GIS DAYS

ТОП-5 причин, почему следует использовать системы киберобмана для защиты бизнеса от целевых атак

Черников Дмитрий

Руководитель направления пресейла

Xello

О компании

Xello — лидер сегмента решений класса Distributed Deception Platform (DDP) на российском рынке информационной безопасности

- Разрабатываем первую российскую платформу киберобмана более 5 лет
- Реализовали более 30 проектов в различных сферах к сентябрю 2023 года

GIS DAYS

xello

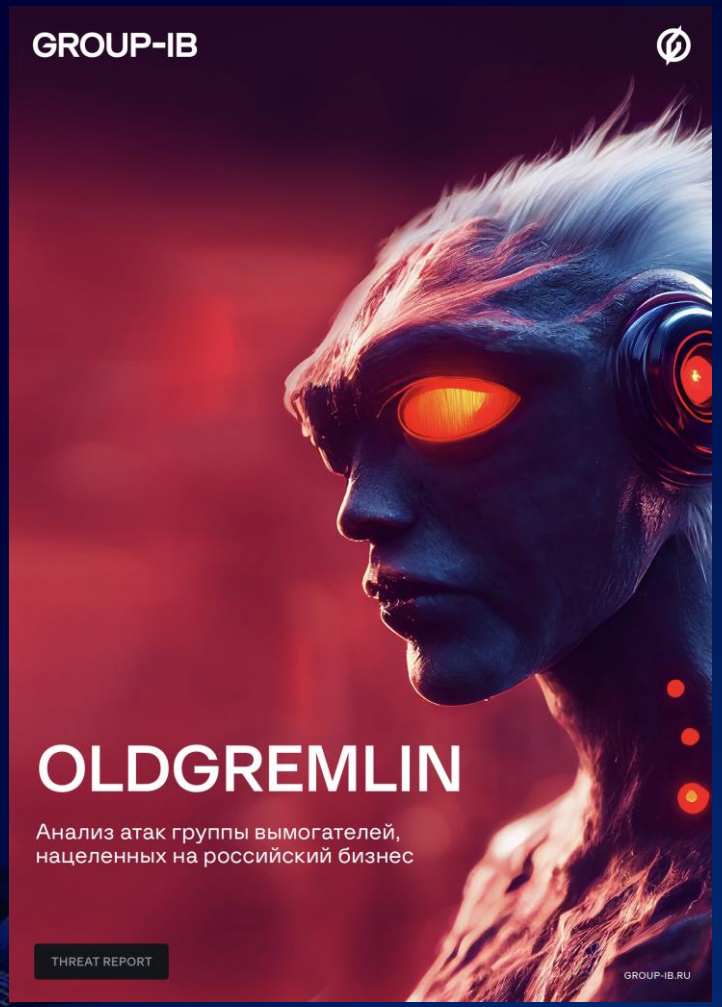
Чем компании сегодня защищаются

- Антивирус
- IPS/IDS
- SIEM-система
- Next generation firewall (NGFW)
- Песочница (Sandbox)
- Network traffic analysis (NTA)
- Web application firewall (WAF)
- Privileged access management (PAM)
- Data loss prevention (DLP)
- Endpoint detection and response (EDR)

GIS DAYS

xello

APT-атаки в 2022 году



positive technologies

Летающие в «облаках»: APT31 вновь использует облачное хранилище, атакуя российские компании

Дата публикации 4 августа 2022

Введение

В апреле 2022 года специалисты PT Expert Security Center в ходе ежедневного мониторинга угроз выявили атаку на ряд российских организаций сферы медиа и ТЭК, в которой использовался вредоносный документ с именем «список.docx», извлекающий из себя вредоносную нагрузку, упакованную VMProtect. Мы проанализировали пакет сетевой коммуникации и выяснили, что он идентичен тому, который мы рассматривали в отчете по исследованию инструментов группировки APT31, что позволило предположить, что и эти инструменты могут принадлежать этой же

BI.ZONE | Eng

Группировка Red Wolf вновь шпионит за коммерческими организациями на территории России

Эксперты BI.ZONE обнаружили новую волну атак группировки Red Wolf (также известна как RedCurl), которая не проявляла себя с 2022 года

Рост количества APT-атак

Рост атак, исходящих от квалифицированных и хорошо организованных групп (APT)

68 %

Успешных атак **в первом квартале 2023** года имели целенаправленный характер

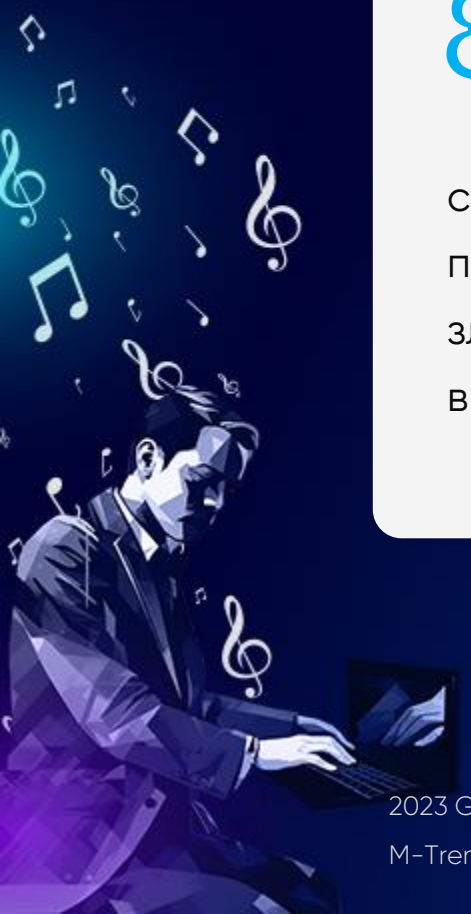
78 %

Успешных атак **во втором квартале 2023** года имели целенаправленный характер

Актуальные киберугрозы: I квартал 2023 года // Positive Technologies
Актуальные киберугрозы: II квартал 2023 года // Positive Technologies

