Black Swan
Or just an ugly duckling?

Can potentially crippling cyber situations be foreseen and mitigated?

Anne Coull

Objective Insight

anne.objectiveinsight@gmail.com

The video of this presentation with voiceover by the author is available from: https://youtu.be/dxY-K0B4-N8

Anne Coull

Anne Coull, from Objective Insight and Getting of Wisdom consulting, is currently working with Australia's largest bank in Financial Crime prevention, leading their premier portfolio of programs implementing directly into the cloud. She is responsible for ensuring sensitive and restricted customer data is stored securely in the cloud, and that Australian and international regulatory bodies are satisfied that adequate cyber security controls have been applied.

Anne is passionate about making cyber security part of every-day life, in the same way that hand-held devices are, and that people are empowered with the knowledge to protect themselves, their families, and their businesses from attack.

With a track record for building high performing teams that deliver business outcomes, Anne creates a growth culture with purpose, accountability, and diversity of thinking. Pragmatic, data-driven, and calm under pressure, she builds genuine partnerships with stakeholders at all levels, and applies her extensive experience in Program Delivery, Organisational Change, Cyber Security, Financial Crime, Software Development, Service Management, Agile, Lean and Six Sigma to deliver Business, Cultural, Technology and Performance Transformations.

Dedicated to continuous learning and research, Anne is an active contributor to the International Academy, Research, and Industry Association (IARIA), co-founder of Women in Cyber Security (WiCys) Australia, and a member of the UNSW ADFA Cyber War and Peace Group and the UNSW School of Engineering & Information Technology (SEIT) External Advisory Committee.

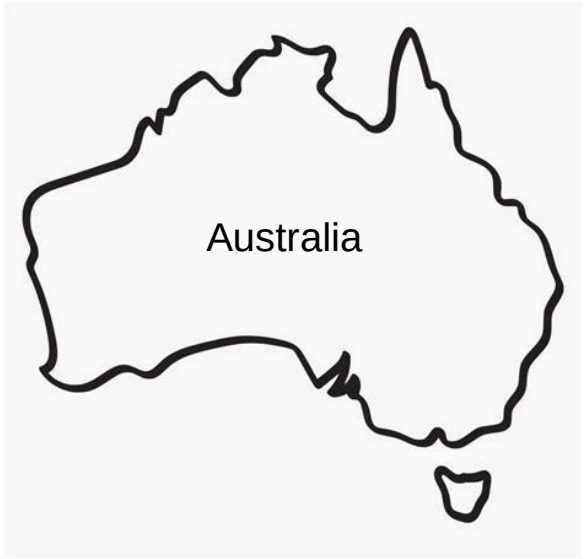
Black swan situations

Termed by Nassim Taleb in his book: “Antifragility, things that gain from disorder.”

A Black Swan situation is an *unexpected* situation with 3 attributes:

I. Before the situation occurs, it is considered extremely unlikely, if not impossible;
II. When it occurs its consequences are significant, either in changing belief, or in consequence;
III. After it has occurred, it makes perfect sense as something that could happen

Unexpected is modus operandi



Black swan situations: Emotet and WannaCry

Emotet Banking Trojan => Botnet as a Service

WannaCry Worm: “largest ransomware event in history”

