SOC FORUM 2023

Форензика в SOC. Опыт и кейсы 2023 года

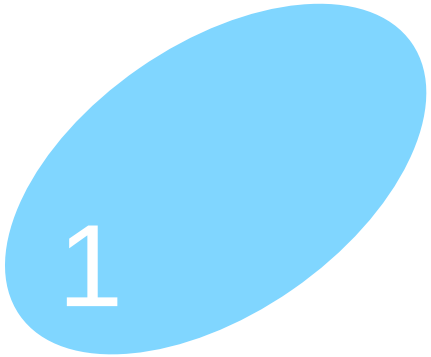
SOC FORUM 2023

Артем Семагин,
ведущий аналитик, группа киберкриминалистики,
[Certified specialist CHFI, FTK…etc]

JET CSIRT
ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

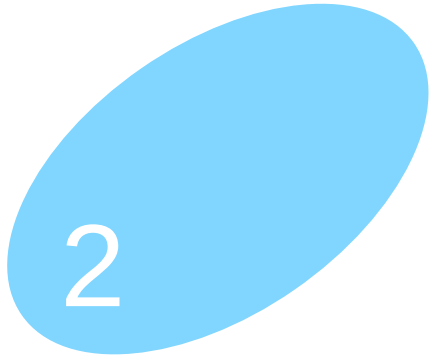
План доклада

SOC FORUM 2023



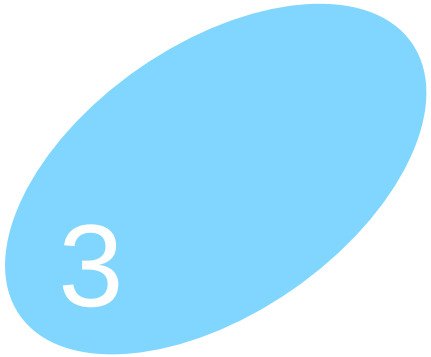
Forensics in SOC

Когда требуется детальное расследование и анализ артефактов?



Примеры кейсов 2023 года

Разбор актуальных расследований и бесплатных инструментов



Рекомендации

Что делать-то?

Forensics in SOC: Когда применять

SOC FORUM 2023

Реагирование
и расследование

Восстановить данные,
последовательность действий

Оценить ущерб, установить
точку проникновения

Получить подробный профиль
атакующего

Подготовить
цифровые доказательства

Forensics in SOC: Что анализируем при расследовании?

SOC FORUM 2023

Base

Logs: Event logs, audit, СЗИ

+

Advanced

- Люди: администраторы, пользователи, менеджеры
- Процессы: информация о технической реализации процессов, а также информация о бизнес-процессах
- Triage Collection (артефакты): MFT, Amcache, Prefetch и др.
- Дампы: ОЗУ, сетевой трафик
- Образы (файловая система, удаленные данные)

SOC FORUM 2023

CASES: уж сколько раз твердили миру…

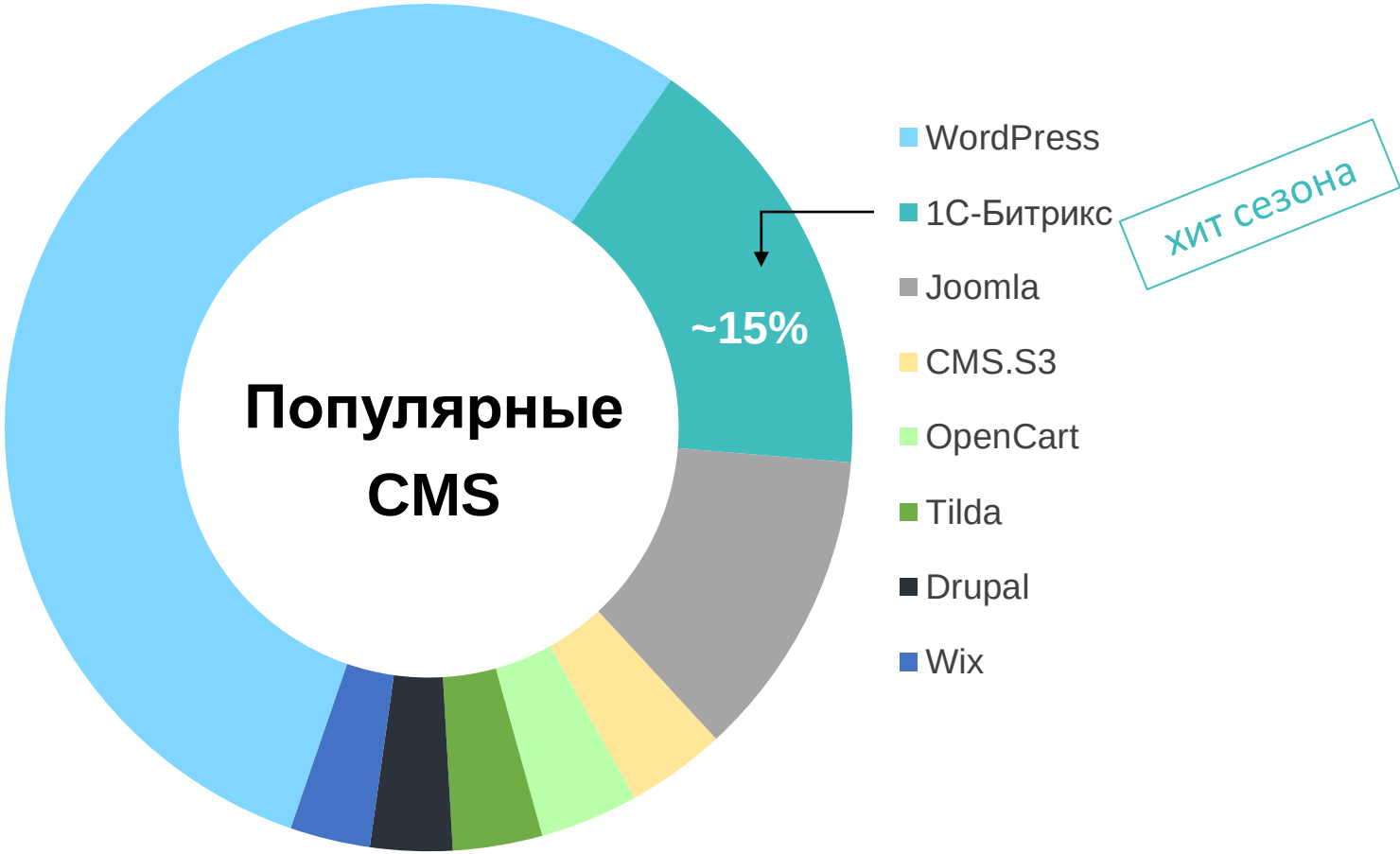
- Уязвимости на периметре
- Misconfigs
- Phishing

Атаки на web

SOC FORUM 2023

Цели:

