Quantum malware

In the modern business world mergers and acquisitions (***M&A***) are a near constant activity between small and global businesses. Quantum International (***Qint***), a small but promising company specializing in big data transfers using quantum technology, has attracted Sir Randolph ‘s attention. Sir Randolph is the President of Prometheus World-Wide (***PWW***), a diversified technology company originally started in the UK medical hardware industry. Just a small startup 18 years ago, PWW has now grown into a large corporation doing business in over 200 countries worldwide.

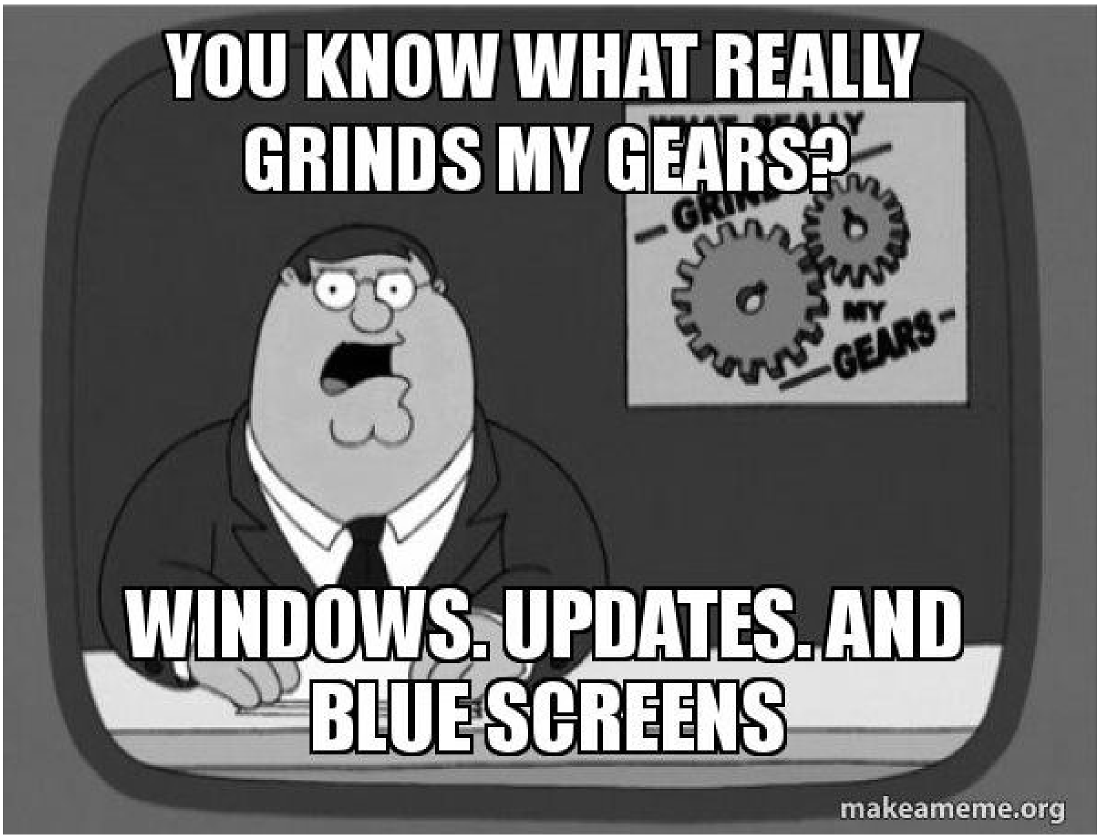
Almost convinced that the acquisition of QInt fulfils a vital business requirement for PWW’s future vision, Sir Randolph has tasked Mr Robert, his trusted friend and Business Officer to also look into this matter and find more links between cutting edge medical instruments and quantum technology.

‘Count on me!’, Robert says, rigorously taking notes in his brown leather journal. Although eager to start his research right away, Robert doesn’t know anything about medical instruments. Back to his office, he dusts out his old Windows laptop and starts searching. Vision microscopes, strange quantum mixers, USB spectrometers, tamper evident jars, all seems to make sense now in his head, when suddenly an unexpected blue screen interrupts his work. Luckily for him, you are his trusted Malware Analyst and Incident Responder.