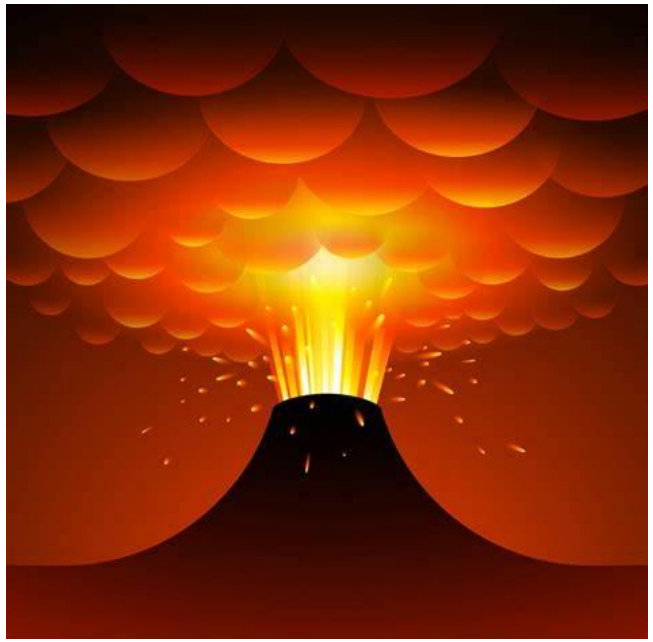
Trigger

+

System & Human Vulnerabilities

Poor situational awareness

Delayed Response

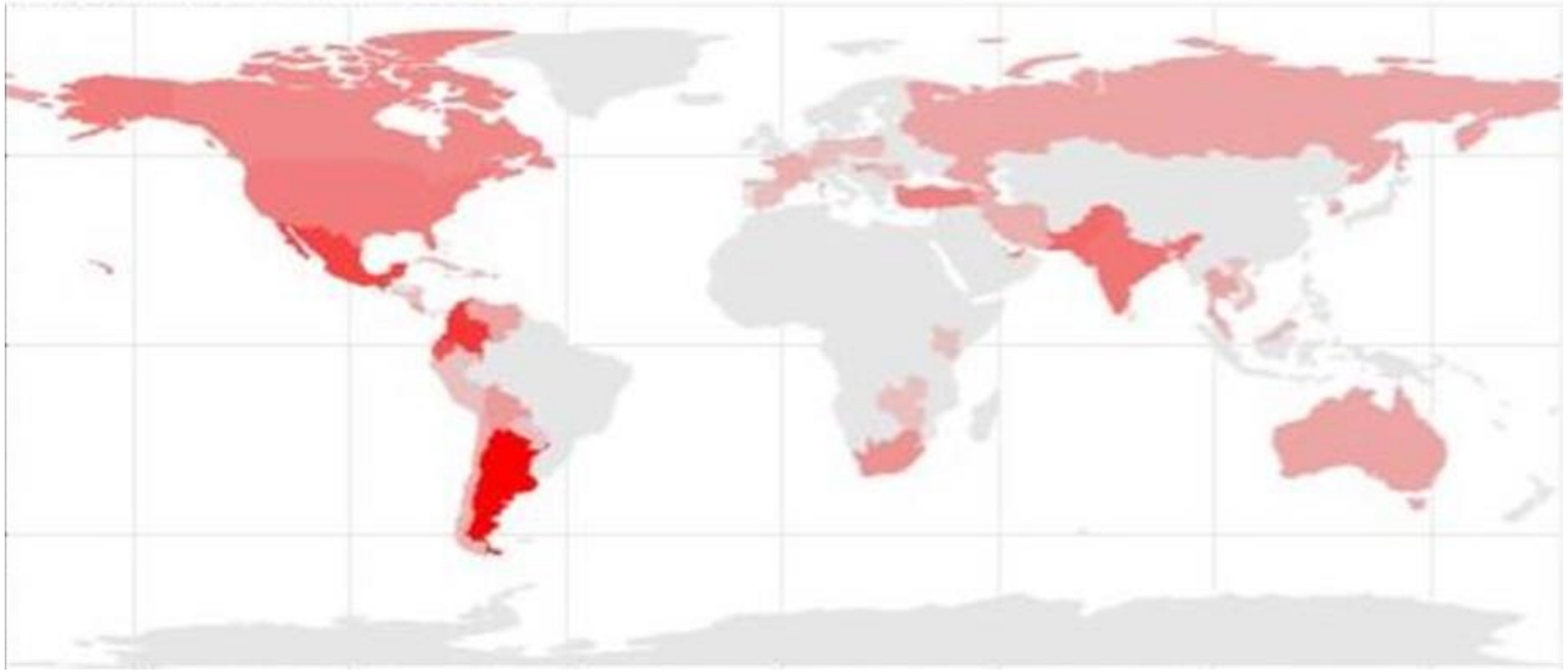


Large scale, high impact globally