- Кража данных
- Разведка, закрепление
- Репутационные потери



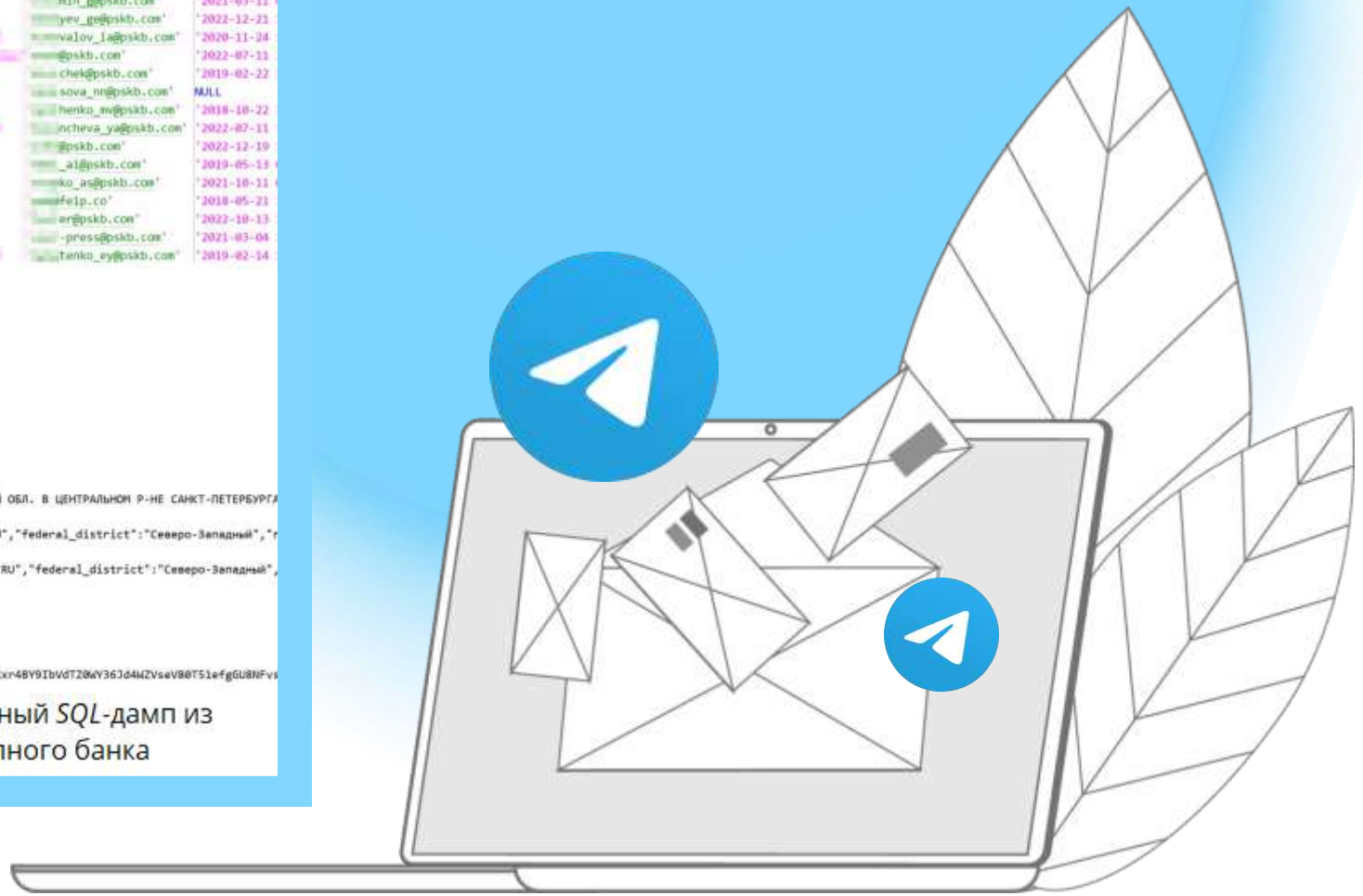
Утро добрым не бывает

SOC FORUM 2023

Утечки информации

[ajax_step] => send
[latinName] => ALEKSANDR
[lastName] =>
[firstName] => Александр
[secondName] =>
[birthDate] => 07.1971
[birthCityClient] => гор. Ленинград
[mobilePhone] => +7(911) 912
[email] =>
[passportId] => 4016
[passportDivisionCode] => 780-
[passportDate] => 21.07.2016
[passportIssued] => ТП №139 ОТДЕЛА УФМС РОССИИ ПО САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАДСКОЙ ОБЛ. В ЦЕНТРАЛЬНОМ Р-НЕ САНКТ-ПЕТЕРБУРГ
[address] => Ленинградская обл, Кировский р-н, г Отрадное, 16-я линия, д
[address_arr] => {"postal_code":"187331","country":"Россия","country_iso_code":"RU","federal_district":"Северо-Западный",
[address_1] => Ленинградская обл, Кировский р-н, г Отрадное, 16-я линия, д
[address_1_arr] => {"postal_code":"187331","country":"Россия","country_iso_code":"RU","federal_district":"Северо-Западный",
[cardTarif] => ТП Восточный + RUR
[cardType] => UnionPay
[isGenerate] => 1
[city_id] => 18
[office_id] => 7534
[g-recaptcha-response] => 03AL8dmwBZPzOyaYjCxw6TvZxuRI6djzKm-61stOyk4PoL_jsqQ3G9DRxr48Y9IbVdTZ0WY36Jd4WZVseV80T51efgGU8NFvs

В свободный доступ был выложен частичный *SQL*-дамп из CMS *«Bitrix»* предположительно сайта крупного банка



CASE #1: Атаки на web (Bitrix)

SOC FORUM 2023

Что видит жертва атаки?

Непубличная атака

- Сайты стали «тормозить»
- «Странные» запросы в логах
- Жалобы от клиентов и партнеров
- Нужно привлечение специалистов по расследованию инцидентов

CASE #1: Атаки на web (Bitrix)

SOC FORUM 2023

Что видит аналитик?

Смотрим access-логи: Обнаружены «странные» запросы к «xx.php» ->
$e=gzinflate(base64_decode('7b1re+K4sjD6uftXuD1ZY5gQgoFcC
CHdhNxI535POr0yxhhwMJjBJiTdk/e3n6qS5Bs2IT2zz7uf5xzWmo
3ocCqSuNwUBhof0p2nNcZP97…->**web shell**

Изучаем запросы с подозрительных IP

Строим Timeline-атаки

Ищем информацию TI, сканируем другие ресурсы

Получаем:

Установлены IP-адреса злоумышленников

Атакованы несколько ресурсов

Уязвимый модуль html_editor

CASE #1: Атаки на web (Bitrix)

Что видит аналитик?

Смотрим БД-логи относительно Timeline

Получаем:

Список скомпрометированных данных

Дата и время	Выгружено байт	Запрос к БД
30.MM.2023 12:25:24	2707003183	SELECT * FROM `api_reception_list`
30.MM.2023 12:34:10	2907005343	SELECT * FROM `api_users`
30.MM.2023 12:34:25	8370443123	SELECT * FROM `b_sales`
30.MM.2023 12:34:39	1250293603	SELECT * FROM `*********`
30.MM.2023 12:35:39	3412597688	SELECT * FROM `*********`

CASE #1: Атаки на web (Bitrix)

Результаты и отчет

SOC FORUM 2023

Блок реагирования

- Удаление web shell, проверка других закладок
- Обновление/закрытие уязвимого модуля
- Рекомендации по недопущению повторных инцидентов

Блок ответов на поставленные вопросы

- Проведено расследование, установлены причины инцидента и его ход
- Атрибуция злоумышленников
- Установлен объем скомпрометированных данных (~10 ГБ)

CASE #1: Атаки на web (Bitrix)

