Defending the Front Lines:

Why the fight against malware is failing?

L. Taron Mattocks

East Carolina University

Defending the Virtual Front Lines: Why the fight against malware is failing

Technology pervades all aspects of our society. The statement appears fairly innocuous but we tend to stereotype technology to high level mainframes and enterprise structures. The reality of the statement is that many computers are no different from the consumer products bought in a local retail store. Many institutions buy large quantities of machines at wholesale prices. The problems that users experience at home, however, carry over to their office.

One of the most persistent threats facing computers are constant waves of attacks coming from attackers looking to pull pranks to professional thieves looking to exploit vulnerabilities for profit. A very serious but lucrative industry has been identity theft. Identity theft, willfully using an identity that belongs to someone else, has become more prevalent over the past two decades but it has always existed. Evidence of identity theft existed long before computers were invented. The most misused Social Security number came from a wallet promotion in 1938. More than 40,000 people used the number including twelve documented cases as late as 1977. (Social Security Administration, 2016) Technology has expanded the routes of misuse allowing easier access to someone who wished to steal identities. The poorly thought marketing ploy has now been replaced with a computer which can scavenge thousands of numbers illegally.

The purpose of this paper will examine the methods of attack and the main target audience. It will, additionally, examine whether our current methods of defense really work. The final goal of the paper will examine solutions which may be implemented. One of the most overlooked, by security experts, computer populations are desktop computers. The desktop population, not coincidentally, becomes the most targeted group amongst attackers. The ultimate goal is to change the way we examine our defense so that we can ultimately provide better methods of protection.

The University of North Carolina at Chapel Hill is a liberal arts institution located in Chapel Hill, North Carolina. The University, hereafter referred to as UNC-CH, is a leading research institution receiving research funding in excess of $750,000,000 annually since 2010. (University of North Carolina at Chapel Hill, 2016) UNC-CH, in fact, has never received less than $345,000,000 since 1999. The total funding reaches nearly $110 billion dollars solely dedicated to research ranks UNC-CH eleventh in the nation in terms of research amongst best colleges. (Bestcolleges.com, 2016) The tremendous amount of funding combined with its high academic and athletic profiles make UNC-CH a target amongst attackers.

UNC-CH, and other universities like it, become ideal target for attackers because they have several avenues to acquire targets. The student population, as of 2016, is at nearly 30,000 with an additional 12,000 plus staff and faculty. (The University of North Carolina at Chapel Hill, 2016) The University's long-noted reputation as a research school brings additional affiliations which makes UNC a one-stop shop of data. Universities also have fewer restrictions on their networks due to the nature of their business. The process of educating college students means a less restrictive network as universities generally try to give students every avenue to pursue their goals. The overall goal of education, however, comes at loosening of security standards. The combination of identities, personal info, and vast financial resources make UNC-CH a tempting target

The University denies approximately four billion connection attempts each year or approximately 86.3 million requests per week. (UNC ITS Security, 2016) 76% of these requests are stopped with border firewalls and never threaten UNC-CH's network. (Jones, 2016) These enterprise firewalls provide expert analysis against known threats and patterns. A common modern attack involves the use of private IP addresses in both the source and destination

addresses in the hope of finding a target without revealing one's location. The attack, known as spoofing, is easily configured into firewall logic. Private IP addresses, by definition, should map to an internal network address which can be appropriately routed. The private IP, therefore, cannot come from an external source.

Attacks such as private IP address spoofing are configured and rarely, if ever, require change. Closer examination of the remaining twenty million daily connection attempts requires a bit more analysis. 90% of the remaining traffic can be stopped, again, at the firewall level. Blacklisted IP ranges and connection attempts from known rogue geographical areas stop at the firewall. (Jones, 2016)

One of the great advantages of firewalls is the ability to configure known exploits and require little to no human maintenance interaction. The sampling of UNC-CH illustrates the effectiveness of firewalls as 97% of the attacks have been stopped. We now must examine the remaining connections to examine their effects on the most vulnerable machines in the network. The remaining connection attempts contain a mixture of computer attacks and legitimate network traffic. Universities, as previously mentioned, already have a lax structure in the mission of education. The natural inclination would allow desktop antivirus programs to protect workstations but this may be one of the massive mistakes that allow attackers access to these valuable workstations.