GIS DAYS

xello



84 минуты

среднее время
проникновения
злоумышленника
в инфраструктуру компании

16 дней

медианное время
незаметного присутствия
злоумышленника
в инфраструктуре

2023 Global Threat Report // CrowdStrike

M-Trends 2023 // Mandiant (Google Cloud)

Причина 1:
защищают от целевых атак (APT)

Классические средства защиты блокируют 90% угроз

- Опираются на описанную логику и правила
- Используют поведенческий анализ
- Быстро принимают решение

но не 10% самых сложных

Особенности APT-атаки

- Финансовые и технические возможности
- Организация подготовленной группой: APT-группировкой
- Долгосрочное и тщательное планирование: закупка инструментов, анализ инфраструктуры и другое
- Сложности обнаружения: чистка логов и других следов
- Нацеленность на конкретный объект: корпоративные секреты, исходники кода, топ-менеджмент
- Длительности атаки: реализуется до конечного результата

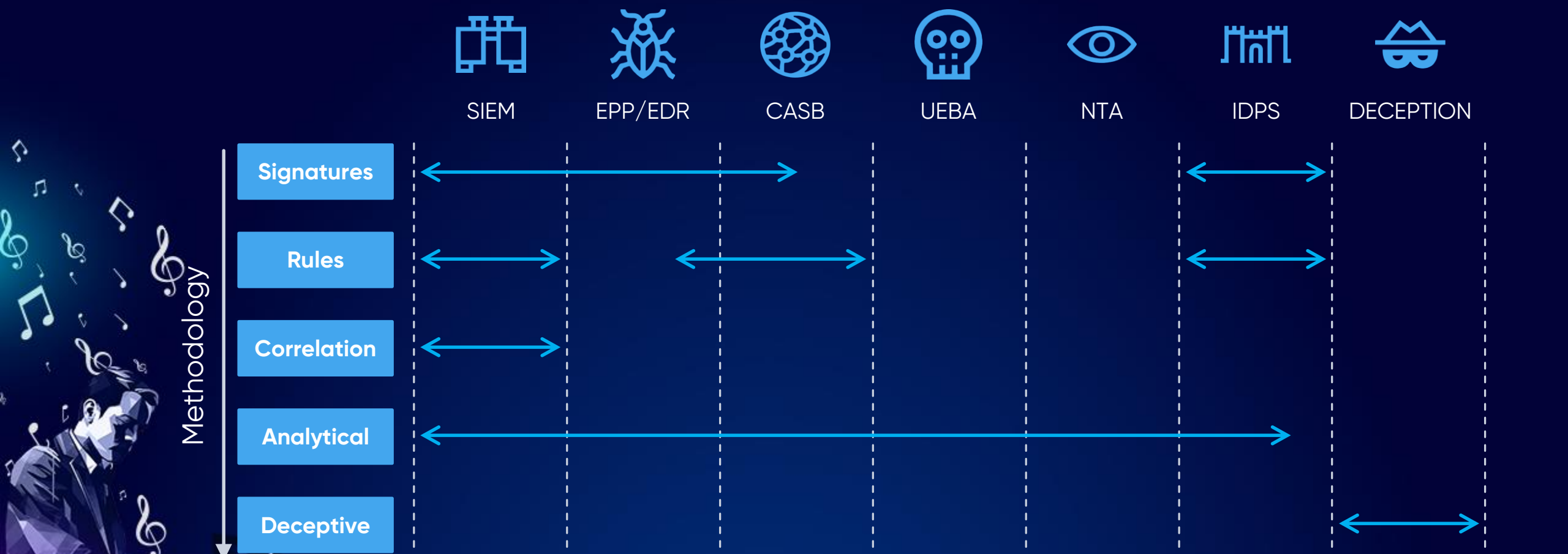
GIS DAYS

xello

Проникновение в корпоративную сеть — вопрос времени

- Уязвимости в Open Source компонентах
- Снижение уровня защищённости
- Компрометация менее защищённых компаний-подрядчиков
- Использование методов социальной инженерии

Другой подход выявления киберугроз



Как это работает

Xello Deception

Сохранённые подключения

Учётные записи

Приманки

Конфигурационные файлы

Документы

Сервер управления

ИТ-сервисы

Приложения

Ловушки

Базы данных и хранилища

Устройства

Интеграция

- SIEM
- SOAR
- EDR
- NGFW
- NAC
- и другие СЗИ

Каталоги FreeIPA/ OpenLDAP/ LDAP (AD)

