Black Swan or Just an Ugly Duckling?

Can potentially crippling cyber situations be foreseen and mitigated?

Anne Coull
Objective Insight
Sydney, Australia
Email: anne.objectiveinsight@gmail.com

Abstract— Black Swan situations and their consequences are considered extremely unlikely before they happen and make perfect sense afterwards. Two malicious exploits that triggered Black Swan situations, Emotet and WannaCry, are assessed, along with their attack sequences comprising of multiple attack vectors operating in sequence and targeted at known vulnerabilities. The early warning signs and the practical actions to prevent these types of Cyber Black Swan situations are outlined. Prevention is based on practical defence in depth controls, along with effective ongoing maintenance, with situational awareness guiding the cyber teams as to where to focus their response efforts.

Keywords- Black Swan; Emotet; WannaCry; Early Warning Indicator; Critical Vulnerability; Situational Awareness; Response.

I. INTRODUCTION

As an Australian, the notion of a Black Swan as an unexpected event is counter intuitive. While the swans in Europe may be white, in Australia the native swans are black. In a country of jumping kangaroos and duck-billed platypus, the unexpected is modus operandi. In his book: "Antifragility, things that gain from disorder," Nassim Taleb [41] uses the term *Black Swan* to describe unexpected situations with 3 attributes: Before the situation occurs, it is considered extremely unlikely, if not impossible; When it occurs its consequences are significant, either in changing belief, or in consequence; After it has occurred, it makes perfect sense as something that could happen [14][41].

With Australian insight it becomes clear that unusual creatures and events do not just suddenly appear, they evolve over time. Similarly, Black Swan situations develop over time and show early warning indicators. Noticing these early signs, and acting upon them, will make the difference between a dramatic event, a well-managed situation, or just another day doing business. The proposed mitigation on these Black Swans is based on situational awareness, basic, practical, and well-maintained cyber controls, and response to emergency situations.

Two black swan cyber situations, the Emotet Trojan, and the WannaCry Worm, are reviewed along with their attack vectors and the vulnerabilities they target. These two cyber attacks that triggered Black Swan situations were selected due to their scale and impact, which in turn can be attributed primarily to the preparation and response of the target organisations. These attacks differed in their initial access approach, their style of attack, and the combinations of attack vectors they utilised [4][36]. For each of these black swan cyber situations, the potential for predictability and reduced impact through stringent maintenance and monitoring, situational awareness, and response to early warning indicators is assessed.

Section 2 outlines the Emotet and WannaCry exploits and their respective impacts. Section 3 analyses their attack sequences for access, escalation, persistence, scanning, spread, exfiltration, and assault [43]. Section 4 looks at how these events could have been foreseen by reading the early warning indicators. Section 5 outlines how these attacks and others like them can be mitigated using practical cyber defence in depth with effective ongoing maintenance, situational awareness, and timely response.

II. EMOTET AND WANNACRY EXPLOITS AND THEIR IMPACTS

Over the last decade two of the most successful cyber attacks, in terms of scale and impact, have been Emotet and WannaCry. Both utilised a combination of exploits to target Microsoft vulnerabilities and gain access to organisations, establish persistence, escalate privileges, and exfiltrate data whilst concurrently spreading, infecting, and implementing assault strategies across the network [4][5][16][20][27] [33][34][37]-[40].

Emotet started as a banking Trojan and has continued to evolve since it was first identified in 2014. In 2019, Emotet was responsible for approximately 60% of malware email spam [36]. By 2020 it had morphed into Botnet as a Service with global distribution. Infected devices themselves become C2 bots. In May 2019, 310 unique infected IP addresses were identified, of which two thirds (208) were confirmed bots, and 8% (17) of these were also infected with Trickbot [36] (see Figure 1).

In January 2021, the German Bundeskriminalamt (BKA) federal police agency coordinated a combined effort of law enforcement agencies to shut down the global botnet of hundreds of Emotet servers [34]. The Trojan malware, or a copycat, returned in November 2021 and infected an estimated 1.2 million systems in 2022 [34].