Computer connections come in many forms. An ideal attack would use a single method of attack to compromise multiple accounts or machines. One of the most common types of attack is the familiar phishing scam. A phishing scam is an email that poses as a legitimate email. The email usually contains a link to a fraudulent website that emulates a legitimate site or downloads malicious software onto a user's machine.

Early phishing attempts usually contain easily detectable telltale signs of fraud. A sample message includes message such as the following:

Date: May 23, 2016 11:17 AM
Subject: Your Urgent Attention is Needed
From: THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL
Welcome to Your THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

We noticed a login attempt to your UNIVERSITY of NORTH CAROLINA at CHAPEL HILL account from an unrecognized device on Monday, 23 May 2016
As part of our Security Agreement we have place your account on "Limitation".

Please follow the link below to keep your UNIVERSITY of NORTH CAROLINA at CHAPEL HILL account safe:

[REDACTED]

Thanks for taking these additional steps to keep your account safe.

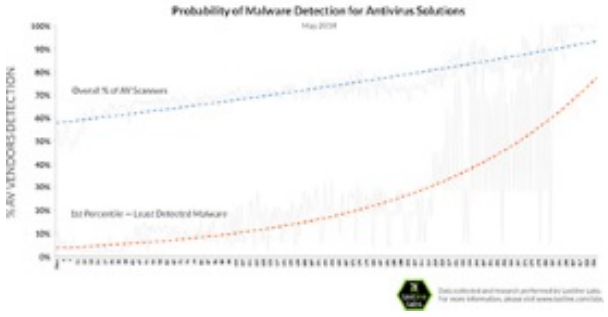
(UNC Information Technology Services, 2016)

The email message contains grammatical and spelling errors which allow a trained eye to easily spot and stop these threats. Attackers, however, have countered with more convincing emails. Recent emails have come with greatly improved language, real (though spoofed) campus users, and even official university logos. The cat and mouse game will undoubtedly continue but we one of the reasons that phishing scams have remained relevant because an uneducated user will eventually click on a fraudulent website and expose themselves to malware.

The job of workstation protection now falls to antivirus software. Antivirus software provides real-time protection at a local level based on defined signatures. The defined antivirus signatures are usually updated regularly in an attempt to keep up with new threats and variants of known threats. When a threatening file is discovered, it is immediately deleted from the system

or quarantined. Quarantined files are isolated such that they cannot interrupt other processes in the machine.

The process appears foolproof on the surface but the effectiveness of various antivirus products has been called into question. Recent studies have revealed that antivirus software fails miserably. According to 2014 studies performed by Lastline Labs, “most of the newly detected malware went undetected by nearly half of the antivirus vendors”. (Wang, 2014) The news worsens as “only 51 percent of the antivirus scanners detected the malware samples found in the past year on the first day of the study”. (Wang, 2014) Some of the tested malware never discovered some of the more elusive malware. The following graph shows the probability of malware detection over a two-month period.



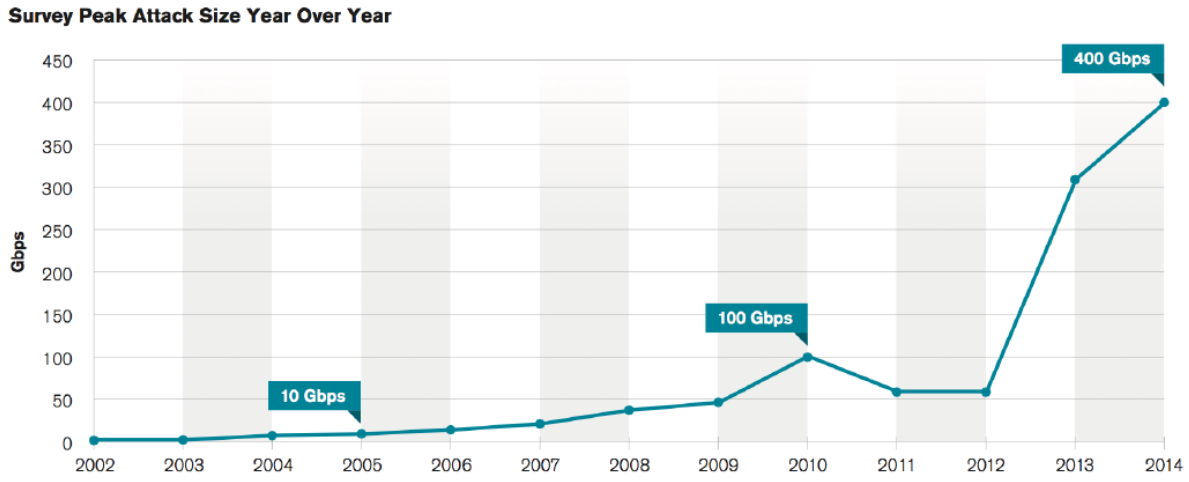
(Wang, 2014)