Black Swan cyber situation: Emotet

Large scale, high impact

Emotet
Banking
Trojan
=>
Botnet as
a Service

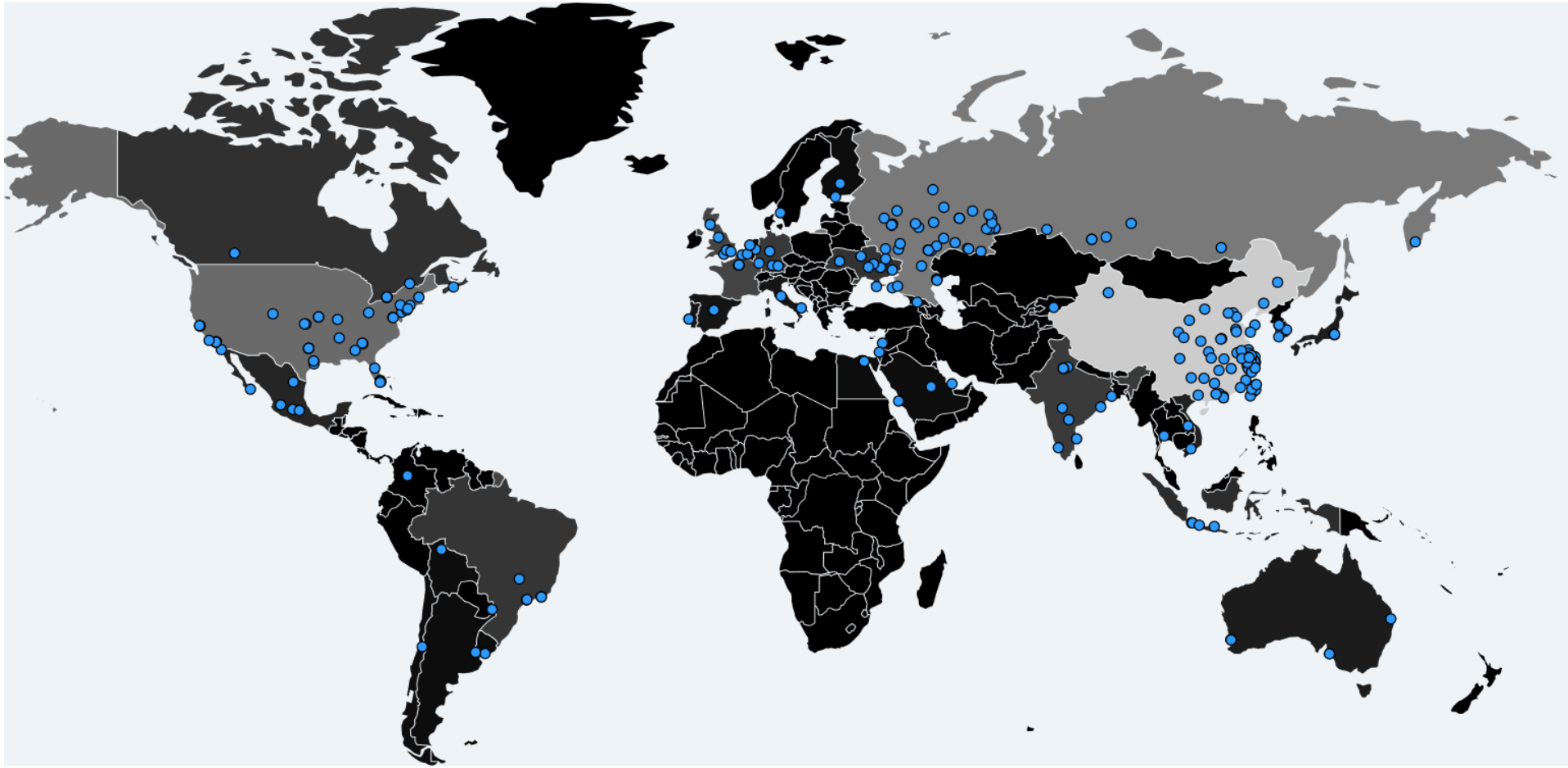


Distribution of Emotet botnet IP addresses, June 2019. [36]

