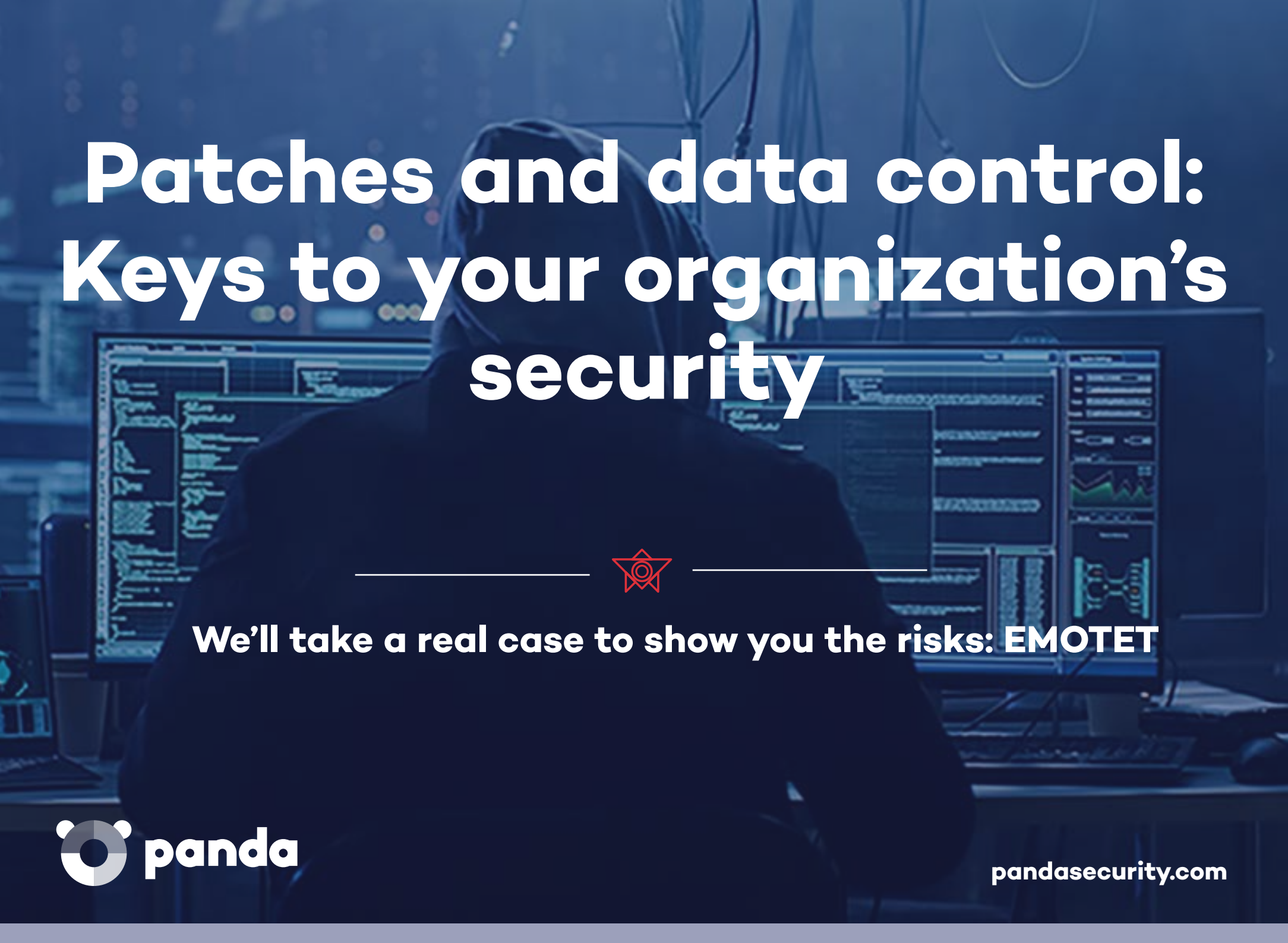


Patches and data control: Keys to your organization's security

We'll take a real case to show you the risks: EMOTET

panda

pandasecurity.com

Introduction

Emotet is a banker Trojan, polymorphic and difficult to detect using signatures. Its objective is to steal data, including user credentials stored on browsers or by spying on Internet traffic.

