Managing Cyber Black Swans

Can potentially crippling cyber situations be foreseen, allayed, and turned into growth opportunities?

Anne Coull
Objective Insight
Sydney, Australia
anne.coull@proton.me

Elena Sitnikova
Flinders University
Adelaide, Australia
elena.sitnikova@flinders.edu.au

***Abstract*— Black Swan situations and their consequences are considered extremely unlikely before they happen and make perfect sense afterwards. Two malicious cyber attacks that triggered Black Swan situations, Emotet and WannaCry, are assessed, along with their attack sequences, and the vulnerabilities they exploited. The early warning signs and practical actions to prevent these types of Cyber Black Swan situations are presented. Prevention is based on protection through practical defence in depth controls along with effective ongoing maintenance. Added to this is the crucial element of situational awareness and a call to action for the cyber teams to focus their response efforts. This robust foundation of security and resilience, when combined with adaptability, are the attributes for antifragility. Enabling the organisation to thrive and grow in the midst of this volatility.**

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

I. INTRODUCTION

In his book: "Antifragility, things that gain from disorder," Nassim Taleb [51] uses the term *Black Swan* to describe unexpected situations with three 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 [1][19][52]. 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 [1].

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 [1]. The proposed approach for responding to 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 lack of preparation and poor 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 [6][44]. 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.

This approach to cyber security and resilience requires a combination of structured, pragmatic thinking and follow-through, along with action-based responses to emerging threats. If the organization is to grow and thrive, rather than merely survive from these events, adaptive thinking is also needed. Antifragility develops through environmental awareness, seeking out and being open to opportunities, and taking action to take advantage of the volatile environment and create new markets.

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. 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. Section 6 addresses the actions needed to contain, manage, and recover from an infection. Section 7 explains how antifragile organisations, that are adaptable and agile, can gain advantage from these situations, and thrive in these volatile cyber environments.

II. EMOTET AND WANNACRY EXPLOITS AND THEIR IMPACTS

Over the last decade two of the most significant 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, establishing a foothold, and implementing assault strategies across the network [6][7][22][27][35][42][43][46][48]-[50].

A. *Emotet scale and impact*

Emotet is believed to be based out of Ukraine [17][44]. It started as a banking Trojan and has continued to evolve since it was first identified in 2014 [17][44] (see Figure 1).