* * *

Robert rushes in, his laptop in one hand and his journal in the other. His words are somehow familiar - *‘I need help with my computer!’*. After calming him down, you promise to help fix his laptop, find the culprit and get him on track with the research.

‘Very intriguing’ you say to yourself, opening another Club-Mate bottle and looking at the extracted **packed capture**. The packet sniffer you installed last week has done its job! You have something to work with. Quickly take a **memory image** before the battery runs out, and you’re good to go.


YOU KNOW WHAT REALLY GRINDS MY GEARS?
WHAT REALLY GRINDS MY GEARS
WINDOWS, UPDATES, AND BLUE SCREENS
makeameme.org

Answer the points below to guide your investigation. The points marked in blue are optional, but can give you extra brownie points from Mr. Robert. Some hints are provided below and more help is available in the forum and discussion list from your fellows detectives trying to help Mr Robert.

Part A – Traffic analysis

1 Which of the following web sites has been visited prior to the incident?

Hint: Setting up[1] your network analyser[2] first will make the analysis considerably easier.

□ www.google.com

□ www.research-instruments.com

□ www.yahoo.com

[1] http://malware-traffic-analysis.net/tutorials/wireshark/index.html

[2] https://www.wireshark.org/

□ www.research-medical.com

2 What search engine was Mr. Robert using and what search terms were queried?

□ Bing - “merger and acquisition”

□ Yahoo! - “mergers”

□ Google - “medical instruments”

□ DuckDuckGo - “investopedia”

3 How did the machine get infected?

□ Hidden iframe on www.woodleyequipment[.]com

□ Click a malicious link on www.woodleyequipment[.]com

□ Hidden iframe on www.research-instruments[.]com

□ Download a malicious file from www.research-instruments[.]com

4 What client side technology was exploited?

□ Flash

□ Java

□ Silverlight

□ PDF

4.1 Find out what vulnerability was exploited.

□ CVE-2012-1330

□ CVE-2012-1723

□ CVE-2016-3610

□ CVE-2012-0158

Hint: You might have to extract the client side object run by the browser and analyse it with an online analysis service.

4.2 What other client-side exploits was the malicious website attempting to deliver?

□ An RTF exploit

□ A Word exploit

□ An Internet Explorer exploit

□ A PDF exploit

Hint: Trace back from the request for the malicious payload to the website serving it. You might have to deobfuscate[3] some[4] JavaScript[5] along the way.

[3] http://jsbeautifier.org/

[4] http://www.kahusecurity.com/2014/javascript-deobfuscation-tools-redux/

[5] http://reverseengineering.stackexchange.com/questions/4561/how-to-deobfuscate-an-obfuscated-javascript-file-

Part B – Malware analysis

5 What malicious software was dropped following the visit to the suspicious website?

□ A ransomware

□ A banking trojan

□ A click-fraud trojan

□ A remote access trojan

5.1 How this malware will affect Mr. Robert specifically, given his privileged access to company's online banking account.

□ It might encrypt all his sensitive financial data

□ It might send fraudulent spam messages from his account

□ It might steal all the company monies accessible from his account

□ It will not affect him at all

Hint: If setting up a sandbox automated malware analysis environment like Cuckoo[6] is too much of a hassle, Malwr[7] provides a convenient and free web-accessible front-end. Use it along with other online analysis services[8] to check the sample's behaviour.

5.2 How will the infection persist on the machine after a restart?

□ It will not persist after restart

□ The sample will overwrite a system library

□ The sample will install itself for autorun in the Windows Registry

□ The sample will hijack a COM object

5.3 What external domain is contacted by the sample for downloading its configuration file?

□ moonmaderats[.]pw

□ bing.com

□ secure-bankofamerica[.]com

□ investopedia.com

like-this

[6] https://www.cuckoosandbox.org/

[7] https://malwr.com

[8] https://virustotal.com