Radically Open Security

Best Practices Guide

Operational Security

V 1.5
Diemen, May 29th, 2020

Document Properties

Title	Best Practices Guide
Version	1.5
Authors	Jan Jaap Vermeulen, Joebin Vahed Monfared, Saif, Collin, Joel and Mohammed Youyou, Joost Agterhoek, Marcus Bointon, Fabian Freyer, Patricia Piolon
Reviewed by	Marcus Bointon
Approved by	Melanie Rieback

Version control

Version	Date	Author	Description
0.9	February 25th, 2020	Jan Jaap Vermeulen, Joebin Vahed Monfared, Saif, Collin, Joel and Mohammed Youyou	Initial draft
1.0	March 2nd, 2020	Joost Agterhoek	Editing
1.1	March 3rd, 2020	Joost Agterhoek	Further edits
1.2	March 4th, 2020	Joost Agterhoek	Added chapter on data minimization
1.3	April 1st, 2020	Marcus Bointon	Review
1.4	May 8th, 2020	Fabian Freyer, Marcus Bointon	Antivirus chapter improvement
1.5	May 29th, 2020	Patricia Piolon	Minor edits and additions

Contact

For more information about this document and its contents please contact Radically Open Security B.V.

Name	Melanie Rieback
Address	Overdiemerweg 28 1111 PP Diemen The Netherlands
Phone	+31 (0)20 2621 255
Email	info@radicallyopensecurity.com

Table of Contents

1 How this guide can help your project

Introduction

This operational security starter document aims to help NGI Zero[1] projects and companies add security to their work culture, promote security awareness, and give people a head start to better secure themselves and their work. In the following chapters you'll find practical tips and concrete solutions for:

- Handling sensitive information
- System segmentation
- Minimize personal data and running code
- Secure download protocols
- Password security
- WiFi security and hacking
- Phishing
- USB safety
- Virus protection
- The importance of backups
- What Edward Snowden thinks about operational security

Each chapter will point you to useful tools and further information to help you improve your everyday operational security.

Please take note: Great care has been given to the content of this guide and best practice guidelines based on current knowledge and expertise. Keep in mind that security is a continual process and new developments will lead to new best practices in the future.

[1] For more information about NGI Zero and the Next Generation Internet initiative, please see the colophon (page 27).

2 Sensitive information

Tips for operational data security

Information security can only be effective when it is an intrinsic part of everyday work culture, regardless of whether you work on your own, collaborate in a (remote) network or environment, or are active in a shared workplace. Many people are still quite lax about the security of sensitive data they are responsible for. Some extra useful tips to secure data are:

- Lock your computer screen or log out from your computer even if you leave just for a moment.
- Encrypt your sensitive data.
- Backup your data, (secure) cloud spaces provide a viable backup option.
- Anti-malware protection is a must.
- Make your old computer hard drives unreadable by wiping the disk and destroying the physical disk.
- Install software updates as soon as possible.
- Automate your software updates.
- Secure your wireless network at your home or business.
- Use a network firewall (IDS+IPS).
- Be careful with opening links and attachments from email addresses you do not recognize.
- Use virtual machines for opening untrusted websites.
- Don’t store unencrypted passwords with your laptop or mobile device.
- Disable file and media sharing if you don’t need it.

3 Segmentation

Isolate your sensitive data

One of the biggest security vulnerabilities in many organizations is the lack of segmentation. If every system can reach every other system and every user can reach every other user, malicious software or intruders can do the same.

Segmentation, also known as compartmentalization, is the discipline of isolating things from each other. It is important to segment roles, documents, information, systems, and networks to protect vital data and infrastructure from attack. Here are tips to segment your organization:

- Only give people access to documents that they actually need for their job.
- Don't give too many roles or rights to one person (for example, letting one person do both the security and security testing of a system).
- Apply a "Default Deny" network rule: Block everything by default, and then explicitly allow access only to the specific services that are needed. This can hurt business continuity but adds a lot of security. Only do this when you have sufficient IT expertise available to maintain the 'white listing'-rules which specify what connections are allowed.
- Segment networks with VLANs, subnets, and routing. You can use an advanced router or firewall to do this.
- Start with easy segments: Guests, Users, Administrators. You can always segment your network more later on. For example, if your organisation adds a new department or premises, you might create a new segment to contain those new users or locations.
- Ensure that future changes do not violate the segmentation strategy. For example: You have two VLANs that cannot talk to each other, but both need to access the same DNS server. This DNS server may leak information about each of the virtual LANs and when hacked, may grant access to both segmented network sections.