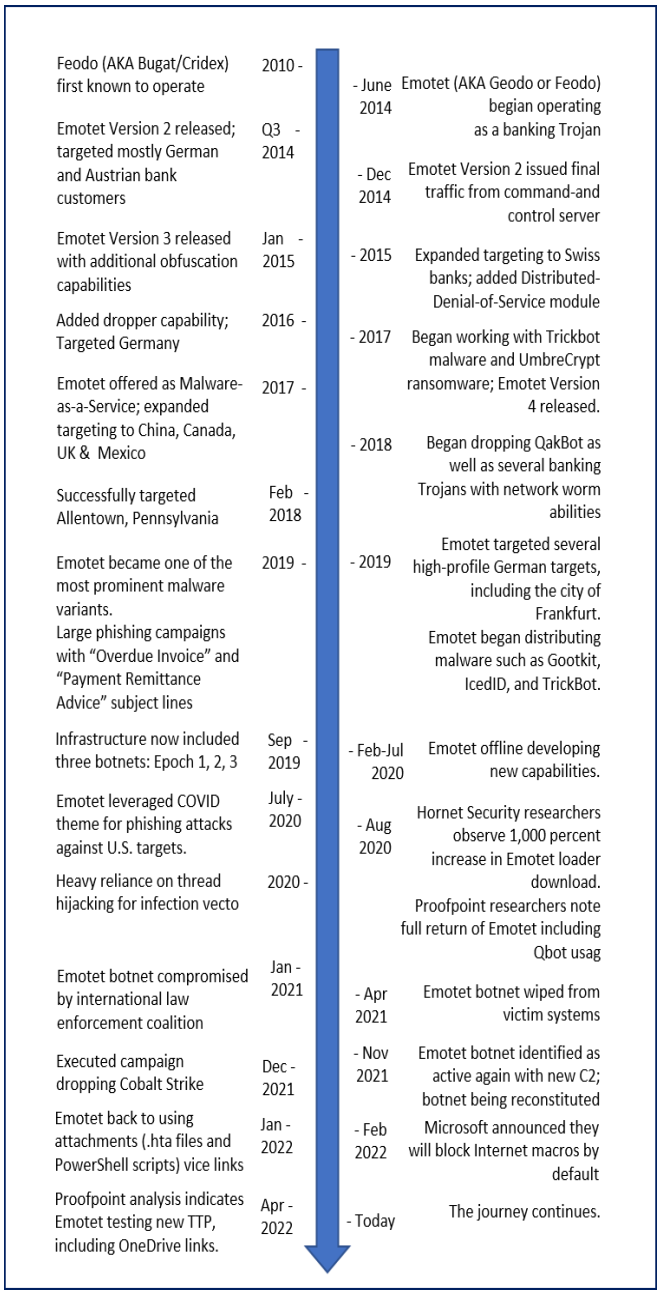

Figure 1. Emotet timeline, adapted from [17].

In 2019, Emotet was responsible for approximately 60% of malware email spam [44]. By 2020 it had morphed into Botnet as a Service, and Malware as a Service (MaaS) with global distribution [55]. Infected devices themselves become command and control (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 [43] (see Figure 2).

Figure 2. Geographic distribution of Emotet Botnet IP addresses, June 2019 [40].

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 [43]. The Trojan malware, or a copycat, returned in November 2021 and infected an estimated 1.2 million systems in 2022 [17][43][55] (see Figure 1).

B. *WannaCry scale and impact*

In May 2017, after infecting more than 300,000 computers and crippling 150+ organisations worldwide. WannaCry was dubbed "the largest ransomware event in history" [43] (see Figure 3). The WannaCry ransomware attack was stopped by a MalwareTech cyber researcher, who identified a key design flaw and purchased the URL WannaCry referenced in its attack sequence [26] (see Figure 4).

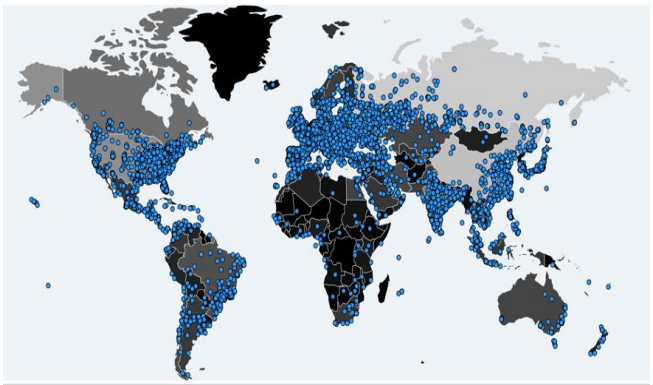

Figure 3. Distribution of WannaCry infections 14 May 2017, after 24 hours [6][23].

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 [43]. WannaCry brought

the British NHS to a standstill [15], including the closure of public hospitals. By June 2022, Emotet had spread from banks to auto & other manufacturers, health, government, education, transport, real estate, and retail [16][17] across Japan, Asia Pacific, Europe, Middle East, Africa, North and South America [17] (see Figure 2). It was estimated as costing in excess of $1 million for every organisation it infected [6][43].

