Монитор безопасности

Проблема долговременных таргетированных атак и защиты от них

О КОМПАНИИ

Ключевые возможности

- Применяем те же технологии, что и реальные хакеры
- Воспроизводим атаки внешних злоумышленников или внутренних нарушителей
- Выявляем уязвимости, недоступные для сканеров безопасности и прочих автоматизированных технических решений
- Акцентируем свое внимание не на широко распространенных ошибках в программном обеспечении и стандартных уязвимостях, а на реальных угрозах, способных нанести урон ИТ-инфраструктуре или привести к финансовым или репутационным потерям

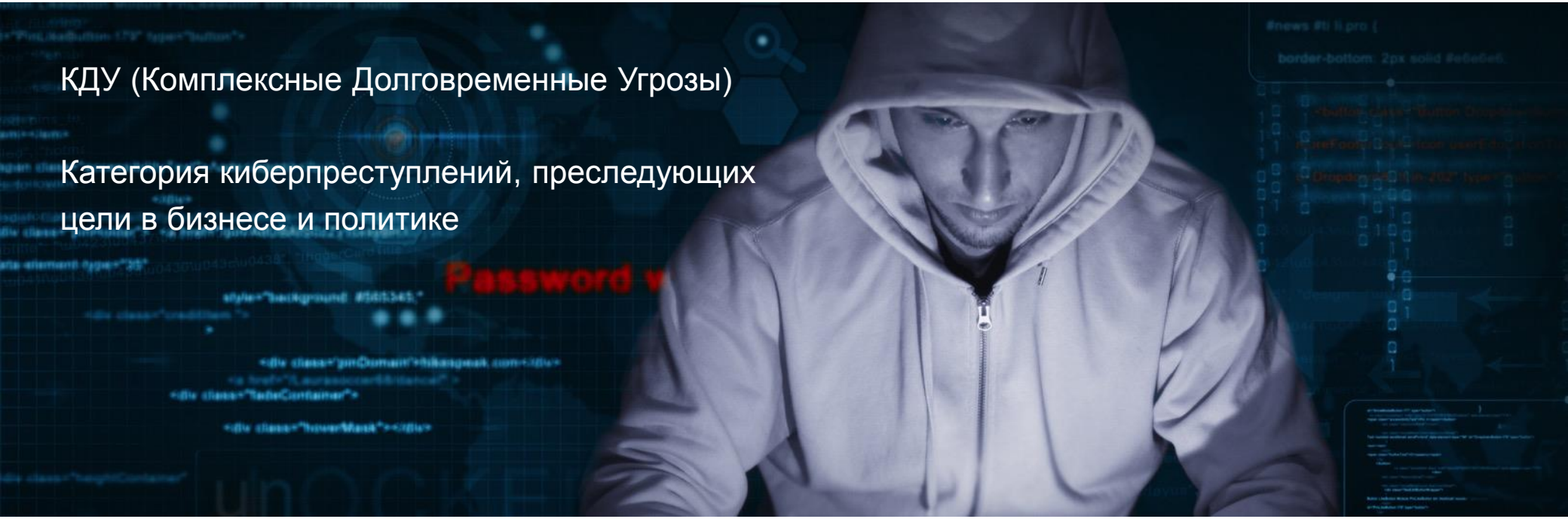
Услуги

- Аудит web-приложений
- Внешний аудит и внутренний аудит:
  - мобильных устройств
  - VoIP
  - WLAN
  - DMZ и т.д.
- Криминалистический анализ
- Обеспечение безопасности при разработке ПО
- Аудит защиты данных
- Собственная лаборатория выявления уязвимостей

Клиенты

Банки, государственные структуры, страховые компании, торговые площадки, он-лайн биржи, инновационные компании и производители в России, Австрии, Германии, Швейцарии, Литве

ТАРГЕТИРОВАННАЯ УГРОЗА



КДУ (Комплексные Долговременные Угрозы)