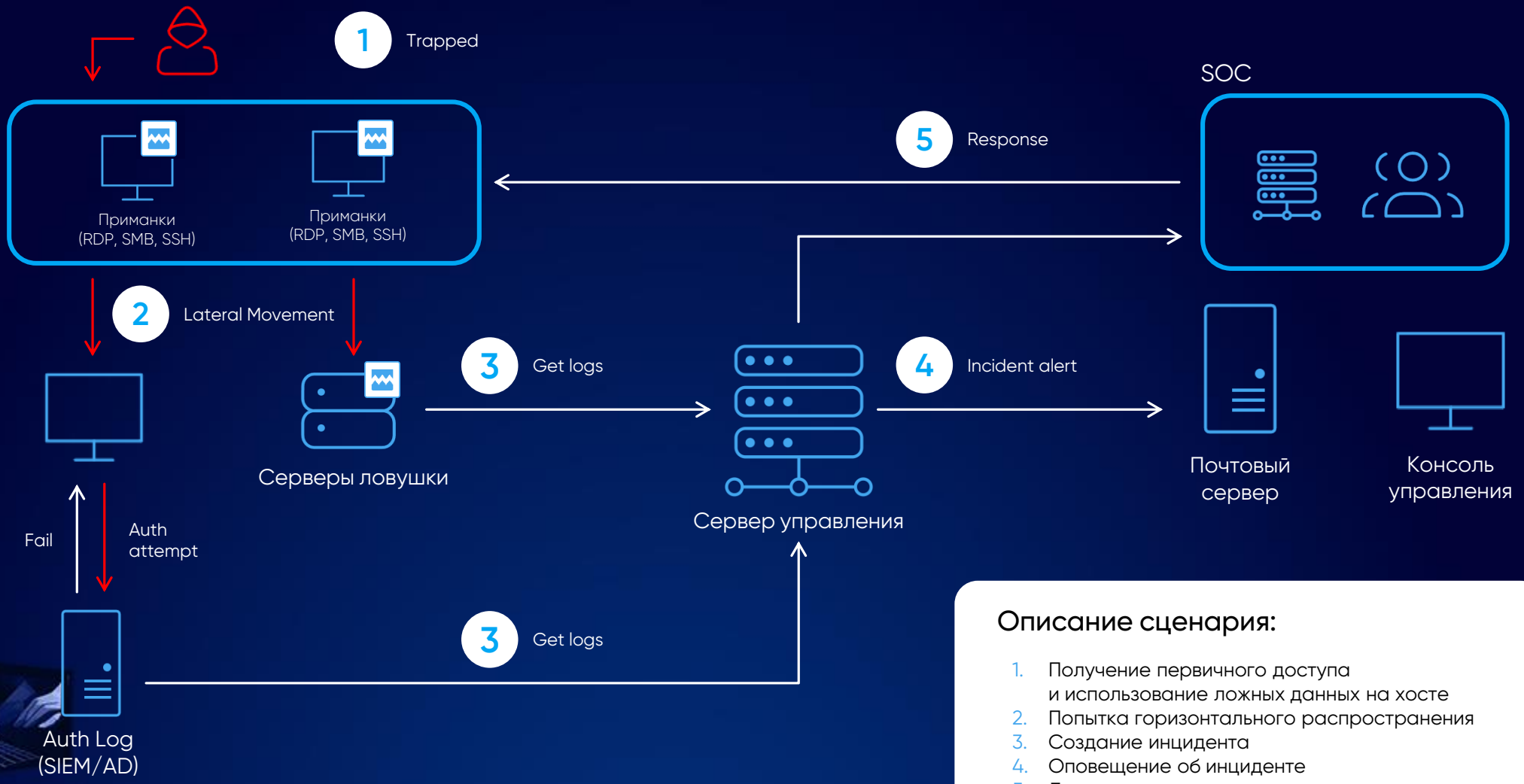
DNS

Конечные устройства

Корпоративная сеть

Технологическая сеть

Сценарии реагирования



Описание сценария:

1. Получение первичного доступа и использование ложных данных на хосте
2. Попытка горизонтального распространения
3. Создание инцидента
4. Оповещение об инциденте
5. Детектирование атаки

Причина 2:
выявляют атаки на самом критическом этапе

Место Xello Deception при APT-атаке

1. Разведка
2. Получение первичного доступа
3. Закрепление в сети
4. Горизонтальное передвижение
5. Повышение привилегий
6. Компрометация системы

