Cybersecurity in Business: The Evolving Threat of Malware

Konrad Wiley, CSCI-412: Computer Networks I

Computers and computer networks are ubiquitous in businesses today, with internet connectivity being required for many business transactions, off-site collaborations, and customer engagement. The vast array of internet-connected cloud services, the depth of knowledge available through web searches, even internet phones provide businesses with solutions to problems that have allowed tremendous improvements in resource allocation and allowed businesses to spend more time solving the problems they're interested in, rather than getting bogged down in infrastructure. However, with this influx of available and accessible technologies come threats which most business leaders greatly underestimate, and even fewer understand.

Securing business networks introduces unique challenges, as "attack vectors" (ways in which hackers can gain access to a network) are seemingly infinite and constantly expanding. Twenty years ago, a business with internet connectivity would have to protect the workstations physically on-site, and ensure that their network was robustly configured (a task that, even as trivial as it seems in the face of today's challenges, was routinely inadequately performed), but today that same business will need to consider the ability of its employees to access the corporate network with smartphones, and how many corporate cloud services its employees may interact with from off-site using devices which the business cannot control (Hart, 2016). Unfortunately, the lack of risk awareness causes too many corporations to fail to take necessary steps to protect themselves, instead adopting a "wait for a crisis" approach to security where they presume they

are not a likely target. This often ends in disaster, as business leaders were simply unaware of the risks to their business. Critical business information can simply disappear forever, sensitive company email logs can be released to the public, financial information can be stolen, business equipment can be damaged, or personal client information can be published, causing irreparable harm to the company's image. Lawsuits, government fines, lack of public or investor trust, or financial burden due to lost revenue can all bring ruin to a company following a successful cyber-attack, effectively shuttering a previously successful business overnight (Brooks, 2019).

Malware has been a feature of computer networks since before the advent of the World Wide Web. In 1988, Robert Tappan Morris gained notoriety for creating and unleashing the "Morris Worm," a program which crippled university and other internet-connected networks across the globe by using exploits he had discovered in the Unix operating system (FBI, 2018). Now, more than 30 years later, malware continues to be one of the most dangerous threats to businesses in the internet age. There are two broad types of malware: executable viruses which contain compiled code which runs on the host operating system, and scripting viruses which use functionality of legitimate and trusted program on the host computer to perform illicit operations (bsi, n.d.). While executable viruses have been popular for attacking the general population, robust antivirus programs have increasingly stepped up their capabilities to analyze, recognize, and neutralize executable viruses before they can have much of an impact. Due to the evolving nature of cybercrime, this has in no way slowed the rate of successful attacks, as cybercriminals have instead largely shifted their focus to various forms of scripting viruses. One of the most dangerous aspects of scripting viruses is their ability to go unnoticed for extended periods, giving attackers persistent access to corporate networks and opening new attack vectors (Joshi, 2018).

In 2017, a rash of attacks left the cybersecurity industry stunned and reeling, with literally thousands of human lives at stake. The UK's National Health Service (NHS) was hit hard with the WannaCry virus, a "ransomware" that encrypts the files on a computer and demands payment to a bitcoin wallet in order to receive a decryption key. Ransomwares have existed since 1989, when a hacktivist biologist gave away infected floppy disks to people attending the World Health Organization's AIDS conference (KnowBe4, n.d.). The program on the floppy disks encrypted the data on user computers, and demanded payment be sent to a P.O. box in order to retrieve decryption keys. This primitive ransomware used a trivial encryption scheme, which made decrypting client data relatively simple. Modern ransomware malwares such as WannaCry use advanced RSA and AES-hybrid encryption, essentially ensuring that no data can be decrypted without the decryption key unless a mistake is made in the design of the malware (Marinho, 2018). These attacks were made possible due to a vulnerability allegedly discovered by the US National Security Agency and published online by a group known as the Shadow Brokers as part of a tool called "Eternal Blue" (Graham, 2017). This tool "take[s] advantage of weaknesses in how Windows implemented the Server Message Block (SMB) protocol" (Malwarebytes, n.d.).

> A bug in the process of converting File Extended Attributes (FEA) from OS2 structure to NT structure by the Windows SMB implementation can lead to a buffer overflow in the non-paged kernel pool. This non-paged pool consists of virtual memory addresses that are guaranteed to reside in physical memory for as long as the corresponding kernel objects are allocated.

