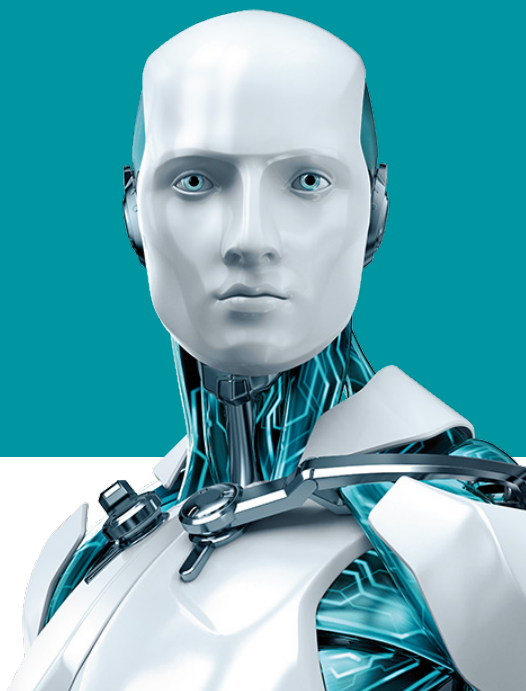
ESET vs. CRYPTO-RANSOMWARE

What, how and why?



ENJOY SAFER TECHNOLOGY™

CONTENTS

INTRODUCTION

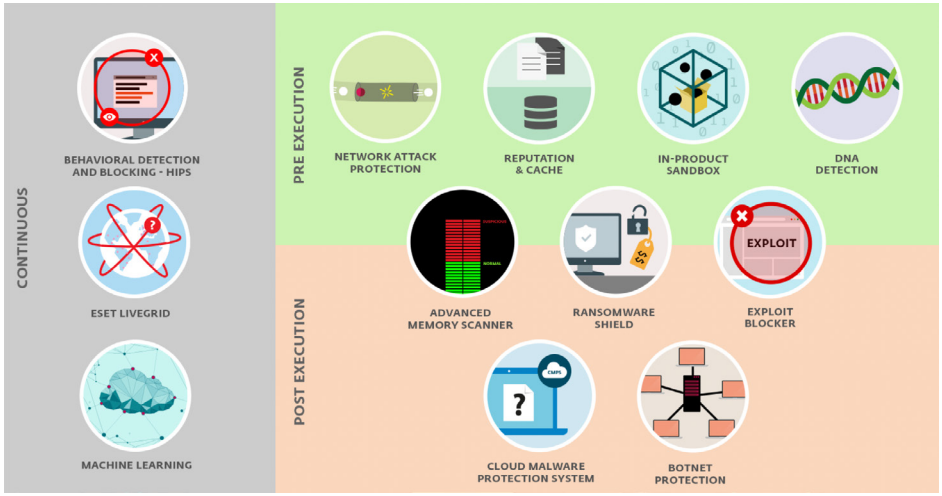
Crypto-ransomware (or filecoders) has been on the rise since at least 2013, when the notorious CryptoLocker appeared. Since then, cyber criminals have collected millions of US dollars by extorting money from victims in return for unlocking their data. In 2016, *estimates based on FBI findings* suggested that ransomware was set to become a **$1-billion-a-year crime**.

Cyber criminals' earnings demonstrate the impact of this exponential trend and are the main reason why crypto-ransomware has become the malware of choice in many campaigns. It should not come as a surprise that most ransomware campaigns use exploit kits and socially engineered emails as their infection vector, which also contributes to their increased prevalence. In fact, according to the PhishMe service, "*more than 97% of phishing emails delivered in 2016 contained ransomware...*"

ESET has been monitoring the ransomware scene closely and responding to its rapid evolution. In 2016, there have been few days on which ESET researchers have not encountered a brand new ransomware family.

However, in spite of it being one of the most serious malware types in the wild, it is still just another type of malware. This means that ESET is fighting it as it does any other malware, via multiple layers.