Защита

Обнаружение

Исследование

Сдерживание и минимизация потерь

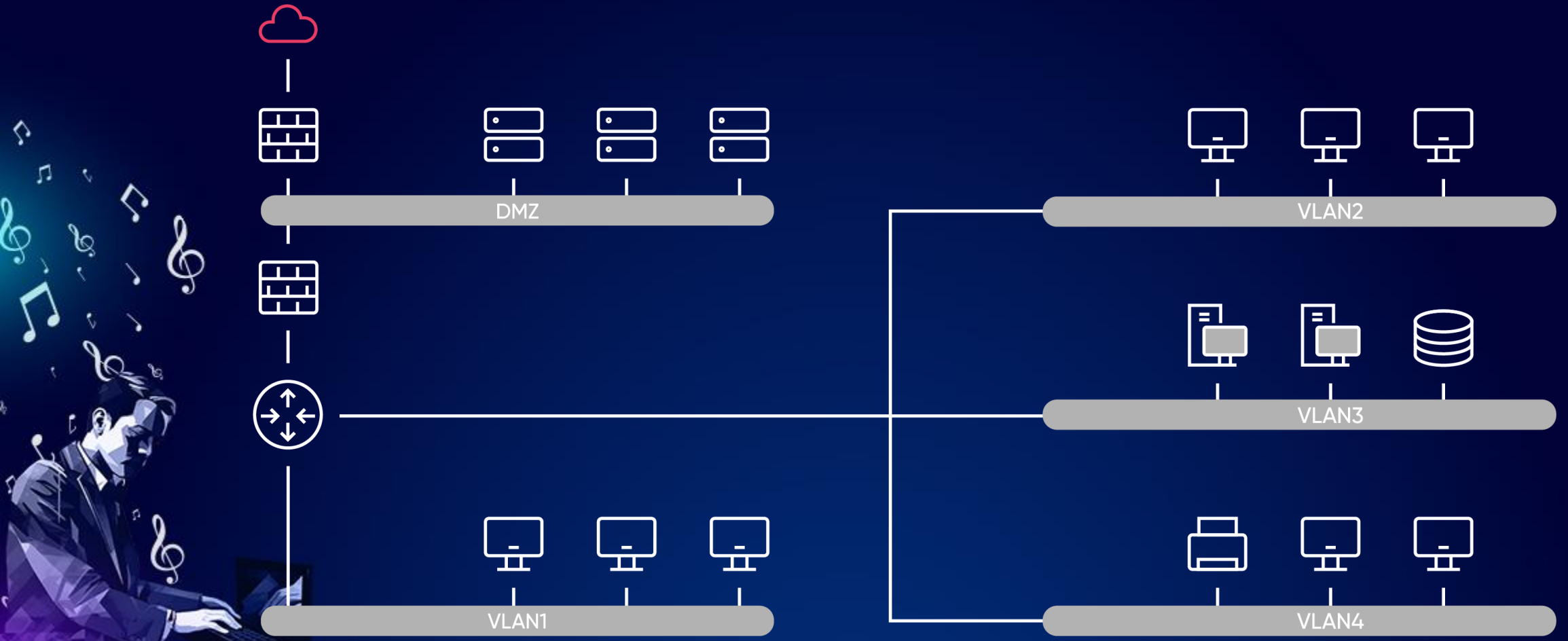
Классические системы защиты

Xello Deception

GIS DAYS

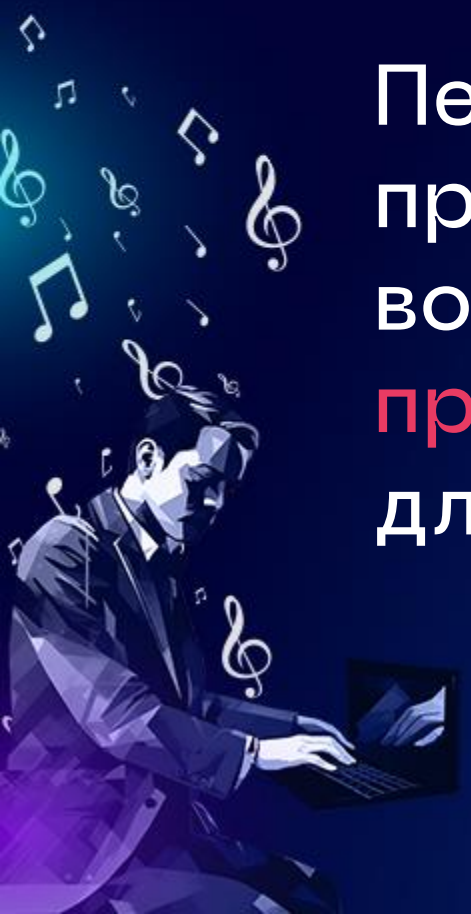
Горизонтальное передвижение — наиболее критический этап атаки

