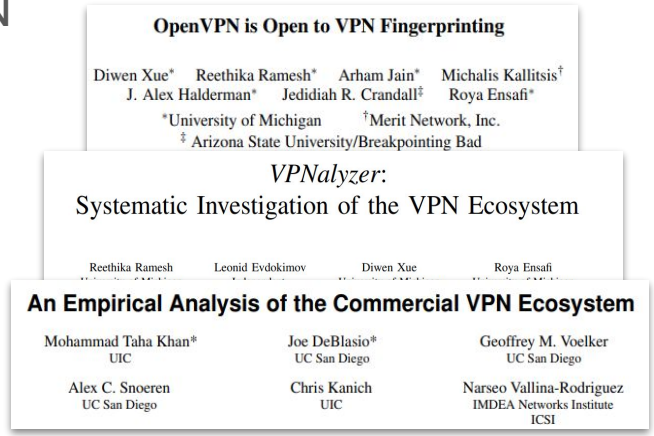
Characterizing the VPN Ecosystem in the Wild

Aniss Maghsoudlou[1], Lukas Vermeulen[1], Ingmar Poese[2], Oliver Gasser[1]

[1] Max Planck Institute for Informatics
[2] Benocs GmbH

Motivation

- Rise of remote work during the pandemic → VPN
- Previous work investigate commercial VPNs
- VPN servers ecosystem in the wild
  - Active measurement: server detection & TLS security
  - Passive measurement: VPN traffic detection



OpenVPN is Open to VPN Fingerprinting

Diwen Xue* Reethika Ramesh* Arham Jain* Michalis Kallitsis†
J. Alex Halderman* Jedidiah R. Crandall‡ Roya Ensafi*
*University of Michigan †Merit Network, Inc.
‡ Arizona State University/Breakpointing Bad

VPNalyzer:
Systematic Investigation of the VPN Ecosystem

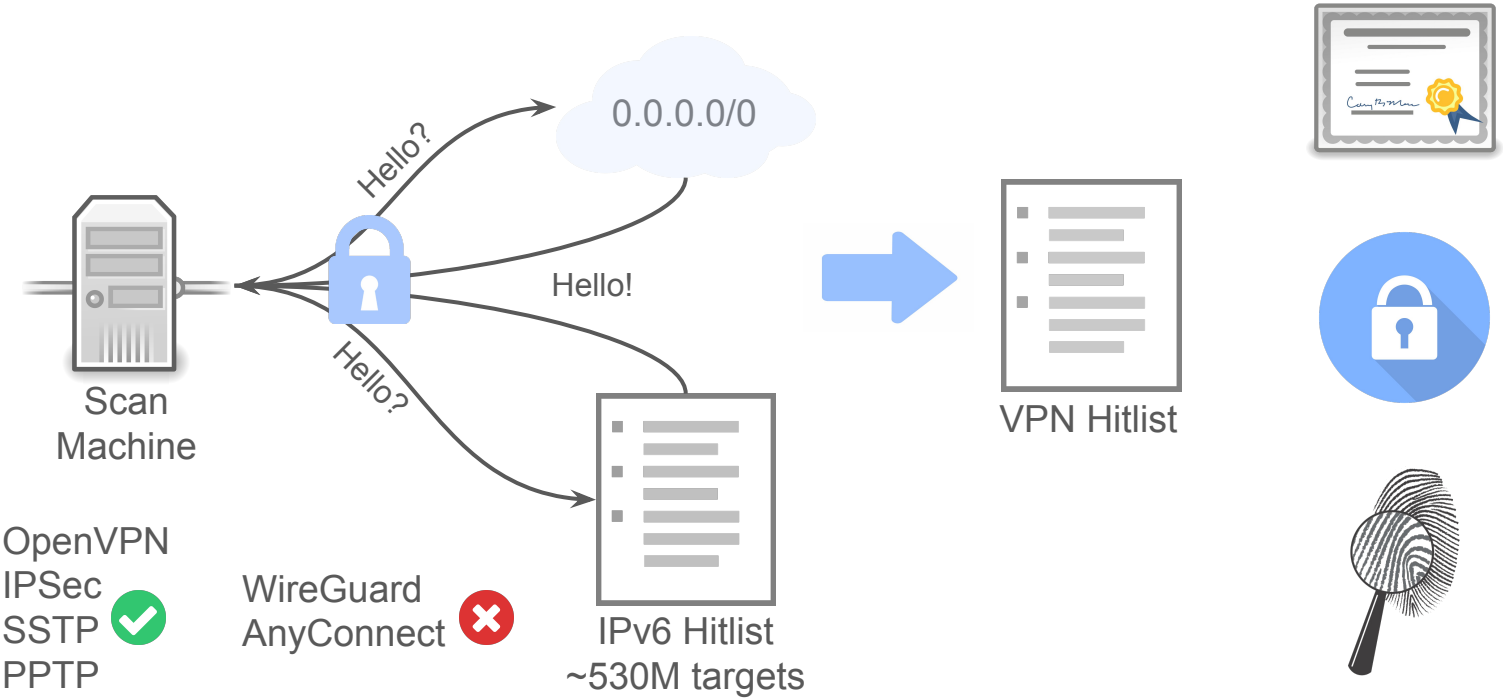
Reethika Ramesh Leonid Evdokimov Diwen Xue Roya Ensafi