4 Data minimization

You cannot leak what you do not collect

Another important principle next to segmentation of roles and user privileges is minimization: minimize the data you collect or process and the code you write and use in your daily business. Data that you do not collect or process cannot be leaked or attract attackers. This approach is one of the data protection principles embedded in GDPR. Beyond the data you handle, reducing the amount of code you write and use reduces the attack surface of your system, or in other words, your Trusted Computing Base (TCB). Here are a few things to keep in mind about minimization and some pointers to useful guides:

- A small TCB means you can easily audit your setup and be reasonably sure it is difficult to breach.
- Build your (online) castle on (complex and shifting) sand: use HTML and Javascript-widgets for example).
- Running your program in a browser may be very user-friendly, but may come at the cost of an enormous and largely unauditable attack surface sensitive to widely used Zero-day vulnerabilities (which hackers can often exploit because the vendor has not patched the vulnerability yet)
- Compartmentalized code isolates privileged processes from non-privileged processes, following the principle of least privilege.
- If you want to know more about data minimization, the GDPR, and when you might be collecting too much (or not enough) personal data, read this guide from the UK's information commissioner
- Data minimization is not just about operational security: 'Datemsparsamkeit' is also good privacy practice
- What happens when you do not compartmentalize properly? Read here how a lack of compartmentalization of accounts can lead to extortion, data loss and online abuse

5 Download protocol

Check your files for viruses

Downloading software from random web sites can lead to an infected computer, as hackers can easily hide malware inside innocent-looking files. Once your computer is infected, a virus can transfer to everybody connected to the same network. This is why it is important to take certain precautions and make sure you download safely.

If you are not sure about a certain file, you can check if it is safe before downloading it. This step-by-step-guide shows how you can make sure there is no malicious code hidden in software you want to download. In other cases you can check in with your IT department (if available) to check any download you are interested in but are unsure of.

Aside from applying common sense, it's good practice to scan all downloads with an up-to-date malware scanner.

6 Password security

Create a strong password (and keep it safe)

This chapter indicates the most common password problems and provides useful tips to avoid them.

National cyber security agencies have guidance on creating passwords and implementing password policies, such as the UK's NCSC, and US NIST agencies.

6.1 What not to do

6.1.1 Easy passwords

Create a password that is easy to memorize, but not so easy that others can guess what it is. Passwords that are too complex for users to remember can lead to sticky notes on a screen that detail exactly how to login somewhere, which is information that you can easily steal.

This is a list of the 25 most used passwords. If your password is in this list, or if your password looks like passwords in this list, please consider changing them ASAP:

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

6.1.2 Social engineering

Don't use your hobbies, pets' or childrens' names, your home town, football club, or anything else that can be easily related to you, as passwords. Hackers will try to obtain clues to these things by reading your social media, LinkedIn, and other sources.

6.1.3 Intuition

Do not create a password that looks or feels insecure. The password `Pa55word!` will pass many password policy checks but is still insecure. Hackers will try such well-known phrases or words when trying to brute-force their way into accounts.

6.1.4 Default passwords

Never keep the default passwords of devices. Always change them. Hackers will try to log in to network devices and accounts with their default passwords, for example:

- Cisco routers use `user:cisco` and `password:cisco` by default.
- Default or newly made accounts often use an `admin` user name combined with a simple password like `password`, `admin`, or even no password at all!

6.1.5 Reuse passwords (don't!)

Never reuse passwords across multiple accounts. Hackers will use passwords they found for one account on other accounts tied to you as well. What's more, they will try passwords that others have used too, because people are often quite predictable!

