Identify the "intrusion kill chain" to stop data breaches in their tracks

By François Amigorena, CEO, [IS Decisions]

To fight a cybercriminal, you have to think like a cybercriminal. If you know how attackers work, how they think and how they act, you stand a better chance of predicting what their next move is going to be — and stopping it before it happens.

The good news is that most attacks today follow a similar pattern. Attackers gain undetected entry by getting their hands on an employee's login credentials, before slowly but surely expanding throughout your network until they find some data of value. In fact the act of obtaining logins is now so valuable that compromised credentials are used in 75% of data breaches today.

But if you understand exactly how attackers conduct themselves at each part of this "intrusion kill chain", you can put a stop to it. So, here's the pattern cybercriminals will often follow.

Obtain credentials

The more endpoints a cybercriminal can access — i.e. smartphones, desktop computers, laptops, tablets — the more likely they are to come across data of value. Gaining access starts with a successful login, the credentials for which are often obtained by cybercriminals through phishing, often through pure patience using a key logger that monitors the key strokes of a user with elevated privileges.

The end goal is to reach an endpoint that has local admin access, and once a cybercriminal has that, there are a number of credential artefacts found in the endpoint's memory that attackers can make use of. This can include password hashes (for use in a pass the hash attack), Kerberos tickets (which can be cracked), logon session credentials (which are stored in clear text), and domain credentials (which can be cracked). Cybercriminals often turn to tools like mimikatz (which requires local admin privileges) to search through an endpoint's memory to find and obtain these artefacts, enabling the hacker to use the credentials with other hacker tools to establish authentication to additional systems.

Authenticate

Once a cybercriminal has gained entry (or enough credentials to facilitate authentication), the next step is to move laterally within the network, from endpoint to endpoint, usually via SMB (to access file systems), remote desktop, PowerShell remoting, and even WMI and RPC.

Establish control

Once an attacker has gained entry to another system, they need to gain control over it. However, the credentials providing initial authentication may not have elevated privileges on this new endpoint, which means attackers often repeat some of the same work from the first two steps in the kill chain, as well as use native and downloadable hacking tools to gain access as a local admin on each endpoint.

Establish stealth

Attackers see each compromised endpoint as a foothold from which they can propel deeper into your systems. So, to keep from being detected, threat actors "live off the land" by using native tools that naturally don't attract very much attention from IT administrators. They stealthily deliver payloads directly to memory to avoid running exes that may raise suspicion, and even redirect malicious traffic over allowed ports.

Establish persistence

Throughout each point in the kill chain, hackers modify an endpoint's configuration to maintain access — just in case someone in IT detects the intrusion. Using similar tactics to malware, attackers run scripts on system reboots or user logons, putting malware, tampered files, scheduled tasks, malicious services, registry entries, and any created accounts back into place, essentially repeating all the work done up to that point to ensure the hacker can persistently access the endpoint.

Stopping actors in the intrusion kill chain

Before you can stop an attack, you need to be able to detect one. But most organisations are poor at breach detection — on average it takes 146 days to detect a data breach, by which point it's much too late to mitigate the damage.

So what can you do about it? The first thing is to understand the *one* action that occurs in every single part of the chain of events I've described above — a *logon*. To obtain credentials other than via phishing, attackers must log on as an admin to a machine. To authenticate, attackers use multiple logons of varying types. To establish stealth, attackers log on with elevated access privileges to live off the land. And to establish control and persistence, attackers need to log on locally as an admin.

Next you need to keep an eye on all logins and any possible anomalies, like logons at strange times of day, logons from strange geographical locations, logons that occur concurrently, or logins that occur for the first time on a particular endpoint.

Keeping on top of all logon information though is difficult to do manually, but simple with technology that exists today. This kind of technology pieces together contextual information about any particular logon and builds up a profile of the person attempting to log on. It then flags anything out of the ordinary, like a logon from a strange location or time of day, immediately to your IT department while blocking the login attempt until you’re able to investigate further.

By auditing logons with technology in this way, you effectively drop the success rate of any attack to zero. Take away the hacker’s ability to log on, and you take away their most valuable asset.

IS Decisions has published a report on how to stop external attacks by addressing the horizontal kill chain. Download the report for free from the IS Decisions website.

About the Author

François Amigorena is CEO IS Decisions