An Empirical Analysis of the Commercial VPN Ecosystem

Mohammad Taha Khan* UIC
Joe DeBlasio* UC San Diego
Geoffrey M. Voelker UC San Diego
Alex C. Snoeren UC San Diego
Chris Kanich UIC
Narseo Vallina-Rodriguez IMDEA Networks Institute ICSI

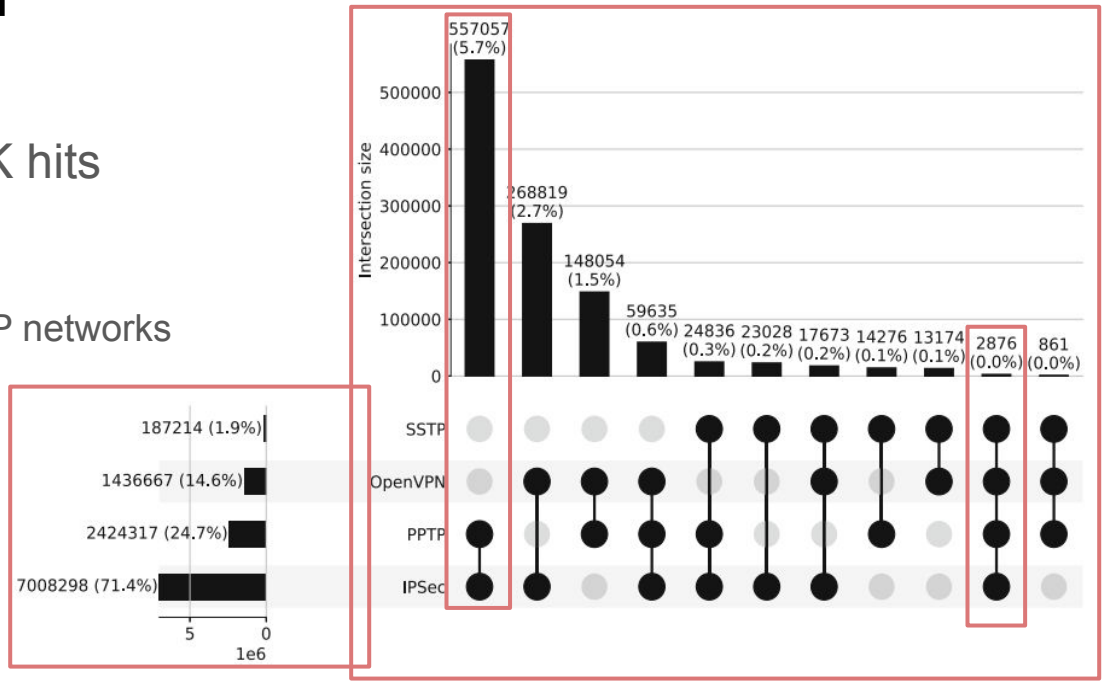
How can we characterize the *VPN server* ecosystem *in the wild*?

