. Средства защиты **оказываются неэффективными** против таких техник обхода. *(аналогичным образом истребитель-стелс может нанести удар, не будучи обнаруженным радаром и другими системами защиты)*

Ænti evasion
BY: STONESOFT

Исследования в области методик обхода

- Первый текст об атаках против систем IDS появился в 1997
- Одно из первых полноценных описаний атак было дано Ptacek and Newsham в техническом отчете 1998
- В 1998, появилась статьяв журнале Phrack с описанием методик обхода сетевых систем обнаружения вторжений
- Handley и Paxson предложили нормализацию в 2001
- Gorton и Champion предложили комбинации в 2004
- Moore и Caswell обсуждали техники обхода на конференции Black Hat в 2006

Ænti evasion
BY: STONESOFT

Применение техник

Большинство техник обхода являются нормальными методами работы протокола, которые повсеместно используются.

IP fragmentation

TCP segmentation

MSRPC fragmentation

TCP urgent pointer

SMB fragmentation

MSRPC alter context

TCP TIME_WAIT

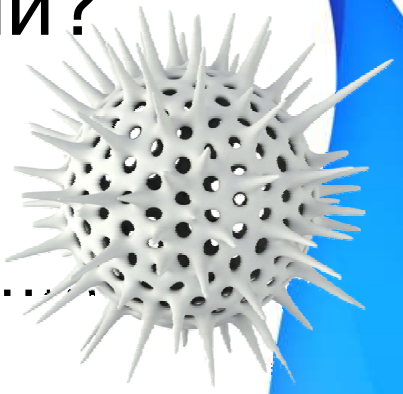
IP random options

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

Æntievasion

BY: STONESOFT

Почему нельзя решить проблему традиционными технологиями?



www.mitre.org

- CVE List содержить >45,000 CVE Identifiers ……

С другой стороны:

- Каждая система IPS имеет примерно 3000–4000 сигнатур
- В большинстве решений при включении дополнительных 1000 сигнатур наблюдаются проблемы производительности
- Если хотя бы 1% из множества комбинаций AET возможен и работает, то это дасть более 1 миллиона!

Æntievasion
BY: STONESOFT

По своей природе.

(на практике)
AETs – это динамические, безусловные, имеющие **виртуально бесконечное количество вариаций**, и нераспознаваемые традиционными методами детектирования.

(с технической точки зрения)
Их можно **стекировать** и они могут работать на **всех уровнях** стека TCP/IP , равно как **для разных протоколов** или их комбинаций одновременно.

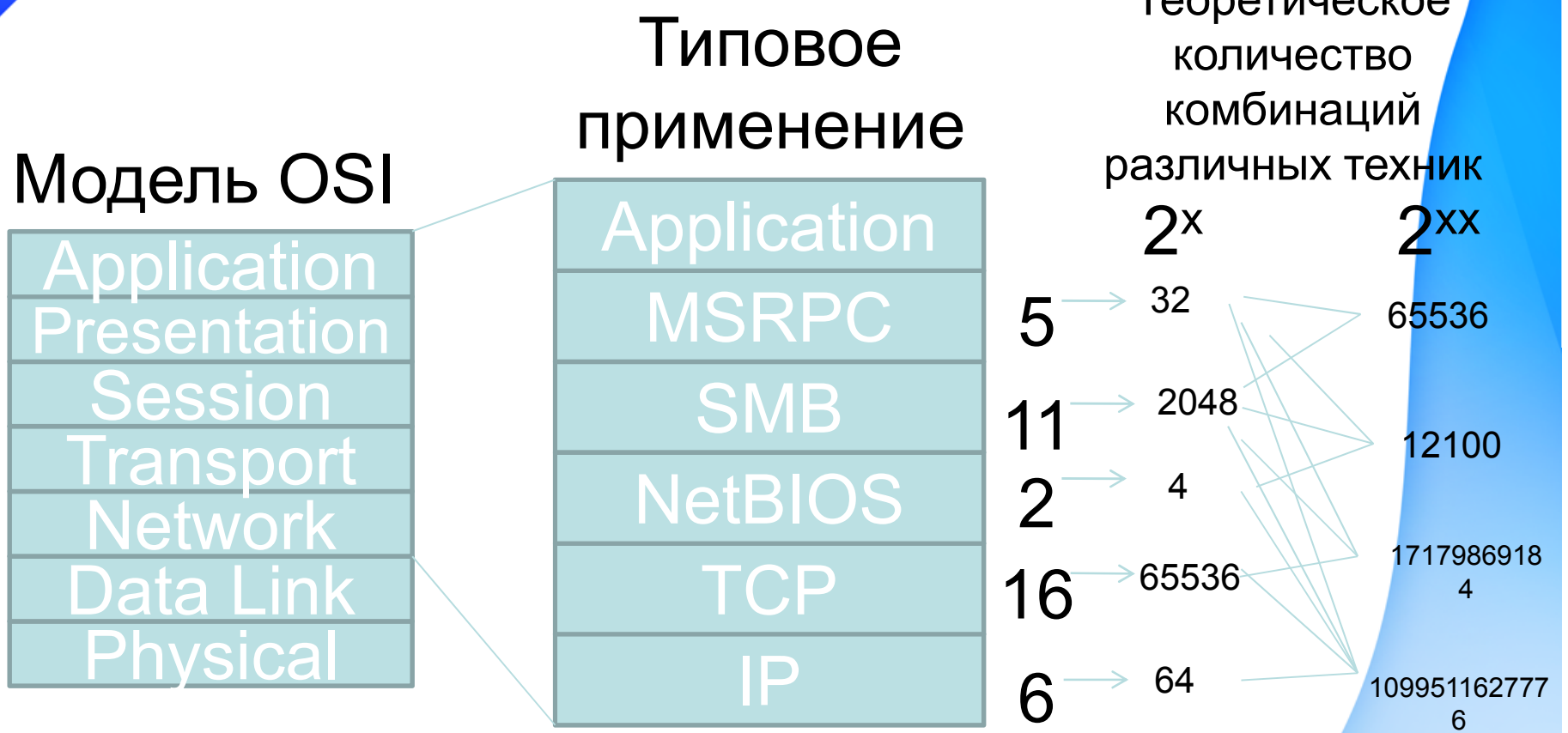
Текущее количество техник обхода...

