Двухфакторная аутентификация или дресскод на входе

2011 г., опрос компании GrlDsure

Результаты:

60% из опрошенных компанией GrlDsure руководителей информационных служб отмечают высокий уровень сложности традиционных методов двухфакторной аутентификации и считают, что реализация этих методов обходится слишком дорого

36% опрошенных считают многоуровневую аутентификацию важнейшим фактором для безопасности доступа

Лишь 34% опрошенных уверены, что сотрудники в состоянии сделать все необходимое для защиты компании от компьютерных угроз.

32% ставят на первое место обучение сотрудников, и только 7% высказываются за полное отключение удаленного доступа

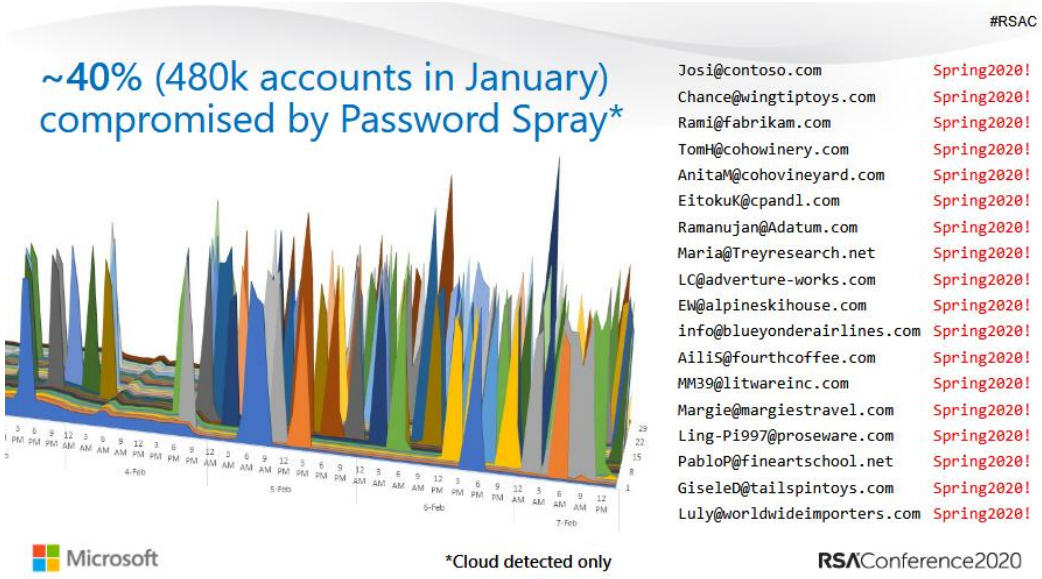
2020 г., конференция RSA 2020

Microsoft:

99,9% взломанных аккаунтов не использовали двухфакторную аутентификацию (2FA) в качестве защитной меры

По какой-то причине пользователи не стремятся активировать 2FA, даже когда речь заходит о корпоративных учётных записях. Например, всего лишь 11% аккаунтов организаций задействовали двухфакторную аутентификацию.

Представители Microsoft отметили, что большинство атак на учётные записи крайне просты: злоумышленник пытается подобрать часто используемые связки «имя пользователя-пароль». Например, атаки вида «password sprayed» привели к взлому 480 тыс. аккаунтов в январе



Источник: https://www.anti-malware.ru/news/2020-03-06-1447/32156

2022 г., официальный блог Google

SAFETY & SECURITY

Keeping you safe online with Google and beyond

Feb 08, 2022 · 4 min read

Jen Fitzpatrick
SVP, Core Systems and Experiences

Share

Keeping your information safe

We provide easy, simple-to-use tools like Security Checkup to give you actionable recommendations on how to strengthen the security of your Google Account. In 2021, we auto-enrolled over 150 million people in two-step verification (2SV). As a result of this effort, we have seen a 50% decrease in accounts being compromised.