Active Measurement - Methodology



VPN Server Detection

- IPv4: 9.8M hits, IPv6: 2.2K hits
- AS analysis:
  - most top ASes are large ISP networks



- Only a few VPN servers with more than one protocol
- Low IPv6 adoption

TLS Certificate Analysis

OpenVPN	
Expired:	6,080 (3.8%)
Self-signed:	109,825 (69%)
CA organizations:	14,548
Unique certificates:	129,143
Total Certificates:	158,705

SSTP	
Expired:	13,370 (9%)
Self-signed:	34,725 (24%)
CA organizations:	2,502
Unique certificates:	104,988
Total Certificates:	143,517

Substantial amount of self-signed certificates

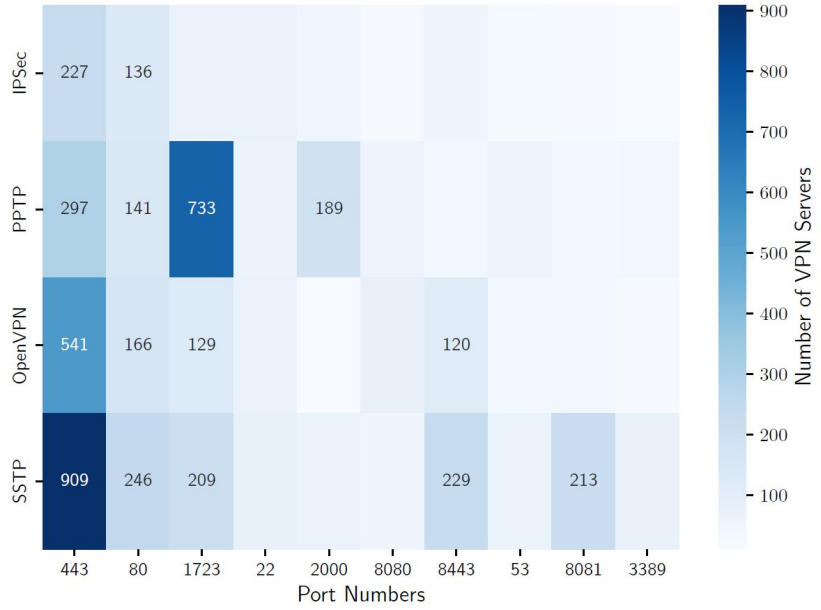
TLS Vulnerability Analysis

	Requirements	OpenVPN	SSTP
RC4	RC4	32,294 (7%)	84,892 (31%)
Heartbleed	OpenSSL Heartbeat	232	10
Poodle	SSL 3.0	7,005 (1.5%)	24,917 (6%)
FREAK	RSA_EXPORT	31	1
Logjam	DHE/512-bit export	8	0
DROWN	SSLv2	0	0
ROBOT	TLS_RSA	95,301 (20%)	174,986 (74%)
Raccoon	TLS_DH	0	0

Only a few outliers for more critical vulnerabilities

VPN Server Fingerprinting

- Nmap OS detection:
  - 609 guesses for 1K servers/protocol
  - Linux as most frequent OS
  - More hardware guesses for PPTP
  - More Microsoft products for SSTP
- Nmap port scan