SOC FORUM 2023

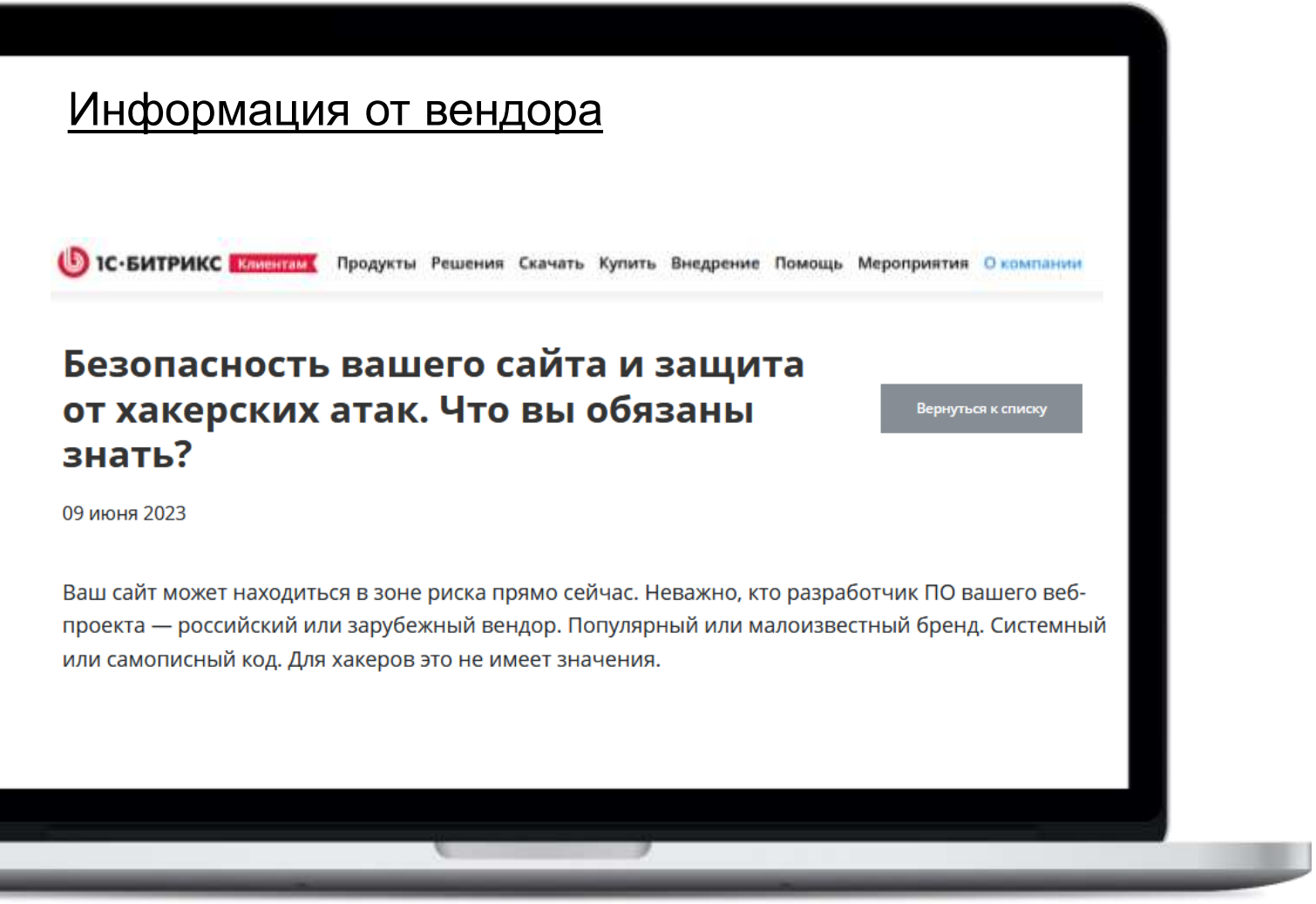
Что используем для проведения расследований?

- SIEM/LogManagment (журналы веб-сервера, журналы БД, срок хранения от 12 мес.)
- Сканеры (Bitrix, Thor, Loki и др.), Decoder CyberChef
- Triage collection (UAC, Unix collector, Velociraptor)
- Штатные утилиты (grep, find, sort и др.)

CASE #1: Атаки на web (Bitrix)

Что используем для проведения расследований

SOC FORUM 2023



Публикации и статьи

Информация о новых уязвимостях

BDU:2023-07457 CVE-2023-1714
BDU:2023-07458 CVE-2023-1720
BDU:2023-07459 CVE-2023-1719
BDU:2023-07460 CVE-2023-1718
BDU:2023-07461 CVE-2023-1717
BDU:2023-07462 CVE-2023-1716
BDU:2023-07463 CVE-2023-1715
BDU:2023-07464 CVE-2023-1713

CASE #2: Ransomware

SOC FORUM 2023

Цели:

- Шифрование инфраструктуры с целью получения выкупа
- Репутационные потери, повреждение данных

CASE #2: Ransomware

SOC FORUM 2023

Что видит жертва атаки?

- >10 зашифрованных серверов
- Жалобы клиентов и партнеров
- Остановка нормальной работы компании
- Удалены бэкапы критичных сервисов

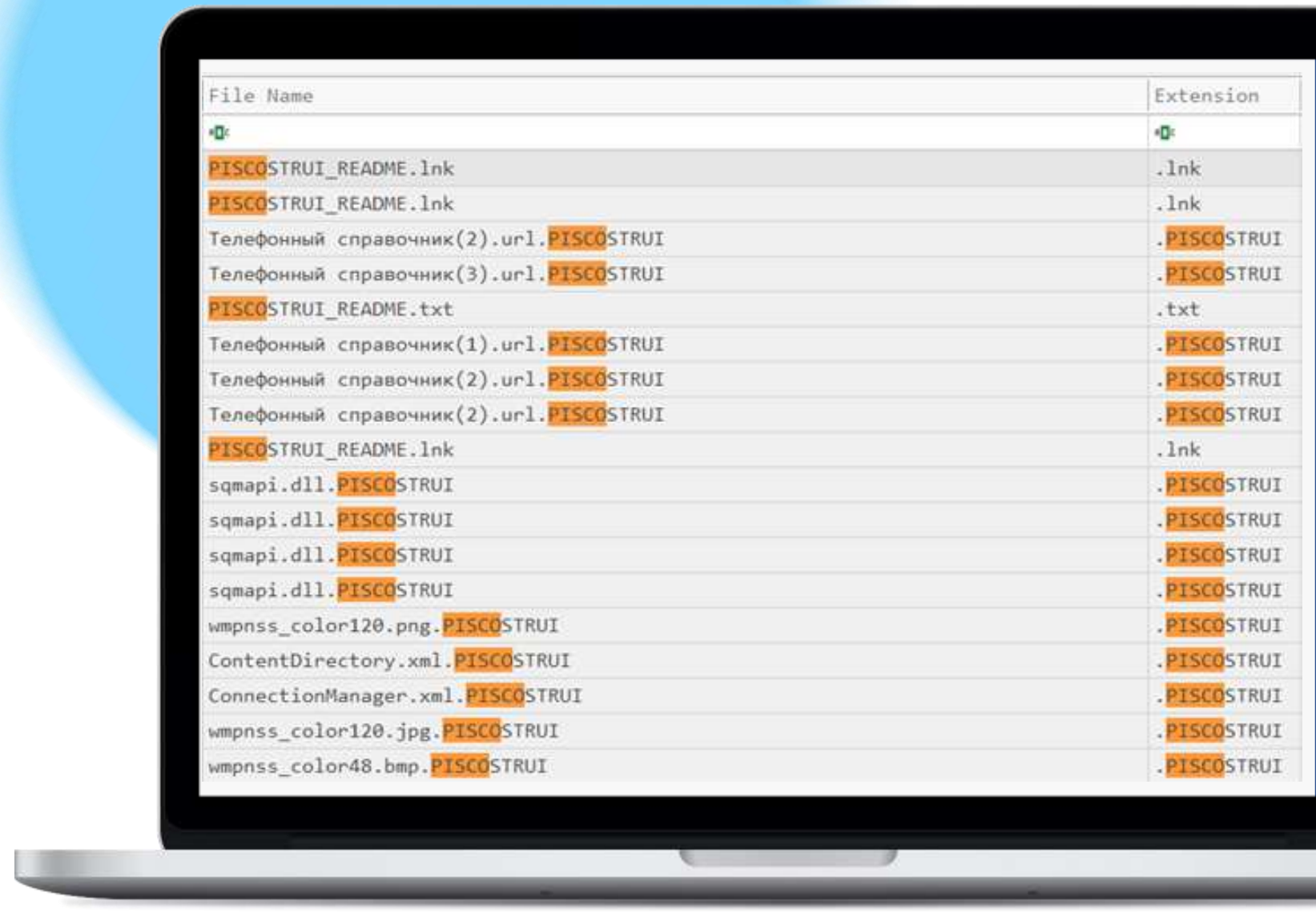
```
Hello, My Dear Friend !!!

ALL YOUR FILES HAVE BEEN ENCRYPTED DUE TO A SECURITY PROBLEM WITH YOUR PC.

If you want to restore them :
1) Send your unique id [alpha-numeric ID] and max 3 files for test decryption..

In subject line please write your decryption ID: [alpha-numeric ID]
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

FREE DECRYPTION AS A GUARANTEE!
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived),
and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

ATTENTION!!!
Do not rename encrypted files!
Do not try to decrypt your data using third party software, it may cause permanent data loss!
Decryption of your files with the help of third parties may cause increased price (they add their fee to our)
or you may become a victim of a scam!
```