The surprising news vastly differed from the advertisements which promoted full system protection. The studied forced antivirus companies to admit that there is no foolproof method. Symantec’s startling admission in 2014 that “anti-virus products stop only 45 percent of the cyberattacks today” (Reah, 2014) capped a long known fact acknowledged previously by programmers and industry standard makers alike; stopping all malware is not realistic. Malware threats will continue to outpace their defense. Antivirus software has gone from a “stop all the bad things” mentality to a best effort model that, in part, concedes control to the attackers. One of the problems with malware is the continual transmogrification of the malware itself. Early virus creators sought to accomplish a goal and normally built code without thought to malicious

or fraudulent behaviors. It was cool to discover a bug and exploit it. The present-day malware community has an overwhelming desire for either profit or destruction.

The distributed denial of service or DDoS attack is one of the common attack modules that scares many network distributors. The typical DDoS attack involves multiple machines (multiple machines may rank into the thousands) flooding a target with more network traffic than it is capable of servicing. The effect of the attack can range from annoyance to complete business shutdown.

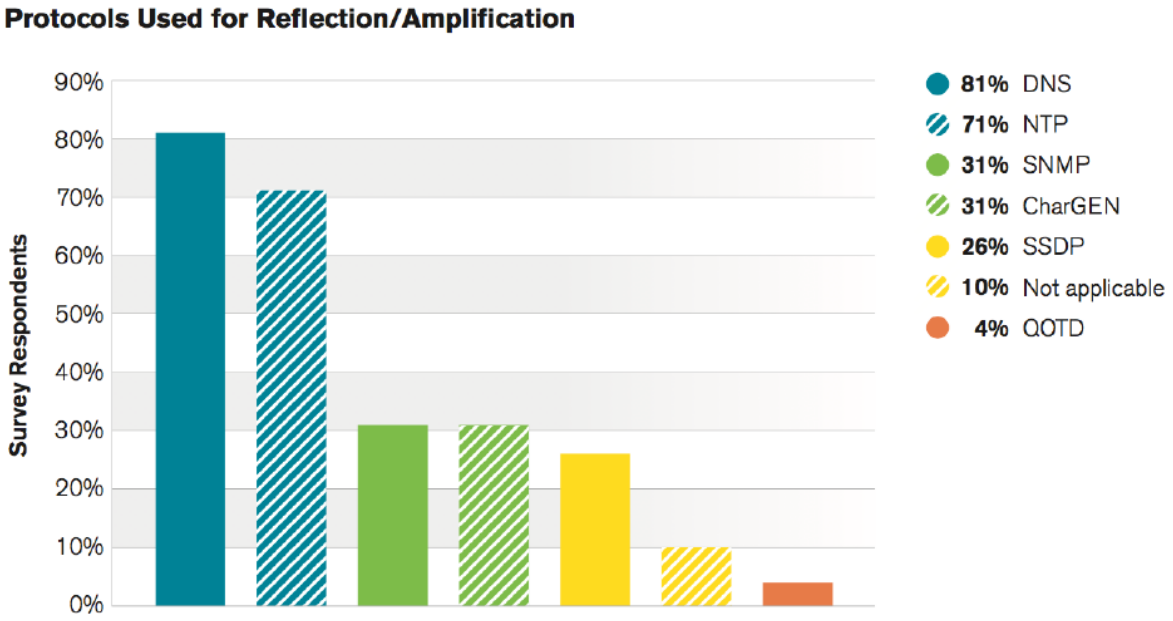
The Microelectronics Center of North Carolina, also known as MCNC, is responsible for operating the North Carolina Residential Educational Network (also known as NCREN) for the networking infrastructure of many North Carolina colleges and universities. (Bizjournals.com, 2007) MCNC is a central hub of networking and thus a target of many denial of service attempts. The following graph shows the attack attempts and the changes in target size.



