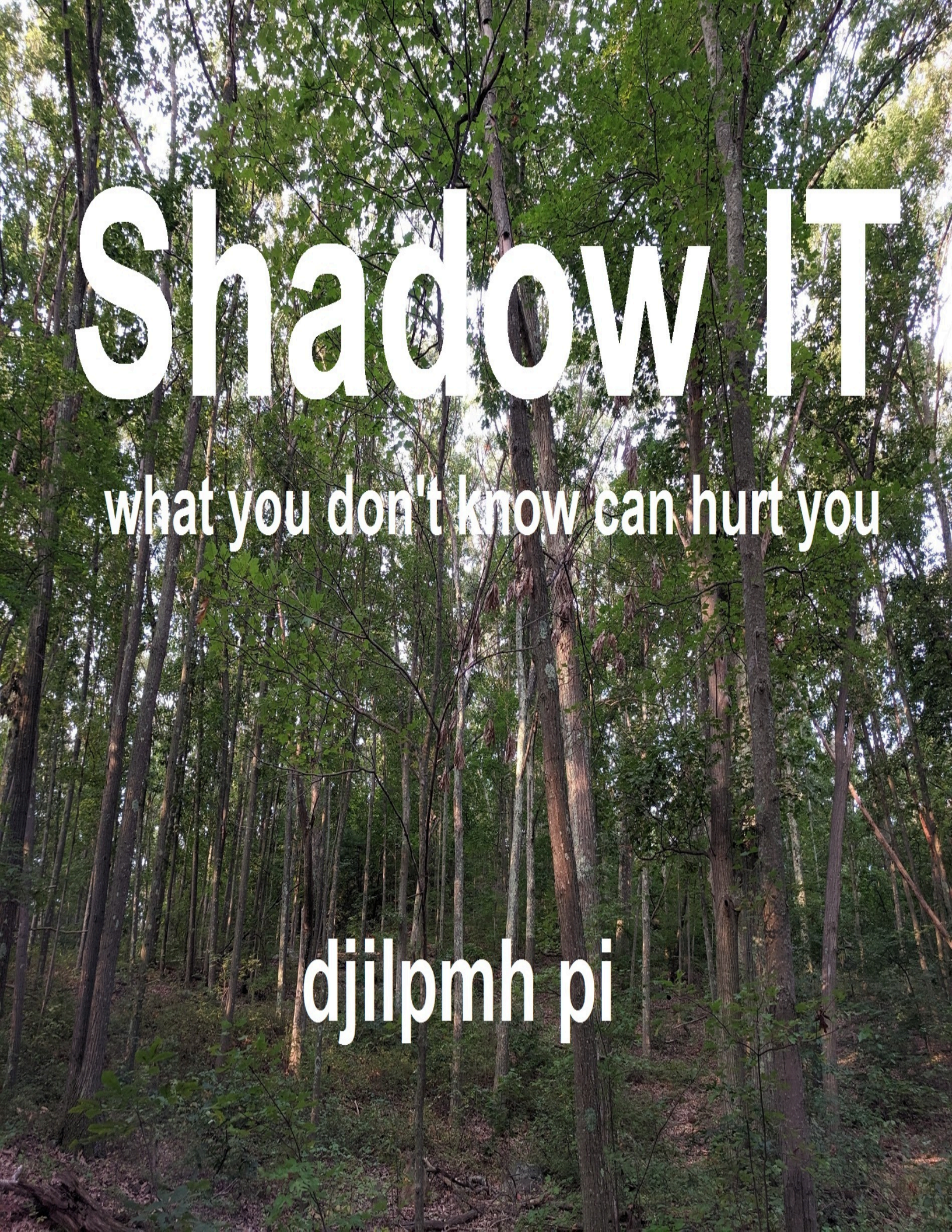
Shadow IT
what you don't know can hurt you
djilpmh pi

Shadow IT

What you don’t know can hurt you.

djilpmh pi

This book is for sale at http://leanpub.com/shadowit

This version was published on 2019-10-08

I dedicate this book to all of you who continue to do things right, instead of just doing things to generate good looking reports. By right, I mean really helping the business move forward in an efficient and secure way, instead of just saying no, we don't do that. I believe most workers do not have malicious agendas (ooh let's get our computers infected!) because that would make it even harder to just do their job. When the helpdesk is not helping, it drives workers towards Shadow IT where the work gets done but leaves the business vulnerable in invisible ways. I dedicate this to those of you who have sought to help lubricate the wheels of business and make progress while maintaining a secure environment and staying true to the spirit of collaboration rather than obstruction by policy. Thank you, and keep up the good work in spite of others who will maintain they are right, but are making themselves increasingly irrelevant.

