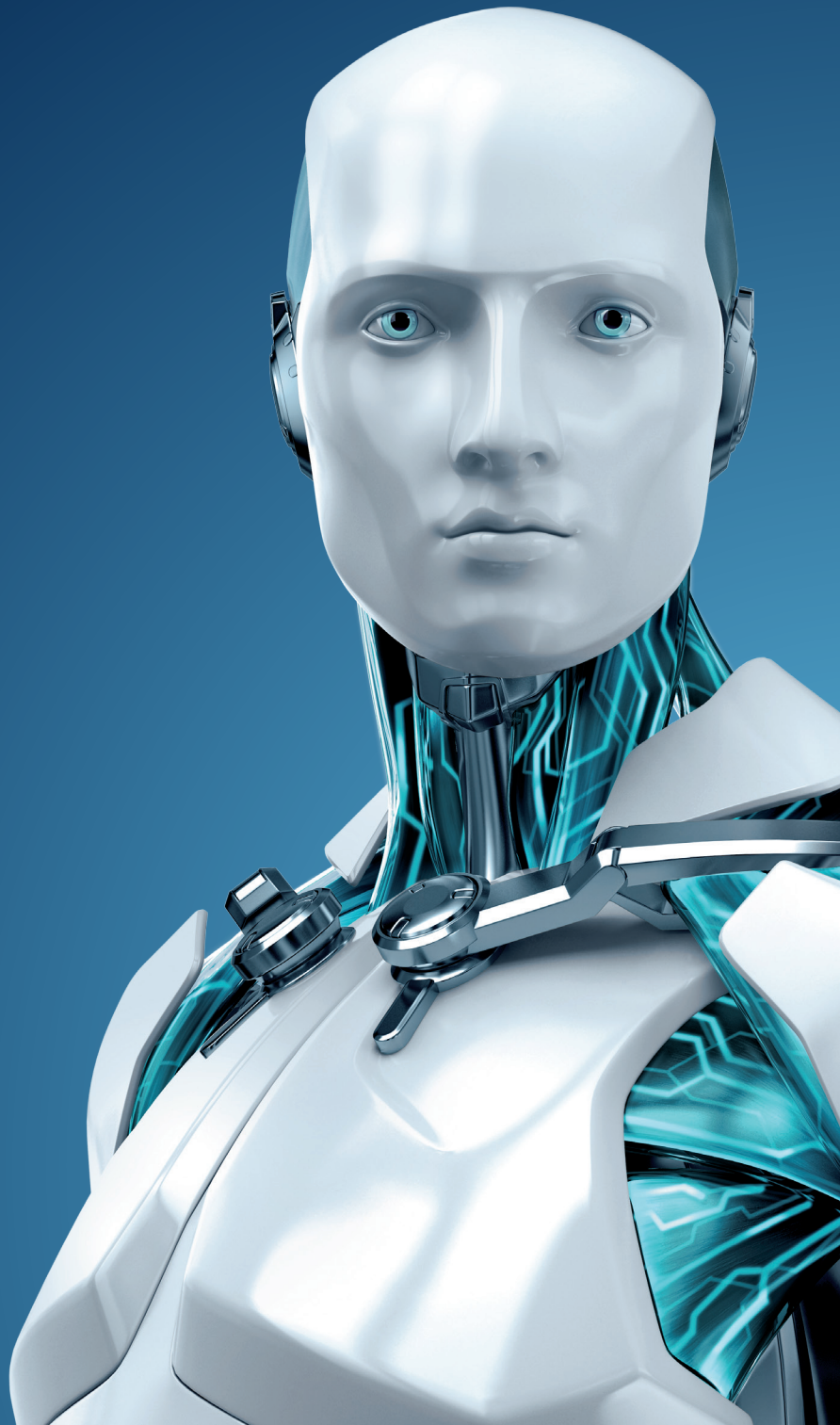
TECH BRIEF

Five steps to take after a company is infected



ENJOY SAFER TECHNOLOGY®

FIVE STEPS TO TAKE AFTER A COMPANY IS INFECTED

By Denise Giusto Bilić, ESET staff

As today's companies increasingly depend on digital assets, information security has become an even more critical factor of the business model.

We know that security is not a goal, but rather an ongoing process. As such, prevention and constant reinforcement of the outer edge of the corporate system are vital elements in the defense of assets in cyberspace.