(Beal, 2015)

The change in target size coincides with the explosive growth of networks from the early days of widespread broadband networks in 2002 to the modern fiber optics networks which

boasts nearly unthinkable transmission rates. The above graph shows the rising popularity of a denial of service attack but these attacks are not of a single signature. The point of an attack is to occupy a network service to the point of shutting it down. The world of networking technology has many avenues that can be attacked. The following illustrates the most common network protocols used.

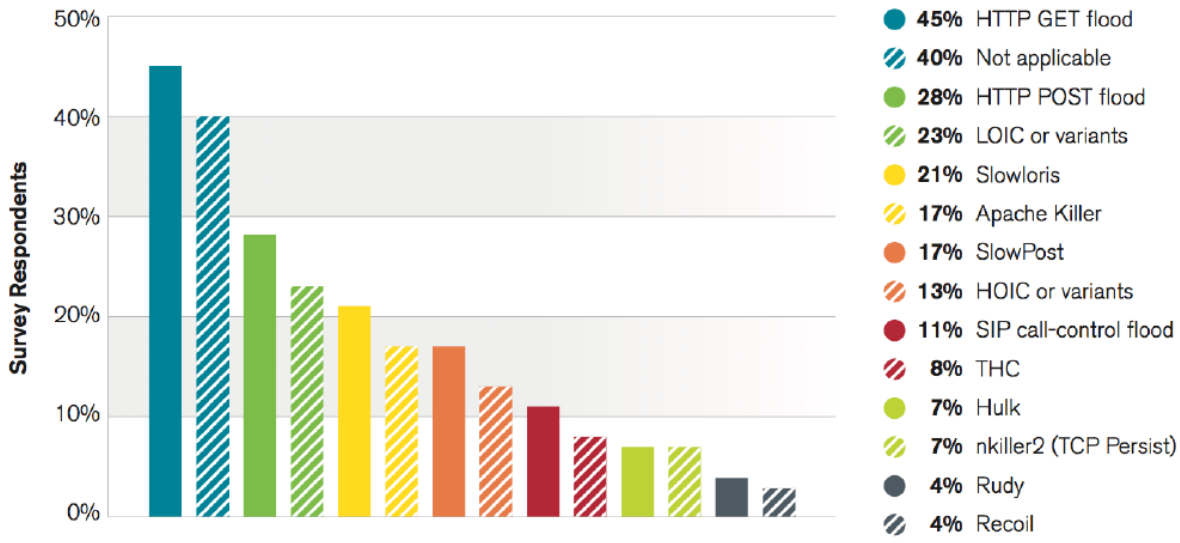


(Beal, 2015)

DNS has long been a popular target for attackers as the nature of the service makes it susceptible to attack. The real surprise comes with lesser known protocols such as Simple Service Delivery Protocol (SSDP) and Network Time Protocol (NTP). The ability to adapt to these protocols shows the versatility of DoS attacks and another headache for network analysts.

Network Analysts must deal with each threat as it attempts to penetrate their network. The versatility of denial of service attacks show just how much trouble comes from a single type of malware. Reports estimate that nearly one million new threats are released daily. (CNN

Money, 2015). The following graph shows various attack strategies used to start a denial of service attack. The requests differ from protocol exploits to specific exploit software.