Немного теории

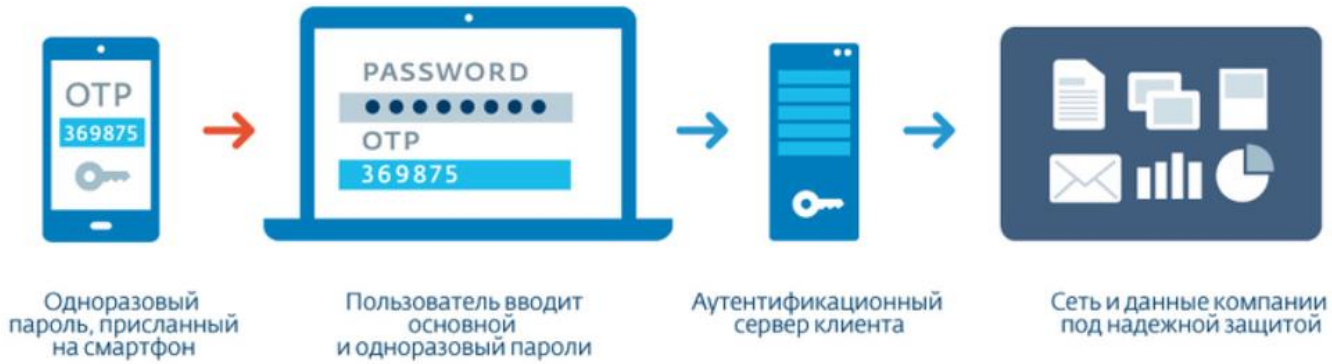
Способы аутентификации, на которых основан метод 2FA:

- пользователь что-то знает
- пользователь обладает уникальными чертами, которые можно оцифровать и сравнить
- пользователь что-то имеет

Первый метод встречается при восстановлении паролей по контрольным вопросам.

Второй способ чаще применяется для защиты данных на мобильных гаджетах и для авторизации клиентских приложений на серверах.

Третий способ – чаще всего это SMS или PUSH с проверочными кодами, генерируемыми по технологии OTP. Код приходит каждый раз разный и может генерироваться на другом устройстве пользователя (аппаратный токен, webPass, смартфон и т.п.)



Способы проверки подлинности с использованием 2FA

Аппаратные токены

SMS-сообщения

Push-уведомления

Проверка подлинности с помощью голосовой связи

Биометрия

Необходимость 2FA

Необходимость 2FA

- В начале 2014 года Федеральная служба по техническому и экспортному контролю (ФСТЭК) утвердила методический документ о мерах защиты информации в государственных информационных системах. Документ прояснил многие аспекты, касающихся организационных и технических мер защиты информации, принимаемых в государственных информационных системах, в соответствии с утверждённым приказом ФСТЭК России от 11 февраля 2013 г. No17.
- ФСТЭК настоятельно рекомендует полностью отказаться от привычной аутентификации на основе статических паролей для всех пользователей без исключения и перейти к более надежной многофакторной аутентификации. Обязательными требованиями для многофакторной аутентификации является использование аппаратных аутентификаторов и механизма одноразовых паролей при удаленном и локальном доступе.

Существующие виды и методы обхода двухфакторной аутентификации

1. Явный обход (недоступность облачного сервиса 2FA)
2. Компрометация сертификата подписи SAML (кража приватного ключа, используемого для подписи сертификатов SAML)
3. Фишинг с последующим MITM (инструменты могут быть разные - Muraena, NecroBrowser, реверс-прокси Modlishka, SEToolkit, PhaaS-сервисы и др.)
4. Эксплуатация разрешенных исключений (к примеру, POP3/SMTP)
5. Трояны
6. MFA bombing или «атака на усталость от MFA» (MFA fatigue attack) Комбо с социальной инженерией

Явный обход (недоступность облачного сервиса 2FA)

В некоторых облачных системах двухфакторной аутентификации имеются настройки, позволяющие войти в целевую систему без второго фактора, если сервис недоступен.

Вход без второго фактора вообще-то легитимный метод, который может разрешить ваш администратор. Называется bypass.

При внедрении и настройке своей системы необходимо обязательно проверять как настроен bypass.