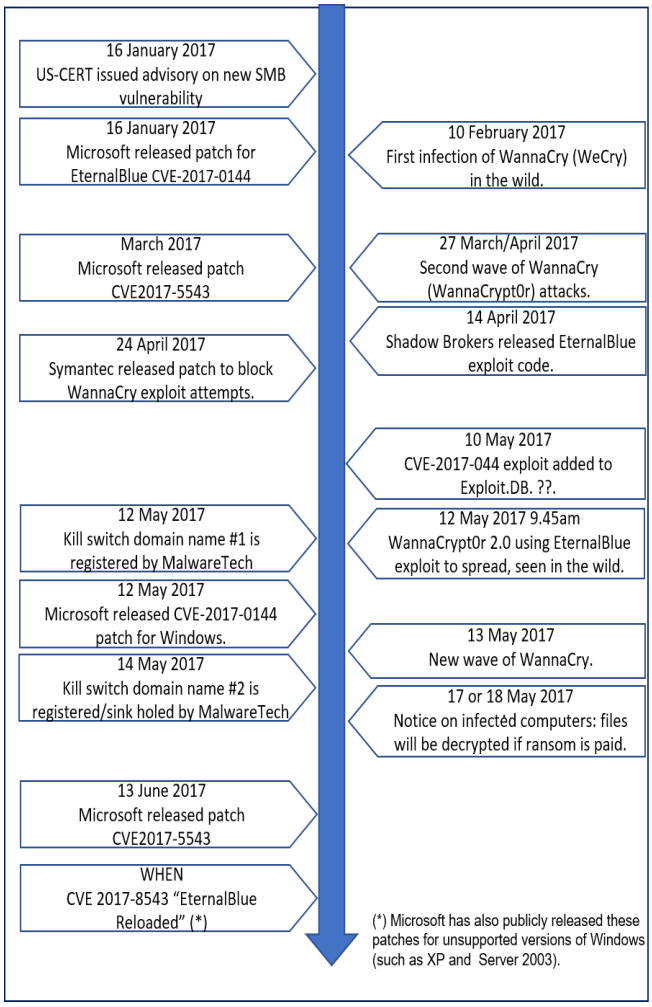

Figure 4. WannaCry timeline, derived from [18][25][26][49].

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, "past-due" invoices [6], or COVID information [41] (see Figure 5). 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 [6][42][43].

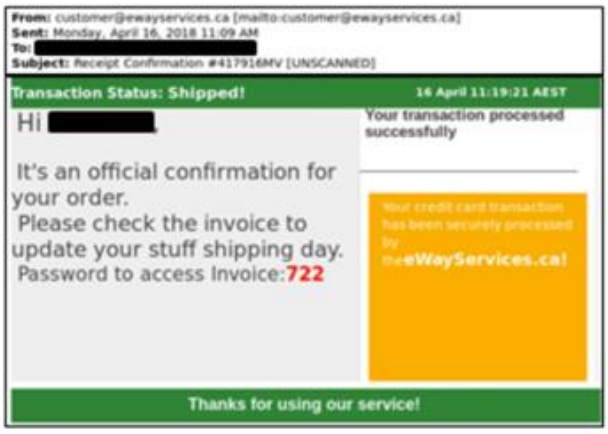

Figure 5. Emotet malicious email Emotet [6].

Emotet spreads by extracting contact lists from infected users' email accounts and using these to send phishing emails so they 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: (i) NetPass.exe from NirSoft extracts passwords stored on the user's system and external drives; (ii) WebBrowserPassView extracts passwords stored on web-browsers such as Google Chrome, Internet Explorer, Mozilla etc.; and (iii) MailPassView extracts passwords stored on email providers such as Gmail, Outlook, Hotmail etc.

Emotet 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 [6][42][43] (see Figure 6).

