

# Форензика в SOC. Опыт и кейсы 2023 года



Арте́м Сема́гин,  
ведущий аналитик, группа киберкриминалистики,  
[Certified specialist CHFI, FTK...etc]

1

## Forensics in SOC

Когда требуется детальное расследование и анализ артефактов?

2

## Примеры кейсов 2023 года

Разбор актуальных расследований и бесплатных инструментов

3

## Рекомендации

Что делать-то?

# Forensics in SOC: Когда применять



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?

## 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

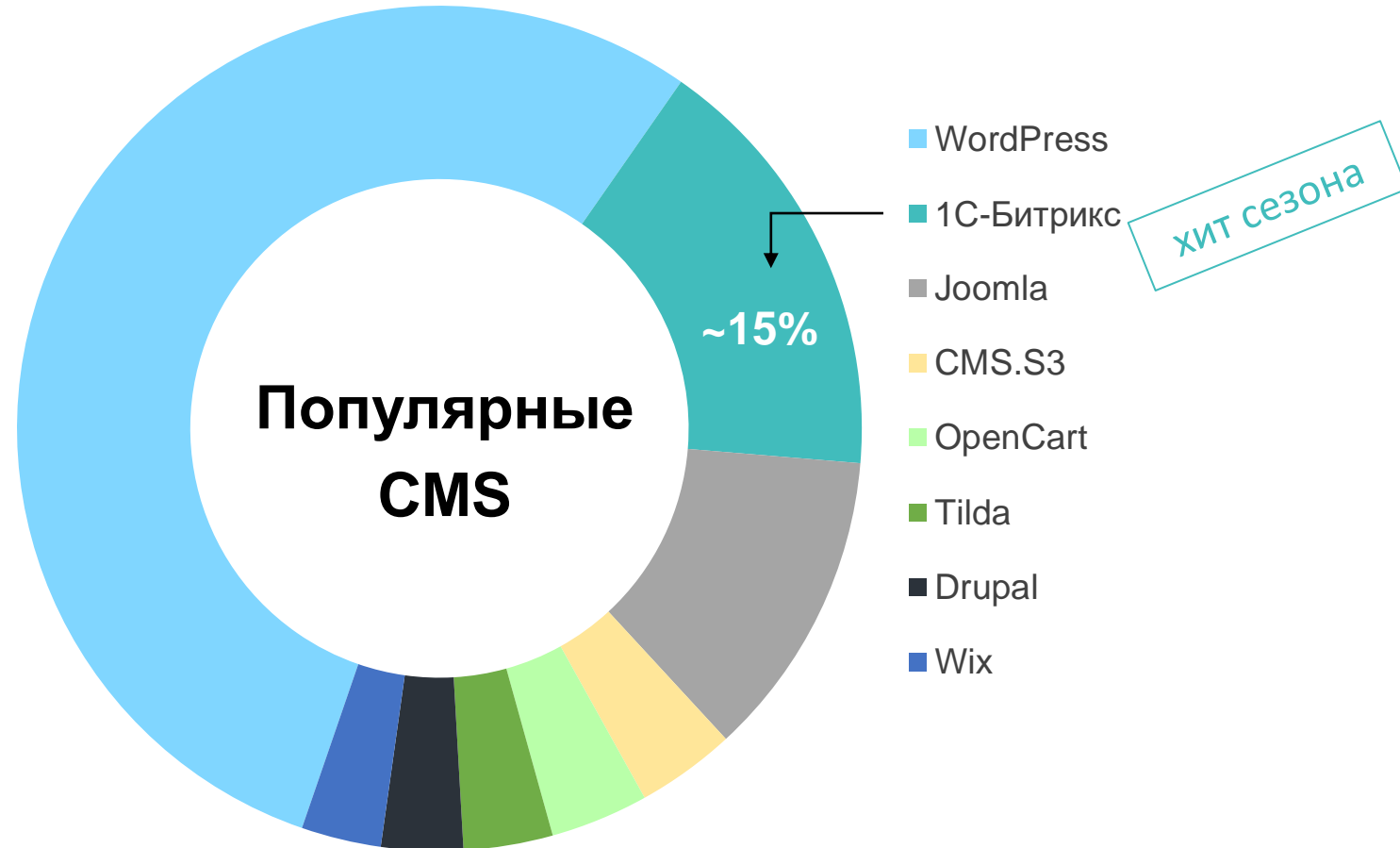
Образы (файловая система, удаленные данные)

