WHITE PAPER

MINERVA

EVASIVE MALWARE:

HOW AND WHY YOUR ANTI-MALWARE STRATEGY NEEDS TO EVOLVE BEYOND ANTIVIRUS

INDEX

INTRODUCTION

The use of malicious software as a means for attackers to invade your environment, steal valuable data, or hold that data for ransom is only becoming more rampant. Crime organizations are keenly aware of the value of your data, so they are intent on devising new ways to ensure they gain access to your network, systems and data. At the same time, anti-malware vendors are working at a similar pace keep up with the bad guys. Signature-based detection of malicious applications has given way to machine learning, heuristics, artificial intelligence, analytics, and other advanced methods – all in an effort to detect even the newest malware strains.

And yet, despite the industry's best efforts, malware is still an ever-growing threat that succeeds at evading security defenses. On average, 33% of businesses have experienced a ransomware attack in the last year, and publicly disclosed incidents were up in Q1 in 2017 – 53% over the previous quarter.

But, with even modern AV solutions in place, how is this even possible?

Adversaries use evasive techniques during their attacks that succeed at getting around even modern anti-malware products. In addition to the malicious code that encrypts files for ransom or provides illicit access to your network, these attacks employ malware built to avoid detection entirely. ***Attackers will continue to find ways around detection-based anti-malware approaches despite the continued enhancement of AV products.***

As you can see from the fact that successful attacks still occur, regardless of the antivirus that the victim uses, relying solely on baseline AV tools simply isn't enough – mostly due to adversaries having the drive and skills to evade anti-malware technologies. In this whitepaper, we'll take a look at the various evasion techniques adversaries use to succeed, discuss why these methods work, and what you can do to evolve your anti-malware strategy to drastically impede attackers' ability to take evasive actions and cause damage on the endpoint.

[1] *KnowBe4, Endpoint Protection Ransomware Effectiveness Report (2017)*

[2] *McAfee, Threats Report (2017)*

EVASION TECHNIQUES OF SUCCESSFUL ATTACKS

Attacks that use malware designed for evasion follow a simple rule to remain effective: Don't Be Detected. While the goal seems simple enough, it requires the use of a number of techniques to ensure that the malicious codes run even on endpoints that use a variety of products dedicated to identifying, detecting, and eradicating malware. Let's take a look at some of them.

REFUSING TO INFECT IN "HOSTILE" ENVIRONMENTS

When an adversary generates malicious code that isn't detected by AV products on given day, the attacker has the incentive to keep the malware sample under the radar of security vendors for as long as possible. To accomplish this, evasive malware is programmed to avoid running in an hostile where the sample may be detected and analyzed. Such a program is designed to terminate itself or put itself to sleep in such a ***"hostile"*** environment, rather than risk being fingerprinted by the security tool. To accomplish this, such malware will examine the environment, looking for the following indicators it considers hostile:

VIRTUALIZATION ENVIRONMENTS

The presence of a virtual machine can indicate that the malware is being analyzed using forensic tools – something no malware author wants. Evasive malware often refuses to run under such circumstances to conceal its true nature.

SANDBOXES

Automated analysis sandboxes "detonating" suspicious files to determine whether they pose a threat. Evasive malware seeks to identify these environments, avoiding any displays of bad behavior.

ENDPOINT SECURITY PRODUCTS

If the adversary believes that a particular AV tool will likely recognize the sample as malware, the attacker often designs the malicious program to avoid running on the endpoint where this product exists. This is because once the tool detects the sample, its vendor will likely share details about the sample with other security products and vendors, making the malware ineffective even on systems without the "hostile" AV product.

From the attacker's perspective, it isn't just about not being detected (and shut down); it's about avoiding situations whether the malicious software might be analyzed and fingerprinted. Adversaries want their attack tools to remain viable for as long as possible, increasing their payout over time. By refusing to run in a hostile environment, malware increases the amount of time it stays under the radar of security vendors.

USING MEMORY INJECTION

Malware struggles to exist in an environment where AV is watching every potentially-malicious application and looking for new and unwanted files or processes to block. So, malware leverages several operating system-specific capabilities to inject itself into known good processes, instead of executing malicious code directly in memory of its own process. These techniques can work without any exploits or vulnerabilities; instead, they abuse legitimate capabilities of the operating system.

Such evasive malware arrives at the endpoint in a file that AV tools will not find suspicious, because the malicious code is concealed within the file using a packer or other techniques. By unpacking and injecting the malicious code into other applications, malware is able to look like a genuine, known process, thriving undetected by AV solutions, and giving attackers the foothold they need.

USING DOCUMENT FILES

Common files used as documents (e.g. Word, Excel, PDF) are no longer the simple data repositories they once were. With an ability to embed code, support macros, interact with websites, and more, malware often hides itself within these documents to bypass enterprise security defenses.

For example, a PDF could have an embedded Word document that contains a macro that launches a web browser to pull down and execute malicious code on an endpoint. Sounds complex – that's because it is... and by design. By utilizing document files in these types of manner, it becomes difficult for AV solutions to separate the malicious from the non-malicious file.

EVASIVE MALWARE – SO EASY ANYONE CAN DO IT

What makes evasion techniques so dangerous, is these methods are well-documented on the Internet and understood by not only "advanced" but even day-to-day attackers. For instance, a simple search of "how to detect if you're within a VM" will provide the technical details on what the evasive malware needs to look for.

