Polymorphic, Preemptive, & AI-Generated Malware

White Paper

Crytica Security
7655 Town Square Way
Suite 212
Reno, NV 89523

Website: CryticaSecurity.com
Email: info@cryticasecurity.com

Polymorphic, Preemptive, & AI-Generated Malware

Contents

1. INTRODUCTION – "THE ONLY CONSTANT IS CHANGE"[1]

… the tendency … [is to study] how to fight the last war[2]

For as long as there have been weaponed conflicts, military planners have been preparing to fight with the weapons and strategies of the previous war. The sophisticated cybercriminals and the malicious state actors who perpetrate cybercrime and engage in cyber warfare know this. They count on this. They know that the cybersecurity industry's predominate malware detection tools rely upon:

- Exact matches to previously seen malware attacks.
- Patterns of code similar to previously seen malware attacks.
- Patterns of attacks that have been previously seen.

Consequently, the malware designers do the obvious. They create "new" malware. They create malware does not resemble the malware previously recognized as such:

- Polymorphic Malware – Malware whose characteristics "morph" dynamically, so that, over time and/or location, it self-alters itself to become unrecognizable.
- Preemptive Malware – Malware that disables a system's malware defenses before those defenses have had a chance to compare the code to previously seen malware code or have had a chance to compare the attack vectors to previously seen malware behavior.
- Totally New Malware – Malware that is so new that it has not been identified previously.

With the advent of powerful Artificial Intelligence (AI) tools, these types of malware are becoming much easier to design and much faster to create.

Making good use of these "obvious" design strategies, the malware designers have experienced, and are continuing to experience, devastating successes. Multiple independent studies have concluded that the cybersecurity industry is suffering from a disastrous inability to detect malware. According to a 2022 IBM/Ponomon Institute Study, the average time for fully deployed AI enhanced malware detection systems to detect a malware infection is over 180 days (181 days in 2022).[3] The overall average detection times, including less "well protected" systems are much worse. (See Figure 1 - Average Detection and Remediation Times.

[1] Heraclitus. This is a paraphrase of his observations that "Everything changes, and nothing remains still; you cannot step twice into the same stream".

[2] While this understanding is as old as time, the quotation here is from Lt. Col. J.L. Schley: "It has been said critically that there is a tendency in many armies to spend the peace time studying how to fight the last war." (Jan-Feb 1929)