(Beal, 2015)

Computer technology continues to amaze as we break new ground daily. No matter the advances that come with technology, it is ultimately computer code. Computer code, ultimately, has weaknesses. All computer software eventually has a weakness exposed and Symantec was no different. The Google Project Zero team found that the desktop protector had multiple vulnerabilities and endangered the operating system through poor coding techniques. (Omandy, 2016)

Rumors of Symantec vulnerabilities have existed for years. The thinking of many technicians and customers alike was that Symantec had to work. The fear of attacking the last line of defense was too much to consider. If Symantec failed, the Internet would become a much more dangerous place as it was the last line of defense. The rumors turned into reality as multiple weaknesses were uncovered. Many of the weaknesses revolve around unpackers which help with size but put the machine and software kernel at great risk. (Omandy, 2016)

Symantec developers also used poor techniques allowing the code to run unchecked through the system. Symantec further complicated this problem as the same engine was used across multiple software platforms. (Omandy, 2016) Symantec's reckless cost-cutting move now endangers customer and enterprise products alike. Patches have since been instituted but the secret has been revealed. No amount of security will overcome the human factor of programming. Humans have shown themselves as the weak link in technology.

All of the problems presented in this paper can dishearten even the most ardent computer enthusiasts. Solutions do exist despite the dire reports. The first addresses the weak link of the human/technology interaction. An amazing number of virus victims become suffer due to simple ignorance. Education does not resolve all problems but an educated employee base will reduce the likelihood of falling victim to simple attacks and phishing scams. An estimated 800,000 phishing links are clicked per year. Educating the everyday user will help them recognize basic scams. The step may appear to be a small one but the philosophy behind education will have positive long-term effects.

Antivirus software, while obviously less effective, is one of the best front-line methods from complete attacker anarchy. Alternatives protection methods have not gained traction in the community at large or involve ideas that ultimately undermine the technological progress that we have achieved. Current antivirus mostly uses signature-based detection methods for detection. Alternatives may involve heuristic scanning, cloud scanning, or even behavioral detection.

Behavioral detection involves observing "how a program executes rather than merely its execution". (Zeltser, 2016) A signature detection will depend on an exact signature. We have seen the number of variants that come with a simple denial of service attack. Behavioral analysis has the potential to help diagnose the pattern of the attacks rather than the exact signature file. A

great advantage is the fact that a piece of malware does not need to be explicitly discovered. It can now be detected based on what it is doing.

One major disadvantage is the idea of legitimate traffic being caught. The initial problems of legitimate traffic can cause business interruption but work between customers and administrators can quickly mitigate these issues with proper configuration. Educational realms would need to carefully configure their firewalls though as they already have more relaxed rules than normal businesses. Finding balance would be the first priority of a particular university setting.

The perimeter firewalls at UNC-CH have done the best job of all of the solutions. 98% of attempted attacks. The desktop percentages (statistics redacted due to security concerns) require more effort as the threats that reach desktops have surprisingly little resistance. The antivirus software which acts as the last line of defense has its own problems to worry about.

UNC-CH is an example of one institution that must deal with the balance of allowing valid data for academic purposes versus stopping malevolent attacks. UNC-CH must take special care to ensure that, as a high-value target, data is secured in every manner possible. The threat of a Sony-level compromise must be taken seriously every day as the University, like all targets, remains only an exploited vulnerability away from chaos.

The illusion of security for UNC-CH shattered as the university revealed a massive security breach. An investigation found a research server for the Carolina Mammography Registry had been compromised. The initial thoughts were promising but the full extent of the damage would reveal much more damage. The machine was found to have been compromised for up to two years. (Charette, 2010) The anti-virus solution in place as the last line of defense experienced a complete and catastrophic failure. User training appears to have been non-existent

as the public learned that a university researcher had administered the machine without consulting a member of the IT department. The university research was later sanctioned by university administration for her lack of oversight. A long battle would later ensue to determine who had the responsibility for the data culminating in the demotion of the researcher. After contentious court battles and negotiations, the sanctions were overturned with no ultimate penalty.

The compromise was followed by a series of smaller breaches which, again, showed how easily the signature-based programs could be compromised. A larger issue also exists. Antivirus software was thought to be completely reliable despite years of evidence to the contrary. A server that housed sensitive information saw very little oversight other than installed detection.

