Современные угрозы и способы борьбы с ними

Максим Лукин

Руководитель направления
Информационная Безопасность

Communications Technology Innovations

Тренды 2015

Communications Technology Innovations

Рост киберпреступности

BYOx

Рост advacnced malware

киберпреступления

Технологии Интернет и связь **22.12.2014** 05:00

Брать по-крупному: группировка хакеров банков

Павел Седаков, Дмитрий Филонов

Хакеры из группы Anunak атакуют крупные банки, а не их клиент
рублей. Почему такие преступления считаются особо опасными

21.04.2015	В Кабардино-Балкарии осужден хакер, остановивший работу сайта правительства
17.04.2015	Хакеров, укравших 160 млн рублей, задержали в Москве
17.04.2015	WikiLeaks опубликовал похищенные документы компании Sony
10.04.2015	Компьютерный вирус украл $24 млн по всему миру
09.04.2015	Захарченко: Киеву «нужна война, пусть даже информационная»

Киберпреступления причиняют ущерб мировой экономике в размере порядка 445 млрд долларов в год

Communications Technology Innovations

Для взлома не нужно быть хакером

Любое ПО и услуги продаются на теневом рынке

[Взлом почты на заказ] Mail.Ru, Yandex.Ru, Rambler.I Smoyk	DroidJack - Android RAT с хорошим функционалом. Marlb0r0
| xakep.click | Взлом Email аккаунтов и Аккаунтов Соц.се Mr.Robot	RMS Builder 6.3.0.5 Box (скрытая установка, новые функции) Ltybcrf
Взлом email на заказ mail.xacking	MKL PRO Keylogger (1 2) Svas
Взлом почты на заказ, без предоплаты mailpass	[Софт] Удаленное управление компьютером (1 2) Zelont
Взлом почты ДЕШЕВО на заказ. hack-inbox	Сдам андроид софт в аренду Verm
Взлом почты на заказ Corp.Rese	NEW PMC сборка в формате XLS Gridmall
Взлом почты Mail, Yandex и Gmail от DizzyCap. DizzyCap	Стиллер Twilight Stealer 4 Marlb0r0
Работа! Нужны специалисты по взлому почты. Качественн Openmail	Kraken ботнет m1st
Взламаю WhatsApp, Skype, Vkontakte, Viber и многое друг ryjov.slavik	Продам исходники бота turbo
взлом электронной почты+корпоративки devergent	Халявный Keylogger Marlb0r0
Взлом почты [Mail.ru Yandex.ru Rambler.ru Gmail.com] burglary.mail	Z*Stealer новый стилер логинов и паролей DamRaiX
Взлом почты на заказ [mail, yandex, gmail, rambler] PupkinV	S&M service (loads/installs-от 60$, крипт/crypt-от 15$) chipddos
взлом практически любой почты, индивидуальный подхо BigStan	
РОСКОМЗАЗОР-ПОМОЩЬ УЖЕ В ПУТИ	

Communications Technology Innovations

Dark Market Silk Road 3.0

Трояны и другое интересное ПО

Escrow ✈ **Monetizing a RAT**
$8 USD / 0.029695 BTC
Vendor: **etimbuk** **+2523** **verified**
Category: **Others**
Ships From: **Worldwide...** Ships To: **Worldwide**

Remote Administration Tools/Trojans

1. Cerberus 1.03.4 BETA
2. Turkojan 4 GOLD
3. Apocalypse 1.4.4
4. Spy-Net 2.6

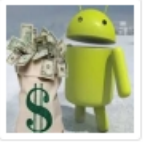
Rar password: Spy-Net

5. Pro Rat v1.9
6. Poison Ivy 2.3.2
7. Bandook Rat v1.35
8. Bifrost v1.0
9. CyberGate v.1.01.0
10. Lost Door v4.2 LIGHT
11. Beast 2.07
12. Shark v3.0.0
13. Sub7 v2.2
14. Pain RAT v0.1
15. xHacker Pro v3.0
16. Seed v1.1
17. Optix Pro v1.33
18. Darkmoon v4.11
19. CIA v1.3
20. Y3k RAT v1.0
21. MiniMo RAT v0.7
22. NetDevil v1.0
23. Deeper RAT v1.0
24. Schwarze Sonne RAT 0.1 Public Beta 2
25. Schwarze Sonne RAT 0.7
26. Schwarze Sonne RAT 0.8
27. Schwarze_Sonne_0.5_Beta
28. Schwarze Sonne RAT 0.2 Beta
29. [BUGFIX]SS-RAT 0.4 Final
30. A32s (fifth) RAT
31. Arctic R.A.T. 0.0.1 Alpha
32. CyberGate v1.02.0
33. CyberGate v1.03.0