xello



GIS DAYS

xello

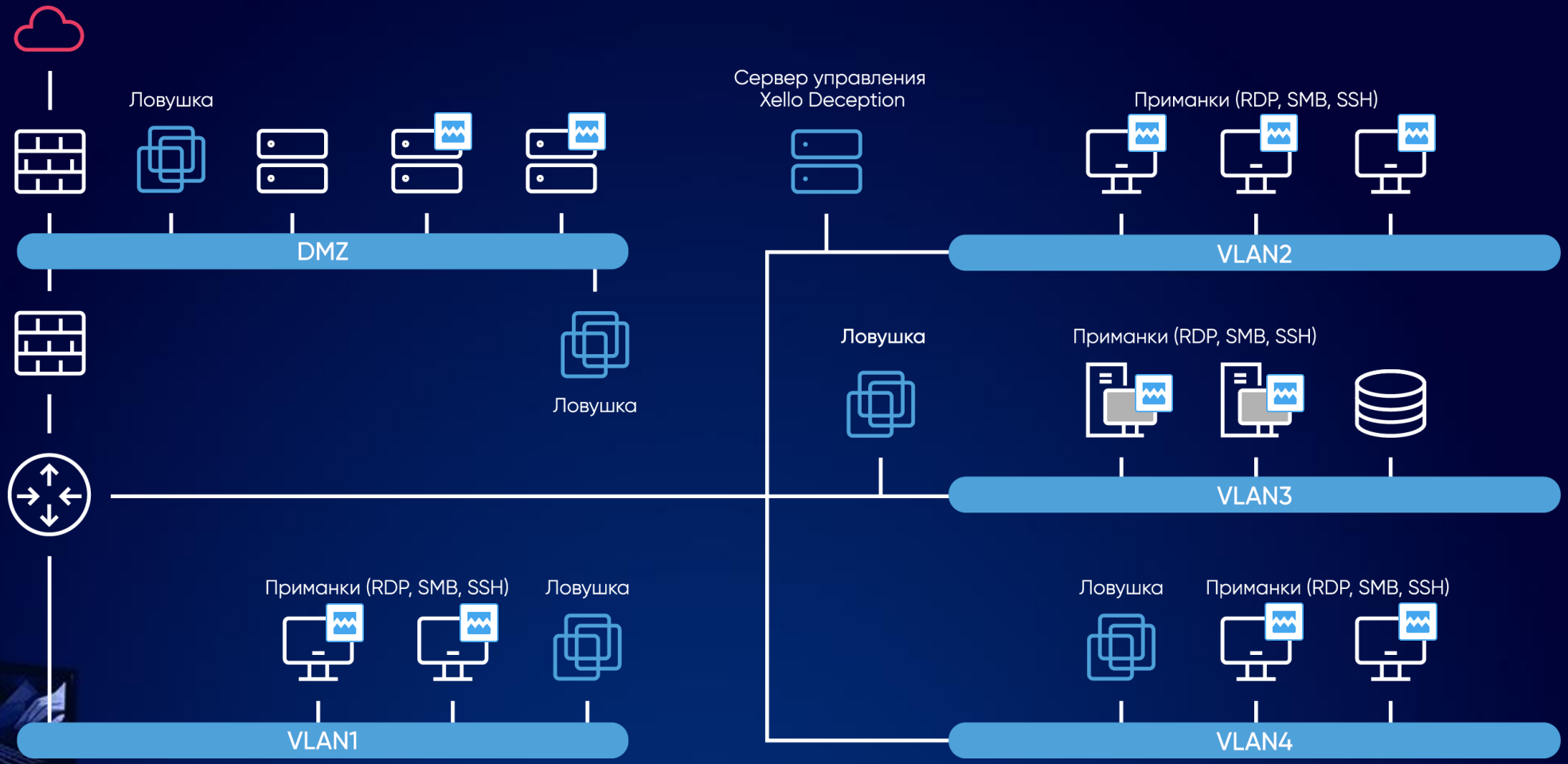


Периметровые средства защиты пропустили хакера и у него появляется возможность использовать легитимные протоколы и учётные записи для дальнейшей реализации кибератаки

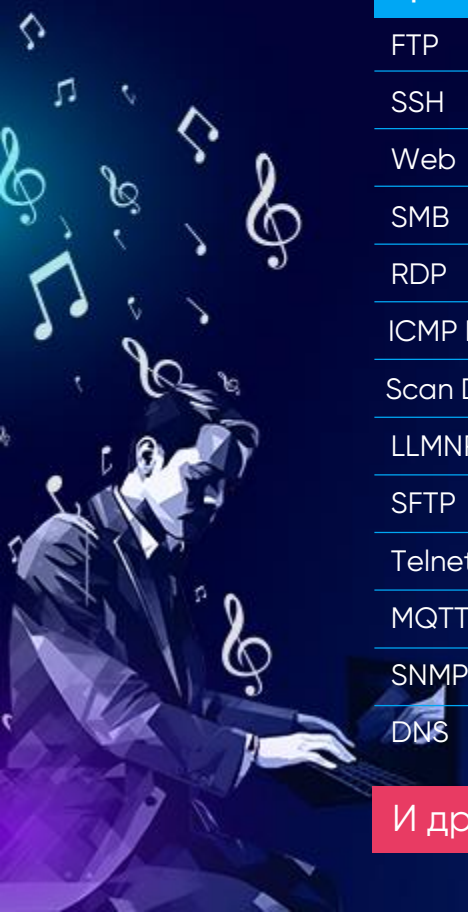
GIS DAYS

Ложный слой инфраструктуры, который невозможно избежать

xello



Примеры эмулируемых данных и активов



Ловушки

Триггер	Порт
FTP	TCP/21
SSH	TCP/22
Web	TCP/80, 443
SMB	TCP/445
RDP	TCP/3389
ICMP Detector	–
Scan Detector	–
LLMNR/NBT-NS Poisoning Detector	UDP/5355
SFTP	TCP/27017
Telnet	TCP/23, 2323
MQTT	TCP/1883
SNMP	UDP/161, 162
DNS	TCP/53

И другие

Примаки

Протокол	Тип приманки
ОС Windows	
Web credentials	Chrome
	Internet Explorer
	Mozilla Firefox
Saved credentials	RDP Sessions
	RAM (LSASS.exe)
	Microsoft Credential Manager
ОС Linux	
SSH	Files
	Bash history
	Known hosts
ОС Mac	
FTP	Bash history
	Configs
	Scripts