6.2 What to do

6.2.1 Password manager

The single best thing you can do to improve password security is to use a password manager like KeePass (free, open source, local storage), LastPass (freemium, closed source, online storage) or 1Password. If used correctly, a password manager means you need to remember one strong password to unlock and automatically fill in the many other passwords you have across all your accounts. Your password manager can also generate strong and secure passwords for you, remembering and storing them safely in a vault that you seal with your one master password. You can also use them to synchronise passwords across devices (e.g. so you can access them from your phone and your laptop), keep online backups, share credentials with family or colleagues securely, check passwords (safely!) against known data breaches, and apply rules to flag problems like weak passwords or password re-use.

6.2.2 Passphrases

Generally speaking, longer, simpler passwords are more secure than shorter, more complex ones. To use a famous example, `Tr0ub4dor&3` will pass most rule checks, but it's hard to remember exactly, difficult to type reliably, and is less secure than a longer, less complex password like `correct horse battery staple`. Ideally these words should be chosen randomly, and it's a good exercise to create a mnemonic or other memory device to help you remember it. You can also use complete sentences, however, these are less secure, but you can improve them by

adding simple variation, for example `7t is a truth universally acknowledged`, though non-random sentences are less resistant to "shoulder surfing".

6.2.3 Change your password

Change your password once in a while and also change it if you think that your password is stolen or if you suspect that someone else knows your password. For example, the Have I Been Pwned project can notify you if your email address pops up in a data breach (and yes, it is safe to use!).

6.2.4 Multi-factor authentication

Use multi-factor (i.e. at least 2-factor) authentication using time-based codes from an authenticator app, SMS text messages (though this is considered relatively weak), known-device sign-in approvals (a.g. Apple ID), or hardware U2F keys. For example:

- FreeOTP
- andOTP
- WinAuth
- Aegis
- Microsoft Authenticator
- Google Authenticator
- 1Password
- Yubico U2F keys

Using multi-factor authentication means that your account can't be accessed by someone who obtains your id and password. Many popular online services such as Twitter, Facebook, Google, GitHub, etc support multi-factor authentication.

6.2.5 Updates

Keep your software and especially your password manager up to date. Some examples:

Linux: Use automatic updates (e.g. see the `unattended-upgrades` package for Debian/Ubuntu) or automated cron jobs with update commands. Packages will be automatically updated.

Windows: Use automatic software (or app) updates on a single system. To automate software updates for multiple systems or in cloud spaces, use software like:

- Chocolatey
- System center configuration manager (SCCM)

macOS: ensure that system updates are set to install automatically, allow apps from the Mac app store to update automatically.

While it's possible for problems to be caused by installing updates automatically, the potential for disruption is far smaller than a compromise of your systems.

7 WiFi hacking

The risks of open, public connectivity

This chapter summarizes the risks of using public or open WiFi connections when working remotely. Note that much of this also applies to bluetooth.

7.1 Threats

7.1.1 Who owns the connection?

Users often don't know who's in charge of the WiFi-network infrastructure or access point and what these parties can actually see in their network traffic. Secret personal or company documents could possibly get leaked or stolen by tracking and extracting data from these open connections, which can be harmful to people and companies.

7.1.2 Hackers/crackers

Users of free public WiFi aren't just at risk from anyone misusing their admin powers. They are also at risk from anyone using the same network that tries to snoop what they are doing. Malicious parties can possibly intercept and steal your precious data and information.

7.2 Protection

There are ways to protect yourself against these threats:

7.2.1 Virtual private networks

A virtual private network or VPN can connect you securely and privately by creating an encrypted 'tunnel', which makes other people using the same WiFi unable to see any data you are sending over the network. There are many service providers offering easy-to-setup virtual private networks, each with their own benefits and downsides. For a comprehensive overview, check out That One Privacy Site.

VPNs give you *some* control over who can see your data, but consider that while a VPN may hide traffic on your local WiFi network, it instead exposes it to the VPN operator (especially if the sites you're visiting don't use TLS), so you need to be sure you can trust the operator, something which can be very difficult to evaluate. If that's critical, you can run your own VPN server, though that carries its own risks.