$$2^{31}$$

...и оно продолжает увеличиваться.

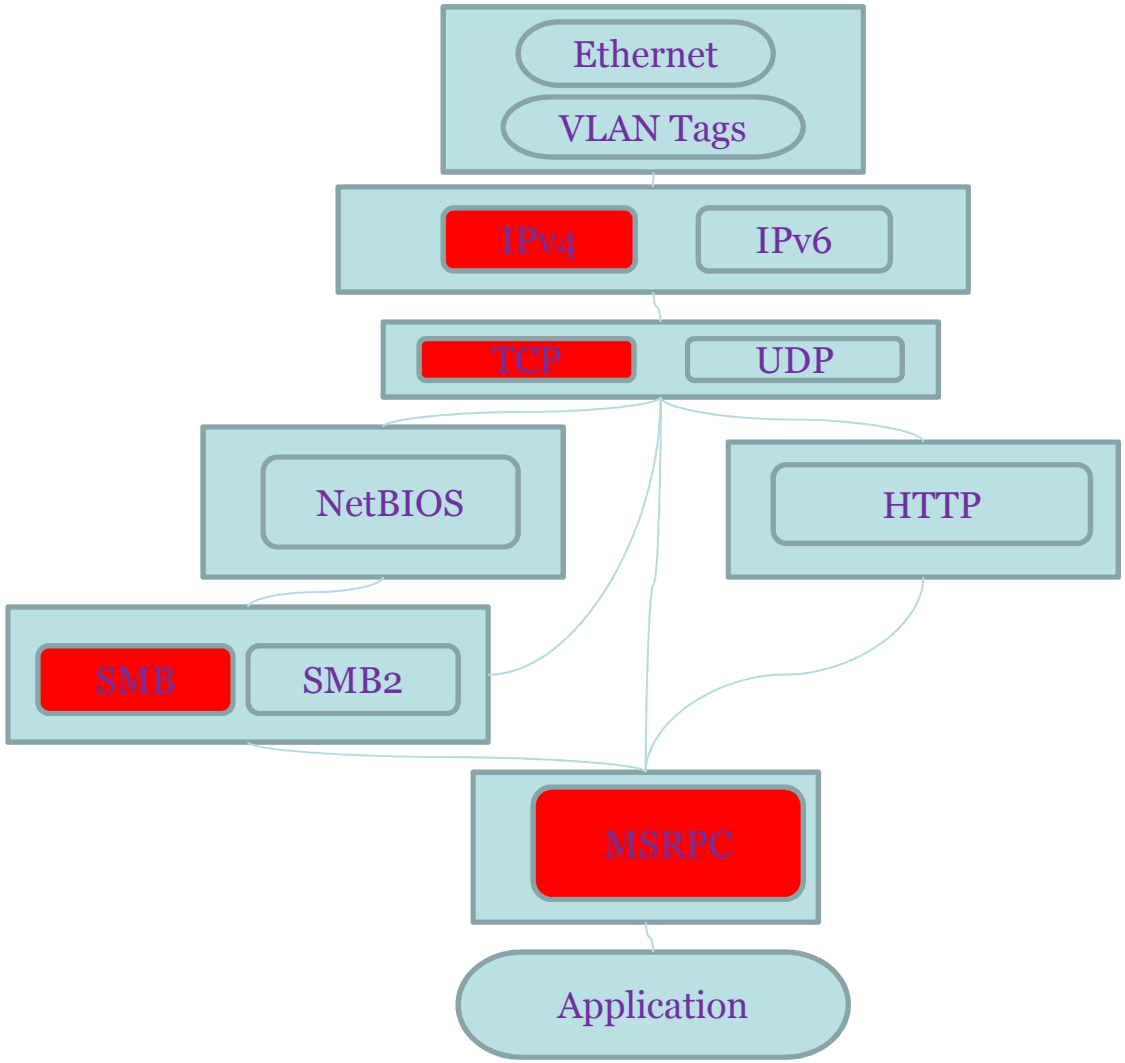
Ætievasion
BY: STONESOFT

Возможные комбинации



Ænti evasion
BY: STONESOFT

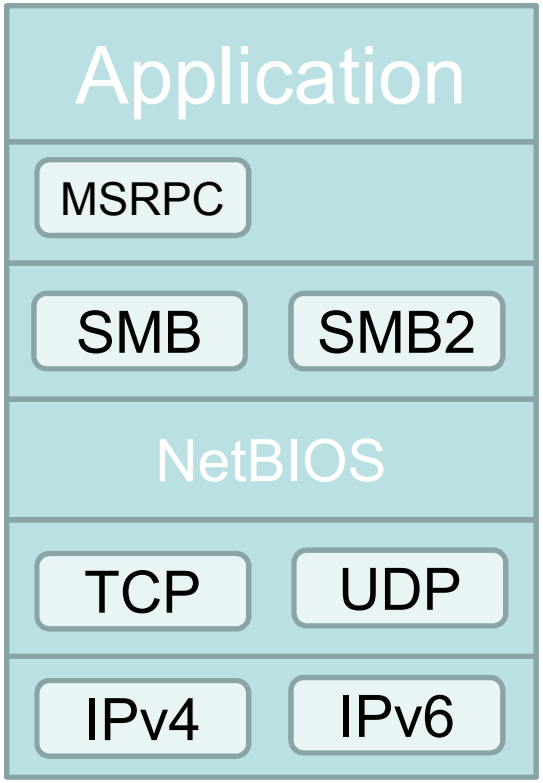
MSRPC Application



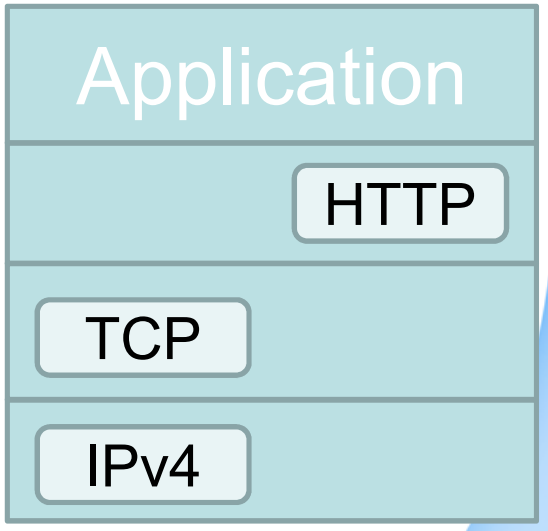
Æntievasion
BY: STONESOFT

Варианты использования

Не все комбинации возможных, поскольку техники обхода зависят от применяемого протокола, и не все комбинации одного и того же уровня можно использовать одновременно