Large number of VPN servers seem to also be Web servers

Passive Measurement - Methodology

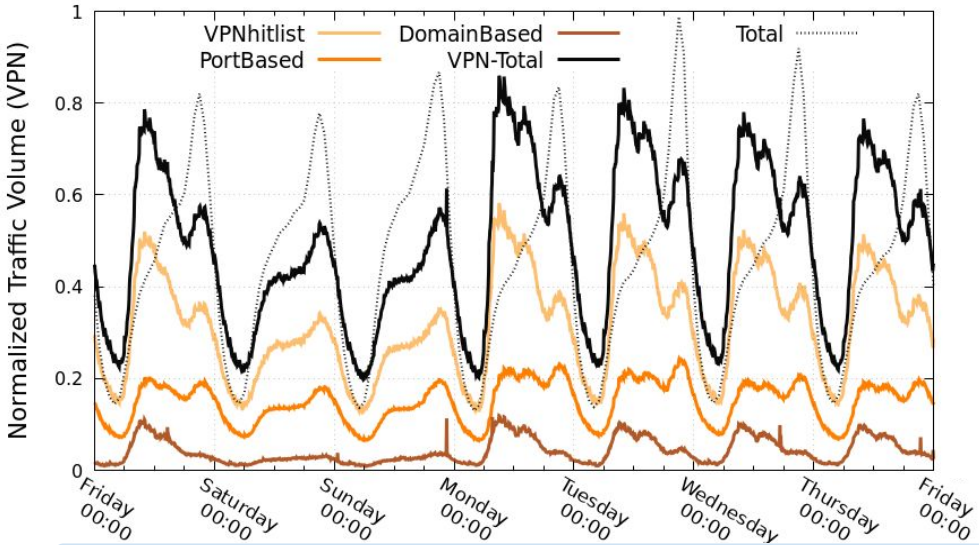
- Traffic volume for the detected IPs (VPN Hitlist)
- Comparison with the existing approach by *Feldmann et al.**:
  - Port-based: port numbers used by VPN protocols
  - Domain-based: domains with "*vpn*" and without *"www."*
- Netflow data from a large European ISP
- Domain names of the detected IPs
  - Captured DNS records at resolvers
  - Reverse DNS look-ups

* Anja Feldmann et al. (2020) The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic. IMC'20.

VPN Traffic Detection

- Domain names found for 23% of IPs in VPN hitlist
- 5 commercial VPN providers in top 10 domains
- Wireguard port 51820 and 1337 observed in VPN hitlist
  - Co-existence of multiple VPN protocols on a server

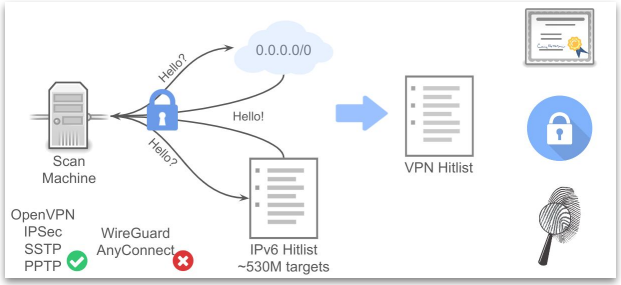
VPN Traffic Detection



- Highest VPN traffic detection with VPN hitlist
- Different diurnal patterns in weekdays and weekends
- VPN traffic 4% of the total traffic

Summary

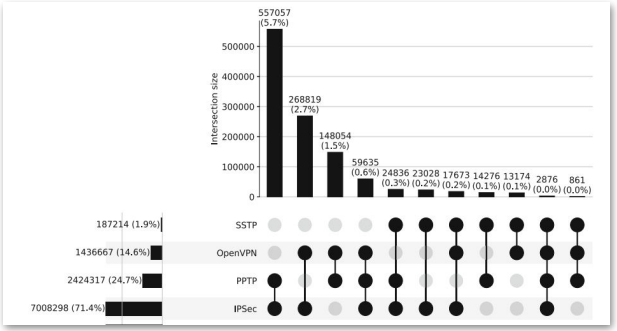
Characterizing the VPN server ecosystem in the wild.



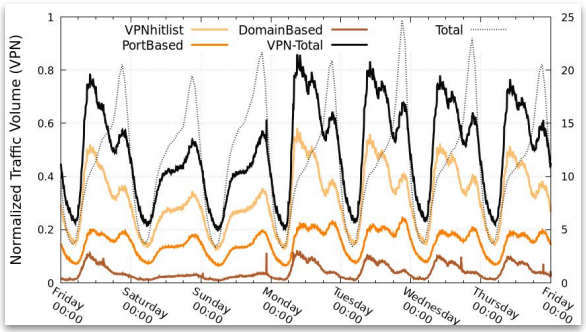
SSTP servers more vulnerable to TLS attacks.