> A buffer overflow is a programming flaw that lets the data written to a reserved memory area (the buffer) go outside of bounds (overflow), allowing it to write data to adjacent memory locations. This means attackers are able to control the content of certain memory locations that they should not be able to access, which attackers then exploit to their advantage. In the case of EternalBlue, they are able to control the content of a heap that has execution permission, which leads to the Remote Code Execution (RCE) vulnerability, or the ability to execute commands on a target machine over the network. (Arntz, 2018)

In the case of WannaCry, a flaw in the malware's design enabled a researcher to effectively disable the virus and stop its wildfire-like spread simply by registering a domain name, however it's been far from the last use of ransomware to attack businesses, acting more as a proof-of-concept than a fumbled attack (Telegraph Foreign Authors, 2017).

In the years since that attack, ransomware attacks have become a staple in the cybercrime industry, with Malwarebytes noting a 9% increase of ransomware attacks against businesses compared to 2017 (Figure 1) (Kujawa, et al., 2019). While ransomware attacks against the general population have fallen out of favor since 2017 (down 29% in 2018), the meteoric increase in ransom

Business Detections 2017/2018		
Pos.	Threat	Y/Y% Change
1	Trojan	132%
2	Hijacker	43%
3	Riskware Tool	126%
4	Backdoor	173%
5	Adware	1%
6	Spyware	142%
7	Ransom	9%
8	Worm	-9%
9	Rogue	-52%
10	HackTool	-45%
Overall Detections		
2017	39,970,812	79%
2018	71,823,114	

Figure 1: 2018 Ransomware attacks up 9% over 2017 (Source: Malwarebytes 2019 State of Malware Report)

amounts demanded of business attacked in 2019 has caused significant alarm in the cybersecurity industry. Investigative journalism has uncovered a politically complicated relationship between the rise of cybersecurity insurance coverage (offering businesses with industry standard audits, and providing financial stability in the face of a successful attack) and the insurance companies' willingness to payout ransom demands made by hackers, fueling additional attacks and often funneling money to enemy nation-states (Dudley, 2019). These reports have studied the dark truth that the ransomware crisis has been good for data recovery companies, IT security personnel, cybersecurity insurers, as well as the attackers. While many cities across the United States have pledged to refuse to make ransom payments in the event of an attack, such a decision can end up costing far more than even astronomical ransoms. In 2018, Atlanta, GA was hit with a $51,000 ransom demand, which they refused to pay. Subsequently, they've spent over $8.5M attempting to recover from the attack (Dudley, 2019).

Fighting malware is a bleeding-edge race, with governments and corporations dedicating teams of brilliant programmers and testers to the task of figuring out how to detect and fix vulnerabilities in their systems. Malwarebytes, and industry leader in "0-day" threat detection is increasingly leveraging AI to detect anomalous or dangerous behavior in programs, allowing malicious programs to be recognized by what they do, regardless of whether they've been seen in the wild before. To aid in the detection of script-based viruses, Microsoft has added a new layer to Windows 10 (Figure 2) which allows antivirus programs to directly interface with its integrated scripting languages (PowerShell and VisualBasic), and monitor the execution steps of scripts, substantially reducing the effectiveness of code obfuscation without crippling endpoint performance (Jacobs & Satran, 2019). This interface has provided a powerful line of defense

against “fileless malware” attacks, where no malicious code is ever saved to a hard disk but is instead loaded directly into memory and executed (Branscombe, 2019). These attacks have proved extremely hard to detect, as standard antimalware and antivirus programs searched files on hard drives for signatures or known-behaviors and were wholly unequipped to detect processes which never touched the hard disk.

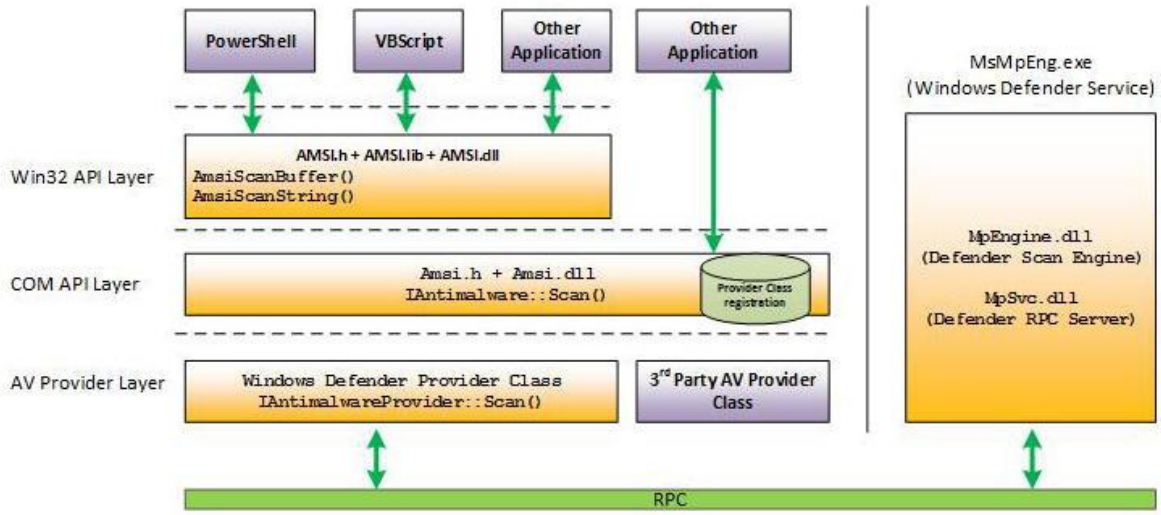

Figure 2: How AMSI intercepts scripts that try to drop fileless malware on systems. (Source: Microsoft)

In an interview with TechRepublic, Tanmay Ganacharya of the Microsoft Defender team had the following to say about the effectiveness of AMSI:

> "Instead of having to deal with a JavaScript file, or a PowerShell script file or Office macro code, and trying to reason on obfuscated content, as the script engine starts executing that content, it's able to check inline with the installed antivirus whether the sequence of events represent malicious behaviour," Ganacharya explains. "This made detections against JavaScript malware, PowerShell malware, any script-based malware extremely durable, because now we're not in the cat-and-mouse game of trying to deal with the different ways JavaScript get can get obfuscated. We didn't have to build heavy-handed parsers for all scripting languages that slow down end user machines: we just

> leveraged the script engine that's on the machine that has to run anyway -- and we're able to see what's happening and to stop it at the right point so that the actual malware never gets stood up." (Branscombe, 2019)

Being able to recognize and halt threats at each attack vector, even without knowing ahead of time what that threat could look like, is the evolving face of cyber security. Modern fileless malware threats such as Emotet are constantly evolving, and even receive updates from their authors to help them hide from detection systems (Malwarebytes, n.d.). In many cases, these malwares are designed to not perform if under observation: Emotet will stay dormant if it detects that it's inside a virtual machine (VM), and SamSam – the ransomware currently ravaging cities and businesses across the United States – requires its author to input an activation command before it will begin operations, effectively nullifying any attempts to study its activities outside of an active infection.

Protecting a business from all cyber threats is a bit like trying to reach the speed of light – the closer you get, the exponentially more resources you must throw at the task, but no amount of prevention can protect you from every possible threat. Since every business, from small business up to national governments, needs protection from cyber threats, several government and private agencies publish documents explaining "best practices" to help mitigate the threats companies face. The National Institute of Standards and Technology, an agency of the United States Department of Commerce, has released a document with recommendations for cybersecurity practices (Souppaya & Scarfone, 2013). Their list of 5 recommendations for threat mitigation include antivirus software on all endpoint devices and servers, intrusion prevention

systems, firewalls, content filtering/inspection, and application whitelisting. While this paper has discussed antivirus software in some detail already, the other tools listed above may require some further explanation. Network-based intrusion prevention systems (IPS) are in-line network systems which detect and halt unwanted network activity, allowing network administrators to have fine-grained control over packets on their network. This can allow a network admin to implement policies to stop 0-day threats before antivirus systems have had time to receive signature updates, decreasing threat vulnerability time. These systems are extremely effective at stopping network or email-based worms from spreading across a corporate network. Firewalls are well-known in popular culture, but just as frequently misunderstood. Simply put, a firewall restricts access into and out of a network's ports. This allows network administrators to enable only specific internet traffic and add restrictions specifically banning known threats from their network space. Content filtering/inspection is frequently done with email or web content, and can quarantine emails containing suspect attachments, or emails originating from questionable domains. Web filtering can also restrict what categories of websites network users have access to, which reduces the threat profile to known sites (although these may still be compromised by an attacker). Application whitelisting restricts what programs are allowed to be run on host computers, further limiting threat vectors to a known set of applications which can be closely monitored.