Black Swan cyber situation: WannaCry

Large scale, high impact

5 minutes

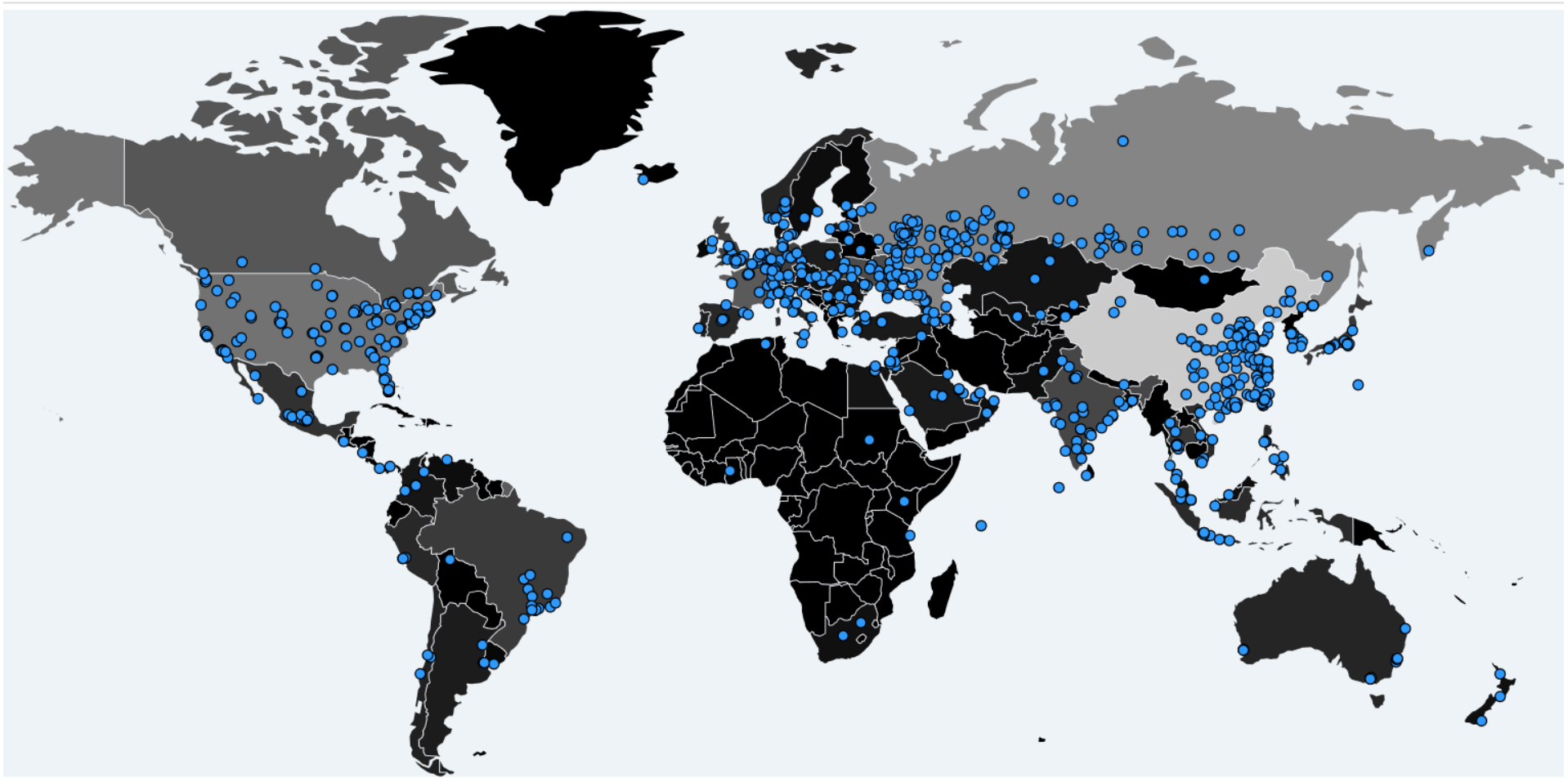


Distribution of WannaCry infections
14 May 2017, after 5 minutes [5][19]