To make this even more accessible to every type of an attacker, the malware is often offered as an easy-to-deploy service by criminal organizations of highly skilled developers who create malware, exploits, and test their product against AV solutions.

It's no longer the targeted attack that "won't happen to our organization" you need to worry about; it's the fact that both malware and evasion tactics are now easily accessible to anyone, and are no longer just the domain of highly-skilled, advanced adversaries.

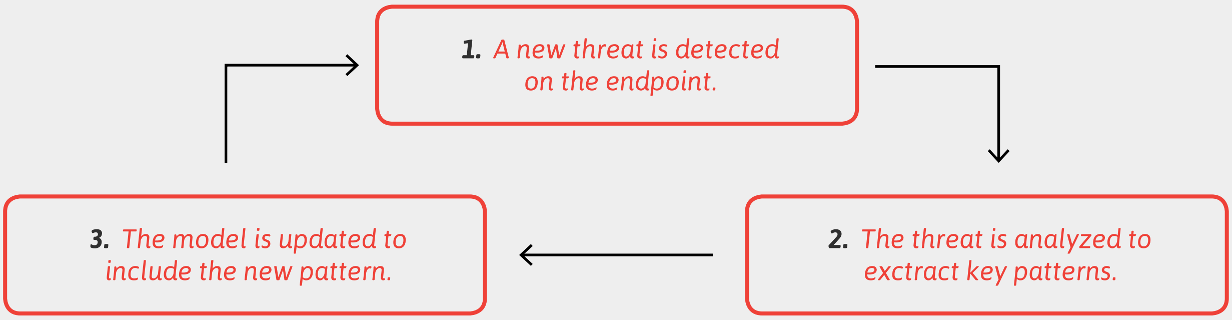
WHY EVASION TECHNIQUES WORK

The endpoint security industry continues to evolve in response to advancements in attack methods. Modern anti-malware tools incorporate a variety of technologies, including signatures, behavioral monitoring, file reputation, machine learning, heuristics, and many others. There are a few reasons why, even with this layered defense approach, it's simply not enough when it comes to evasion techniques.

REASON 1: AV IS HISTORY

Every AV defense is based on historical information. Despite the fancy use of terms like machine learning and heuristics, at the end of the day, modern AV solutions rely on previously gathered information to act as the basis for finding malware (or new variants using similar behavior). Security solutions that block URLs or processes are no better, as they too rely on historical relevant lists and behavior data to identify suspicious threat potential.

As shown below, the approach security vendors take to detecting threats relies heavily on matching historical threat artifacts.



1. *A new threat is detected on the endpoint.*

2. *The threat is analyzed to exctract key patterns.*

3. *The model is updated to include the new pattern.*

How AV Solutions Approach Detecting Threats

In essence, the antiquated model of using pattern matching has simply been updated to now include behavior patterns which act in a similar manner. Next-generation AV (NGAV) takes a more holistic system-centric approach, looking at processes, files, etc. analyzing activity to see if it appears threatening. But even so, that definition of what may or may not be a threat is still based on historical data.

Recognizing the limitations of AV and NGAV tools, adversaries devise malicious software to differ from the expected patterns. The resulting evasive malware leverages the techniques outlined in this paper, taking steps to change aspects of the attack. These methods can get around anti-malware approaches that try to identify malicious files as well as those that implement behavior-related detection. Which brings us to the next reason.

REASON 2: MALWARE GETS UPDATES TOO

With each update to an AV solution, adversaries react to these improvements by creating advancements of their own to evade detection. In essence, if they know your AV is looking for behaviors or threat artifacts that fit a given definition, malware is devised and tested against AV solutions to ensure it has an ability to not be detected.

REASON 3: EVASIVE MALWARE AVOIDS DETECTION

Evasive malware authors routinely build and test their malware against current implementations of solutions to deviate from expected signature and behavior patterns, trying to ensure that their malware remains unknown for as long as possible. Evasive malware takes additional measures to never be detected, making even NGAV solutions ineffective. They hope to detect every bit of malware they come into contact with, but, like a ninja attacking in the dark of night, AV and NGAV solutions may never see their adversary's attack.

EVOLVING YOUR ENDPOINT PROTECTION STRATEGY

Baseline AV products play an important role in thwarting non-evasive malware. However, enterprises need to evolve their understanding of endpoint attacks to realize the limitations of these solutions in their ability to stop threats designed to bypass them. There will always be a gap between these tools' ability to detect and block malware and attackers' ability to evade detection.

Organizations need to augment their endpoint protection strategy to include solutions designed to stop evasive attacks by blocking attempts to bypass baseline AV tools. So, rather than trying to detect malicious software, solutions like Minerva's Anti-Evasion Platform control how malware perceives its environment on the endpoint, deceiving malware in a way that neutralizes threats in a manner drastically different from your existing security layers. As a result, Minerva turns the strength of evasive techniques into a weakness with no impact on the end user.

ABOUT MINERVA

Minerva Labs is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva Anti-Evasion Platform blocks unknown threats which evade existing defenses by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva's solution deceives the malware and causes it to disarm itself, thwarting it before the need to engage costly security resources.
Minerva boosts customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture.

To learn more about Minerva Labs, visit **www.minerva-labs.com.**