Компрометация сертификата подписи SAML

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

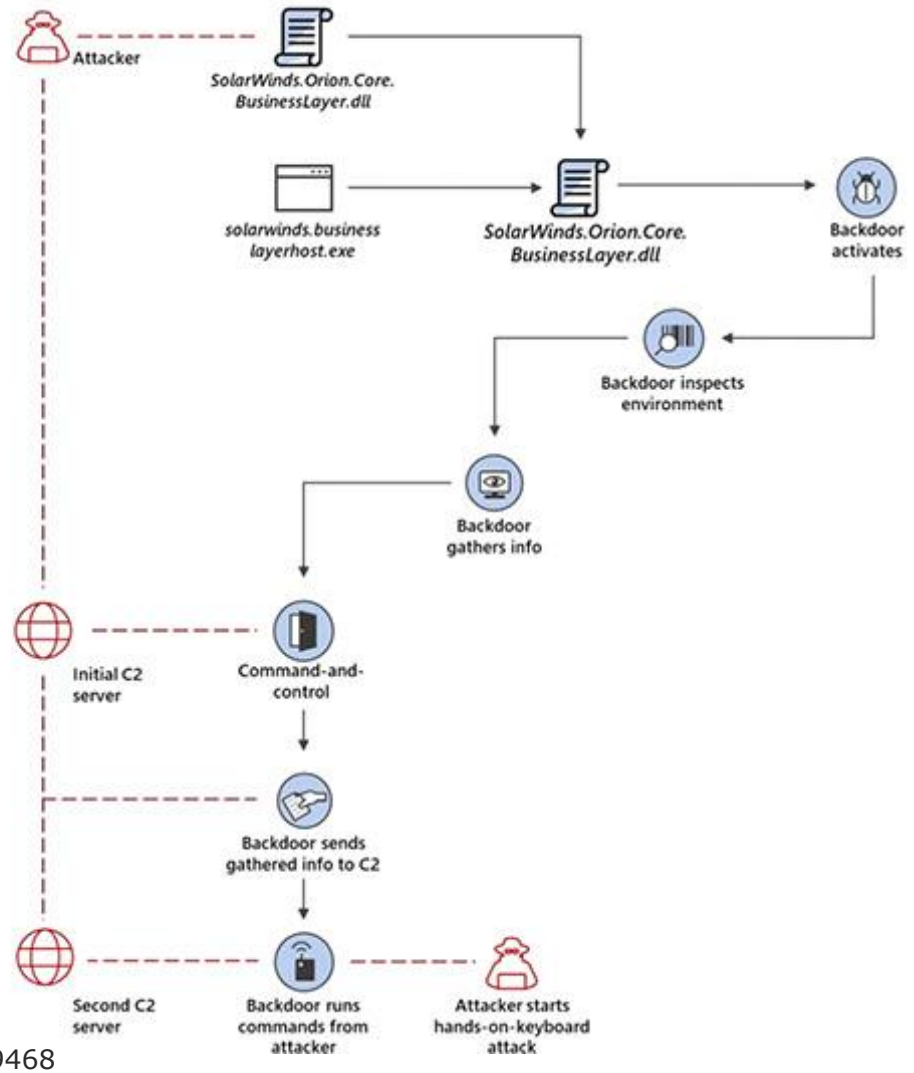
DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