Black Swan cyber situation: WannaCry

Large scale, high impact

1 hour

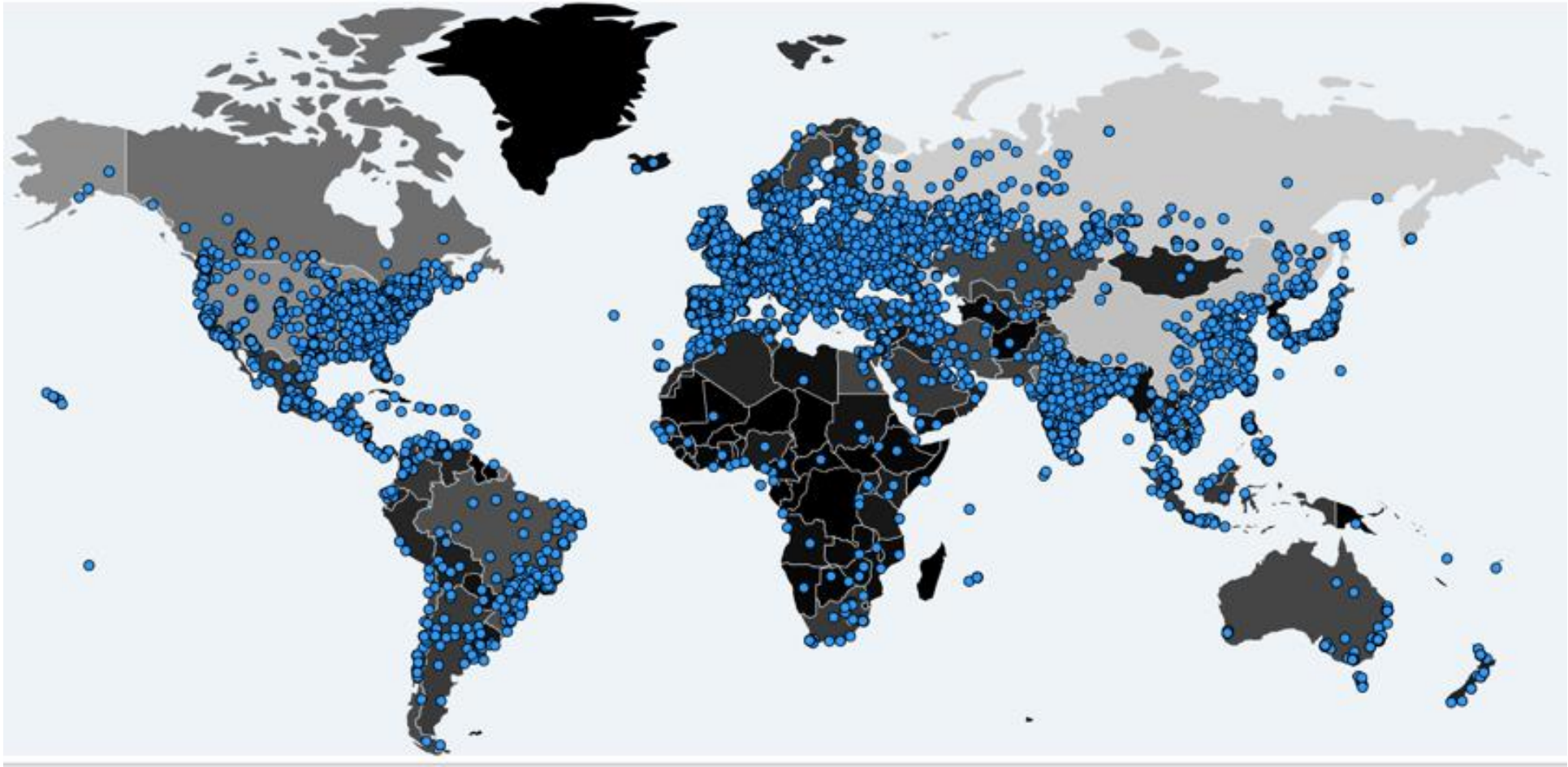


Distribution of WannaCry infections
14 May 2017, after 1 hour [5][19]

