There IS No Cyber Defense

Bryson Bort

ABSTRACT

There is a general principle driving the massive cybersecurity ecosystem that has flourished from the beginning: the necessary trade-off in balancing ease of deployment, the simplicity of operation, stability, and efficacy. While the entire ecosystem is predicated on constraints inherent in the foundational architecture, most in the defender community do not realize or understand what these are.

Reliance on flawed fundamental assumptions from what worked years ago has led us to a deeply entrenched, but intrinsically vulnerable environment that is continually compromised by an endless number of exploits. Exploitation occurs in an infinite space that is unsolvable. We are building skyscrapers on quicksand, yet are surprised when they fall.

Well-intentioned defenders, faced with constant attacks, compensate for this situation in two primary ways. We enthusiastically buy new tools, of which there is an endless supply, promising not only new but better results. And we aggressively build overlapping defense-in-depth, seeking comfort from the expertly plotted proverbial Venn-diagram that illustrates the breadth of our robust defensive portfolios.

But what actually works? In 2017, a CISO confided to me that while breaches are terrible, no good, evil things, he looks forward to an intrusion. It's the only chance he gets at some level of real validation of his defense infrastructure—both what worked and what didn't.

In fairness, security product offerings typically start out being useful. Everyone is excited about the next great thing, but as it achieves enough critical mass, it registers on attackers' radar. Then the product's efficacy begins to diminish, leading at best to the disappointing but often seen product half-life.

Bryson Bort is the Founderr/CEO of SCYTHE, Founder/Chairman of GRIMM, and Founding Member of the ICS Village, a non-profit advancing education and awareness of security for industrial control systems. Prior, Bryson led an elite Computer Network Operations research & development (R&D) division that directly contributed towards national security. Because of his background as an Army Officer and extensive operational cybersecurity experience, Bryson's primary interest is advancing "cyber" to integrate with the warfare domains.

Bryson received his Bachelor of Science in Computer Science with honors from the United States Military Academy at West Point and completed numerous U.S. Army professional education courses in tactical communications and information assurance. He holds a Master's Degree in Telecommunications Management from the University of Maryland and a Master's in Business Administration from the University of Florida in addition to completing graduate studies in Electrical Engineering and Computer Science at the University of Texas.

Why a half-life? Because our well-established enterprise computer architecture positions the securityecosystem's primary solution as a kernel-level or Ring 0 module. At Ring 0, the module theoretically has complete visibility and access that software can have on a computer. Threads, hardware access requests, and memory are all managed here. So any general user-mode malware attempting malicious behavior would be identified and handled when it pursues access beyond the established parameters. This concept is architecturally sound.

Reality says otherwise. While the kernel is the logical place for a defense solution to deploy, maintaining kernel stability requires that the module operates predictably. That means it has to be in thesame place(s) every time. And that creates vulnerability. Once an intrusion detection technology reaches the tipping point of industry saturation, attackers take notice and work to exploit its predictable location. It simply becomes part of their development and test matrix. As malicious code deploys, the security module is avoided, disabled, or deceived by the intruding exploit.

Take antivirus, for example. Fifteen years ago it was the starting point for staying safe on your computer. Antivirus followed the classic example. Acting from the kernel, an antivirus program had full system visibility and thereby prevented the wrong things from occurring. Initially, these programs looked for malicious signatures, but as attacks became more sophisticated and complex, products were bolstered to identify malicious behaviors. Before long, antivirus technology was widely adopted, becoming the de facto ante for hackers to get onto a computer, and giving rise to industry giants like Symantec and McAfee. Vendors followed the same defensive approach because of the architectural tradeoffs, and as a result, they became vulnerable to the same flaws.

The ubiquity of antivirus solutions quickly challenged bad actors to find innovative ways of defeating them. Reverse engineering antivirus products ultimately revealed their predictability in regards to the kernel-mode security module, enabling attackers to work around a known constant and try successive penetration tactics until something worked. Symantec and McAfee got solved. The ante was met. The paradigm was established.

Hackers work to manage the "eyes". It's an eventuality. The solution resides outside of software's vulnerability. That is not going to happen. Such an approach is just too difficult, too expensive, and too resource-intensive to be practical. Thus we continue to build based on a foundation of what is intrinsically weak.

The one place an attacker is vulnerable is the network. As malware transits the established network infrastructure, it is harder for it to observe defender sensors and relies primarily on stealth. If you have a network tap, it cannot see it; if you have a transparent traffic manager, it cannot see that either. Its best chance at successful exploitation is attempting to innocuously blend in with other network traffic. Although identifying bad traffic from good is a complicated problem, many are trying to solve it. How successful that will be is unknown today. There is, however, one caveat to the network being a kind of safe haven and that is during instrumentation, even network devices are vulnerable to compromise.

Aside from network-level detection, hackers are only caught if they make a mistake, or if there is an environmental change that causes their malware to function outside of developed parameters. Malicious code must be precisely tailored to achieve its aims—it's like a thread through a needle, traversing a tightly woven computer fabric, but causing the computer to work in a way it was not designed. If there is a change to that "needle," the thread will miss such that it likely tips off a defender. For example, experiencing multiple Blue Screens of Death would undoubtedly trigger an investigative follow-up that would lead to the discovery of the instigating malware. But this does take time. There is an average of 206 days from breach to discovery. [1]

There are those who see machine learning (ML) and artificial intelligence (AI) as potential solutions to the pitfalls of predictable implementations. While ML and AI are enhancements that enable better data analytics, the fundamental data veracity and feature-selection is still questionable. How can you analyze what you never saw in the first place?

Consider how this works. Products incorporating ML are supervised: Someone curates the rules in the vendor's offline environment that will be pushed to the products. The curation will reduce both false positives and false negatives if done correctly. But this implies that the system only detects anomalies within the range for which it was designed.

On the attacker's side, new security products incorporating ML and AI are easily added to his or her testing cycle. The malware is validated against the test matrix, ensuring no tested product detects it.

For now, we have consigned ourselves to perpetually shifting quicksand when we need firm ground to build on. Recognize that. Understand the root cause. Suck it up. New intrusion prevention products may offer temporary relief, but just as a drunk man looks for his keys where the streetlight is already shining, staying in our comfort zone is not going to solve this problem.

Like death and taxes, exploitation is a certainty in life, so the cybersecurity focus should be on detection and response. Reducing the initial scope helps figure out what you've got that matters, then circle the wagons around your crown jewels to protect and control what you can.

NOTES

1. 2017 Ponemon Cost of Data Breach Study, https://www.ibm.com/security/data-breach.