ALL LAYERS ACTIVATED



The vast majority of ransomware attacks are blocked by *ESET's multi-layered technology* even before the actual ransomware infection reaches victims' computers. A good example of this is the detection of email messages containing droppers that would eventually download and execute the ransomware.

Another example is detection of exploitation attempts that allow the attackers to get remote control over the victims' machines and in many cases lead to extortion by ransomware. ESET Network Detections are designed to prevent such attempts by targeting network vulnerabilities and exploit kits. In addition, **ESET Exploit Blocker** monitors processes of running applications and looks for abnormalities in their behavior. Its design enables ESET to detect and effectively block exploitation of vulnerabilities – even those that are previously unknown, so-called zero-days – that could be used by crypto-ransomware to enter the targeted system.

To further fortify users' systems, **ESET Advanced Memory Scanner** is designed to uncover the true nature of heavily obfuscated processes, often detecting crypto-ransomware prior to it encrypting valuable files. Such obfuscated malware constitutes a significant part of today's malicious traffic, mostly due to automated repacking/obfuscating services, available on black markets. But even the most obfuscated code in the world needs to reveal itself at some point in order to be executable. And that is exactly the point at which it gets caught by our Advanced Memory Scanner, which is triggered by ESET's Host-Based Intrusion Prevention System (HIPS) at just the right moment.

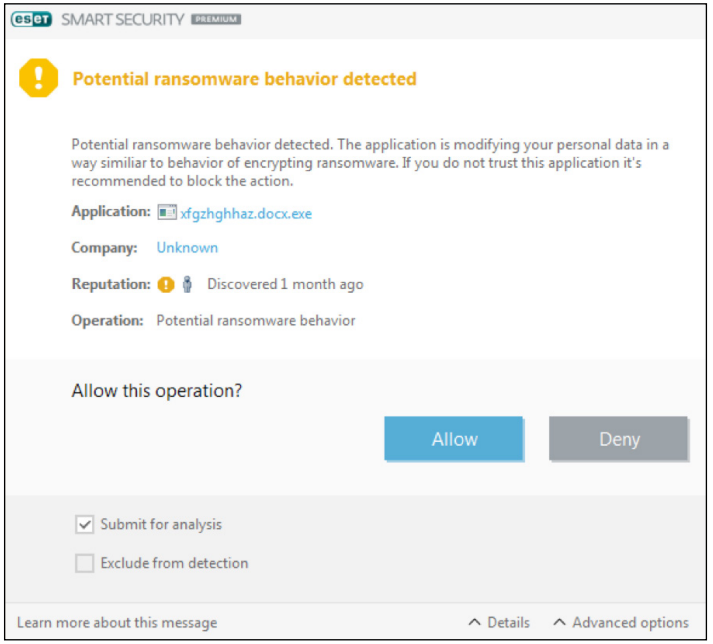
To sum up, every single layer of ESET's multi-layered technology uses different means to take part in effective blocking of crypto-ransomware. Moreover, metadata from each of these layers can be sent to our **ESET LiveGrid®** cloud systems, providing further intelligence to our machine-learning algorithms. These automated systems, in combination with the expertise of our researchers and engineers, enable us to cut the reaction time to new emerging threats down to minutes.

In an effort to get as close as possible to perfect security, ESET has added yet another layer to address the phenomenon of ransomware.

ESET Ransomware Shield

ESET Ransomware Shield monitors and evaluates executed applications using behavioral heuristics. It is designed to detect and block behavior that resembles ransomware.

The technology is activated by default. If ESET Ransomware Shield is triggered by a suspicious action, then the user will be prompted to approve/deny a blocking action.



Furthermore, the dialog window allows the user to submit the suspicious application for analysis – or exclude it from future detection.

WHY THIS WAY AND NOT SOME OTHER?

