

7 types of virus – a short glossary of contemporary cyberbadness

28 DEC 2019



by Paul Ducklin

OK, technically, this article is about malware in general, not about viruses in particular.

Strictly speaking, *virus* refers to a type of malware that spreads by itself, so that once it's in your system, you may end up with hundreds or even thousands of infected files...

...on every computer in your network, and in the networks your network can see, and so on, and so on.

These days, however, the crooks don't really need to program auto-spreading into their malware – thanks to always-on internet connectivity, the "spreading" part is easier than ever, so that's one attention-grabbing step the crooks no longer need to use.

But the word *virus* has remained as a synonym for malware in general, and that's how we're using the word here.

So, for the record, here are seven categories of malware that give you a fair idea of the breadth and the depth of the risk that malware can pose to your organisation.

To jump to a specific item, click in the list below:

- 1. [KEYLOGGERS](#)
- 2. [DATA STEALERS](#)
- 3. [RAM SCRAPERS](#)
- 4. [BOTS, aka ZOMBIES](#)
- 5. [BANKING TROJANS](#)
- 6. [RATS \(Remote Access Trojans\)](#)
- 7. [RANSOMWARE](#)
- 8. [WHAT TO DO?](#)

1. KEYLOGGERS

Keyloggers are surprisingly simple, and can be implemented in many different ways.

Simply put, they hook into the stream of data that comes from your keyboard, allowing them to tell [what you typed](#) and when.

In fact, keyloggers often don't merely know "you typed F" – they get enough detail to tell that you pressed the left Shift key down, then depressed F, then released F, then let go of the shift.

That means they can even keep track of keystrokes that don't produce any visible output, such as function keys, backspaces and other key combinations that turn options on or off.

Importantly, keyloggers don't always need to be implemented down at the operating system level, and they often don't need administrative or root powers to hook themselves into the keystroke data stream.

For example, JavaScript code inside your browser can monitor (and alter, if it wants) the flow of keystrokes as you browse, meaning that rogue JavaScript injected into a login page could, in theory, recognise and steal your usernames and passwords.

Banking trojans [\[q.v.\]](#) very commonly include a keylogger module so they can try to capture your passwords when they recognise that you're in the middle of logging in to your bank.

Interestingly, keyloggers also exist in hardware form – a tiny device that's connected between an external keyboard and the computer port it's plugged into.

Hardware keyloggers can't reliably be detected by software (they usually just identify themselves to your computer as a regular keyboard), but they can often be spotted by [visual inspection](#) of your normal keyboard or cable.

2. DATA STEALERS

A data stealer is malware that does pretty much what its name suggests: it goes hunting around your hard disk, and perhaps even around your whole network if it can, looking for files that contain [data that's worth money](#) to the crooks.

In the early days of malware, most attacks were true computer viruses, meaning that they spread automatically by themselves, often by spewing out emails containing an infected attachment.

Back then, many viruses included a data-matching toolkit that went through pretty much every file on your computer looking for text strings that matched a pattern such as `[spaces][alphanumeric]{A}[alphanumeric]{DOT}[alphanumeric]{}`, on the reasonable assumption that this was probably an email address.

By deliberately harvesting email addresses from everywhere, not just from your email software, they came up with extensive lists of potential new victims, even people whom you'd never contacted but whose addresses showed up in documents, marketing material, or saved pages from websites.

These days, the crooks are interested in much more than email addresses to steal – anything that can be reduced to a text-matching pattern is surprisingly easy to hunt out and thief, including bank account details, ID numbers, passport data, credit cards and account passwords.

Data stealers also know how to recognise special files by their name or their internal structure, such as password vaults that contain login details, and browser databases that may contain tell-tale data such as authentication tokens and browsing history.

Many other types of malware, notably bots [\[q.v.\]](#) and banking trojans [\[q.v.\]](#), include data stealing modules as one useful way of extending their criminality.

3. RAM SCRAPERS

Malware can't always find what it wants in files on your computer, even if the malware itself already has administrator or root level access.

That's because some data only ever exists temporarily in memory, and then gets scrubbed without ever reaching disk.

One reason for that concerns data security regulations such as [PCI-DSS](#), the Payment Card Industry Data Security Standard, and [GDPR](#), the European General Data Protection Regulation.

Those regulations say that there are some data items you simply aren't allowed to keep after you've finished with them – you should use them only at the moment you need them, and then get rid of them forever.

An obvious example is the CVV number (the short code) on the back of your credit card – that code is used to authorise a transaction but should never be saved to disk or otherwise retained beyond that point.

That's bad news for cybercrooks, because it means they can't easily get hold of CVV codes for transactions that have already happened...

...but with RAM scraping malware that keeps an eye on data as it is stored temporarily in memory, the crooks may be able to [identify critical data](#) such as CVVs and full credit card information and "scrape" it straight out of RAM.

Other secret data often appears in RAM, albeit briefly, such as decryption keys, plaintext passwords and website authentication tokens, and RAM scrapers can watch for these, too.

4. BOTS, aka ZOMBIES

A bot, short for *robot program*, is malware that opens a backdoor into your computer so that crooks can send it commands from afar.

A collection of bots is known, in turn, as a botnet, short for *robot network*, and crooks who control an army of networked bots can command them remotely all at the same time, with much more dramatic results than just having control over one or two computers on the internet.

Bots are also commonly known as *zombies*, because they act a bit like "sleeping agents" that the crooks can [turn against you](#) on demand.

Commands often built into bots include: sending spam in [vast quantities](#), searching locally for files, sniffing out passwords, attacking other people's websites, and secretly [clicking online ads](#) to generate pay-per-click revenue.

One important thing to remember about bots is that they don't rely on the crooks connecting *inwards* to your computer to send them commands, so they aren't automatically blocked by your home router, which usually prevents all incoming network connections.

Most bots work by regularly calling home, only ever making *outbound* connections – something your home router probably does allow – and downloading the latest list of commands published by the crooks.

Another important fact about bots is that almost every bot ever released includes a command that allows the crooks to upgrade or even to replace it whenever they want.

Sadly, that means it's hard to predict in advance what damage crooks might do to your computer if you find you're infected with a bot, because it could have been doing something else yesterday and might move on to a completely new attack tomorrow.

5. BANKING TROJANS

This is the general term for malware that goes after information about your online banking.

As you can imagine, banking trojans typically include a keylogger [\[q.v.\]](#) component, to sniff out passwords as you type them in.

They also often have a data stealer [\[q.v.\]](#) part to trawl through likely files such as browser databases and password vaults in the hope of finding unencrypted passwords or account details.

Another trick widely used by banking trojans is known as *web form injection*, where the malware sneakily adds extra data fields into forms that are displayed in your browser.

By doing this they hope to trick you into entering additional data, such as your credit card number or date of birth, at a point where you wouldn't normally be asked such questions.

Perhaps the best known name in the banking trojan scene is [Gozi](#), a large and loosely-defined family of malware that first appeared more than a decade ago.

The original Gozi source code was published online many years ago, and this threat family has [proliferated and evolved](#) ever since.

6. RATS

The name RAT is short for Remote Access Trojan, typically the sort of remote access tool that lets creeps spy on you by taking surreptitious screenshots or secretly turning on your webcam.

The best-known RAT is probably Blackshades, which made the headlines a few years ago when a variant of this malware family was used by a cybercriminal called Jared James Abrahams to spy on hundreds of women, including then [Miss Teen USA](#), Cassidy Wolf.

Abrahams ended up with an [18-month prison sentence](#); the [authors](#) and [distributors](#) of the Blackshades malware itself were variously arrested and convicted, too.

One question that RATware often raises is, "Can a malware author activate my webcam without the light turning on?"

The answer is, "It depends."

Some webcams have their LED wired in with the webcam itself, so that it comes on with the webcam no matter what; others have the LED set up so that it can be programmed independently of the webcam, and on this sort of webcam you could, in theory at least, record without any visible sign.

If in doubt, a [webcam cover](#) or a tiny piece of [electrical tape](#) will provide you with a web shield that malware can't deactivate!

7. RANSOMWARE

This is probably the most feared sort of malware of the past decade: generally speaking, ransomware scrambles all your files, uploads the one-and-only copy of the decryption key to the crooks, and then offers to sell you back the decryption key so you can unlock your computer and get back to work.

In an ideal world, ransomware wouldn't work for the crooks at all, because you'd simply wipe your computer clean (handily removing the ransomware at the same time), restore your most recent backup, and be up and running without paying the crooks anything.

But life is seldom that simple, and today's ransomware crooks maximise their leverage against you in several ways:

- **They usually find a way into your network first, so they can scramble hundreds or even thousands of computers at the same time.** Even if you have backups for all of them, reimaging and restoring thousands of computers might take longer than just paying up.
- **They look around for online backups on the network, and wipe them out in advance of the ransomware attack.** Unless you have a reliable process of regularly making and keeping offline backups, the crooks may have you over a barrel.
- **They spend time researching your cybersecurity setup first so they can turn off parts that might stop or limit the ransomware.** Never ignore anything in your logs that looks like unusual or unexpected changes to network security settings – it might be crooks loosening you up for attack.

Ransomware demands have risen dramatically since 2013, when the [CryptoLocker ransomware](#) extorted \$300 per computer.

Modern ransomware attacks such as [SamSam](#), [Bitpaymer](#) and [Ryuk](#) typically take out whole networks and demand anywhere from \$50,000 to \$5,000,000 to undo the damage across an entire infected network.

8. WHAT TO DO?

- **Patch early, patch often.** A lot of attacks start because someone, somewhere, has left a security hole open that the crooks already know how to exploit. Even if you're using automated updating everywhere, check up on the state of your patching regularly – if you don't check your own networks, the crooks will do it for you!
- **Look for and act on warning signs in your logs.** Many malware attacks last for some time, or follow up on previous warnings or "scouting expeditions" that leave telltale signs in your logs. The unusual creation of new accounts; the use of administration tools where you wouldn't expect them; and evidence of someone fiddling about with security settings should always be investigated. Authorised staff should know better, and can be counselled accordingly; unauthorised users can be identified and booted off the system sooner rather than later.
- **Go for defence in depth.** Look for an anti-virus with behaviour-blocking and web filtering as well as plain file scanning. Most modern malware attacks involve a sequence of small steps. The crooks have to succeed at every step to complete their attack, whereas you can often stop the attack by blocking any one of the stages.

While you're about it, why not check out and subscribe to our weekly [Naked Security podcasts](#) and to our new [Naked Security YouTube channel](#)?