Detecting 5th Column Malware

White Paper

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

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

… they come not single spies, but in battalions[1]

1. THE DANGERS OF 5TH COLUMN MALWARE ATTACKS

What Is Malware?

According to Wikipedia:

> Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.[2]

Although this definition is an excellent one, and the one that is generally accepted by the industry, it is too narrow for those seeking to detect malware before it can wreak its havoc. Rather, for those who must detect malware, a better definition is: "**Any unauthorized set of instructions injected into and/or resident in a device that can affect how that device operates**." If the instructions are not authorized by those whose responsibility it is to control how a device operates, then those instructions are malware. It matters not that those instructions "seem" to be benign. At the moment, they might seem benign, and six months down the road they will be locking up the device and/or exfiltrating confidential data.

The Growing Wave of Sophisticated Malware Attacks

Destructive malware attacks, including malicious computer viruses, ransomware, and the theft of critical data, are increasing in both their frequency and their efficacy. With the advent of "Generative AI malware"[3], that is, Artificial Intelligence (AI) created malware, the danger of devastatingly "successful" malware attacks is now increasing exponentially. Generative AI can produce more malware, more sophisticated malware, and more variations of malware than were ever previously imagined. Sophisticated malware is no longer in the exclusive purview of the truly talented and resource-rich malware creators. Catastrophically effective malware is now available to the cybercriminals of even mediocre skills and resources.

5th Column Malware

Perhaps some of the most dangerous of this new generation of malware is 5th Column malware. It is able to evade the vast majority of malware detection systems. It can then enter an environment undetected and, on its own time-schedule and according to its own plan of attack, accomplish its intended damage. It is, therefore, important to understand what 5th Column malware is, how it penetrates undetected, and how to prevent it from launching successfully.

---

[1] Shakespeare, *Hamlet*, Act IV Scene 5

[2] https://en.wikipedia.org/wiki/Malware

[3] "Generative AI malware" is malware that is created by "Generative Artificial Intelligence, the AI technology that is currently taking the world by storm.

© 2023 Crytica Security, Inc.

What are 5th Columns?

In common parlance, a "5th column attack" is one that is launched from the inside of a protected area. Although the precise origin of the term "5th Column" is subject to some dispute, it seems to have first been coined during the Spanish Civil War[4]. Some sources attribute it to Generalissimo Francisco Franco: "[T]here were four Nationalist columns approaching Madrid, and a fifth column waiting to attack from the inside."[5] The expression rapidly entered common usage. It has come to mean any attack that is launched by hostile forces that are already inside a defensive perimeter.

What is 5th Column Malware?

5th Column malware might be considered to be any malware that has managed to penetrate through the perimeter defenses and then, once inside, launches an attack from within the "protected" environment. However, that *modus operandi* is essentially how most malware works. Hence, a more focused definition is required for "*5th Column malware*."

A good working definition of 5th Column malware is "***malware that is infiltrated into an environment in a non-actionable format and then is converted into an actionable format (the format it must have in order to affect how a device operates) at the time that it is ready to launch its attack.***"

Typically, 5th Column malware takes one of two forms:

- Encrypted Malware – the malware is encrypted, in order to pass through the perimeter defenses (no perimeter defenses can detect encrypted malware). It is then subsequently decrypted just prior the launch of the attack.
- Disassembled Malware – the malware is disassembled into "non-malicious" component parts. These are then passed through the perimeter defenses (which again cannot detect them as being malware), and then reassembled just prior to the launch of the attack.

The second of these, the "disassembled malware", is analogous to a group of terrorists who pass individually through a security checkpoint, each carrying an "innocuous" component of a weapon (e.g., perhaps each carries a component of a bomb). Then, once past the checkpoint, they come together to reassemble the weapon and use it. In the cyber world, one can think of the "checkpoint" as being a system's (an environment's) perimeter defenses, e.g., a firewall.

To understand why 5th Column attacks are particularly troubling to the cybersecurity industry, it is important to realize that many of the most relied upon cyber defenses are "perimeter" defenses. As an example, consider how 5th Column malware might pass through one of the most relied upon and predominant mainstays of a cybersecurity infrastructure's perimeter defenses, a firewall.

---

[4] July 17, 1936 – April 1, 1939

[5] Ruiz, Julius (2014), *The 'Red Terror' and the Spanish Civil War*, Cambridge, p. 187

© 2023 Crytica Security, Inc.

