

Максим Лукин Руководитель направления Информационная Безопасность



# Тренды 2015 СТТ Іссhnology Іппочатіоня

#### Рост киберпреступности



#### **BYOx**



#### Pост advacnced malware



#### киберпреступления



Технологии Интернет и связь 22.12.2014 05:00	21.04.2015	В Кабардино-Балкарии осужден хакер, остановивший работу сайта правитель
Брать по-крупному: группировка хакеров	17.04.2015	Хакеров, укравших 160 млн рублей, задержали в Москве
банков	17.04.2015	WikiLeaks опубликовал похищенные документы компании Sony
Павел Седаков, Дмитрий Филонов	10.04.2015	Компьютерный вирус украл \$24 млн по всему миру
Хакеры из группы Anunak атакуют крупные банки, а не их клиент рублей. Почему такие преступления считаются особо опасными	09.04.2015	Захарченко: Киеву «нужна война, пусть даже информационная»

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



### Для взлома не нужно быть хакером







### Любое ПО и услуги продаются на теневом рынке



	E	☑ [Взлом почты на заказ] Mail.Ru, Yandex.Ru, Rambler.I 🔙 Smoyk	E	DroidJack - Android RAT с хорошим функционалом. Marlb0r0	
	E	xakep.click   Взлом Email аккаунтов и Аккаунтов Соц.се Mr.Robot	E	RMS Builder 6.3.0.5 Box (скрытая установка, новые функции) Ltybcrf	
	E	Взлом email на заказ mail.xacking	E	MKL PRO Keylogger ( 12)	
M	E	Взлом почты на заказ, без предоплаты mailpass	•	[Софт] Удаленное управление компьютером (№ 12) Zelont	
	4	Взлом почты ДЕШЕВО на заказ. hack-inbox			
_		nack-indox	E	Сдам андроид софт в аренду	
		Взлом почты на заказ Corp.Rese		rm	
F			(inc.	NEW РМС сборка в формате XLS	
	Взлом почты Mail, Yandex и Gmail от DizzyCap.			ridmall	
M	A	Работа! Нужны специалисты по взлому почты. Качественн Openmail	E	Стиллер Twilight Stealer 4 Marlb0r0	
	E	Взламаю WhatsApp, Skype, Vkontakte, Viber и многое друго ryjov.slavik	E	Kraken ботнет m1st	
		взлом электронной почты+корпоративки devergent	E	Продам исходники бота turbo	
	E	Взлом почты [Mail.ru Yandex.ru Rambler.ru Gmail.com] —— burglary.mail	-	Халявный Keylogger	
	E	Взлом почты на заказ [mail, yandex, gmail, rambler] PupkinV	E	Marlb0r0	
	E	взлом практически любой почты, индивидуальный подхо, BigStan	E	Z*Stealer новый стилер логинов и паролей DamRaiX	
<u></u>	0	РОСКОМЗАЗОР-ПОМОЩЬ УЖЕ В ПУТИ	E	S&M service (loads/installs-от 60\$, крипт/crypt-от 15\$) chipddos	



# Dark Market Silk Road 3.0







# Трояны и другое интересное ПО



Escrow A 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



#### Android App Profits



How I banked in \$14,580 in 14 Days



Price: \$.99 USD / 0.003674 BTC

Price: \$.99 USD / 0.003674 BTC

Ultra Hacker Tools with 83 RATs and 21 Binders



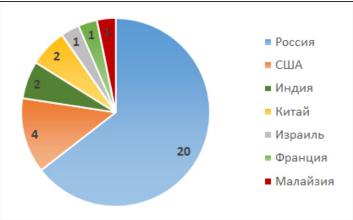
Price: \$50 USD / 0.185597 BTC

Price: \$50 USD / 0.185597 BTC

# Как украсть у банка деньги?





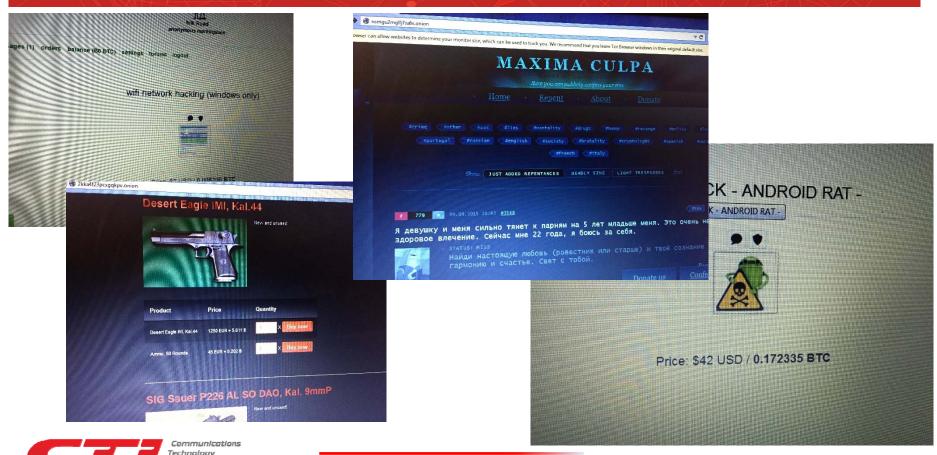






# Еще немного про TOR

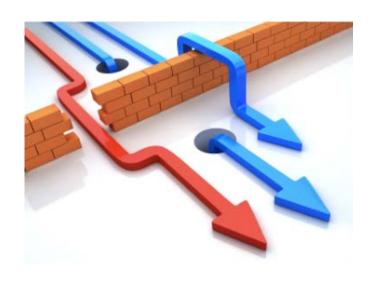




### С чего начать борьбу с угрозами?



#### Проведение комплексного аудита ИБ

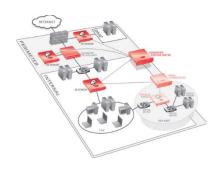


- Анализ документации
- Экспертный аудит ИБ в том числе может включать аудит на соответствие Best Practice
- Анализ защищенности WEB приложений
- Анализ защищенности сети
- Тестирование на проникновение



#### 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



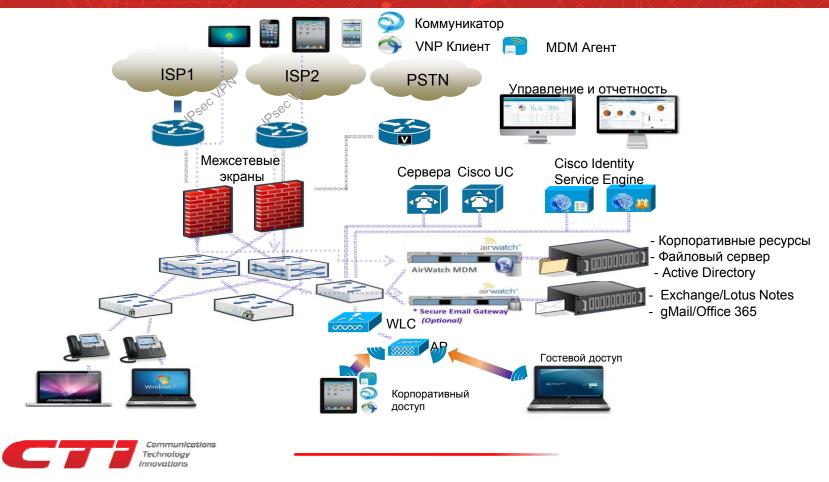
NIST Специальное издание 800-124 Редакция № 1

Рекомендации по менеджменту и обеспечению безопасности мобильных устройств на предприятии

2.	Обзо	ор мобильных устройств	2
	2.1. 2.2.	Определение характеристик мобильного устройства	
3.	Техн	нологии менеджмента мобильных устройств	
	3.2.	Начало	8 11
		4.4.4. O	12
	4.2.	4.1.1. Ограничения по типам мобильных устройств и уровням доступа 4.1.2. Дополнительные требования к пользователям	13
	4.3. 4.4.	4.1.2. Дополнительные требования к пользователям	13 14 15

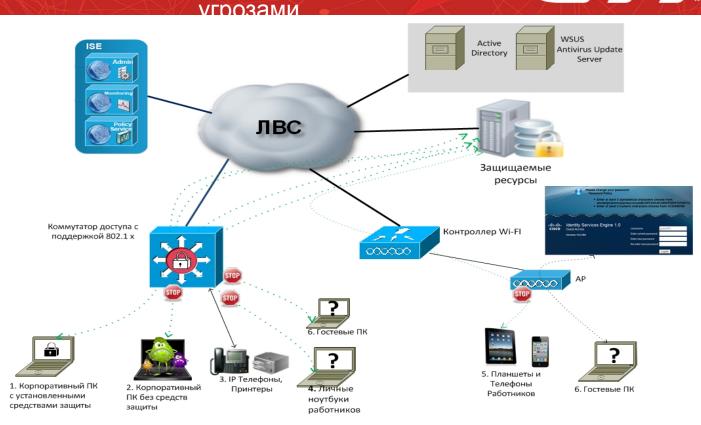


## Борьба с внутренними угрозами. Дизай — Торьба с внутренними угрозами. Дизай с внутренними угрозами. Дизай — Торьба с внутренними угрозами. Дизай с внутренними угрозами и внутренними и внутренн