Given its effectiveness in terms of persistence and network propagation, Emotet is often used to download other malware, and is particularly popular as a tool for spreading banker Trojans, such as Qakbot and TrickBot.

Compromised systems are contacted regularly with Emotet's command and control (C&C) servers to find updates, send information from compromised computers and run fileless attacks with the downloaded malware.

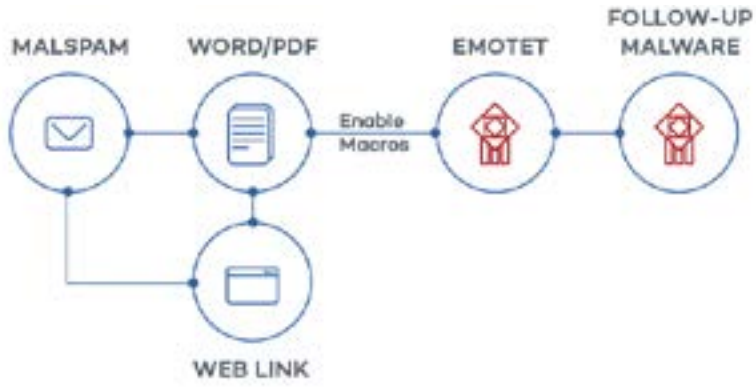
Once Emotet has infected a computer on a network, it exploits the EternalBlue vulnerability to spread and exploit endpoints with unpatched systems.

Emotet: How does it spread and persist?

Propagation

Emotet normally spreads via email, in infected attachments or encrusted URLs.

The emails may appear to come from reliable sources, as Emotet takes over the email accounts of its victims. **This helps to trick other users into downloading the Trojan onto their system.**



Given the way in which Emotet spreads across a corporate network, any infected computer on a network will **re-infect others** that were cleaned when they join the network.

Persistence

Emotet is designed to ensure it remains on the infected system and become active even though the system is restarted or the session closed, etc. To this end, it creates:

- Copies of itself
- Registry keys with random names.
- Services to remain active.

Damage

Emotet is dangerous not only because of its unlimited ability to spread by exploiting the EternalBlue vulnerability, but also because it downloads and installs other malware, leaving the door open to any type of Trojan, spyware or even ransomware.

Possible **consequences** include:

- **Theft of personally identifiable information (PII)**
- Leaking of **financial and confidential information**, which can be used for blackmail
- **Theft of login credentials**, making other accounts vulnerable
- **Long remediation periods** for network administrators
- **Loss of productivity** of employees whose endpoints have to be isolated from the network

panda

Endpoint Protection

Protecting yourself from the Emotet campaign is not especially difficult as it spreads using **malicious spam**. Nevertheless, users in your organization may easily become victims of the **phishing** and **social engineering** techniques that are frequently used.

What makes this Trojan really dangerous is its **ability to automatically change its own code**, making it far more difficult for a traditional antivirus to detect it.

Fortunately, however, companies protected by Panda Security are protected from this Trojan, even if employees open the email and download the document.

What's more, organizations protected with **Panda Adaptive Defense** and **Panda Adaptive Defense 360** are also protected against any known or unknown variant, Trojan or malware that exploits the **EternalBlue** vulnerability.

Panda Adaptive Defense 360 is undoubtedly the best preventive protection against any type of known and especially unknown malware as it prevents it from running.

Its managed Attestation service for classifying 100% of applications and processes prevents them from running until they are classified as trusted.

For more information on ***Panda Adaptive Defense 360, r***efer to the product ***data sheet*****.** For more information on other advanced solutions from Panda Security, go to our website:

https://www.pandasecurity.com/business/

Response to incidents and remediation

Remediation

Cleaning a network infected with Emotet involves following some **key steps** as rapidly as possible:

1. Identify the **computers affected** by Emotet.
2. Eliminate malicious **executable files** and roll back **system changes**.
3. Find out (or request from the IT team) the list of computers **vulnerable to EternalBlue**.
4. **Isolate** vulnerable computers.
5. **Reconnect** computers to the network.

Implementing these steps **without the adequate tools**, automated and integrated in the security solution, is a **risk-laden** and **lengthy** procedure, which can even take months. During this time, an organization runs the serious risk of falling victim to this or any other cyberattack.