Техники обхода зависят также от приложениия/цели атаки, поскольку ПО/система поддерживает только определенные протоколы



Æntievasion
BY: STONESOFT

Суть системы IPS (= virtual patch)

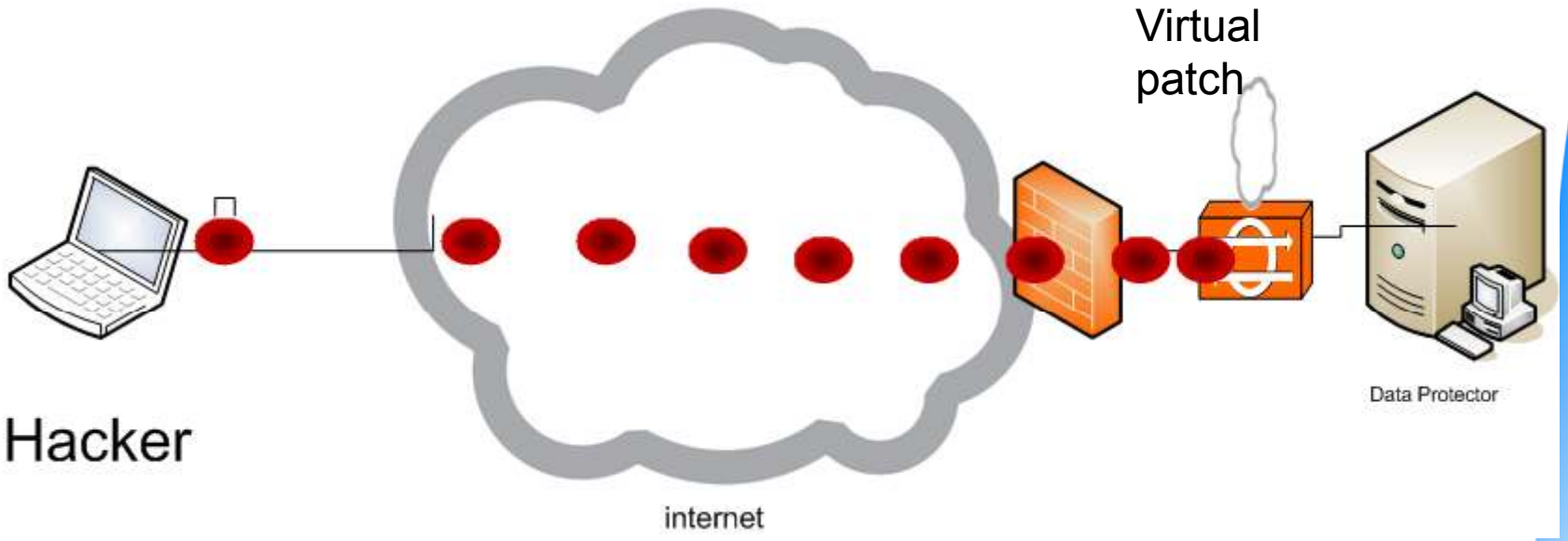
- Защита уязвимых (узлов) систем и серверов от удаленных эксплоитов
- «глубокая инспекция» пакетов
- Нормализация трафика и идентификация эксплоитов
- примеры: МЭ класса NG, IDS/ IPS и UTM

