The hidden backdoor: how droppers spread malware

Executive summary

One of CERT-UK's roles is to promote cyber-security situational awareness across industry, academia, and the public sector. This paper aims to increase understanding of how malicious actors use droppers and downloaders, how they work, what their role is in malware distribution, and how they can be detected and defended against. We hope to provide clarity to those non-technical readers about this aspect of malware and how it actually gets from the internet to your computer.

Droppers are small pieces of code that initialise a foothold onto the system that can be used to install malicious code onto a target computer. They can be a delivery vehicle integral to criminal malware campaigns and, despite having some legitimate usage, it is possible to reduce risk of infection from malware by defending against them.

Droppers come in many forms and are often a part of another piece of malware, or a group of malware brought together to create more comprehensive functionality, otherwise known as a malware suite.

The great advantage to criminals of the more complex droppers is that they need minimal technical knowledge to use, and so minimal user interaction; many are even available as malware-for-hire from online criminal enterprises. Unfortunately, the commonality of function means it can be very difficult for automatic systems to distinguish between genuine and malicious droppers. However, depending on risk appetite, there are steps businesses can take to reduce the risk of infections.

Using droppers to spread malware

In order for an attacker to get the dropper onto the target's computer, the victim needs to be deceived into some sort of interaction to install it by clicking a link or opening a malicious attachment in a phishing email[1]. Other methods can be even less obvious, like a 'drive-by-download' where a webpage automatically forces a download via the web browser. These methods can be preferable to an attacker as they do not have to force their way through defences; the users themselves unwittingly invite them inside.

Once the dropper has been delivered to the target computer, it will normally seek to gain administrator rights. Administrator rights are required to make system changes, such as installing or uninstalling programs, and the dropper will be installed with the rights of whichever user they infected. With these elevated privileges, it can then attempt to install a 'backdoor' through which the attacker can have access (via the internet) to the victim computer, even after the dropper has been removed. More advanced droppers will also then try to deactivate anti-virus programs and firewalls without notifying the user, further reducing the defences on a computer.

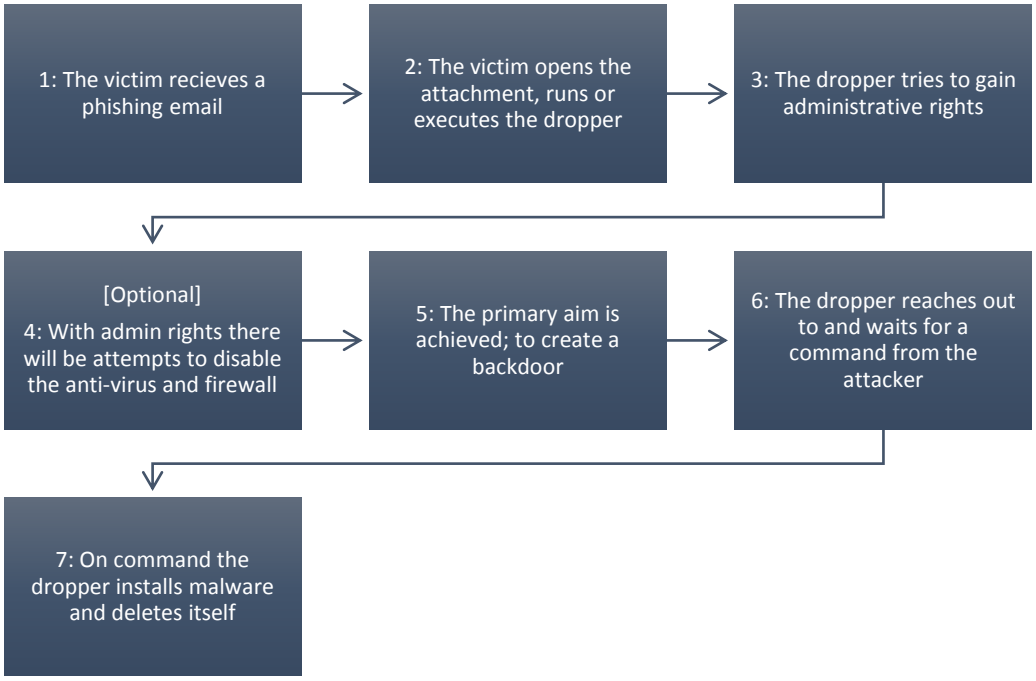
Now that the backdoor has been opened, the dropper contacts a command and control (C2) system administered by the attacker. This can come in various forms, from dedicated malicious systems set up by the attacker, compromised systems of legitimate organisations, or even using IRC chat rooms, where instructions can be delivered in a text based format. The particular method chosen depends on the specific dropper and is usually hardcoded. The C2