Panda Adaptive Defense 360, in addition to protecting against Emotet and all its variants, provides you with other tools that facilitate and speed up the response to a potential incident[1]:

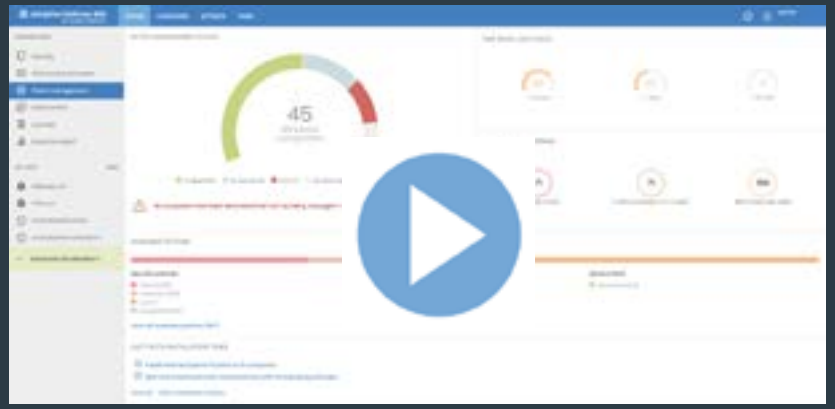
- **Automated remediation** that destroys all traces of Emotet.
- For each detection, you can access the **timeline of the actions** taken during the incident. This timeline lets you identify where and when the attack took place, how it entered, and what the malware or attacker did while it was active on endpoints.

[1] For example, in the case of a previously infected computer.

Don’t let your organization be next on the list

Simple patching and updating from a single management console

In addition, **Panda Patch Management**, which is fully integrated into the **Panda Adaptive Defense 360 management console**, automatically identifies all computers vulnerable to EternalBlue or any other operating system or program vulnerability, and patches all of them in real time from the console with just a simple click.



Video:Panda Patch Management

We advise all organizations not to wait until they fall victim to this or any other attack and to keep their endpoints updated at all times.

There is no doubt that Panda Patch Management facilitates and speeds up this task both for the IT Operations team and for the Security team, who must ensure that this measure for reducing the attack surface is applied systematically.

More information on ***Panda Patch Management*** is available in the **Data Sheet** and on our website:

https://www.pandasecurity.com/business/solutions/#patchmanagement

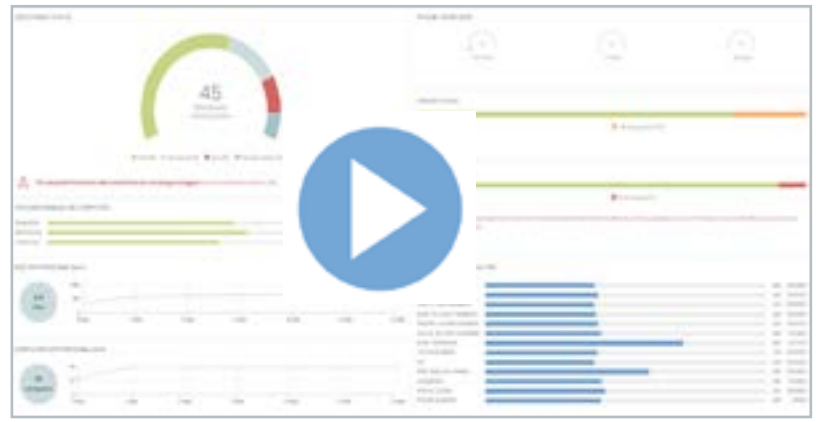
Control your organization's sensitive data

Panda Data Control

Finally, the presence of **Personally Identifiable Information (PII) or sensitive data that could attract attackers**, such as financial or confidential information, on users' endpoints represents a latent security risk for your organization.

Panda Data Control helps organizations and the data steward identify this information in unstructured files on endpoints across the organization.

This assessment is the first step in the data breach risk management program. The **automated classification** of personal information, the **search** for sensitive information on endpoints, and the **inventory** and **data evolution analysis** are tools that help mitigate this risk.



Video: Inventory of personal and sensitive data files in Panda Data Control

For more information, refer to:

- The **Panda Data Control** product data sheet.
- Our website at ***https://www.pandasecurity.com/business/modules/#datacontrol***

panda

More information at:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

by calling:

+0 00 00 00 00

or by email xxxxxx@pandasecurity.com

panda