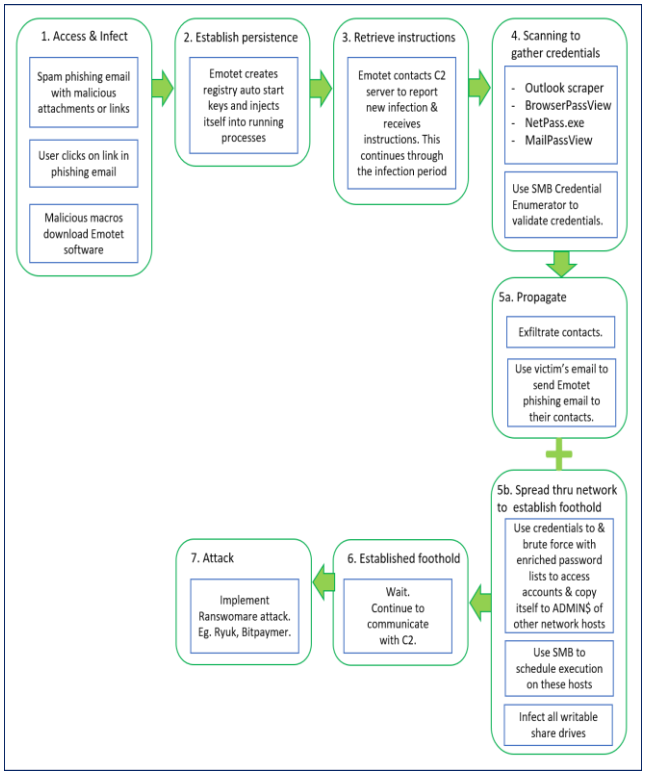

Figure 6. Emotet attack sequence, derived from [6][42][43].

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) [6][9][11]-[13][29][31]-[33][36][38]-[40][42]. 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 [42].

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 [54]. These ports are used to communicate using the SMB network protocol that enables remote code execution in MS Windows & sharing across networks [7][22][50].

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) [9][10][29][30][36][37][49] which enabled remote code execution over SMB v1, EternalBlue then accessed the vulnerable target systems and installed the DoublePulsar exploit for persistence [7][27][35]. 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 [18][46][48][49] (see Figure 8).

It then displayed a ransomware image to the users of infected devices [7][24] (see Figure 7).

Figure 7. WannaCry image displayed on infected user's desktop [7][24].

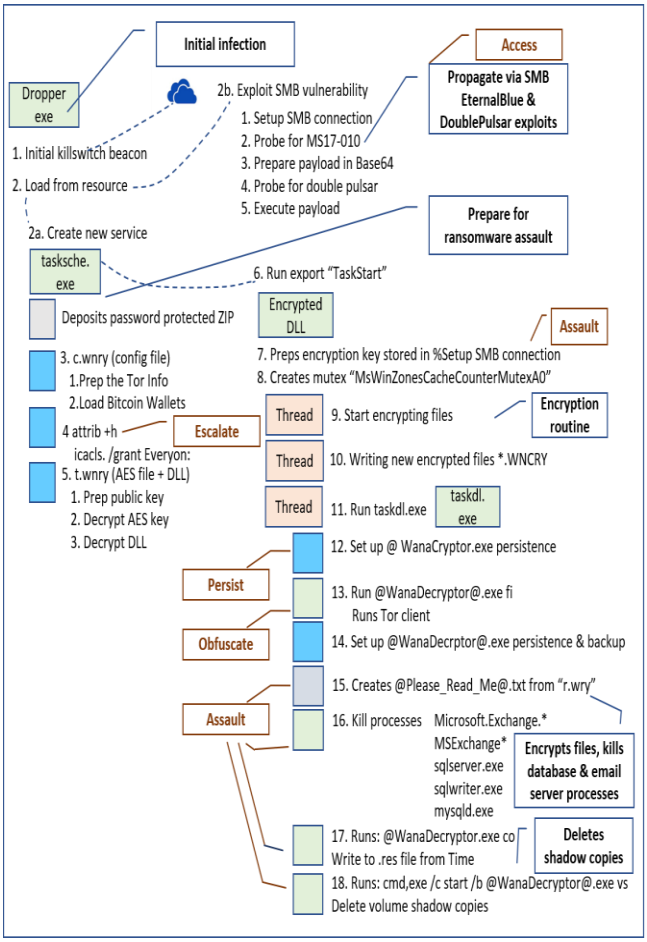

Figure 8. WannaCry infection process, adapted from [46].