2. FIREWALLS AND 5TH COLUMN MALWARE

Firewalls are very much the cyber analog to traffic checkpoints and guarded castle gates. At a firewall, all traffic coming in and out of an environment is examined and checked for legitimacy. Previously known malware can easily be identified and prevented from passing through. However, consider the insurmountable challenges to a firewall when the traffic contains:

- Malware that has not been previously identified. Since the malware is "new" and does not appear in any of the databases of known malware, the "checkpoint guards" have no way of knowing that it is malware.
- Malware that is encrypted. Since the malware is encrypted, it is disguised. Its true form is not visible to the guards, and so they have way of knowing that it is really malware. If it is encrypted, they can have no idea of what it really is.
- Malware that has been disassembled. Malware that has been disassembled into components and then sent in as piece parts rather than as a coherent whole is invisible to perimeter detectors. Since each individual piece of the malware cannot be identified as being dangerous, the guards have no way of knowing that what they are seeing is a component of something truly dangerous.

The latter two on this list can be considered 5th Column Malware. No firewall will recognize them as being dangerous, as indeed, they are not dangerous until:

- The encrypted malware is decrypted.
- The disassembled components of the malware are reassembled.

Even the programs employed by the malware to decrypt encrypted malware and/or to reassemble disassembled malware usually cannot be detected as being malicious. They are, after all, on their own, not malicious. They do nothing that is inherently malicious, nor inherently unusual. There is nothing dangerous in the process of decryption nor in the functionality of combining files/components. These are perfectly normal system functions that occur all the time as part of legitimate information processing. However, the result of these "innocent" activities is that highly malicious malware may now exist inside the protective perimeter, inside the environment that a firewall, or any perimeter defense, is supposed to protect.

3. GENERATIVE AI AND 5TH COLUMN MALWARE

Prior to the wide availability of Generative AI, the creation of quality 5th Column malware was a non-trivial task. It required expert skills and, often, significant access to high-quality resources. Generative AI has completely changed that paradigm. It has brought about the potential for ***the industrialization of malware generation***. Whereas previously, the creation of quality malware was an art, one that required skilled artisans to create, now, sophisticated malware can be "mass produced" in infinite varieties in "factories" that utilize the "cheap and available labor" of Generative AI systems.

© 2023 Crytica Security, Inc.

The effect of widely available AI-Generated malware, especially 5th Column malware, upon most existing malware defense systems promises to be catastrophic. Most current defensive systems, even those inside a defensive perimeter, rely upon:

- Artificial Intelligence
- Virus Signature Matching
- Previously Identified Malicious Behavior
- Threat Intelligence Compilations

None of these can be seriously effective against the coming wave of Generative AI produced malware attacks. Indeed, the recent track record for the "most sophisticated" malware detection systems, even prior to the appearance of Generative AI malware, has been abysmal.[6]

Consider:

- Artificial Intelligence – Defensive AI systems are based mostly upon pattern matching, using the patterns of previous identified malware. They stand little chance against the very new and innovative malware that Generative AI can produce, especially if that new malware penetrates an environment as 5th Column malware.
- Virus Signature Matching – The efficacy of Virus Signature Matching has been on the wane for years. The sheer quantity of new viruses[7] (even previous to Generative AI) and the polymorphic[8] (that is "shapeshifting") nature of many new viruses have rendered Virus Signature Matching almost totally obsolete, except for very old and often previously identified and cataloged malware.
- Previously Identified Malicious Behavior – Waiting for malware to launch, watching for previously identified malicious behavior, and then trying to stop the attack before it does "too much damage" is a very risky, and usually futile, strategy. The increasing sophistication of Generative AI malware will render this approach even more risky and far less reliable.
- Threat Intelligence Compilations – Intelligence gathering on the Dark Web and other known hangouts of the denizens of the cyber underworld has always been of questionable of value. No quality malware designer would post his/her latest and greatest creations on the Dark Web for all to see. Mostly, only "kiddie scripts" (very unsophisticated malware) and malware that has already been used

[6] "[In 2022] Organizations with fully deployed security AI and automation took an average of 181 days to identify [a malware infection]." *Ponomon Cost of Data Breach Report 2022*, p.24.

[7] "There are currently more than 1 billion malware programs out there", *Malware Statistics & Facts: Frequency, Impact & Cost*, Darren Craft, 16 February 2023.

[8] "Polymorphic Malware" is malware that dynamically changes how it looks and/or how it acts. Either over time and/or when it travels, polymorphic malware is designed to change its own features so as not to be recognizable by malware detection systems.

