THE PRINCIPLE OF CHAOS AND ITS WAR AGAINST CYBER THREATS

CYBER 2.0



Erez Kaplan, CTO of Cyber 2.0

By Erez Kaplan

IN DIFFERENT situations of war, it always seems that one side precedes the other, and sometimes the opposite happens – the other side is a step ahead.

Why, then, in the cyber world, with thousands of cyber companies that employ the best minds in the world, the permanent situation is that attackers are always one step ahead and that a focused attack will always penetrate all the existing defense systems?

I have been preoccupied with this problem for a long time. Against all the protection systems deployed in the organization, and at every level of information security, attackers always manage to penetrate, spy, exploit and destroy.

The explanation is seemingly trivial: there is no system that cannot be hacked, so the hackers will always find a way to penetrate all the organizational defenses. It has always been so, and it is likely to be like that forever.

As a result, information security personnel are constantly in pursuit of the next hacking, preparing for the next penetration, and finding themselves drowning in a sea of alerts from various systems, all of which can eventually be bypassed.

The conventional concept is that every defense system is a type of perforated network, so the more layers we add to each other, the less likely it is that a future attack will penetrate the first layer, and even if it does not stop at a second layer, it will stop at a third or fourth.

Since each network has an additional cost, the more economically based the organization is, the more money it allocates to the cyber protection field, and as a result, it is more protected against future attacks.

Every new solution, which comes up now and then, comes to provide a solution for a new type of attack that until now has not been blocked by the existing defense systems.

Cyber systems in the world, both offensive and defensive, are based on biological models; for billions of years of life, nature

has established effective and advanced defense systems, and it's natural to investigate and imitate them. Yet, nature itself is in that infinite loop; the attackers find a loophole, change the cell model, develop resistance or create a new mutation. And nature, belatedly fashionable, locates and solves the problem. "Viruses" and "anti-viruses" are not terms accidentally borrowed from the world of nature.

It seems that cyber attackers are even more sophisticated than those in nature. For example, we can see cases in which attackers hack the organization's data through its users by sending a link or email, passing the known defense systems, and installing and disguising themselves as a known program: a macro browser, an upgrade of a PDF reader, etc., ostensibly with the user's consent (without the user knowing it, of course). In the next stage, after the malicious software has tricked the initial defense, it systematically neutralizes all the existing defenses and spreads over the Lateral Movement network, encrypts files, sends out information, enables remote control or just waits for instructions from its senders.

How, then, do you break this vicious circle?

In the first stage, I understood that the solution had to come from outside the biological world. It was not yet clear which world it would come from. Most of the difficulty stemmed from the fact that a new study was published every day, which breached the way natural forces worked, and tried to imitate them (how bees interact with each other, what fungi do, how viruses and bacteria deceive the defense systems in the body, etc.). It was clear that any such solution, based on one biological model or another, would suffer inherently from the same problems.

About three years ago, while listening to the weather forecast, I heard that they talked about it being fickle and unpredictable. The term that came up was "chaos." The dictionary defines chaos as disorder. However, "chaos theory" is a term from mathematics and is a term that expresses order – not just order, but perfect order; two systems that start from the same point and pass through the same path will always produce the same result. But the slightest change in one of the systems on the way will result in its increasing deviation over time – and a completely different result. Chaos systems are dynamic, with very high sensitivity to very small changes.

I thought it would be possible to build a system based on the same chaos laws, but using a mathematical axis instead of a time axis, and that the chances of it being hackable, even if all hackers in the world tried to attack it, would be equal to the chance that all forecasters and scientists would be able to breach the weather system, in a way that would allow them to give a very accurate forecast, for every minute of the day over the next 15 years.

I worked on this system for several years until I breached it. On this basis, I founded Cyber 2.0, which creates a kind of virtual protection in the range of computers, relying on the chaos of communication between them, and any attempt to topple, bypass or cheat the system will cause imbalance produced by the chaos between computers and block the malicious code.

All the systems that exist today in the cyber world work according to the same principle: first detection and then prevention. That is, they first try to identify the malicious software, and then warn them or stop them. Naturally, identification cannot be absolute. However, Cyber 2.0 skips a stage: blocking without detection, using the chaos principle.

Even in the blocking phase, we identify failures in the existing cyber systems, which are the result of the system being destroyed or bypassed by the attackers. As soon as the system fails or is hacked, blockage will fail too. Cyber 2.0 is programed to continue protecting the organization, even if it completely falls, is hacked, removed or modified.

How is this possible? The organization defines the software that is allowed to go out of the computer (dozens of software programs, all of which were installed by the IT managers, including email, accounting, Office, etc.), and we define it as "legitimate" software. Any software that is not defined as legitimate, whether it is not legitimate, new, an unknown virus, or any other program, will automatically be defined as "illegitimate."

Unlike all other cyber programs that try to stop what they think is not legitimate, the Cyber 2.0 system installed on each computer works the other way around: if the software is defined as legitimate, the system will scramble the port through which it leaves. At the entrance to the next computer, the system scrambles the port again, which then returns it to its original number, and enters the computer as planned.

If, on the other hand, the program attempting to go out is not defined as legitimate, the port at the exit will not be scrambled, but at the entrance to the next computer it will be scrambled and therefore will be blocked.

Why is the system so powerful? Because any attempt to bypass or penetrate the software will cause the malicious software to go out from its original port. However, from the start, Cyber 2.0 was supposed to let it go out from its original port, so the system's downfall or bypass will not cause any changes and the software will be blocked.

An attempt to change the list of legitimate programs is also doomed to failure, since the chaos mechanism will block it.

What does this actually mean?

This means the capacity to stop any cyber attack, of any kind, completely, including new and unknown attacks. In addition, there is no longer an unceasing race of attacker, defender, and so on.

Most importantly, there is no need for many layers of defense. There is no need to pursue and analyze alerts, and, primarily, the IT manager has peace of mind. ■

The writer is CTO of Cyber 2.0, a Tel Aviv-based company