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 cybersecurity capability 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 [2][3][8].
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 [29]-[31] and corresponding CVE reports [9]-[11] and NIST reports published on 16 March 2017 [36]-[38].
    b. Microsoft CVE-2019-0630 & CVE-2019-0633 vulnerability reports published in the Microsoft Vulnerability Update Guide on 12 February 2019 [32][33] and corresponding CVE reports [12][13] and NIST reports published on 3 May 2019 [39][40].
3. Threat alerts and reports:
    a. Threat alerts and reports are readily available through research centres such as Fifth Quadrant [14], Malwarebytes [25], MalwareTech [26], Metasploit [28], Qualys [45], Proofpoint [44], Talos [53], Truesec [57][58], and Verizon [61].
    b. Cyber teams in peer organisations sharing information. Australian organisations, including the big-4 Banks, openly share information in a joint effort to fight cyber crime, directly and through the Joint Cyber Security Centre (JCSC) [20].
    c. Up-to-date information is available through the reports provided by the Australian Signals Directorate (ASD) and US Cert [4][6].

V. Preventing 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, maintaining situational awareness, and monitoring and responding when a threat is identified, or suspected.

A. 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 or unpreviewed attachments 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 [6][8].

2. Incorporate desired cyber practices into policies. For example, implement a policy requiring users to forward suspicious emails to the security team [6].

3. Control and monitor who has access to what, when. Implement Privileged Access Management based on the principle of least privilege [8].

4. Keep all operating system and application patching up-to-date, by applying tested patches and updates as a priority. In particular, test and apply critical patches immediately. Five weeks prior to the main WannaCry attack, both the Australian Signals Directorate [4] and Microsoft had issued updated CVE reports. Microsoft released emergency patches to the Windows SMB vulnerabilities that enabled WannaCry's EternalBlue and DoublePulsar exploits recommending updates be applied immediately [7][8][34].

5. Regularly perform vulnerability scans to identify any unpatched devices [8][45].

6. 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 [6].

7. 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 [6][8].

8. 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 [6][8].

9. 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 [6][8].

10. Disable macros and PowerShell to prevent macro driven PowerShell commands, such as those utilised by Emotet [6][8].

11. 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 [6].

12. 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 offline or on a separate network and restoration is tested regularly to prevent failure when restoration is really needed [2][3][6][8].

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 such as XP and Server 2003 [18] [38][46][49].

B. Maintaining situational awareness

Security teams need to be tasked with staying abreast of the current and emerging threats, the vulnerability-state of the organisation's systems and people, the effectiveness of existing controls, and availability of updated controls to address emerging vulnerabilities. The Cyber Security Strategy, based on robust risk management, needs to be maintained in-line with the evolving environment. Ongoing communication to key stakeholders is critical to ensure organisational support and resourcing.

C. Responding proactively to emerging threats and exploits

Historically, Australia has faced the global-scale cyber attacks after Europe and North America. This has provided a short window in which to act, and mitigate known vulnerabilities. On Sunday 14th of May, Australian organisations had a few hours during which to ensure critical windows-based systems were patched or segregated to protect themselves from the ensuring WannaCry attack, prior to business opening on the Monday morning.

As cyber exploits are combined in new and crafty ways, the ingeniousness of the response needs to match that of the adversaries.

VI. MANAGING AN INFECTION

Priority response actions are needed to minimise the impact of these cyber Black Swan situations, for organisations that become infected.

