Social and phishing

Target: **Individual users**
purpose:
- Pre-attack Intelligence recon
- Build trust using fake social profiles
- Initial infection

Malware, zero-day and botnets

Target: **Endpoint systems and servers**
purpose:
- Obtain access to systems
- Create backdoors
- Establish command-and-control over large network of devices

Passwords and configs

Target: **Endpoint systems and servers**
purpose:
- Initial penetration
- Expansion of reach
- Escalation of privileges

Distributed denial-of-service

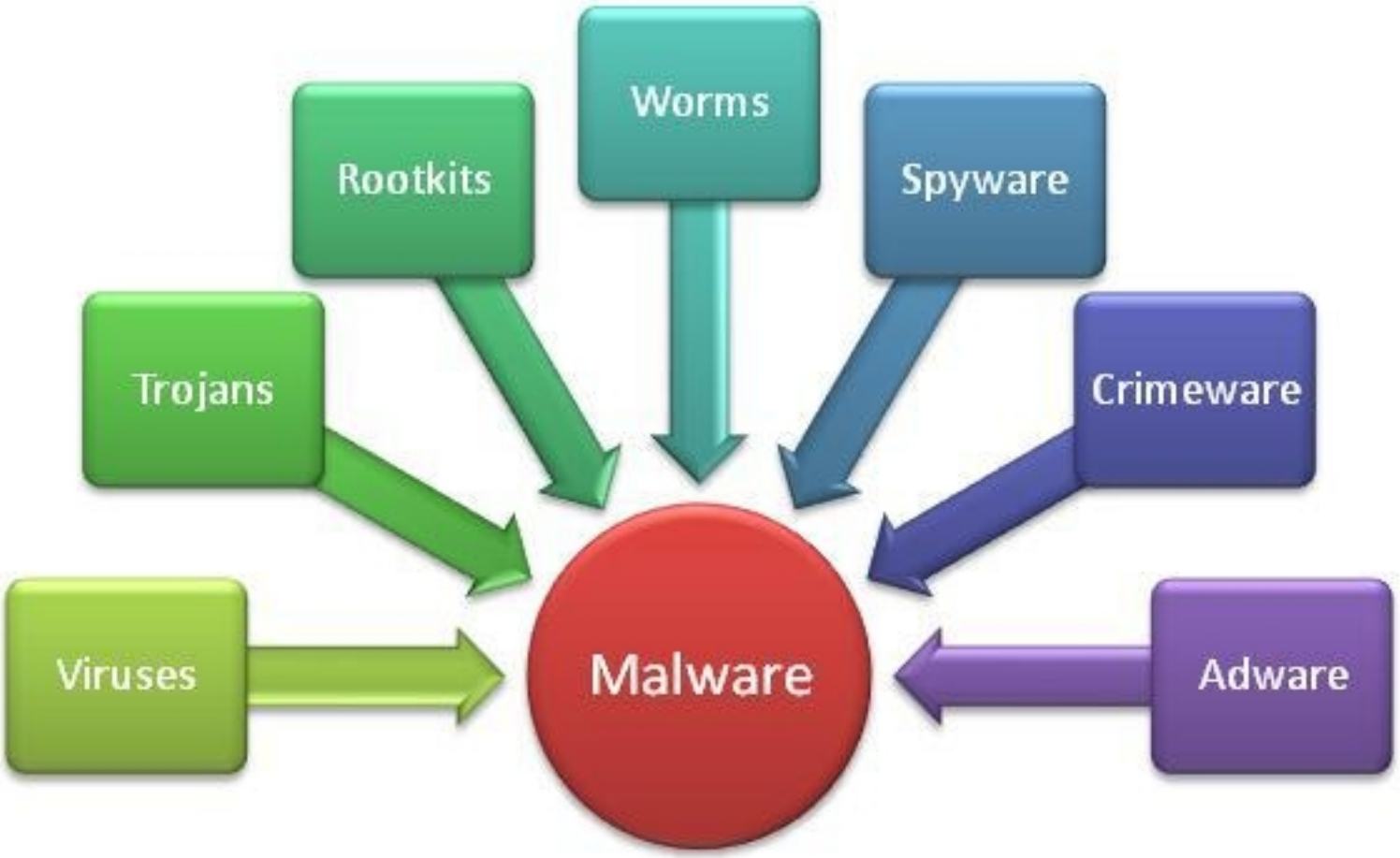
Target: **Network and application infrastructure**
purpose:
- Cause operational disruption
- Create diversion for other attacks