Contents

0. Disclaimer

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

0.1 How to Use / Read This Book

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1. Shadow IT: An Introduction

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.1 What You Know For Sure That Ain't So

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.2 Applicability

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.3 Types of Shadow IT

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.4 Hire Competent People

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.5 Whitelist your security

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.6 Training, education and "good security practices" are still necessary

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.7 End of Scolding

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.8 No Secrets Here

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

1.9 Summary and Looking Forward: The Need for Leadership With Vision

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

2. Local Tunnels

2.1 What is it, and what's the danger?

Local tunnels are exemplified by a clever tool called 'ngrok'. Undetected and uncontrolled local tunnels bypass inbound security controls and potentially expose the most important internal network segments to open access from anywhere on the public internet.

Anyone on the public internet who knows the link can thus bypass conventional firewalls and reach the workstation or server on the internal network.

2.2 How does it work?

A server inside a firewall protected network initiates an outbound connection (generally on an unrestricted port such as TCP port 443) to an ngrok server on the Internet. The ngrok server advertises a service that can be accessed anywhere on the public internet, that travels back through that initial connection to the service on your internal server. These can be SSH servers, web servers, database servers, almost anything that runs on TCP. Older versions of TFTP that run on UDP would therefore not be supported. Details are found at https://ngrok.com/product.

Local tunnels are much more interesting than traditional configuration of inbound port forwarding on the internet facing firewall. It can be very dangerous to allow inbound connections from "outside" (public internet) to an internal system rather than to a tightly controlled DMZ (demilitarized zone). Remember, this connection can be to an internal server that might be running on a VM on some internal desktop or laptop, and the connection is to an internal system, not on an isolated DMZ.

Local tunnels can be very convenient when someone wants to bypass conventional firewalls to get something done. Any TCP connection can publish an internet accessible port from anywhere, to view the web page, or open an SSH session. Belaboring the obvious, an internal resource (supposed to be protected by corporate firewalls) is now available to be accessed from anywhere on the internet, and your corporate firewalls have been completely bypassed.

Some local tunnel applications and services include:

* Ngrok "localtunnel" https://ngrok.com/
* http://pagekite.net/ $3/month
* https://showoff.io/pricing $5/month
* https://forwardhq.com
* http://localtunnel.me

2.3 How to detect and stop

Enforcing prohibitions of this sort can be difficult if the outbound connection uses HTTPS/SSL (TCP port 443). Local tunnel applications such as ngrok are particularly insidious because they do not require administrative rights to install; just run it from your USB drive or copy it from a locally attached storage unit.

At a minimum, corporate security policy and education should be in place to prohibit the use of such tools, with appropriate consequences. Unless you are already deep scanning – looking at binary signature of every file in every hard drive of every workstation and server, searching by filename is fruitless if someone just renames the executable file from ngrok.exe to showme.exe .

Since the only observable network connection is outbound, conventional firewall rules are not effective since the ngrok or other localtunnel server might be installed anywhere. But at least block (blacklist) known ngrok and enumerated localtunnel servers that are known and published.

Locking down software installations and limiting such actions to domain administrators is not effective since ngrok and other applications don't need to be "installed" in any way. All that's needed is for someone to bring it in on a USB stick, and run the app from the stick. See the section on Portable Apps for other software that does not require any admin rights to run, since they don't actually need to be installed.

As already noted in Part 1.5, if the policy governing egress traffic leaving your network is whitelisted (allow only those service ports known to be necessary), you're well ahead of this since the ngrok and other localtunnel services won't be allowed by default. This is neither easy nor efficient and can generate a lot of workload in combination with user frustration relating to their work being delayed while their requests are reviewed and processed.

2.4 The Irony of Security Education

The irony of educating a user population "don't use ngrok or localtunnel applications" tells some parts of that user population a clever tool that they had not heard of until you told them. It's like telling them "don't use that tunnel from the back of the bank vault to the street outside" - the one they didn't know was there until you told them.

2.5 Observation

Ngrok and other local tunnel software are being mentioned (google it yourself) as nice tools to test a locally installed database or application. How convenient, I don't have to submit another firewall request that I don't know what they want anyway. Various recommendations to use ngrok often do not warn of the danger, that the internal corporate network is exposed to any random user on the internet who has the link.

3. Zero Knowledge services

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

3.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

3.2 How Is This Different from File Sharing in the Clouds?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

3.3 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

4. Use of Nonstandard Service Ports

4.1 What is it, how does it work, and what's the danger?

As a specific example: SSH servers by convention and in normal use listen for connections on tcp port 22, so most firewalls that block encrypted external connections via SSH block port 22. But browser traffic on tcp port 443 are often unrestricted, because an employee's connection to their banking server is generally respected as their own private business. Knowing this, having an SSH server on the outside listen on tcp port 443 can abuse this trust and arbitrary permission, and allows an SSH session to exit the enterprise network and connect to an external SSH server.