Black Swan cyber situation: WannaCry

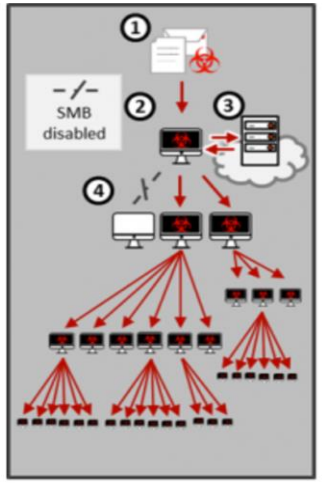
Large scale, high impact

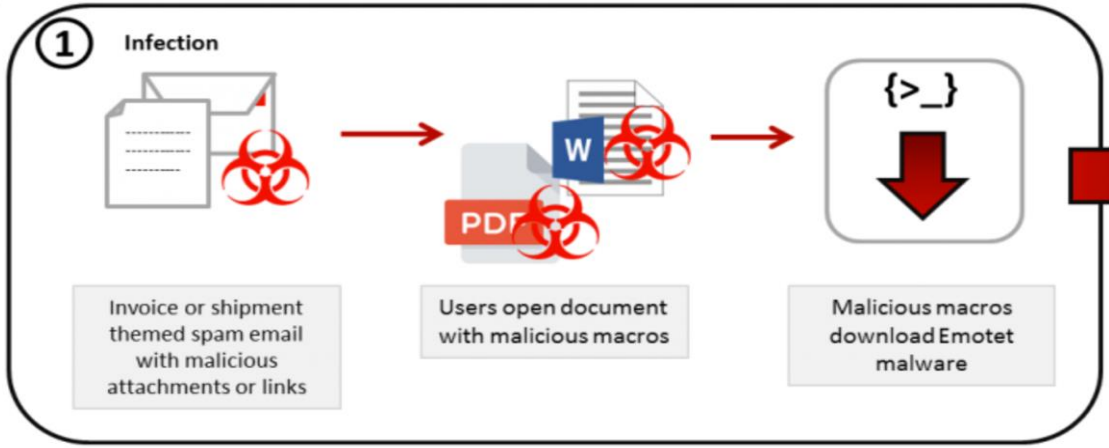
24 hours

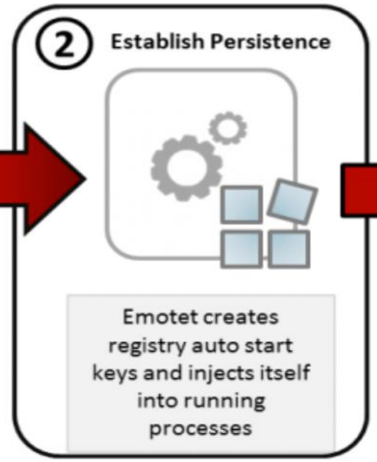


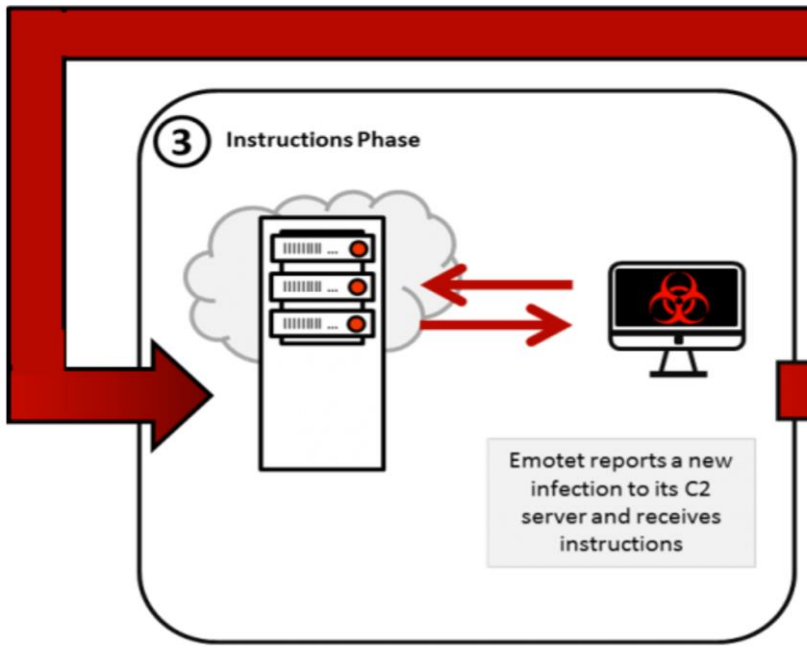
Distribution of WannaCry infections
14 May 2017, after 24 hours [5][19]