Категория киберпреступлений, преследующих цели в бизнесе и политике

КОМПЛЕКСНЫЕ

Злоумышленники используют сложные методологии для компрометации цели

ДОЛГОВРЕМЕННЫЕ

Злоумышленники работают медленно и скрытно, их основная цель - не быть обнаруженными как можно дольше

УГРОЗЫ

Злоумышленники целенаправленно выбрали Вашу организацию: они охотятся за критически важной для Вас информацией. Они хорошо подготовлены, организованы, мотивированы и не испытывают недостатка в средствах

ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

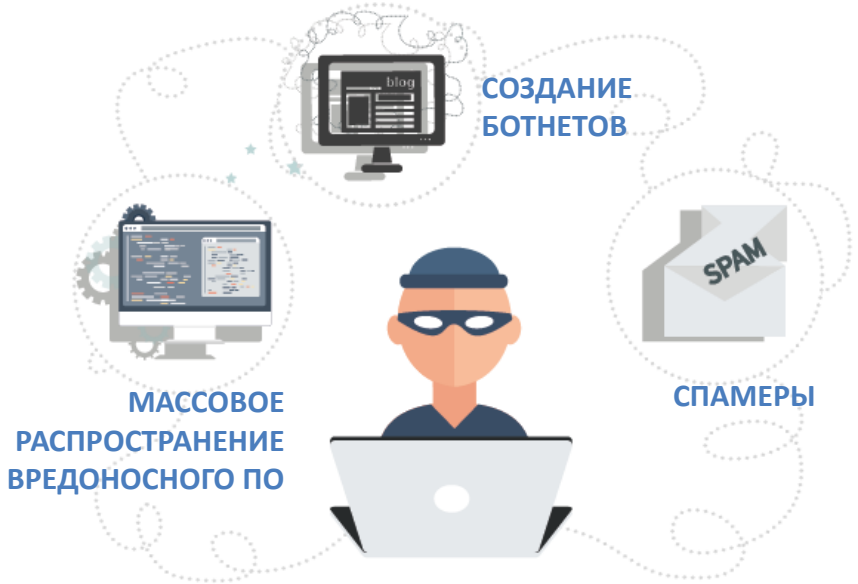
Что это?

ТАРГЕТИРОВАННАЯ АТАКА

КТО ЗЛОУМЫШЛЕННИК?

- Энтузиасты
- «Обиженные» сотрудники
- Организованные преступные группировки

НЕТАРГЕТИРОВАННАЯ АТАКА



КТО ЗЛОУМЫШЛЕННИК?

- Любители
- «Скрипт-школьники»

ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

Нарушитель

- Сбор сведений о цели
- Точка входа
- Внедрение вредоносного ПО

КРИТИЧЕСКИЕ УЯЗВИМОСТИ В ВЕБ-ПРИЛОЖЕНИЯХ

ЗАГРУЗКА ВРЕДОНОСНЫХ ФАЙЛОВ

ЦЕЛЕВОЙ ФИШИНГ

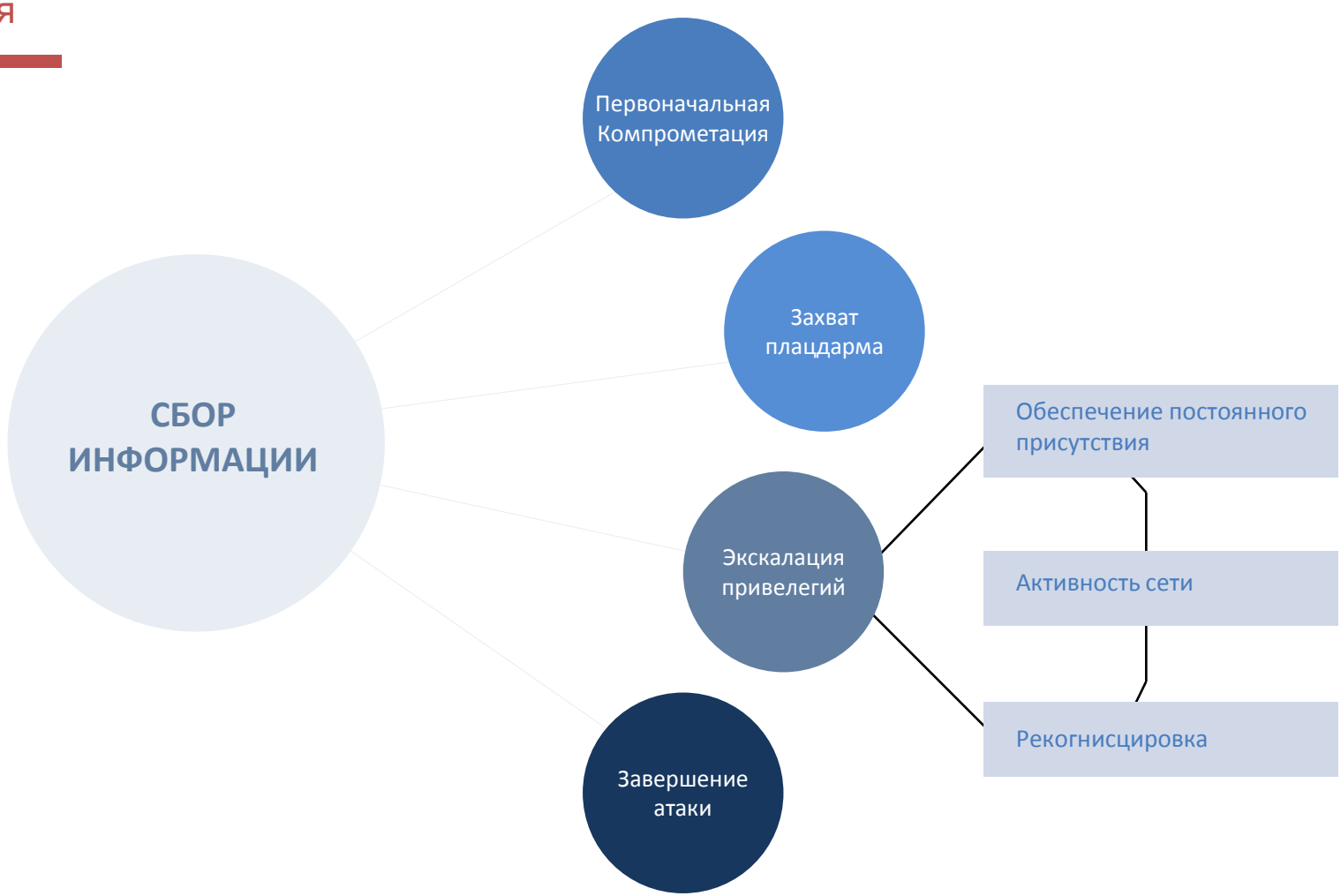
СБОР ИНФОРМАЦИИ

ПЕРВОНАЧАЛЬНАЯ КОМПРОМЕТАЦИЯ

СОЗДАНИЕ ПЛАЦДАРМА

ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

Анатомия



ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

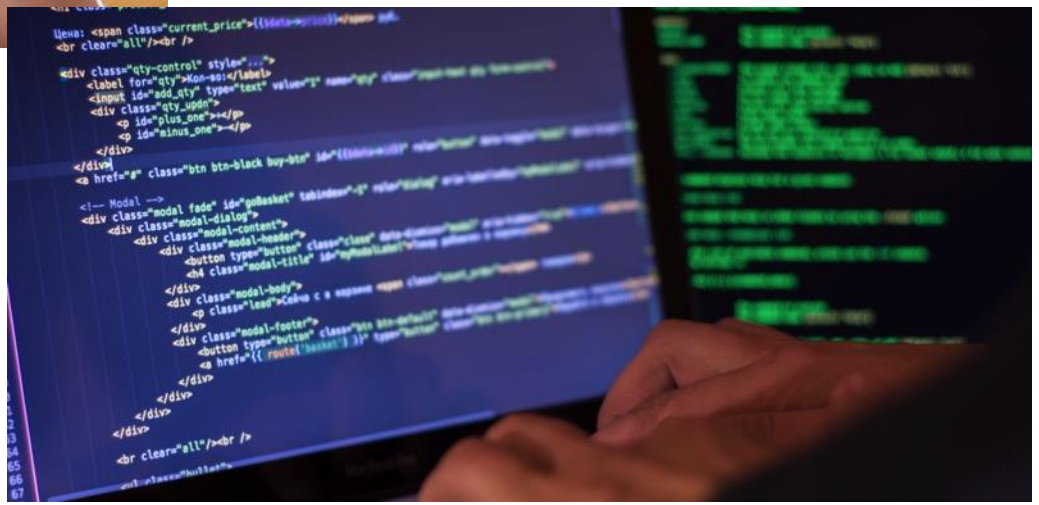
Опыт ПЕРВЫЙ

ИСХОДНЫЕ ДАННЫЕ

- Крупная инфраструктурная компания
- Изолированные сегменты сети
- Разветвленная и распределенная сеть
- Сотрудники знали о проводимой атаке

ФИЗИЧЕСКОЕ ВНЕДРЕНИЕ

- Без специальных мероприятий по обеспечению скрытности
- 2 недели взлом оставался незамеченным
- Компрометация критически важных серверов



ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

Опыт ПЕРВЫЙ

РЕЗУЛЬТАТЫ

Скомпрометированы критически важные сервера

На момент обнаружения взлома мероприятия по противодействию разрознены и неэффективны

Потенциально огромный ущерб компании

ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

Опыт ВТОРОЙ

ИСХОДНЫЕ ДАННЫЕ

- Крупная международная логистическая компания
- Распределенная сеть
- Большое количество сотрудников
- Сотрудники знали о проводимой атаке

ВЗЛОМ

- Без специальных мероприятий по обеспечению скрытности
- Взломаны почтовые сервера и файлообменники
- Распространено «вредоносное ПО»
- «Инфицированы» компьютеры руководящего звена

ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

Опыт ВТОРОЙ

РЕЗУЛЬТАТЫ

Скомпрометированы критически важные рабочие станции

Мероприятия по противодействию разрознены не проводились

Получен доступ к конфиденциальным данным наивысшего уровня

Потенциально критический ущерб компании

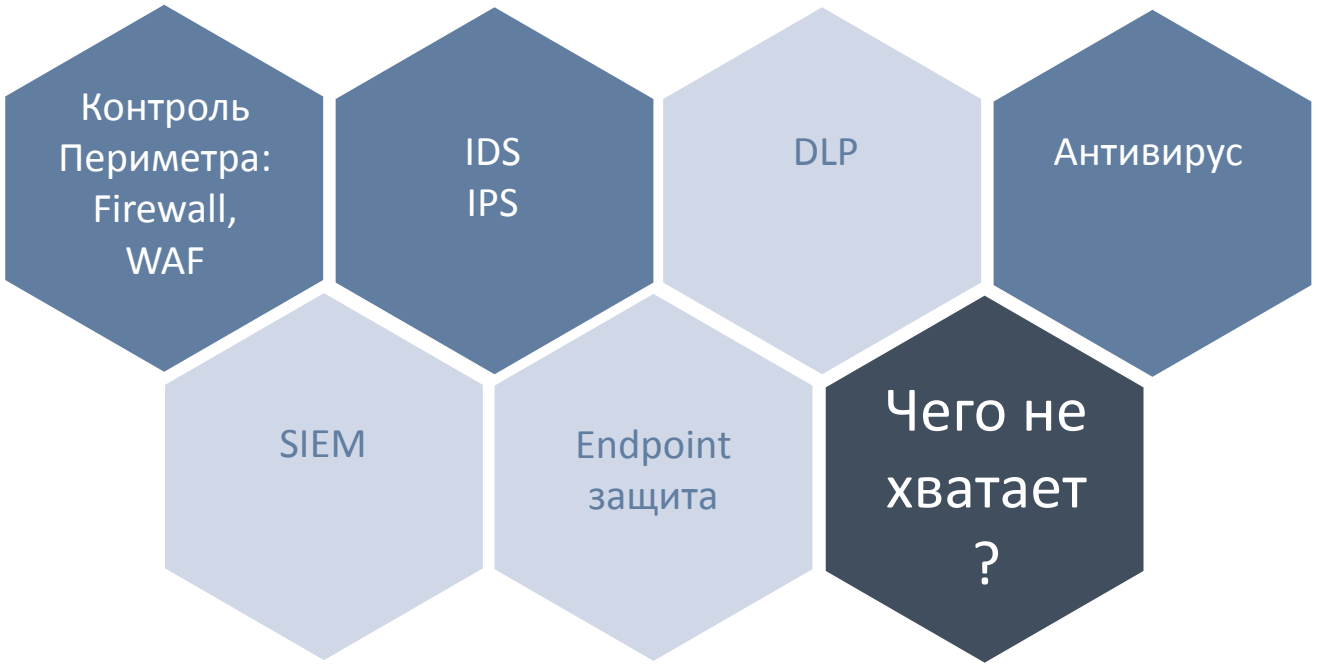
ДОЛГОВРЕМЕННЫЕ ТАРГЕТИРОВАННЫЕ АТАКИ:

Сложности противодействия

- Общепринятые мероприятия по обеспечения ИБ малоэффективны
- Колоссальные затраты на предотвращение атак
- Недостаточное внимание мониторингу и оперативным мероприятиям
- Нарушения безопасности неизбежны

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Комплексный подход



МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Комплексный подход

КАК БЫТЬ БЛИЖЕ К ВРАГУ?

ЗАДАЧИ

1. ОБНАРУЖИТЬ ТОЧКУ ВХОДА
2. ОПРЕДЕЛИТЬ ИНСТРУМЕНТЫ
3. ОПРЕДЕЛИТЬ ЦЕЛИ
4. УЗНАТЬ МОТИВЫ
5. ОТВЛЕЧЬ ЗЛОУМЫШЛЕННИКОВ ОТ РЕАЛЬНЫХ ЦЕЛЕЙ

ТРЕБОВАНИЯ

- Мониторинг в реальном времени вредоносной активности
- Правдоподобность и интерактивность для злоумышленника
- Возможность интеграции в продуктовую среду
- Возможность получать детальную информацию об угрозе
- Профилировка злоумышленника
- Контрмеры (например, документы с callback-функциями)
- Невидимость для злоумышленников
- Масштабируемость
- Поддержка облачных технологий
- Отсутствие ложных срабатываний