Smart and mobile hacking

Target: **Mobile and embedded services**
purpose:
- New attack surface and entry point to enterprise network
- Gain access to user data through vulnerable mobile OS and apps

SQL[1] injection

Target: **Database servers**
purpose:
- Obtain account and user credentials
- Steal sensitive data


Worms
Rootkits
Spyware
Trojans
Crimeware
Viruses
Malware
Adware

Firmware Security

AN OVERLOOKED THREAT

Firmware, the hard-coded software that frequently is stored in Read-Only Memory (ROM), is a vulnerable and increasingly attractive entry point for hackers. Solutions regarding firmware security – such as using manufacturers that allow enterprises to independently validate the integrity of their devices – are emerging, but many security professionals and their enterprises are not aware of the need for preparedness.

LACK OF A PLAN

FEWER THAN 1 IN 4
Enterprises fully include firmware in their enterprise's processes and procedures for deploying new equipment

MORE THAN 1 IN 3
Are not monitoring, measuring or collecting firmware data or are unsure if their enterprises are doing so

MORE THAN 1 IN 3
Received no feedback on firmware controls in compliance audits

ONLY 13%
Of security professionals' enterprises **HAVE FULLY IMPLEMENTED** controls for firmware

LACK OF PREPAREDNESS

ONLY 8%
Of respondents feel their enterprise is fully prepared for firmware-related vulnerabilities and exploits

MORE THAN 50%
Of enterprises that place a priority on security within hardware lifecycle management report at least one incident of malware-infected firmware

AT LEAST 70%
Of enterprises that do not place emphasis on security in hardware life cycle management feel unprepared to deal with an attack