 ISBN: 978-1-61208-996-6

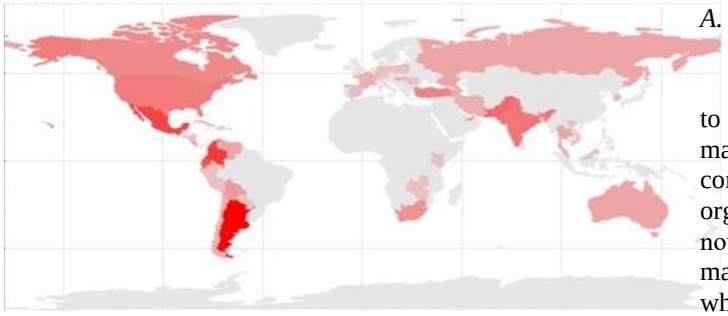

Figure 1. Geographic distribution of Emotet Botnet IP addresses, June 2019 [36].

In May 2017, after infecting more than 300,000 computers and crippling 150+ organisations worldwide. WannaCry was dubbed "the largest ransomware event in history." The WannaCry ransomware attack was stopped by a MalwareTech cyber researcher [19] who identified a key design flaw and purchased the URL WannaCry referenced in its attack sequence (see Figure 2).

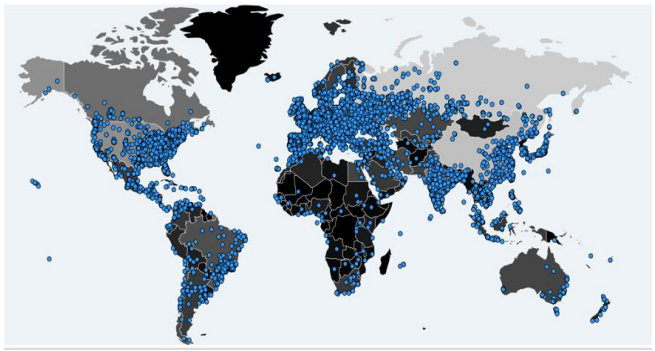

Figure 2. Distribution of WannaCry infections 14 May 2017, after 24 hours [5][19].

The situations triggered by WannaCry and Emotet could both be regarded as Black Swans. Each was considered extremely unlikely before they were experienced and identified. Each gained the attention of Europol and Eurojust due to their scale and the significant and costly consequences for those affected [34]. WannaCry brought the British NHS to a standstill [12], including the closure of public hospitals. Emotet was estimated as costing in excess of $1 million for every organisation it infected [4][34].

III. ATTACK SEQUENCE ANALYSIS

While there are some commonalities in the zero-day exploits targeting Microsoft SMB remote control vulnerabilities, Emotet and WannaCry utilise different attack vectors in the infection process.

A. Emotet access, escalation, persistence, scanning, spread, exfiltration, and assault

Emotet utilises social engineering phishing campaigns to entice recipients to click on a link that downloads a macro-infected Microsoft office file. These emails appear to come from a friend or colleague, or from a known organisation and include PayPal receipts, shipping notifications, or "past-due" invoices [4] (see Figure 3). The macro executes the payload malware for the next stage where it establishes persistence using auto-start registry keys and services to embed a scheduled task at startup [4][33][34].

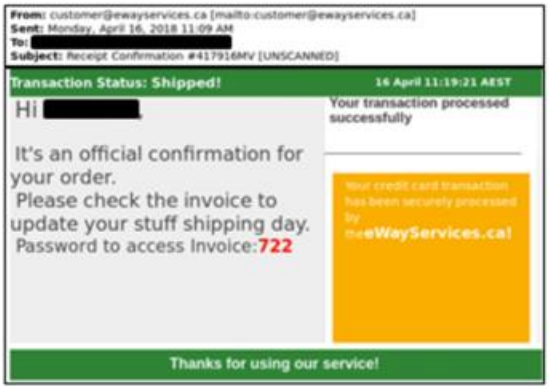

Figure 3. Emotet malicious email Emotet [4].