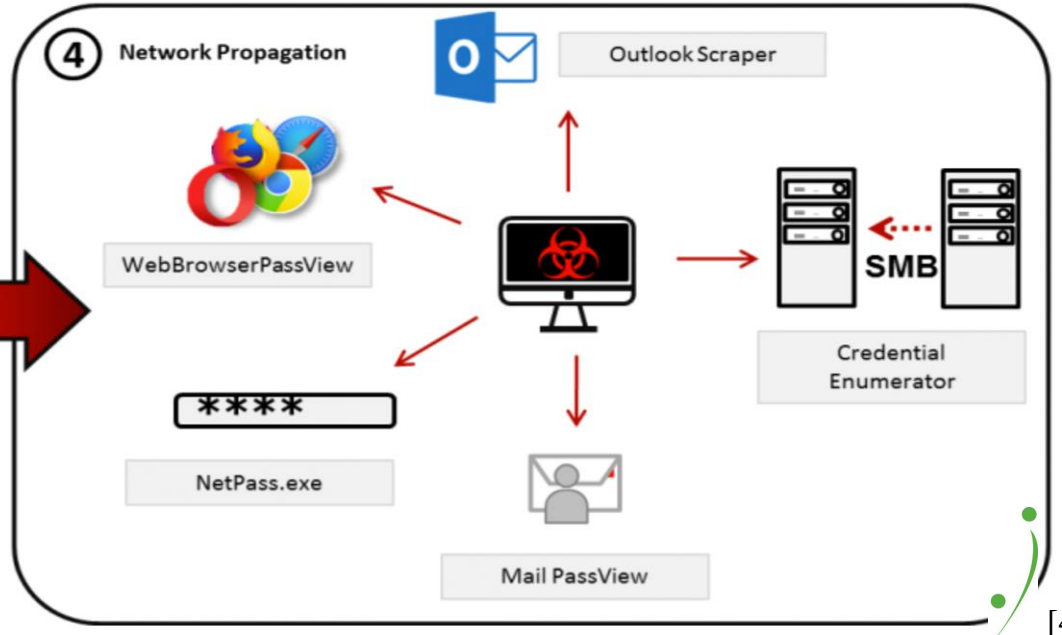
Emotet infection process

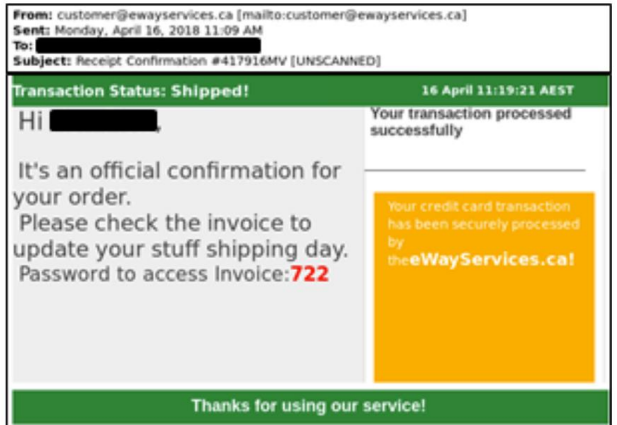






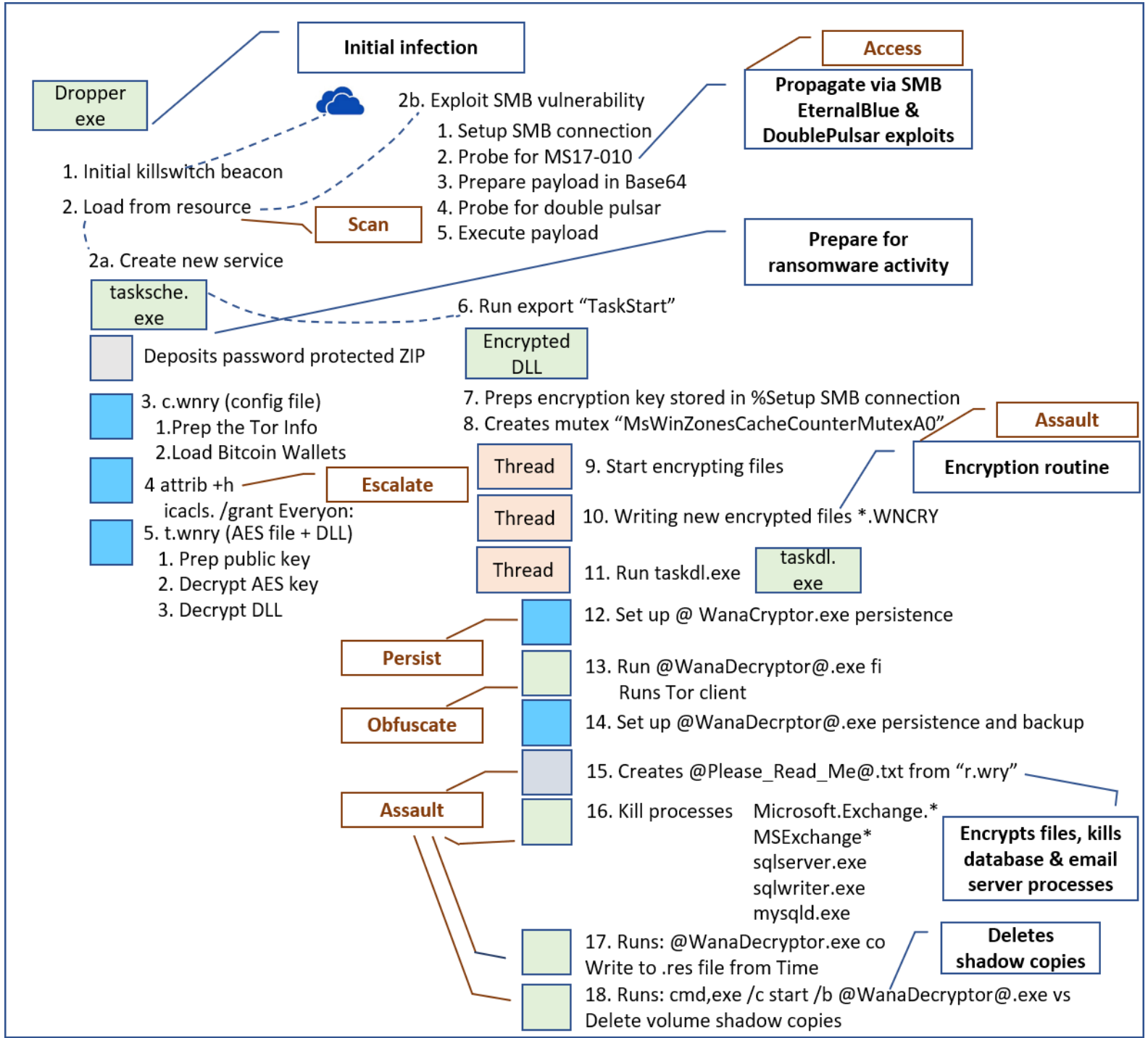






[4

WannaCry attack sequence



[5][18][36]

Notice early warning indicators through situational awareness of vulnerabilities and threats.

There to be found by those who seek them: friend or foe.

1. Current state of the organisation
    - Cyber-risk awareness of personnel based on click-rate
    - Compliance with cyber security standards and guidelines
    - Maintenance of these

2. Critical Vulnerability Reports
    - Microsoft CVE & NIST

3. Threat alerts and reports from cyber research centres
    - MalwareTech
    - Metasploit
    - Qualys

    Open communications between cyber teams, sharing information

Preventing these Black Swan situations

Be alert, take action!

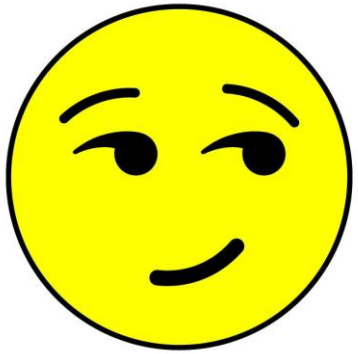
1. Address the weakest link: people
2. Incorporate cyber into policies
3. Control who accesses what, when
4. Maintain a technology barrier
5. Be prepared for the worst, with backups
6. **Maintain current state situational awareness**
7. Limit exposure of critical systems and data
8. Apply emergency zero-day patches immediately

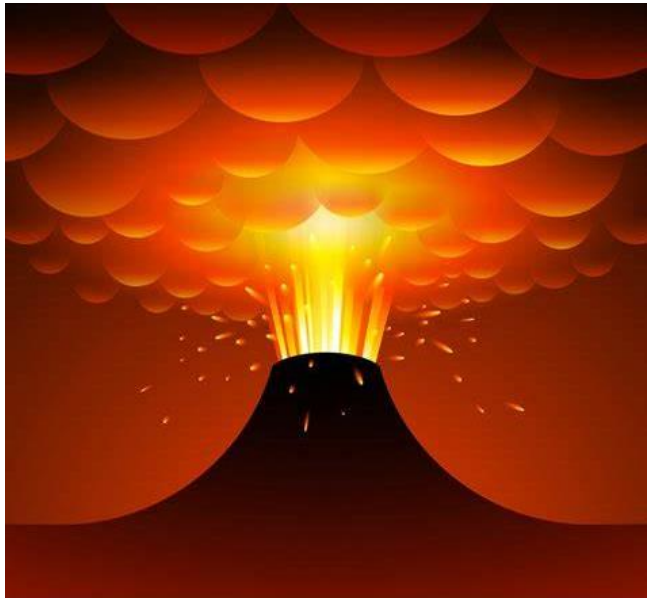
[1][2][4][6]

Black swan cyber situations develop

Trigger

Situational awareness + Preparation & Response





Conclusion

Situational awareness
+
Preparation and Response

Black Swan situations are preventable

1. Policies, processes and practices that align with current state
2. Individual accountability for *everyone*
3. **Situational awareness through timely and relevant information**
4. Constantly changing:
    1. Cyber environment
    2. Malicious actors
    3. Threats
    4. Vulnerabilities

5. **Situational awareness is key to preventing malicious exploits developing i**nto Black Swan situations.
6. Notice the early warning signs, prepare for and respond to emerging situations

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 2020.

[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 May 2017.

[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 2017.

[17] P. Rascagneres & 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 29 August 2017.

References (cont 1)

[18] LogRhythm, “A technical analysis of wannacry ransomware, LogRhythm Labs, ” 16 May 2017, accessed 31 august 2017, Available from: https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/, accessed 31 august 2017.

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

[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 15 October 2017.

[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 2017.

[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.

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

[33] Perin, A, “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.

References (cont 2)

[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 2017.
[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 2017.
[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 2017.
[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 2017.
[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.

Questions?

Please email your questions to

Anne Coull

anne.objectiveinsight@gmail.com