Other protocols can easily be configured to use nonstandard ports. Some organizations feel it is OK to allow FTP (file transfer protocol) on TCP port 21 because standard FTP functions are not encrypted and all conventional FTP traffic is readily visible and logged for analysis.

4.2 How to Detect and Stop

A smart firewall could be configured to detect the traditional SSH client/server handshake, much like an IPSec VPN handshake that is used to set up a session, but there needs to be sufficient capacity to perform deep inspection of the traffic to recognize the SSH handshake, among protocols that could establish unauthorized communications and transfer files while bypassing standard information controls.

Training of the user community so everyone understands this is a violation, evokes the same problem already noted in Part 2.4 - it tells many others who never thought of it, that such a mechanism is possible.

Ideally a whitelist policy (allowing only authorized connections between inside and outside) would prevent unauthorized connections to SSH or other servers on the internet.

A comprehensive strategy to detect and stop the use of nonstandard ports would rely on all of these strategies and others that are appropriate to the specific situation at hand.

4.3 Similarity to Anti-Censorship Strategies

Strategies used by TOR (the Onion Router) software to circumvent censorship as enforced by the GFWC - The Great Firewall of China has led to development of "pluggable transport" alternatives

including a method called ScrambleSuit, that mimics other types of (encrypted) traffic, some of which might well be allowed to pass through various firewalls, even those specifically intending to block TOR.

Elsewhere in this book ”Anti-Censorship” and distributed methods create other problems for information and network security. The masquerading of SSH (should be on port 22, normally blocked) as HTTPS (port 443, normally allowed to pass) is a strategy similar to other Anti-Censorship tools.

5. SSL VPNs

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

5.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

5.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

5.3 Observation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

5.4 (Web) Application Proxies

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

6. Misused Online Conferencing Tools

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

6.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

6.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

6.3 Examples of Browser Plugin Based and Application Based Conferencing Services

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

7. Encrypted File Transfer in Browser

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

7.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

7.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

8. Cloud Services

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

8.1 Almost anyone with a credit card can start a cloud based server

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

8.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

8.3 Observation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

9. File Sync Danger

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

9.1 What is it

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

9.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

9.3 Observation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

10. Portable Apps

10.1 What is it, how does it work, and what's the danger?

Portable Apps are versions of many applications that can run on your system without administrative rights; they all run from USB or file system without "installation". Corporate standard software is rendered meaningless if anyone can bring in their own browser, word processor, file zipper, and email clients, and use them at will. See https://portableapps.com for the range of tools that can run from your USB

10.2 How to detect and stop

Group policy could block a specifically identified application such as the portable apps launcher, but if a portable app is launched individually without running the launcher, it is harder to block.

Security training and education could point out the obvious danger of using unauthorized software brought in on a USB drive. Since such portable apps are not actually installed and no registry changes are required, most of these can be executed without local administrator privileges. The security training and education has to emphasize that the danger of using such randomly obtained software is as stupidly risky and dangerous as opening email attachments from people you don't know.

Perhaps the most effective strategy would be to forestall a sense in the user community that they need to circumvent corporate IT and corporate security policy: be helpful and directly support the users and deliver services they need, that have been reviewed and secured, and verified to be compliant applications. If using approved software is the path of least resistance, and it supports user needs, users who deliberately continue to violate good security practice and corporate policy – perhaps should be appropriately disciplined.

10.3 Observation

There are many applications that do not require "installation" (which typically requires administrative rights); one already mentioned is ngrok.

Another way to run software on company owned computers without needing administrative rights is covered in the next part, under Desktop Virtualization: it's possible to run a Windows or Linux operating system in a virtual machine on your Windows, Linux, or Mac. One free platform is Oracle's VirtualBox. Since the user is the creator and admin of the virtual machine, she can install and use any software at all! More in the next section.

11. Desktop Virtualization

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

11.1 What is it

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

11.2 How to block

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

11.3 Observation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

11.4 Observation 2

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

12. Desktop Virtualization and TOR

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

12.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

12.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

13. Unblocked TOR Access

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

13.1 Unblocked TOR access

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

13.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

13.3 Many Networks Do Not Block TOR

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

13.4 Observation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

14. Anti-Censorship Services

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

14.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

14.2 How to detect and stop

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

15. QUIC! Encrypted UDP Transport

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

15.1 What is it, how does it work, and what's the danger?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

15.2 How to Block

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

15.3 Observation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.

15.4 Observation 2

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/shadowit.