Пример использования

- Позволяет администраторам увеличить время на установку патча
- Позволяет более тщательно тестировать патчи перед установкой на «боевые» системы
- Иногда патча от вендора для уязвимости недостаточно, а IPS дает дополнительную защиту

Æntievasion
BY: STONESOFT

Технология «виртуального патча»

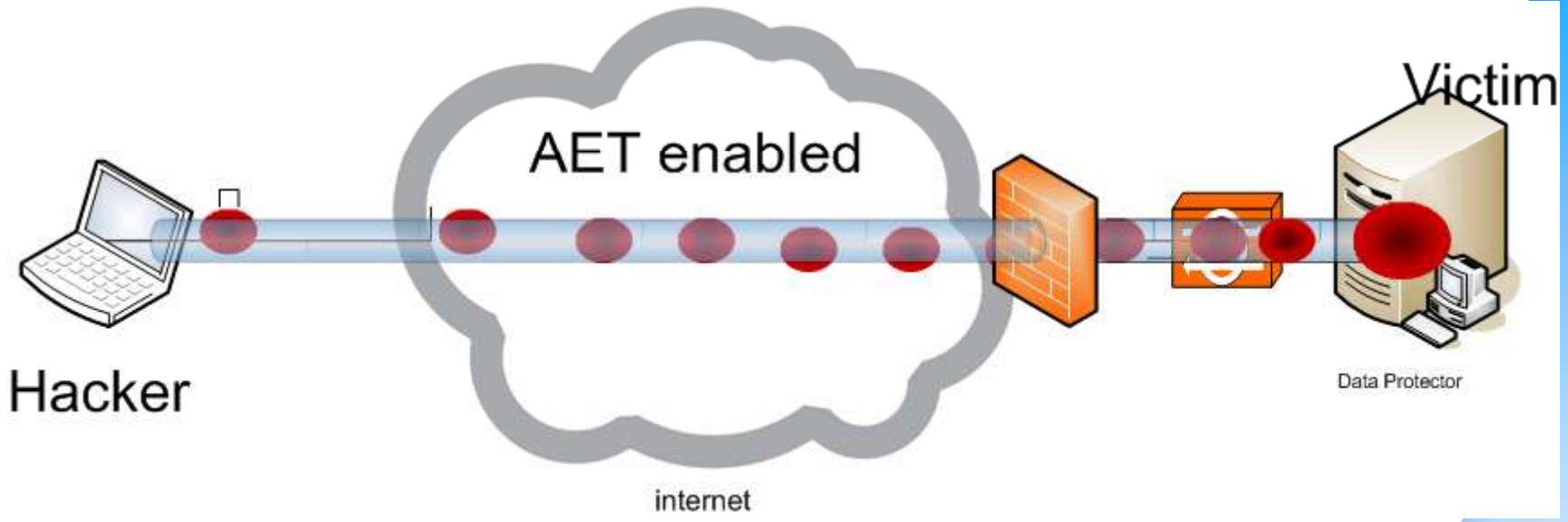


IPS детектирует атаку и блокирует подключения к уязвимым сервисам

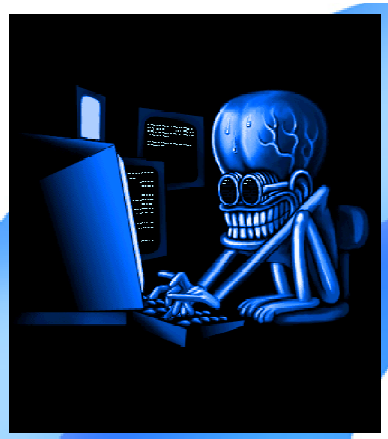
Æntievasion
BY: STONESOFT

«Evasion» можно сравнить со скрытым каналов доставки

IPS или МЭ не видят атаку!



Æntievasion
BY: STONESOFT



Использование AET

- Изощренные направленные атаки против хорошо защищенных систем.
- Организованными преступными группироваками, имеющими широкий арсенал средств и сильную мотивацию.
- С точки зрения хакеров, AETs работает как универсальная отмычка ко всем замкам. Техники позволяют спокойно перебрать эксплоиты и выбрать тот, который работает.
- Техники являются страховкой от поимки.