© 2023 Crytica Security, Inc.

for its intended purposes are posted "in public" and for sale, for the intelligence gathers to see. The truly new, sophisticated, and effective malware, the malware used in the most devastating attacks and in cyberwarfare, are kept confidential until they are no longer of very much value.

The malware produced by Generative AI, especially the newest and most sophisticated 5th Column malware, cannot and will not be detected by any of the above techniques. That does not, however, mean that cybersecurity is defenseless against such attacks. 5th Column malware **can** be detected; and once detected, **it can be stopped**.

4. DETECTING 5TH COLUMN MALWARE

A malware detection system that is powerful enough to defend against 5th Column malware must, **at the very least**, include the abilities to:

- Detect new and previously unseen/unidentified malware.
- Detect malware before it launches (optimally at the time of injection).
- Be resilient to malware attacks against itself.

Detecting new and previously unseen/unidentified malware

Although not all 5th Column malware consists of new and previously unseen/unidentified strains of malware, many are. With the onset of Generative AI, it can be expected that most 5th Column malware attacks will be "new malware". Thus, in order to be effective against 5th Column malware, a malware detection system must be able to detect new and previously unseen/unidentified malware.

Detecting malware before it launches

It is **always** better to detect malware before it launches. If one waits until after the malware launches, the race against time is often a losing one. Optimally, detection should occur almost immediately, at the time of malware injection. In the case of 5th Column malware, that means at the time of decryption and/or reassembly. Detection should not, and cannot, take place until many hours later; certainly not after the malware has already launched. This is especially true of 5th Column malware.

A significant component of the danger of 5th Column malware is that much of it does, and shall, fall into the class of Advanced Persistent Threats (APTs). An APT is malware that, before it finally launches, resides ("persists") undetected in its target systems for a long period of time, even many months. While doing so, it establishes the foundations for what is usually a devastating attack.

APTs are designed to have the time to prepare, to gather intelligence, to spread their tentacles across and throughout networks, and to position themselves to launch simultaneous and highly targeted attacks. During their "Persistent" phase they may analyze a system's defenses and determine how best to disable and/or get around those defenses. They may read communications within a system so that they themselves can send bogus, but legitimate seeming, communications, as a way of furthering their destructive behavior.

© 2023 Crytica Security, Inc.

APTs are the foundations upon which many of the most destructive attacks have been built. It is therefore imperative that malware detection systems be able to detect APTs rapidly, to detect them when they first enter a system as malware. APTs must not be allowed to "persist". With the advent of Generative AI and with the proliferation of 5th Column malware capable of injecting APTs right through all perimeter defenses, the "imperative" for rapid detection becomes that much more urgent.

Resiliency to "Preemptive Malware"

It is axiomatic that any defense system cannot function well if it is easily disabled. Preemptive malware is malware specifically designed to disable malware defenses. It usually does so prior to doing anything else. In recent years, there have been some spectacularly successful Preemptive attacks. The Hive Virus is one such example[9].

It is also axiomatic, therefore, that in order to protect against 5th Column malware, a malware detection system must itself also be resilient to Preemptive malware attacks. Otherwise, it will be vulnerable to the one-two punch of:

- A Preemptive Attack, to disable its defenses, followed by,
- The Injection of the Intended Malware Payload

That both of these types of attacks can be 5th Column malware is highly logical and highly probable. Therefore, in order for a malware detection system to be viable against 5th Column malware, it must also be resilient to being disabled by Preemptive malware.

5. DETECTING 5TH COLUMN MALWARE IS POSSIBLE

Currently, there is at least one malware detection system that can detect 5th Column malware. It is a system that meets all of the above listed criteria. That system is Crytica's patented malware detection platform. Employing it, or another that is equally as effective, is essential for all cybersecurity defenses. The logic is obvious: "If you can't detect, you can't protect ™ "; and that detection must be both timely/actionable and itself resilient to attacks.

As discussed above, 5thColumn malware is very difficult to detect. However, Crytica 's platform **can** detect even 5th Column malware. Therefore, it **is** still possible to protect the critical cyber infrastructure. For more information on Crytica's patented malware detection platform, its resilience to attacks launched against it, and its ability to detect 5th Column malware attacks, contact Crytica Security, Inc.

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

[9] See the US Cybersecurity & Infrastructure Agency's bulletin: "*#StopRansomware: Hive Ransomware*", Alert Code: AA22-321A, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a

© 2023 Crytica Security, Inc.