И другие

GIS DAYS

xello

Причина 3: предоставляют высокодоверенные триггеры

Приманки и ловушки направлены исключительно на злоумышленника

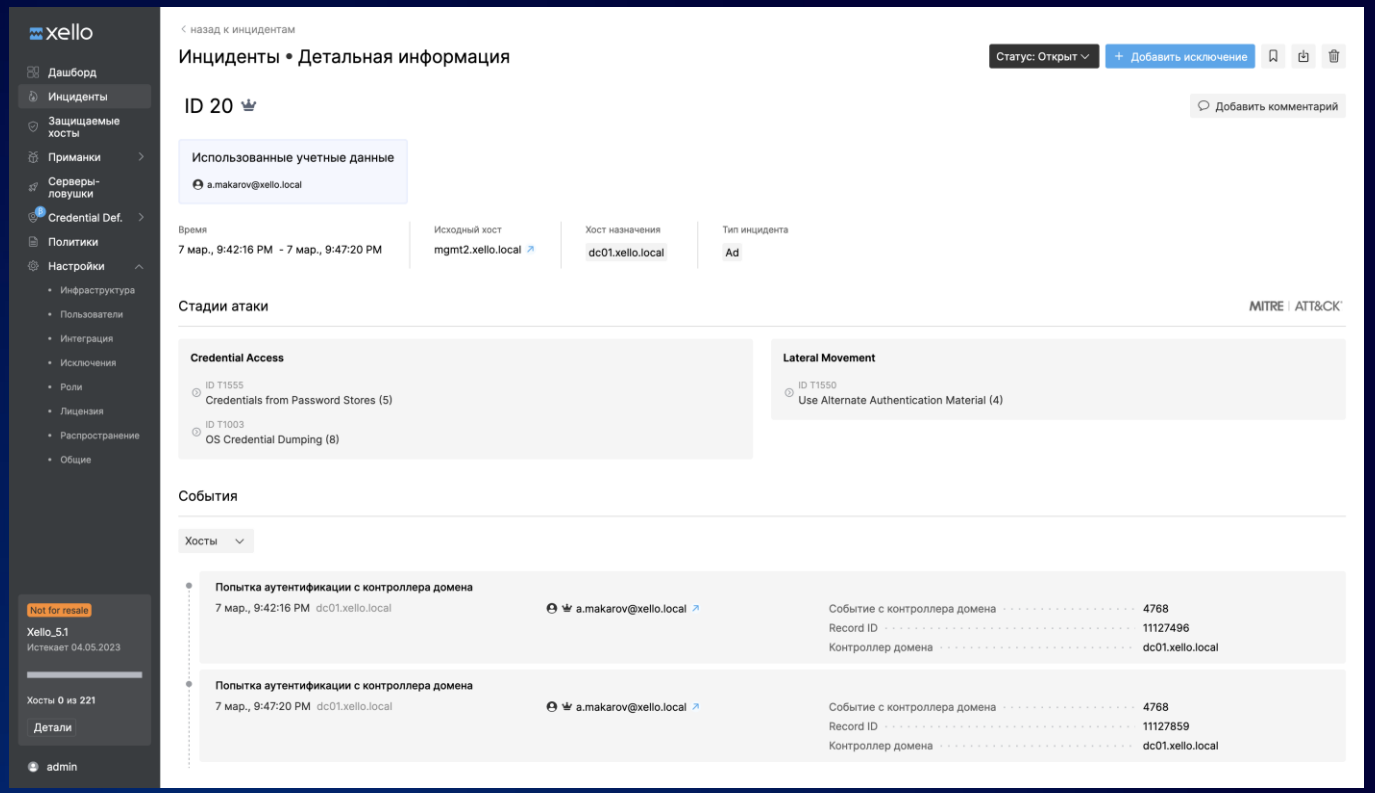
Не видны легитимным пользователям, поэтому не создают ложных срабатываний

Отсутствуют агенты на хостах, поэтому сложно выявить деятельность системы киберобмана

Причина 4: предоставляют форензику для расследования киберинцидентов

Криминалистические артефакты

- Первоначальная точка компрометации
- Следы запуска используемых инструментов
- Следы коммуникации злоумышленника с ложными активами
- Методы доступа, которые могут стать индикаторами компрометации



