What is XOR Obfuscation | What to know about OpenVPN scramble

Written by Douglas Crawford ⋮ 7-9 minutes

OpenVPN Scramble is a way to hide (obfuscate) OpenVPN traffic so that it doesn't look like OpenVPN traffic. It is highly effective against many deep packet inspection (DPI) techniques, and is good at bypassing even sophisticated VPN blocks.

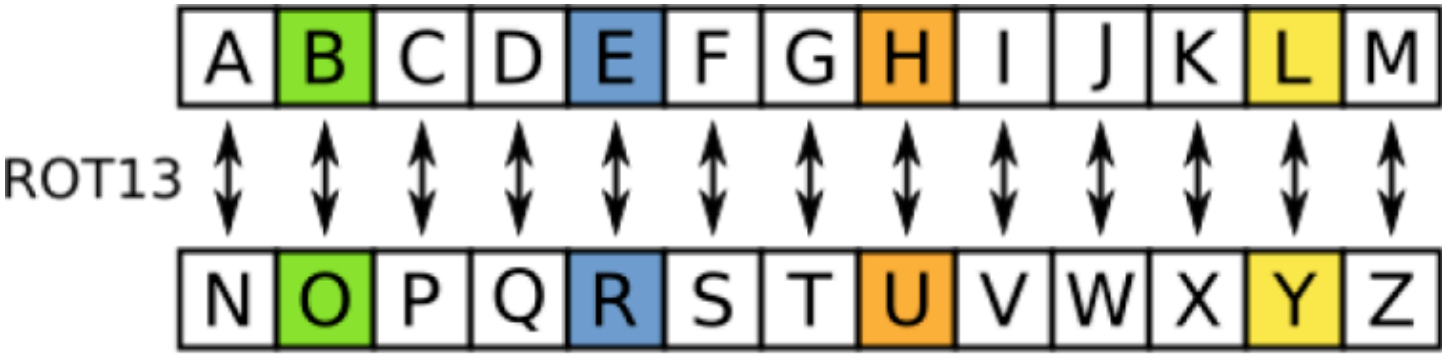
OpenVPN Scramble uses the XOR encryption algorithm. It is very easy to apply and also very lightweight. Many VPN services are turning to OpenVPN Scramble in order to defeat advanced VPN blocks of the kind used by China and Egypt.

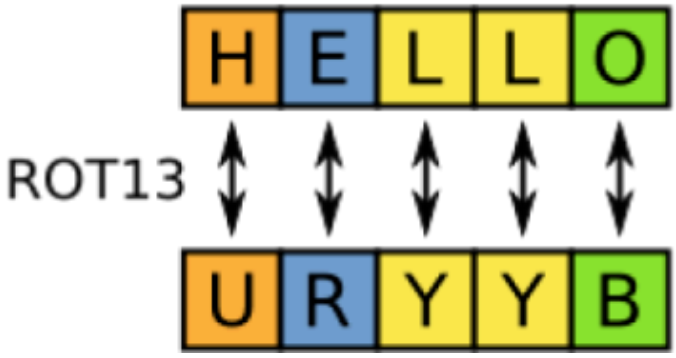
The XOR cipher

XOR is usually pronounced Ex-or and stands for *Exclusive or,* a type of mathematical operation used by the XOR cipher. The XOR algorithm is basically a simple substitution cipher. In other words, it just replaces each alphanumeric in a string that is fed into it with another number.

Crucially, the algorithm is reversible. So if you feed the output string back into the same algorithm, you end up with the original string with the cipher removed.

This kind of cipher is also called an additive cipher, and is the simplest kind of cipher there is. It is the kind of ROT13 cipher that clever kids often use to create secret messages. Except that it uses a much more sophisticated algorithm than most children can devise.





If this doesn't sound very secure, it isn't. Indeed, a simple XOR cipher can be easily broken using simple frequency analysis techniques (looking for patterns in the output string).

OpenVPN Scramble does not use the XOR cipher to secure your data. OpenVPN does that.

OpenVPN does, however, give encrypted data a distinctive signature which can be detected using DPI. By replacing the value of each bit of data protected by OpenVPN with another value, XOR scrambles the data in a way that makes this signature very hard to detect.