Along with policies to protect corporate networks from malware intrusion, the NIST also recognizes that incident response is just as critical to cyber security. The four major phases outlined in NIST SP 800-61 are Preparation, Detection & Analysis, Containment / Eradication /

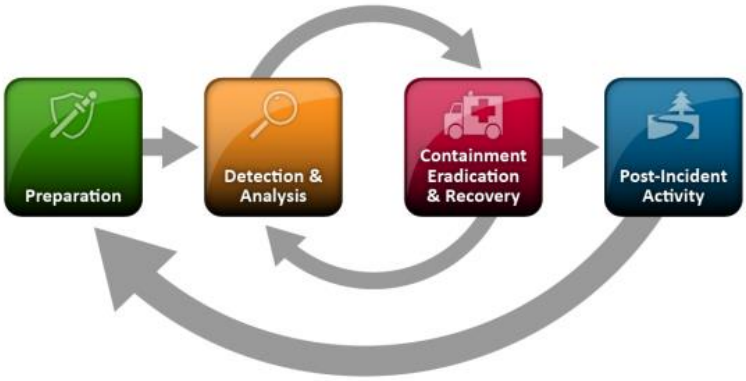

Figure 3:NIST Incident Response Life Cycle (Source: NIST)

Recovery, and Post-Incident Activity (Figure 3). Every organization would do well to follow these general guidelines and understand that even the best prevention policies will never be able to full protect a network from a successful attack and knowing how to detect and recover from an attack are invaluable components to a cyber security policy. While there can be no guarantee of safety from cybercrime, keeping software updated and implementing cyber security best practices can reduce your threat levels to acceptable margins which, when paired with cyber crime insurance, can help you feel confident that your business will be able to keep going tomorrow and the day after.

Works Cited

Arntz, P. (2018, December 14). *How threat actors are using SMB vulnerabilities*. Retrieved from Malwarebytes Labs: https://blog.malwarebytes.com/101/2018/12/how-threat-actors-are-using-smb-vulnerabilities/

Branscombe, M. (2019, Sepember 11). *What is fileless malware and how do you protect against it?* Retrieved from TechRepublic: https://www.techrepublic.com/article/what-is-fileless-malware-and-how-do-you-protect-against-it/

Brooks, C. (2019, June 16). *Talking Shop: How to Protect Your Small Business From Malware*. Retrieved from Business: https://www.business.com/articles/malware-small-business-prevention/

bsi. (n.d.). *Protecting your business from malware*. Retrieved from bsi Group: https://www.bsigroup.com/en-GB/Cyber-Security/Protecting-your-business-from-malware/

Dudley, R. (2019, August 27). *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*. Retrieved from ProPublica: https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

FBI. (2018, November 2). *The Morris Worm: 30 Years Since First Major Attack on the Internet*. Retrieved from FBI: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Graham, C. (2017, May 20). *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history*. Retrieved from The Telegraph: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

Hart, J. (2016, June 6). *10 years of cyber security; what the past decade has taught us*. Retrieved from Gemalto: https://blog.gemalto.com/security/2016/06/06/10-years-cyber-security-past-decade-taught-us/

Jacobs, M., & Satran, M. (2019, April 18). *Antimalware Scan Interface*. Retrieved from Microsoft Windows Dev Center: https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal

Joshi, N. (2018, December 21). *The anatomy of a cyber attack: Dissecting the science behind virtual crime*. Retrieved from Allerin: https://www.allerin.com/blog/the-anatomy-of-a-cyber-attack-dissecting-the-science-behind-virtual-crime

KnowBe4. (n.d.). *AIDS Trojan or PC Cyborg Ransomware*. Retrieved from KnowBe4: https://www.knowbe4.com/aids-trojan

Kujawa, A., Zamora, W., Umawing, J., Segura, J., Tsing, W., Arntz, P., & Boyd, C. (2019). *2019 State of Malware.* Retrieved from https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf

Malwarebytes. (n.d.). *Emotet*. Retrieved from Malwarebytes: https://www.malwarebytes.com/emotet/

Malwarebytes. (n.d.). *EternalBlue*. Retrieved from Malwarebytes Labs: https://blog.malwarebytes.com/glossary/eternalblue/

Marinho, T. (2018, August 30). *Ransomware encryption*. Retrieved from Medium: https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9

Souppaya, M., & Scarfone, K. (2013, July). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

Telegraph Foreign Authors. (2017, May 13). *Cyber attack crisis 'isn't over': Warning from researcher who found ransomware 'kill switch'*. Retrieved from Telegraph: https://www.telegraph.co.uk/technology/2017/05/13/cyber-attack-crisis-isnt-warning-researcher-found-ransomwarekill/