WHITE PAPER

RISING THREATS: EVERYTHING YOU SHOULD KNOW ABOUT HYBRID MALWARE

GATEWATCHER

OVERVIEW

Everybody knows it: cyber threats evolve constantly. Hackers use more and more sophisticated and crafted methods to deceive information security software. The most recent observed phenomenon: new malware variant, called hybrid have appeared. Almost undetectable, they hide a very powerful payload.

In this White Paper, we'll give you all the keys to understand them better and detect them before it's too late!

1.
CYBER THREATS: TODAY'S PICTURE

According to Gartner, security products and services related expanses reached $114 billion in 2018, increasing by 12.4% in one year.

Amongst the different types of cyber threats (phishing, DDoS, ...), malware are one of the most common variants. Whether it is ransomware (such as WannaCry, Petya, NotPetya), virus, Trojan horse or backdoors, these malware target information systems to steal data or damage them.

Cyberattacks in companies and industries

Companies around the world have been affected by cyberattacks. All types of businesses are potentially at risk : VSB, SMB, majors groups... According to a study by Hiscox, 45% of businesses in the USA and Europe were hit by a cyberattack in 2018.

What impact for companies?

On the one hand, these cyberattacks have a financial impact such as slowing down or stopping the production, and the loss of turnover; on the other hand it can cause other damages like the theft of personal data or confidential information.

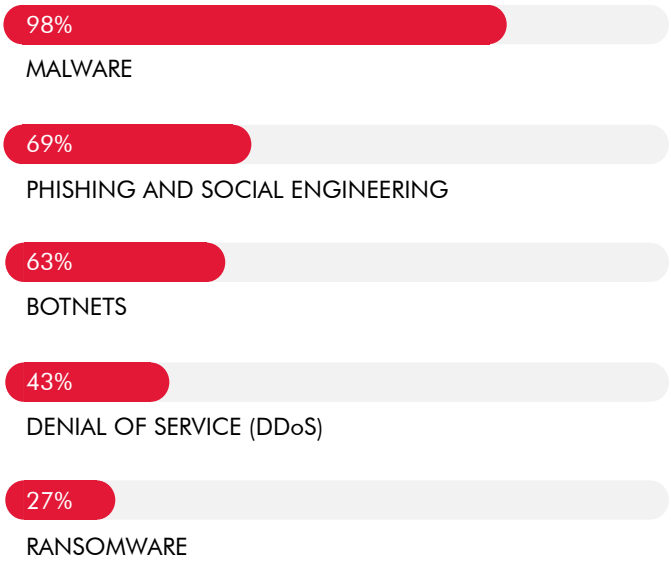
The financial aspect has a major impact when we know that one data breach costs to businesses $3.7 million in average. Another study by CDNetwork expects cybercrime to reach $2 trillion this year.

Cyberattacks become more complex. Hackers hybridize their techniques to make their attacks less detectable but always more disastrous.

Jacques de La Rivière (CEO, Gatewatcher) and Philippe Gillet (CTO, Gatewatcher)

One of the most used attack types is ransomware, which will continue to grow over the next years. Ransomware damage costs will rise to $11.5 billion in 2019 and a business will fall victim to a ransomware attack every 14 seconds (Cybersecurity Ventures).

Most frequent cyber attacks by companies worldwide:



Data from Statista : «Cyber crime: attacks experienced by companies worldwide 2017»

Ransomware damage costs will rise to $11.5 billion in 2019 and a business will fall victim to a ransomware attack every 14 seconds.

Study by Cybersecurity Ventures

Discover how hybrid malware work and how to counter them in the next chapters!

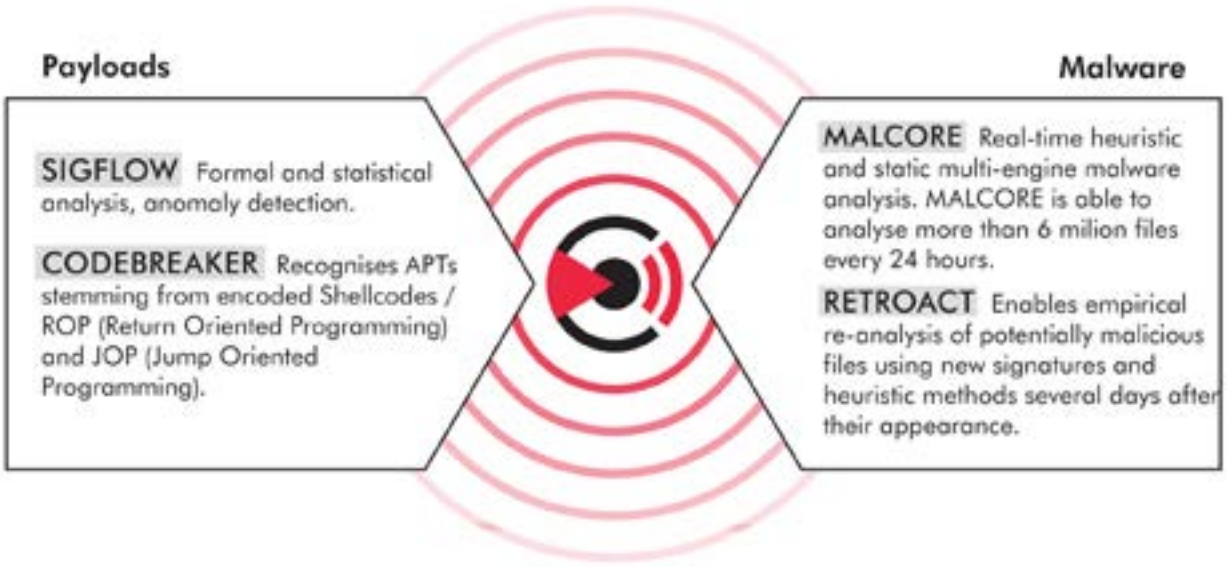
HOW DOES GATEWATCHER DETECT THREATS?

The defence tools deployed today, Firewall, Proxy and IPS probes, can be bypassed by encoding shellcodes or reusing authorised executables against themselves. Sandbox, once presented as infallible, have been deceived by evasion techniques, and do not cater for performance constraints. A new detection approach had become inevitable.

Trackwatch® detection system, published by Gatewatcher, combines signature-based and sandboxing solutions with machine learning algorithms. This unique technology targets abnormal behaviour by running a dynamic analysis of weak signals within network flows.

It auto-adapts to polymorphic threats, in order to guarantee a strong accuracy towards the evolution of APTs.

Our technology uses four next-generation engines:



2. HYBRID MALWARE: THE RISING THREAT

Today hackers use more and more sophisticated malware that don't seem malicious, at first glance. They're recognised as unsuspicious at 99.9%. The 0.01% left represents the payload. That part is really hard to detect and to analyse, which makes this type of malware even more dangerous.

This new malware variant is also called hybrid malware. We chose to focus on two of them in this White Paper: one-liners and shellcode-embedded malware.

ONE-LINERS

The payload is a single command line, that controls and schedules all malware actions.

These attacks are using automation mechanisms on operating systems like Windows. Indeed, Microsoft OS makes it really easy for hackers to handle the system. Windows created these features to simplify tasks likely to be repetitive for network administrators and allow them to take control of multiple computers with a single line of code. The default language on Windows systems, Powershell, provides access to computers network via command lines. By diverting this language, hackers can install software, take remote control, give a regular instruction or take confidential files out of the network. Everything is automated, from A to Z. Pirates therefore exploit Microsoft capabilities to respond orders, using one-liners.

Powershell script extracted from the one-liner

This is what makes this technique dangerous. Since the entry point is only one line of code, the malware becomes very difficult to interpret and detect. Is the administrator automating his tasks, or is there an outside threat aiming at harming the system?

Anti-viruses cannot see this difference. This is one of the reasons why hackers use this technique.

How to counter them?

The main challenge is to distinguish a potential malicious command line from a command sent by the administrator. The purpose is to succeed in extracting active payloads from the malware. To counter this threat, it is essential to differentiate what's malicious from what's normal behaviour. It is then necessary to find patterns to detect this difference.