Emotet spreads by extracting contact lists from infected users' email accounts and using these to send phishing emails, so they will appear to come from a friend or colleague. Concurrently, Emotet spreads to systems across the network by enlisting a credential enumerator with service and bypass components. It utilises publicly available tools to recover passwords stored on: (i) the user's system and external drives; (ii) web-browsers such as Google Chrome, Internet Explorer, Mozilla etc.; and (iii) email providers such as Gmail, Outlook, Hotmail etc.

It concurrently utilises a malicious-actor-developed spreader module that applies brute force with enriched password lists to move through the Windows Admin Shares. It uses these credentials to access accounts and copy itself to the ADMIN$ of other network hosts, before using Server Message Block (SMB) to schedule execution on these hosts. It locates writable share drives and infects the entire disk by writing the Emotet service component onto the network [4][33][34] (see Figure 4).

 ISBN: 978-1-61208-996-6

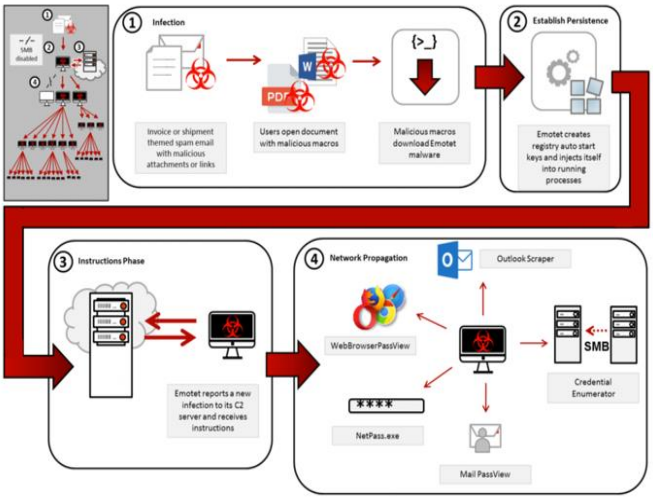

Figure 4. Emotet infection process [4].

From 2016 Emotet incorporated a Trickbot banking trojan which evolved to exploit the Microsoft Windows SMBv1 and NBT Remote Code Execution Vulnerabilities (CVE-2017-0144, CVE-2017-0147), and the Windows SMB Remote Code Execution Vulnerabilities (CVE-2019-0630, CVE-2019- 0633) [4][33]. The Trickbot is used to launch the malware payload, bypass Microsoft security measures, communicate with the command-and-control infrastructure, upload data and download DLL updates [33].

B. WannaCry access, escalation, persistence, scanning, spread, exfiltration, and assault

WannaCry identified its targets using EternalBlue to scan externally facing hosts across the internet where TCP ports 139 and 445 were open [42]. These ports are used to communicate using the SMB network protocol that enables remote code execution in MS Windows & sharing across networks [5][16][40].

When it identified the Microsoft SMB Windows Server Remote Code Execution Vulnerability (CVE-2017-0144) and the Microsoft SMB Windows Server Remote Code Execution Vulnerability (CVE-2017-0145) [39] which enabled remote code execution over SMB v1, EternalBlue then accessed the vulnerable target systems and installed the DoublePulsar exploit for persistence [5][20][27]. It continued to scan, access and replicate while it encrypted files and destroyed backups on every computer it infected: disrupting businesses by denying users access to their critical data [13][37]-[39]. It then displayed a ransomware image to the users of infected devices (see Figure 5).

Figure 5. WannaCry image displayed on infected user's desktop [5][18].

IV. PROACTIVELY LOOKING FOR THE EARLY WARNING INDICATORS

Situational awareness is key to preventing malicious exploits developing into Black Swan situations. It enables organisations to notice the early warning signs and prepare for and respond to emerging situations. The early warning signs are there for Emotet and WannaCry, but they will only be noticed by those who actively seek them out. The early warning signs include:

1. The current state of the organisation:
    a. The cyber-risk awareness of personnel, based on their click-rate on targeted phishing campaigns.
    b. The level of compliance with standards and guidelines for basic defence maintenance practices, including compliance to the Australian Signal Directorate's Essential Eight cyber mitigations, in particular: the extent of unpatched Microsoft windows systems; privileged access management; ability to download macro-enabled email attachments; and availability of separately stored backup data [6].
2. Critical vulnerability reports:
    a. Microsoft CVE-2017-0144, CVE-2017-0145, & CVE-2017-0147 vulnerability reports published in the Microsoft Vulnerability Update Guide on 14 March 2017 [22]-[24] and corresponding CVE reports [7]-[9] and NIST reports published on 16 March 2017 [28]-[30].
    b. Microsoft CVE-2019-0630 & CVE-2019-0633 vulnerability reports published in the Microsoft Vulnerability Update Guide on 12 February 2019 [25][26] and corresponding CVE reports [10][11] and NIST reports published on 3 May 2019 [31][32].

3. Threat alerts and reports:
    a. Threat alerts and reports are readily available through research centres such as MalwareTech [19], Metasploit [15], and Talos [17].
    b. Cyber teams in peer organisations sharing information. Organisations, such as the Australian Banks, openly share information in a joint effort to fight cyber crime.

V. PREVENTING THESE BLACK SWAN SITUATIONS

Emotet, WannaCry and similar trojan and worm-based malware exploits can be prevented, and/or their effects limited by applying basic cyber defence maintenance practices.

1. Address the weakest link. Educate all people in the organisation on the risks and indicators of cyber exploits, such as emails with links and attachments. Educate people to *not* click on links and to run their mouse over to see where it links to, even if the email comes from a trusted colleague or friend. Educate them to *not* click on online advertisements, and to never share unencrypted sensitive information through external email or on the phone [4][6].

2. Incorporate desired cyber practices into policies. For example, implement a policy requiring users to forward suspicious emails to the security team [4].

3. Control who accesses to what, when. Implement Privileged Access Management based on the principle of least privilege [6].

4. Maintain a technology defence barrier. Keep all operating system and application patching up-to-date, by applying tested patches and updates as a priority. In particular, apply critical patches within 48 hours. Five weeks prior to the main WannaCry attack, Microsoft had released updated CVE reports and emergency patches to the Windows SMB vulnerabilities that enabled WannaCry's EternalBlue and DoublePulsar exploits [6].

5. Set a Firewall rule to restrict inbound SMB communication between client systems, using Windows Group Policy Object, or if using a non-windows host-based intrusion prevention system [HIPS], implement custom modifications for the control of client-to-client SMB communication [4].

6. Using antivirus programs on clients and servers, with automatic updates of signatures and software will mitigate against many other malware exploits that are signature based [4][6].

7. Whitelist IP addresses and block suspicious and known malicious IP addresses at the firewall. Filter out emails with known malspam indicators, such as known malicious subject lines, by implementing filters at the email gateway [4][6].

8. Block or scan file attachments commonly associated with malware, such as .dll and .exe and those that include macros, as well as attachments that cannot be scanned by antivirus software, such as .zip files [4][6].

9. Disable macros and PowerShell to prevent macro driven PowerShell commands, such as those utilised by Emotet [4][6].

10. Implement Domain-Based Message Authentication, Reporting & Conformance (DMARC), a validation system that minimises spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures [4].

11. Be prepared for the worst. Take daily backups for timely recovery and restoration of service to the business and its customers. Ensure these are stored on a separate network and restoration is tested regularly to prevent failure when restoration is really needed [1][2][4][6].

12. Maintain current situational awareness. Stay abreast of alerts and threat reports.

13. Limit exposure of critical systems to zero-day exploits.Take vulnerable, critical systems off-line and/or restrict their external accessibility when a zero-day exploit is underway.

14. Apply emergency zero-day patches immediately. During the WannaCry event, Microsoft released emergency patches for out-of-support versions of MS Windows.

VI. CONCLUSION

The Black Swan situations generated by the Emotet and WannaCry malicious exploits demonstrate the potential for preventing these situations from developing.

