

Trends 2018: The ransomware revolution

BY **DAVID HARLEY** POSTED 7 MAR 2018 - 02:52PM



This is actually where I came in, [nearly 30 years ago](#). The first malware outbreak for which I provided consultancy was Dr. Popp's extraordinary [AIDS Trojan](#), which rendered a victim's data inaccessible until a 'software lease renewal' payment was made. And for a long time afterwards, there was not much else that could be called ransomware, unless you count threats made against organizations of persistent [DDoS \(Distributed Denial of Service\)](#) attacks.

All-too-plausible deniability

While Denial of Service attacks amplified by the use of networks of bot-compromised PCs were becoming a notable problem by the turn of the century, DDoS extortion threats have accelerated in parallel (if less dramatically) with the rise in ransomware in the past few years. However, statistics may be obscured by a reluctance on the part of some victim organizations to speak out, and a concurrent rise in DDoS attacks with [a political dimension](#) rather than [a simple profit motive](#). There are other complex interactions between malware types, though: there have been [instances](#) of ransomware variants that incorporated a DDoS bot, while more recently the charmers behind the Mirai botnet [chose](#)

to [DDoS](#) the WannaCryptor (a.k.a. WannaCry) “kill switch” in order to allow dormant copies of the malware to reactivate.

The worm turns

Of course, there’s [a great deal more](#) to the malware ESET calls [Win32/Filecoder.WannaCryptor](#) than the Mirai factor. The combination of ransomware and worm accelerated the spread of the malware, though not as dramatically in terms of sheer volume as some of the worm attacks we saw in the first decade of the millennium, partly because its spread was reliant on a vulnerability that was already widely patched. However, its financial impact on major organizations caught the attention of the media worldwide.

Pay up! and play *our* game*

One of the quirks of WannaCryptor was that it was never very likely that someone who paid the ransom would get all their data decrypted. That’s not unique, of course: there are all too many examples of ransomware where the criminals were unable to recover [some](#) or [any](#) data because of incompetent coding, or [never intended to enable recovery](#). Ranscam and [Hitler](#), for example, simply deleted files: no encryption, and no likely way the criminal can help recover them. Fortunately, these don’t seem to have been particularly widespread. Perhaps [the most notorious example](#), though, is the Petya semi-clone ESET detects as [DiskCoder.C](#), which *does* encrypt data. Given how competently the malware is executed, the absence of a recovery mechanism doesn’t seem accidental. Rather, a case of ‘take the money and run’.

Wiper hyper

While the DiskCoder.C malware sometimes referred to as NotPetya clearly doesn’t eschew making some profit by passing itself off as ransomware, other ‘wipers’ clearly have a different agenda, such as the (fairly) recently revived Shmoon malware. Malware with wiper functionality aimed at Ukraine include KillDisk ([associated with BlackEnergy](#)) and, more recently, one of the payloads deployed by [Industroyer](#).

What can you learn from these trends?

Holding your data to ransom is an easy way for an attacker to make a dishonest profit, and destroying data for other reasons such as a political agenda seems to be on the rise. Rather than speculate about all the possible variations on the theme of data mangling, let’s look at [some measures](#) that [reduce the risk](#) across the board.

1. We understand that [people choose to pay](#) in the hope of getting their data back even though they know that this encourages the criminals. Before paying up, though, check with your security software vendor (a) in case recovery may be possible without paying the ransom (b) in case it’s known that paying the ransom won’t or can’t result in recovery for that particular ransomware variant.

2. Protecting your data proactively is safer than relying on the competence and good faith of the criminal. Back up everything that matters to you, often, by keeping at least some backups offline – to media that aren't routinely exposed to corruption by ransomware and other malware – in a physically secure location (preferably more than one location). And, obviously, backups defend against risks to data apart from ransomware and other malware, so should already be part of a disaster recovery plan.
3. Many people and organizations nowadays don't think of backup in terms of physical media like optical disks and flash storage, so much as in terms of some form of cloud storage. Which are very likely to be offsite, of course. Remember, however, where such storage is 'always on', its contents may be vulnerable to compromise by ransomware in the same way that local and other network-connected storage is. It's important that offsite storage:
 1. Is not routinely and permanently online
 2. Protects backed-up data from automatic and silent modification or overwriting by malware when the remote facility is online
 3. Protects earlier generations of backed-up data from compromise so that even if disaster strikes the very latest backups, you can at least retrieve some data, including earlier versions of current data.
 4. Protects the customer by spelling out the provider's legal/contractual responsibilities, what happens if the provider goes out of business, and so on.
4. Don't underestimate the usefulness of backup media that aren't rewriteable/reusable. If you can't modify what's been written there, then neither can ransomware. Check every so often that your [backup/recovery operation](#) is (still) working properly and that your media (read-only, write-disabled, or write-enabled) are still readable (and that write-enabled media aren't routinely writeable). And back up your backups.
5. I'm certainly not going to say that you should rely on backups instead of using security software, but bear in mind that *removing* active ransomware with security software that *detects* ransomware is by no means the same as recovering data: removing the ransomware and then deciding to pay up means that the data may no longer be recoverable even with the cooperation of the criminals, because the decryption mechanism is part of the malware. On the other hand, you certainly don't want to restore your data to a system on which the ransomware is still active. Fortunately, safe backups can save your data if/when something malicious slips past your security software.