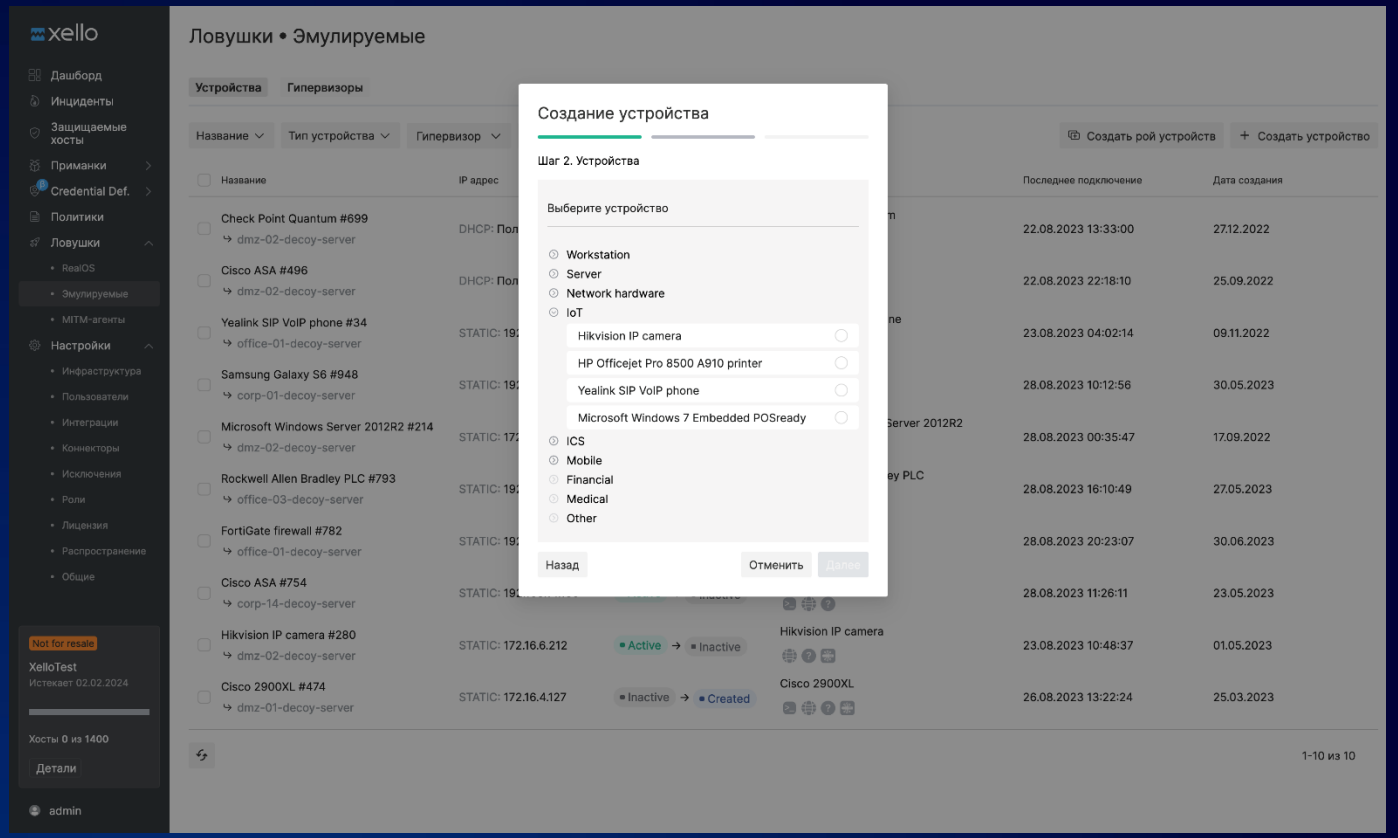
Причина 5:
простая интеграция и эксплуатация

