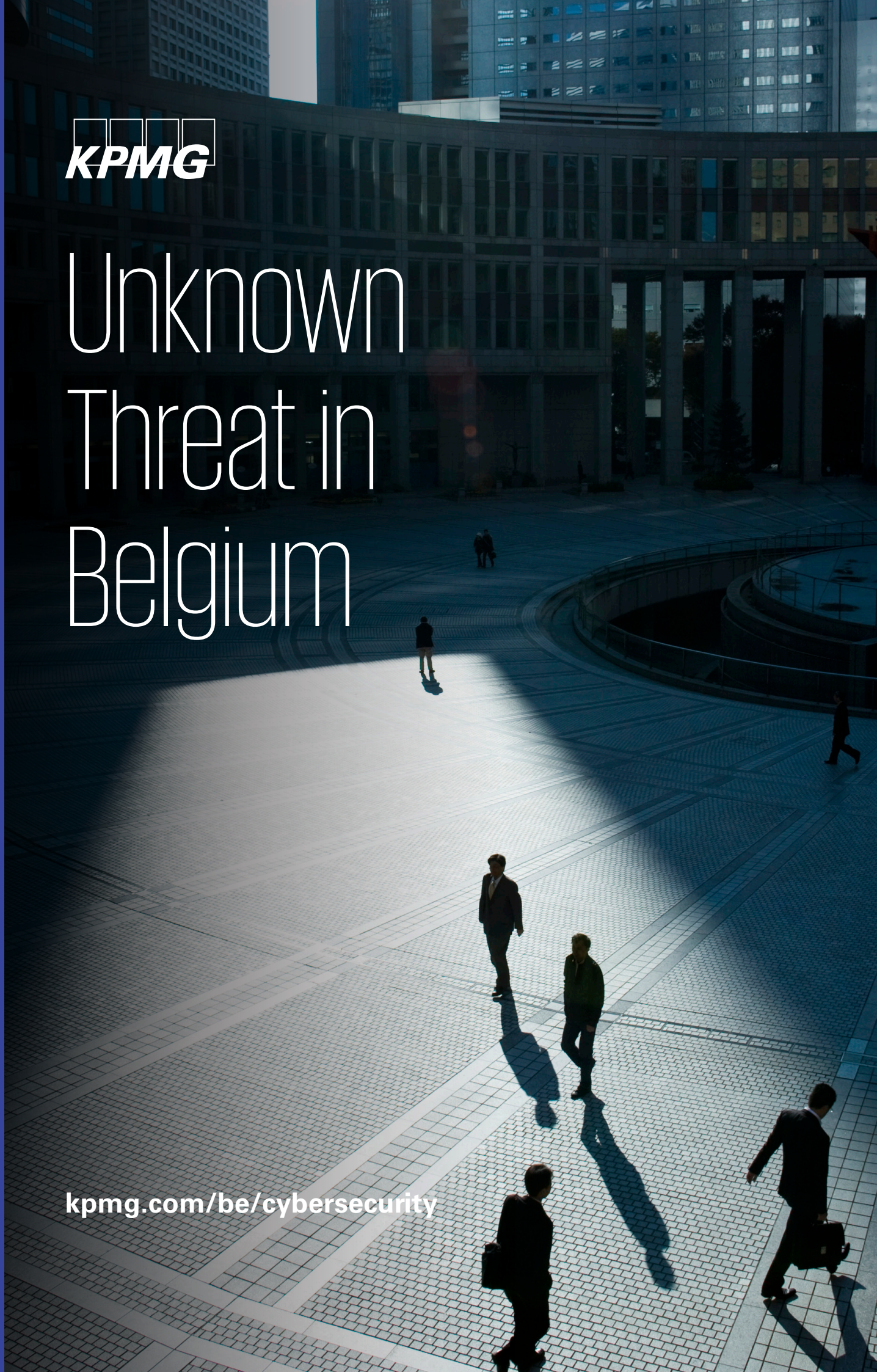

KPMG
Unknown Threat in Belgium
kpmg.com/be/cybersecurity

Contents

Technology support provided by
Exclusive Networks and FireEye

Introduction

Cyber security is a persistent business risk with an impact that can now extend from the executive board to the organization's bottom line. The risk is constant and serious, but are Belgian firms prepared to defend against, and detect modern cyber threats?