A. Managing an Emotet infection.

Emotet progresses with credential extraction, captures the user's credentials on all accounts and systems, and spreads across the network prior to issuing a ransomware demand that makes the user eventually aware of the infection. By this time Emotet is embedded throughout the network. Immediate action is required to:

1. Contain the infection, to prevent it spreading across the network. Identify, shutdown, and take the infected machines off the network. Don't use domain or shared local administrator accounts to log into infected systems [5].
2. It may be necessary to temporarily take the network offline [5].
3. Remove the Emotet malware from infected devices by reimaging these devices, and ensure the windows patches provided by Microsoft have been applied [5][32][33][36][38].
4. Apply backups.
5. Prevent re-infection. Scan the reimaged and clean systems and move these to a segregated virtual local area, away from the infected network [5].
6. Issue password resets for all affected credential groups, including password vaults [5].
7. Identify the original source of the infection. ie. The device that was first infected [5].
8. Review the log files for this user's account to ensure any auto-forward rules for emails are turned off, and prevent further data breaches [5].
9. Use the clean systems to return to normal business operations.
10. Continue to monitor for any unidentified infections, affected systems, and users.
11. Document the incident report.
12. Communicate with senior stakeholders, employees and customers, throughout. Sensitive customer

information may have been exfiltrated during the infected period. Communicate to impacted entities and regulatory bodies in line with company policy and regulatory requirements.
13. To prevent re-infections: Review the operating system maintenance and patching processes; and Educate users to not click on phishing email links.
14. If not already in place, implement targeted educational phishing campaigns.
15. Post Incident Review to assess protection, response, and restoration effectiveness and identify improvements.
16. Communicate findings, and action improvements.
17. Post Implementation Review the system maintenance processes, and measure the click rate in the organisation 3 & 6 months later to ensure the required changes have been made and the desired click rated achieved.
18. Implement further improvements, if required.

B. *Managing a WannaCry infection.*

Those infected with WannaCry malware were immediately made aware by the ransomware messages, and the loss of data availability due to WannaCry encrypting all the word, excel, pdf etc. files [6][21]. Immediate action was required to:

1. Contain the infection, to prevent it spreading across the network and prevent re-infection, by identifying unpatched devices applying the Windows patches provided by Microsoft [32][33][39][40].
2. Implement regular vulnerability scanning to identify unpatched devices [45]. Targeted vulnerability scanners that focus on finding the specific Windows vulnerabilities that enabled WannaCry, are now also available [59].
3. Recover the encrypted files from backups. At the time of the original WannaCry attack, the only way to recover lost or encrypted files, was to restore from backup. Since then, WannaCry decryptors have been developed [60].
4. Return to normal business operations.
5. Continue to monitor for any unidentified infections and affected files.
6. Document the incident report.
7. Communicate with senior stakeholders, employees, and customers, throughout. Communicate to regulatory bodies in line with company policy and regulatory requirements.
8. Review the operating system maintenance and patching processes to prevent similar infections.
9. Post Incident Review to assess protection, response, and restoration effectiveness and identify improvements.
10. Communicate findings, and action improvements.
11. Post Implementation Review these processes 3 & 6 months later to ensure the required changes have been made.
12. Implement further improvements, if required.

VII. FROM SURVIVE TO THRIVE

The practices of situational awareness, proactive risk management, systems' maintenance, and priority response to threats and infections are the fundamentals of good cyber and systems' management practices. When performed consistently over time, these practices provide a solid foundation for robust security and business resilience. Significantly reducing the likelihood that the organization will be heavily impacted by a cyber attack. But routine procedures are designed to operate within known thresholds. When unexpected and unknown events exceed these thresholds, such as those experienced in cyber black swan situations, these alone cannot necessarily be relied upon to perform optimally. These situations require more flexible response [47].

Fragility relates to how systems are negatively impacted when the environmental volatility exceeds a threshold [52]. Organisational risk management is typically based on known historical events. The thresholds of the risk management are defined by these past events. By definition, black swan events are unexpected, and lie outside the threshold [51][52].

The process of evolution through natural selection produced the Australian platypus and kangaroos. Evolution is, at its core, an example of antifragility [56]. Only organisms that are adaptable to the changing environmental conditions and variables survive, thrive, and proliferate. Those that are only robust within stable environments do not survive when this environment changes rapidly or unexpectedly.