But despite this, contingencies occur, and the risk of suffering a security breach must always be considered. Here's what to do in the face of this type of scenario.

STEP 1: Determine the scope of the infection

Time and time again, companies that have been victims of infections assess the traces of the impact just by using their intuition, rather than thorough analytical examination. Clearly, after detecting an infection at the company, reaction speed is extremely important. However, hurrying to make groundless appraisals can divert your attention away from the right actions to take.

If you've taken the necessary precautions and planned for this contingency, you can quickly gather the bits of evidence you need to answer some of the first key questions.

To begin with, establish which systems have been compromised and in what manner. Is the infection limited to a single piece of equipment or subnetwork? Has any sensitive data leaked out? Are we talking about corporate data, or private data relating to employees and/or customers?

STEP 2: Ensure continuity of service

In the case of an information leak that might compromise employees or end users, you'll need to warn them of a possible breach and advise them to watch out for any unusual activity regarding their data.

If any physical equipment has been seriously compromised, you must activate backup resources in order to maintain customer service. For this reason, it is critically important to plan ahead for attacks on availability by creating redundancy of equipment and connections. This, together with a clear plan of action in case of breach, will enable a rapid response to any events that lay siege to corporate security.

STEP 3: Contain the infection

Containing an infection begins with isolating the equipment that has been compromised. Shutting down the segments of the network that include this equipment prevents the infection from continuing to spread throughout the corporate network, and interrupts any connection that may have been established with the attacker for the purpose of stealing information.

If the traffic generated by the malicious agent turns out to be encrypted, your analysts must try reverse-engineering it to obtain the cryptographic keys. However, if communication is taking place on non-confidential protocols like HTTP, it will be exponentially easier to track the commands used by the attacker.

Either way, studying these commands can lead to the discovery of new infected equipment, and the generation of traffic patterns should be translated into firewall rules to quickly generate a first line of defense.

To achieve this, it is necessary to have correctly labeled traffic captures in order to speed up processing. Once again, this shows that proactive prevention and detection of threats are the cornerstone of information security that define a company's capacity to respond in times of crisis.

Because most of the procedures mentioned involve non-automated analysis of information, it's clear that you must plan a comprehensive solution in advance. This allows you to instantly deploy actions to block any harm that a malicious agent might attempt to inflict after penetrating your defenses.

The latest generation of ESET corporate solutions was developed to be a key factor in the containment process, preventing the spread of infectious components through the company's different transaction systems.

STEP 4: Mitigate the infection and eliminate the line of attack

Removing the infection involves a detailed analysis of the code to understand how it works. Antivirus solutions support this type of activity by enabling automatic disinfection and saving valuable time in the process of responding.

Remember that if the attackers are not completely eradicated from the network, they can resume their activity on the infected equipment through another line of attack. It's vital to isolate the flaw that allowed them to enter in the first place, and then remove it from the system.

Even after the affected equipment has been cleaned, there's still a risk that undiscovered infected equipment is still in operation. To prevent this from occurring, it's time to reinforce the analysis of the packets transmitted by the network—now that the communication protocols and commands used are known thanks to the analysis of the infection.

Changing the passwords on corporate networks is another preventive measure to take after detecting compromised resources.

At this point, it's worth determining whether the infection was the simple result of carelessness online, or whether it constitutes a successful link in a chain of persistent targeted attacks. If the infection was specifically targeting your organization, the real question to answer will be who lies behind these events, bearing in mind that another attack could be imminent.

STEP 5: Learn from any errors

Carrying out an in-depth investigation into what happened can help you improve security processes within the organization. Removing vulnerabilities whose existence was previously unknown provides an opportunity to reinforce the perimeter of the corporate networks by identifying potential weaknesses that had not previously been considered.

Infections are always absolutely negative events for a company. However, they offer opportunities to learn. They show which elements of the system's design need to be strengthened and they allow you to discover the flaws in your current defense measures.

At that point, you can determine whether you have the best possible protection and business continuity measures in place.

ESET security solutions provide multiple layers of protection for businesses in every industry, safeguarding each access point from gateways to servers and offering affordable solutions for mobile, cloud and virtual workplaces. In addition, our backup and recovery solutions deliver easy-to-implement backup and recovery to support your business continuity strategy. Learn more or request a consultation at www.eset.com