Among several possible approaches to combating ransomware, we believe that our multi-layered approach is the right one. And it's not just our belief; its efficacy has been proven in countless independent tests by reputable testing organizations. For instance, in a *test by independent third-party organization SE Labs, focused on detection of ransomware, ESET scored 100%. The word* "reputable" is very important: there are tests out there that provide no informational value whatsoever. Some of these are even misleading, for instance the so-called *RanSim*.

RanSim

This software might be a simulator, but certainly does NOT simulate the behavior of crypto-ransomware. Since it modifies only the files it has created itself, it in fact simulates only "ransomware" that demands payment for decrypting its own files. Were all of the hundreds of ransomware families in the wild to share such an ingenious design, there would be no actual ransomware at all.

ESET products do not – nor will they ever – detect this behavior as malicious, and so repeatedly "fail" in such tests. Actually, if they were to detect it they would also have to detect digital rights management techniques used by digital distribution platforms, such as Steam. These behave similarly, by downloading their own encrypted files – games in the case of Steam – and decrypting them at the right moment.

But let us get back to the topic of this section and discuss why we do not approach crypto-ransomware differently.

Application whitelisting is not a silver bullet

The idea of simple whitelisting of known benign applications is often discussed as a candidate for an all-powerful crypto-ransomware treatment. Irrespective of the task of keeping the number of false positives as low as possible, there are several issues that need to be addressed.

Problematic cases, for instance, include crypto-ransomware that injects itself into a process belonging to a whitelisted application. Or when some of the whitelisted applications might be interpreters, like wscript, autoit or cmd, and it might be challenging to decide whether to allow or block their execution, since the code they are about to interpret (carry out) might be malicious. This is not to mention cases where a legitimate application that is able to encrypt files (an archiver, for instance) is misused directly to encrypt files.

This is not to say that application whitelisting is pointless. It contributes to the overall detection capabilities of ESET products. However, without other layers of protection it would be significantly weaker.

Shadow Copy is useful, but not against crypto-ransomware

Shadow Copy is a technology that allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use. However, there are some facts to consider before trying to use this as a rollback solution after crypto-ransomware strikes.

Firstly, potential performance degradation related to shadow copy creation and storage should be considered. Secondly, shadow copies can be deleted or encrypted by ransomware if they are not protected. Moreover, if the ransomware starts to repeatedly encrypt the files, the buffer dedicated to store the incremental file changes might reach its limit. And most importantly, one should not forget about disk-encrypting ransomware (such as *Petya*) against which shadow copies would be entirely helpless.

Why no rollback as a last resort?

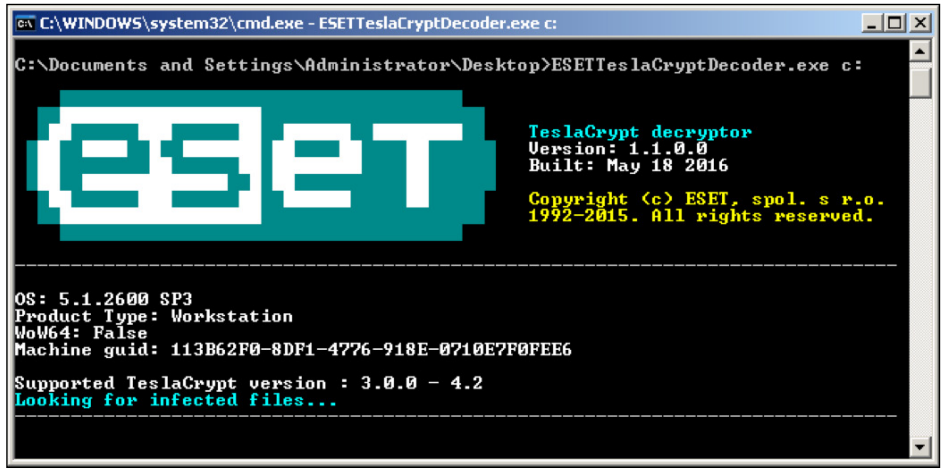
There clearly are benefits to having a rollback functionality implemented directly in a security solution. We are continuously testing and evaluating the overall impact of such a solution and might implement one in the future. At this point, however, our analyses suggest that the current approach – with the focus primarily on proactive measures – provides optimal results.