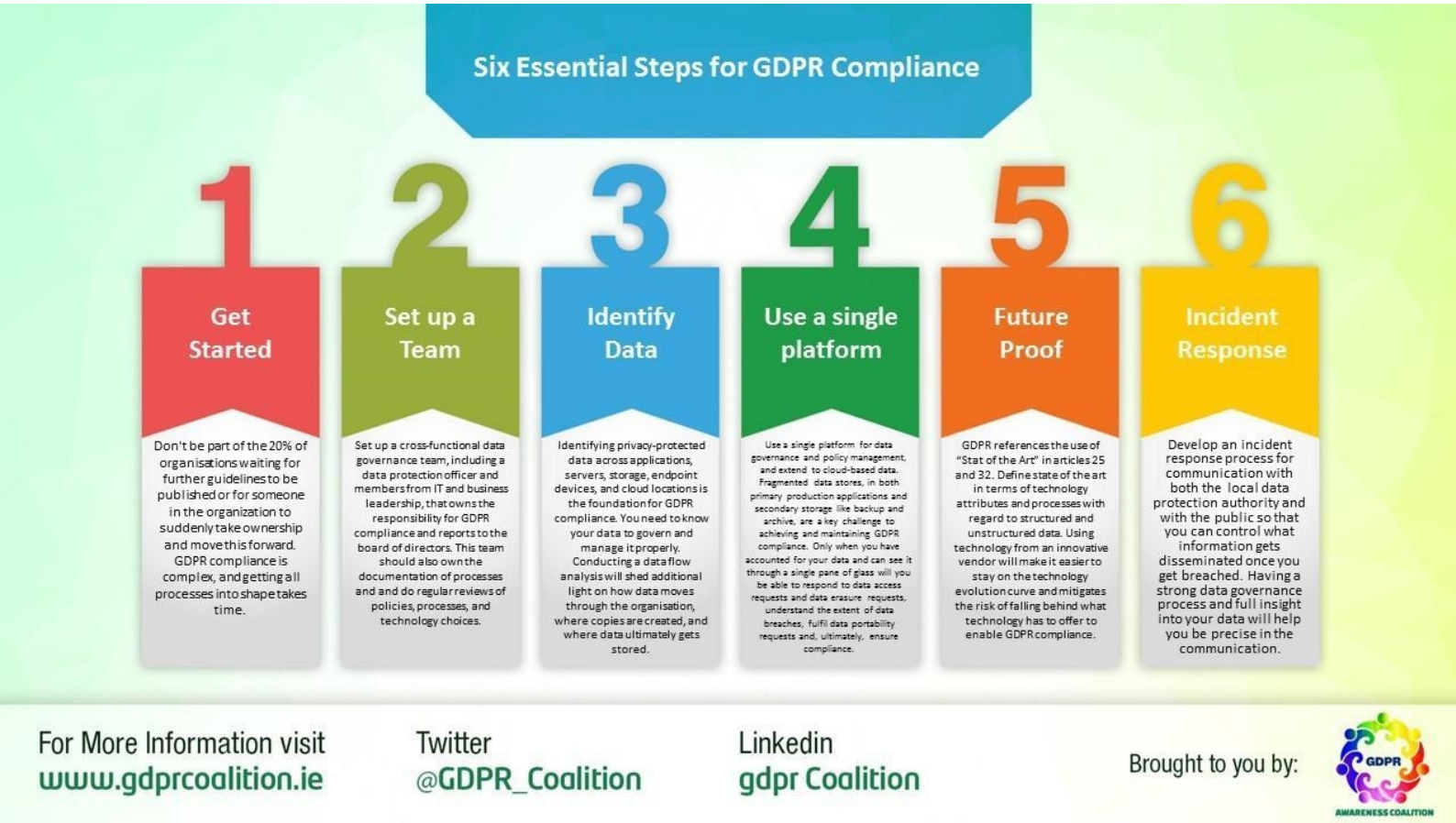
3 out of 10
Respondents who plan to implement firmware controls in next 12 to 24 months have had firmware malware introduced into corporate systems