Concern over cyber threats has reached a high as more and more firms are discovering breaches and vulnerabilities within their internal networks. Businesses have been discovering previously unknown threats within their network and consequently suffering from reputational damage and direct business losses.

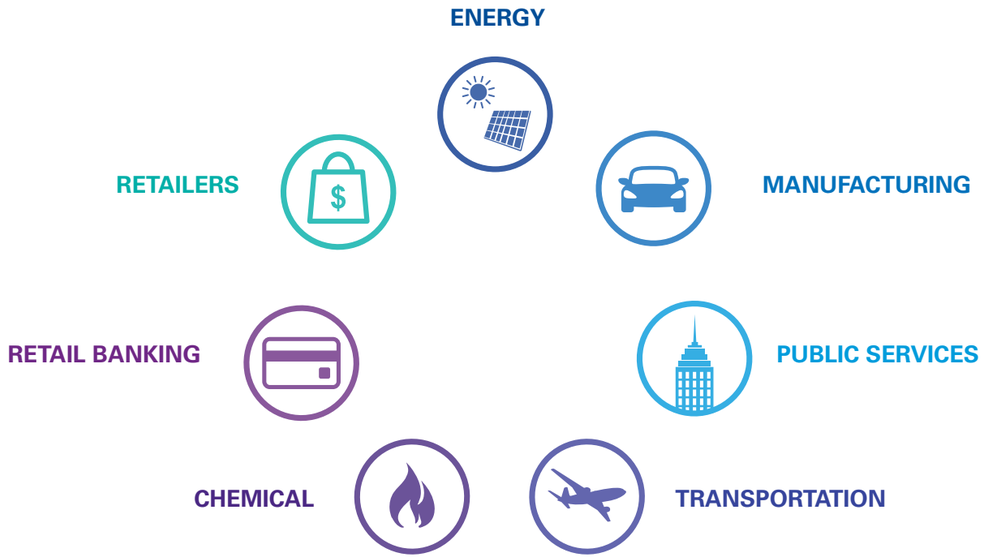
We wanted to know more.

In order to better understand the threats companies are currently facing, we, KPMG in Belgium, organized a study to analyze network traffic inside 10 different enterprises operating in varying sectors in Belgium. The goal of the study was to determine whether unknown threats were hiding within organizations' infrastructure and if current information security practices and technology were effectively preventing and detecting these threats.

This study started in November 2014 and continued through June 2015. The technology supporting the study was provided by FireEye, a leading vendor in advanced attacks prevention technology, cyber security intelligence and is responsible for the M-Trends report, an influential Cyber Intelligence report on threat actors and cyber terrorism groups. Over the course of eight months, we placed 10 advanced threat detection appliances within company networks to see what we could find. The results are now in.

Prevention isn't dead.
But it's certainly not enough.

Our greatest takeaway from this study is that traditional prevention techniques used by companies are not enough. The most common information security practices have not evolved sufficiently to prevent and detect modern threats. During our study we found enterprises both big and small which were infected with malware, although all are following traditional best practices in prevention.



Observation #1:

Most firms were breached, but didn't know it

Detecting modern malware that has already gained a foothold in the network is difficult, and firms are not succeeding.

All participants in our study were followers of traditional IT best practices: up-to-date antivirus, anti-spam gateways, internet gateways & proxies. However, we noticed how difficult it is for these technologies to detect malware that is constantly changing the way it looks, talks, and behaves.

We placed FireEye appliances to analyze network traffic right before endpoints – this means after all other network protection solutions have determined the network traffic is clean. We were able to determine when malware bypassed traditional defenses and reached an endpoint.

Most modern malware that wants to achieve something must send messages "back home". These messages are called callbacks and they are sent to Command and Control (C&C) servers.

If we detected a callback, this means that the malware had successfully installed itself on to the host and was ready to start achieving its objectives. With 80% of our participants, we observed that malware running within the network was actively communicating back to the internet.

80%
OF PARTICIPANTS WERE ALREADY BREACHED
THESE FIRMS HAD ACTIVE MALWARE INFECTIONS

Modern malware changes so often that traditional solutions for generating alerts are no longer effective.

We found that most of our participants relied on the following alerting mechanisms in order to detect malware running in their network:

- **Reporting from network gateways of denied requests** – network proxies are effective at recognizing and blocking domains and IP addresses known to be malicious. If an endpoint tries to access one of these addresses, they will be blocked and an administrator can be notified.

- **Reporting from antivirus software –** most commonly, our participants only knew about their malware infections if their antivirus software reported it and an administrator was notified.

We captured Zeus malware samples that were successful at compromising endpoints and found:

- The command and control servers used by the malware were not black listed on any reputation list, meaning they would not be blocked by IP reputation filters such as web proxies.

- When analyzed on VirusTotal, less than five of 52 available antivirus vendors could identify the samples as potentially malicious. The file hashes themselves had never been seen before.

- These shortcomings in signature-based and reputation-based detection contributed to these infections being successful.

Network solutions don't prevent enough malware traffic from reaching the endpoints.

For an endpoint to be compromised the host must be vulnerable to the exploit and the host based antivirus must fail to detect the malware. All participants in the study had up-to-date antivirus that did stop many infections, but not all. The trend of allowing so much malware traffic to reach the endpoint and trusting on antivirus to prevent an infection was found to be inadequate in sufficiently protecting networks.

In our study, all of our participants had malware traffic reaching endpoints. This means that either an exploit kit ran, a malware object was downloaded, or a callback was detected.

Your malware is unique, just like everyone else's.

In all of the malware we analyzed, we identified 59 unique samples. However, these 59 unique samples were traced back to only 11 families of malware. The task of antivirus being able to block so many variants of the same malware families is daunting.

The sophistication of malware and its ability to hide from anti-virus software is a contributing factor to why so many participants in our study were breached. So, having a unique malware sample does not make an attack targeted, but it underscores the difficulty in keeping up with malware.

In total

Malware binaries were downloaded

Unique samples

ZEUS is a highly prolific crimeware, focused on stealing user credentials

of participants had zeus infections

of participants had malware traffic reaching endpoints

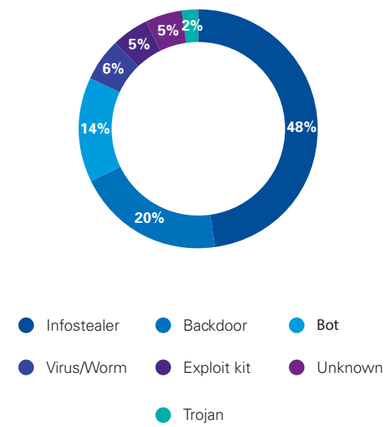
Observation #2:

Malware capabilities are extensive and dangerous

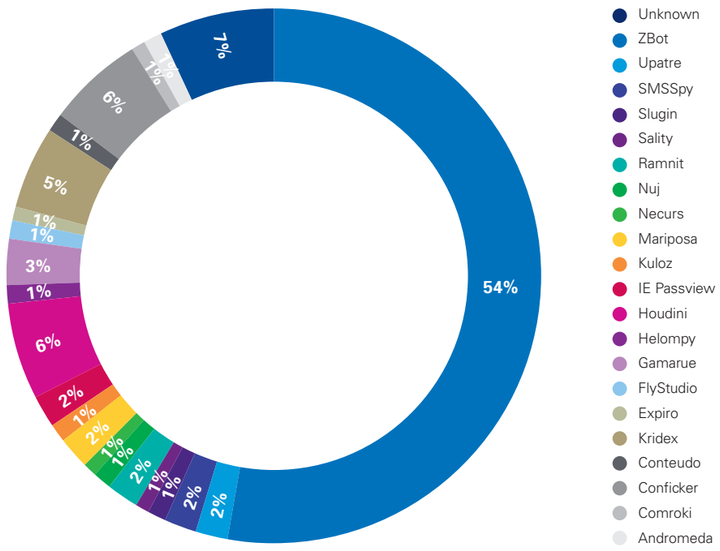
We divided our malware detections and samples into several groups based upon their capability:

- **APT** – Advanced persistent threat; a targeted malware that is sophisticated and from an attacker who is committed
- **Trojan** – malware that takes control of certain functions of the computer, usually to install other malware to perpetuate different frauds, leverage the endpoint for other attacks, or steal information from the user.
- **InfoStealer** – a Trojan that specializes in stealing information from the hard disk, the network, or sensitive user credentials, such as online banking logins.
- **Backdoor** – malware that grants full access to the system and often comes with lateral movement tools.
- **Virus/Worm** – malware that can spread on its own to other hosts, usually consuming network traffic, infecting legitimate files, and downloading other malware for further infections.

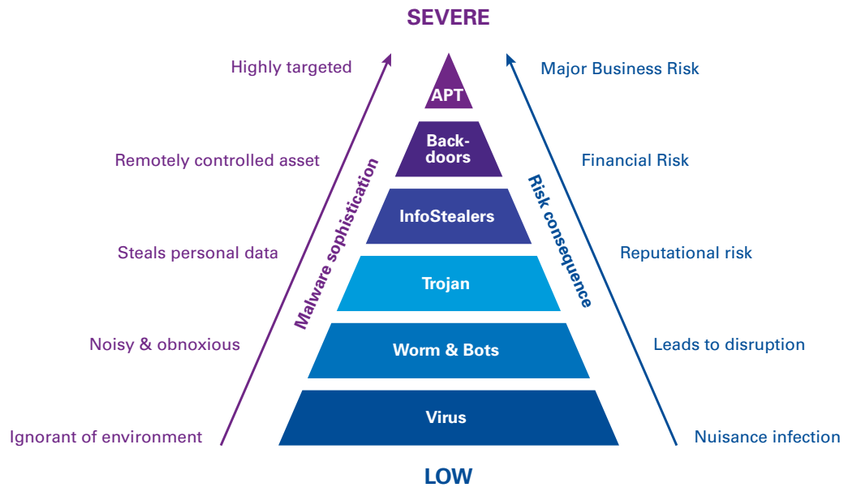
Distribution of Malware Types



Detected Malware Families



Understanding which malware has compromised an endpoint helps understand the business risk introduced into the network. Our threat intelligence did not attribute any attacks to an APT*.



While all malware infections present risks, we found several examples of very serious infections that represented major business risks.

The malware samples and detections we collected show both known and unknown malware affecting endpoints. By analyzing how the malware acted in a virtualized environment as well as inspecting the callbacks, we were able to better understand the risk posed by the malware.

Conteudo Trojan

Conteudo is a highly functional remote access Trojan that is able to hide its presence from the operating system. Once it has infected a machine, its success is reported back to its controllers who then sell access to the machine on the black market. For one of our participants, the credentials and login URL to their SAP system were sent in clear text to an external attacker so they could be used later to gain access to the system.

Houdini Backdoor

The Houdini backdoor is a remote access trojan that allows an outside attacker to gain full control of the infected endpoint. This trojan, which is based upon Visual Basic Scripting (VBS), has been known to target the international energy industry in spam email campaigns. This malware uses special techniques to avoid being detected by antivirus. Once a system is infected, the malware will report its existence to its controller and allow the attacker to begin moving data off the network.

Zbot Citadel InfoStealer

Originating from the Zeus family, the Citadel variant of Zeus is a premier crimeware kit with features exceeding that of its predecessors. Citadel is known to use excellent encryption features to hide its stealing of user credentials. Once it infects an endpoint, it monitors important processes in order to steal usernames and passwords. The malware is particularly dangerous given how it targets password managers commonly used by businesses, including Nexus and Keypass .

*APT attacks have been known to use the least sophisticated method necessary to breach an organization. While we did not observe any malware known to be in use by an APT group, we cannot conclude that no targeted activity took place as this was out of the scope of this particular study.