	Requirements	OpenVPN	SSTP
RC4	RC4	32,294 (7%)	84,892 (31%)
Heartbleed	OpenSSL Heartbeat	232	10
Poodle	SSL 3.0	7,005 (1.5%)	24,917 (6%)
FREAK	RSA_EXPORT	31	1
Logjam	DHE/512-bit export	8	0
DROWN	SSLv2	0	0
ROBOT	TLS_RSA	95,301 (20%)	174,986 (74%)
Raccoon	TLS_DH	0	0

VPN servers in the wild detected for 4 VPN protocols.



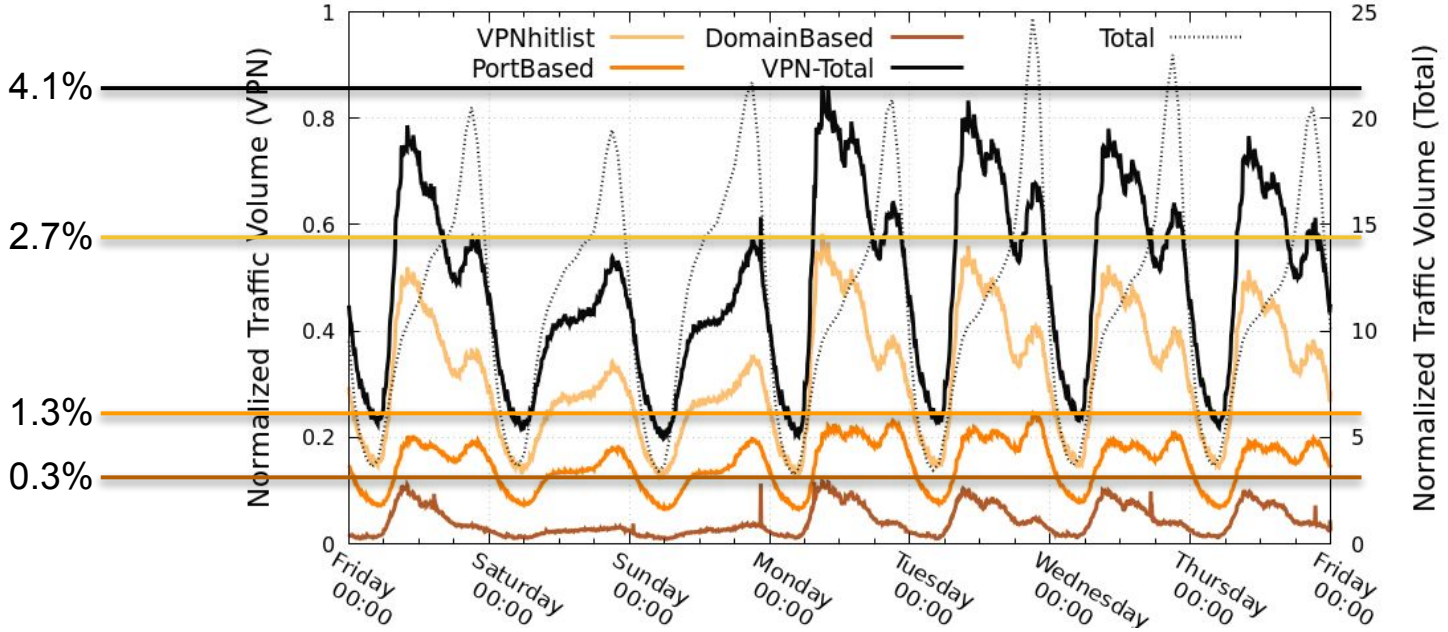
Our approach detects the most VPN traffic.