# CASES: уж сколько раз твердили миру...

- Уязвимости на периметре
- Misconfigs
- Phishing

## Цели:

- ✦ Кража данных
- ✦ Разведка, закрепление
- ✦ Репутационные потери



### Утечки информации

u_a1@pskb.com	"UKp0QEV15d8"UG5Ueki"Y"	"Студия	vila-s@3dots.ru"	"2022-12-27"
g@pskb.com	"8X\X6-Tv7e"nzliqZDE"N"	"Анастасия	nova_a1@pskb.com"	"2017-12-29"
v_c_ia"	"n859p2IE5b5"dsvzv3Z"N"	"Источни	rn_n_g@pskb.com"	"2021-03-11"
b.com"	"Ur-10o}6768"ez7hWzI"Y"	"Георгий	yeu_ge@pskb.com"	"2022-12-21"
@pskb.com"	"4c_nHu-978"6d86zbn"Y"	"Игорь	va1ov_la@pskb.com"	"2020-11-24"
c_rn@pskb.com"	"8e4vuoTut30"E3HkUdF"Y"	"Наталья	@pskb.com"	"2022-07-11"
o_ev@pskb.com"	"3815Zhq1648"9WOGDfN"Y"	"Галина	chek@pskb.com"	"2019-02-22"
iva_ya@pskb.com"	"Qz8K6894d3"8VE1x8E"Y"	"Наталья	sova_n@pskb.com"	"NULL"
pskb.com"	"M9}5a15647"zou9FuI"Y"	"Маргарит	henko_ev@pskb.com"	"2018-10-22"
"	"6uQ754wP17a"CDW95d"Y"	"Ана	ncheva_ya@pskb.com"	"2022-07-11"
"	"T:6g}w9728"u18c9hd"Y"	"	@pskb.com"	"2022-12-19"
"	"qk836uv848"wt20vwd"Y"	"Артём	_a1@pskb.com"	"2019-05-13"
"	"b4*3pE}261d"UJNTSV"Y"	"Аранко А	ko_a@pskb.com"	"2021-10-11"
"	"u8yLRY72e"1GwtyP8"Y"	"Тестер	fe1p.co"	"2018-05-21"
"	"j7W\770}2f"6w3bsu"N"	"	er@pskb.com"	"2022-10-13"
"	"318Kv71adca"tgng7yI"Y"	"Евгения	press@pskb.com"	"2021-03-04"
"	"1a0iR14e834"vL3TQ1"N"	"	tenko_ev@pskb.com"	"2019-02-14"

```
[ajax_step] => send
[latInName] => ALEKSANDR
[lastName] =>
[firstName] => Александр
[secondName] =>
[birthDate] => 07.1971
[birthCityClient] => г. Ленинград
[mobilePhone] => +7(911) 912
[email] => @inkompro.ru
[passportId] => 4816
[passportDivisionCode] => 788
[passportDate] => 21.07.2016
[passportIssued] => ТП №139 ОТДЕЛА УМНС РОССИИ ПО САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАДСКОЙ ОБЛ. В ЦЕНТРАЛЬНОМ Р-НЕ САНКТ-ПЕТЕРБУРГА
[address] => Ленинградская обл, Кировский р-н, г Отрадное, 16-я линия, д
[address_err] => {"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_err] => {"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] => 83AL8dmsZPz0yWYjCw6T4vZxwRtEdj2Kk-61st0yKAPol_jsq3G9DRxv48Y9IbVd7Z6wV36JdMzVseV80T51efgU8HFv
```

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





## Что видит жертва атаки?

### Непубличная атака



Сайты стали  
«тормозить»



«Странные»  
запросы в логах



Жалобы от клиентов  
и партнеров



Нужно привлечение  
специалистов  
по расследованию  
инцидентов

#### Server Error

**500 - Internal server error.**

There is a problem with the resource you are looking for, and it cannot be displayed.

# CASE #1: Атаки на web (Bitrix)

## Что видит аналитик?



**Смотрим access-логи:** Обнаружены «странные» запросы к «xx.php» ->  
\$e=gzinflate(base64\_decode('7b1re+K4sjD6uftXuD1ZY5gQgoFcC  
CHdhNxl535POr0yxhhwMJjBJiTdk/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.ММ.2023 12:25:24	2707003183	SELECT * FROM `api_reception_list`
30.ММ.2023 12:34:10	2907005343	SELECT * FROM `api_users`
30.ММ.2023 12:34:25	8370443123	SELECT * FROM `b_sales`
30.ММ.2023 12:34:39	1250293603	SELECT * FROM `*****`
30.ММ.2023 12:35:39	3412597688	SELECT * FROM `*****`

# CASE #1: Атаки на web (Bitrix)

## Результаты и отчет

### 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)

## Что используем для проведения расследований?

✦ SIEM/LogManagement  
(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

### Информация от вендора

 **1С-БИТРИКС** Клиентам [Продукты](#) [Решения](#) [Скачать](#) [Купить](#) [Внедрение](#) [Помощь](#) [Мероприятия](#) [О компании](#)

### **Безопасность вашего сайта и защита от хакерских атак. Что вы обязаны знать?**

[Вернуться к списку](#)

09 июня 2023

Ваш сайт может находиться в зоне риска прямо сейчас. Неважно, кто разработчик ПО вашего веб-проекта — российский или зарубежный вендор. Популярный или малоизвестный бренд. Системный или самописный код. Для хакеров это не имеет значения.

