



ГАРДА
ТЕХНОЛОГИИ

КАК СОТРУДНИКИ СТАЛИ САМЫМИ ОПАСНЫМИ ХАКЕРАМИ ДЛЯ КОМПАНИИ

А ВЫ ЗЕМЕТИЛИ?

” Роман Жуков

ДИРЕКТОР
ЦЕНТРА КОМПЕТЕНЦИЙ

О СПИКЕРЕ

ГАРДА
ТЕХНОЛОГИИ

Роман Жуков

Директор центра компетенций



9+ ЛЕТ В СФЕРЕ ИБ



ЗАКАЗЧИК ⇒ ИНТЕГРАТОР
⇒ ОПЕРАТОР ⇒ ВЕНДОР



УЧАСТНИК ЭКСПЕРТНЫХ ГРУПП
(ФСТЭК, ЦБ, МКС)



ROZHUKOV.BLOGSPOT.COM

О РАЗРАБОТЧИКЕ

ГАРДА
ТЕХНОЛОГИИ



ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания обладает многолетним опытом в сфере информационных технологий и разрабатывает решения для различных задач безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Решения Гарды Технологии внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.



100 +

Внедрений
на территории
России и стран СНГ



150 +

Высококвалифицированных
сотрудников



10 лет

Опыт разработки
систем высокой
сложности



5

Запатентованных
технологий собственного
исследовательского центра



ПОЛНОСТЬЮ РОССИЙСКИЕ РЕШЕНИЯ

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий
- Решения сертифицированы ФСТЭК
- Включены в реестр отечественного программного обеспечения

АНОНИМНЫЙ ОПРОС

СОБЛЮДАЙТЕ РЕГИСТР

bit.ly/
2qfb9Uw

SCAN ME





С ЧЕГО ЧАСТО НАЧИНАЮТСЯ ПРЕЗЕНТАЦИИ ПО ИБ

**МЫ ВСЕ УМРЕМ ОТ СТРАШНЫХ
ВИРУСОВ И ХАКЕРОВ...**

**...ПОГОДИТЕ, ЕСТЬ ЖЕ КЛАССНАЯ
ИГРУШКА**

DISCLAIMER

ГАРДА
ТЕХНОЛОГИИ



НЕТ СКРЫТОЙ РЕКЛАМЫ,
ВСЕ СОВПАДЕНИЯ СЛУЧАЙНЫ



МАКСИМУМ СОЗИДАНИЯ, ПРИМЕРОВ И
ПРАКТИКИ



КАРТИНКИ ПРИВЕДЕНЫ
ИСКЛЮЧИТЕЛЬНО
В ЦЕЛЯХ ДЕМОНСТРАЦИИ



ГАРДА
ТЕХНОЛОГИИ

НА ЧЕМ ГЛАВНЫЙ ФОКУС ИБ В КОМПАНИЯХ

ЧТО МЫ ЗАЩИЩАЕМ

ГАРДА
ТЕХНОЛОГИИ



ПК VIP-ПЕРСОН



БИЗНЕС-СИСТЕМЫ



WEB-ПРИЛОЖЕНИЯ



ПОЛЬЗОВАТЕЛИ



АДМИНИСТРАТОРЫ

ОТ ЧЕГО МЫ, КАК ПРАВИЛО, ЗАЩИЩАЕМЩАЕМ



ПК VIP-ПЕРСОН



БИЗНЕС-СИСТЕМЫ



WEB-ПРИЛОЖЕНИЯ



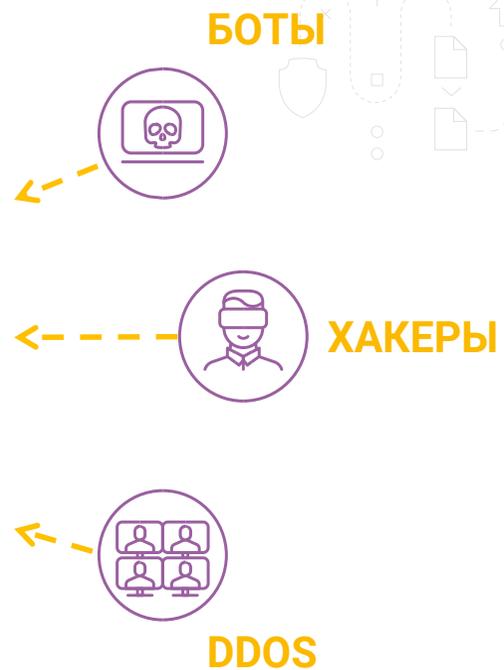
ПОЛЬЗОВАТЕЛИ

СПАМ
ВИРУСЫ



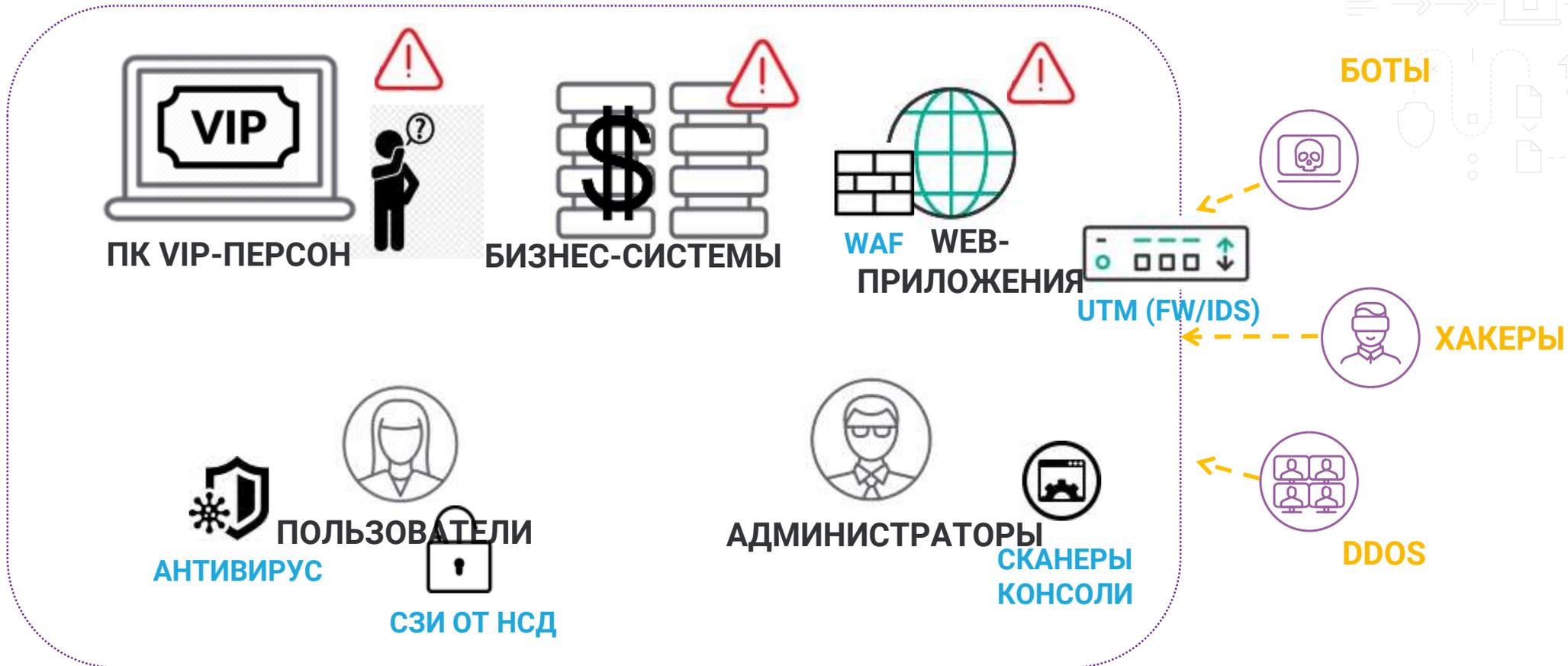
АДМИНИСТРАТОРЫ

АРТ-АТАКИ



КАК МЫ ЗАЩИЩАЕМ

ГАРДА
ТЕХНОЛОГИИ



ДОРОГИЕ И МОДНЫЕ «ИГРУШКИ»

ГАРДА
ТЕХНОЛОГИИ

1

SIEM, IRP

2

AntiAPT, EDR

3

Deception

4

DAM/DFM

5

SOAR, BAS, CASB ...



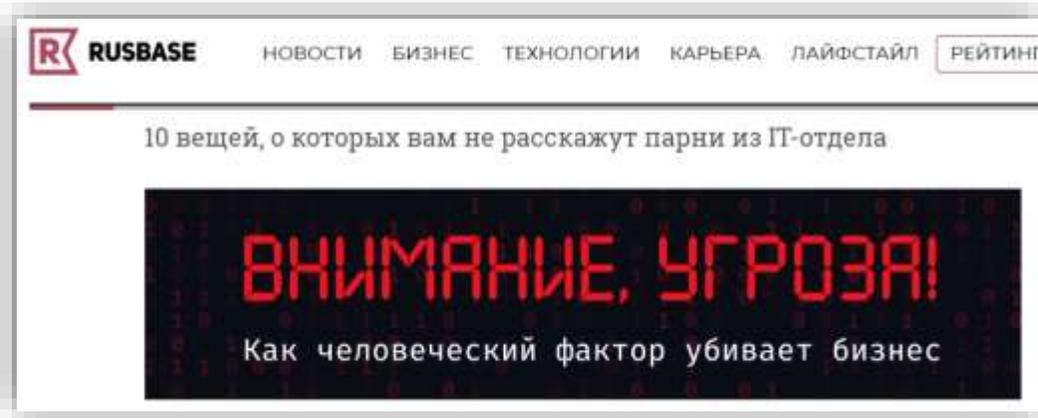
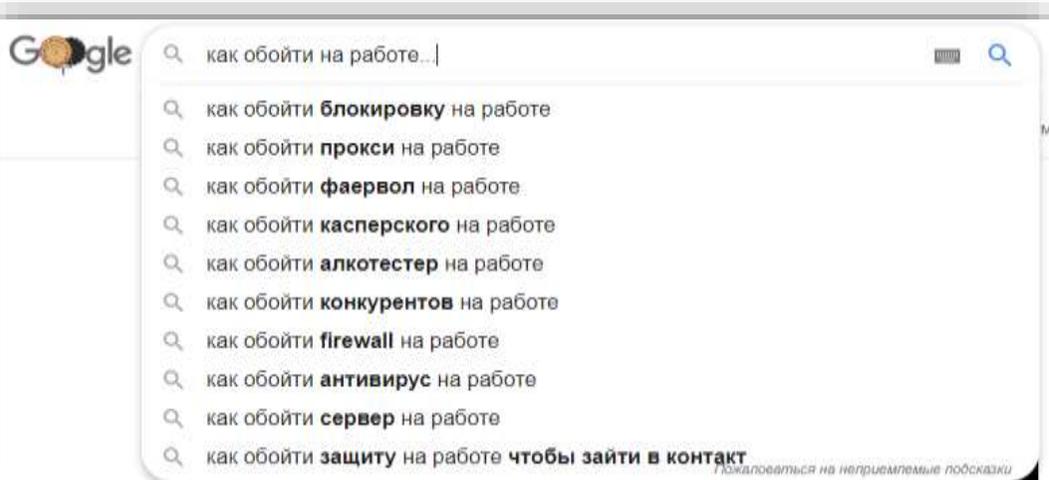


ГАРДА
ТЕХНОЛОГИИ

А ТЕМ ВРЕМЕНЕМ...

ТОП ЗАПРОСОВ СОТРУДНИКОВ В ПОИСКОВИКАХ

ГАРДА
ТЕХНОЛОГИИ



- ✓ Как отправлять большие файлы по почте
- ✓ Как использовать ПО, которое компания запрещает
- ✓ Как заходить на сайты, заблокированные компанией
- ✓ Как замести следы на корпоративном ноутбуке
- ✓ Как найти рабочие документы из дома
- ✓ Как хранить рабочие файлы в онлайн
- ✓ Как сохранить тайну личной переписки
- ✓ Как получить удаленный доступ к рабочей почте с телефона
- ✓ Как сделать вид, что вы работаете

ДЕЛУ – ВРЕМЯ, ПОТЕХЕ – ЧАС

ГАРДА
ТЕХНОЛОГИИ

No.	И протокол	UDP	DNS	PLAYSTATION
	Списки	Нет данных		
0	Политики	Игровой трафик		
1	HTTP хост	Нет данных		
2	Размер (Б)	83.14	DMZ	
3	Продолжительность сессии	< 1с		
	IP отправителя	188.1		
4	Порт отправителя	43484		
	MAC клиента	00:0F:24:57:9D:1B		
5	Аккаунт отправителя	Нет данных		
	Компьютер клиента	Нет данных		
	Страна клиента			
	IP получателя	83.14		

Протокол	Содержание
DNS	Standard query 0x73ea A trophy01.np.community.playstation.net
DNS	Standard query 0x73ea A trophy01.np.community.playstation.net
DNS	Standard query 0x73ea A trophy01.np.community.playstation.net
86 DNS	Standard query response 0x73ea CNAME trophy01.np.community.pl g.akamaiedge.net A 88.221.73.194
86 DNS	Standard query response 0x73ea CNAME trophy01.np.community.pl g.akamaiedge.net A 88.221.73.194
86 DNS	Standard query response 0x73ea CNAME trophy01.np.community.pl g.akamaiedge.net A 88.221.73.194



СКАЧИВАНИЕ ФАЙЛОВ – ПОД ЗАПРЕТОМ? НЕ БЕДА

ГАРДА
ТЕХНОЛОГИИ

Группа протоколов

Другие

Протокол

TCP ▶ HTTP

Списки

Нет данных

Политики

Нет данных

HTTP хост

Нет данных

Размер (Б)

1402

Продолжительность сессии

1м 0с

IP отправителя

● 1.123.90

Порт отправителя

57435

Аккаунт отправителя

okozlovs@ ru

Компьютер клиента

wsus01. DN.R

Top Downloads
Лучшие файлы

Категории

- Все
 - Каталог файлов
- Программы
- Игры
 - Каталог игр
- Архивы
- Музыка
 - Каталог музыки
- Видео
- Документы
- Разное

Рейтинг авторов »

Все время Год/Месяц **7 дней** Вчера Сегодня

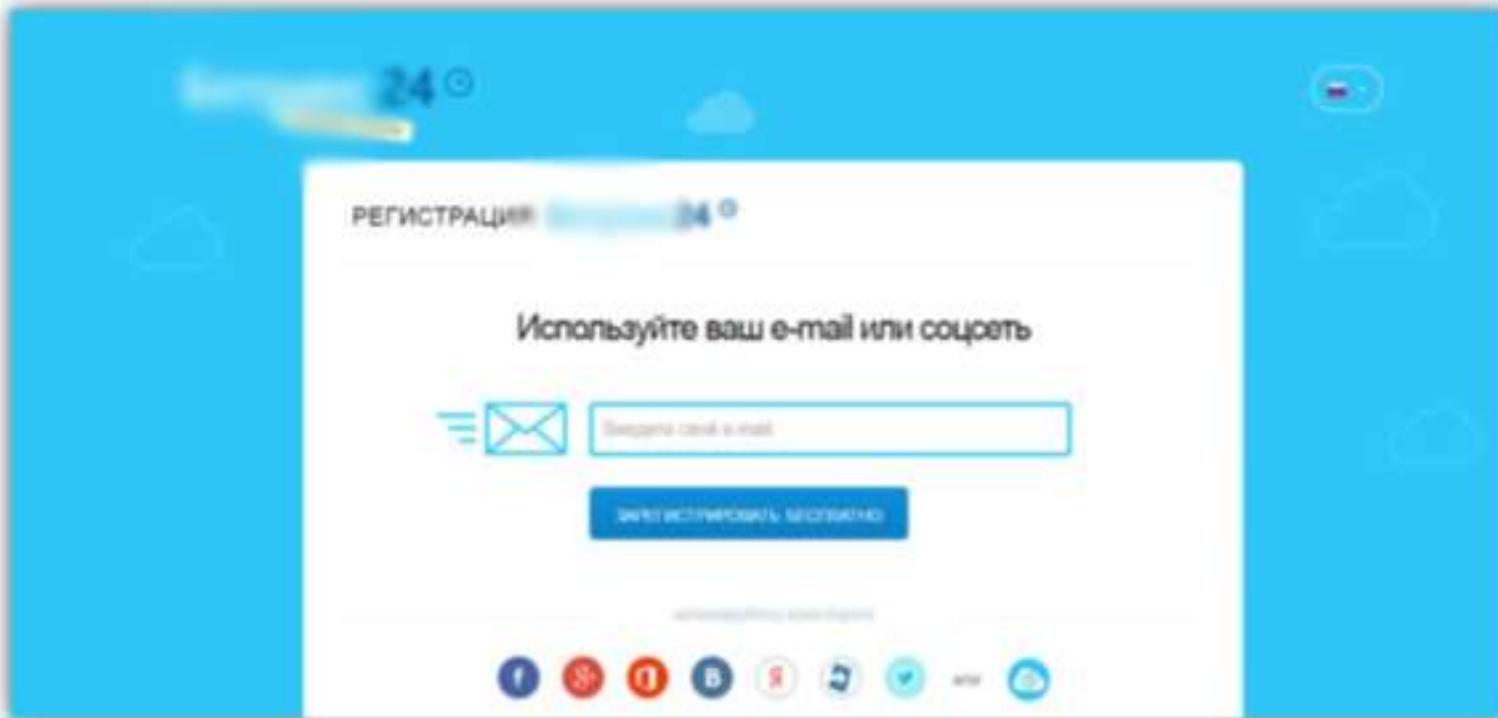
Популярные файлы
за 7 дней 07/10/2019 - 13/10/2019