VPN hitlist, analysis code, custom scan modules:

vpnecosystem.github.io

Back-up: Passive Measurement Results



- Different diurnal patterns in weekdays and weekends
- Highest VPN traffic detection with VPN hitlist

Back-up: Detected VPN Protocols

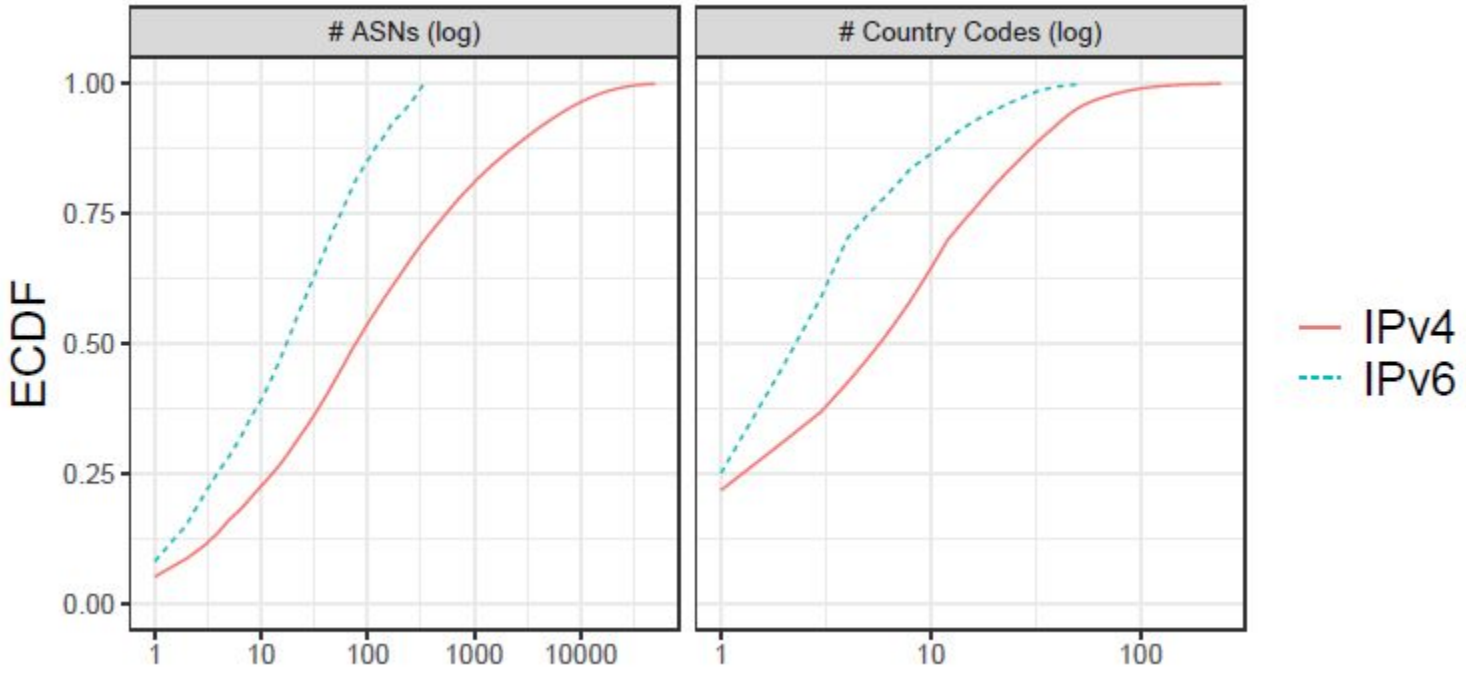
IPv4

VPN protocol	Detected servers
SSTP	187,214
OpenVPN	2,424,317
PPTP	1,436,667
IPSec	7,008,298
TOTAL	9,817,450

IPv6

VPN protocol	Detected servers
SSTP	949
OpenVPN	2,070
TOTAL	2,221

Back-up: AS Analysis



Back-up: Top 10 ASes

IPv4

AS number	AS name	VPN servers
4134	ChinaNet	515,830
7922	Comcast	356,327
1221	Telstra	257,821
3320	Deutsche Telekom	242,433
4766	Korea Telecom	228,863
4713	NTT Communications	145,286
7018	AT&T	137,698
4837	China Unicom	133,861
3462	HiNet	119,612
20115	Charter Communications	97,109