OTHER WAYS THAT ESET FIGHTS RANSOMWARE

We at ESET know that fighting malware, especially types as nasty as crypto-ransomware, needs to go beyond our standard security solutions and the technology implemented within them. That is why our researchers are on constant lookout for opportunities to disrupt cyber criminals' operations.

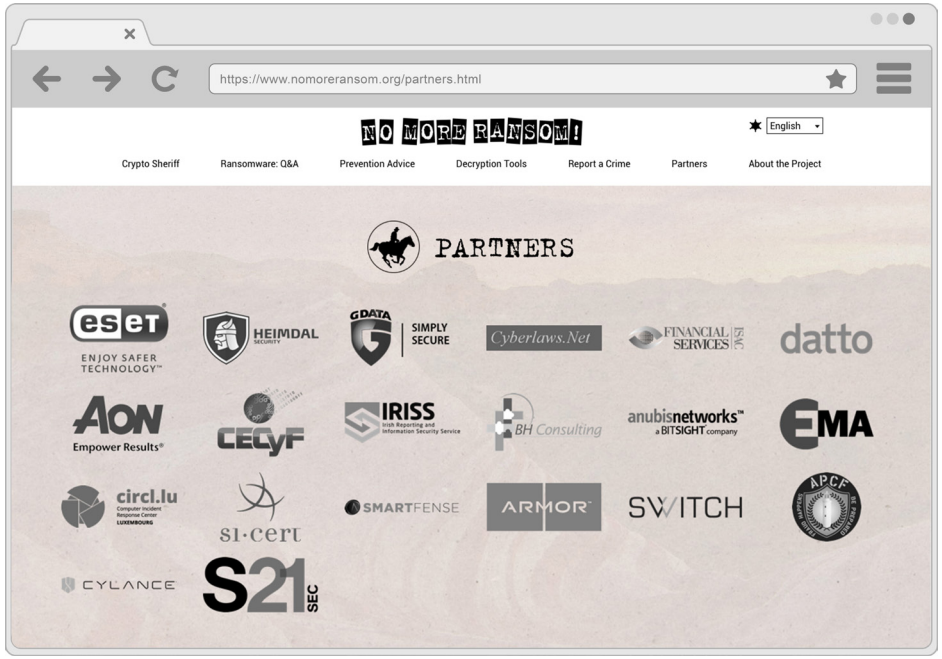
In the case of crypto-ransomware, this means finding errors in its implementation or holes in the cyber criminals' infrastructure. We embrace every opportunity to create ransomware decryptors that help those who have fallen victim to get their data back. In most cases, we develop decryptors tailored to the victim's specific case, as there are usually many system-specific variables to be taken into account. However, whenever possible, we create such decryptors and provide them free of charge to the wider public. Our TeslaCrypt decryptor, which has been downloaded more than 100.000 times, is one such case.

Similar to the proactive approach our products take in handling crypto-ransomware, we proactively share the results of our crypto-ransomware research, conducted across ESET's several research centers.



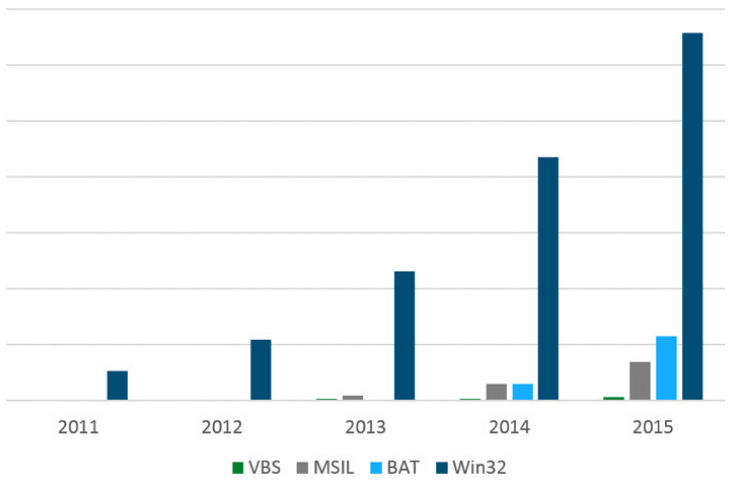
We frequently release research articles and whitepapers about crypto-ransomware on our company blog *www.WeLiveSecurity.com*, present on the topic at numerous international conferences, and even go into schools to raise awareness among the youngest generation.