Место	Файл / Программа
1	Download Master 6.19.4.1649 7.43 МБ Комментарии: 875 » Добавить комментарий + Зеркал: 5
2	Convertilla 17.10 МБ Комментарии: 4 » Добавить комментарий + Зеркал: 1
3	Adobe Flash Player 15 1.01 МБ Комментарии: 6 » Добавить комментарий +
4	Dr.Web CureIt! 192.52 МБ Обновился! Комментарии: 6 » Добавить комментарий + Зеркал: 1
5	DriverPack-17-Online.exe 6.00 МБ Добавить комментарий + Зеркал: 1



АВТОРИЗАЦИОННЫЕ ДАННЫЕ – В ОТКРЫТОМ ВИДЕ

ГАРДА
ТЕХНОЛОГИИ



5	0.000000	60	75.117	1.2	TCP	[TCP Dup ACK 5#1] 23545 > http [ACK] Seq=1 Ack=1 Win=8190 Len=0
6	0.000000	1132	75.117	174.2	HTTP	POST /sso/oauth2/tokeninfo?access_token=82d8a60d-6874-4d9b-82d4-43c507923820
7	0.000000	1132	75.117			POST /sso/oauth2/tokeninfo?access_token=82d8a60d-6874-4d9b-82d4-43c507923820
8	0.000000	60	71.2	5.117	TCP	http > 23545 [ACK] Seq=1 Ack=1079 Win=16170 Len=0

МАЛО ПРАВ – НЕ ПОВОД УНЫВАТЬ

ГАРДА
ТЕХНОЛОГИИ

Дата и время	IP источника	IP цели	Название угрозы	Тип угрозы	Уровень...
14.10.2019 12:13:28	5.23 [DM]	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:28	23 [DM]	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:27	5.23 [DM]	0.230	GPL SQL service_name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:27	25.23 [DM]	0.230	GPL SQL service_name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:26	5.23 [DM]	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:26	8.23 [DM]	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий



Время	Имя БД	Экземпляр БД	Логин/Логин ...	IP клиента	Логин ОС	Приложение	Операции
14 октября 2019 12:07:52	is_stb	service_g	ps_aniv	53.17...	aniv	plsqldev.exe	Grant
14 октября 2019 12:00:41	is_stb	service_g	ps_aniv	53.17...	aniv	plsqldev.exe	Grant
14 октября 2019 12:00:37	is_stb	service_g	ps_aniv	53.17...	aniv	plsqldev.exe	PL/SQL
14 октября 2019 07:49:14	is_stb	service_g	ps_aniv	63.17...	aniv	plsqldev.exe	Grant
14 октября 2019 07:49:02	is_stb	service_g	ps_aniv	3.17...	aniv	plsqldev.exe	Grant
14 октября 2019 07:37:30	is_stb	service_g	ps_aniv	63.17...	aniv	plsqldev.exe	Grant