How I banked in $14,580 in 14 Days

Price: $.99 USD / **0.003674 BTC**

Android App Profits



Price: $.99 USD / **0.003674 BTC**

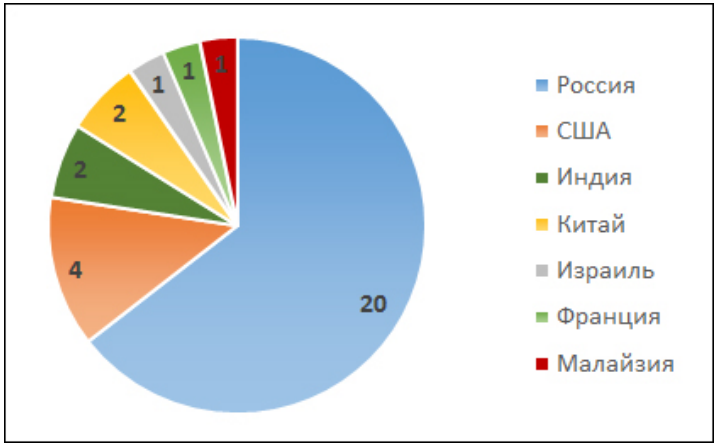
Ultra Hacker Tools with 83 RATs and 21 Binders

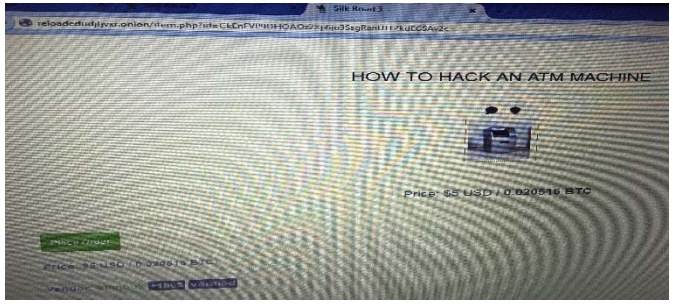
Price: $50 USD / **0.185597 BTC**

Place Order

Price: $50 USD / 0.185597 BTC

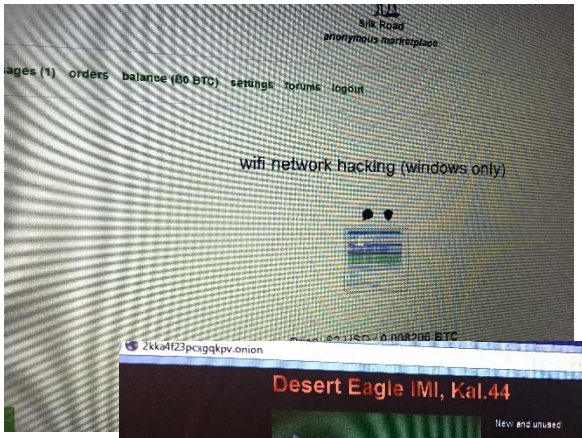
Как украсть у банка деньги?