Paradoxically, cyber antifragility is built on a foundation of structure, standardisation, and good cyber and systems practices, combined with behavioural adaptability to volatile situations to take advantage of opportunities emerging from the disruption [56].

Going beyond security and resilience to antifragility moves the focus from surviving to thriving in the face of adversity. The critical attribute displayed by antifragile organisations is their ability to modify goals and behaviours when in crisis. This requires flexible thinking, problem solving, and in the case of cyber black swan situations, ability to utilise technology to obtain and interpret information in real time [56]. Leaders, and teams need to be able to adjust their ways of working and coordinate

differently; To adjust their performance strategies, and adapt to the new situation [47].

Antifragile organisations turn crises into opportunity by rapidly modifying their business model and organisational behaviours to take advantage of the situation. This requires foresight, a hunger for new opportunities, agility to rethink and change the way they work, ongoing research to determine how this can be achieved, and capital investment to enable it [56].

Cyber antifragility is more than just defence or resilience as it necessitates both stability and growth in the face of adversity, of any scale. Rather than just recovering to the pre-event state, after the incident, antifragile organisations improve as a result of being regularly challenged by new cyber events and situation [56].

VIII. Conclusion

Analysis of the Black Swan Situations generated by the Emotet and WannaCry malicious exploits highlight the ways in which these types of situations can be predicted and prevented.

Situational awareness enables organisations to notice and interpret the early warning signs; to stay abreast of and prepare for emerging vulnerabilities and threats. Preparation involves addressing the weakest link as well as implementing practical controls, such as privileged access management, maintaining defence in depth, and keeping reliable backups.

Awareness of its cyber capability and open vulnerabilities also ensures the organisation can respond to zero-day exploits by limiting exposure of critical systems and immediately applying emergency patches to vulnerable systems. Priority protection and response action when an infection is detected limits the extent of the infection, its effects, and the impact on the business and customers. These are the fundamentals of good systems and cyber management practice, providing security and resilience.

Antifragile organisations take this to the next level by developing the agility to adapt in the face of adversity, to take advantage of the situation. While others survive, these organisations thrive, benefiting from the constantly changing threat landscape and the cyber black swans.

References

[1] A. Coull, “Black Swan or Just an Ugly Duckling?, Can potentially crippling cyber situations be foreseen and mitigated? ” IARIA CYBER 2022 : The Seventh International Conference on Cyber-Technologies and Cyber-Systems. Available from: https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2022

[2] 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.

[3] 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.

[4] ACSC, Australian Signals Directorate - view all alerts, Available from: https://www.cyber.gov.au/acsc/view-all-content/alerts, accessed February 2023.

[5] 3+1Any run, “Emotet”, 2021, Available from: https://any.run/malware-trends/emotet, accessed October 2022.

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

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

[8] 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.

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

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

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

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

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

[14] Fifth Quadrant, “Customer Experience Research, Design & Consulting,” 2017, Available from: https://www.fifthquadrant.com.au/customer-experience-research-design-consulting-fifth-quadrant, 2022, accessed October 2022.

[15] J. Graham, “How to Rapidly Identify Assets at Risk to WannaCry Ransomware and ETERNALBLUE Exploit,” 2017, 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.

[16] J. Hanrahan, “Suspected Conti Ransomware Activity in the Auto Manufacturing Sector,” Dragos Blog 16 March 2022, Available from: https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/, accessed March 2023.

[17] HC3 Health Sector Cybersecurity Coordination Centre, Office of Information Security, “The Return of Emotet and the Threat to the Health Sector,” June 2, 2022, Available from: https://www.hhs.gov/sites/default/files/return-of-emotet.pdf, accessed March 2023.

[18] 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.

[19] 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.

[20] JCSC, "Joint Cyber Security Centre", 2022, Available from: https://www.cyber.gov.au/acsc/view-all-content/glossary/joint-cyber-security-centre-jcsc, accessed December 2022

[21] 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.

[22] 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.

[23] M. Lee, W. Mercer, 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.