Situational awareness enables organisations to notice the early warning signs, prepare for and respond to emerging vulnerabilities and threats. Preparation involves addressing the weakest link, privileged access management, maintaining a technical defence barrier and keeping reliable backups. Current situational awareness ensures the organisation can respond to zero-day exploits by limiting exposure of critical systems and immediately applying emergency patches to vulnerable systems.

 ISBN: 978-1-61208-996-6

The threat landscape is constantly changing and evolving, with new malicious actors entering the scene and malicious exploits being released into the wild that can easily be combined for increased effect. But the impact of these exploits is ultimately driven by the preparedness, situational awareness, and response of the target organisations.

REFERENCES

[1] ACSC, “Strategies to mitigate cyber security incidents, “Australian Government, Australian Signals Directorate, 2017, Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents, accessed October 2022.

[2] ACSC, “Essential eight explained, Australian Government,” Australian Signals Directorate, 2019, Available from: https://www.cyber.gov.au/sites/default/files/2020-01/PROTECT%20-%20Essential%20Eight%20Explained%20%28April%202019%29.pdf, accessed October 2020.

[3] Any run, “Emotet”, 2021, Available from: https://any.run/malware-trends/emotet, accessed October 2022.

[4] CISA 2018-2020, “Alert [TA18-201A] Emotet Malware,” Available from: https://www.cisa.gov/uscert/ncas/alerts/TA18-201A, accessed October 2022.

[5] A. Coull, “WannaCry Malware Case Study," Cyber Security Operations 2017, UNSW.

[6] A. Coull, “How much cyber security is enough,” The Fourth International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2019, September 22, 2019 to September 25, 2019 – Porto, Portugal, Available from: https://www.iaria.org/conferences2019/CYBER19.html/CYBER19.html, accessed October 2022.

[7] CVE, “CVE-2017-0144 - CVE.report,” Available from: https://cve.report/CVE-2017-144, accessed October 2022.

[8] CVE, “CVE-2017-0145 - CVE.report,” Available from: https://cve.report/CVE-2017-145, accessed October 2022.

[9] CVE, “CVE-2017-0147 - CVE.report,” Available from: https://cve.report/CVE-2017-147, accessed October 2022.

[10] CVE, “CVE-2019-0630 - CVE.report,” Available from: https://cve.report/CVE-2019-630, accessed October 2022.

[11] CVE, “CVE-2019-0633 - CVE.report,” Available from: https://cve.report/CVE-2019-0633, accessed October 2022.

[12] J. Graham, “How to Rapidly Identify Assets at Risk to WannaCry Ransomware and ETERNALBLUE Exploit,” Available from: https://blog.qualys.com/vulnerabilities-threat-research/2017/05/12/how-to-rapidly-identify-assets-at-risk-to-wannacry-ransomware-and-eternalblue-exploit, accessed October 2022.

[13] A. Hern and S. Gibbs, “What is 'WanaCrypt0r 2.0' ransomware and why is it attacking the NHS?,” the guardian, Saturday 13 May 2017, Available from: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20, accessed October 2022.

[14] H. Jankensgard, “The Black Swan problem: Risk management strategies for a world of wild uncertainty,” 2022, John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex, P019 8sQ, United Kingdom.

[15] D. Kennedy, J. O’Gorman, D. Kearns, & M. Aharoni, “Metasploit: the penetration tester’s guide,” 2011, No starch press, 245 8th Street, San Francisco, CA 94103.

[16] L. Kessem, “How did the wannacry ransomware begin?” IBM Security, 26 May 2017, Available from: https://www.quora.com/How-did-the-Wannacry-ransomware-begin, accessed October 2022.

[17] P. Rascagneres and C. Williams, “Player 3 Has Entered the Game: Say Hello to 'WannaCry'," Talos Intelligence, 12 May 2017, Available from: http://blog.talosintelligence.com/2017/05/wannacry.html, accessed October 2022.

[18] LogRhythm, “A technical analysis of wannacry ransomware, LogRhythm Labs, ” 16 May 2017, Available from: https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/, accessed October 2022.

[19] MalwareTech, “Botnet tracker,” MalwareTech, 2017, Available from: https://intel.j.com/botnet/wcrypt/?t=1h&bid=all, accessed October 2022.