CASE #2: Ransomware

SOC FORUM 2023

Что видит аналитик?

- Зашифрованы не все узлы
- Есть что анализировать, даже если логи очищены
- Неполнодисковое шифрование



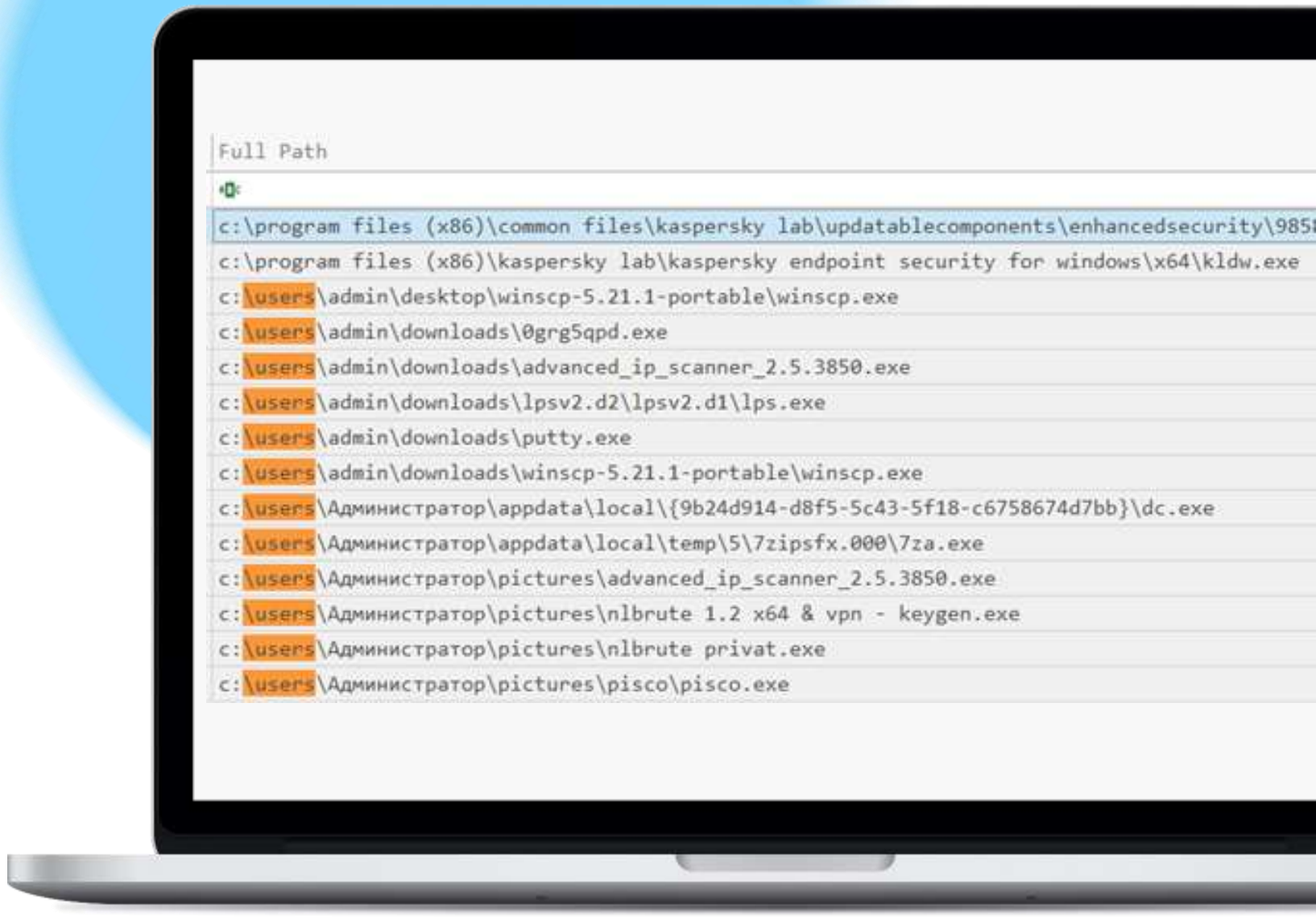
File Name	Extension
PISCOSTRUI_README.lnk	.lnk
PISCOSTRUI_README.lnk	.lnk
Телефонный справочник(2).url.PISCOSTRUI	.PISCOSTRUI
Телефонный справочник(3).url.PISCOSTRUI	.PISCOSTRUI
PISCOSTRUI_README.txt	.txt
Телефонный справочник(1).url.PISCOSTRUI	.PISCOSTRUI
Телефонный справочник(2).url.PISCOSTRUI	.PISCOSTRUI
Телефонный справочник(2).url.PISCOSTRUI	.PISCOSTRUI
PISCOSTRUI_README.lnk	.lnk
sqmapi.dll.PISCOSTRUI	.PISCOSTRUI
sqmapi.dll.PISCOSTRUI	.PISCOSTRUI
sqmapi.dll.PISCOSTRUI	.PISCOSTRUI
sqmapi.dll.PISCOSTRUI	.PISCOSTRUI
wmpnss_color120.png.PISCOSTRUI	.PISCOSTRUI
ContentDirectory.xml.PISCOSTRUI	.PISCOSTRUI
ConnectionManager.xml.PISCOSTRUI	.PISCOSTRUI
wmpnss_color120.jpg.PISCOSTRUI	.PISCOSTRUI
wmpnss_color48.bmp.PISCOSTRUI	.PISCOSTRUI

CASE #2: Ransomware

SOC FORUM 2023

Что видит аналитик?

- IP-scanner
- Сканер портов lps
- Winscp для передачи файлов
- NlBrute для горизонтального перемещения
- Шифровальщик семейства mimic/n3ww4v3



CASE #2: Ransomware

SOC FORUM 2023

Что видит аналитик?

- Выявлен ряд уязвимостей Exchange Health Checker, журнал ISS очищен
- Удаленные файлы в C:\root\ (ProxyNotShell?)