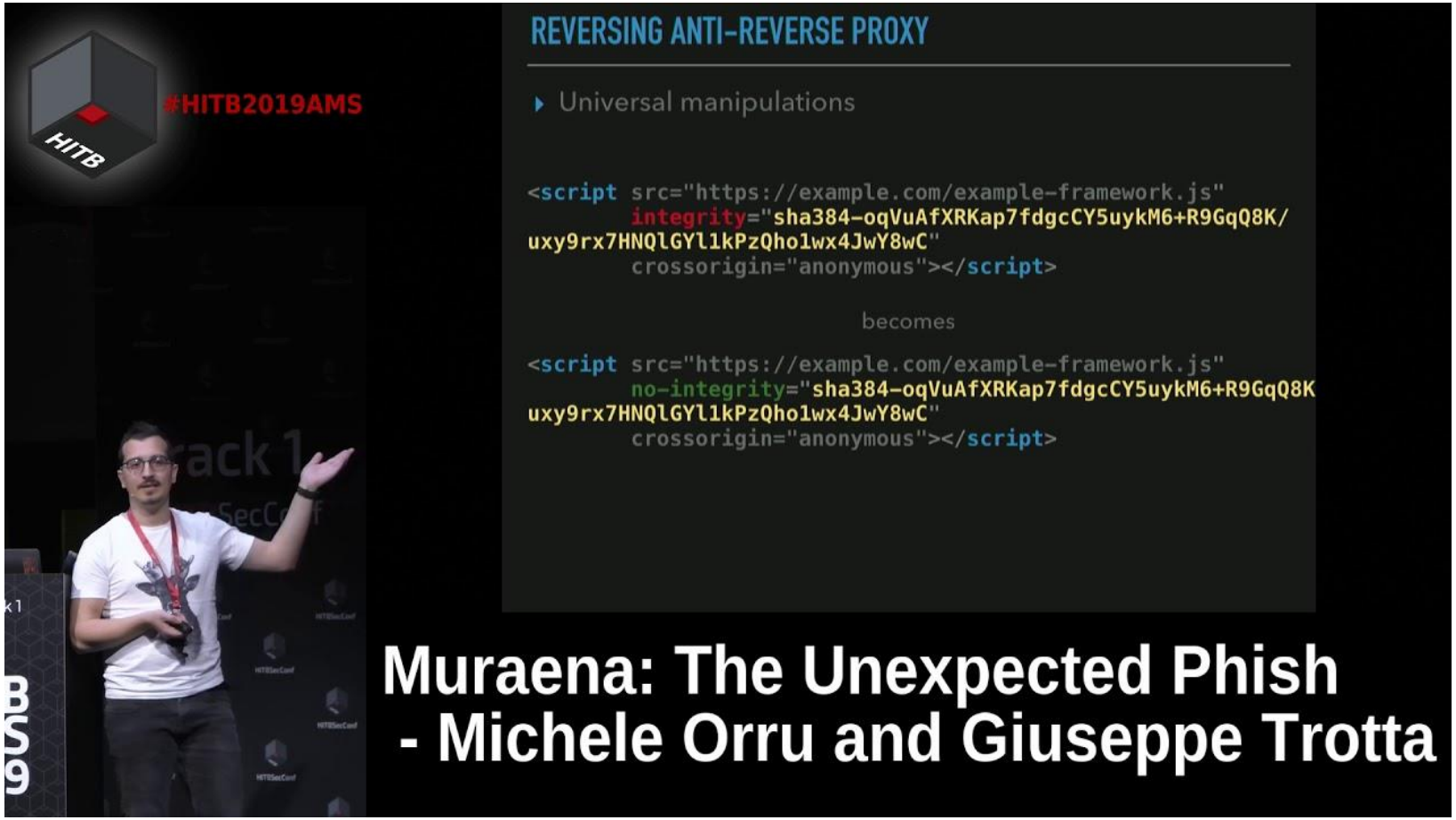
Источник: https://www.anti-malware.ru/news/2022-09-05-114534/39468

Фишинг с последующим MITM

Если нет проверки происхождения HTTP трафика и ключ 2FA отправляется через Интернет, фишинг может выполняться почти прозрачно посредством MiTM с использованием обратного прокси-сервера.