[3] IBM Cost of Data Breach Study 2022

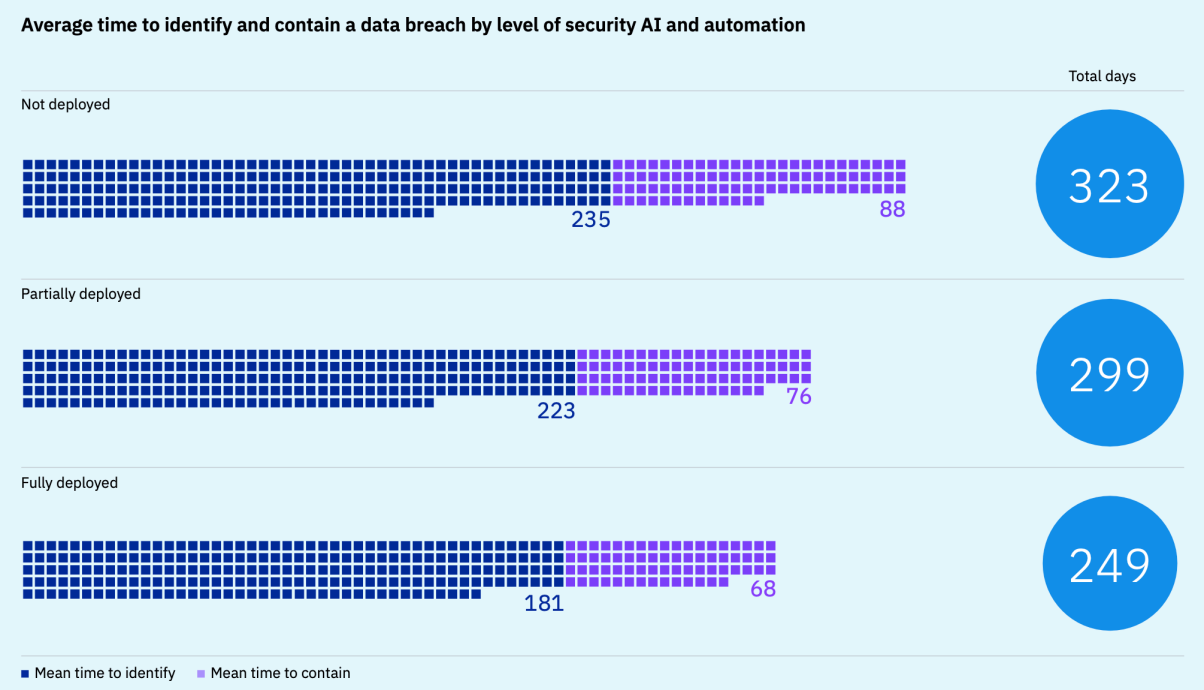

Figure 1 - Average Detection and Remediation Times[4]

Detection times that are measured in months rather than in seconds or even minutes are not a new phenomenon. They have been the rule for years, and they are clear indicators that the current generation of malware detection systems, and their predecessors, are, to quote an old Chinese expression, "paper tigers". They are far more "Security Theater" than they are weapons for real security.

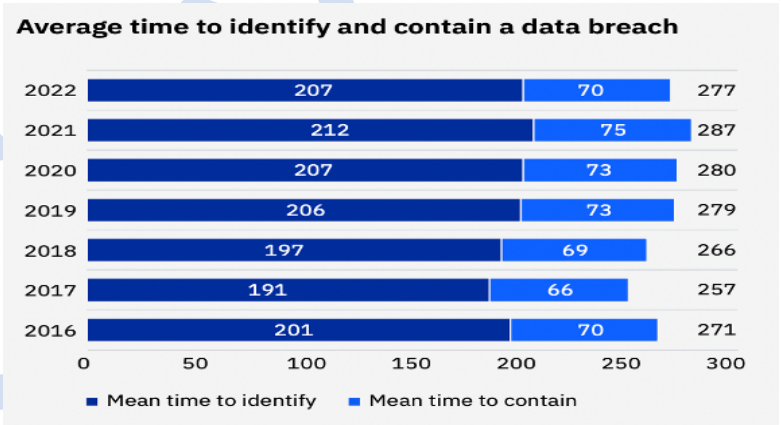

Figure 2 - Average Malware Detection Times Over the Last Few Years[5]

In the high-speed world of computer systems, the many months between malware infection and malware detection are the equivalent of "eons", more than enough time for the malware to wreak whatever damage it is designed to inflict.

[4] Ibid.
[5] Ibid.

One of the root causes of this "disastrous inability to detect" malware is that, in an environment of polymorphic, preemptive, and AI-Generated attacks, the predominant malware detection systems are designed to detect static, non-dynamic, non-preemptive, and well-known attacks. The majority of malware detection systems' basic design paradigms render them incapable of detecting sophisticated dynamic attacks. It is an uneven battle; a battle in which the results are a foregone conclusion.

Fortunately, new detection paradigms are now available, detection systems designed to detect the newest and most sophisticated, dynamic malware attacks; even polymorphic, preemptive, and AI-Generated malware.

