The Eradication of Malware

Bradford Tuckfield

The history of warfare is a story of recurrent alternation between offensive and defensive supremacy. Malware technology today is in a state of offensive supremacy: like the time between the invention of the chariot and the development of the caltrop, we live in a time when attack is relatively easy and effective defense is especially hard. The cost of malware attacks – sometimes estimated in the trillions of dollars annually – represents a forced transfer from the innocent to the evil, and for that reason eradicating malware is not only an economic desideratum but also a moral imperative.

Some of today's worst malware attacks are perpetrated by botnets, which often require years of effort to take down. We need technical tools for quick counterattacks to efficiently destroy any botnet as soon as it starts to attempt malicious activities. Anti-botnet counterattacks also need careful cleanup efforts, to make sure that a destroyed botnet's machines don't get re-recruited to other botnets immediately after getting taken down. We also need better threat detection tools and utilities that improve the legibility of internet traffic so we can find botnets quickly and reliably.

We could also make huge progress in lowering the risk of malware attacks by strengthening some very fragile parts of the world's tech infrastructure. There are many small software projects that most of the world's top websites and supercomputers rely on, whose upkeep depends entirely on the efforts of a small group of part-time, unvetted volunteers. These volunteers are highly vulnerable to infiltration by malicious actors who could surreptitiously insert malware with the potential to cause global disasters. We could cheaply and easily provide the "adults in the room" that these projects desperately need, including transparently audited full-time professionals who pore over every line of code to ensure perfect security.

Malware has been with us for so long that it's easy to take it for granted and assume that it's just a natural part of the world or the price to be paid for the technology we love and depend on. But it's not so: just as we eradicated smallpox, so too can we eradicate malware. Malware defense projects need to be treated as public goods like roads or vaccines or clean rivers or aircraft carriers, and funded accordingly. It's time to energetically build defensive technology that will end the offensive supremacy of malware, fight evil and promote technological security and peace.

Bradford Tuckfield is the founder of Kmbara, a technology consulting company.