[24] 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.

[25] Malwarebytes Labs, "Threat Types", 2023, Available from: https://www.malwarebytes.com/blog/threats, accessed January 2023.

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

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

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

[29] 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.

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

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

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

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

[34] Microsoft, "Security Update Severity Rating System (microsoft.com)," available from: https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system, accessed March 2023.

[35] 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.

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

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

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

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

[40] NIST, "CVE-2019-0633 Detail," 2019, Available from: https://nvd.nist.gov/vuln/detail/CVE-2019-0633, accessed October 2022.

[41] D. Palmer, "Emotet: The world's most dangerous malware botnet was just disrupted by a major police operation," ZDNET 27 January 2021, Available from: https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/, accessed March 2023.

[42] A. Perin, "Emotet Re-emerges with Help from TrickBot," 6 January 2022, Available from: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/06/emotet-re-emerges-with-help-from-trickbot, accessed January 2023.

[43] A. Petcu, "Emotet Malware Over the Years: The History of an Infamous Cyber-Threat," 23 February 2022, Available from: https://heimdalsecurity.com/blog/emotet-malware-history/, accessed January 2023.

[44] Proofpoint, "Q4 2020 Threat Report," 2020, Available from: https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes, accessed November 2022.

[45] Qualys, "IT Security and Compliance Platform," 2023, Available from: https://www.qualys.com/, accessed January 2023.

[46] 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.

[47] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A. Tomassetti, K. Repchick, S. Zaccaro, R. Dalal, and L. E. Tetrick 2015, "Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research," IEEE Security & Privacy, Multidisciplinary Security July/August 2015 Vol. 13, No. 4, Available from: https://www.researchgate.net/publication/281467215_Improving_Cybersecurity_Incident_Response_Team_Effectiveness_Using_Teams-Based_Research, accessed February 2023.

[48] 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.

[49] 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.

[50] 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.

[51] N.N. Taleb, "Antifragile, things that gain from disorder", Random House, Penguin Random House LLC, New York, 2021.

[52] N. N. Taleb and J. West, "Working With Convex Responses: Antifragility From Finance to Oncology," Tandon School of Engineering, New York University, 2015

[53] Talos, "Talos Threat Intelligence", 2023, Available from: https://talosintelligence.com/ , accessed January 2023.

[54] 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.

[55] Trendmicro, "EMOTET malware resurges with new detections (trendmicro.com)," Available from: https://success.trendmicro.com/dcx/s/solution/1118391-malware-awareness-emotet-resurgence?language=en_US, accessed March 2023.

[56] TQM 2021, "Turning crises into opportunities in the service sector: how to build antifragility in small and medium service enterprises," The TQM Journal, December 2021.

[57] Truesec, "Threat Intelligence Report 2021," 2021, Available from: https://www.truesec.com/hub/report/threat-intelligence-report-2022, accessed January 2022.

[58] Truesec, "Threat Intelligence Report 2022", 2022, Available from: https://www.truesec.com/hub/report/threat-intelligence-report-2022, accessed January 2023.

[59] TWC, "Free vaccinator & vulnerability scanner tools for WannaCry ransomware," 15 May 2017, The Windows Club, Available from: https://www.thewindowsclub.com/free-vaccinator-vulnerability-scanner-tools-wannacry-ransomware, accessed January 2023.

[60] TWC, "WannaCrypt or WannaCry ransomware decryptors are available," The Windows Club, 19 May 2017, Available from: https://www.thewindowsclub.com/wannacrypt-wannacry-ransomware-decryptor, accessed January 2023.

[61] Verizon, "Latest Cybersecurity Risks and Events", Verizon Business, 2023, Available from: https://www.verizon.com/business/en-au/resources/security/cybersecurity-news-and-events/, accessed January 2023.

[62] S. Winterfeld and J. Andress, "The basics of cyber warfare: understanding the fundamentals of cyber warfare in theory and practice", 2013, Elsevier, Inc, United States of America.