You Must Remember This: Memory-Based Attacks Are the New Battleground

The multitude of recent cyberattacks have a number of things in common: they are sophisticated, multi-pronged, use fileless techniques, and target applications at the memory level—largely invisible to conventional security products.

Attacks including WannaCry, Petya, NotPetya, SystemD, Industroyer, and Apache Struts all leveraged memory-based attacks to infiltrate, pivot, and hijack valuable data. What used to be viewed as arcane, theoretical attacks have now become easily accessible through the Shadow Brokers leak of NSA memory corruption tool kits. Now, even B-Grade actors have easy access to cyber warfare tools created at the nation-state level.

This new wave of attacks highlights some fundamental flaws in how most practitioners approach cyber security: we're not looking deep enough, we're usually looking backwards, and our reaction time is far too slow.

Not looking deep enough

Most security solutions focus on protecting against file-based attacks. While there is plenty to do here, it is well-worked ground with reasonable visibility for IT professionals. Precisely because incoming malicious files are easier to defend against, advanced hackers have found ways to dig beneath the surface and manipulate binaries at the memory-level or by using fileless malware (such as scripts and interpreted code) that activate legitimate tools on the victim's system, such as PowerShell or Java Script. It's like trying to guard a fence when the bad guys have dug a tunnel under your feet.

Looking the wrong way

Most security is inherently backwards-looking—identifying what's happened in the past, and hoping that the next threats will be similar. Some vendors claim to have "next generation" technology that can predict the future, based on artificial intelligence and machine learning. While these techniques can analyze more data, they still use a historical knowledge base consisting of traditional pattern-matching or heuristic models. Today's advanced hackers are extremely innovative and adept at fooling knowledge bases. In fact, AI is being used on both sides as hackers increasingly use machine learning to identify defenses and vulnerabilities.

Reacting too slowly

Whenever there is a major cybersecurity incident, the race begins—name the malware, create signatures, and push the patches out to customers as quickly as possible. But no matter how fast the reaction time is, the largest threats come from vulnerabilities that have not yet been discovered, named, and added to the

catalog of known patterns. For example, WannaCry exploited the SMBv1 vulnerability that had existing unnoticed for 16 years, and flew under the radar of most security products until massive damage was done. Cybercriminals have also become more adept at hiding their tracks, and memory-based attacks have natural persistence thereby becoming effectively invisible, even after a targeted machine has been rebooted or even reformatted.

The Next Frontier in Cybersecurity

The unchartered vectors associated with fileless and memory-based attacks requires a shift in thinking for effective security. Because hackers are not using binary executables, signature-based security, even if it leverages AI, is irrelevant. And by flying under the radar, manipulating applications at the memory level or using benign looking scripts such as web shells or Power Shell scripts, conventional security tools are blind to the latest attacks.

To counter these new threats, new technology has shifted focus to the applications themselves, at run-time. Rather than using the past to guess what's coming in the future, these systems deal with the present, asking a fundamentally different question—are your applications doing the right thing?

A good analogy for this process is a map. Imagine your application is traveling from San Francisco to Seattle, going through several known points—Sacramento, Reading, Eugene and Portland. If you use Google to map this route, there may be a few choices, but from each on-ramp to the next off-ramp, there is really only one correct way to get to the next stop. This is a process that's predictable and deterministic. If you suddenly turn right and go to Reno, something is seriously wrong.

Your applications may be complex, but they are predictable, if they're doing the right thing. By mapping the known correct behavior of an application, down to the memory level, it's possible to instantly identify deviations if your application is going off the rails. This deterministic approach does not depend on signatures or heuristics and is inherently precise, providing real-time protection from fileless attacks and attempts to trick applications into doing the wrong thing.

About Virsec

Virsec is an innovative cyber security leader protecting organizations from today's most sophisticated and damaging cyberattacks. Through its unique technology, Virsec definitively prevents zero-day threats, fileless attacks and memory corruption exploits that are invisible to conventional security tools. Virsec's patented Trusted Execution™ system deterministically stops advanced security attacks in real-time, delivering unprecedented accuracy, without false positives. Virsec is headquartered in San Jose, California with a global presence in Europe, Asia, and Australia.

As seen in SC Magazine

SC MAGAZINE

virsec

226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems