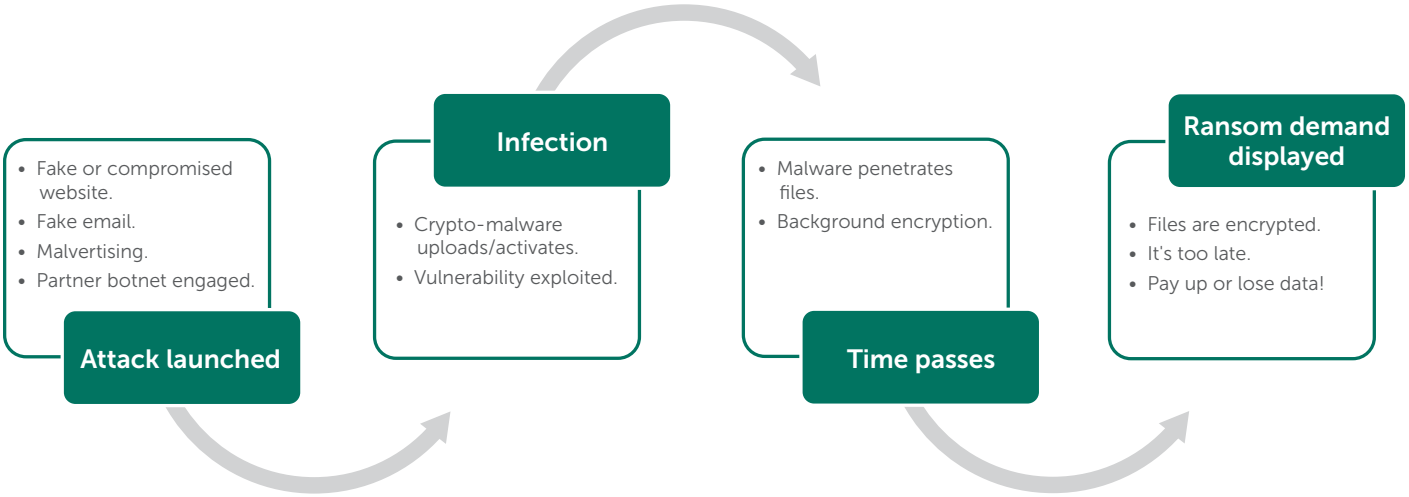
RANSOMWARE IS REACHING EPIDEMIC PROPORTIONS

- Over the first six months of 2015 alone, the number of ransomware attacks overtook the total for the whole of 2014.
- More than 40 percent of all CryptoLocker victims agreed to pay up last year.[1]
- Ransomware rakes in $30 million every 100 days.[2]
- Ransomware has shifted its attention to the enterprise, targeting more than 230 file types (up 200 percent from 70 file types in 2013).[3]

How ransomware attacks



To avoid becoming a victim:

EDUCATE YOUR STAFF

Make sure every user receives IT security awareness training, such as Online or CyberSafety Games Training from Kaspersky Security Intelligence Services.

PROTECT FROM INFECTION

Deploy the world's best-of-breed security solution – Kaspersky Endpoint Security for Business:

- Get the latest version and keep up to date.
- Enable critical (better still – all) solution modules.
- Tune up security module settings (e.g., enable heuristics).
- Enable Kaspersky Security Network.
- Patch software vulnerabilities in your infrastructure regularly with automated patch management from Kaspersky Endpoint Security for Business – Advanced.

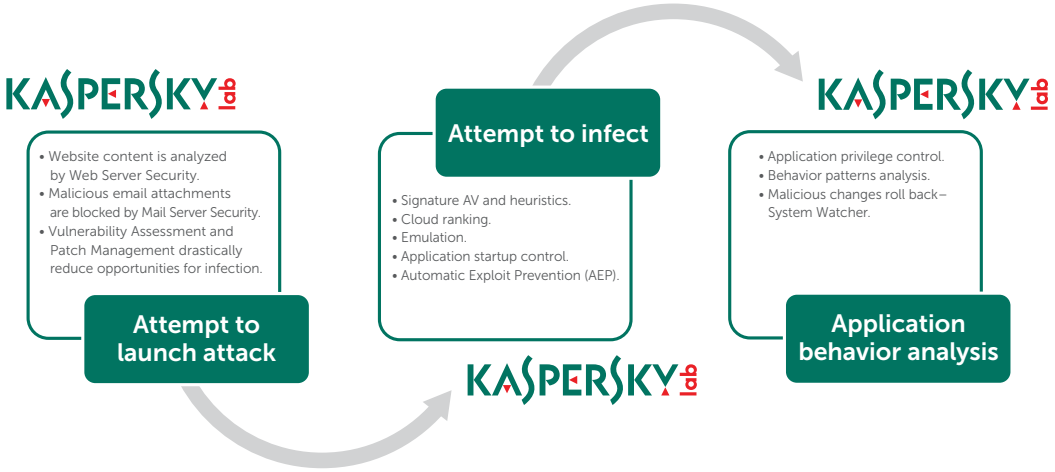
[1] 2014 survey by the Interdisciplinary Research Centre in Cybersecurity, University of Kent.
[2] Dell SecureWorks report.
[3] Vadim Kotov and Manteg Singh Rajpal, "Understanding Crypto-Ransomware," Bromium, http://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf.

Put ransomware out of business

Here's how. Whenever any file categorized by the business as "important" is about to be accessed, Kaspersky System Watcher immediately creates a local, protected backup copy. If Kaspersky System Watcher spots a subsequent action it considers malicious, such as an attempt to encrypt the file, it will automatically roll back any unsolicited changes. All you'd see is an update process.

There is no point asking for a ransom to decrypt files when any damage done by the hostage takers has been rolled back and the files are not encrypted. So you win, and they lose. And if everyone takes the same precautions, ransomware will soon become unprofitable and simply die away.

How ransomware is stopped



Get yourself back in business, fast

If you've worked in IT for a while, you'll know that sooner or later a disaster such as a successful ransomware attack will take place – it's just case of when, not if. You can't control the when, but you can ensure your ability to recover. When the time comes, the solution you have installed must be ready to step up to the plate for you.

Your ability to mitigate the risk, sustain as little damage as possible and get back to business as fast as you can will make all the difference. Organizations need to keep their doors open and ready for business at all times, regardless of any incidents or disasters. This is why choosing the right disaster recovery solution is critical to the survival of your business.

For more information about defending your organization against ransomware, please contact your Kaspersky Lab reseller or visit www.kaspersky.com.

KASPERSKY lab

Kaspersky Lab delivers the most powerful anti-malware on the market by combining world-leading threat intelligence with a unique comprehensive security platform. Only Kaspersky Lab can offer the research, technology and support your company needs. Our solutions are designed with the flexibility to align with your business objectives. This means we are always on standby to protect your organization against threats to your physical and virtual nodes, mobile devices, mail systems, servers and gateways.

AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com
To learn more visit us at: usa.kaspersky.com

KASPERSKY lab THE POWER OF PROTECTION