Exploits of Yesteryear Are Never Truly Gone

GIAC (GCIA) Gold Certification

Author: Marsha Miller, mmiller@mastersprogram.sans.edu
Advisor: Chris Walker
Accepted: 12/12/2015

Abstract

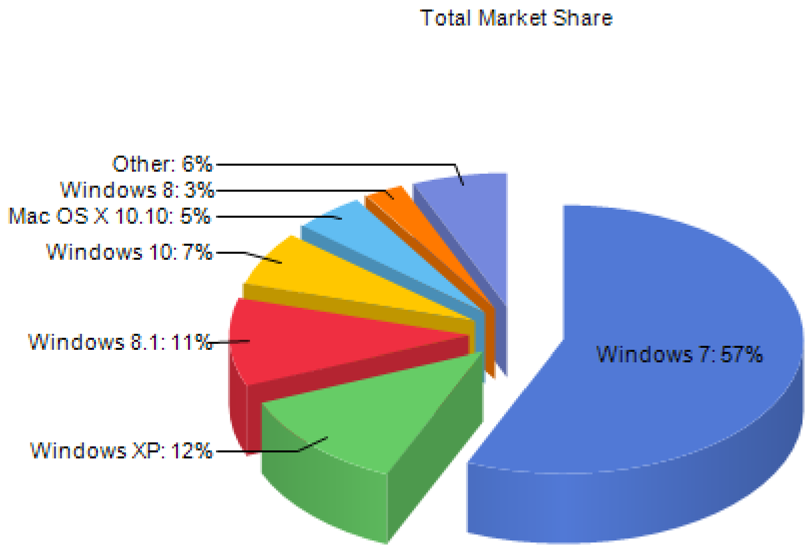
Attacks that once garnered so much attention years ago are rarely remembered today. Worms and viruses such as Sasser and Melissa caused pandemonium with far reaching consequences. But are these exploits dead and gone? Although mainly forgotten, malware that gained prominence more than 10 years ago still circulates in today's traffic, looking for unsuspecting victims. Owners still use outdated software, unable or unwilling to upgrade, perhaps containing unpatched vulnerabilities. At other times, a manufacturer may forget and change a setting, causing the vulnerability to reappear, even in a later version of the software. Using packet captures and open-source IDS set up to detect traffic with signatures of older attacks, this paper will explore the lingering existence of these exploits and the systems that may still be vulnerable. Then it will propose ways to protect systems and mitigate the vulnerabilities.

1. Introduction

Once, mentioning the name of certain viruses and worms put fear into the hearts of millions. Blaster, Sasser, and even ILoveYou, a seemingly innocuous phrase used every day, became household names that led to loss of money and productivity. Like an infection of the body that is resistant to antibiotics, some viruses just won't die. But unlike its medical counterpart, viruses in the digital world are different.

Older viruses can persist long after the initial wave of community response. Largely, this is due to poor patching practices and maintenance of older operating systems and software applications. Often, software is written for a particular platform and support is eventually discontinued as newer systems enter the market. For businesses, older systems may need to be maintained for periods long after the manufacturer sunset date, sometimes determined by regulations such as Sarbanes-Oxley (SOX). When software patching is discontinued by a manufacturer, future vulnerabilities are left unchecked. If businesses do not have the staff to update the vulnerable software or make the necessary compensating modifications, the risk of compromise may not be addressed. For various reasons, home users may choose not to pay for the next version released and therefore continue using outdated and possibly vulnerable software. After all, not everyone can afford the latest and greatest.

According to Net Market Share, XP still has a decent presence at 12%. Older operating system versions such as Windows 98, Windows 95, Windows NT, and Solaris 8 also still exist in some areas, maintained for various personal and professional reasons. A recent article surprised many when it revealed a French airport was forced to temporarily close due to a glitch on a system still using Windows 3.1 (Longeray, 2015).



(Net Market Share, September 2015)

While there is nothing wrong with maintaining older systems for legitimate business and professional reasons, it is important to remember the vulnerabilities involved. Patches and support are no longer available for these systems, so any new vulnerabilities will not be addressed by the manufacturer. Furthermore, patches already available may remain unapplied to these older systems for various reasons.

2. Background on Viruses and Worms

Although many viruses and worms have been created to date, both intentional and unintentional, some gained notoriety simply for being more prolific or damaging than others. Klez, SQL Slammer, Conficker, MyDoom, Blaster, Sasser, Nimda, Melissa, ILoveYou, and Storm fall into this category.

Virus/Worm	**Year of Prominence**
Melissa	1999

ILoveYou	2000
Code Red, Nimda, Klez	2001
SQL Slammer, Blaster, Sobig	2003
MyDoom, Sasser	2004
Storm	2007
Conficker	2008

MyDoom, Klez, Melissa, and Sobig were mainly distributed via email taking advantage of software features in email programs such as Outlook. They relied on address lists to spread, but were mainly intended for notoriety. Storm, which also spread via email using attachments to infect the PC, took self-replicating malware to a new level. While previous worms were written to garner fame, the inventors of Storm had a more devious intention. Although not the first to do so, infected computers became zombies that belonged to a botnet which were used to send spam. Unfortunately for security professionals, it was also difficult to contain due to the stealthy design which allowed it to persist (Schneider, 2007).

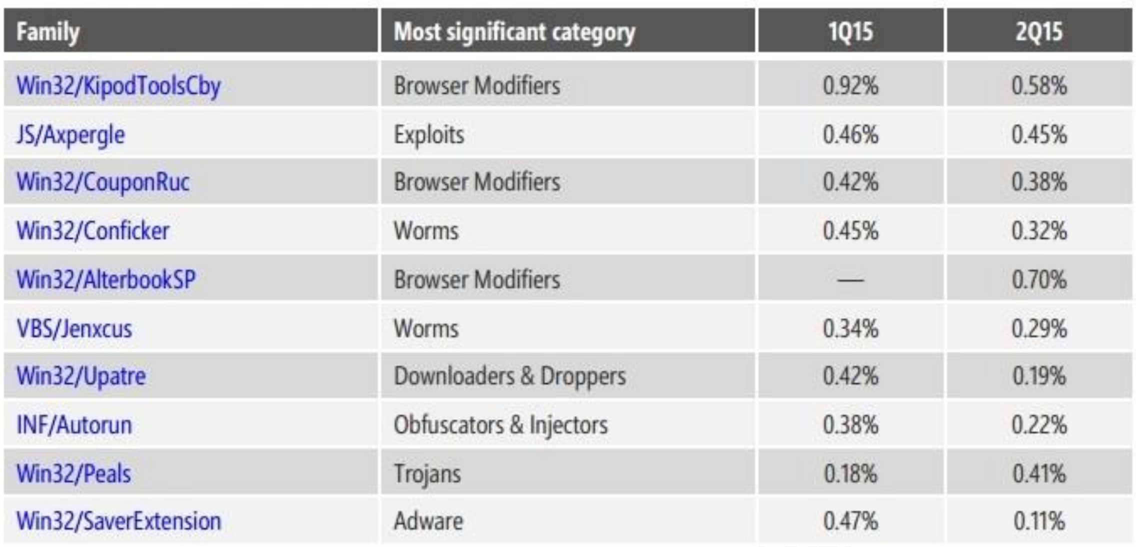
Buffer overflows are a common form of attack that can cause system instability or even crash the kernel. Blaster, Sasser and SQL Slammer all fall under this category. Unlike other viruses that spread through email, Sasser and Blaster targeted well-known RPC ports. Affecting the Local Security Authority Subsystem Service (LSASS), Sasser scanned IP ranges for TCP 445 looking for target victims (MITRE, 2003). Blaster's main target was the DCOM RPC Interface using TCP port 445 as well as TCP 135 and 139 (Symantec, 2003). Using another well-known port but with a different protocol, SQL Slammer used UDP port 1434 for propagation and quickly overwhelmed many systems that use SQL, including root servers.

Code Red spread utilizing a vulnerability in Microsoft IIS and actively looked for other vulnerable web servers by scanning on TCP port 80 (Danyliw & Householder, 2001). Nimda was rare in that it used several techniques to spread. Email, network shares, compromised web sites and IIS were all methods employed. This clever technique still used by some malware increased the ways in which it could spread. It also meant that administrators and security professionals had to employ more than one method of defense.

While some worms may no longer pose a serious threat due to updated operating systems and patching efforts, a vulnerable computer may still risk infection. Worms that have been repurposed can still pose a threat.