КОМПОНЕНТЫ

ПРИВЛЕКАТЕЛЬНАЯ ЛОВУШКА

ЦЕЛЬ: Отвлечение внимания злоумышленников

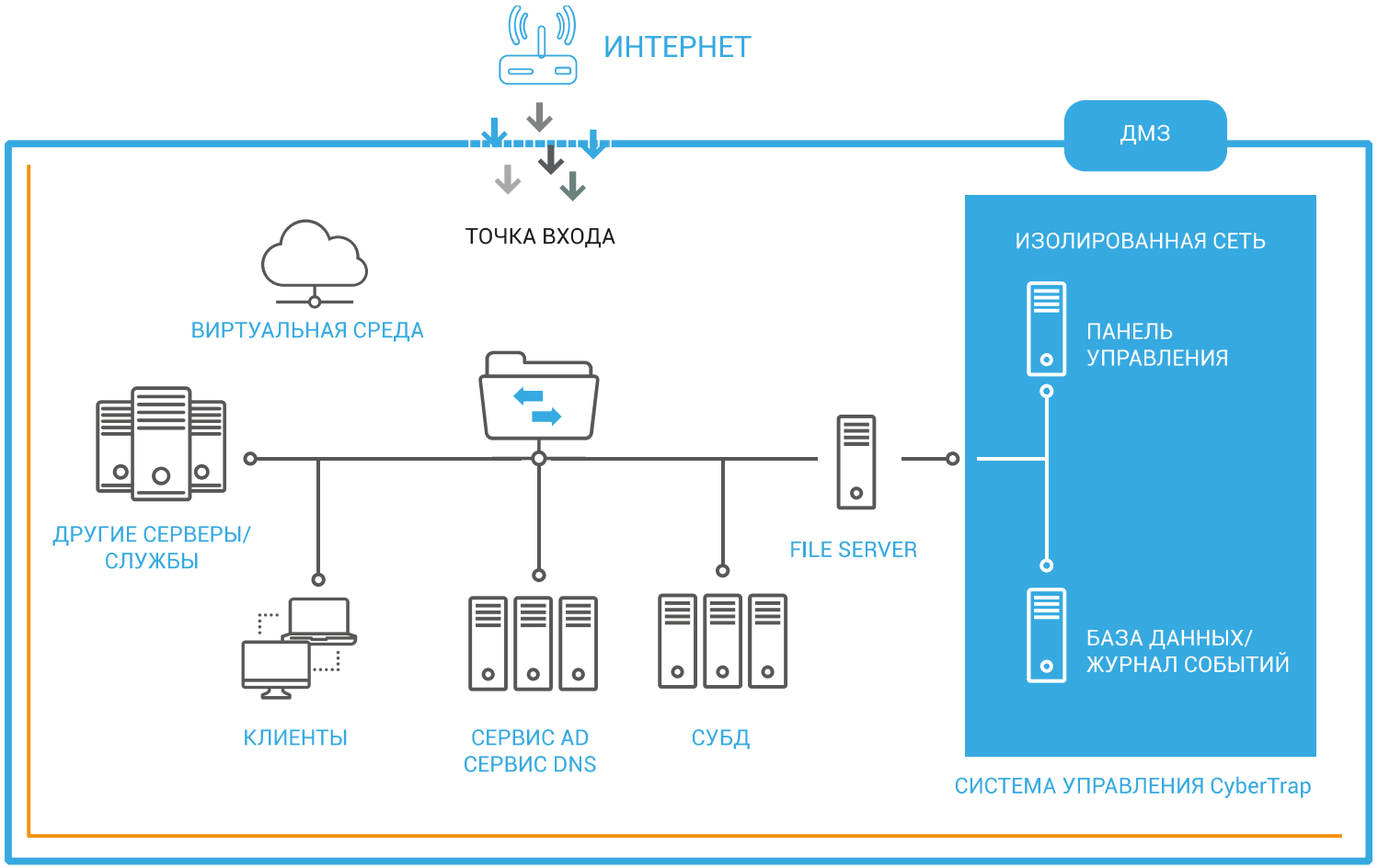
РЕАЛИСТИЧНЫЕ КОПИИ ИНТЕРЕСУЮЩИХ ЗЛОУМЫШЛЕННИКОВ ОБЪЕКТОВ

ЗАДАЧА: Направить злоумышленника по ложному следу

СИСТЕМА МОНИТОРИНГА

РЕЗУЛЬТАТ: Фиксация всех действий злоумышленника

КОМПОНЕНТЫ


ИНТЕРНЕТ
ДМЗ
ТОЧКА ВХОДА
ВИРТУАЛЬНАЯ СРЕДА
ИЗОЛИРОВАННАЯ СЕТЬ
ПАНЕЛЬ УПРАВЛЕНИЯ
ДРУГИЕ СЕРВЕРЫ/ СЛУЖБЫ
FILE SERVER
БАЗА ДАННЫХ/ ЖУРНАЛ СОБЫТИЙ
КЛИЕНТЫ
СЕРВИС AD
СЕРВИС DNS
СУБД
СИСТЕМА УПРАВЛЕНИЯ CyberTrap