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Cre
No image data			■	■	—
	good.txt	.\Users\Администратор\Pictures	☐	☑	2023-0
	credentials.txt	.\Users\Администратор\Pictures	☐	☑	2023-0
	servers.txt	.\Users\Администратор\Pictures	☐	☑	2023-0
	pass.txt	.\Users\Администратор\Pictures	☐	☑	2023-0
	login.txt	.\Users\Администратор\Pictures	☐	☑	2023-0
	settings.ini	.\Users\Администратор\Pictures	☐	☑	2023-0
	key.txt	.\Users\Администратор\Pictures	☐	☑	2023-0
	NlBrute Privat.exe	.\Users\Администратор\Pictures	☐	☑	2023-0
	processhacker-3.0.4365-setup.exe	.\Users\Администратор\Pictures	☐	☑	2023-0
	Advanced_IP_Scanner_2.5.3850.exe	.\Users\Администратор\Pictures	☐	☑	2023-0
	pisco	.\Users\Администратор\Pictures	☑	☑	2023-0

Image Icon	Name	Parent Path	Is Dir	Is Deleted
No image data			■	■
	6Ci4rjFS9PVOhgepGvBp2OpR5akyLHchTR5t1jl0DXs.exe	.\root\Архив	☐	☐
	decr_payload.exe	.\root\Архив	☐	☑
	qNlIGnA1v2PzMhM-bzgACC3S52Y1tfmvrmdXAMQ230U.exe	.\root\Архив	☐	☑
	ulLdLgwmbCMzKcVVu27s2ANZASxn8mP5Zh6LHt-0AXg.exe	.\root\Архив	☐	☑

CASE #2: Ransomware
Результаты и отчет

SOC FORUM 2023

Блок реагирования

- Обновление Exchange
- Очистка инфраструктуры
- Рекомендации по недопущению повторных инцидентов (аудит и хардеринг)

Блок ответов на поставленные вопросы

- Атрибуция злоумышленников, IP-адреса, инструменты
- Установлена вся цепочка атаки, построили Timeline
- Декриптор на данный момент отсутствует

CASE #2: Ransomware

SOC FORUM 2023

Что используем для проведения расследований?

- SIEM/LogManagment (настроенный Windows Audit, Auditd для Linux)
- Triage collection (Kape, Magnet, Belkasoft, Velociraptor)
- Triage parser (Zimmerman Tools)
- Сканеры (Thor, Loki и др.)
- PowerShell скрипты, в том числе Microsoft Health Checker

CASE #2: Ransomware

SOC FORUM 2023

Что используем для проведения расследований?

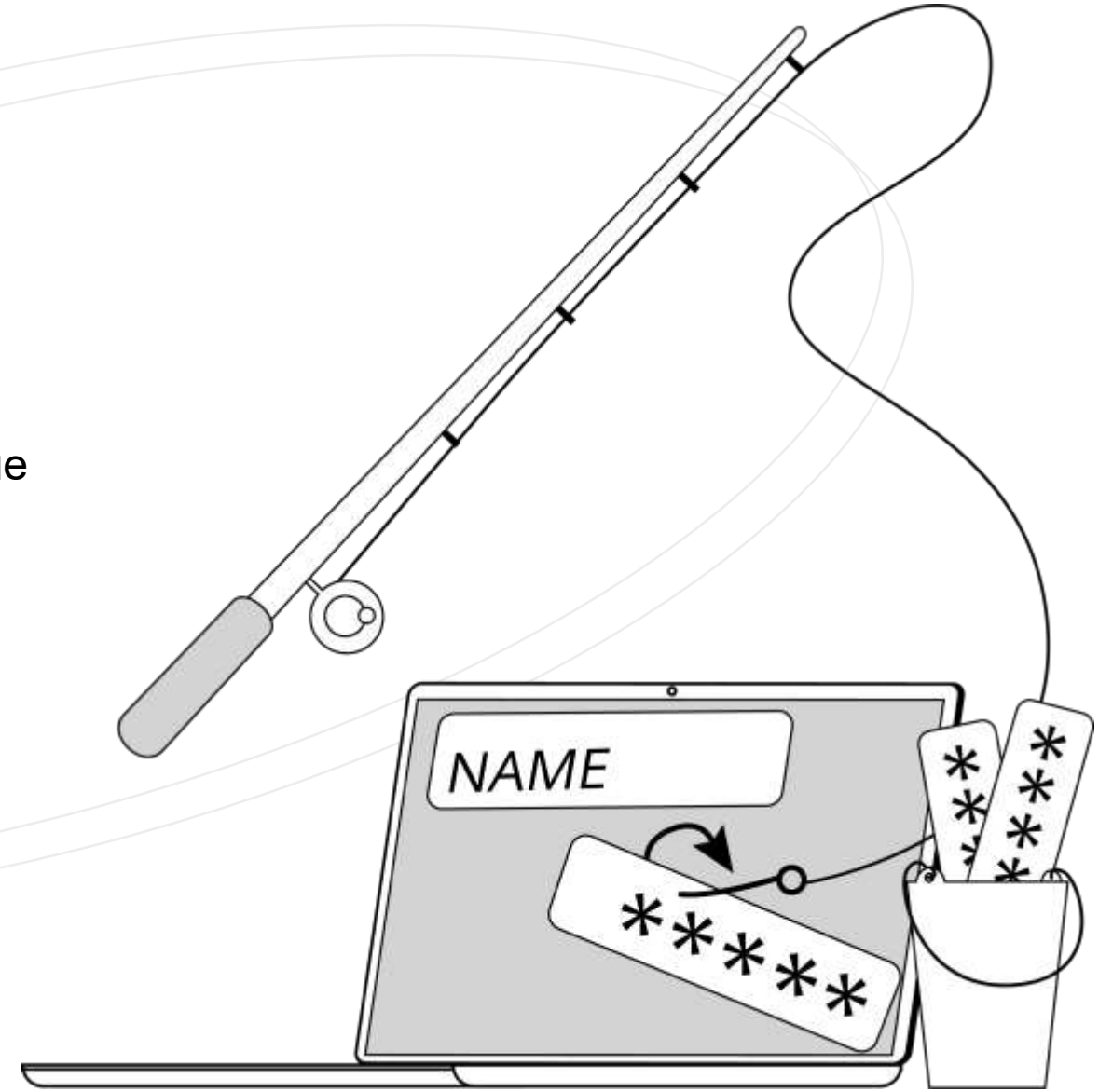
- Отчеты от вендоров и исследователей
- TI-базы
- Проекты и форумы No More Ransom

CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Цели:

- Финансово мотивированные группы
- Разведка и кража данных
- Репутационные потери



CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что видит жертва атаки?

- Финансовые потери XX млн руб.
- Жалобы от поставщиков
- Приостановка бизнес- процессов
- Нужно привлечение специалистов по расследованию инцидентов

CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что видит аналитик?

- В копии писем менеджера появляется поддельный почтовый домен

  например: @consulting.com
  и @consuiting.com

- Проверка гипотезы о взломе почтового ящика менеджера

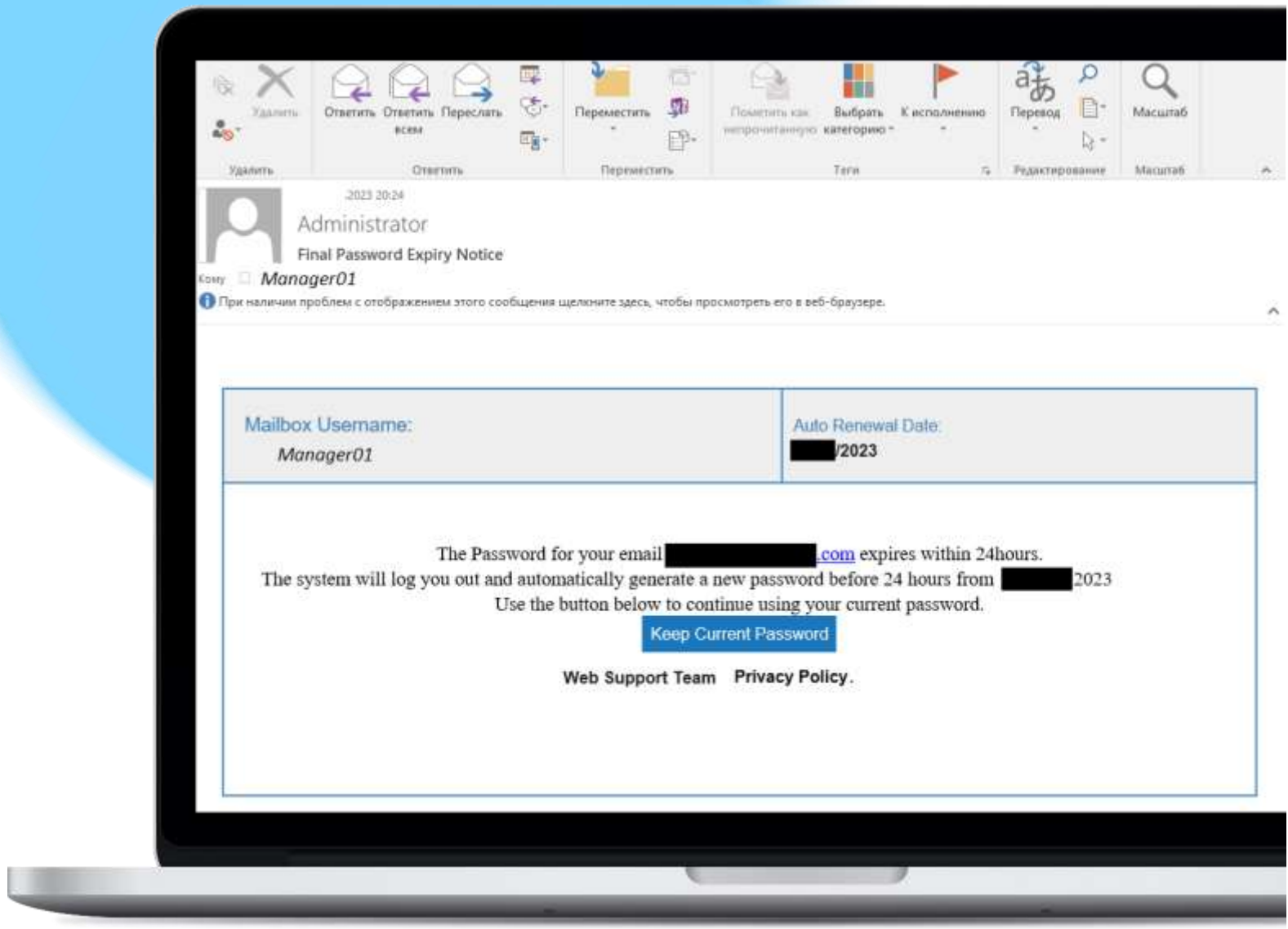
- Ищем письма с «высокой» важностью, нетипичное время отправки, подозрительные отправители, массовые рассылки

CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что видит аналитик?

- Хорошо подготовленное письмо, нет опечаток и явных фейлов
- Похожие письма приходили ранее
- Детектировать можно только по техническим заголовкам

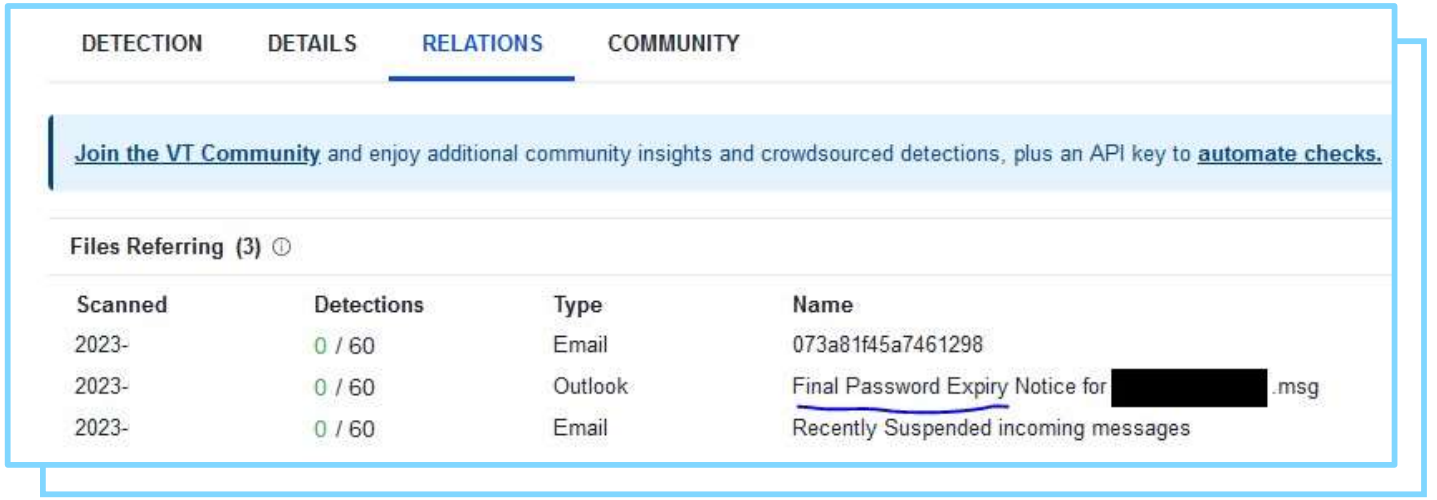


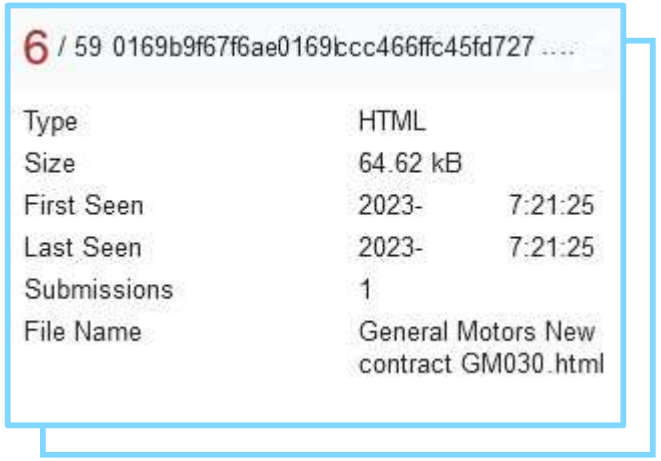
CASE #3: Phishing (BEC-атака)

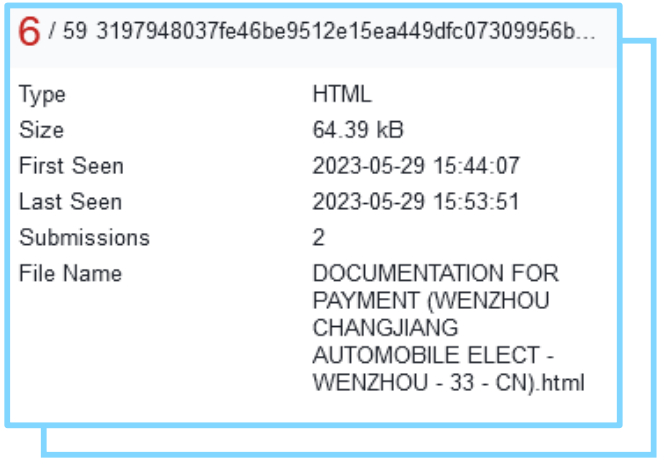
SOC FORUM 2023

Что видит аналитик?

- Подделан технический заголовок, письмо отправлено с недавно зарегистрированного домена
- Ссылка типа IPFS (InterPlanetary File System) сейчас недоступна
- Анализируем TI





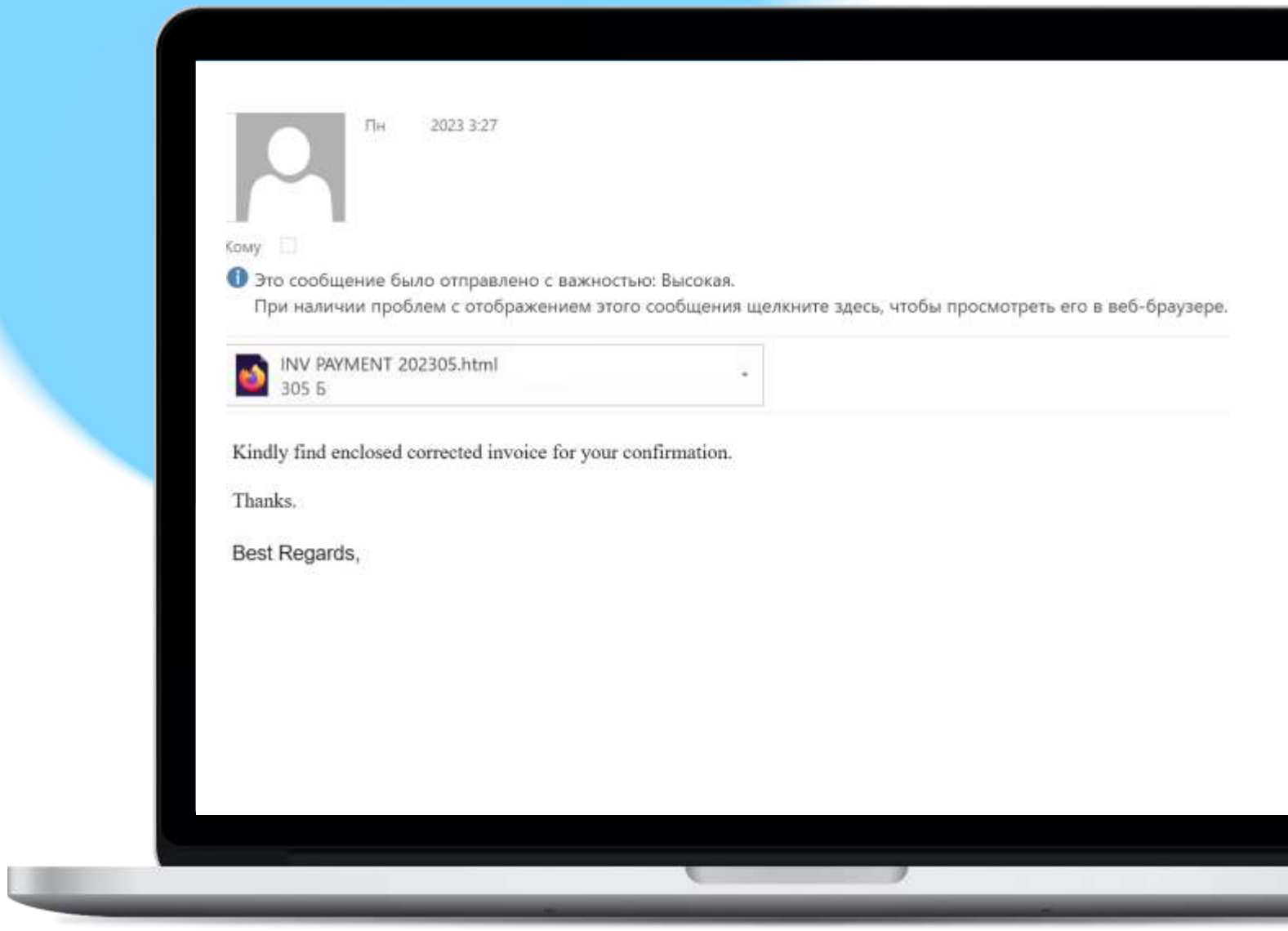


CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что видит аналитик?

- Изучение бизнес- процесса
- Дополнительный Spear Phishing
- Внедрение, использование бизнес- процесса для реализации атаки

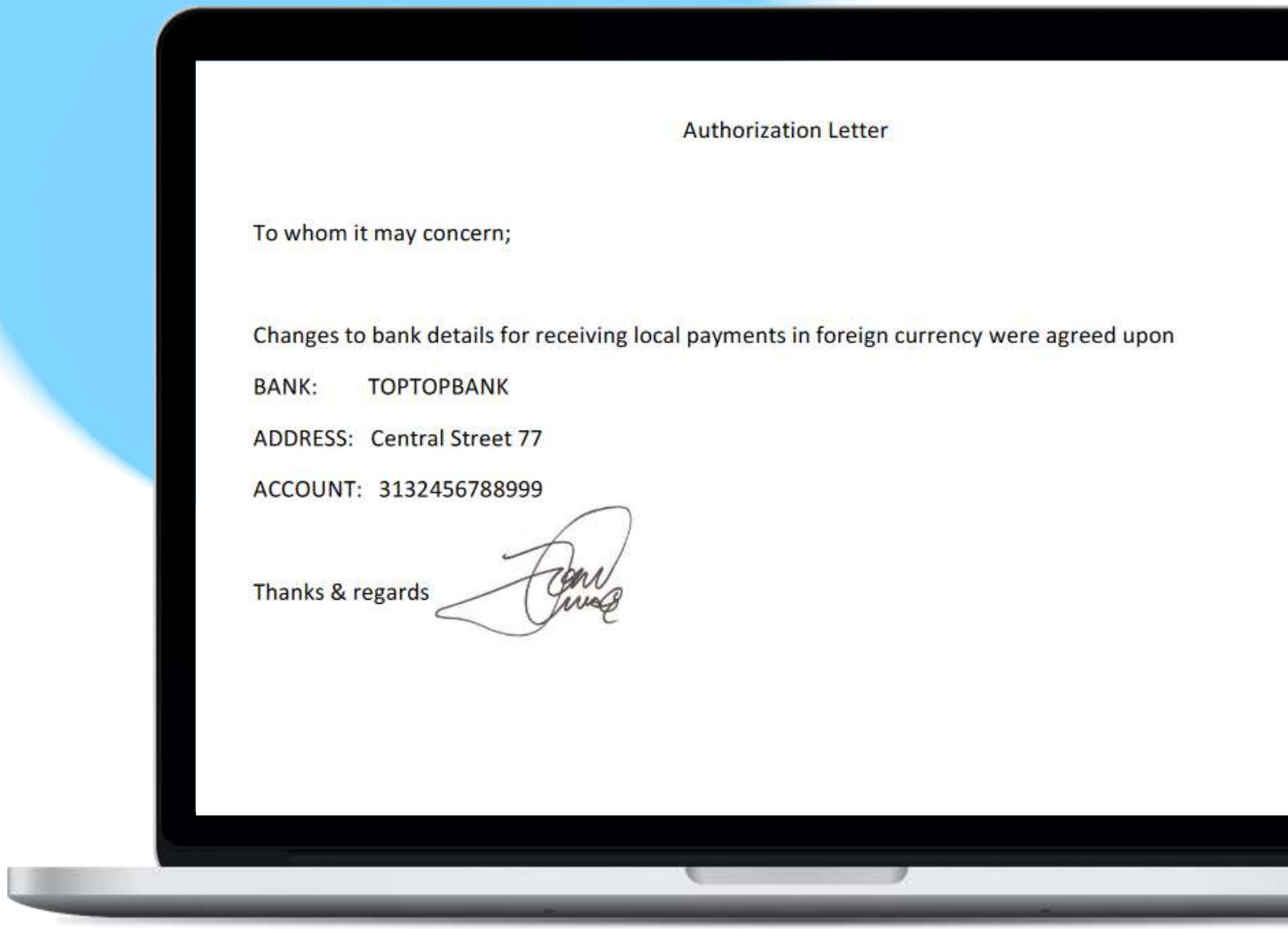


CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что видит аналитик?