[20] A. McNeil, “How did the WannaCry ransomworm spread?” Malwarebytes, 19 May 207, Available from: https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/, accessed October 2022.

[21] Metasploit, “Metasploit | Penetration Testing Software, Pen Testing Security,” Available from: https://www.metasploit.com/, accessed October 2022.

[22] Microsoft, “Windows SMB Remote Code Execution Vulnerability CVE-2017-0144,” 2017, Available from: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144, accessed October 2022.

[23] Microsoft, “Windows SMB Remote Code Execution Vulnerability CVE-2017-0145,” Available from: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0145, accessed October 2022.

[24] Microsoft, “Windows SMB Information Disclosure Vulnerability CVE-2017-0147,” Available from: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0147, accessed October 2022.

[25] Microsoft, “Windows SMB Remote Code Execution Vulnerability CVE-2019-0630,” Available from: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0630, accessed October 2022.

[26] Microsoft, “Windows SMB Remote Code Execution Vulnerability CVE-2019-0633,” Available from: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0633, accessed October 2022.

[27] P. Muncaster, “Wannacry didn’t start with phishing attacks,” says Malwarebytes, Infosecurity, 22 May 2017, Available from: https://www.infosecurity-magazine.com/news/wannacry-didnt-start-with-phishing, accessed October 2022.

[28] NIST, “CVE-2017-0144 Detail,” Available from: https://nvd.nist.gov/vuln/detail/CVE-2017-0144, accessed October 2022.

[29] NIST, “CVE-2017-0145 Detail,” Available from: https://nvd.nist.gov/vuln/detail/CVE-2017-0145, accessed October 2022.

[30] NIST, “CVE-2017-0147 Detail,” Available from: https://nvd.nist.gov/vuln/detail/CVE-2017-0147, accessed October 2022.

[31] NIST, “CVE-2019-0630 Detail,” Available from: https://nvd.nist.gov/vuln/detail/CVE-2019-0630, accessed October 2022.

 ISBN: 978-1-61208-996-6

[32] NIST, "CVE-2019-0633 Detail," Available from: https://nvd.nist.gov/vuln/detail/CVE-2019-0633, accessed October 2022.
[33] A. Perin, "Emotet Re-emerges with Help from TrickBot," Available from: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/06/emotet-re-emerges-with-help-from-trickbot, accessed October 2022.
[34] A. Petcu, "Emotet Malware Over the Years: The History of an Infamous Cyber-Threat," Available from: https://heimdalsecurity.com/blog/emotet-malware-history/, accessed October 2022.
[35] Qualys, "IT Security and Compliance Platform, " Available from: https://www.qualys.com/, accessed October 2020.
[36] Proofpoint, "Q4 2020 Threat Report," Available from: https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes, accessed November 2022.
[37] A. Rousseau, "WCry/WanaCry ransomware technical analysis," End Game, 14 May 2017, Available from: https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis accessed September 2022.
[38] Symantec, "WannaCry: Ransomware attacks show strong links to Lazarus Group," Symantec Security Response, 22 May 2017, Available from: https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group, accessed October 2022.
[39] Symantec, "Ransom.Wannacry", Symantec, 24 May 2017, Available from: https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99, accessed September 2017.
[40] Symantec, "WannaCry variant protection details and information", Symantec Support, 26 May 2017, Available from: https://support.symantec.com/en_US/article.INFO4361.html, accessed October 2022.
[41] N.N. Taleb, "Antifragile, things that gain from disorder", Random House, Penguin Random House LLC, New York, 2021.
[42] I. Thomson, "Wannacry: everything you still need to know because there were so many unanswered Qs", The Register, 20 May 2017, Available from: https://www.theregister.co.uk/2017/05/20/wannacry_windows_xp/ accessed October 2022.
[43] S. Winterfeld & J. Andress, "The basics of cyber warfare: understanding the fundamentals of cyber warfare in theory and practice", 2013, Elsevier, Inc, United States of America.

 ISBN: 978-1-61208-996-6