Ætievasion
BY: STONESOFT

Нормализация

- Нормализация протоколов – это способ **борьбы** с техниками обхода
- **Суть «готовности к борьбе с техниками обхода» (Anti Evasion readiness)** зависит от способностей и эффективности систем осуществлять нормализацию на всех уровнях
- Это означает, что осуществляется нормализация для **всех** протоколов при декодировании, а эксплоиты могут быть детектированы сравнением по регулярным выражениям -> нужно только знать, как выглядит эксплоит

Æntievasion
BY: STONESOFT

```
root@ipforge:/usr/local/predator# sh pwn-through-snort
Initializing IPForge based on the configuration..
      -Using random key 20186458297206748233838858027203322352 2
Started at IP 10.0.1.101, MAC de:ad:01:00:01:02. Attacking against 10.0.1.200
Exploit run 1: TCP evasion: time_wait, MSRPC fragstyle: 16byte, MSRPC evasion: big_endian,alter_context}
-Failed to connect to shell
Exploit run 2: IP fragstyle: 16byte,8byte,out_of_order,fwd_overwrite,last_first,24byte, TCP fragstyle: 1byte, SMB fragstyle: 16byte
Exploit run 3: IP fragstyle: random_order,8byte,last_first,256byte, TCP fragstyle: 1byte, MSRPC evasion: random_object}
Exploit run 4: IP fragstyle: 16byte,8byte,out_of_order,last_first,one_duplicate,256byte,24byte, TCP evasion:
      time_wait,urgent_ptr, MSRPC fragstyle: 16byte
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

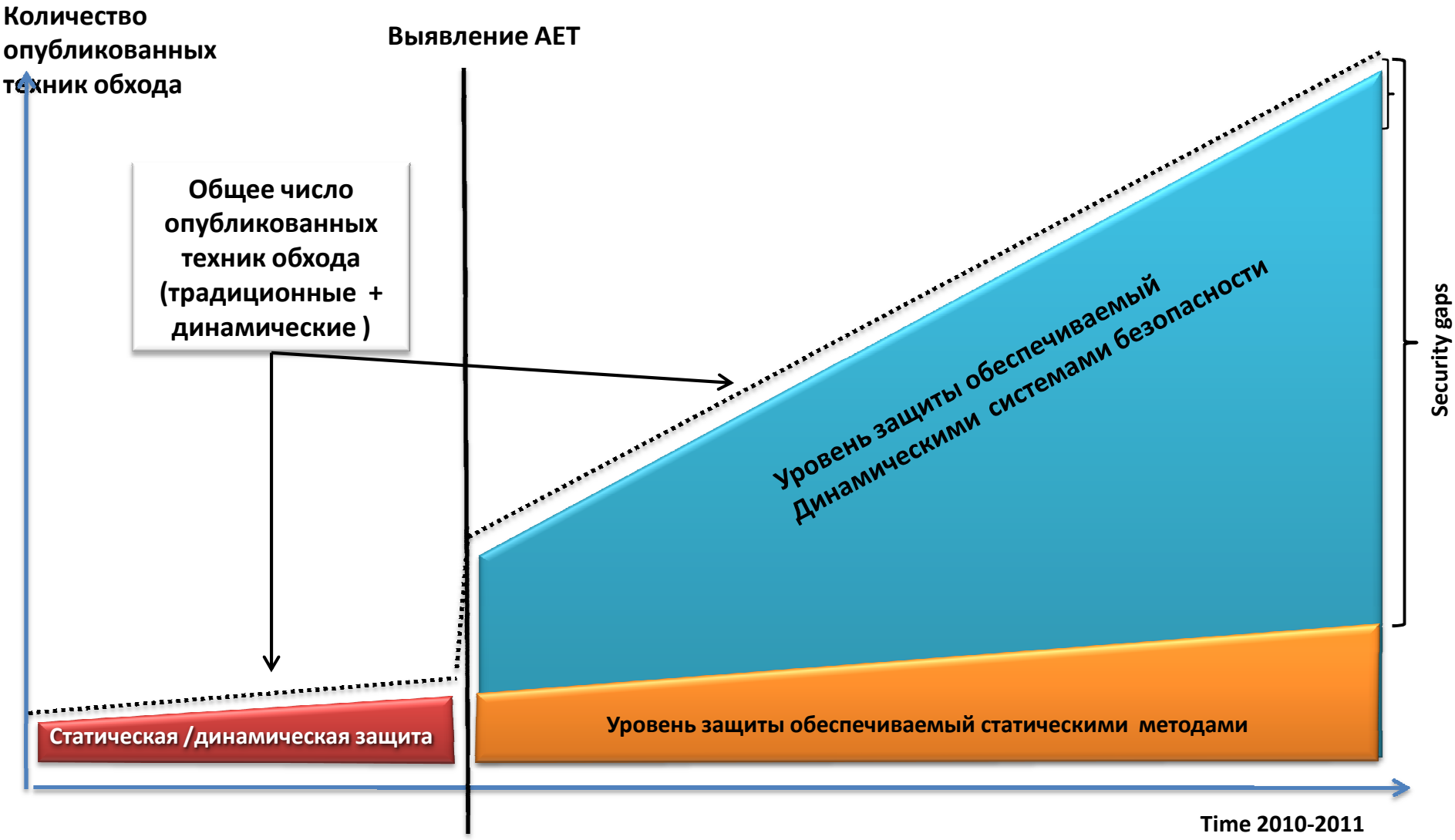
Если нормализация не работает, то эксплоиты проходят «насквозь»....

...а технология **предотвращения вторжений**...

...оказывается **неэффективной и бесполезной.**

Æntievasion
BY: STONESOFT

Рассчетный уровень опубликованных техник и уровни защиты (динамические vs. статические).



«Мысли вслух»

- Согласно любому стандарту (например СТО БР ИББС), оценка актуальности угроз безопасности и целесообразности применяемых мер противодействия должна основываться на **вероятностях реализации этих угроз**.