Attackers only care to obtain sensitive information. We have examples from all walks of life that an attack. Neither academic institutions or large corporations have immunity from a remote invader wishing to illegally obtain information. The examples, however, continue to accumulate as more attacks are reported daily. The common thread of these attacks is the idea that poor security standards can be overcome with an abundance of automated tools. One of the key items missing in each case is sufficient user training on the best way to remain secure.

The Internet presents the best and worst that ingenuity can offer. We have seen tremendous advances in all fields. Mankind has surely benefitted from the advances of being able to communicate ideas on a global scale instead of the localized methods which have dominated civilization. Our advances, however, cannot overshadow the fact that this new global communication is still in its infancy and we do not know exactly what will happen from here.

The world of technology, however, will continue to grow as we have even more devices set to join the Internet. Internet Protocol version 6 promises more network addresses than we can

possibly use and internet speeds continue to rise at a breakneck pace. Items such landline telephones illustrate this growth as we have transitioned from the POTS (Plain Old Telephone System) to data networks completely dependent upon Ethernet networks. Security must take priority so that the progress that we have made is not halted under the crush of malicious attacks. The phone example cannot tolerate denial of service attacks. The lack of basic communication methods could have calamitous effects from a simple occurrence. Security will, therefore, continue to take top priority. The effective use of firewalls, reduced dependency on desktop antivirus software, and increased training will help raise awareness and mitigate the effects. No single threat eliminator exists but a change in philosophy will give us our best chance to defend ourselves and continue to ultimately advance technology.

Bibliography

Beal, C. (2015). *Introduction to DDoS Attacks.* Research Triangle Park.

Bestcolleges.com. (2016, July 1). *Highest Research & Development Funding*. Retrieved from Bestcolleges.com: http://www.bestcolleges.com/features/colleges-with-highest-research-and-development-expenditures/

Bizjournals.com. (2007, February 23). *MCNC chief executive resigns*. Retrieved from Bizjournals.com: http://www.bizjournals.com/triangle/stories/2007/02/19/daily46.html

Charette, R. (2010, October 26). *Who Should Be Held Accountable For an IT Security Breach?* Retrieved from IEEE Spectrum: http://spectrum.ieee.org/riskfactor/computing/it/who-should-be-held-accountable-for-an-it-security-breach

CNN Money. (2015, May 14). *Nearly 1 million new malware threats released every day*. Retrieved from CNN Money: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

Jones, T. (2016, July 13). Information Security Specialist. (T. Mattocks, Interviewer)

Omandy, T. (2016, June 29). *How to Compromise the Enterprise Endpoint*. Retrieved from Google Project Zero: http://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html

Reah. (2014, May 6). *Symantec admits anti-virus software is no longer effective at stopping virus attacks*. Retrieved from dottech.org: https://dottech.org/157355/symantec-admits-anti-virus-software-is-no-longer-effective-at-stoping-virus-attacks/

Social Security Administration. (2016, July 1). *Social Security Cards Issued by Woolworth*. Retrieved from Social Security Administration: https://www.ssa.gov/history/ssn/misused.html

The University of North Carolina at Chapel Hill. (2016, July 1). *Facts and Figures*. Retrieved from The University of North Carolina at Chapel Hill: http://uncnews.unc.edu/facts-about-carolina/facts-figures/

UNC Information Technology Services. (2016, May 23). *UNC Phishing Alerts*. Retrieved from UNC Information Technology Services: http://its.unc.edu/phish-alert/urgent-attention-needed/

UNC ITS Security. (2016, July 1). Security Statistics. Chapel Hill, North Carolina, United States of America.

University of North Carolina at Chapel Hill. (2016, July 1). *Research Funding*. Retrieved from UNC Research: http://research.unc.edu/about/facts-rankings/research-funding/

Wang, A. (2014, June 11). *Is Antivirus Software Ineffective?* Retrieved from PCmag.com: http://securitywatch.pcmag.com/security/323973-is-antivirus-software-ineffective

Zeltser, L. (2016, July 1). *How antivirus software works: Virus detection techniques*. Retrieved from TechTarget: http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques