**Yara Rule for PsiXbot**

**(CS-5202)**

**2021-2022**

**Anurag Chowdhury**

**MT20ACS496**

**AREA DIRECTOR NAME FACULTY NAME**

**Dr. Debashish Sengupta Dr Ashu Sharma**

**What is PsiXBot?**

PsiXBot is yet another trojan-type virus designed to record various user-system information. In most cases, cyber criminals proliferate PsiXBot using spam email campaigns and exploit kits. Therefore, PsiXBot usually infiltrates computers without permission.

PsiXBot is capable of recording data, cookies, and logins/passwords saved in browsers and the FileZilla FTP client. Furthermore, it extracts passwords from the Outlook application. Another data tracking feature includes keylogging - PsiXBot records keystrokes to gain access to various personal accounts in social networks, emails, and especially banks. Data-tracking trojan developers aim to generate as much revenue as possible. Therefore, hijacked bank accounts are misused with online purchases, money transfers, and other similar transactions. Email and social network accounts can also be used to borrow money and proliferate malware even further by sending malicious files to all contacts. Another feature is installation of a desktop-type application that allows cyber criminals to monitor the screen and interact with it. Note that PsiXBot creates a scheduled task to re-run itself every 60 seconds. This is to ensure that the bot is running and to make difficult to shut down. The presence of this malware can lead to serious privacy issues, various system infections (ransomware, cryptominers, adware/browser hijackers), and significant financial loss (debt, lost savings, etc.), For this reason, PsiXBot should be eliminated as soon as possible.

|  |  |
| --- | --- |
| **Threat Summary:** | |
| **Name** | PsiXBot virus |
| **Threat Type** | Trojan, password-stealing virus, banking malware, spyware. |
| **Detection Names** | Avast (Win32:ReposFxg-F [Trj]), BitDefender (Trojan.GenericKDZ.54738), ESET-NOD32 (A Variant Of Win32/Kryptik.GQZC), Kaspersky (Trojan-Banker.Win32.Emotet.coso), Full List (VirusTotal) |
| **Symptoms** | Trojans are designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are clearly visible on an infected machine. |
| **Distribution methods** | Infected email attachments, malicious online advertisements, social engineering, software 'cracks'. |
| **Damage** | Stolen passwords and banking information, identity theft, the victim's computer added to a botnet. |

There are dozens of data-stealing trojans that share similarities with PsiXBot including FormBook, TrickBot, Adwind, and Tefosteal - these are just some examples from many. Note that, although the developers are different, all of these viruses have identical behavior - they record data, thereby posing a significant threat to your privacy and financial safety. Therefore, eliminate these infections immediately.

### How did PsiXBot infiltrate my computer?

PsiXBot is mainly distributed using spam email campaigns and exploit kits (such as Spelevo and Smoke Loader). Spam campaigns are straightforward. Cyber criminals send thousands of deceptive emails that contain malicious attachments together with messages encouraging users to open them. These attachments are typically presented as legitimate documents (bills, invoices, receipts, etc.), however, this is simply a disguise - opening them leads to various system infections. As with trojan-type infections, exploit kits essentially infiltrate computers and continue to stealthily inject additional malware, such as PsiXBot. All this happens in the background, without users' consent. After successful infiltration, PsiXBot checks if the system locale is Russian. If so, the malware terminates itself. If not, it continues running. This suggests that cyber criminals are from Russia and aim to protect people from this country.

### How to avoid installation of malware?

Be very cautious when browsing the internet and downloading, installing, and updating software. Think twice before opening email attachments. Files/links that are irrelevant and those received from suspicious/unrecognizable email addresses should never be opened. Download software from official sources only, using direct download links. Third party downloaders/installers often include rogue apps, and thus these tools should never be used. The same applies to software updates. Installed applications and operating systems must also be kept up-to-date. This should be achieved through implemented functions or tools provided by the official developer. Software cracks are also used to proliferate malware. Therefore, you should never take part in software piracy, since it a cyber crime and the risk of infections is extremely high. Lastly, have a reputable anti-virus/anti-spyware suite installed and running, since these tools detect and eliminate malware before the system is damaged. The key to computer safety is caution. If you believe that your computer is already infected, we recommend running a scan with Combo Cleaner Antivirus for Windows to automatically eliminate infiltrated malware.

PsiXBot malware has been updated a number of times since its first release. However, its last release has been implemented with a feature that is used for sextortion purposes. The malware continually monitors user's web browsing activity and searches for certain porn-related keywords in visited sites. If user visits a site that contains some sort of adult content, malware instantly starts recording video (via webcam) and audio (via microphone). The captured media file is saved in .avi format and sent to a remote (Command & Control) server. After gaining such material cyber criminals start their sextortion campaign - they send users various emails stating that they have compromising material and that they'll share it with all of user's friends and colleagues if a ransom is not paid. Now it is worth mentioning that there are many sextortion campaigns which are fake - crooks send hundreds of thousands of emails pretending to have such material and hoping to trick gullible users into paying. Unfortunately, a lot of people actually fall for such scam messages. In this case, however, the statements are very likely to be true. If anyone has visited adult websites while having PsiXBot installed on your computer, there's a credibility that they have been recorded. However, if anyone received such email afterwards, paying is not an option, because crooks merely blackmail them. These persons are likely to ask for even more money after the initial payment. Moreover, there's a high credibility that they will not delete anything even if they agree to pay. For this reason, nobody should trust them.

The below string is behaves like a spyware

$a= "PeekMessage"

$b= "GetMessage"

$c= "DispatchMessage"

$d= "GetUserName"

The below string looks suspicious

$e= "L-V3"

$f= "86B("

The below strings represents that a RDP connection is being created and the string WTSUnRegisterSessionNotification" is used to suppress notification.Probably a spyware

$g= "WTSSendMessage"

$h= "WTSEnumerateServers"

$i= "WTSUnRegisterSessionNotification"

$j= "WTSVirtualChannelOpen"

$k= "WTSFreeMemory"

$l= "WTSDisconnectSession"

The below Strings Detects that it is a behaviour or nomaclature of malware. KillAV string will atempt to disable the AV

$m= "KillAv"

$n= "Ransomeware"

$o= "Psix"

$p= "BotModules"

$q= "Malware.exe"

$r= “Trickbot”

$s= “Crypter.HDUISAHU”