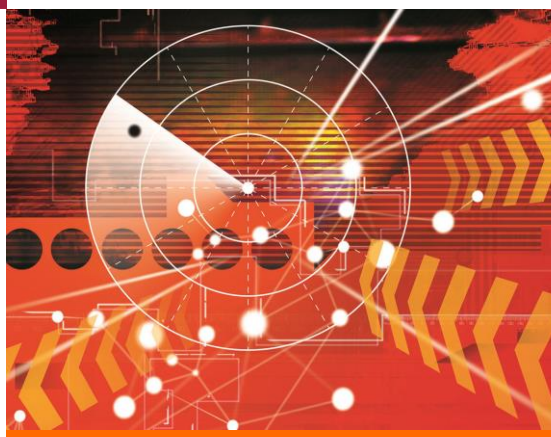
Ransomware
WannaCry

CGI
Experience the commitment®

Current
Security Information



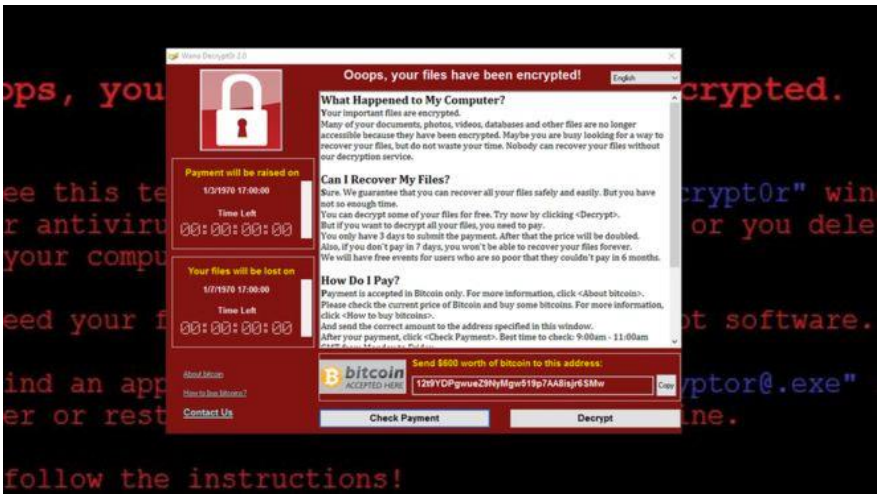
The Ransomware WannaCry / Wcry / WannaCrypt escalated fast starting on May 12th 2017. Computer systems in more than 150 countries were impacted, their storage encrypted and business processes stopped.

THE THREAT

The WannaCry malware, a type of Crypto trojan, spreads itself over the network after an initial infection by email. The malicious code is then executed from this email distributed macro. Essentially the malware contains two parts;

- Propagation – Spread via use of exploit (see MS17-010).
- Payload – Encryption of data and screen lock on infected computers.

The following image shows on infected computers:



THE CAUSE

The Ransomware WannaCry uses one of the NSA-attributed exploits called EternalBlue. The exploit was leaked online in April 2017 by the hacker group Shadowbrokers. The vulnerability – found in the outdated SB v1 Protocol is described in the Microsoft Security Bulletin - MS17-010. This vulnerability is exploited to allow WannaCry malware to spread as a worm across the network from the initial infection.

THE CONSEQUENCES

WannaCry encrypts the data of the infected systems and requests a payment of ransom in the form of bitcoins. In this case, the price doubles after three days and after seven days the data is deleted. In the event of a punctual payment, the users should receive a code to decrypt their data.

FACT SHEET

WANNACRY & DEFENSE

Overview of Cybersecurity Solutions:

Strategy, Compliance & Transformation

- Information Security and Emergency Management
- Best Practices according to ISO 27001, ISO 25999, IT-Grundschutz and A-960/1
- Vulnerability Assessments and Penetration Testing
- Risk Management Strategies
- Implementing Security Processes
- Date Protection and Data Security
- Awareness Training

Secure Systems Engineering

- Secure Network Architectures
- Identity & Access Management
- Secure Software Development
- Security Testing

Managed Security Services

- Managed Services
- Monitoring & Alerting
- SIEM as a Service
- Forensics & Malware Analysis
- Advanced Threat Intelligence

de.cgi.com/cybersecurity

Among those effected:

- Hospitals, which were forced to shut down to all non-emergency patients.
- Car manufacturers including Peugeot, whose production lines were halted a day long.
- Transport service providers such as Deutsche Bahn with the failure of their live timetable displays.

THE REASONS

Put simply users of the infected computer have two key deficits:

1. **Lack of Awareness**
   Users click too fast on links or attachments of unsolicited e-mails.
2. **Missing Updates** and **Outdated Systems**
   Microsoft has released patches against the vulnerability on March 14, 2017. However, these patches for non-supported Windows systems had not been released until May 12.

AD HOC COUNTERMEASURES

If patching of Windows systems is not possible in a timely manner, there are the following options to reduce the risk of infection:

- Current Malware Protection: Windows Defender has the corresponding signatures for Ransom:Win32/WannaCrypt available from May 12th.
- Intrusion Prevention System: IPS Snort has released the corresponding rules on May 12thand IPS Suricata on May 13th.
- Kill-Switch: First versions of WannaCrypt have a mechanism that sets a kill function when "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" can be reached. This domain has been registered on May 12th activating the kill switch.
- Network Segmentation: By closing the ports required for SMB shares at the network boundaries (these should not be allowed for any shares) the spread can be restricted.

PREVENTIVE PROTECTION

- Carry out Awareness Campaigns and Vulnerability Assessments.
- Optimize Patch-Management and Malware-Protection in terms of Risk Management.
- Design and implement of a backup infrastructure that is safe from Crypto-Trojans.
- Secure network segmentation with isolation and migration of legacy systems.
- SIEM Services from our Security Operation Centers (SOC) for the instant detection and analysis of attacks.
- Preparation of countermeasures, e.g. Intrusion Prevention Systems (IPS) can be equipped with additional ad-hoc rules in addition to manufacturer rules after analysis of the SOC

CGI will gladly advise you on this and offer you our upcoming German based and German speaking SOC service, because

“Cybersecurity is part of everything we do.”

ABOUT CGI

CGI is a global service provider for IT and business processes. We were founded in 1976 and have a total of 70,000 employees at 400 locations in 40 countries. We are on-site for our customers - with business and IT consulting, system integration and outsourcing services at a top level. We support them in making better use of ongoing investments, while at the same time leveraging new digital technologies and business strategies that enable clients to achieve the best solutions across the entire value chain. Regarding time and budget, we are regularly awarded due to our strict delivery discipline.

To this end, we have consistently achieved more than nine out of ten potential points in customer satisfaction.

YOUR CONTACT PERSON

CGI Deutschland Ltd. & Co. KG

Practice Cybersecurity

(Practice Head: **Frank Reiländer**)

Ettore-Bugatti-Straße 6-14
51149 Köln
T: +49 2203 6993 1050

For more information please contact us at csi@cgi.com
or visit us
de.cgi.com/cybersecurity.