7.2.2 The Onion Router (Tor)

The Tor Project site project provides a way of hiding your origin and identity without relying on trusted third parties (such as VPN providers), by tunnelling your traffic through anonymous secure connections. It's most often used through a specially adapted web browser, but it's possible to also use it much like a VPN for other kinds of traffic.

7.2.3 Not using WiFi? Turn it off!

Turn off your WiFi when you are not using it, especially when travelling. That way your WiFi connectors don’t scream for possible connections with networks around you. These transmissions can be picked up and reveal additional information about where you are and what you are doing. You'll also improve battery life!

8 Phishing

Untrusted messages

8.1 What is phishing?

Phishing is a cyberattack where an attacker tries to trick a victim by sending them a message, usually in the form of an email that tries to pass as being from a trustworthy entity like a bank, or someone they know. The attacker tries to obtain some kind of sensitive information such as login credentials or personal information that facilitates identity theft, usually by providing a link to a fake site that looks like a regular login page.

8.2 Different forms of phishing

Phishing comes in a lot of different forms:

- Normal phishing: A fake message containing a malicious link.
- Vishing: Phishing with an invoice, voicemail message, or by simply calling the target over the phone. SIM-swapping through a provider is one example of this.
- Spearphishing: Phishing directed at a specific target.

8.3 How to recognize and stop phishing

In order to protect yourself and the people around you against phishing, education is essential. You have to first be aware of this problem and be able to recognize certain characteristics of such attacks.

- Public domains: One recognizable characteristic is that a lot of phishing messages are sent from a publicly accessible and usable email domain (think @gmail.com). Organizations and companies usually have their own domain name for email.
- Trusted sources: Some phishing mail can also be sent from trusted domains and sources. If one of your colleagues or friends is hacked, the hacker can send mails from their account as well. These attacks are very effective because people tend to trust their colleagues and friends.

8.4 Grammar & spelling

Another characteristic of phishing mail is grammatical errors and unusual phrases. Here you can see a phishing example with bad spelling and grammar:


ING

ING storing verholpen

Samen met onze klanten stappen wij over op nieuwe servers

Beste klant,

ING Bank Nederland heeft gister problemen ondervonden door een technische storing. Hierdoor kunt u problemen hebben gehad met uw toegang tot Mijn ING of andere ING betaaldiensten. Onze excuses voor het ongemak, het probleem is inmiddels opgelost.

Let op: Meld u binnen twee weken aan voor de nieuwe servers

Om soortgelijke storingen in de toekomst te voorkomen, stapt de ING Bank, samen met onze klanten, over op nieuwe servers. U dient zich binnen twee weken aan te melden op de nieuwe servers. Aanmelden voor de nieuwe servers kunt u regelen met één gemakkelijke klik op de knop, en is geheel vrij van kosten! Bent u op vakantie of kunt om andere redenen op dit moment niet inloggen op Mijn ING? Dan verzoeken wij u telefonisch contact op te nemen met 0900 7000 (0,80 euro p/m)

Aanmelden op de nieuwe servers

U kunt zich nu direct aanmelden met bovenstaande button. U wordt doorgeleid naar een beveiligde internetpagina van de ING Bank Nederland. Nadat u zich heeft aangemeld, hoeft u verder geen actie te ondernemen.

Hartelijk dank voor uw medewerking

Met vriendelijke groet,

ING Bank N.V.
Afdeling IT zaken

Deze e-mail is afkomstig van ING Bank N.V., statutair gevestigd te Amsterdam, Handelsregister nr. 33031431.

These errors are often deliberate – those likely to spot the mistakes are also less likely to fall for the scam, so it's a kind of cynical pre-filter for the scammers to avoid wasting time on the less gullible.

Be sure to read the email properly and don't just trust that whoever sends that mail is who he says he is. Some messages can come from abroad, like the well-known Nigerian "419" scams. The victim is promised something like a large sum of money, but needs to share some information or payment beforehand. By properly reading and checking the mail for errors, you can spot some of these phishing mails.