GIS DAYS

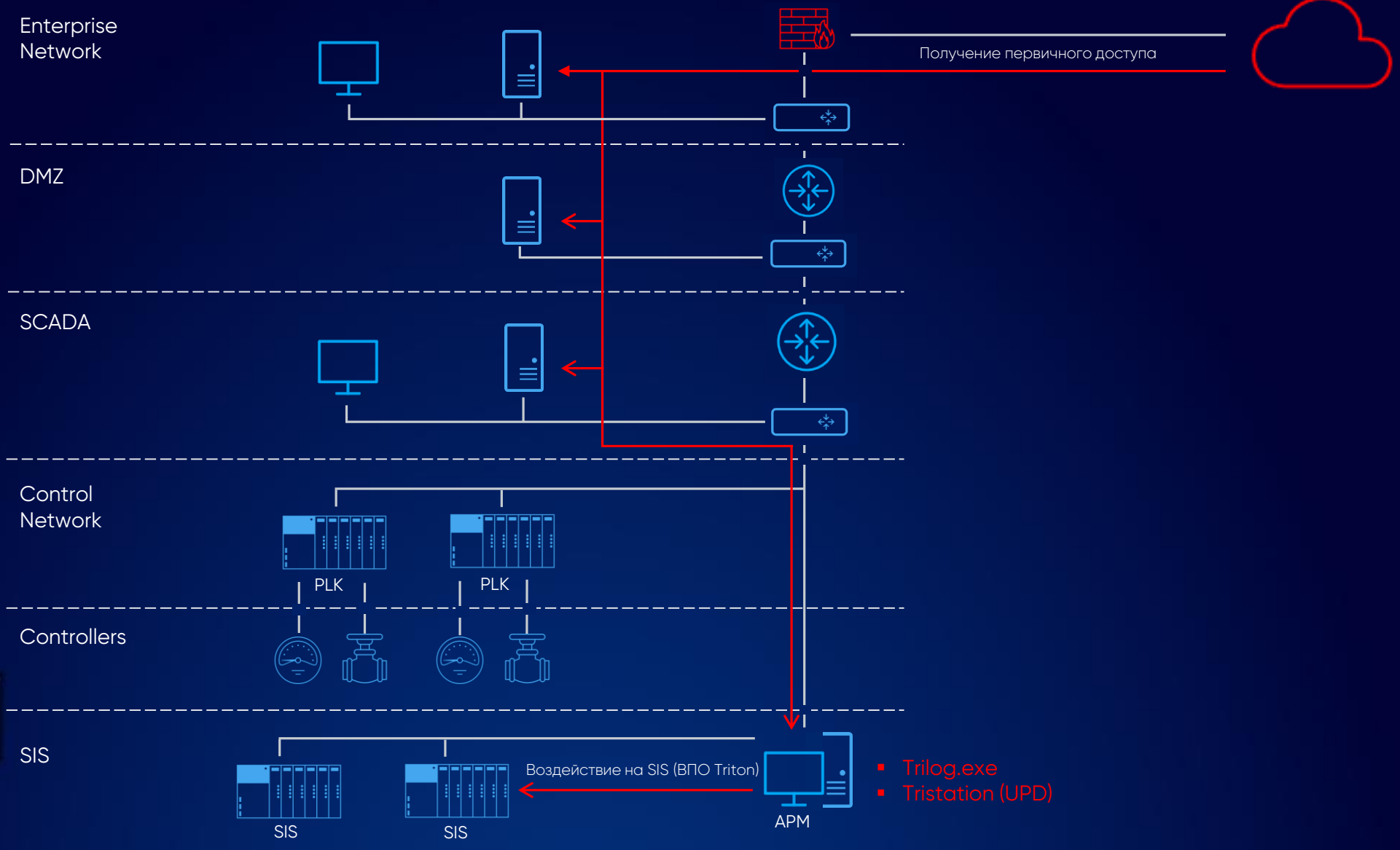
Автономность решения

xello

- Механизмы ранжирования и обновления приманок на хостах
- Адаптивная генерация приманок
- Автоматическое создание ловушек
- Гибкое управление ложным слоем инфраструктуры на распределённых площадках



Кейс. Triton в Petro Rabigh



Кейс. Сложности выявления атаки

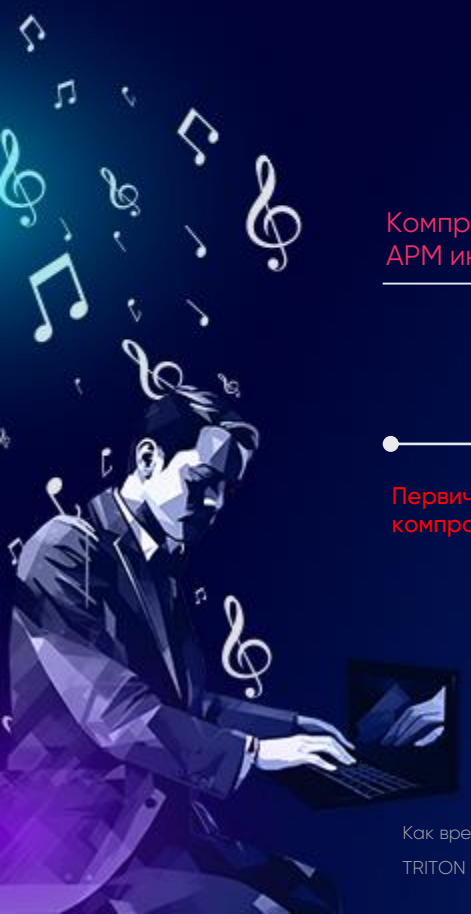
- переименовали файлы, чтобы они выглядели как легитимные, например, KB77846376.exe (как обновление для ОС Windows)
- использовали легитимные инструменты (RDP и PsExec/WinRM)
- модифицировали существующие легитимные файлы flogon.js и logoff.aspx

TOOL	COMPONENTS	PURPOSE	ATTACK LIFECYCLE STAGE						
			Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
SecHack	KB77846376.exe	Credential harvesting			x	x			
	KB77846376.exe.x64								
NetExec	NetExec.exe	Remote command execution					x		
	runsvc.exe	NetExec runner							
Cryptcat-based backdoor	cryptcat.exe cryptsvc.exe svchostpla.exe	Backdoor							
	compattelprerunner.exe	C&C domain name generator		x					
	ProgramDataUpdater.xml	Scheduled task file (persistence mechanism)							
PLINK-based backdoor	napupdatedb.exe	Backdoor		x				x	
Bitvise-based backdoor	alg.exe userinit.exe csrss.exe	Backdoor							
	tquery.dll txflog.dll cryptopp.dll DEFAULT DEFAULT.BAK	Backdoor components					x	x	
OpenSSH-based backdoor	spl32.exe WinSAT.exe csrss.exe	Backdoor							
	clusapi.dll PolicMan.dll verifier2.dll misc.mof setup.ini	Backdoor components					x	x	
WebShell	logoff.aspx	Modified legitimate Outlook Web Access Component							
	flogon.js	Modified legitimate Outlook Web Access Component				x		x	
	ftpexts.tlb	Output file containing credentials harvested by logoff.aspx							

FIREEYE

TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping

Кейс. Если бы был внедрен киберобман



- Распространение ложных УЗ в оперативную память процесса lsass.exe
- Распространение ложных устройств разных производителей

Компрометация АРМ инженера ПАЗ

Использование SecHack для кражи УЗ

Установка бэкдора (RDP/SSH)

Исследование ОТ сети и устройств

Изменение состояния контроллера

Отправка неавторизованных команд

Первичная компрометация

T0818: Engineering Workstation Compromise

T1003: OS Credential Dumping LSASS Memory

T1021: Remote services

T0808: Control Device Identification

T0808: Modify Controller Logic

T0808: Unauthorized Command Message

Воздействие на АСУ ТП

Как вредонос Trisis может парализовать целый завод, и есть ли шанс от него защититься // Ростелеком-Солар

TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping

GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ!

xello.ru

xello