We share our findings with researchers all around the world, whether they work for our biggest competitors or for law enforcement entities, such as the FBI. Being one of the first private companies to become a supporting partner of the *"No More Ransom" project* is one of the many ways that ESET has proved its dedication to fighting crypto-ransomware.



FOCUS ON PETYA CRYPTO-RANSOMWARE

ESET has covered *the evolution of crypto-ransomware* previously, showing its growing prominence. The number of families, variants and targeted platforms has increased significantly since 2011.



Number of Windows file encrypting ransomware programs in the period from 2011 to 2015

Let's take a closer look at how encryption was used in one newly infamous crypto-ransomware family, Petya We explore three additional families in *this blog post*.

Petya took a different approach from that of other crypto-ransomware Instead of encrypting files individually, it aimed at the file system. The target is the victim's *master boot record* (MBR), which is responsible for loading the operating system.

When Petya is executed, it starts a two-stage attack intended to encrypt the MBR. This process of encrypting the MBR starts by modifying the MBR in order to cause a *BSOD* to get the system rebooted. It then displays a fake *CHKDSK* screen while it performs the MBR encryption, and finally it reboots the system again. When this happens, it shows a blinking screen of a skull and the ransom message.

Evolution of Petya ransomware skull screens and ransom screens (initial red, and more recent green and gold variants)

While this message is undoubtedly frightening, it still is possible to undo the damage caused, due to several flaws in the way Petya handles encryption.

Petya's developers committed an implementation error in the Salsa20 core which reduces the security level of the encryption. Only half of the key is actually applied, which reduces it from 92-bit to 46-bit security, which is feasible to break within seconds using brute force.

However, the latest version of the ransomware doesn't have these flaws anymore, as they were spotted and fixed by the malware operators.

Learn more about the Petya ransomware outbreak of June 2017 in *this ESET blog post*.

FUNDAMENTAL RECOMMENDATIONS FOR PROTECTING YOURSELF AGAINST RANSOMWARE

Ransomware is just another malware family. The only difference is that it's going after your files – so on top of everything you do to prevent being infected (the attack vectors are emails and exploit kits mostly), you need to have a reasonable backup policy in place, meaning the ability to quickly restore. Journaling solutions are CPU/disk heavy and you do not really want to use them until a ransomware problem appears (by which time it's too late). To limit the attack vectors:

1. Properly configure endpoints and your security software.
2. Update and patch your OS and software regularly, as ransomware often uses known vulnerabilities. Pay special attention to internet browsers in this regard.
3. Endpoint and perimeter security solutions are a must, and they must be properly configured to be able to use the full feature set, such as fast cloud-based detections.
4. Use whatever capabilities your operating systems provide for hardening:
   - remove the ability to run untrusted code with AppLocker or Software Restriction Policies;
   - disable scripting in operating systems and web browsers;
   - disable unnecessary services like RDP;
   - make the operating system display file extensions;
   - consider using a System Restore service;
   - consider disabling Windows Script Host;
   - set "Open with..." for extensions often used for infections with a reader (such as Notepad) rather than an interpreter;
   - block application execution from %LocalAppData% and %AppData% folders;
5. Disable unnecessary access to network shares.
6. Do not use servers as standard desktops (e.g. for browsing the internet).

Download PDF

Download PDF


ENJOY SAFER TECHNOLOGY™