comtact
PERFORMANCE THROUGH TECHNOLOGY

www.comtact.co.uk

HOW RANSOMWARE WORKS

Ransomware is Gaining Momentum!

Over the past three years, ransomware has jumped into the spotlight of the cyber threat landscape.

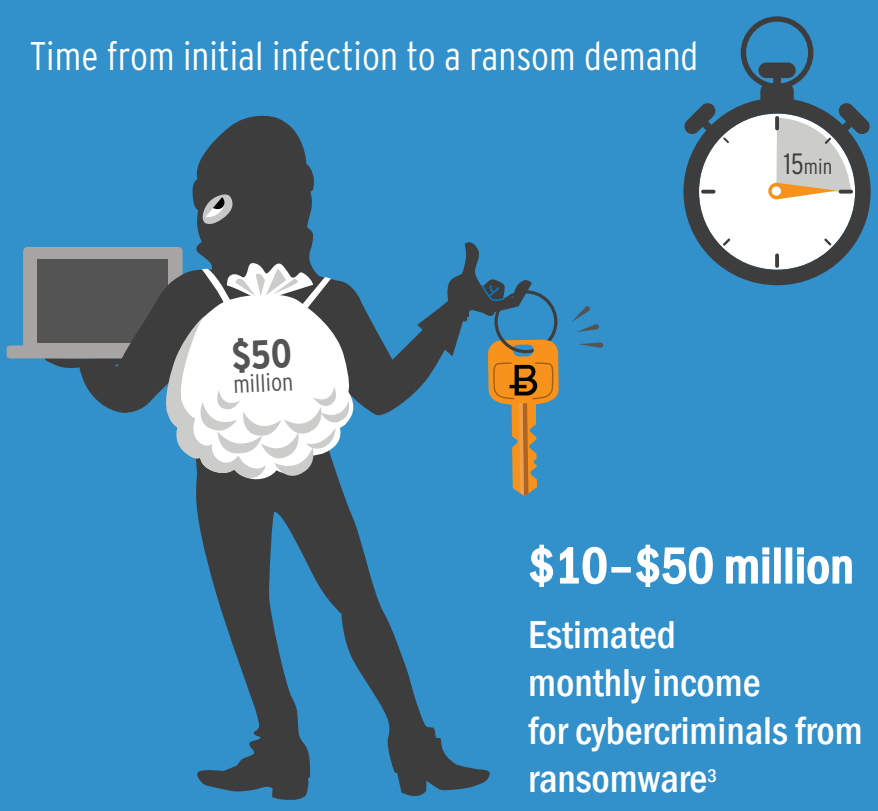
Just What is Ransomware?

Ransomware is a malicious software that allows a hacker to restrict access to an individual's or company's vital information and then demands some form of payment (usually Bitcoins) to lift the restriction.

209 million Amount paid in Q1 2016 to cyber-criminals using ransomware[1] FBI

1 billion estimate for losses to be incurred in 2016 due to ransomware[1]

Time from initial infection to a ransom demand



$10–$50 million

Estimated monthly income for cybercriminals from ransomware[3]

72%

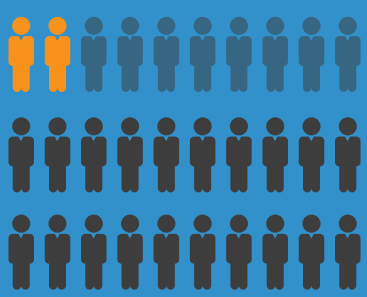
Percent of companies affected by ransomware that could not access data for at least 2 days following the attack[4]

32%

Percent that lost access to their data for 5 days or more[4]

86%

Attacks that affected **2** or more employees[4]



47%

Attacks that affected more than **20** employees[4]

$17,000

Amount paid by the Hollywood Medical Center in 2016 to unlock files and return to business as usual[5]

$100,000

Amount the hospital was losing **PER DAY** just on its inability to perform patient CT scans[5]

[1]CNN-Money, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/, April 15, 2016
[2]Security Magazine, "'Ransomware' Attacks to Grow in 2016," November 23, 2016
[3]David Common, CBC News, "Ransomware: What You Need to Know," March 11, 2015
[4]Intermedia blog post, "When ransomware strikes your business, are you prepared? Our new report findings may surprise you.", March 17, 2016
[5]PYMNTS.com, " City Held Hostage – Via Bitcoin Ransomware," March 22, 2016

THE 5 PHASES
of a Ransomware Attack

There are 5 distinct phases of a ransomware attack. Understanding what happens at each phase and recognising the indicators of compromises (IOCs) can increase your likelihood of successfully defending against—or at least mitigating the effect of—an attack.

The timeline of an attack is very compressed. You often have as little as 15 minutes from the exploitation and infection to receiving the ransom note. Recognising the early indicators is critical to your success in stopping an attack.

1

Phase 1: Exploitation and Infection (T –00:00)

In order for an attack to be successful, the malicious ransomware file needs to execute on a computer. This is often done through a phishing email or an exploit kit. In the case of the CryptoLocker malware, the Angler Exploit Kit is a preferred method to gain execution.

2

Phase 2: Delivery and Execution (T –00:05)

During this phase, the actual ransomware executables are delivered to the victim's system. Upon execution, persistence mechanisms will be put into place.

3

Phase 3: Backup Spoliation (T –00:10)

A few seconds later, the ransomware targets the backup files and folders on the victim's system and removes them to prevent restoring from backup. This is unique to ransomware—other types of crimeware don't bother to delete backup files.

4

Phase 4: File Encryption (T –02:00)

Once the backups are completely removed, the malware will perform a secure key exchange with the command and control (C2) server, establishing those encryption keys that will be used on the local system.

5

Phase 5: User Notification and Cleanup (T –15:00)

With the backup files removed and the encryption dirty work done, the demand instructions for extortion and payment are presented. Quite often, the victim is given a few days to pay. After that time, the ransom increases.

Finally, like the Mission Impossible recordings that self destruct, the malware cleans itself off the system so as not to leave behind significant forensic evidence that would help to build better defenses against the malware.

Ransomware attacks are just starting to ramp up. Because these attacks are so lucrative for the perpetrators, they are certain to become more common, more damaging and more expensive.

Your organisation's success in defending against a ransomware attack is largely dependent on your level of preparation and the tools you deploy to monitor your systems to detect, respond to and neutralise suspicious activity.

Securing the UK's leading organisations 24x7x365 from our UK SOC

comtact
PERFORMANCE THROUGH TECHNOLOGY

Comtact Ltd. (Head Office) Clive House
12 - 18 Queen's Road Weybridge, Surrey KT13 9XB

Tel: 08452 75 75 75 Email:
enquiries@comtact.co.uk

FOLLOW US Comtact-Ltd

@comtact_ltd

www.comtact.co.uk