Malware fundamentals

1 [Text on screen] The different types of malware.
2 Welcome, everybody!
3 Over the next few minutes we will discuss the changing malware environment, including the impact it has on individuals, its role in cybercrime, how it spreads, and, finally, how Kaspersky solutions can help you to get deeper and more comprehensive protection for your network.
4 *Malware,* or *malicious software,* is a collective term for all kinds of threats, including viruses, worms, and Trojans.
5 Of these, Trojans dominate the threat landscape.
6 Often people believe these terms all mean the same thing, but in fact, each term refers to a distinct type of malware.
7 A computer virus is designed to infect objects on a disk and travel autonomously from computer to computer.
8 This is often triggered by an individual's action, such as opening an infected email attachment.
9 A worm also spreads automatically.
10 However, instead of writing its code to multiple objects on a disk, it installs itself once, and then looks for another computer to infect.
11 Some worms—for example email worms—require the action of an individual in order to spread, but others—such as network worms—spread without the need for human interaction.
12 Trojans are named after the mythical Trojan horse.
13 This is because, historically, they were often malicious programs that masqueraded as something benign or even useful.
14 Some Trojans still work this way.
15 Someone might download at random in the expectation of the file performing a useful function, but instead, it carries out a harmful operation on their computer without their knowledge or consent.
16 A Trojan may also be installed silently on a computer when the victim visits a webpage that is being compromised and contains malicious code.
17 This code runs automatically when they view the page, and is referred to as a *drive-by download.*
18 Trojans are distinct from viruses and worms because they don't self-replicate but rely on a connectivity provided by the Internet.

19 There are several different kinds of Trojan, each designed to carry out a specific purpose.
20 For example, backdoor Trojans permit system access by an uninvited party, potentially allowing remote administration of a system.
21 Often they include a key logger that records every key pressed in the hope of finding out the victim's password or some other piece of confidential data.
22 Other types of Trojan include banking Trojans, which are designed to steal money from a victim's bank account, and Trojan downloaders, that download updated code to the computer.
23 More recently, we have seen the emergence of hybrid threats that combine the functionality of a virus, worm, and Trojan in one package, providing cybercriminals with greater flexibility in their method of attack.
24 Once a cybercriminal is in control of the computer, they can do pretty much anything, from collecting confidential data to sending spam.
25 The list is almost endless.
26 The first thing they will typically do, however, is connect the computer with other infected computers, effectively creating an infected network, commonly known as a *botnet.*
27 This infected group of machines can be instructed by the criminals in control of the botnet to do any number of things, from sending out thousands of spam messages to launching targeted attacks on specific organizations.
28 One example of this would be a distributed denial-of-service attack.
29 This is where thousands of machines send a small amount of data to one target to interrupt the normal running of a website, email server, or any other business system.
30 [Text on screen] How malware evolves.
31 When malware first emerged, it simply caused damage with no financial gain, commonly referred to as *cybervandalism.*
32 This could be deletion of files, renaming of data, or the erasing of data storage media.
33 Some were designed to do nothing at all, although they could have unintended side effects.
34 While viruses might not have been visibly running, a victim could sometimes feel them, perhaps through a sluggish machine or slow Internet connection.

35 Nowadays, the overwhelming majority of malware is created to make money illegally, often by collecting confidential data from the victim's computer.
36 To do this, malware is designed to install as discreetly as possible, running without disturbing the victim, and ensuring that the machine is up and ready to be used.
37 A damaged offline machine is of no value to cybercriminals, but an infected machine is a powerful asset, able to perform any number of tasks.
38 There has always been lots of speculation about the financial impact of cybercrime.
39 If you search on line for "costs of cybercrime," you will find estimates ranging from millions to hundreds of billions, but the illegal nature of cybercrime activities makes it impossible to give an accurate figure of how much it costs.
40 One thing is for sure: the growing volume of attacks makes it clear that it's highly profitable for those involved in the dark market that is cybercrime.
41 The threat landscape has been dominated for almost a decade by random speculative attacks on anyone unfortunate enough to be infected.
42 However, the number of targeted attacks is growing.
43 Such attacks are normally aimed specifically at one business.
44 The motives can vary.
45 Attackers may want to steal confidential business or customer data, damage a company's reputation, sabotage the normal running of an organization, or even make a political statement.
46 Targeted attacks are highly sophisticated, but they often start by tricking individuals into disclosing information that allows the attacker to access corporate systems.
47 The widespread use of social networks and the vast amount of data that we all post on line makes it easy to set up such attacks.
48 Since 2003 malware has been used for criminal purposes, targeting both businesses and consumers.
49 Commonly known as *cybercrime,* it's effectively the use of malware for profit.
50 The malware employed in cybercrime typically has some simple well-known objectives.