And for VPN services, the XOR gold doesn't stop here. The open source openvpn_xor scramble patch makes it almost trivially easy for them to implement XOR Scramble and offer it to their customers.

How effective is OpenVPN Scramble?

Scrambling OpenVPN-encrypted data with the XOR cipher makes it harder for systems such as the Great Firewall of China to detect.

XOR obfuscation has achieved a certain level of notoriety. Its small size and ease of implementation makes it a popular choice for malware developers wishing to hide their nasty bits of code from anti-malware detection.

Many malware developers are happy to just use a 1-byte value to act as the key. The code obfuscated by this key then iterates through every byte of the data that needs to be encoded, XOR'ing each byte with the selected key.

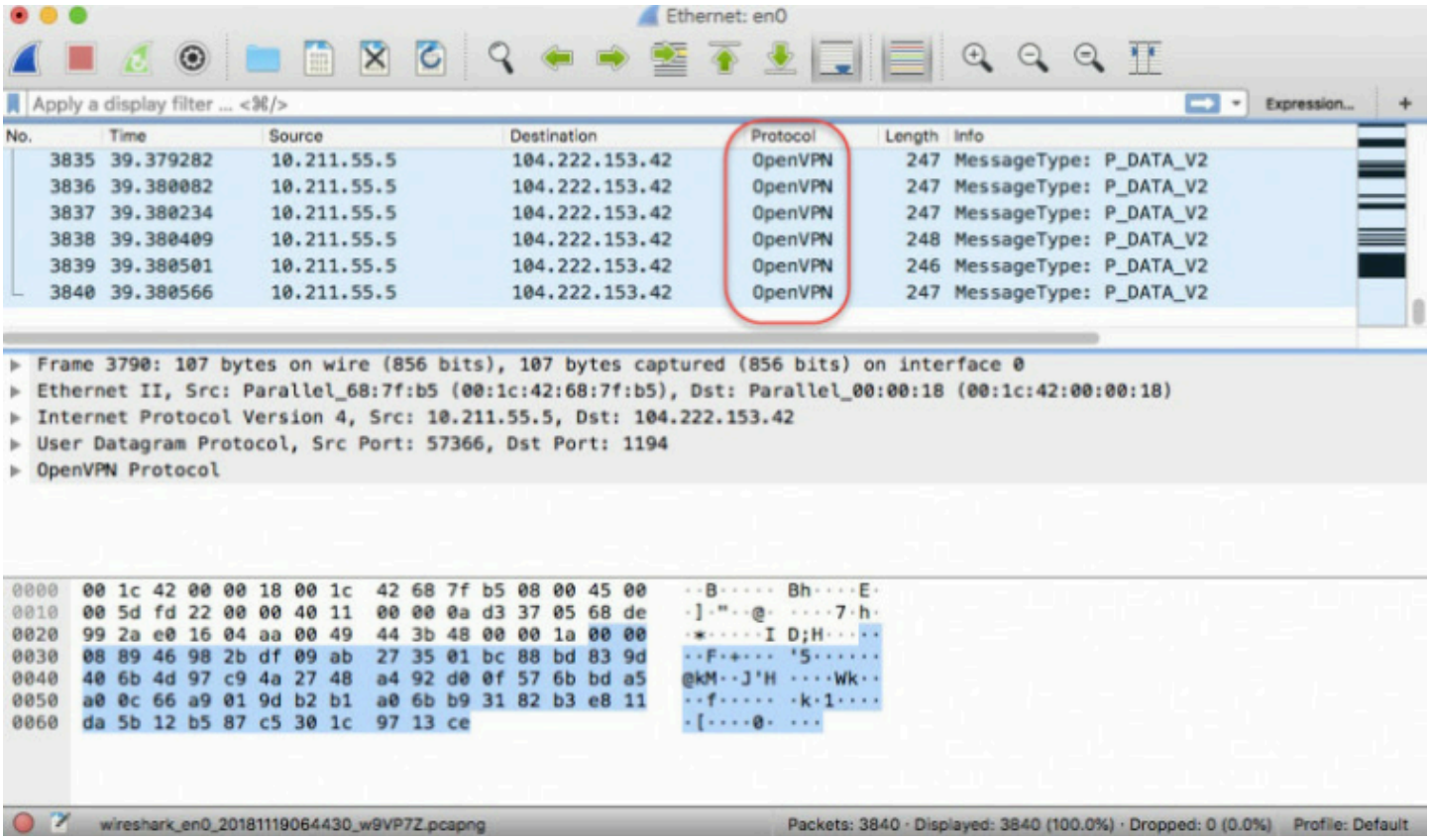
Data obfuscated with a 1-byte value key is relatively easy to spot as it creates repetitive patterns in the otherwise random-seeming code. A number of programs have been developed to do just this.

It is possible to pick longer keys, though, up to the byte value of the data being obfuscated. The effectiveness of the XOR function at scrambling data is fully dependent on how random the key is that it uses.

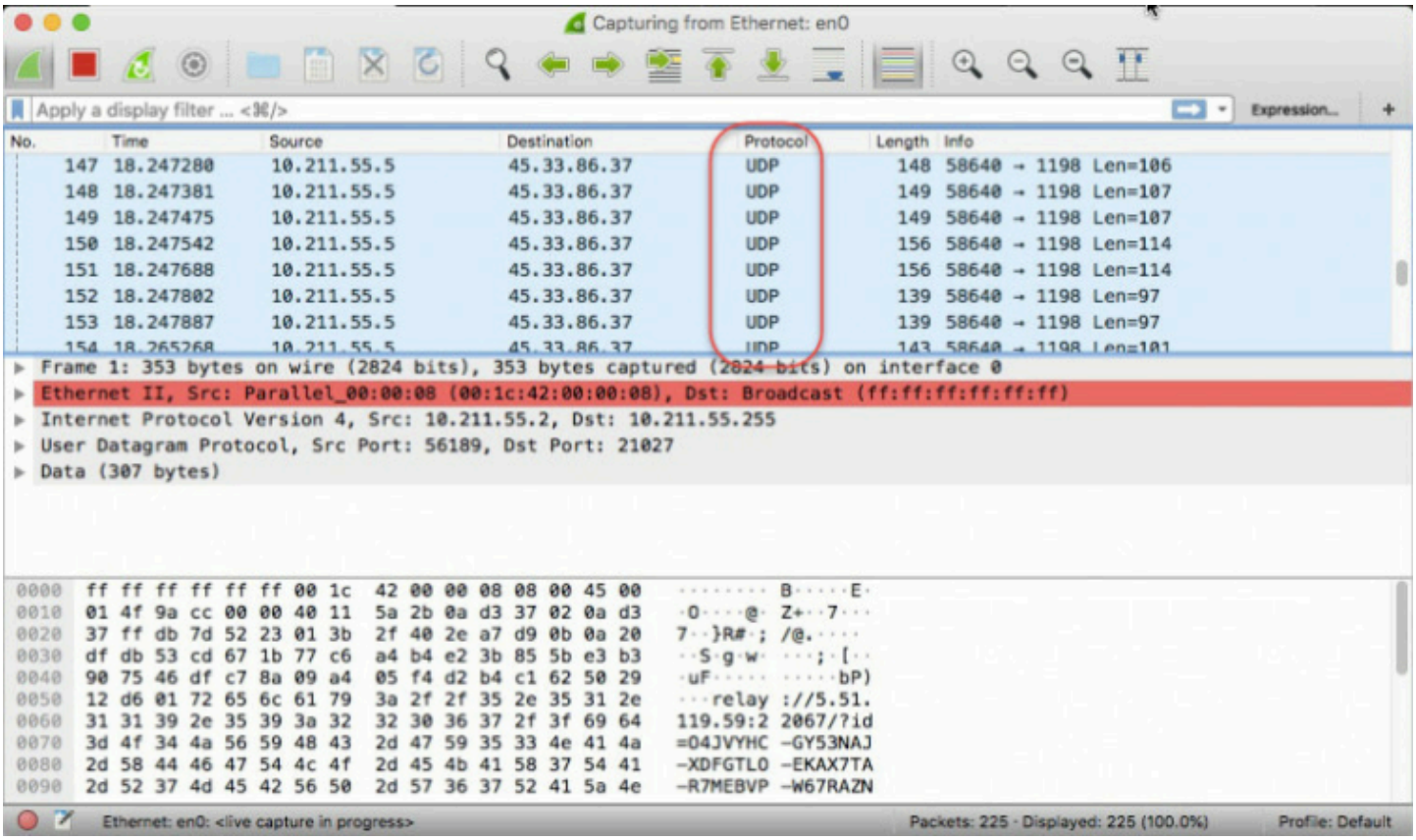
So what does all this mean? Well, the widespread use of XOR obfuscation for malware is something of a testimony to its effectiveness.