# Механизмы контроля доступа для борьбы с внутренними

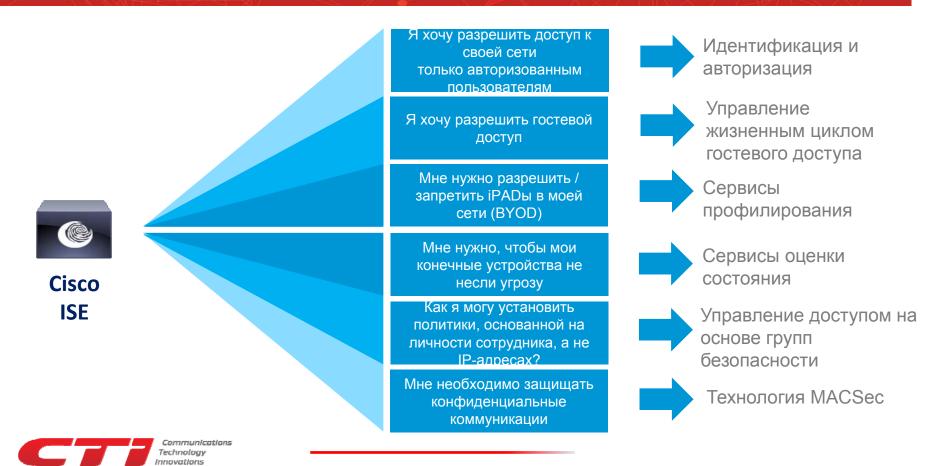






### Реализация политик ИБ





## Про Advanced Malware







# Защищен ли ваш бизнес от Advanced Malware?



→ G	malshare.com/index.ph

		7 C   mashale.com/index.php				
COGLE	malware for testing		MalShare Home Pull Sample	Request	API Key Daily Digest About	
			cd203e7e822bc0be03707ea419e55036	PE32	1429690806 http://get.ddlmedia1002.info/DownloadManager/Get?p=7302	
	Поиск Новости Видео Картинки Ещё <del>v</del> Инстр		8a750d993f27a670f122f2e64a656191	HTML	1429690273 http://4shared.com/download/woblvZ0Jce/w7_online.exe	
	Результатов: примерно 6 560 000 (0,22 сек.)  WICAR.org   Malicious Website for Testing Internet www.wicar.org/ ▼ Перевести эту страницу The wicar.org website was designed to test the correct operation your a malware software. The name "WICAR" is derived from the industry WICAR.org - Anti-malware Results - About - Resources		299f03c026ae8507c4b7056f14382dae	HTML	1429690271 http://4shared.com/download/27cK2tfSce/w8_online.exe	
			daa5938de67149edcbb40b77f5b38cf1	PE32	1429690016 http://cdn1.upsa1a.com/tgtudp.exe	
			ade239e3c4c1b65a096078634b75e1bf	PE32	1429688692 http://get.ddlmedia1002.info/DownloadManager/Get?p=7302	
			9ea61b7dc0d526b683477a3db656c6db	PE32	1429688588 http://a.datacardbar.info/v20030?product_name=burn4free	
	malware - Are there faux/fake malicious websites to security.stackexchange.com//are-there-faux-f ▼ Перевести э 12 июня 2013 г NSS labs used that technique for its recent tests this IE, Chrome, and Firefox. One of the sources of malicious URLs that NS Вы посещали эту страницу 15.04.15.		1a7a54665e24942bedb71fc21b6f3095	PE32	1429688586 http://a.datacardbar.info/v377?product_name=torrentplus3.4.2	
		s	5802272f554d6a7b914b79818053b913	PE32	1429688585 http://a.datacardbar.info/v22597?product_name=clash	
			f47ad735bb7290baaf0a2c55f31c92cf	PE32	1429688584 http://a.datacardbar.info/v3400?product_name=witches	
	Malware Sample Sources for Researchers - Lenny и https://zeltser.com/malware-sample-sources/ ▼ Перевести эту с 30 янв. 2015 г Malware researchers have the need to collect malwa research threat techniques and develop defenses. Researchers can col Вы посещали эту страницу несколько раз (2). Дата последнего пос 15.04.15		21153e0c14824f6deac048ed4350548e	PE32	1429688582 http://a.datacardbar.info/v20030?product_name=Video+Download	
		1	46dfb4d85e39e3d3174b0f6b58cc75e9	PE32	1429688581 http://a.masternae.com/v2356?product_name=TusFiles&filesize=	
			14d8065a30ffd7d7d4f69beded9d6803	PE32	1429688579 http://a.masternae.com/v23583?product_name=Badoo	
	Malware Samples - TekDefense - Downloads		883e88eba7909e74bbbdadbe983860a0	PE32	1429688577 http://a.masternae.com/v2356?filesize=850.0+MB&installer_fil	
	www.tekdefense.com//malware-samples/ ▼ Перевести эту стр The MobiSec Live Environment Mobile Testing Framework project is a		d559b0f87ee30b4feb2aefb23480814a	PE32	1429688575 http://a.masternae.com/v3026?product_name=TSSTCORPTS-L633FDr	



for testing mobile environments, ... Downloads > Malware Samples. Вы посещали эту страницу несколько раз (4). Дата последнего посещения:

#### Антивируса достаточно?





SHA256: c79ac8a613c7a25793b2a0167d48a6a5e8e7c811ccdaf01d0a47efc7dff99dbd

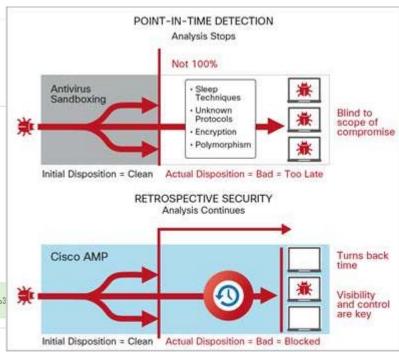
Имя файла: 0.exe.zip

Показатель

0 / 56

Дата анализа: 2015-04-20 10:05:15 UTC (1 день, 22 часов назад)

© Похоже, безвреден! C большой долей уверенности можно предположить, что файл безопасен для использ





#### Пример работы АМР



#### Network File Trajectory for eb271e84...62d8003d File SHA-256 eb271e84...62d8003d 🖳 Banker.exe , Bocinex.exe , Brontok.exe , Bubnix.exe (+24 more) File Type MSEXE File Category Executables Malware 0 Threat Score oooo Very High @ Trajectory Apr 20 22:15 03:19 10.0.108.58 192.168.0.37 10.130.10.116 172.16.0.57 10.131.15.55 10.0.202.83 10.112.10.193 10.112.10.99 10.0.112.59 10.0.228.70 10.120.10.200 10.131.12.63 Dispositions O Unknown O Malware O Clean O Custom (7 Unavailable 64,4.23,145 192.168.0.221 Last updated less than a minute ago +1 \* W32,CD13C635C6-71,58 +1 @ W32,Trojan,Breach,VRT -1 \$ W32.Lamechi +I @ Lamechi:MalOb-tpd +1 Trojano: VBTroj-tpd O W32.EB271E846F-100.SBX.VIOC +1 Troxa:Kunkka-tod +1 & Bamital: Trojan-tpd +1 \* FakeAlert: XPACK-tod +1 ft Bamital: NEID-tpd Last updated less than a minute ago

#### Загрузка файла приостановлена

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

+1 P Bogon

-2 & Malware

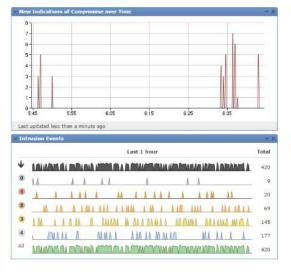
ChC

Last updated less than a minute ago

+1 1 Bots

Название файла: fut-rtsi.doc

Please click Continue to download/upload the file.



Connections by Security Intelligence Category	
Security Intelligence Category	▼ Total Connections
Bots	626
Attackers	343
Malware .	310
Open_proxy	286
Bogon	281
+2 Tor exit node	238
Open relay	234
-2 - Phishing	232
Spam	197
<u>CnC</u>	194
Last updated less than a minute ago	
Traffic by Security Intelligence Category	
Security Intelligence Category	▼ Total Bytes (KB)
+1 🕏 Open relay	7,350.88
-1 & Attackers	6,403,44
Tor exit node	5,091.00
+1 P Spam	3,820,62

3,683.67 2.673.24

2,481.00

1,239.17

802.83



## Пример отчета из песочницы АМР



#### 1 File Information

File Type	PE
File Signer	
SHA-256	c9ecd256f252dad75d867c358b233d3fc469341e64816f28c23a4c
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	1
C:\Documents and Settings\All Users\Application	Create	375808	exe	md5:45677€	ľ
Data\{c555e591-3910-7f17-c555-5e5913919844}\sample.exe				bb1a692bd3	H
				fc5	
				sha1:72e3a	П
				d4f1ddccdf1	ŀ
				d08b8c7073	h
				sha256:c9e	
				52dad75d86	H
				233d3fc469	١.
				816f28c23a	ш
				10d32	ľ
					ŀ
C:\Documents and Settings\All Users\Application	Create	860	unknown	md5:736ed4	

	Behavior	Severity
a40	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.	100000000
	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.	10000111111
_	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.	000000000
	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.	•••••
677e	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.	•
e3a cdf1 7073 c9e 5d86	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.	000000000
469: 23a 6ed4	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.	000000000
	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.	••••







Заполните анкету на стенде СТІ и получите доступ!

Спасибо!