Exploit Kits: The malware delivery eco-system

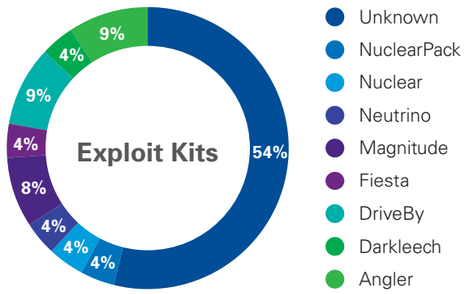
During the study, we observed both spam and exploit kits being used by attackers to compromise endpoints. While spam relies on an unsuspecting user to download and run an attachment, an exploit kit can succeed without user intervention. Exploit kits will take advantage of a known (or zero day) vulnerability in the user's browser to deliver malware. Something of note was the occurrence of the Angler exploit kit which delivered malware that breached multiple participants. Angler is a highly advanced exploit kit designed to avoid detection from traditional security controls and deliver malware to endpoints through very sophisticated means.

Regardless of how opportunistic some malware infections may be, it's still an attack, and bad things can happen.

Behind every malware there is a person who has an objective and is seeking to steal or disrupt its target. The motivations vary by who's doing the hacking, but all modern malware that wants to achieve something must send messages back to the internet. These callbacks are the key to the malware achieving its objectives.

A callback signifies a successful infection and a breached endpoint.

The messages sent by the malware can be anything from a notification to a hacker that the attack was successful, to updating its own software code to remain more stealthy. These messages offer proof that an organization was compromised. For an attacker to be successful, it needs only to compromise a company once. In this study, we observed some participants who had been compromised multiple times by unknown attackers.



Observation #3:

Malware is mimicking normal internet traffic to avoid detection

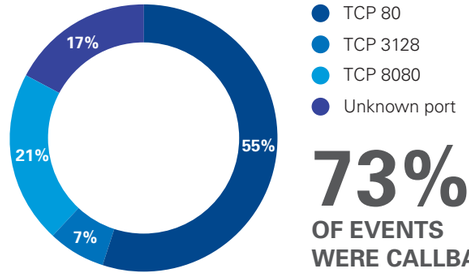
We found that most callback traffic was sent through TCP port 80 because this port is not normally blocked at the firewall. Once these connections are established, the malware begins to install other components and steal data.

We observed data being stolen during the course of our study. When the data was not encrypted and we could see what information was being stolen, we saw:

- SAP User Names & Password credentials
- Operating System and host details
- Internal network information
- SMS Messages from Android Phones

We observed malware communicating through HTTP post requests and checking in several times a day to get new instructions or send internal data out of the network.

Callbacks by Destination Port

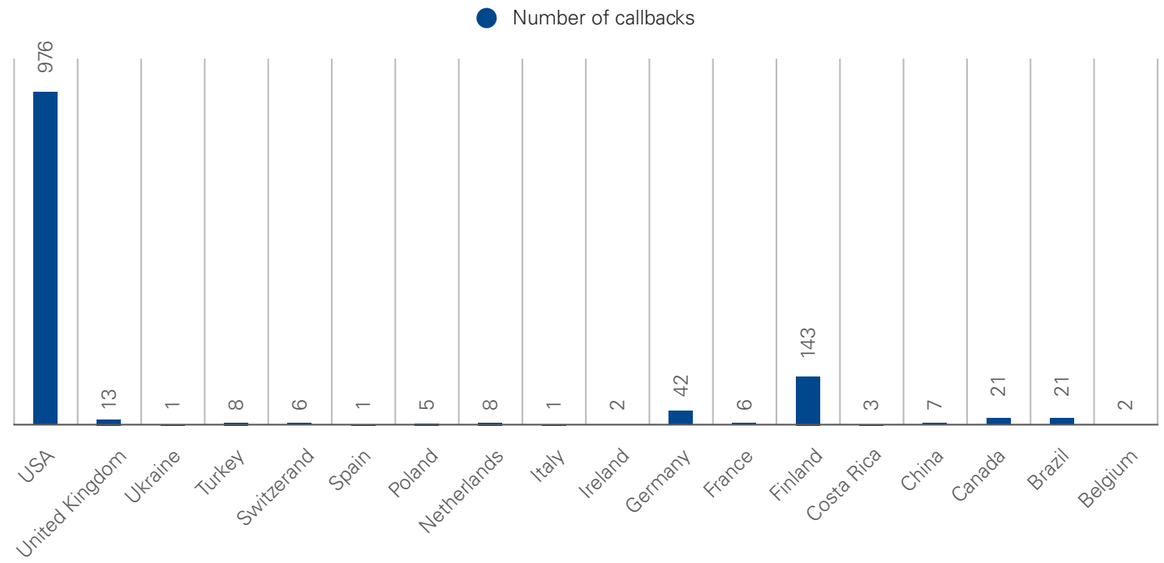


73%
OF EVENTS WERE CALLBACKS

Callback destinations

The destinations of callbacks were geographically dispersed. The destination doesn't indicate the hacker's location. Only the location of the server the malware was talking to.

Number of Callbacks per Destination Country



A Business Perspective

Cyber threats are now recognized globally as one of the most serious threats to business. The risk is real and defenses have not kept up.

An organization facing the risks similar to what we identified in our study should consider the following key business impacts:

- **False feeling of security.** Our observations showed that many firms believe they are secure, when in fact they have been breached by malware that can accomplish significant damage to the business. This "unknown threat" when not recognized can lead to unexpected harm to the business.

- **Direct losses to business functions.** The reputational and liability impact of data breaches resulting from a malware attack can be life threatening to a business. With new European legislation introducing fines to breached firms on the way, in combination with the reputational harm caused by the theft of confidential client information, the direct losses from a breach can be significant.

- **IT expenditures related to a breach.** Downtime, investigation costs, and system rebuilds can force significant unexpected IT costs following a breach. The disruption and system damage could cause system replacements and reengineering costs.

Solutions to modern cyber threats

Responding to the threats outlined in this report cannot be adequately accomplished by any one solution. Firms should take a defense-in-depth approach that can constantly evolve to meet new challenges posed by cyber threats. The following are some good starting points of how firms should respond:

Complement signature-based defenses with solutions that do not use signatures. As seen in our study, malware evolves too quickly to rely solely on signatures. As an additional line of defense, new, behavioral-based analysis adds significantly to the ability to prevent these threats.

Focus on detection just as much as prevention. Modern attacks have shown us that you can take all the necessary prevention measures and still be compromised. This is why firms should understand where their most critical data and systems are and setup sufficient monitoring and detection mechanisms to determine if/when they are compromised.

Don't wait until an incident to find out if your network defenses and detection work. Organizations should regularly test defenses with red team exercises. These exercises are full-out attempts at compromising a network that allow you to know how well your people, processes, and technology respond to a cyber attack.

Conclusions

Firms in Belgium must continue to evolve and adapt to a changing threat landscape.

KPMG organized this study to understand the state of an unknown cyber security threat in Belgium. In our study, we monitored the network traffic of 10 organizations and used behavioral analysis techniques to identify attack traffic.

The most important takeaway from our study is that nearly all of the organizations that participated in the study were already compromised by malware on endpoints. This allows us to conclude that those organizations cannot be certain that their information assets are secured from outside attackers by traditional security protections.

Cyber security breaches have real consequences: direct losses, indirect losses, and reputational damage amongst others. Enterprises large and small should re-evaluate their security posture to determine their resilience to the newest malware threats.

All businesses and organizations should evaluate the following:

- Make sure that traditional information security controls are implemented and maintained. These are foundational to everything else an organization must do to protect itself.

- Know what your critical systems are and where your most sensitive data is stored. Good security that is aligned to the business takes into account the level of protection that's needed for each information asset.

- Raise awareness of the latest cyber security threats from End Users to the Board, the impacts, and their role in protecting the organization.

- Don't let preventative controls give the organization a false sense of security. Increase monitoring capabilities to detect breaches after they have occurred. Preventative controls fail to mitigate all risks.

Contact us

Want to know if you have been breached?

Stephan Claes
Partner
KPMG IT Advisory

T. +32 2 708 48 50
E. sclaes3@kpmg.com

Benny Bogaerts
Director
Information Protection

T. +32 3 821 18 93
E. bbogaerts@kpmg.com

kpmg.com/be

kpmg.com/socialmedia