СЛУЖЕБНАЯ УЧЕТКА – ВСЕГДА ЛУЧШЕ

ГАРДА
ТЕХНОЛОГИИ

Логин\Логин БД	IP клиента	Логин ОС	MSISDN	STATUS	JUR_TYPE	Рыноч. сегмент	Внутр. сегмент	SUBS_SUBS_ID	PACK_PACK_ID	NAME_R
EMERGENCY	10.163.17...	maria.shiroi	921876	Действующий	Физическое лицо	B2B LA	B2B TOP+	124986909	8587	Безлимитный корпоративный приоритет ФК
EMERGENCY	10.163.17...	maria.shir	92187	Действующий	Физическое лицо	B2B LA	B2B TOP+	124986909	1607	Безлимитный федеральный корпоративный приоритет ФК
EMERGENCY	10.163.17...	maria.shi	92187	Действующий	Физическое лицо	B2B LA	B2B TOP+	124986909	8607	Безлимитный федеральный МегаФон-при ФКК
EMERGENCY	10.163.17...	maria.shir	921876	Действующий	Физическое лицо	B2B LA	B2B TOP+	124986909	9009	TEMP_Федеральный Интернет-при ФКК
EMERGENCY	10.163.17...	maria.shir	93126	Временно закрыт	Юридическое лицо	B2B SME	B2B SME	121050256	8587	Безлимитный корпоративный приоритет ФК
EMERGENCY	10.163.17...	maria.shi	9312	Временно	Юридическое	B2B	B2B	121050256	1607	Безлимитный



PASSPORT

ПРОТОКОЛ НА НЕСТАНДАРТНОМ ПОРТУ

Трафик

Новый фильтр - Поиск по всем регионам Расширенный

protocol=HTTP x non_standard_port x 09.09.2016 00:00:00 - 15.09.2016 23:59:59

Отображено 1-50 из 1170 результатов.

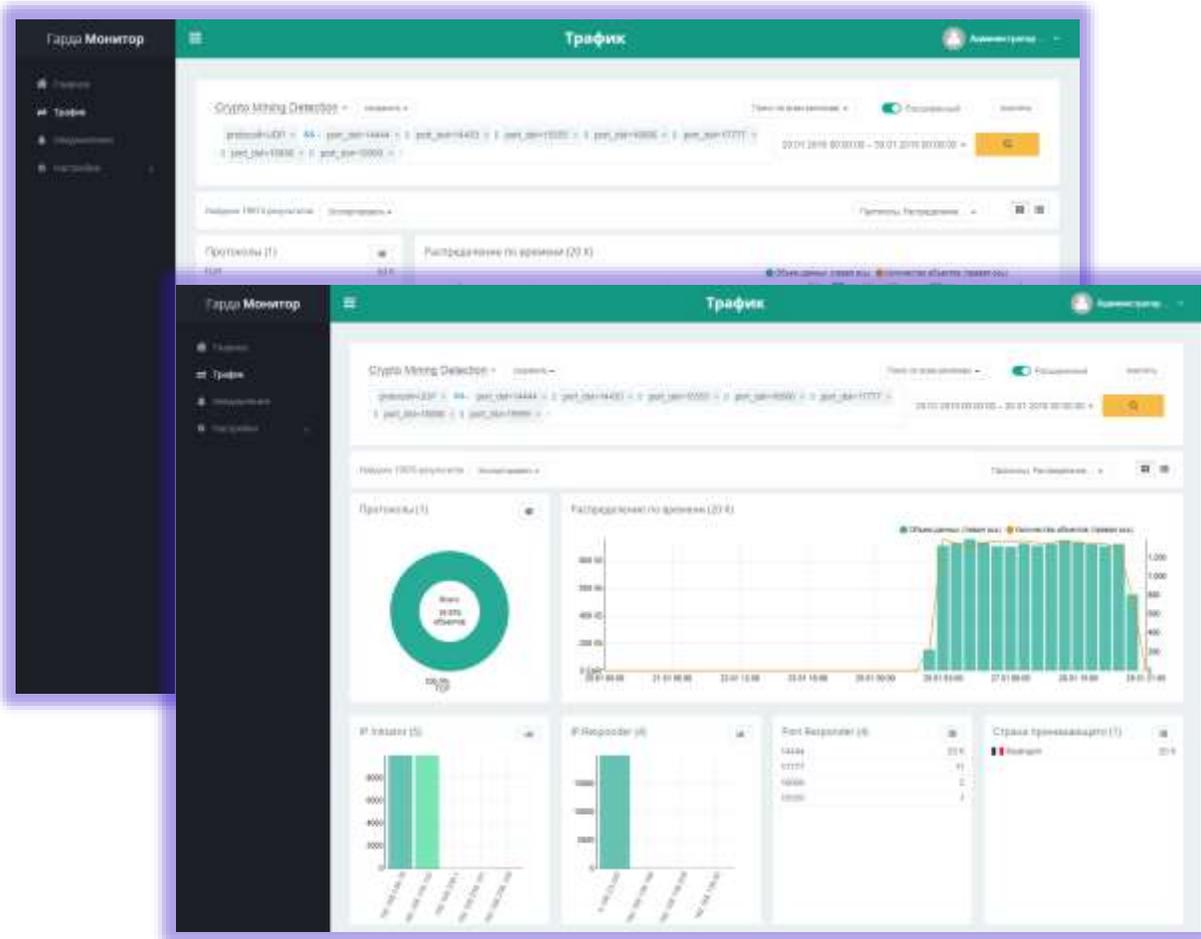
Тип	Узел	Протокол	IP клиента	Порт	IP сервера	Порт	Размер	Время
🟢	NN	HTTP	192.168.21.116	49706	192.168.21.107	8200	1.4 КБ	15.09.2016 11:35:18
🟢	NN	HTTP	192.168.21.116	49706	192.168.21.107	8200	5 КБ	15.09.2016 11:35:18
🟢	NN	HTTP	192.168.21.116	49706	192.168.21.107	8200	1.4 КБ	15.09.2016 11:35:18

```
[localhost-192.168.21.123 /]# curl 192.168.21.107:8200
{"name": "George Tarleton",
 "version": {
  "build_hash": "218bdf10790eef486ff2c41a3df5cfa32dadcfde",
  "build_timestamp": "2016-05-17T15:40:04Z",
  "build_snapshot": false,
  "version": "0.0.0"
},
 "url": "The Way, The Shell"
}
```