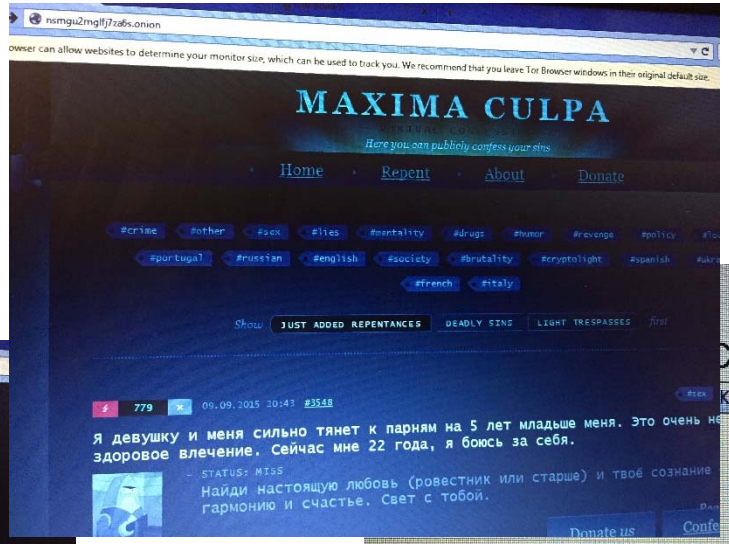


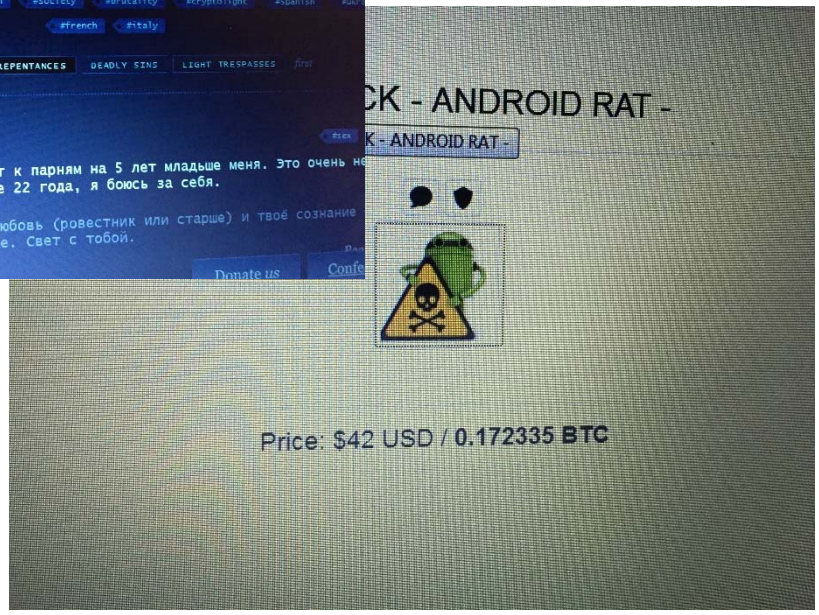


Еще немного про TOR

Communications Technology Innovations







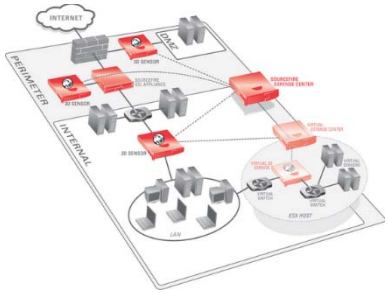
Communications Technology Innovations

С чего начать борьбу с угрозами?

Проведение комплексного аудита ИБ

- Анализ документации
- Экспертный аудит ИБ в том числе может включать аудит на соответствие Best Practice
- Анализ защищенности WEB приложений
- Анализ защищенности сети
- Тестирование на проникновение

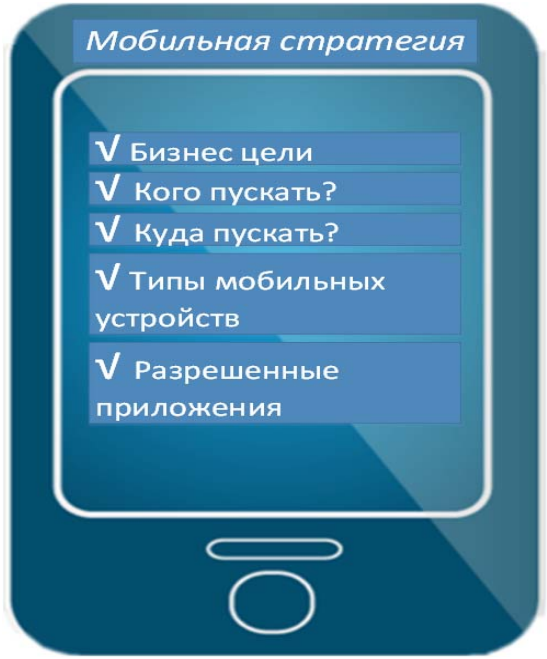
Тест на проникновение



- Тест на проникновение сети (внешний периметр,внутренний периметр,VOIP, Wi-Fi)
- Тест ДБО (системы мобильного банкинга, интернет банкинга)
- Анализ безопасности приложений
- Тестирование на проникновение WEB сайтов

Борьба с мобильными угрозами. Основные шаги

- Разработка мобильной стратегии
  - Идентификация бизнес-целей (Почта, телефония, доступ к ресурсам, совместная работа, продажи)
  - Определение типов поддерживаемых устройств
  - Разработка профилей безопасности
  - Разработка матрицы доступа
- Реализация мобильной стратегии

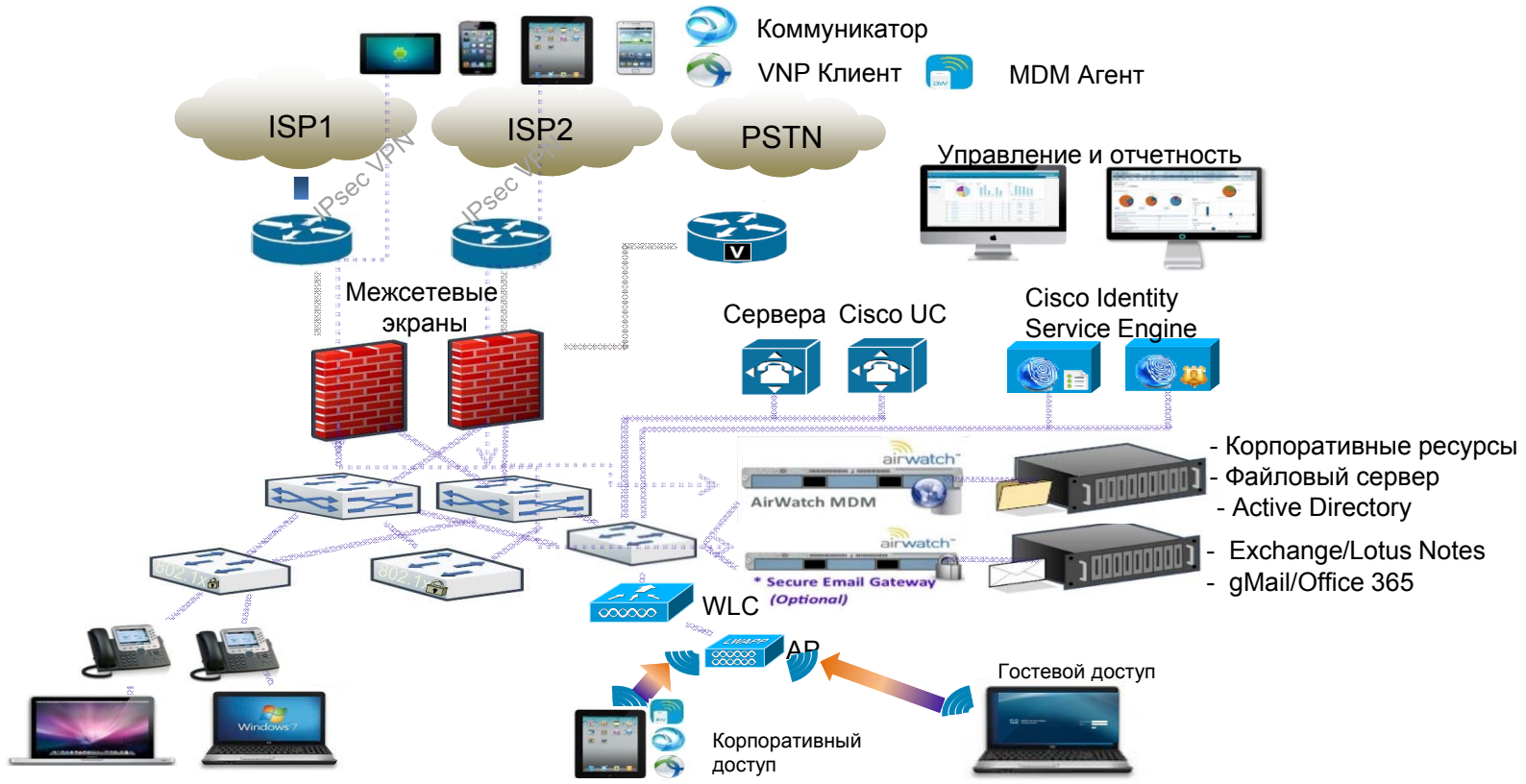


Разработка мобильной стратегии

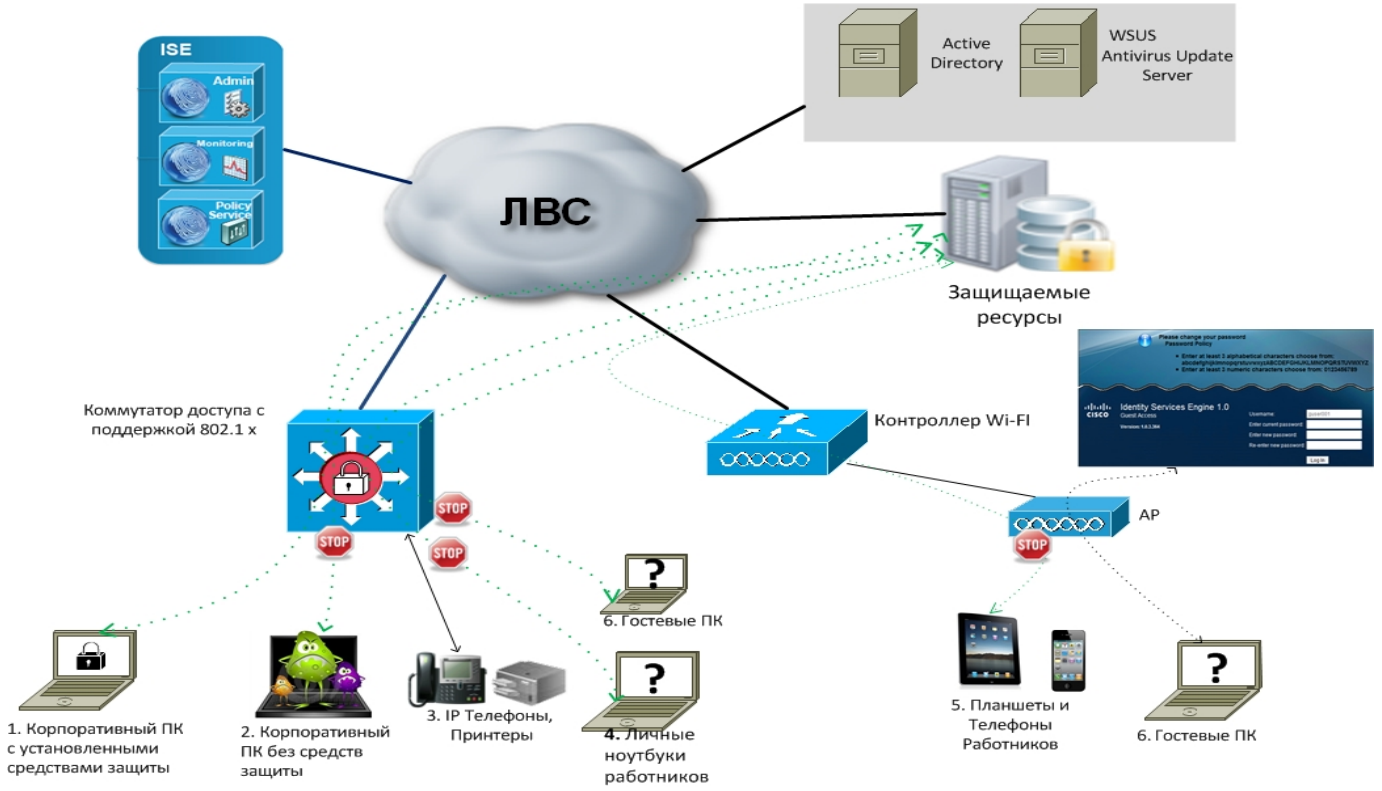
NIST Специальное издание 800-124
Редакция № 1

Рекомендации по менеджменту и обеспечению безопасности мобильных устройств на предприятии