Learn more at ***www.isaca.org/firmware***

SOURCE: 2016 ISACA Firmware Security Survey

CSX CYBERSECURITY NEXUS

ISACA



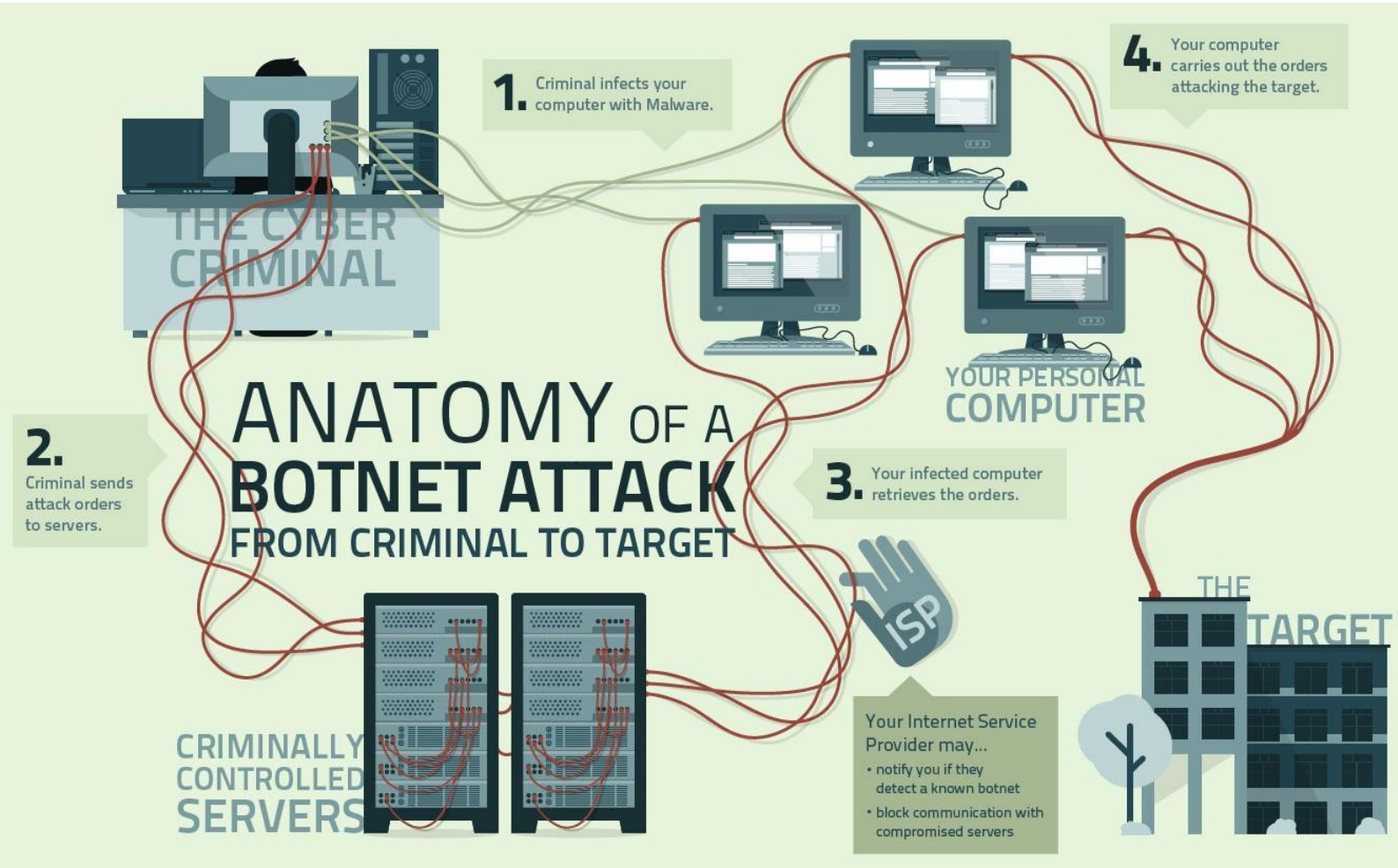
For More Information visit
www.gdprcoalition.ie

Twitter
@GDPR_Coalition

Linkedin
gdpr Coalition

Brought to you by:

GDPR
AWARENESS COALITION


1. Criminal infects your computer with Malware.
THE CYBER CRIMINAL
4. Your computer carries out the orders attacking the target.
YOUR PERSONAL COMPUTER
ANATOMY OF A BOTNET ATTACK
FROM CRIMINAL TO TARGET
2. Criminal sends attack orders to servers.
3. Your infected computer retrieves the orders.
ISP
THE TARGET
CRIMINALLY CONTROLLED SERVERS
Your Internet Service Provider may...
• notify you if they detect a known botnet
• block communication with compromised servers

CYBERSECURITY STRENGTHENS U.S. MANUFACTURERS

Cybersecurity protects the confidentiality, integrity and availability of your information.
A cybersecurity program provides advantages for small and mid-sized manufacturers:

- **Improve Recovery Times After Disruptions**
- **Avoid Potential Losses**
- **Protect Valuable Data**
- **Ensure Employee and Customer Privacy**
- **Mitigate Risks**

Reality of Cyberattacks and Breaches

55% of small and mid-sized business have experienced a data breach or cyberattack.

43% of all spear-phishing attacks are targeted at small businesses.

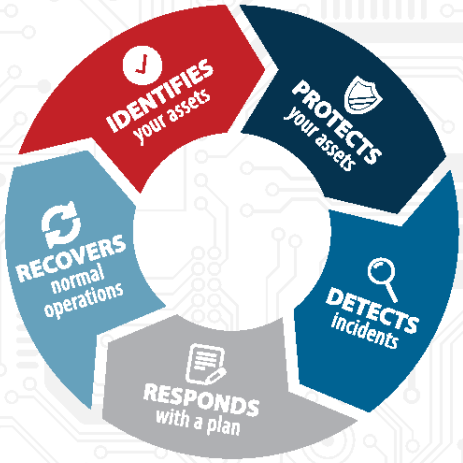
60% of impacted businesses are left severely impaired.