Незамеченная атака на непропатченные ресурсы дает очень высокую вероятность !

Текущая ситуация

AETs не работают традиционным образом и текущий уровень защиты от них **близок к нулю**.

Не имеет значения*:

- Чей продукт у Вас используется
- Насколько часто он обновляется
- Какие награды он получил
- Какие тесты он прошел

Ætievasion
BY: STONESOFT

Проблемы

- Исправление или переписывание стека протоколов занимает время
- Исправление или переписывание сигнатур для включения всех «техник обхода» занимает еще больше времени
- Идентификация всех возможных техник обхода и их комбинаций
- Тестирование на возможность реаизации техник обхода автоматизированным способом

…а в большинстве своем, зачастую почти невозможно.

Ænti evasion
BY: STONESOFT

Набор утилит ограничен

- Есть утилиты, в которых заложено несколько техник обхода
- Однако, эти утилиты ориентированы на эксплоиты, а не на техники обхода
- Полноценное исследование / наличие утилит для тестирования в области техник обхода отсутствует

Ætievasion
BY: STONESOFT

Текущие “УБЕЖДЕНИЯ”

Нет ПО, которое позволяло бы использовать несколько техник обхода на разных уровнях стека протоколов одновременно

Вывод: **поэтому это должно быть невозможно**

Такой инструмент потребует создание вручную стека протоколов TCP/IP, ориентированного на техники обхода.

Вывод: никто не будет этим заниматься – это нецелесообразно.

“Таким образом, текущего уровня тестирования недостаточно. Используется только небольшое число известных техник обхода и, более того, они реализуются только по одной и только на заданных уровнях стека”

Ætievasion
BY: STONESOFT

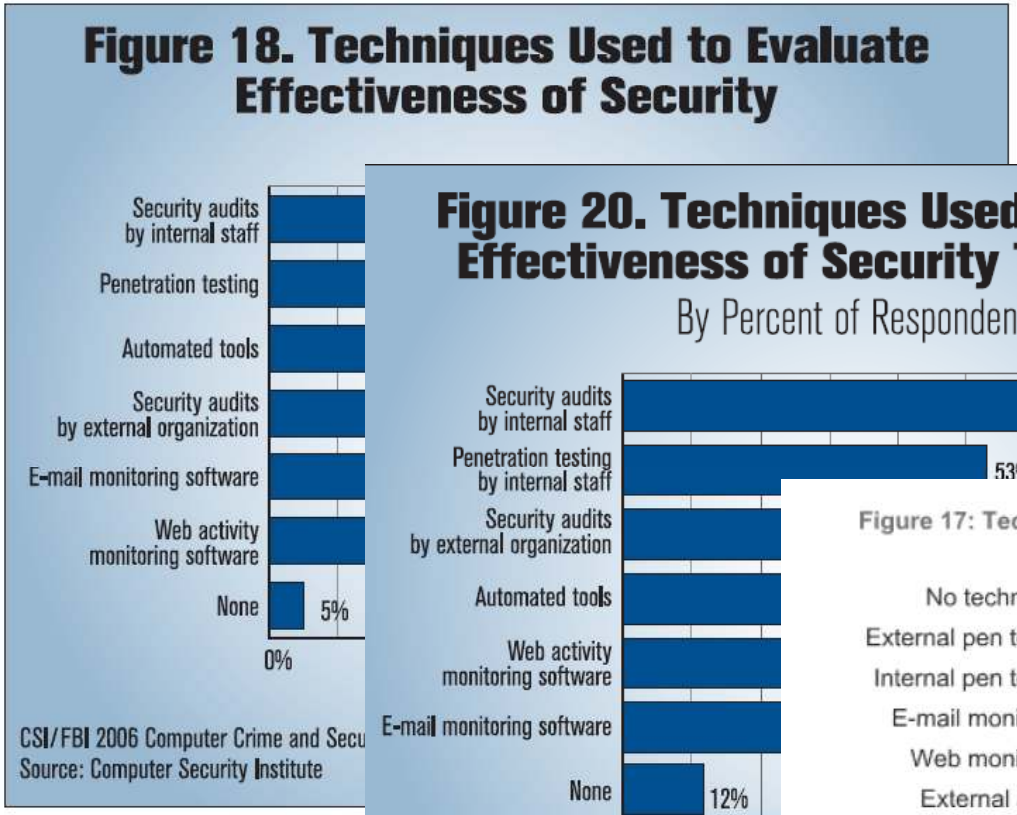
Текущие “УБЕЖДЕНИЯ”

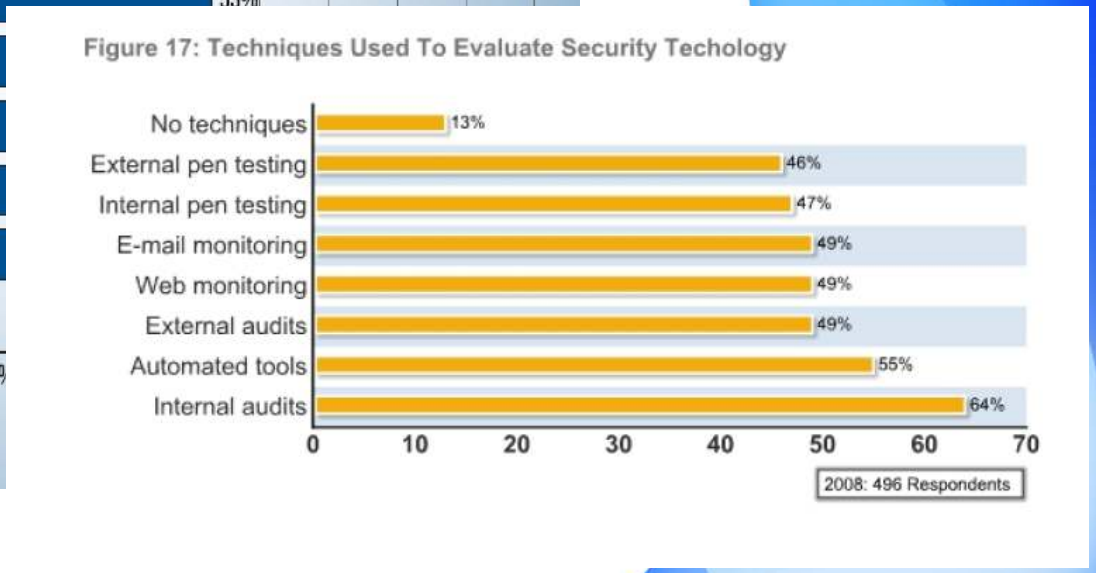
В конце концов, хакеры и преступники с большим количеством ресурсов не будут ничего делать нестандартного, не так ли?

…И они ограничены известными утилитами и техниками обхода.