8.5 Attachments

Phishing mails also often include some kind of suspicious attachments or links. This could be a malware-infected work document like a PDF or Word-file. You will be asked to download the file and open it, or to click a link to another malicious website where you have to login or leave some sensitive information. Essentially you should never open an attachment unless you are certain where the email comes from.

8.6 Call to action

Another common attribute of phishing messages is an urgent call to action, for example "You must log in to your account within the next 24 hours or your account will be deleted". In spearphishing, it might be a message from the victim's boss asking them to make an urgent payment. Inducing a sense of fear may make it more likely that victims bypass

procedural controls. Such calls to action should provoke a sense of suspicion rather than urgency, so be careful to scrutinize such messages and verify them via other channels (e.g. call your boss) before taking action. Better safe than sorry!

8.7 How to prepare for and prevent phishing

Spam filters will never completely get rid of phishing messages. Which is why it is better to prepare for them and learn how to protect yourself and the people you work with. Here are some useful tools and concrete pointers:

- Deploy strict DKIM, DMARC and SPF checks on inbound mail servers. In the past it was relatively easy for attackers to fake messages from real domains, but these checks (which are applied at the domain level, rather than per-user) not only make it very difficult, they can also report the malicious activity to the domain owners. That said, passing these checks does not necessarily mean that messages are safe, but messages that fail them should raise immediate suspicion.
- Hover over a link before clicking it to see the actual link destination. Never log in to an unsecured "http" site, verify that the website link is "https" instead, though scammers are getting better at making use of such measures. Watch out for shortened links like `bit.ly` or `goo.gl` which are often used to disguise real destinations.
- Use anti-spam solutions, these can be as simple as Outlook or Gmail “spam” folder or more thorough commercial scanning services.
- Make use of multi-factor authentication; this doesn't make it any less likely that your credentials will be obtained, but it prevents them being used if they have.
- Educate your project, organization or company on phishing. Tell them to report it to you or a security department if they think that they have been phished.
- Thank everyone who reports spam or phishing attempts to you. This motivates users to help you and adopt security as part of their own work culture while making them less afraid to inform you about security breaches. Don't forget: users usually see these mails first!

8.8 Help, I have been phished!

- Notify your security team (if you have one)
- Change any passwords you may have revealed
- Disconnect your WiFi and network until you have scanned your computer
- Scan your computer for viruses

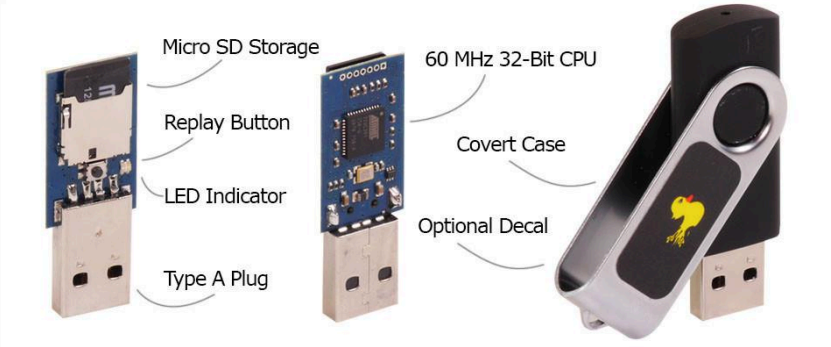
9 USB

Peripheral devices and what can go wrong

Universal Serial Bus (USB) is a standard for connecting peripheral devices to computers. So how can a USB be a security issue?

There are different examples of USB vulnerabilities relating to three types of devices:

- USB flash drives are meant for storage – but they can store malware equally well.
- USB devices can provide network connectivity, possibly allowing external connections and exfiltration of data.
- Devices that look like USB flash drives can actually act as input devices like keyboards and mice, and when connected to your computer can start typing key sequences and clicking buttons. Many operating systems automatically trust USB input devices and allow their connection and operation without requiring any user interaction. Below is an example:



- "USB killers" when plugged in store a small amount of power in capacitors and send this energy back to the device, repeating this process until the computer is fried. This destroys the input/output-controller often built into the motherboard and can cause damage elsewhere too.