At Gatewatcher, we are aware of this growing threat. Our Research and Development teams are providing an additional effort to detect this new threat.

Make sure you read the next chapter to know everything about shellcode embedded malware.

SHELLCODE-EMBEDDED MALWARE

The second hybrid malware we're focusing on is also very difficult to detect. In these cases, nothing appears when the malware is analysed. The embedded shellcode is completely opaque.

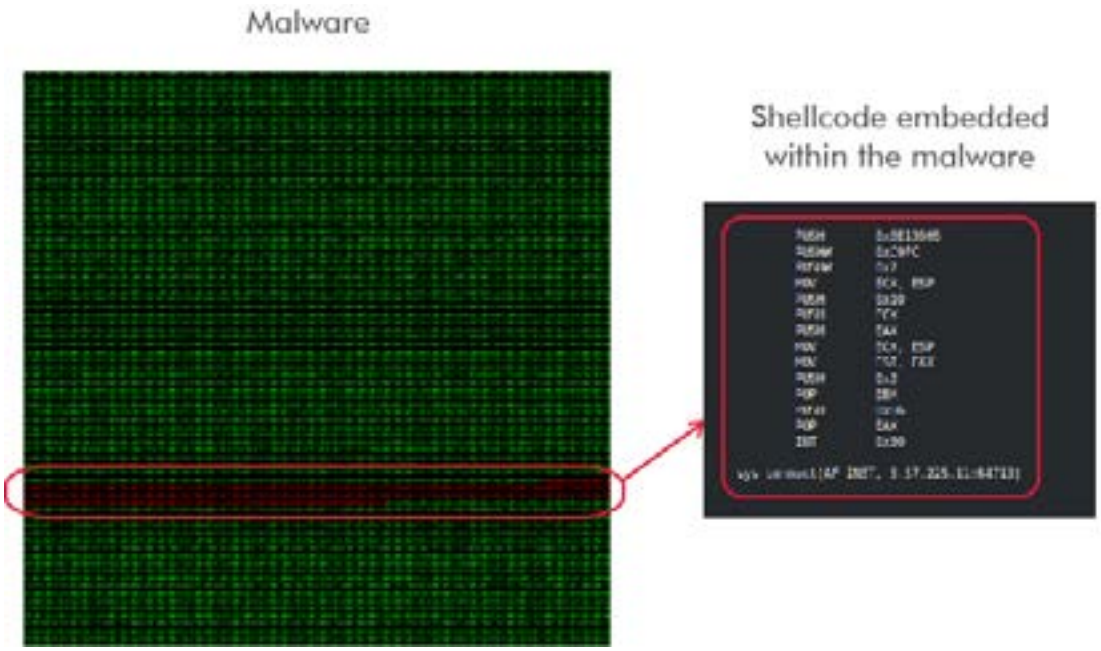
Why? The anti-viruses available on the market do not scan shellcodes. Gatewatcher has integrated shellcode detection and analysis in its advanced threat technology.

One of the best-known examples of embedded shellcode attacks is the NSA's EternalBlue. The US agency exploited a Microsoft Server Message Block (SMB) vulnerability. With this access, it was then easy to access files, printers or other resources of the same network. EternalBlue was then used in 2017 in the global cyberattacks WannaCry and Petya. EternalBlue was difficult to detect thanks to the use of a shellcode shipped by a binary.

Embedded shellcodes have various entry points. The detection lies in the diversity of these entry points.

Reading a shellcode is like reading a foreign language. As long as the entry point has not been found, we cannot understand that language.

Philippe Gillet (CTO, Gatewatcher)



Example of a shellcode embedded within a malware

How to counter them?

It would therefore be necessary to do a shellcode analysis on each byte. But that would be too time-consuming (1Mega = 1 year of analysis). In order to avoid this very long analysis, we need to know the potential entry points to reduce the areas to control. Convergence between shellcodes and malware makes it even more difficult.

Gatewatcher's teams are developing a new detection technology. It enables effective research of a shellcode embedded in a binary.

GATEWATCHER

REAL-TIME DETECTION OF ADVANCED THREATS

www.gatewatcher.com