NordVPN is VPN company that offers XOR encryption, so we asked its digital privacy expert, Daniel Markuson, to comment on how effective it is at defeating VPN blocks. He suggests running the following experiment using the Wireshark packet analyzer (check out our how to setup Wireshark guide):

1. Turn on regular VPN. Wireshark sees the traffic as OpenVPN.



2. Turn on Obfuscated VPN over TCP (the NordVPN's XOR option). Wireshark no longer identifies the traffic as OpenVPN.



"*XOR definitely works. Is it always effective against government efforts to block OpenVPN traffic? No, not at all. But as the above experiment shows, it's more complicated to identify VPN traffic if XOR is used. It is therefore harder to block.*"

Controversy

Despite its advantages, the openvpn_xorpatch is somewhat controversial. Indeed the OpenVPN developers have declined to implement it in any official version of OpenVPN, and advise against its use.

"*We (OpenVPN developers) do not encourage people building their own versions of OpenVPN changing the wire-protocol like this, without the patch being through a proper patch review and having evaluated possible security risks related to such a change.*

And we especially discourage using such an approach when there exists a far better solution, used by the TOR community. It is called obfsproxy and can be used together with OpenVPN without needing any re-compilation of OpenVPN.

"

Despite these warnings, however, the developers of open source macOS VPN client, Tunnelblick, have opted to include a modified version of the XOR patch in their software:

"*Regardless of the OpenVPN developers' decision not to include the patch in OpenVPN, the patch is attractive because it is so easy to implement: simply apply the patch to both the OpenVPN server and the OpenVPN client and add a single, identical option to the configuration files for each. Using obfsproxy is more complicated because it involves running another, separate program on both the server and the client.*

Because the patch is so easy to implement, the patch is included in all versions of OpenVPN that are included in Tunnelblick as of build 4420."

It is worth noting that the Tunnelblick developers found the original XOR patch to have critical flaws, and therefore released an updated version of the patch that fixed all issues found:

"*Large organizations have the ability and power to 'unscramble' traffic and detect it as OpenVPN traffic, and the obfuscation provided by this patch is so rudimentary that relatively simple cryptanalysis will probably be able to unscramble the content, too."*

We certainly hope that VPN providers who offer OpenVPN Scramble use this improved XOR patch, or have made similar changes to the original.

Alternatives to OpenVPN Scramble

Obfsproxy

The OpenVPN developers have clearly at their favored obfuscation tactic is obsfproxy, a tool designed to wrap data into an obfuscation layer.

Obfsproxy was developed by the Tor network, largely as a response to China blocking access to public Tor nodes. It is independent of Tor, however, and can be configured for OpenVPN.

Obfsproxy is used to run pluggable transports which scramble the VPN (or Tor) traffic. It supports a number of these pluggable transports but obfs4 is the latest state-of-the-art "looks-like nothing" obfuscation protocol from Tor Project.

Stunnel

This is another good VPN obfuscation tactic. It works by routing VPN traffic through a TLS/SSL tunnel. TLS/SSL is the encryption used by HTTPS, so VPN connections (usually OpenVPN) routed

through these TLS/SSL tunnels are therefore very difficult to tell apart from regular HTTPS traffic. See our HTTPS guide for more information.

This is because the OpenVPN data is wrapped inside an additional layer of TLS/SSL encryption. As DPI techniques are unable to penetrate this "outer" layer of encryption, they are unable to detect the OpenVPN encryption hidden inside the tunnel.

Conclusion

OpenVPN Scramble is easy for VPN services to deploy, and can be highly effective at evading VPN blocks, but it is not as robust at hiding VPN traffic as either obfsproxy or stunnel.

Simply trying to use a VPN is illegal in very few places in the world, so if your VPN connection is blocked there is little harm in seeing if OpenVPN Scramble will unblock it, it probably will.

In those rare circumstances where you might actually get into trouble if VPN use is discovered, however, then obfsproxy or stunnel are safer.