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

## Цели:

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



## 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!
```



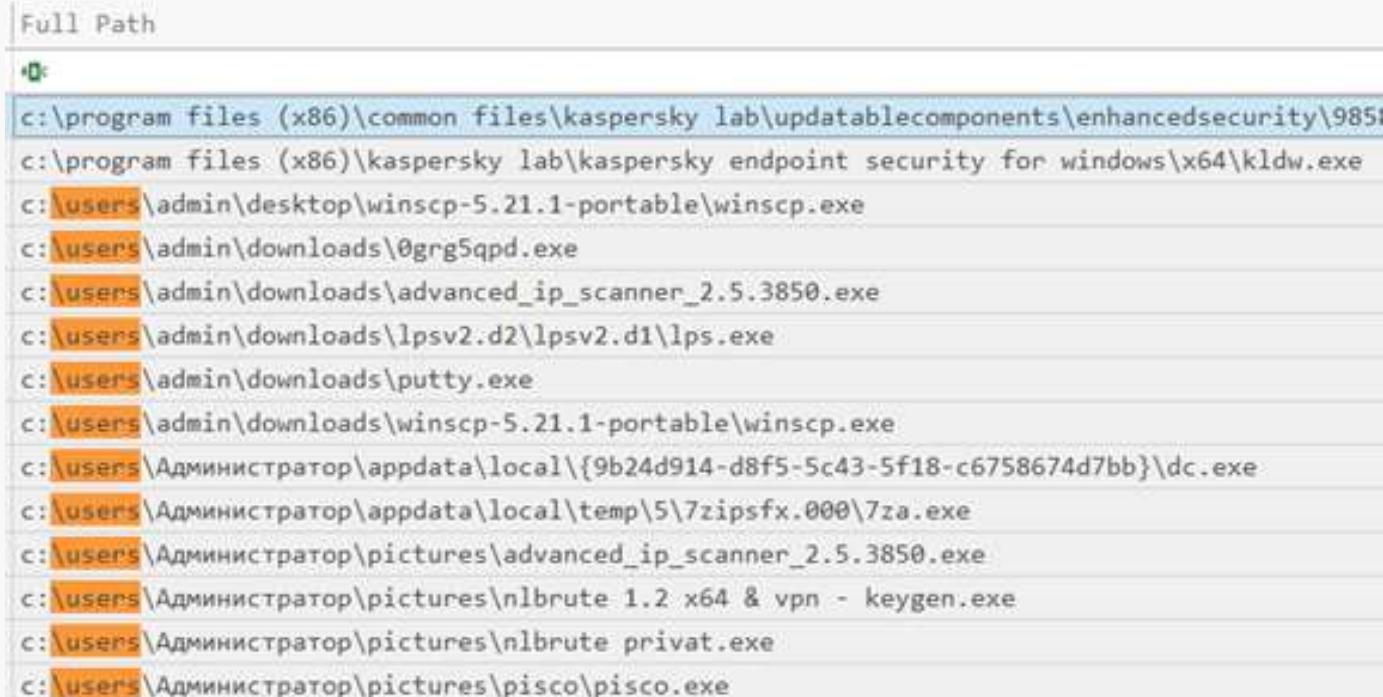
## Что видит аналитик?

- ✦ 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

## Что видит аналитик?

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



```
Full Path
c:\program files (x86)\common files\kaspersky lab\updatablecomponents\enhancedsecurity\985
c:\program files (x86)\kaspersky lab\kaspersky endpoint security for windows\x64\kldw.exe
c:\users\admin\desktop\winscp-5.21.1-portable\winscp.exe
c:\users\admin\downloads\0grg5qpd.exe
c:\users\admin\downloads\advanced_ip_scanner_2.5.3850.exe
c:\users\admin\downloads\lpsv2.d2\lpsv2.d1\lps.exe
c:\users\admin\downloads\putty.exe
c:\users\admin\downloads\winscp-5.21.1-portable\winscp.exe
c:\users\Администратор\appdata\local\{9b24d914-d8f5-5c43-5f18-c6758674d7bb}\dc.exe
c:\users\Администратор\appdata\local\temp\5\7zipsfx.000\7za.exe
c:\users\Администратор\pictures\advanced_ip_scanner_2.5.3850.exe
c:\users\Администратор\pictures\nlbrute 1.2 x64 & vpn - keygen.exe
c:\users\Администратор\pictures\nlbrute privat.exe
c:\users\Администратор\pictures\pisco\pisco.exe
```

# CASE #2: Ransomware

## 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	C:	C:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-
	good.txt	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	credentials.txt	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	servers.txt	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	pass.txt	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	login.txt	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	settings.ini	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	key.txt	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	NIBrute Privat.exe	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	processhacker-3.0.4365-setup.exe	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	Advanced_IP_Scanner_2.5.3850.exe	. \Users\Администратор\Pictures	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0
	pisco	. \Users\Администратор\Pictures	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2023-0

Image Icon	Name	Parent Path	Is Dir	Is Deleted
No image data	C:	C:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	6Ci4rjFS9PVOhgepGvBp2OpR5akyLHchTR5t1jl0DXs.exe	. \root\Архив	<input type="checkbox"/>	<input type="checkbox"/>
	decr_payload.exe	. \root\Архив	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	qNIIgNA1v2PzMhM-bzgACC3S52Y1tfmvrmdXAMQ230U.exe	. \root\Архив	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	ulLdLgwmbCMzKcVvu27s2ANZASxn8mP5Zh6LHt-0AXg.exe	. \root\Архив	<input type="checkbox"/>	<input checked="" type="checkbox"/>

# CASE #2: Ransomware

## Результаты и отчет

### 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

## Что используем для проведения расследований?

- ✦ SIEM/LogManagement  
(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



## Что используем для проведения расследований?



Отчеты от вендоров  
и исследователей



TI-базы



Проекты и форумы No More  
Ransom

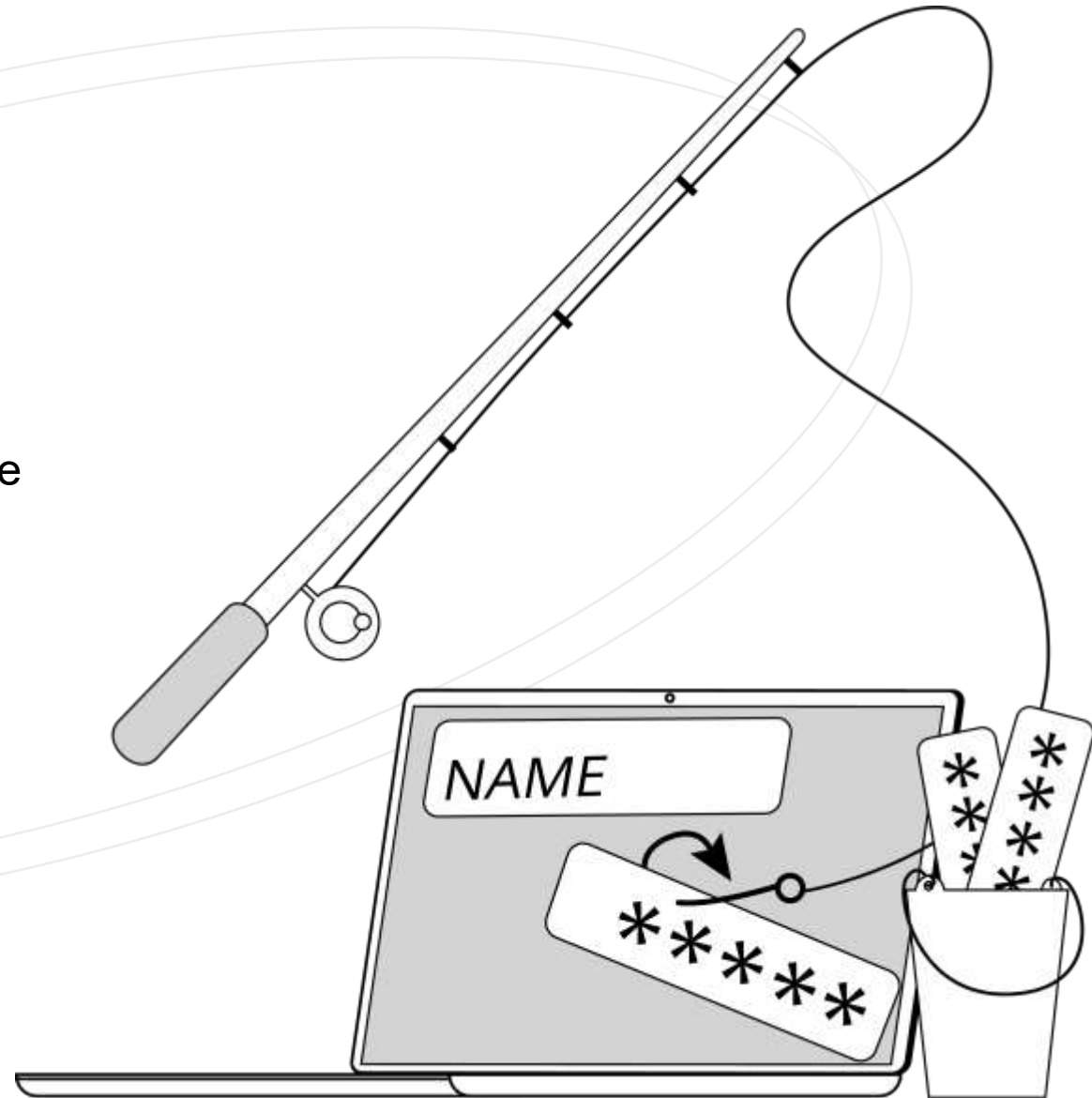




# CASE #3: Phishing (BEC-атака)

## Цели:

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



## Что видит жертва атаки?

✦ Финансовые  
потери XX млн руб.

✦ Жалобы  
от поставщиков

✦ Приостановка  
бизнес- процессов

✦ Нужно привлечение  
специалистов  
по расследованию  
инцидентов

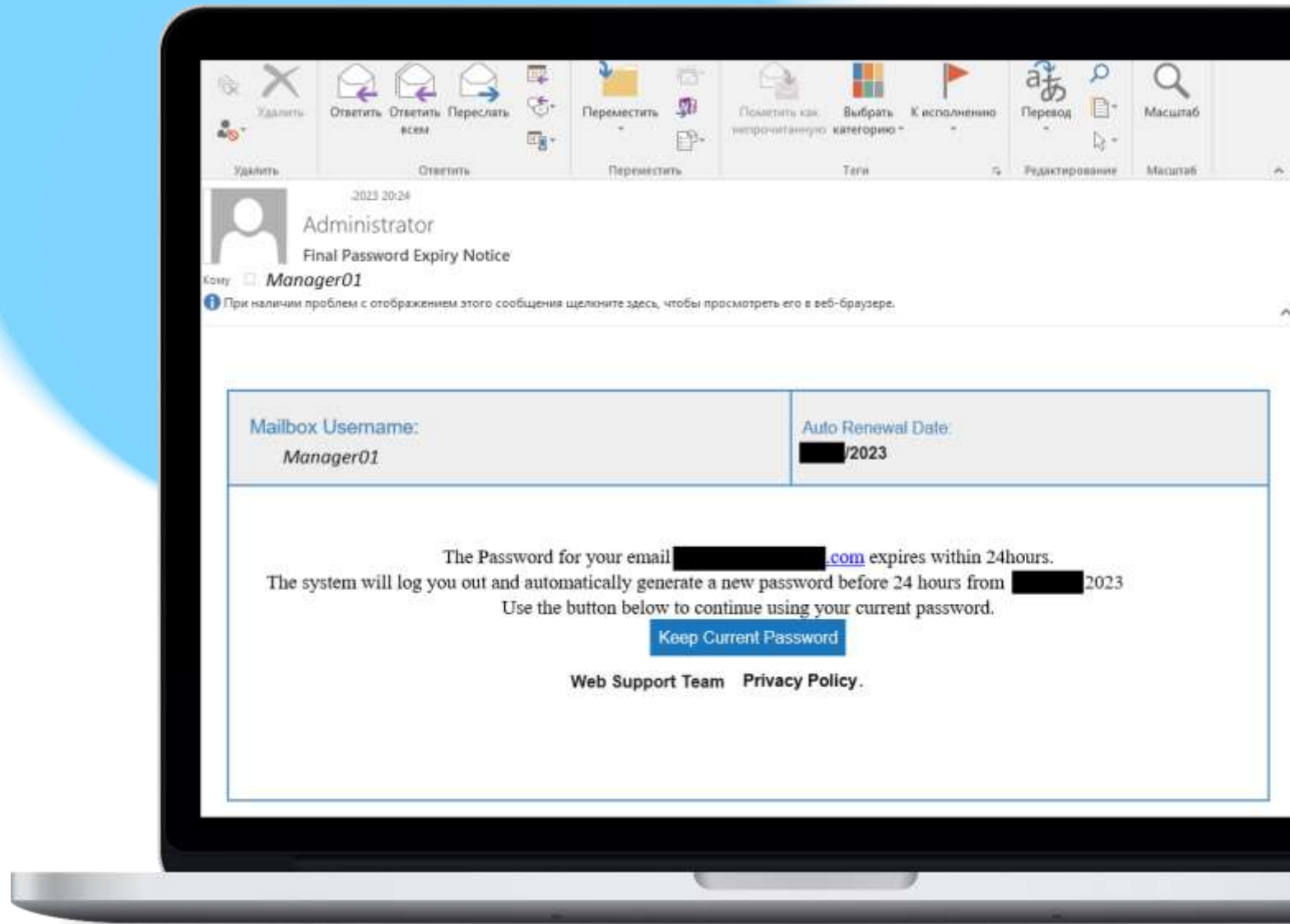


## Что видит аналитик?

- ✦ 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

## 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)

## Что видит аналитик?

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

DETECTION    DETAILS    **RELATIONS**    COMMUNITY

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Files Referring (3) ⓘ

Scanned	Detections	Type	Name
2023-	0 / 60	Email	073a81f45a7461298
2023-	0 / 60	Outlook	Final Password Expiry Notice for ██████████.msg
2023-	0 / 60	Email	Recently Suspended incoming messages

6 / 59 0169b9f67f6ae0169bcc466ffc45fd727 ...

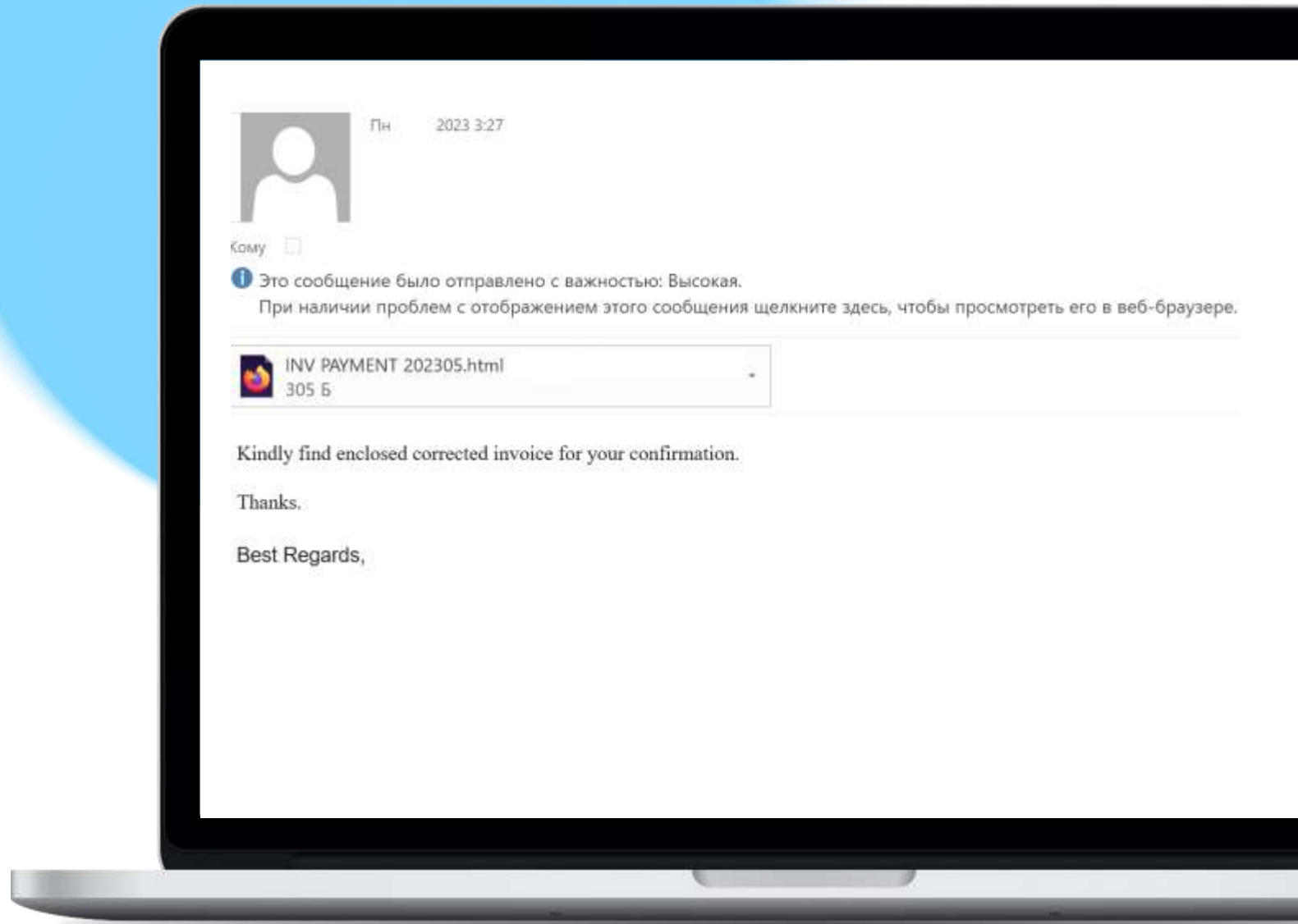
Type	HTML	
Size	64.62 kB	
First Seen	2023-	7:21:25
Last Seen	2023-	7:21:25
Submissions	1	
File Name	General Motors New contract GM030.html	

6 / 59 3197948037fe46be9512e15ea449dfc07309956b...

Type	HTML
Size	64.39 kB
First Seen	2023-05-29 15:44:07
Last Seen	2023-05-29 15:53:51
Submissions	2
File Name	DOCUMENTATION FOR PAYMENT (WENZHOU CHANGJIANG AUTOMOBILE ELECT - WENZHOU - 33 - CN).html

## Что видит аналитик?

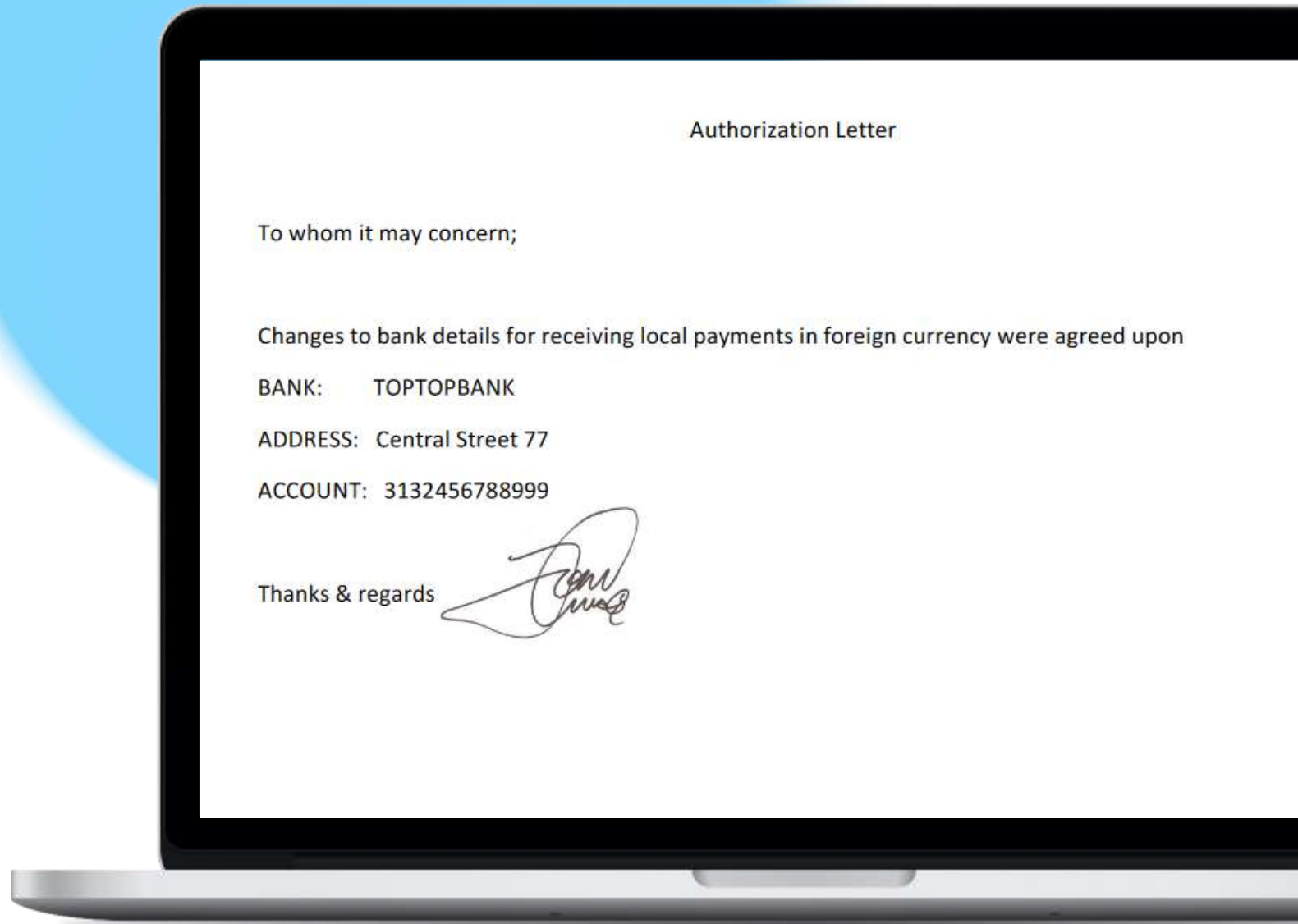
- ✦ Изучение бизнес- процесса
- ✦ Дополнительный Spear Phishing
- ✦ Внедрение, использование бизнес- процесса для реализации атаки



## Что видит аналитик?

✦ The payment that is attached has not been accepted by our bank...

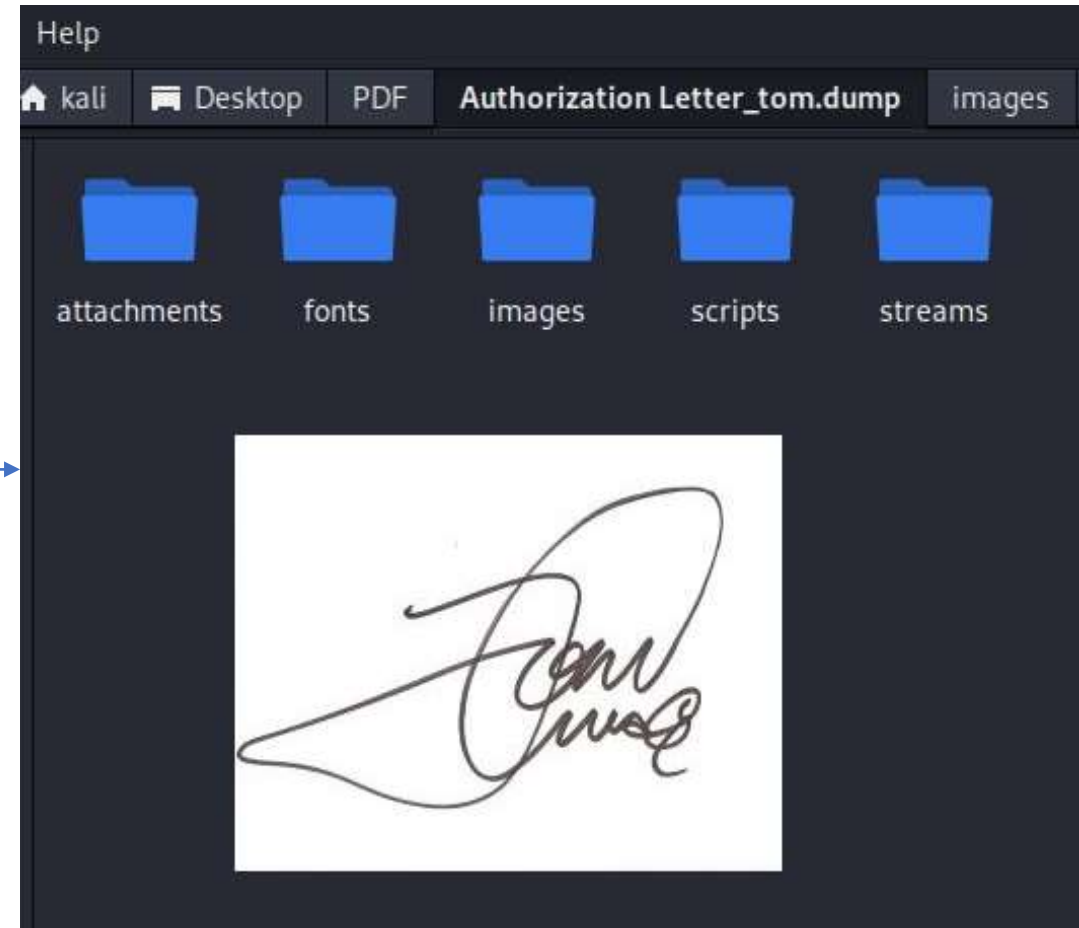
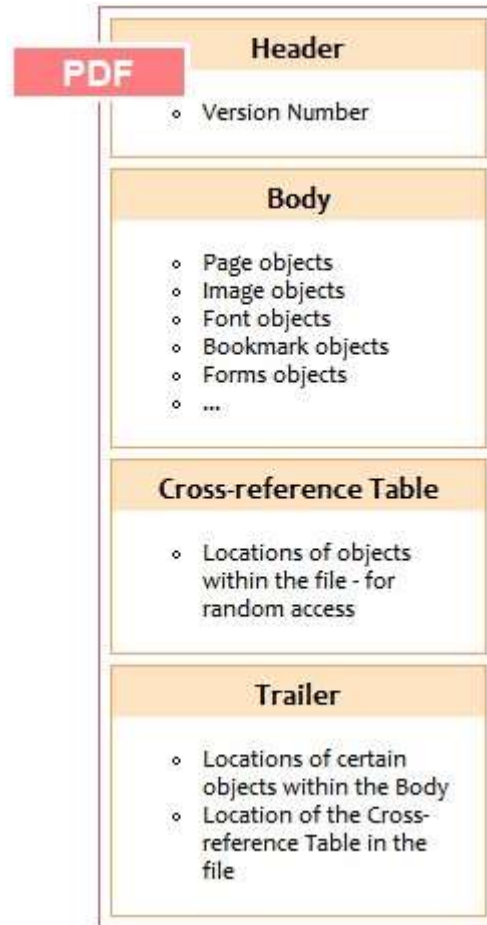
✦ Не беда, подделаем PDF



# CASE #3: Phishing (BEC-атака)

## Что видит аналитик?

✦ Разбираем PDF



PDFextract

# CASE #3: Phishing (BEC-атака)

## Результаты, инструменты для анализа

### 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**



## 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.)

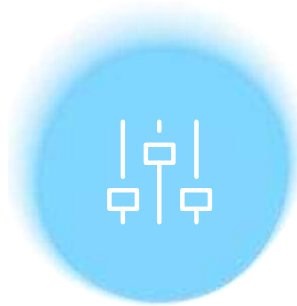






## **НЕ ПАНИКОВАТЬ**

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