And the future?

"Don't make predictions about computing that can be checked in your lifetime" – wise words from [Daniel Delbert McCracken](#). Still, we can risk some extrapolation from the recent evolution of ransomware in order to offer some cautious thoughts about its future evolution.

Targeting

The AIDs Trojan was pretty specific in its targeting. Even then, not many people were interested in the minutiae of AIDS research, distribution of the Trojan by floppy disk was relatively expensive, and the mechanism for paying the ransom didn't really work to the attacker's advantage. (Of course, in 1989 Dr. Popp didn't have the advantage of access to cryptocurrency or the Dark Web, or easy ways to use Western Union (the 419 scammer's favorite) or to [monetize nude photographs](#).)

The attack itself was 'classic' ransomware, in that it deprived the victim of his or her data. Later, DoS and DDoS attacks deprived companies of the ability to benefit from the services they provided: while customers were deprived of those services, it was the provider who was expected to pay. However, as the non-corporate, individual use of the Internet has exploded, the attack surface and the range of potential targets have also widened. Which probably has an influence on the promiscuous distribution of most modern ransomware.

Non-targeting

While the media and security product marketers tend to get excited when a highly visible or high-value victim is disclosed – healthcare sites, academic institutions, telephony service providers, ISPs – it's inappropriate to assume that these institutions are always being specifically targeted. Since we don't always know what vector of compromise was used by a specific campaign, we can't say 'It never happens!'. But it looks as if ransomware gangs are doing quite nicely out of payments made by large institutions compromised via lateral attacks from employees who have been successfully attacked when using their work accounts. The UK's NHS Digital, for example, [denies](#) that healthcare is being specifically targeted – a view I happen to share, in general – while acknowledging that healthcare sites have 'often fallen victim'.

Could this change?

At the moment, there still seem to be organizations that are prepared to spend relatively large sums in ransom payment. In some cases, this is a reasonable 'backup strategy', acknowledging that it's sensible to keep a (ransom)war(e) chest topped up in case technical defences fail. In other cases, companies may be hoping that paying up will be more cost-effective than building up complex additional defences that cannot always be fully effective. That in itself may attract targeting of companies perceived to be a soft touch or especially able to pay (financial organizations, casinos). The increased volume of wiper attacks and ransomware attacks where payment does *not* result in recovery may mitigate this unhealthy trend, but companies that are still perceived as unlikely to harden their defences to the best of their abilities might then be more specifically targeted. It is, after all,

likely that a successful attack on a large organization will pay better and more promptly than widespread attacks on random computer users and email addresses.

Data versus Devices

Looking at attacks on smartphones and other mobile devices, these tend to be less focused on data and more on denying the use of the device and the services it facilitates. That's bad enough where the alternative to paying the ransom may be to lose settings and other data, especially as more people use mobile devices in preference to personal computers and even laptops, so that a wider range of data might be threatened. As the Internet of Unnecessarily Networked Things becomes less avoidable, the attack surface increases, with networked devices and sensors embedded into unexpected items and contexts: from [routers](#) to [fridges](#) to [smart meters](#), from [TVs](#) to [toys](#), from [power stations](#) to [petrol stations](#) and [pacemakers](#). As everything gets 'smarter', the number of services that might be disrupted by malware (whether or not a ransom is demanded) becomes greater. In previous years we've discussed the possibilities of what my colleague Stephen Cobb calls the [Ransomware of Things](#). There are fewer in-the-wild examples to date of such threats than you might expect, given the attention they attract. That could easily change, though, especially if more conventional ransomware becomes less effective as a means of making a quick buck. Though I'm not sure that's going to happen for a while...

On the other hand, there's not much indication that Internet of Things security is keeping pace with IoT growth. We are already seeing plenty of hacker interest in the monetization of IoT insecurity. It's not as simple as the media sometimes assume to write and distribute malware that will affect a wide range of IoT devices and beyond, so there's no cause for panic, but we shouldn't underestimate the digital underworld's tenacity and ability to come up with surprising twists.