2. POLYMORPHIC MALWARE

The Malware Designer's Logical Strategy

Consider the challenge from the point of view of the enemy, the point of view of the malware designer. It is well known that most malware detection systems use databases of previously detected malware as the basis for detecting malware attacks. These malware databases may contain one or both of:

- Malware (or "Virus") Signatures – "Signatures" are the series of ones-and-zeros that comprise the unique set of computer instructions (the "program") that, when executed, is the malware. By comparing each malware signature against the contents of every file present in a system, the malware detection systems can determine whether any malware stored in the malware database is present in any of the files in a system.
- Malware Behavior Patterns – When malware launches, it begins to execute a set of actions, either malicious behavior or a prelude to malicious behavior. The pattern of these actions are idiosyncratic to that specific malware. By storing known malware behavior patterns in a database of such patterns, malware detection programs can monitor system behavior and issue alerts when such patterns start to execute.

Thus, the logical strategy for the malware designer is to create malware that is not an exact match for anything in the malware databases, and not even a close-enough match for the AI pattern-recognition software to flag it.

Creating Previously Unrecognized Malware

There are several ways that a malware designer can create malware that is not a match for anything in the databases of known malware. The designer can create:

- New Malware – Writing new malware, malware that is truly unique and innovative, is not easy. It is both time and resource intensive. It is, however, the strategy of choice when the target is important and valuable, and when success is mission critical. Resource rich cybercriminals and well-funded malicious state actors are the sources of most of the truly new and innovative malware.
- Polymorphic-Image Malware - One of the easiest methods of producing malware that does not appear to be in the malware signature (image) databases is to write malware that changes its "signature", that is, it changes the strings of ones-and-zeros

that are its instruction set. Padding the malware computer-code with meaningless instructions (e.g., a = a;) and/or filling the object code with meaningless lines of code that the actual instructions simply jump over (i.e., ignore) is one way to accomplish this. To avoid detection, this malware changes the meaningless padding, the ignored code, based upon time-triggers and/or location triggers. While doing so, it keeps the essential set of instructions intact. Since the new total set of ones-and-zeros that comprise the overall malware code is not the same as any that was previously identified and stored in the malware database, malware detectors that rely upon malware "signatures" cannot detect the new, "morphed", malware.

- Polymorphic-Action Malware – Just as image signatures are stored in malware detection databases, so are activity ("action") sequences. To defeat this type of detection, malware designers create malware that can, again based upon time-triggers and/or location triggers, or even "random" factors, "morph" its activity sequences and even the nature of its malicious behavior. This type of malware is also very easy to create. A simple "switch" (conditional) statement in the code can influence the malware to behavior in a plethora of diverse behaviors; rendering "activity matching" a very difficult proposition.
- Polymorphic-Image and Action-Malware – Sophisticated malware designers can combine the two previous described techniques to produce malware that changes both its own image and its activity patterns. Detection of such malware, especially if it is well-designed and constructed, is far beyond the capabilities of any of the malware detection systems that rely solely upon matching malware against the malware stored in the malware databases.

Understanding the Polymorphic Malware Threat

In response to the growing threat of polymorphic malware, many malware detection systems that continue to rely upon malware databases have pursued the chimera of AI-enhanced malware detection. They use AI pattern matching to find malware that is "similar" to the malware stored in the malware databases. Some even employ AI predictive techniques to try to "guess" what future versions of malware might be like.

Unfortunately, these AI-enhanced malware database detection systems suffer from a number of inherent fatal flaws. These include:

- The Sheer Quantity of Malware – There are today over a billion known instances of malware, with "17 million brand new malware instances … registered every single month".[6] With such a vast quantity of malware that must be stored in malware databases, and even worse, that must be compared to on every scan for malware, the strategy of malware database comparisons is now untenable. Even the power of AI cannot mitigate such numbers.
- A Plague of False Positives – From its very inception, AI-enhanced malware detection has been the source of a tsunami of "false positives", that is, the identification of something as being malware when, in reality, it is not malware. The resources

[6] Darren Craft, www.WorthInsurance.com, *Malware Statistics & Facts: Frequency, Impact & Cost*, 16 February 2023.

wasted in pursuing and examining "false positives" have drawn many analysts to declare that false positives are often more expensive than an actual malware attack. Despite advances in AI technology, AI-enhanced malware identification is, by its nature, probabilistic and not deterministic[7], therefore, false positives will be, for the foreseeable future, endemic to all AI-enhanced malware detection.

- An Unwinnable Arms Race – Just as the cybersecurity defenders have access to AI technology, so too do the attackers, the malware designers. It would be fatal hubris to assume otherwise. As the AI-enhanced cybersecurity defenses improve, so too do the AI-enhanced attacks. To rely only upon AI-enhanced cybersecurity and the rapid improvements in AI technology is to engender an AI arms race that is ultimately endless and unwinnable. The defenders need to win every encounter. The attackers can afford to lose myriad battles. The attackers need to win only one. From the point of view of a defender, the AI arms race is a strategy that can lead only to catastrophe.

Polymorphic malware is not, however, invincible. It can be detected and defeated. To do so, new malware detection algorithms, ones that do not rely upon malware databases and history, must be implemented.

3. PREEMPTIVE MALWARE

There already exist in the wild some relatively successful "intelligent" malware programs that know how to bypass and even disable many of the most popular anti-malware systems. These are of the class of malware known as "Preemptive" Malware. They are designed with an awareness of the types of defenses that they may encounter as they attempt to infect systems. As such, they are designed to launch preemptive attacks against those defenses; disabling defenses before the defenses can be employed against them.

The "Hive" virus is a very good example. It continued to run rampant for well over a year even after it had been identified by the cybersecurity community. The reason for the Hive virus' proficiency and longevity was that Hive had the ability to disable malware detection and defensive systems before those systems could detect and mitigate the virus. According to the US's Cybersecurity and Infrastructure Security Agency: "Hive ransomware removes virus definitions and disables all portions of Windows Defender and other common antivirus programs in the system registry."[8]

[7] "Probabilistic" systems calculate the probability that what is found is real malware; and the probability is rarely 100%. There is almost always a gray area, always a possibility for false positives. For "Deterministic" systems, the calculation is always a "yes-or-no", "true-or-false" calculation. Hence deterministic systems do not suffer from false positives.

[8] US Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, *#StopRansomware: Hive Ransomware*, 25 November 2022, Alert Code: AA22-321A

The trend for this type of preemptive, pro-active, defense-disabling malware is just beginning to gain momentum. On May 28th, 2023, it was reported in LinkedIn[9] that:

> A threat actor that goes by the moniker "spyboy" claims to have devised a method to terminate all AVs/EDRs/XDRs. The software has allegedly been tested on most AVs/EDRs/XDRs that exist in the market.

The claim is that this new malware can bypass/disable all the best-known anti-malware systems. Whether this specific claim is verifiable or not, the danger is clear. Preemptive malware is quickly finding ways to overcome traditional malware detection systems. It is a growing threat that must be countered.

As with polymorphic malware, preemptive malware is not invincible. Preemptive malware can be detected and defeated, but only by detection systems that:

- detect at the moment of "malware infection", and do not wait to detect until after the malware launches,
- are designed to be resilient to attacks and compromise, and are not designed as vulnerable single-points of catastrophic failure.

4. AI-GENERATED MALWARE

The AI-Generated Malware Threat

With the advent of easily accessible AI systems, systems that can be given access to the vast libraries of existing malware, AI systems now have the ability to create, with unprecedented rapidity and in endless variety, "new" forms of malware. AI systems can design and create all the strains of polymorphic malware and preemptive malware, and even invent new strains of both.

As noted above, there are over a billion malware programs already existing.[10] This enormous trove can comprise the raw fodder for malicious AI systems to ingest, digest, and then produce a new "super breed" of malware. These AI malware design systems can also be fed with the essential detection algorithms currently in use, including the AI enhanced detection algorithms. This knowledge can be used by the AI malware design systems to create new malware that is able defeat any of the already known AI detection algorithms. Although it is true that new AI detection systems will be designed, their paradigms can also be fed into the malicious AI malware design systems and those malicious AI system can create ways to defeat the new AI detection systems as well.

Nevertheless, AI-Generated malware can be defeated. No matter what types of attacks AI systems create and "invent", computer systems are deterministic environments. There is nothing "magical" nor "mystical" about them. By understanding and utilizing the basic principles of detection and prevention, even AI-Generated malware can be defeated.

[9] https://www.linkedin.com/posts/kaushik~pal_a-threat-actor-that-goes-by-the-moniker-activity-7068631930040188929-aAMT/

[10] Darren Craft, www.WorthInsurance.com, *Malware Statistics & Facts: Frequency, Impact & Cost*, 16 February 2023.

5. PREVENTING A CYBERSECURITY MELTDOWN

The rapidity and the variety, the sophistication and the efficacy, of the new AI-Generated malware will inexorably overwhelm all of the current malware detection systems that are based upon malware databases and based upon detection "after launch". The new AI-Generated malware will soon become the nail in the coffin for all those detection systems that are currently so prevalent.

Nevertheless, the specter of AI-Generated malware inducing a total meltdown of cybersecurity defenses can be prevented. Even AI-Generated Polymorphic, Preemptive, and new Malware can be detected. More to the point, they can be detected rapidly enough to prevent them from wrecking total havoc. They can be detected sufficiently rapidly to contain them and limit, and even prevent, the damage they are designed to inflict.

To do so, the basic principles required to detect the most sophisticated malware must be implemented and maintained. These include:

- Malware Detection at the Time of Infection
- Malware Detection Based Upon the Essence of Malware
- Malware Detection that is Comprehensible

Malware Detection at the Time of Infection

Waiting for sophisticated malware to launch and then looking for previously known attack patterns is an exercise in futility. Sophisticated malware, when launched, can use, and has used, preemptive techniques to destroy/disable the defensive systems before the defensive systems can respond. In order to reliably detect a malware attack, the attack must be detected at the time of infection, at the time when the malicious code is first injected into the system, and not at the time of launch.

Very often, sophisticated malware will employ a "launcher" program. This is used when the malware is ready to launch the attack. The launcher program does nothing apparently suspicious. It appears to be nothing out of the ordinary, that is, it displays no malicious behavior. Hence, most malware detection systems will not flag it as being malware. But when the time comes to launch the malware attack, the launcher will collate all the requisite malware components and launch them. … At which point, it will be too late to stop them.

Effective detection mandates that even "innocuous" instruction code sets, including launcher programs, are flagged as being malware. The principle must be that: "any unauthorized executable code, not matter what it seems to do, must be flagged as malware."

Malware Detection Based Upon the Essence of Malware

As elucidated above, any malware detection that is based primarily upon malware already seen and identified is doomed ultimately to fail. The only solid foundation for malware detection is the principle that: "Any unauthorized instruction set injected into a system constitutes malware." It does not matter if, for the nonce, those instructions do not seem to be engaged in malicious activities. They may be benign today, but horrifically destructive six months down the road.

Malware Detection that is Comprehensible

All security, especially cybersecurity, is a human endeavor. As such, all cybersecurity measures must be logical, reasonable, and comprehensible for all engaged in that endeavor. The mystical, arcane, esoteric (and often meaningless) buzzwords that are so ubiquitous in cybersecurity today are antithetical to real security. They harm far more than they help. True security, not security theater, requires that all participants understand the basic principles and concepts that they employing to keep their systems secure.

6. CRYTICA SECURITY, INC.

Crytica Security, Inc. has created a unique malware detection platform that adheres to all the above principles and suffers from none of the shortcomings explained in this document. For more information on Crytica's easily understood platform and its ability to detect malware at the time of injection, prior to launch, and to detect polymorphic, preemptive, AI-Enhanced, and AI-Generated malware, contact Crytica Security, Inc.:

Website: CryticaSecurity.com
Email: info@cryticasecurity.com