$38K is the average cost for a small business to overcome a data breach.

Common Types of Attacks and Breaches

5 Steps to Reduce Cyber Risks

Protecting the information of your company, employees, and customers is an ongoing process. Manufacturers will benefit from a program that:



⚠ Defense Suppliers: Compliance ⚠

Manufacturers in the DoD supply chain have until **December 31, 2017** to be in compliance with new DFAR cybersecurity requirements.

Learn more at **nist.gov/mep/cybersecurity**

Enhance Your Cybersecurity

Whether you're a manufacturer implementing a cybersecurity program, or a DoD supplier looking to achieve compliance, the MEP National Network can help you with your cybersecurity needs.

Contact your local MEP Center or learn more at **nist.gov/mep/cybersecurity**

MEP National Network www.nist.gov/mep 1-800-MEP-4MFG

Sources: Symantec 2016 Threat Report, Kaspersky Labs, Global Corporate IT Security Risks: 2015, 2016 State of Cybersecurity in Small and Medium-Sized Business

INFOGRAPHIC DESIGNED BY: 24K Creative, A Division of Gold Group

NIST National Institute of Standards and Technology U.S. Department of Commerce

6 THINGS GDPR IS:

1 A Total Data Protection Game Changer!

Global Applicability – applies to organisations anywhere who control or process EU citizen data

2 Applies Equally in all EU member states

As a regulation, the GDPR in directly effective, and does not leave room for jurisdictional interpretation of all its rules

3 Legislation with teeth!

For Irish organisations, this is a whole new world. The current Data Protection Act lacks the teeth to really punitively effect wrongdoers. New powers will be given to the Data Protection Commissioner to impose fines to a maximum of 4% of turnover/€20 million. Individuals will also be entitled to claim for compensation where they have suffered a loss.

4 Encouraging of a risk based approach to systems, strategies, product development etc.

The fundamental rights and freedoms of individuals to privacy must be balanced against the operations of the organisation. Risk assessments and in-built privacy considerations are to factor in every new approach taken by organisations.

5 Making organisations accountable.

The requirements for Data Protection Officer, Mandatory Breach Reporting and documenting compliance are pushing the onus on the data controllers and processors to prove they are taking individuals' fundamental rights seriously.

6 Long over due!

Privacy has never been so challenged and technology has never been so advanced. Legislators are finally catching up!

For More Information visit
www.gdprcoalition.ie

Twitter
@GDPR_Coalition

Linkedin
gdpr Coalition

Brought to you by:

GDPR AWARENESS COALITION

Advice for Customers

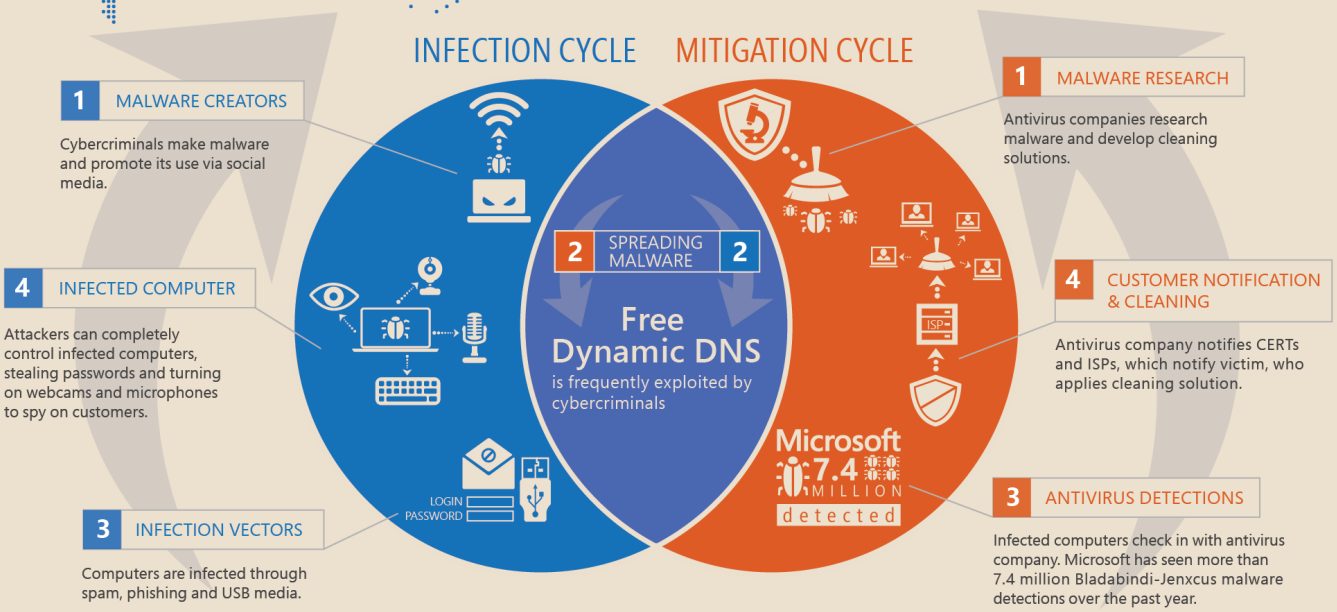
Keep operating system up to date

Install a current AV client/scanner

Don't click on suspicious emails, links or attachments

Who should keep malware at bay?

Bad actors exploit poorly managed subdomains to spread malware and control infected computers worldwide, leaving people and businesses at risk. See how cybercriminals take advantage of free Dynamic DNS and learn what you can do to help ensure a safe online experience.



Help keep your computer safe; visit www.microsoft.com/security

Microsoft

Pop-Up Ads

It pops up advertisements and various kinds of messages on a user's system.

Antivirus disabled automatically

Your real-time protection might be disabled. A full scan with an anti-malware program is essential.

New/unknown programs launching

It is probably a malware infection that was installed previously with some other software.

Web browser acting out of control

Browser Hijacking is a form of malware which makes your web browser begin to act weird.

Friends complain about spam

Accounts can be used to send spam messages to your contact list and spread malware to your friends' computers.

Slow-down of PC

Malware uses up available system resources leaving less space for other legitimate programs to operate normally.

Increased bandwidth usage

Due to an increase in network activity, internet bandwidth gets utilized at a faster pace.

Seven signs that your PC/laptop is definitely infected with a malware

RANSOMWARE
RESCUE PLAN

What is ransomware?

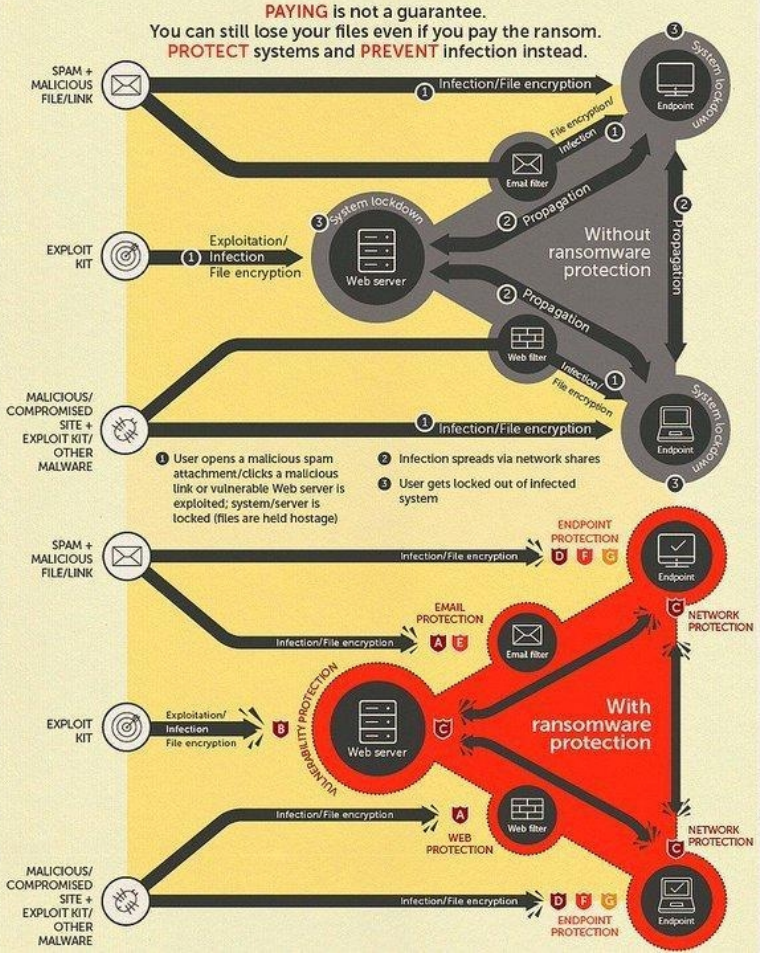
Ransomware is the term for malware that prevent or limit users from accessing their files or even computers. They force victims to pay ransom, usually in the form of Bitcoins, before they can get access back, hence the name.

Ransomware started preying on individuals but have since then become a huge threat to even the largest organizations. We've seen individuals, small businesses, and government agencies give in to ransom demands just to get back access to their files/systems.

How big is the ransomware problem?

- Trend Micro blocked **100M+** ransomware threats (September 2015–April 2016)
- Threats that use the ransomware business model spotted: **50** new families (January–May 2016) > **49** families (2014–2015)
- **US$325M** lost due to 1 ransomware family in 2015 —Cyber Threat Alliance (CTA)

PAYING is not a guarantee.
You can still lose your files even if you pay the ransom.
PROTECT systems and **PREVENT** infection instead.



Enterprises

Multilayered defense is key when dealing with ransomware.

- **Email and Web protection:** Prevent ransomware from entering your network by blocking spam and access to malicious links.
- **Server protection:** Protect servers from exploitable vulnerabilities.
- **Network protection:** Shield your network by preventing ransomware from spreading from server or endpoint to endpoint.
- **Endpoint protection:** Protect endpoints by preventing ransomware from running.

Small businesses

Two-layer ransomware protection works for small businesses.

- **Email protection:** Stop ransomware-laden spam from even getting to inboxes.
- **Endpoint protection:** Protect endpoints by blocking access to malicious/compromised sites and preventing ransomware from running.

Consumers

All it takes is one step to protect against ransomware.

- Block ransomware with a security solution that stops spam, prevents access to malicious links, and terminates infection.

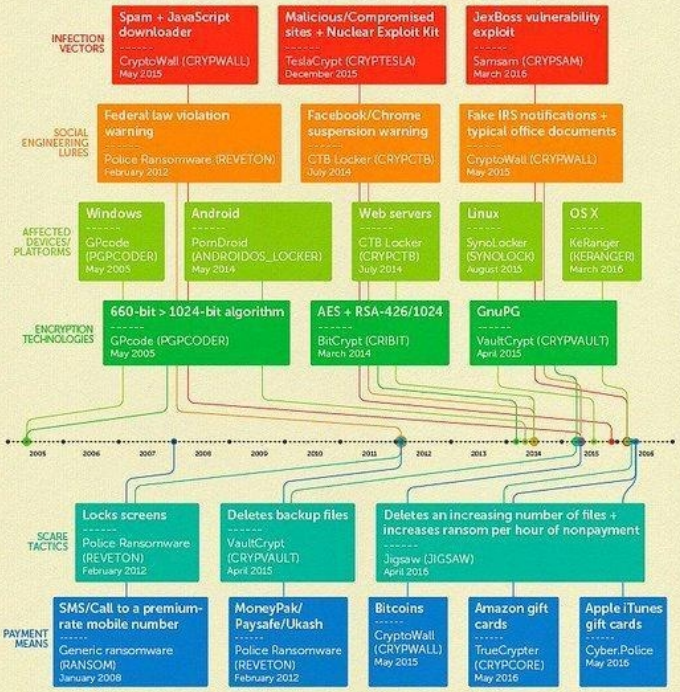
Best practices

- Avoid opening unverified emails or clicking links embedded in them.
- Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location.
- Regularly update software to protect against the latest vulnerabilities.