IPv6

AS number	AS name	VPN servers
7922	Comcast	183
63949	Akamai	159
12322	Proxad Free SAS	138
7506	GMO Internet Group	89
9009	M247 Ltd	63
9370	Sakura Internet Inc	58
14061	DigitalOcean	55
2516	KDDI Corporation	54
7684	Sakura Internet Inc	39
680	DFN-Verein	36

Back-up: The Effect of Not Using SNI

- Re-run TLS scans with SNI and domains from rDNS resolution
  - 3% mismatches for OpenVPN, 5.5% mismatches for SSTP
- Re-run without SNI and compare again
  - 3 times fewer mismatches for OpenVPN, less than half for SSTP

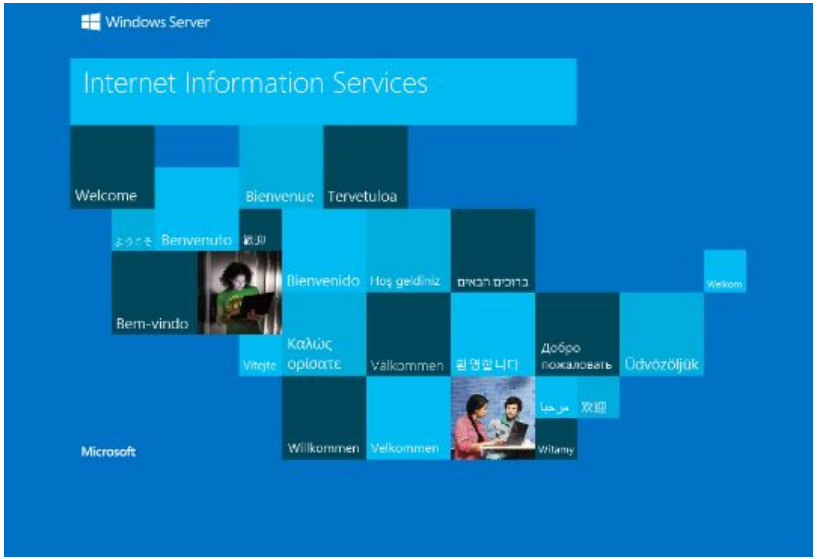
- overall, less than 1% of certificates are affected
- effect is negligible

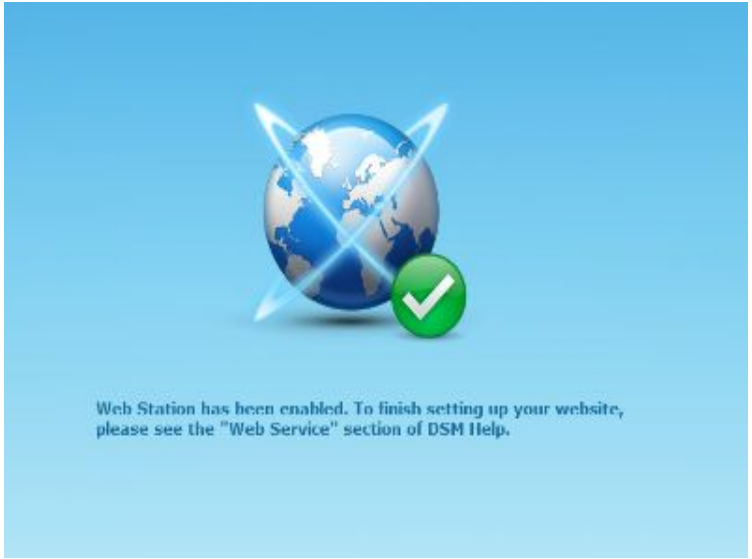
Back-up: OpenVPN Limitations and Protocol Versions

- Sent out requests with HMAC requiring pre-shared key
  - Only 84 out of 1.4M servers accepted our random HMAC
- Follow-up scans: suggest insecure key exchange method
  - No server accepted the key-method
  - ~6,500 responded with secure key exchange method

- we can only detect a subset of OpenVPN ecosystem
- insecure key exchange is truly deprecated

Back-up: Sample Websites for Some VPN Servers





Many servers only display generic default pages