РЕЗУЛЬТАТЫ

Профиль злоумышленника	Детализированные методы и инструменты, используемые во время атаки	Углубленный анализ (какие цели преследуют хакеры, какую информацию они ищут)
История и хронология взлома	Источники происхождения злоумышленников на основе их IP-адресов и данных DNS	

ХРОНОЛОГИЯ ОБНАРУЖЕННОЙ APT

BREACH DETAILS

DATE	Host	Activity	Remark	IP / MD5	Measures in production
23-Mar	IIS (EntryPoint)	Start reconnaissance	stealth vulnerability scan with "NetSparker". Requests every 3-5 minutes for ~ 3 weeks.	59.188.231.49	Block IP IP pDNS Attribution Monitoring
13-Apr	IIS (EntryPoint)	SQL Injection	attacker stealing credentials (to login to the web app)	182.138.149.50	Block IP IP pDNS Attribution Monitoring
13-Apr	IIS (EntryPoint)	Webshell upload	r00ts.aspx Chinese webshell	221.163.238.146	Block IP IP pDNS Attribution Monitoring
13-Apr	IIS (EntryPoint)	Internal reconnaissance	Checking which AV is running. Trying to resolve corporate website and mail gateway (to verify if they are in the same network). Basic network discovery. Lookup local and domain administrators.		Monitoring Usage of Domain Admins
13-Apr	IIS (EntryPoint)	Deployment of RAT Malware	**mcsync.exe is a valid and digital signed executable from McAfee.** The malware used DLL hijacking mechanism to abuse the trustworthiness of the signed exe.	C&C communication with 14.206.231.75 a13fbda3962858fa767505128a7cfc7f ipfcajkmp 501eed51578e795af7f2f5fb3078178 mcsync.exe bf3e07c48a1dd5dc08beddc9db09eef2 mcutil.dll b2d11d56b0e324de962a4e76afb8afd8 mcutil.dll.sys 890f86d6f8315ed6189a42dde6c5556f rcjbsgzpmwcm	Block IP IP pDNS attribution monitoring Create AV signatures Create IPS signatures
13-Apr	IIS (EntryPoint)	Upload of misc tools	portscanner and password extraction tools. Working directories are folders which are default hidden by MS ("Hide protected operating system files") like c:\Recovery	log.exe: df840ac27051d26555a109cc47d03fe4	Create AV signatures Create IPS signatures
13-Apr	IIS (EntryPoint)	dump of cached passwords			
13-Apr	IIS (EntryPoint), Database	Jumping to database host	copy malware over CIFS and trigger start of the executable with cronjob		Monitor new cronjobs

ХРОНОЛОГИЯ ОБНАРУЖЕННОЙ APT

14-Apr	Database	Internal reconnaissance	Looking up for domain controllers and external hosts (to verify if they are in the same network)	
15-Apr	Database	Looking for specific user and systems	trying to resolve exposed corporate mail gateways, **internal** productive hostnames and **internal** users	Internal investigations: attacker is aware about internal information. In-Depth monitoring of affected systems and users. Checking usage of these usernames on other Systems Issue Warning to these specific Users.
15-Apr	Database	Looking for classified information	evidence through dedicated search strings	Raising Awareness on the specific research teams. Check that all measures with this user group are intact and working (eg. Encryption, DLP, ...)
16-Apr	IIS (EntryPoint), Domain Controller	Jumping to Domain Controller	copy malware over CIFS and trigger start of the executable with cronjob	
16-Apr	Domain Controller	Internal reconnaissance	looking up trust relations to other domain controllers	Review configurations of domain-controller
16-Apr	Domain Controller	Extraction of all credentials from DC		Create Dummy Users with passwords from CT. Implement Alerting mechanism on abuse.

Монитор безопасности

119334, г. Москва, 5-й Донской проезд, д. 15, стр. 11.
Тел.: +7(495) 984-08-34
E-mail: info@securitymonitor.ru