- Обнаружили использование протокола HTTP на нестандартном порту
- Выяснилось, что на сервере компании сотрудник для удобства доступа установил open source продукт
- Default-настройки: открытые порты
- Кто-то уже стучался

МАЙНИНГ НА РАБОЧЕМ МЕСТЕ

ГАРДА
ТЕХНОЛОГИИ



- IP-адрес из «подозрительного» пула
- Обнаружили постоянный трафик на компьютере
- Ретроспектива – не первый случай

МОЖНО ДАЛЕКО ЗАЙТИ...

ГАРДА
ТЕХНОЛОГИИ

12 августа 2019, 16:09

12 августа 2019, 14:42
Отключение СМС-оповещений

12 августа 2019, 14:42
Заказ детализации

12 августа 2019, 14:43
Включение СМС-оповещений

Приложение	LK
Уровень доступа	3
Канал аутентификации	PASSWORD
MSISDN аккаунта	+793
Тип аккаунта	MASTER
Филиал	I
Регион	TV
IP	1.125
UserAgent	MOZILLA/5.0 WINDOWS NT 5.0 R (52.0) GECKO/20100101 FIREFOX/52.0
MSISDN события	+793
Uid	DF2C8D63-38C9-2F82-7DEF-B43

12 августа 2019, 16:09

12 августа 2019, 14:42
Отключение СМС-оповещений

12 августа 2019, 14:42
Заказ детализации

12 августа 2019, 14:43
Включение СМС-оповещений

Формат	COLLECTOR_USERS
Приложение	MLK
Уровень доступа	3
Канал аутентификации	PIN
MSISDN аккаунта	+793
Тип аккаунта	MASTER
Филиал	I
Регион	TV
IP	1.125
UserAgent	MLK ANDROID PHONE 3.3.0
MSISDN события	+793
Uid	DF2C8D63-38C9-2F82-7DEF-B43



ГАРДА
ТЕХНОЛОГИИ

ПОЧЕМУ ТАК ПРОИСХОДИТ

ТОП ПРИЧИН

ГАРДА
ТЕХНОЛОГИИ



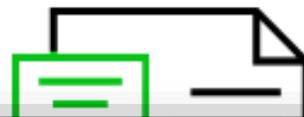
- 1 Внимание на атаки, а не на инциденты
- 2 Оповещение – уже по факту атаки
- 3 Формальные модели угроз
- 4 Модель нарушителя (даже спецслужбы)
- 5 Мотивация – только внешняя