9.1 Safe USB

- Encrypt your USB-drives with software. You can use Bitlocker on Windows 10 and the gnome-disk-utility on (Ubuntu) Linux.
- Lock down your USB-ports on your machine. There are mainly three ways to do this:
  - 'Turn off' USB in the BIOS/UEFI-firmware settings of your device.
  - You can physically plug your USB-ports with USB-port locks.
  - Block USB-ports within Windows (use group policies) or Linux ((USBguard).

- Scan every USB-drive you use with an antivirus tool.
- Don’t throw away a USB-drive when data is still on it. Sensitive documents are known to be retrieved this way. Clean or wipe the drive first, though be aware that simple deletion is not sufficient, and really deleting data can be surprisingly difficult. If data is very sensitive, physically destroy the device.

10 Antivirus

The advantages and disadvantages of anti-virus software (AV) are controversial. While AV can mitigate against some threats, it also introduces significant additional attack surface (see TCB) and potential for data leakage. These tradeoffs need to be considered carefully when evaluating whether it is sensible to use AV. We cannot therefore give a simple recommendation for or against using AV, but instead aim to give a more nuanced view on the topic. Most importantly, **AV does not provide a comprehensive defence against all kinds of threat**. If you follow our other advice in this document (including security updates, compartmentalization, least privilege, and not using files from untrusted sources), you will probably not benefit greatly from AV.

10.1 What is Malware?

The definition of malware varies according to perspective, and what it actually does can vary enormously. It may consume your resources (e.g. CPU power for cryptomining), steal your data for use in identity theft, encrypt your data and hold it to ransom, steal credentials to try to gain access to other systems, and many other things. Malware typically consists of malicious or unwanted applications, code, or software that is run without your knowledge, or by pretending to be something useful. It can represent a serious threat and can be well-hidden on your system or distributed throughout your network via multiple methods. Unfortunately not all malware will or even can be detected by popular operating and AV systems. Spouseware, adware, government backdoors and trojans, and other grey-area programs that might be considered malware by users are often not considered as such by AV vendors.

10.2 How does AV protect you?

10.2.1 Signature-based AV

The most basic AV engines will compare parts of files they scan against a database of known-malicious "signatures". These signatures are regularly downloaded by the AV software and need to be kept up-to-date to be able to recognize newer malware. This is effective against **known** (i.e. old) malware, but signature-based AV is trivial to bypass by changing the bytes that are detected by the AV, so fresh strains will evade most AV. Underground commercial services exist that help malware writers to change their products so they are not detected any more, and some malware may modify itself when it is run in order to evade signature matches – for example if a virus emails itself to everyone in your address book, it may alter itself so that every copy that is sent is different.

The detection abilities of commercial AV are by definition public – anyone can buy and use the software – so malware authors are able to test detection of their code before launching attacks, making this whole process an arms-race that AV cannot (and doesn't want to for the sake of their profits) win.

10.2.2 Heuristics

Many AV engines run files they encounter in an emulator and/or sandbox (a way of running software that is isolated from your real system, and thus able to prevent it from causing damage). They record the behaviour, i.e. what a piece of software does when run, and use some heuristics to decide whether these actions are malicious or not. This means that to some extent, AV engines can detect malicious files they have never seen before. However, malware writers are aware of this, and there are techniques to detect and evade such emulators and sandboxes, making the process an arms race between malware and AV authors.

10.2.3 Unpacking

Malware authors often "pack" their malware in multiple layers of obfuscation, compression, and encryption to evade detection by antivirus engines and inhibit analysis by reverse engineering. Therefore, most antivirus engines will recursively unpack files they encounter when scanning. Often this includes opening or executing a file inside an emulator or sandbox. This process in itself can be a vulnerability, consuming excessive memory and disk space.

10.3 What risks does AV pose?

10.3.1 Additional attack surface

AV runs as a privileged user so it can usually access all files and investigate the state of your system, and can upload and download arbitrary files from the internet. This makes AV engines a prime target for attacks. The unpackers, emulators, and virtual machines that execute malware in sandboxed environments are very complex and have a history of serious vulnerabilities being found in them. These threats are especially important when attempting to protect against skilled or well-resourced attackers (e.g. state actors).