Борьба с внутренними угрозами. Дизай



Механизмы контроля доступа для борьбы с внутренними угрозами



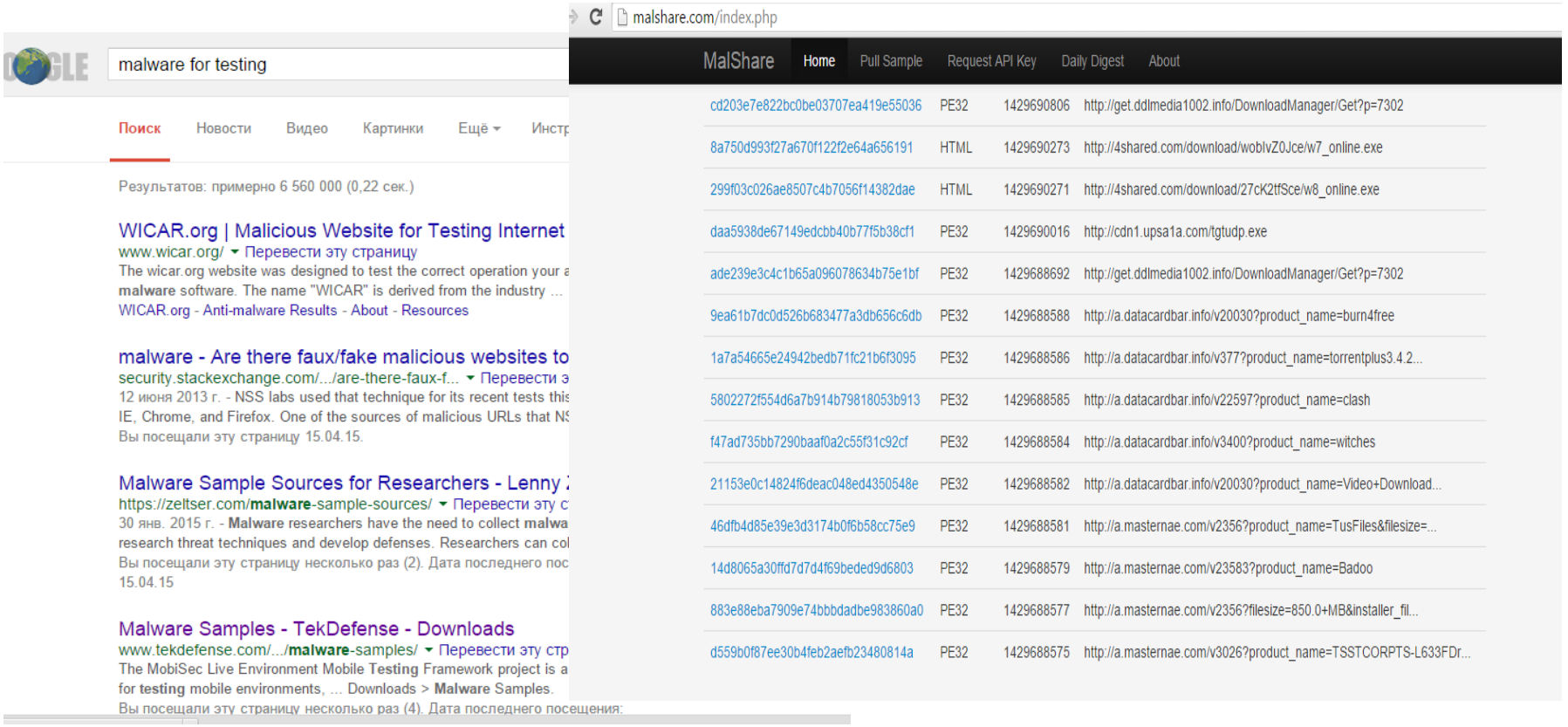
Реализация политик ИБ

Cisco ISE

- Я хочу разрешить доступ к своей сети только авторизованным пользователям → Идентификация и авторизация
- Я хочу разрешить гостевой доступ → Управление жизненным циклом гостевого доступа
- Мне нужно разрешить / запретить iPADы в моей сети (BYOD) → Сервисы профилирования
- Мне нужно, чтобы мои конечные устройства не несли угрозу → Сервисы оценки состояния
- Как я могу установить политики, основанной на личности сотрудника, а не IP-адресах? → Управление доступом на основе групп безопасности
- Мне необходимо защищать конфиденциальные коммуникации → Технология MACSec

Про Advanced Malware

Защищен ли ваш бизнес от Advanced Malware?