[1] https://www.cert.gov.uk/resources/best-practices/phishing-what-is-it-and-how-does-it-affect-me/

systems will then provide instructions to the dropper; often this means downloading malware (the focus of this paper), but this is not the only use. Some of the more complex droppers are able to gather system information, such as the Operating System, installed applications, browser and plug-in versions etc. Whilst these are rare in droppers, the information is useful to deliver more targeted attacks and malware, and is more common in exploit kits[2] that are used in some of the drive by download attacks.

If the aim was to install malware on the target computer the attacker has achieved their primary use for the dropper and is then no longer required. The malware they have added can carry out whatever tasks it has been assigned: be that accessing personal information, keylogging, or acting as a weakness in a network's defences for further exploitation, among many others.

The following is a summarised example process of the actions a dropper could carry out. In this case the attack vector is a phishing email.



Defending against droppers

The difficulty of defending against droppers varies greatly depending on its complexity, the skill of its programmer, and the method of distribution. Defence relies on good practice, and droppers are only a part of the malware problem out there. With that in mind, you should maintain a well-rounded defence against all attacks with some general rules that apply to all malware, as outlined by the 10 Steps to Cyber Security[3].

With spam/phishing and drive-by-downloads as the most common delivery methods, prevention is the best defence. A combination of using spam blockers (to prevent users ever receiving the mail) and user training to help users recognise spam/phishing emails should

[2] https://www.cert.gov.uk/resources/best-practices/demystifying-the-exploit-kit/
[3] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

minimise the risk. Ensuring that macros in document files are disabled by default prevents the common Office document droppers from being able to run without user interaction. Keeping web browsers and plug-ins up to date ensures vulnerabilities are patched and so only drive by downloads using previously undiscovered exploits should work. Plug-ins that are commonly exploited, such as Flash or Java, should be disabled or uninstalled where appropriate. In such a case, it may be possible to almost entirely remove that risk. These are common anti-malware practices and there is more information in the 10 Steps to Cyber Security section covering malware prevention[4].

It is important to note that there will always be zero-day exploits (those previously undiscovered and therefore without patches), and someone in an organisation will eventually always click on a phishing emails, despite defences. This means you can never be completely impregnable. However, there are different layers of defences and therefore risk that an organisation can take on. Anti-malware programs can detect and remove common malicious droppers, and ensuring general users do not have admin rights can prevent droppers (and users) being able to install files, likewise, only allowing whitelisted programs (specifically named programs that are the only ones allowed to run) can prevent the droppers running in the first place. Finally, maintaining Intrusion Detection Systems[5] allows monitoring of networks and/or machines, depending on the type used, for suspicious activity to prevent the spread of a successful attack.

There is no doubt that as security professionals find ways to combat malware the authors will find increasingly effective ways to counter the new defences and this cyber 'cat and mouse' will continue far into the foreseeable future. Droppers remain a crucial part of initial infection for many of the most common and effective malware in operation today, and as such it is essential to understand the processes they use, what the intentions behind them are, and how to defend against them.

Becoming a member of the Cyber-security Information Sharing Partnership will allow your organisation to stay on top of the latest droppers and malware in the wild.

Stay informed and become a member at www.cert.gov.uk/cisp.

[4] https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-malware-prevention--11

[5] https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-monitoring--11

www.cert.gov.uk

@CERT_UK

A CERT-UK PUBLICATION