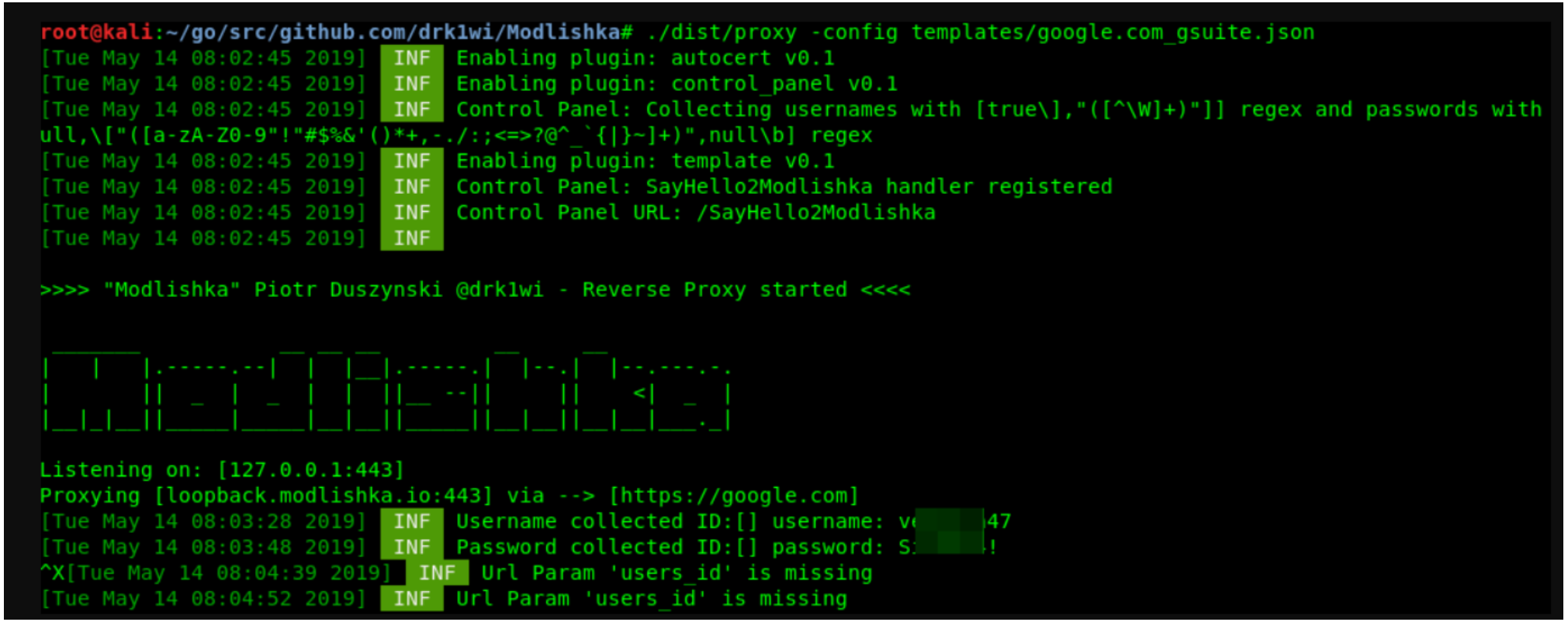
Фишинг с последующим MITM

- Muraena & Necrobrowser



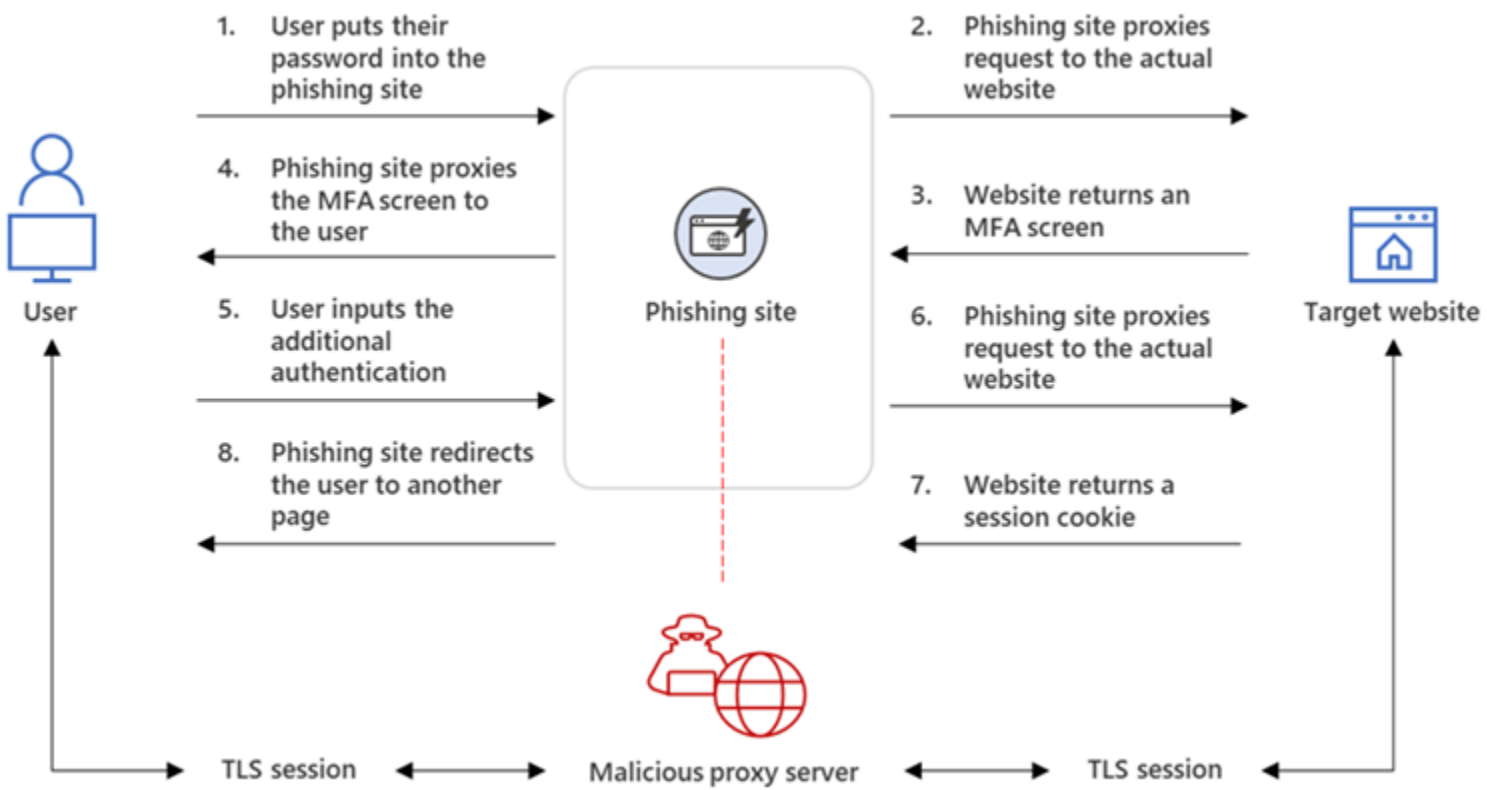
Фишинг с последующим MITM

- реверс-прокси Modlishka



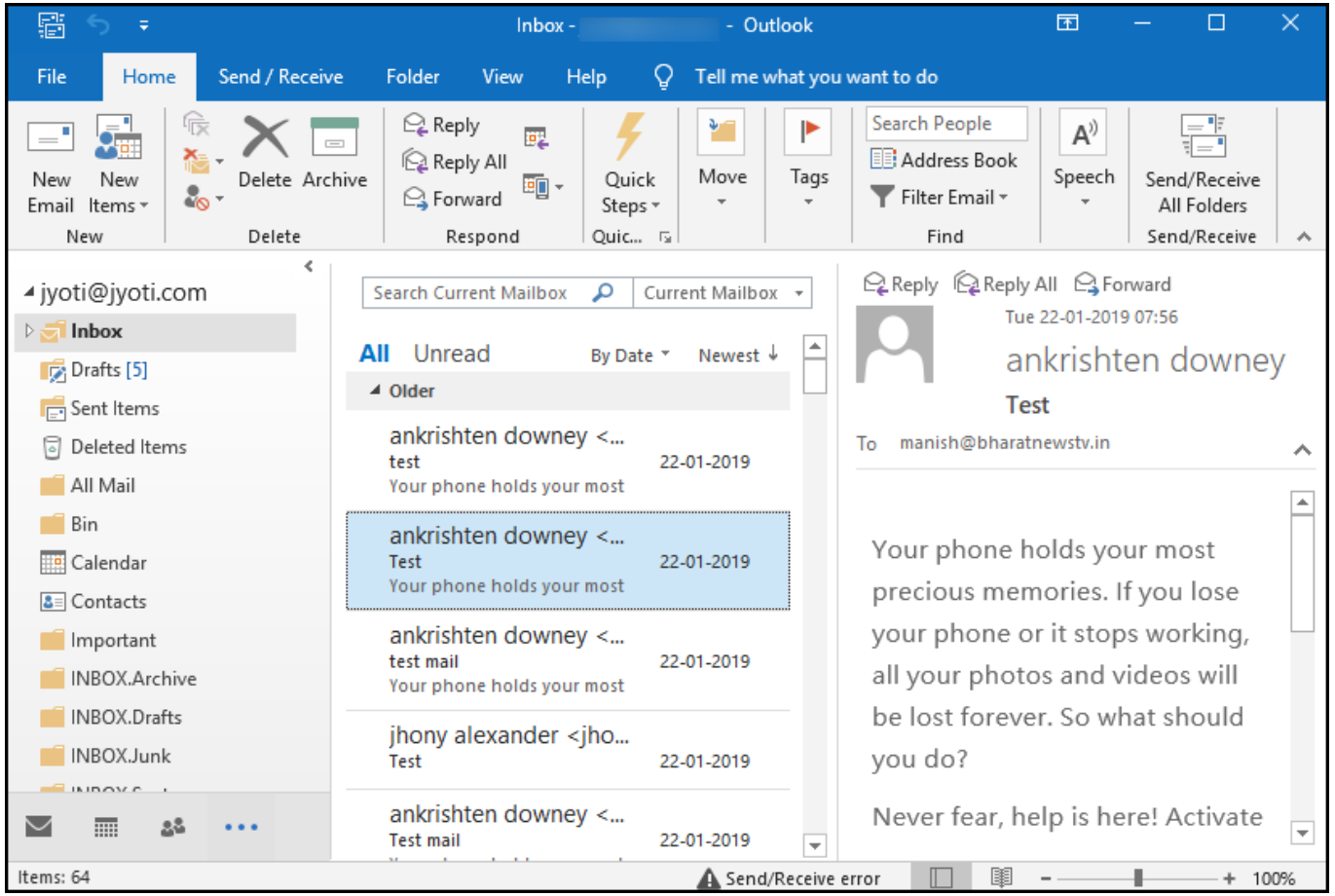
Фишинг с последующим MITM

- PhaaS – сервисы



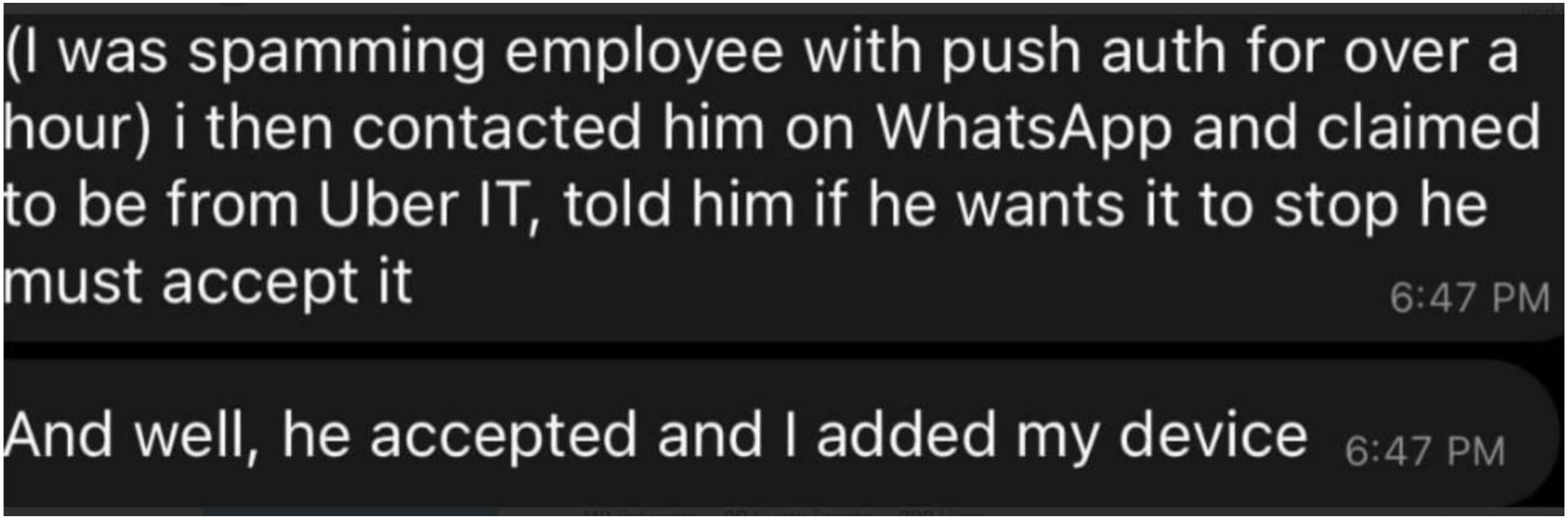
Источник: https://www.anti-malware.ru/news/2022-09-05-114534/39468

Эксплуатация разрешенных исключений (к примеру, POP3/SMTP)



Трояны

MFA bombing


(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it
6:47 PM
And well, he accepted and I added my device
6:47 PM

Комбо с социальной инженерией

Что будет завтра?

- Нас заставляют использовать современное решение по многофакторной аутентификации (MFA), неподверженное фишингу или атакам «человек посередине»: к примеру токены FIDO2 или решения на базе WebAuthn.
- Дополнительный фактор – биометрия?
- Вход без паролей по адресу электронной почты? Доп. Фактор будет приходить по этому адресу?

Итоги

Необходимо, но недостаточно

!Только внимание, ответственность и хранение яиц в разных корзинах защитит вас в полной мере!

Для передачи второго фактора:

не используйте голосовые сообщения

не используйте СМС

не юзайте HTTP

Берегите себя!