"New" Malware and Advanced Persistent Threats

A Warning

Crytica Security

7655 Town Square Way

Suite 212

Reno, NV 89523

Website: CryticaSecurity.com

Email: info@cryticasecurity.com

1. ADVANCED PERSISTENT THREATS (APTs)

> *a skilled military leader will strategically select when and where to engage in combat, putting them in the most advantageous position against their opponent*[1].

Massive Simultaneous Malware Attacks

Massive simultaneous malware attacks, those attacks that hit hundreds and thousands of devices all at once, do not suddenly emerge out of thin air. They are not the result of a sudden unstoppable wave of malware injections and infections. Instead, they are the result of careful planning and an on-going process of gradual infection. Although it may seem as if these massive attacks materialize all of a sudden, like Claudius sorrows[2], they typically result from a single, undetected infection. This infection then spreads slowly, propagating its malicious and undetected code throughout the entire environment; each new instance potentially becoming the source of a new epicenter of infection, and potentially propagating exponentially. Once the infection has spread sufficiently, a command is given that launches all of the malware in all of the infected devices all at once. As has been documented repeatedly, the results of these massive attacks are typically catastrophic.

2. WHY ARE APTs NOT DETECTED BEFORE THEY CAN LAUNCH?

One might assume that with all of the cybersecurity malware detection systems deployed across the vast Information Technology (IT) infrastructure, especially when those systems are augmented with Artificial Intelligence (AI), that it would be impossible for such massive malware infections to avoid detection for as long as they do. Of course, real world experience has shown over and over again that such an assumption of malware detection efficacy would be tragically wrong.

Industry statistics, collected for more than ten years, have repeated revealed an unconscionable inability to detect most of the sophisticated malware. The average malware "Dwell Time", that is the time between malware infection and malware detection, has consistently been over six months[3]; meaning that most malware is detected not by the cybersecurity systems' detection algorithms, but by the malware actually launching and wreaking its havoc.

Why Is Malware So Difficult to Detect

Actually, it is not true that malware is so difficult to detect, but rather the problem resides in the basis for most detection algorithms. Their underlying principle is flawed. Most detection algorithms detect through "identification", that is, they seek for the presence of previously documented, previously "identified" malware and thereby detect it. That way, they not only detect the malware, they simultaneously identify it. The obvious flaw in this logic is that they are, using this logic, unable to detect new,

---

[1] Attributed to Sun Tzu.

[2] "When sorrows come, they come not in single spies but in battalions." Hamlet, Act IV Scene V.

[3] IBM and Ponomon Institute annual *Cost of a Data Breach Report* published annually 2014-2024.

previously undocumented malware, unless that new malware has an uncanny resemblance to some previously documented malware. Consequently, any skilled Threat Actor (TA) who wishes to penetrate an environment and elude most cybersecurity systems, i.e., avoid detection, will simply create "new" malware, malware that does not sufficiently resemble previously documented malware.

Prior to the advent of generative AI systems, such a strategy required significant skill and cunning. The creation of sophisticated new malware was non-trivial. Today, however, generative AI systems are able rapidly to create malware the likes of which have never been documented before. These new strains of malware will easily pass undetected through all malware detection systems that rely upon identification for detection.

> Note: A very significant exception to the use of this manifestly flawed malware detection through identification strategy is found in Crytica's Rapid Detection & Alert (RDA) system. It does NOT rely upon previously documented malware in order to detect. It does NOT rely upon "identification" as its primary mode of detection. It is able to detect new and never before documented malware with the same alacrity and efficacy that it does any previously documented malware.

3. AN EASY WAY TO EXPLOIT THE "DETECTION-BY-IDENTIFICATION" FLAW

Even without using generative AI, it is easy to exploit the "Detection-by-Identification" flaw in malware detection systems. This is accomplished by creating some "new" malware out of the old, well-documented malware. The steps are straightforward:

1. Take any existing malware that one wishes to launch into an environment, even previously well-documented malware.
2. Encrypt that malware with a one-time random encryption key.
3. Package up the encrypted malware in a "wrapper" program. This is the "Payload". Upon execution of this "wrapper" program, this "Payload", it will:
    a. Decrypt the previously encrypted malware and then
    b. launch the now decrypted virulent malware.

    This wrapper program, the "Payload", is essentially a "new" strain of malware. As such, it will not be detected by any of the malware detection algorithms that rely upon previously documented malware. Its contents, consisting essentially of a well-documented malware program, will be invisible to the detectors guarding the systems because that malware, up until execution, is encrypted.

4. CREATING AN "APT" OUT OF THE "PAYLOAD"

It is relatively easy to create an Advanced Persistent Threat (APT) out of the "Payload" described above:

1. Package up the Payload in another wrapper program, the "Distributor". The "Distributor" will have the "Payload", inside of it. The only function of the "Distributor" is to propagate the "Payload" throughout the environment being attacked. The "Distributor" uses well-known malware propagation techniques to

navigate its way throughout its host network(s), replicating itself and leaving a copy of the "Payload" in each device it penetrates. Once again, it should be noted that the "Payload" will not be detected by any resident malware detection systems because its malware has been encrypted.

2. When the APT attack is ready to launch, a command is sent to each copy of the "Payload" to launch. The "new" malware, the "Payload" on each of the infected devices will execute. When launched/executed, the "Payload" program will decrypt the old, well-documented malware it contains and then launch it … but by then, in most cases, it will be too late to stop the multi-pronged attack.

5. HOW TO STOP NEW MALWARE AND APTs

As described above, it is very easy to generate "new" malware. Of equal, if not more concern, is that it is relatively easy, using "new" malware, to design and implement APT attacks. The only way to stop new malware and APTs is to detect them at the time of infection, preventing them for residing undetected, and, in the case of APTs, preventing them from being able to propagate. This requires a detection system that can detect "new" malware at the time of infection, one that does not rely upon identification for detection. Essentially, APTs, such as that described in Section 4 above are "new" malware. Therefore, the way to stop APTs is to use a malware detection, such as Crytica's RDA system, which is capable of detecting new malware efficiently and effectively, without reliance upon any previously documented malware.

Website: CryticaSecurity.com

Email: info@cryticasecurity.com