Не правда ли?

Немного статистики...





Ætievasion
BY: STONESOFT

Predator 3.0

- **среда исследования** сетевых средств защиты, построеная для *автоматизированного* тестирования
- **Evasion fuzzer**
  - «играет» параметрами протокола-контейнер, оставляя в целостности полезную нагрузку (ровно в том виде, в котором ее интерпретирует цель)
  - Способен одновременно использовать несколько случайно выбираемых техник обхода на разных уровнях

Æntievasion
BY: STONESOFT

Архитектура «Хищника»

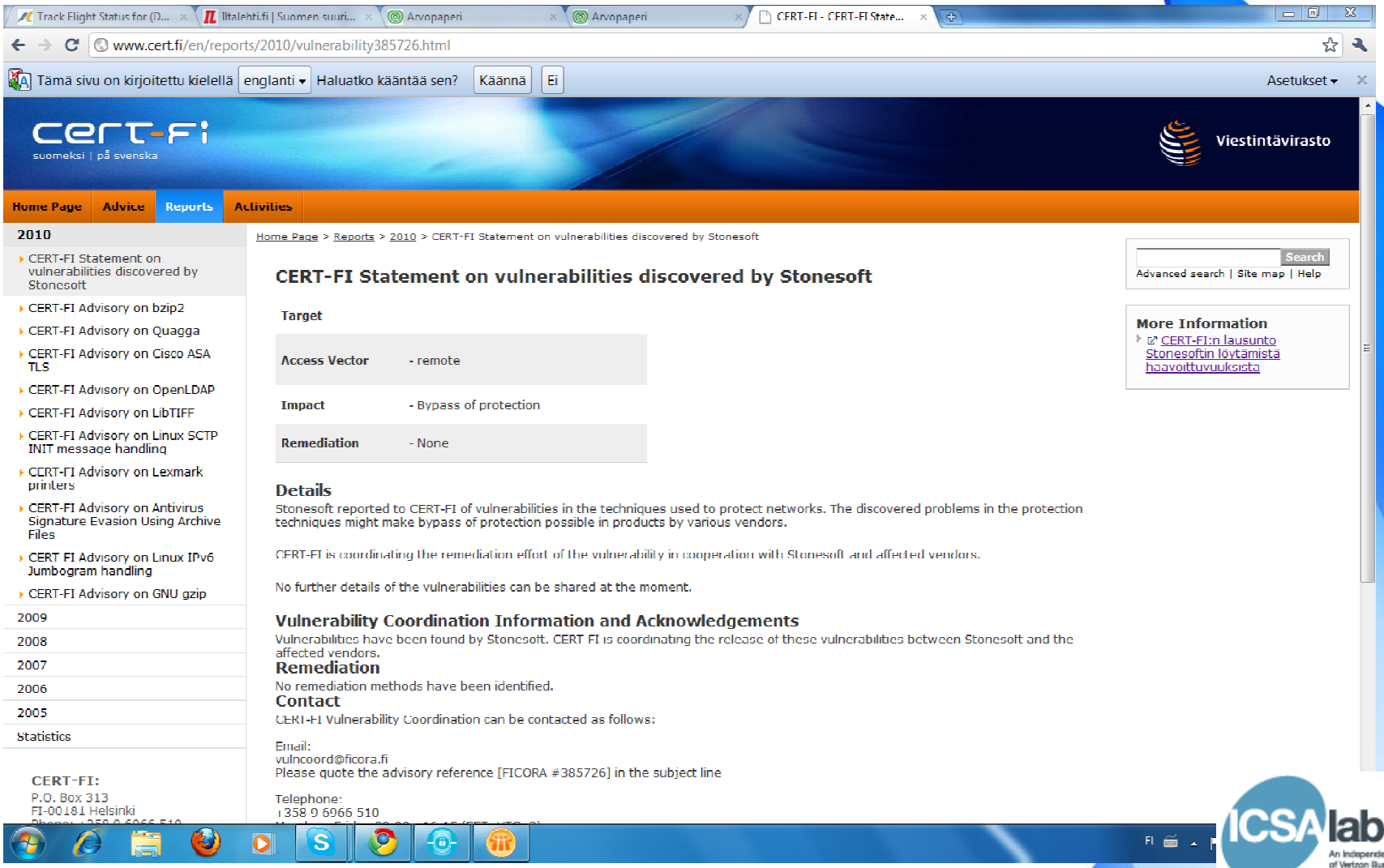
- Не использует **TCP/IP стек ОС**
- **Нарушает правила** консервативной передачи/свободного приема (RFC 791)
- Использует **более** одной техники обхода за раз
- Не полагается на убеждения, что **нижние уровни** стека TCP/IP статические и хорошо защищены
- Построен на базе IPForge
  - TCP/IP стек создан на базе Ruby, независимо от стека ОС
  - Позволяет тестировать на всех уровнях

Ætievasion
BY: STONESOFT

Развитие «Хищника»

- Первая версия в 2007
  - 12 техник обхода, которые не стекировались
- Текущая верия 3.0 имеет более 180+ техник обхода, которые стекируются. И развивается…
- 2^{180} = 1532495540865888858358347027150309183618739122183602176
- 180! = 2008960624991342996569513368984668389175403407988677779404353351600448609533959809411801381120973097356315941010373996096710321321863314952736095985319667309729456535588198064750643538568581574450408092095603584633196446648911142564300178241417967538181923386423026933278187319860396032000000000000000000000000000000000000000000000000000000
- Становитсяневозможно проверить все комбинации
- IPv6 добавляет большее пространство вариантов

Подтверждения со стороны - Cert



Ænti evasion
BY: STONESOFT

ICSA labs
An Independent Division of Verizon Business

New era of Advances Evasion techniques