- The payment that is attached has not been accepted by our bank...
- Не беда, подделаем PDF

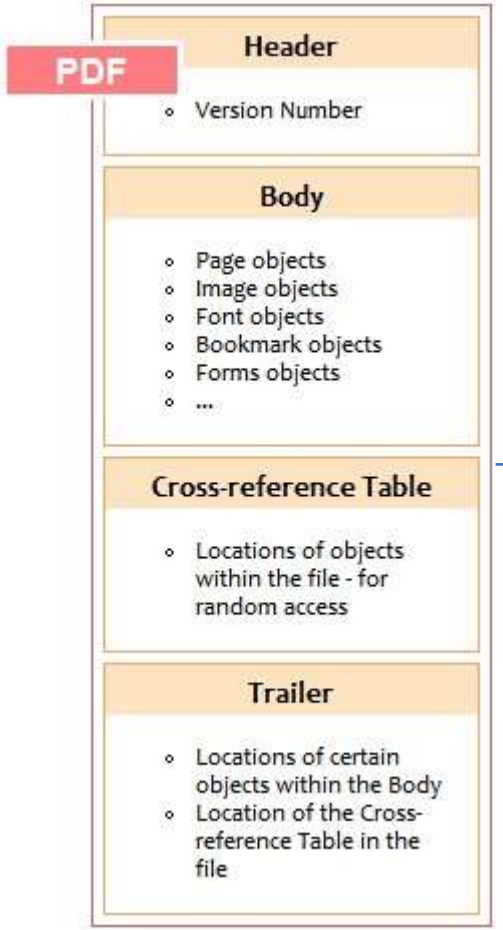


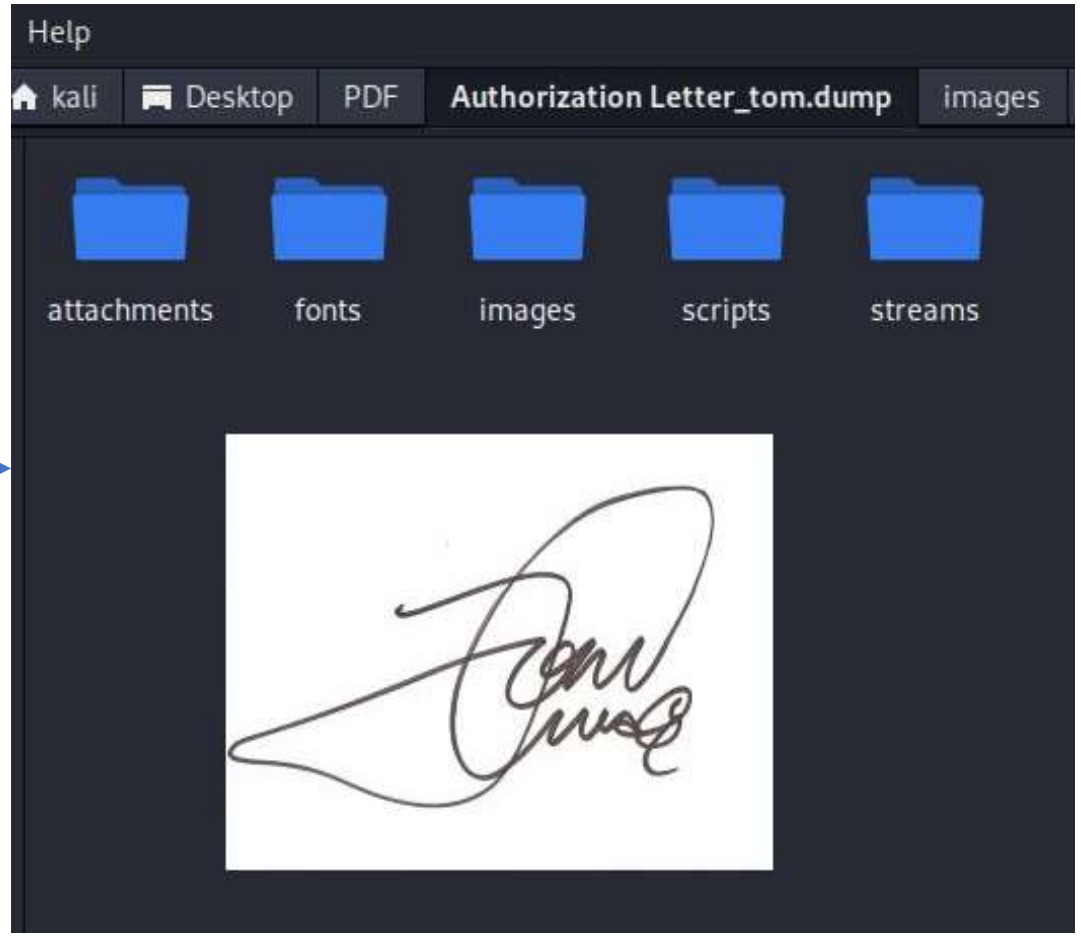
CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что видит аналитик?

- Разбираем PDF





PDFextract

CASE #3: Phishing (BEC-атака)
Результаты, инструменты для анализа

SOC FORUM 2023

Блок реагирования

- **Рекомендация: обращение в правоохранительные органы и финансовую организацию (частично удалось вернуть деньги)**
- Аудит и хардеринг ИТ-инфраструктуры (прежде всего Exchange)
- Изменения в бизнес- процессе

Блок ответов на поставленные вопросы

- Установлена цепочка атаки
- Установлены технические признаки подделки документа
- IP-адреса и инструменты злоумышленников

CASE #3: Phishing (BEC-атака)

SOC FORUM 2023

Что используем для проведения расследований?

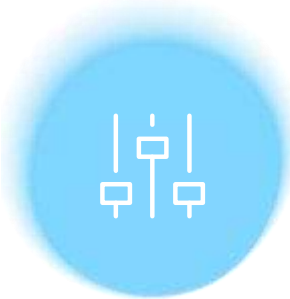
- Exchange Online – встроенные механизмы логирования и eDiscovery-модуль
- TI-базы и открытые источники (MxToolbox, Whois и др.)
- Текстовый редактор для анализа технических заголовков (Sublime Email Header Plugin)
- PDF analyzer (pdf parser, oletools и др.)

Рекомендации

SOC FORUM 2023

НЕ ПАНИКОВАТЬ

Использовать план
по реагированию



ИЗОЛИРОВАТЬ АТАКОВАННЫЕ СИСТЕМЫ НА УРОВНЕ СЕТИ

Приостановить бизнес-
процессы

НЕ ВЫКЛЮЧАТЬ АТАКОВАННЫЕ СЕРВЕРЫ И СИСТЕМЫ

Иначе данные будут утеряны
(многое хранится только в оперативке)

ПРИВЛЕЧЬ КОМПЕТЕНТНЫХ СПЕЦИАЛИСТОВ

В ПЛАНЕ ПО РЕАГИРОВАНИЮ УЧИТЫВАТЬ ПРЕСС-РЕЛИЗЫ ОТ КОМПАНИИ

JET CSIRT

ЦЕНТР МОНИТОРИНГА
И РЕАГИРОВАНИЯ
НА ИНЦИДЕНТЫ ИБ

Артем Семагин
ведущий аналитик, группа киберкриминалистики
«Инфосистемы Джет»

SOC FORUM 2023