LACK OF RESPONSE TO BOTNETS

Q: "Why is there still lack of experts and resources when it comes to fighting botnets?" – Akshay Awasthi question for paper on botnets

A: The roots of inaction in cyberdefense against botnets are fundamental problems we face in the field of information assurance (IA).

One of the key problems is that there is no comprehensive source of statistical information about cybercrime and other IA problems.

- First, there's the problem of ascertainment: many attacks, including malware infections, are deliberately designed to elude observation. Antimalware systems and security information and event management software (SIEM) are constantly having to adapt to new attack methods. This situation is inherently leading to delayed awareness of attacks. For example, zero-day exploits increased in 2015.[1]
- Second, there's the problem of reporting and data aggregation: as far as I know, there is no legal requirement anywhere in the world forcing victims of all cybercrime to report the breaches of security. In the US, "Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information."[2] However, the wide range of sites attempting to compile and report on computer crimes and other violations of IA rely entirely on voluntary input. In addition, even if victims recognize security breaches, many have no idea where or how to report them; a 2014 British report indicated that more than half of the UK victims didn't know what to do with the information.[3]

Another issue is that lack of awareness allows too many people and organizations to fail to maintain – or even to install – adequate antimalware and security-monitoring software or hardware. For example, a 2013 report suggested that about 24% of personal computers worldwide lack security software.[4] The failure to take even the most elementary measures for cyberdefense suggests that there is a massive problem of awareness. Awareness involves three elements: belief, attitude and behavior. It may be that many people worldwide believe that there is no threat to their systems; the classic belief is "Oh, no one would bother with my little computer." The attitude is thus dismissive: "It's not important." The behavior is the refusal to install and maintain even free security software.

In the corporate world, failure to maintain an adequate IA program is increasingly resulting in serious consequences for negligent officials. For example, a 2015 report listed specific examples of security failures in US government organizations that resulted in dismissal of responsible officials.[5] On the other hand, financial analysis suggests that some commercial entities choose to ignore IA because they don't cost much.[6]

* * *

[1] (Loeb, 2016)
[2] (National Conference of State Legislatures, 2016)
[3] (Palmer, 2014)
[4] (Meisner, 2013)
[5] (Claburn, 2015)
[6] (Hackett, 2015)

Works Cited

Claburn, T. (2015, Jul 14). *14 Security Fails That Cost Executives Their Jobs.* Retrieved Jul 15, 2016, from InformationWeek Government: http://www.informationweek.com/government/cybersecurity/14-security-fails-that-cost-executives-their-jobs/d/d-id/1321279

Hackett, R. (2015, Mar 27). *How much do data breaches cost big companies? Shockingly little.* Retrieved Jul 15, 2016, from Fortune: http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/

Loeb, L. (2016, Apr 15). *New Report Finds Zero-Day Vulnerabilities Increased in 2015.* Retrieved Jul 15, 2016, from Security Intelligence: https://securityintelligence.com/news/new-report-finds-zero-day-vulnerabilities-increased-in-2015/

Meisner, J. (2013, Apr 17). *Latest Security Intelligence Report Shows 24 Percent of PCs are Unprotected.* Retrieved Jul 15, 2016, from Microsoft Blog: http://blogs.microsoft.com/blog/2013/04/17/latest-security-intelligence-report-shows-24-percent-of-pcs-are-unprotected/

National Conference of State Legislatures. (2016, Jan 4). *Security Breach Notification Laws.* Retrieved Jul 15, 2016, from NCSL: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Palmer, D. (2014, Oct 21). *Half of Britons have been victims of cyber crime - but many don't know where to report it.* Retrieved Jul 15, 2016, from Computing: http://www.computing.co.uk/ctg/news/2376819/half-of-britons-have-been-victims-of-cyber-crime-but-many-dont-know-where-to-report-it