51 The first is to make money by stealing sensitive information, such as online banking logins, credit card numbers, or intellectual property.
52 This is identity theft, stealing the victim's online credentials and using these to impersonate them.
53 Cybercriminals can access accounts and use them in a number of ways, including simple theft, digitally laundering money, or selling on the data to other criminals.
54 Another objective of cybercrime is to extort money.
55 This is often achieved by encrypting the data with a password and asking for money to decrypt it.
56 This method is known as *ransomware,* and can be very lucrative, given the high value that an individual or business places on digital information.
57 Extortion of money can also take the form of what is known as *fake antivirus scam.*
58 These scams revolve around making someone believe they do not have adequate protection.
59 The bottom line is that the victim is asked to download, and pay for, removal of malware that isn't actually on their computer.
60 The way they work is very simple.
61 The online victim may see pop-up windows or an inescapable barrage of warning messages that seem to indicate the presence of malware.
62 Criminals even manipulate search engine results so that their adverts appear at the top of the search list.
63 Not only has the victim paid to remove something that doesn't exist, but the criminals now have their credit card details.
64 [Text on screen] How malware spreads.
65 There are several ways in which malicious code can spread.
66 Someone may be infected just by visiting a seemingly harmless website.
67 Cybercriminals look for security loopholes in web service.
68 This service may host more than one website.
69 Criminals hide their code in pages stored on the server, and when someone views one of those pages, malware is transferred automatically to their computer hidden inside the rest of the content they were expecting.
70 This is often referred to as a *drive-by download.*

71 As well as being served from infected webpages, malware may also spread via email, typically via attachments or links.
72 Malicious links can also spread rapidly through social networks like Twitter and Facebook.
73 Malware can spread through traditional storage media such as CDs or USB memory sticks.
74 Of course, since it's physical media, the spread of malware is significantly slower.
75 Malware doesn't always rely on human interaction to spread.
76 In fact, it often takes advantage of holes in software, also known as *vulnerabilities,* to infect other devices.
77 These vulnerabilities, or bugs, can be found within the operating system or in widely used software, such as Java, Adobe PDF Reader, Microsoft Office, or other applications.
78 These flaws are not uncommon, and cybercriminals exploit them in order to run malware.
79 With an ever increasing range of malware being created and multiple ways of it entering corporate networks, organizations need to ensure their businesses are protected.
80 [Text on screen] How to stay protected.
81 Virus analysts at Kaspersky analyze over 70,000 unique virus samples every day.
82 The bulk of these are modifications of existing viruses, commonly referred to as *variants.*
83 Historically, antivirus solutions have worked by searching for snippets of code that identify a known virus, worm, or Trojan.
84 These snippets are commonly referred to as *signatures.*
85 Kaspersky adds more than 3500 new signatures to its databases every day.
86 But we've seen a flood of malware in recent years.
87 So the days when we could protect our customers using signatures alone are long gone.
88 Kaspersky provides a range of proactive technologies to secure our customers from malware.
89 This includes heuristic analysis, sandboxing, application whitelisting, behavioural analysis, and more.
90 Kaspersky also has an extensive cloud-based infrastructure, called the Kaspersky Security Network, that provides analysts with intelligence on what's happening across the Internet and enables us to deliver more comprehensive protection than ever before.

91 All these technologies are used in combination to ensure that, even if a virus is new or unknown, we can detect it without a signature.
92 By applying multiple layers of detection, Kaspersky can achieve swift, accurate, and comprehensive analysis, offering the best protection against all the latest threats with minimal impact on system performance.
93 With Kaspersky security solutions our customers can truly manage and protect their network effectively, ensuring their staff and infrastructure are protected.