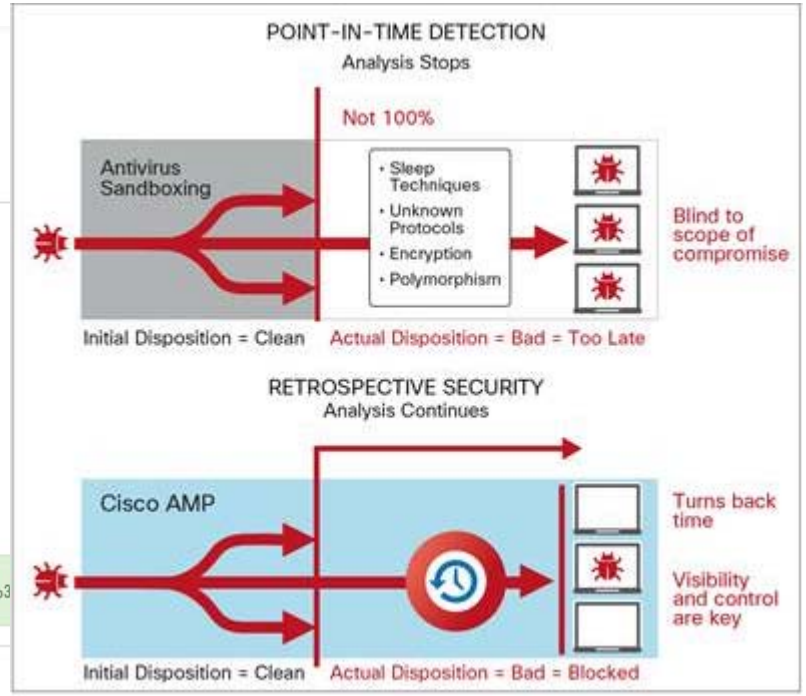


Антивируса достаточно?

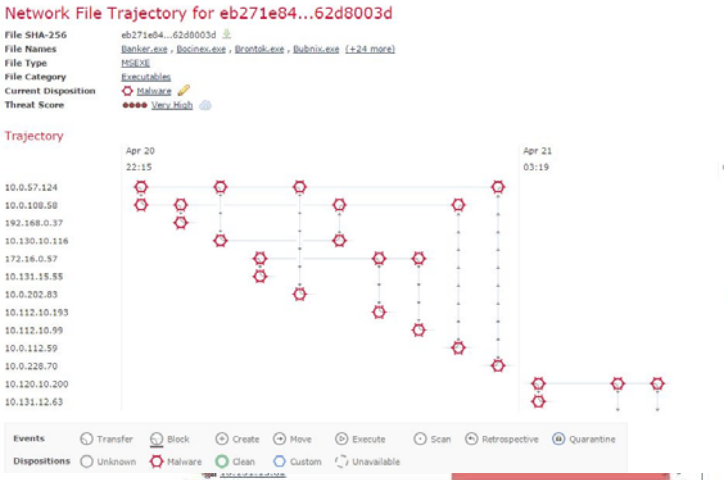
virustotal

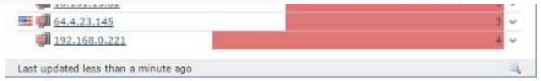
SHA256:	c79ac8a613c7a25793b2a0167d48a6a5e8e7c811ccdaf01d0a47efc7dff99dbd
Имя файла:	0.exe.zip
Показатель выявления:	0 / 56
Дата анализа:	2015-04-20 10:05:15 UTC (1 день, 22 часов назад)

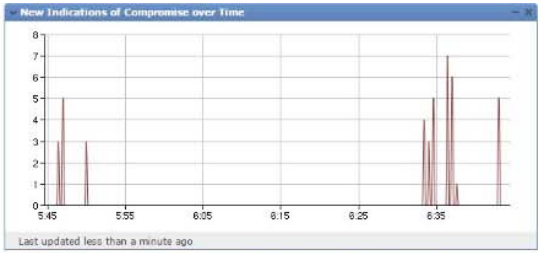
☺ **Похоже, безвреден!** С большой долей уверенности можно предположить, что файл безопасен для использ

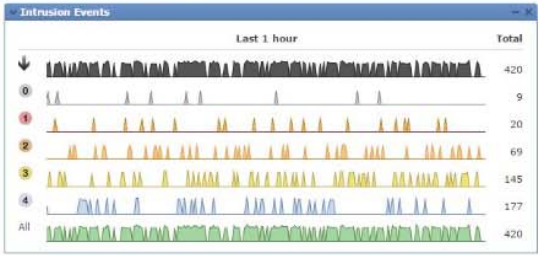


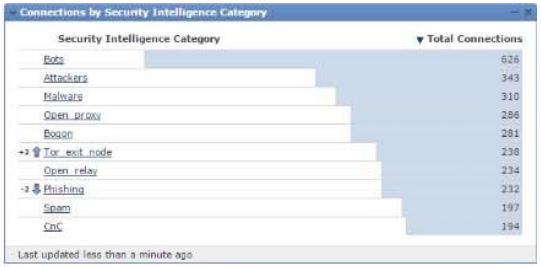
Пример работы AMP

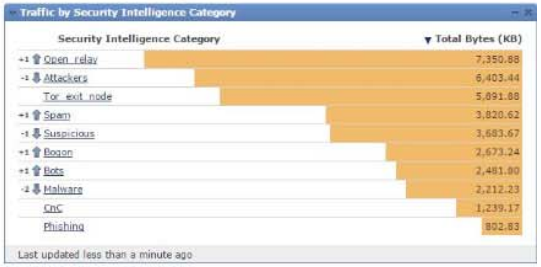












Загрузка файла приостановлена

Файл, который вы пытаетесь скачать, возможно содержит вредоносный код. Файл отправлен на проверку в облачный сервис
файл, нажмите кнопку Continue

Название файла: fut-rtsi.doc

Please click Continue to download/upload the file.

Пример отчета из песочницы AMP

Communications Technology Innovations

1 File Information

File Type	PE
File Signer	
SHA-256	c9ecd256f252dad75d867c358b233d3fc469341e64816f28c23a4
SHA-1	72e3a9f00b16d4f1ddccdf1fb9323d08b8c70732
MD5	45677e3ffca83bb1a692bd3ee5df8fc5
File Size	375808 bytes
First Seen Timestamp	2015-04-16 08:33:40 PST
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2.1.3. Host Activity

Process Name - sample.exe

(command: c:\documents and settings\administrator\sample.exe)

File Activity

File	Action	Size(B)	File Type	Hash
C:\Documents and Settings\All Users\Application Data\{c555e591-3910-7f17-c555-5e5913919644}\sample.exe	Create	375808	exe	md5:45677e bb1a692bd3 fc5 sha1:72e3a d4f1ddccdf1 d08b8c7073 sha256:c9e 52dad75d86 233d3fc469 816f28c23a 10d32
C:\Documents and Settings\All Users\Application	Create	860	unknown	md5:736ed4

Behavior	Severity
Created a file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Used the HTTP POST method The HTTP POST method requests that a system accept the data enclosed in the body of the message. Malware often uses the POST method to exfiltrate large blocks of data over HTTP.	
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	
Installed a Windows service Windows services are background applications that are typically invisible to users. Unlike processes, services can run when no user is logged on. Malware often installs services to establish persistence on the system, or as a precursor to loading malicious device drivers.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Modified the Windows Registry to enable auto-start The Windows Registry Run keys allow an application to specify that it should be launched during system startup. Malware often leverages this mechanism to establish persistence on the system and ensure that it will be run each time the system boots up.	
Modified Internet Explorer security settings Modern browsers provide a variety of security controls that are effective at mitigating or preventing malicious activity. Malware often modifies the settings for these controls to subvert a system's built-in security measures.	
Modified proxy settings for Internet Explorer Rather than communicate directly with a server, a client may route requests through a proxy. If the proxy is malicious, it may modify what a user sees when accessing web pages or even execute a man-in-the-middle (MITM) attack, potentially gaining access to sensitive user information.	

Communications Technology Innovations

Заполните анкету на стенде CTI и получите доступ!

Спасибо!

Communications Technology Innovations