10.3.2 Data leakage

To keep signatures and heuristics up to date, antivirus companies rely on continuously capturing and analysing a wide variety of malware seen "in the wild". But how do they get these malware samples? Many antivirus engines will upload files they deem suspicious (but might be legitimate and private!) to their producers to be analyzed. Antivirus companies often share malware samples they have identified with others, and public sample sharing sites such as VirusTotal exist for user-submitted samples. Some paid or business versions of AV engines may allow different configurations, but these are usually targeted at larger companies with internal security teams reviewing suspicious files. Depending on your

threat model and privacy needs, automated sample submissions, and other telemetrics may compromise your security or privacy.

10.3.3 Alternatives

If you want to check manually whether a file (that you don't mind sharing publicly) is recognized as malicious by AV engines, you can use online services such as VirusTotal. These services will scan uploaded files using multiple AV systems, but since the AV engines are not running on your system, it does not expose any additional attack surface. Furthermore, you need to make a conscious decision to share the file, so it does not represent an unexpected privacy exposure.

To further lock down your system, you can employ binary white-listing or code-signing. These allow you to limit the software that can run on your system.

If you follow the other recommendations in this guide, most importantly to ensure your system always applies the latest security patches automatically, and to not download programs from sources other than known vendors, you should be protected against most of the threats that AV protects against without the associated risks of running AV.

11 Backups

How to defend against ransomware

Regular backups are an important part of a secure IT infrastructure. Backups largely prevent damage from attacks with ransomware, which is a growing threat for organizations and businesses right now. Follow these tips to increase your backup efficiency:

- Make the backup process as simple as possible – see Apple's Time Machine system for a great example; manual backups get forgotten.
- Let the backup server and the backup client authenticate each other, so that a hacker cannot set up a rogue backup server.
- Check if the backup task is actually running from time to time.
- Check once a year if you can 'roll back' your backups, i.e. that a restore process actually works.
- Check if your backup procedures are clear and easy to follow in case of emergency so that a quick recovery of all data can be achieved. This is a must against ransomware attacks.
- Keep your backup software (client and server side) up to date.
- Keep your backup infrastructure (servers and network) up to date.
- Create a on-site and off-site backup. You can use a cloud provider like Microsoft Azure or Amazon S3 for cloud backup servers, or a dedicated online backup service such as Backblaze.
- Don't make your backup servers directly accessible from the internet or from other networks that should not be able to reach it.
- Encrypt your backups so that they can't be used if access to them is obtained by unauthorised users.
- Test your backup infrastructure for security regularly, or hire a security specialist to do this for you.
- Do a risk assessment on your data. Critical data needs more frequent backups, while this may not be worth the effort for other information on your systems. Company documents can have invaluable worth for an organization, while any file that is freely available on the internet can be downloaded again after a system wipe.
- Struck by ransomware? Your encrypted files might still be saved. The No More Ransom project has created a repository of keys and applications that can decrypt data locked by various known types of ransomware. This initiative of the Dutch police, Europol's European Cybercrime Center, McAfee and Kaspersky offer decryption tools to victims of ransomware attacks and also aims to educate users how to protect themselves against infection.

12 Want to learn more?

Useful operational security guides

Here are some useful operational security guides and other sources for further information and protection of your systems and data.

- Digital Guardian – What is Operational Security? The Five-Step Process, Best Practices and More
- National Cyber Security Centre – Small Business Guide: Cyber Security
- ESET – Guide to Small Business Cybersecurity
- TechRepublic – The five militairy OPSEC steps that businesses can learn from
- Open Banking – Participant guide: information security operations
- The Intercept – Edward Snowden Explains How to Reclaim Your Privacy

Appendix 1 Colophon

This operational security starter document was developed to help projects funded by the NGI Zero Discovery and NGI Zero PET programs, which are part of the Next Generation Internet research and development initiative. This guide can also help readers add security to their work culture, promote security awareness, and give people a head start to better secure themselves and their work.

Front page styling by Patricia Piolon