- *"Stonesoft has **discovered new ways** AETs can evade many network security systems," said Jack Walsh, intrusion detection and prevention program manager at ICSA Labs. "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.**"*

Ænti evasion
BY: STONESOFT

ICSA labs
An Independent Division of Verizon Business

Коммерческие организации

- 2009

Product Line	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	FTP Evasion	TOTAL

  - 63 evasion техники

- 2010

Product Line	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	HTML Evasion	FTP Evasion	TOTAL

  - 74 evasion техники

- + новые проверки в 2011!

Ænti evasion
BY: STONESOFT

NSS Labs
Security. Certified.

Методы тестирования

- Куплены системы IPS разных вендоров (главным образом «challengers» или «leaders» из «Gartner Magic Quadrant»)
- Все с последними версиями ПО и обновлениями
- Конфигурация по умолчанию или самая строгая из возможных встроенных

Æntievasion
BY: STONESOFT

Основные открытия

- Некоторые вендоры уязвимы техникам обхода, которые существуют в автоматизированных средствах более 10 лет
- Все вендоры уязвимы хотя бы каким-то техникам обхода, которые обсуждались в статьях, но не были доступны в виде утилит
- Идентифицированы новые техники обхода, которые работают против каждого вендора

Æntievasion
BY: STONESOFT

Другие открытия

- Сложные (комбинированные) техники обхода имеют большую вероятность успешного использования, чем они же, но по отдельности

- Существующие методики тестирования, применяемые для опробования атак / pen.test-ов, не являются идеальными для тестирования методик обхода

Æntievasion
BY: STONESOFT

Планы на будущее

- Исследование, очевидно, окажет положительное влияние на качество всех решений отрасли IPS / FWNG
- Лаборатории и исследователи будут уделять больше внимания техникам обхода
- Нужно проделать еще много работы ☺

Ætievasion
BY: STONESOFT

Вступайте в виртуальную армию
борьбы с техниками обхода на сайте...

www.antievasion.com