Ransomware: Bigger, bolder over time

Over the years, ransomware have evolved in terms of arrival, lure, encryption, and preferred payment method, making them one of the biggest security threats to date. Cybercriminals realized how profitable the ransomware business model is. That's why we're seeing an average of 10 new ransomware families per month.

(Note that the list of ransomware in the timeline below is not exhaustive. And the dates refer to when the ransomware first showed the characteristics in the timeline.)



FOR MORE INFORMATION ON RANSOMWARE:
http://cyberthreatalliance.org/pr/pr-102915.html
http://www.trendmicro.com/vinfo/us/security/definition/ransomware

FOR RANSOMWARE SOLUTIONS:
http://www.trendmicro.com/us/security-intelligence/enterprise-ransomware/index.html
http://www.trendmicro.com/us/security-intelligence/small-business-ransomware/index.html
http://www.trendmicro.com/us/home/consumer-ransomware/index.html

Created by **TrendLabs**,
The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO


Too Many
Threats
62%
INCREASE IN BREACHES IN 2013[1]
1 IN 5
ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK[4]
US $3 TRILLION
TOTAL GLOBAL IMPACT OF CYBERCRIME[3]
8 MONTHS
IS THE AVERAGE TIME AN ADVANCED THREAT GOES UNNOTICED ON VICTIM'S NETWORK[2]
2.5 BILLION
EXPOSED RECORDS AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]
Too Few
Professionals
62%
OF ORGANIZATIONS HAVE NOT INCREASED SECURITY TRAINING IN 2014[6]
1 OUT OF 3
SECURITY PROS ARE NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS[7]
<2.4%
GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES[8]
1 MILLION
UNFILLED SECURITY JOBS WORLDWIDE[9]
83%
OF ENTERPRISES CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

10 Steps To Cyber Security

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Malware Prevention

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Monitoring

Establish a monitoring strategy and develop supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Incident Management

Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the corporate system

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

TIPS & ADVICE

EUROPOL EC3 European Cybercrime Centre

To Prevent Identity Theft Happening To You

Identity theft is big business! Personal and financial data stolen online is sold in the underground economy, and is misused by criminal organisations all over the world. Protecting your data doesn't just save you the inconvenience of having to change your passwords and credit cards, by making it more difficult for criminals to obtain your details you can help in the fight against organized crime and terrorism.

DOS

BE AWARE. Treat unsolicited emails or pages asking for personal information with suspicion, particularly those claiming to be from banks and credit card companies. A quick web search can tell you if the email you've received is a known scam. Remember that you can always check with your bank or credit card company if the email you received is really from them.

UPDATE YOUR SOFTWARE REGULARLY. Many malware infections are the result of criminals exploiting bugs in software (web browsers, operating systems, common tools, etc.). Keeping these up to date can help to keep you safe.

USE ANTI-VIRUS SOFTWARE. Anti-virus (AV) software can help keep your computer free of the most common malware. You can easily find many free options of such software. Always check downloaded files with AV software. Do not install programs or applications on your computer if you don't know where they have come from.

DON'TS

CLICK ON ATTACHMENTS AND LINKS WITHOUT KNOWING THEIR TRUE ORIGIN. What looks like a harmless video or image can actually be malicious software designed to steal your data. Even opening a spam email can put your address on a spammer's future hit list.

GIVE AWAY MORE INFORMATION THAN NECESSARY. Your bank and credit card provider already know your PIN number and address. They don't need you to tell them via email, phone or a web page.

ACCESS ONLINE BANKING FROM SHARED OR PUBLIC COMPUTERS. You never know what might be lurking on their hard drives.