МОДЕЛЬ УГРОЗ – В 1 КЛИК

ГАРДА
ТЕХНОЛОГИИ

Не нужны специальные знания

Чтобы получить готовый документ вам необходимо только заполнить анкету. Вопросы в анкете просты, поэтому заполнять их может человек, не имеющий специальных знаний в области информационной безопасности. После ввода информации в анкете



Модель угроз безопасности ИСПДн

Сохранить, скачать или распечатать этот документ вы сможете сразу после оплаты

Оплатить 250 рублей

100%
ГАРАНТИЯ

Вернем деньги, если документ не подошел

ВЫСОКИЙ УРОВЕНЬ ДОВЕРИЯ К «СВОИМ»

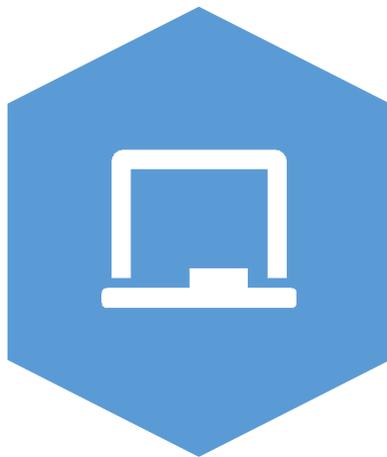
ГАРДА
ТЕХНОЛОГИИ

Модель угроз и нарушителя:

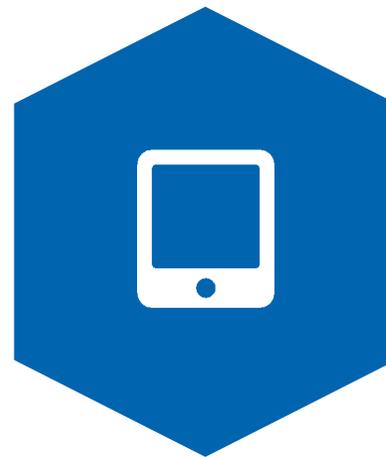
«Наша кадровая политика по подбору персонала – самая лучшая» (с)



НЕТ ОСНОВАНИЙ
НЕ ДОВЕРЯТЬ



ПРОНИКНОВЕНИЕ ИТ
ТЕХНОЛОГИЙ



УДОБСТВО VIP
ПОЛЬЗОВАТЕЛЕЙ

ПСИХОЛОГИЯ, ОТНОШЕНИЯ, ЗАКОН

ГАРДА
ТЕХНОЛОГИИ

ДОВЕРИЕ
«BY DESIGN»



ПОСТОЯННЫЙ
КОНТРОЛЬ =
ДИСКОМФОРТ



УВАЖЕНИЕ
PRIVACY



ЗАКОНЫ
ГОСУДАРСТВА



СЛУЖБА ИБ – ВРАГ НАРОДА

ГАРДА
ТЕХНОЛОГИИ



1 Всегда все запрещают

2 Создают невыполнимые требования

3 Не понимают трудностей персонала

4 Умеют только наказывать

5 Инструкции – не читабельны



ГАРДА
ТЕХНОЛОГИИ

...ЧТО ДЕЛАТЬ

ИНФОРМАЦИОННЫЙ ВАКУУМ

ГАРДА
ТЕХНОЛОГИИ

ПЕРИМЕТР

VS

ENDPOINT



ЧТО ДЕЛАТЬ БЕЗОПАСНИКУ

ГАРДА
ТЕХНОЛОГИИ

1 Повышать удобство,
вводя безопасные сервисы

2 Контролировать максимум,
запрещать минимум

3 Проверки извне
и изнутри

4 Программы
Security Awareness

5 Повышение престижа
службы ИБ



РЕЗУЛЬТАТЫ ОПРОСА

ГАРДА
ТЕХНОЛОГИИ





ГАРДА
ТЕХНОЛОГИИ

**СПАСИБО
ЗА ВНИМАНИЕ!**



г. Москва, Ленинская слобода, 26\5
8 (495) 116 56 61



info@gardatech.ru



/gardatechnologies



/garda_tech