Although Sobig deactivated in September of 2003, and others may be less effective due to upgrades in software, old attacks can be made relevant once again. Sobig and others continue to spread even after the command and control systems or payloads are deactivated. Newer versions of the virus are released, or users make the mistake of opening unsafe attachments or simply not patching the vulnerable systems. MyDoom made a return several years after the initial attack (Zetter, 2009). There may also be a more recent variant that affects Windows 7 that is currently being investigated by Symantec (Xiao, 2015). This illustrates how these older attacks can reemerge years later.

The Conficker Working Group was formed by a coalition of security professionals to tackle the difficult job of defeating this incessant worm ("Conficker Working Group," 2011). Despite the fact that the command and control structure for Conficker has since been dismantled, it still remains a threat to vulnerable systems. Still appearing on the top ten domain-joined list of the Microsoft Security Intelligence Report, it is spread using various methods including removable media drives, weak passwords and the MS08-067 vulnerability. (*Microsoft Security Intelligence Report*, 2015, p. 97)



Family	Most significant category	1Q15	2Q15
Win32/KipodToolsCby	Browser Modifiers	0.92%	0.58%
JS/Axpergle	Exploits	0.46%	0.45%
Win32/CouponRuc	Browser Modifiers	0.42%	0.38%
Win32/Conficker	Worms	0.45%	0.32%
Win32/AlterbookSP	Browser Modifiers	—	0.70%
VBS/Jenxcus	Worms	0.34%	0.29%
Win32/Upatre	Downloaders & Droppers	0.42%	0.19%
INF/Autorun	Obfuscators & Injectors	0.38%	0.22%
Win32/Peals	Trojans	0.18%	0.41%
Win32/SaverExtension	Adware	0.47%	0.11%

(Microsoft Security Intelligence Report, 2015, p. 95)

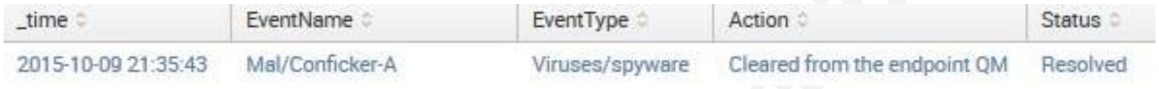
To be fair, Linux systems are not completely immune. From non-resident viruses that infect ELF format files to those that target OpenOffice, zip files and social media, there are versions of malware specifically crafted for the Linux operating system as well as cross-platform versions that include it. ("Meet Linux Viruses," 2012).

Virus/Worm	**Year of Prominence**
Bliss	1997
Vit (cross platform)	1999
Virus.Linux.Winter.341	2000
Ramen, Zipworm, Satyr	2001
OSF.8759	2002
Alaeda, Rike	2003
Kaiten	2006
Badbunny	2007
Koobface	2010

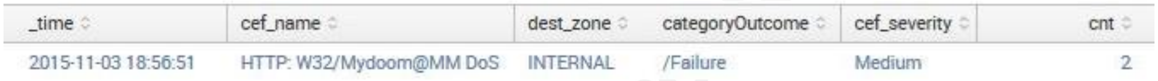
("Meet Linux Viruses," 2012)

3. Malware Detections

Since there are many legacy systems still in use, not having the proper protections in place can be detrimental. For instance, these two notifications show that Conficker and MyDoom are both still present and active, and would have compromised unprotected systems.



_time	EventName	EventType	Action	Status
2015-10-09 21:35:43	Mal/Conficker-A	Viruses/spyware	Cleared from the endpoint QM	Resolved



_time	cef_name	dest_zone	categoryOutcome	cef_severity	cnt
2015-11-03 18:56:51	HTTP: W32/Mydoom@MM DoS	INTERNAL	/Failure	Medium	2

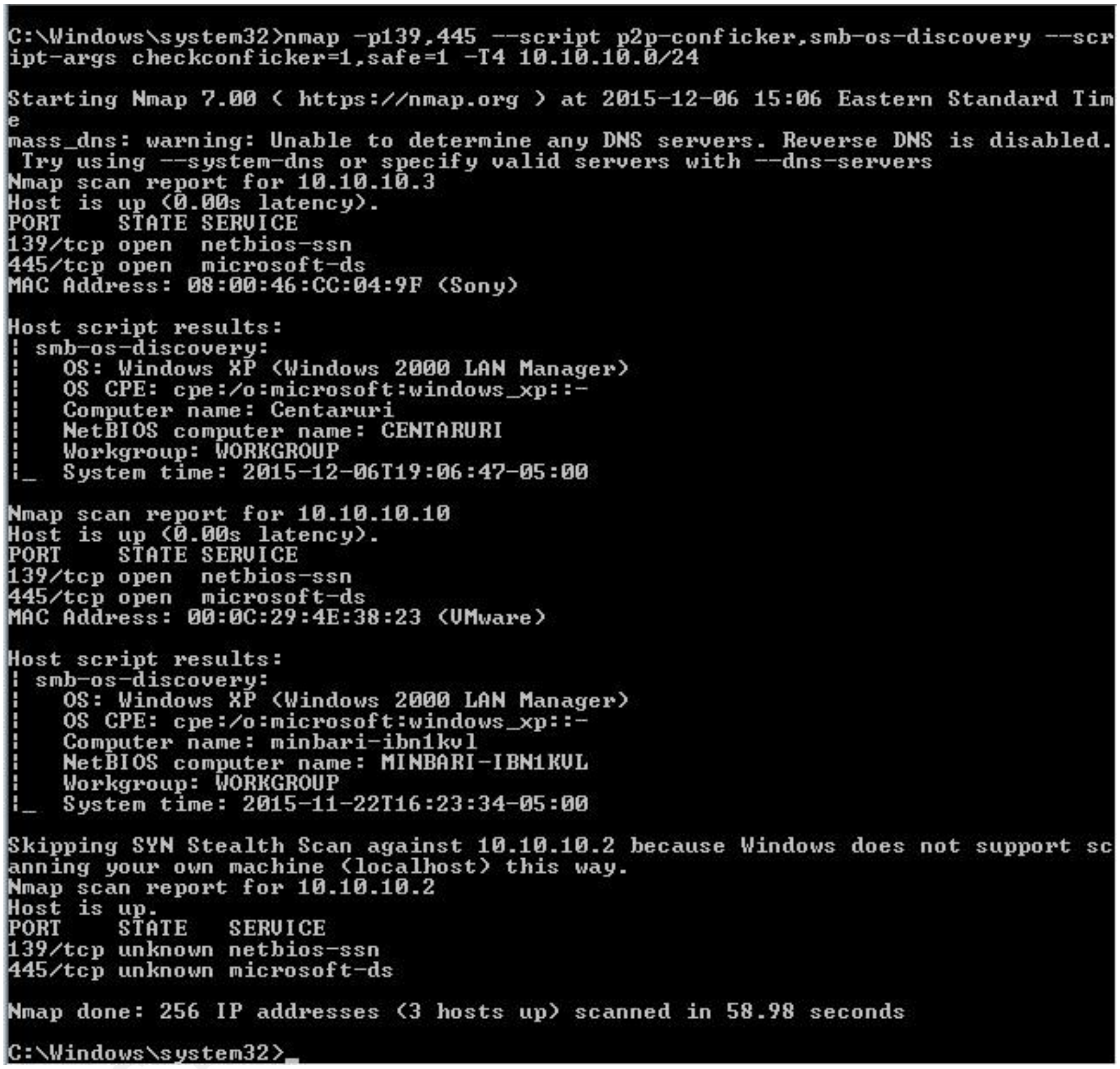
In November of 2015, iPower Technologies discovered that several police body cameras manufactured by Martel Electronics were shipped with the Conficker worm included (*Martel Police Body Camera Virus Found Embedded into Camera*, 2015). Once the camera was connected to a computer via USB, anti-malware solutions detected and quarantined the virus. Although the cameras themselves were not affected, they are able to spread the virus to vulnerable systems. To date, no reports have been released of police departments or other government agencies currently using the cameras along with vulnerable systems that may have become infected from the connections.

Intrusion Detection Systems (IDS) such as the freeware Snort software can be used to detect different types of traffic, including these older attacks, by using signatures. Older attacks already have signatures written and installed in the rules file provided by Snort as a separate download; however this does not ensure detection. The IDS can be set up as a passive sensor or an inline sensor. Typically, it is recommended to set it up inside the firewall or router so that the traffic is already filtered, decreasing the load on the sensor.

There are several websites dedicated to providing packet captures (pcap) to the public for research purposes. By setting up a Snort sensor and loading a pcap file, it can be read by Snort which will trigger the appropriate signature to fire. In this manner, items can be researched and additional signatures may be developed.

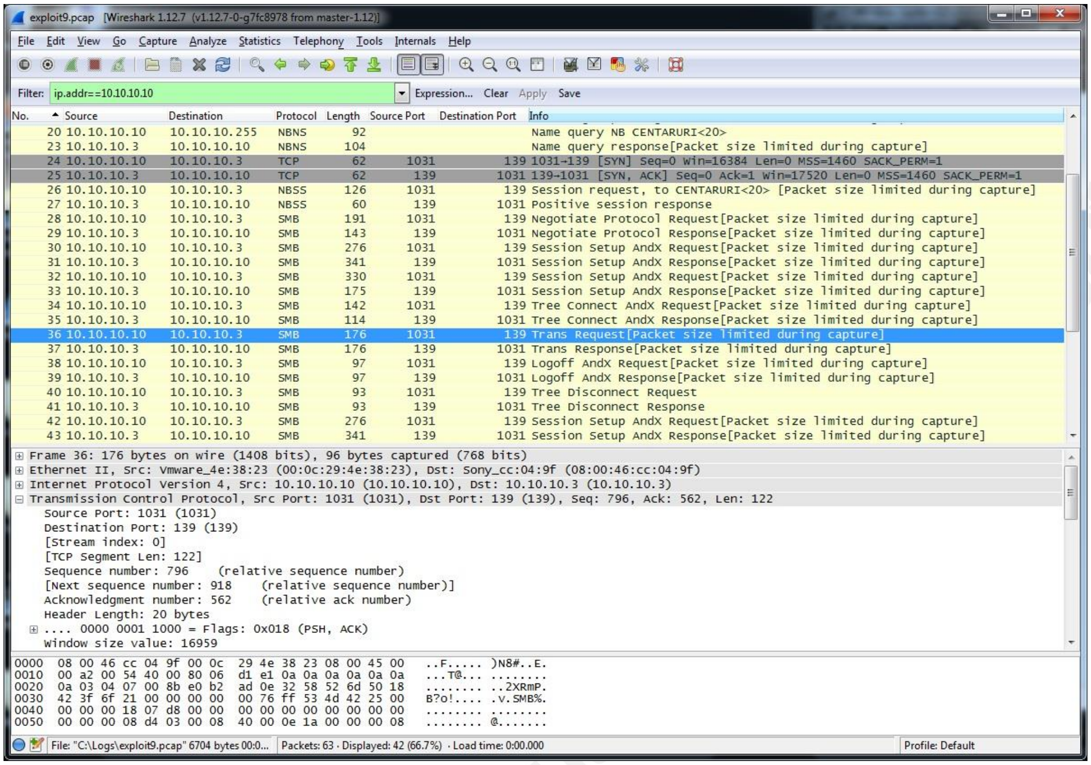
As a test environment, a Windows 7 computer was used to monitor the interaction between two XP machines using Snort and tcpdump. One XP instance was created as a virtual machine (VM) on the Windows 7 host and the second was installed on a physical laptop. The devices were connected to a hub to allow all traffic to be visible to every device. Conficker binaries were transferred to the XP VM and activated. The traffic was monitored by Snort and also captured by tcpdump.

The Nmap program has some scripts that help detect whether or not a computer is vulnerable to Conficker by determining if TCP ports 139 and 445 are open. It is interesting to note that the malware renamed the infected computer with the addition of a hyphen and random characters.



```
C:\Windows\system32>nmap -p139,445 --script p2p-conficker,smb-os-discovery --scr
ipt-args checkconficker=1,safe=1 -T4 10.10.10.0/24

Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-06 15:06 Eastern Standard Tim
e
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.10.3
Host is up (0.00s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:46:CC:04:9F (Sony)

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: Centaruri
|   NetBIOS computer name: CENTARURI
|   Workgroup: WORKGROUP
|_  System time: 2015-12-06T19:06:47-05:00

Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:4E:38:23 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: minbari-ibn1kvl
|   NetBIOS computer name: MINBARI-IBN1KVL
|   Workgroup: WORKGROUP
|_  System time: 2015-11-22T16:23:34-05:00

Skipping SYN Stealth Scan against 10.10.10.2 because Windows does not support sc
anning your own machine (localhost) this way.
Nmap scan report for 10.10.10.2
Host is up.
PORT    STATE   SERVICE
139/tcp unknown netbios-ssn
445/tcp unknown microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 58.98 seconds

C:\Windows\system32>_
```

This Wireshark capture shows traffic between the two Windows XP devices. The infected device began searching for other hosts to infect.


exploit9.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.addr==10.10.10.10

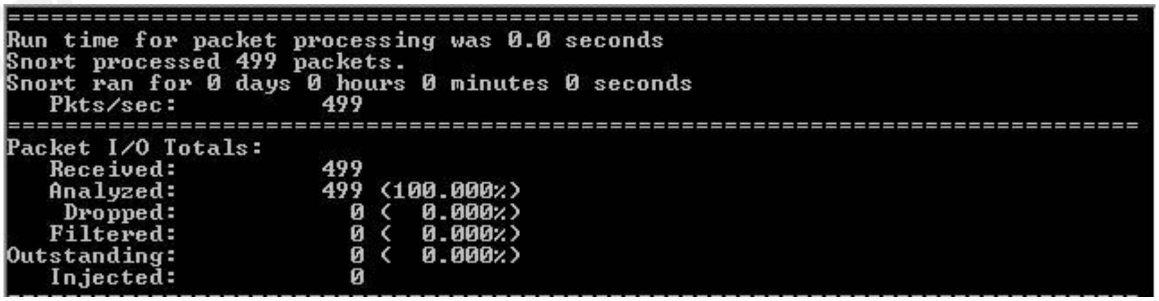
```
No.  Source       Destination   Protocol Length Source Port Destination Port Info
  20 10.10.10.10  10.10.10.255  NBNS      92                      Name query NB CENTARURI<20>
  23 10.10.10.3   10.10.10.10   NBNS     104                      Name query response[Packet size limited during capture]
  24 10.10.10.10  10.10.10.3    TCP       62    1031        139 1031→139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
  25 10.10.10.3   10.10.10.10   TCP       62     139       1031 139→1031 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PERM=1
  26 10.10.10.10  10.10.10.3    NBSS     126    1031        139 Session request, to CENTARURI<20> [Packet size limited during capture]
  27 10.10.10.3   10.10.10.10   NBSS      60     139       1031 Positive session response
  28 10.10.10.10  10.10.10.3    SMB      191    1031        139 Negotiate Protocol Request[Packet size limited during capture]
  29 10.10.10.3   10.10.10.10   SMB      143     139       1031 Negotiate Protocol Response[Packet size limited during capture]
  30 10.10.10.10  10.10.10.3    SMB      276    1031        139 Session Setup AndX Request[Packet size limited during capture]
  31 10.10.10.3   10.10.10.10   SMB      341     139       1031 Session Setup AndX Response[Packet size limited during capture]
  32 10.10.10.10  10.10.10.3    SMB      330    1031        139 Session Setup AndX Request[Packet size limited during capture]
  33 10.10.10.3   10.10.10.10   SMB      175     139       1031 Session Setup AndX Response[Packet size limited during capture]
  34 10.10.10.10  10.10.10.3    SMB      142    1031        139 Tree Connect AndX Request[Packet size limited during capture]
  35 10.10.10.3   10.10.10.10   SMB      114     139       1031 Tree Connect AndX Response[Packet size limited during capture]
  36 10.10.10.10  10.10.10.3    SMB      176    1031        139 Trans Request[Packet size limited during capture]
  37 10.10.10.3   10.10.10.10   SMB      176     139       1031 Trans Response[Packet size limited during capture]
  38 10.10.10.10  10.10.10.3    SMB       97    1031        139 Logoff AndX Request[Packet size limited during capture]
  39 10.10.10.3   10.10.10.10   SMB       97     139       1031 Logoff AndX Response[Packet size limited during capture]
  40 10.10.10.10  10.10.10.3    SMB       93    1031        139 Tree Disconnect Request
  41 10.10.10.3   10.10.10.10   SMB       93     139       1031 Tree Disconnect Response
  42 10.10.10.10  10.10.10.3    SMB      276    1031        139 Session Setup AndX Request[Packet size limited during capture]
  43 10.10.10.3   10.10.10.10   SMB      341     139       1031 Session Setup AndX Response[Packet size limited during capture]
```

```
⊞ Frame 36: 176 bytes on wire (1408 bits), 96 bytes captured (768 bits)
⊞ Ethernet II, Src: Vmware_4e:38:23 (00:0c:29:4e:38:23), Dst: Sony_cc:04:9f (08:00:46:cc:04:9f)
⊞ Internet Protocol Version 4, Src: 10.10.10.10 (10.10.10.10), Dst: 10.10.10.3 (10.10.10.3)
⊟ Transmission Control Protocol, Src Port: 1031 (1031), Dst Port: 139 (139), Seq: 796, Ack: 562, Len: 122
    Source Port: 1031 (1031)
    Destination Port: 139 (139)
    [Stream index: 0]
    [TCP Segment Len: 122]
    Sequence number: 796    (relative sequence number)
    [Next sequence number: 918    (relative sequence number)]
    Acknowledgment number: 562    (relative ack number)
    Header Length: 20 bytes
  ⊞ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 16959
```

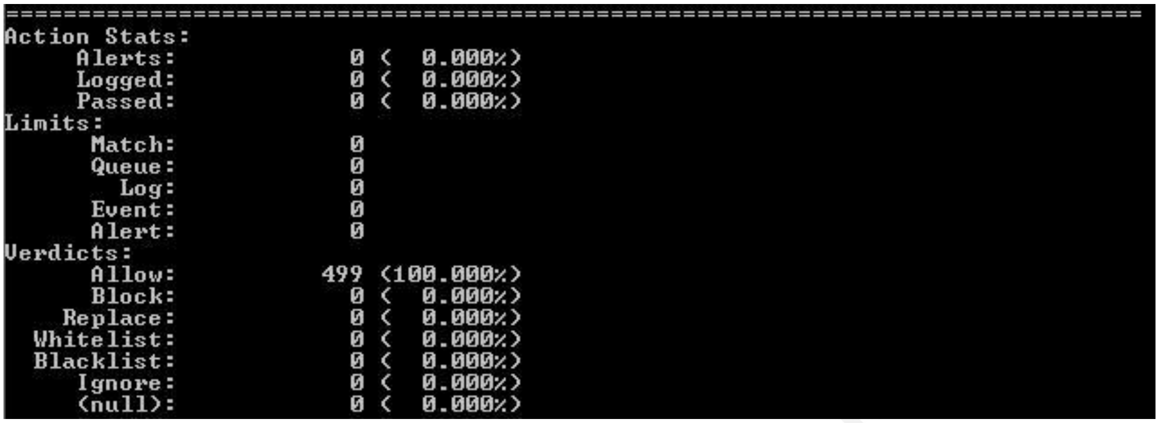
```
0000   08 00 46 cc 04 9f 00 0c  29 4e 38 23 08 00 45 00   ..F..... )N8#..E.
0010   00 a2 00 54 40 00 80 06  d1 e1 0a 0a 0a 0a 0a 0a   ...T@... ........
0020   0a 03 04 07 00 8b e0 b2  ad 0e 32 58 52 6d 50 18   ........ ..2XRmP.
0030   42 3f 6f 21 00 00 00 00  00 76 ff 53 4d 42 25 00   B?o!.... .v.SMB%.
0040   00 00 00 18 07 d8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050   00 00 00 08 d4 03 00 08  40 00 0e 1a 00 00 00 08   ........ @.......
```

File: "C:\Logs\exploit9.pcap" 6704 bytes 00:0... | Packets: 63 · Displayed: 42 (66.7%) · Load time: 0:00.000 | Profile: Default

The Snort sensor sniffing the network traffic never created an alert to indicate that a rule had fired. In effect, the traffic appeared benign to the sensor which was using the default rule set. This includes all previously commented out rules which were activated before the malware was initiated, as well as a few that were added to the local rule set as written in a released Conficker paper (Leder & Werner, 2009, p. 8).

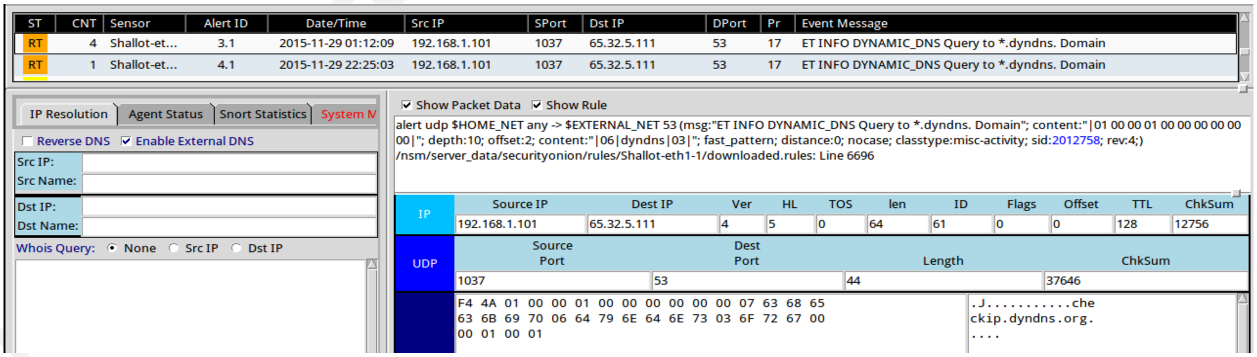


```
===============================================================================
Run time for packet processing was 0.0 seconds
Snort processed 499 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          499
===============================================================================
Packet I/O Totals:
   Received:          499
   Analyzed:          499 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
```



```
===============================================================================
Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:          499 (100.000%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
     (null):            0 (  0.000%)
```

A packet capture (pcap) of Conficker B was also downloaded and read through the same Snort sensor as a baseline test. All resulted in the same negative response by Snort. To completely rule out the possibility of a corrupted installation, Security Onion, a Linux-based suite of tools that includes Snort and Sguil, was installed on a different VM. After the initial configuration was completed, tcpreplay was used to run the included sample of the Conficker B pcap while running tools in detection mode. This also produced no stated Conficker alerts, although it did trigger some alerts for DNS in Sguil.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	Shallot-et...	3.1	2015-11-29 01:12:09	192.168.1.101	1037	65.32.5.111	53	17	ET INFO DYNAMIC_DNS Query to *.dyndns. Domain
RT	1	Shallot-et...	4.1	2015-11-29 22:25:03	192.168.1.101	1037	65.32.5.111	53	17	ET INFO DYNAMIC_DNS Query to *.dyndns. Domain

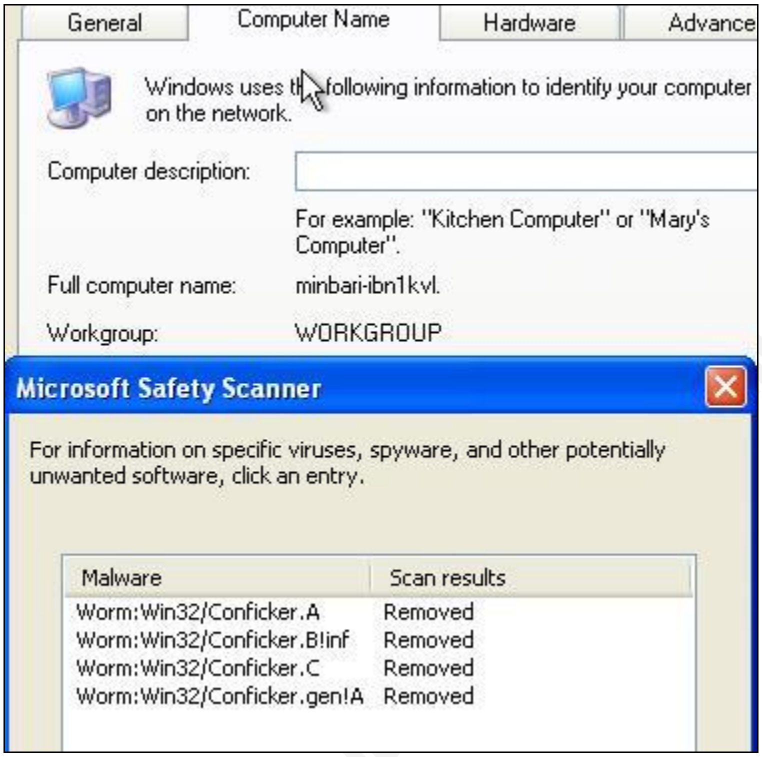
```
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET INFO DYNAMIC_DNS Query to *.dyndns. Domain"; content:"|01 00 00 01 00 00 00 00 00|"; depth:10; offset:2; content:"|06|dyndns|03|"; fast_pattern; distance:0; nocase; classtype:misc-activity; sid:2012758; rev:4;)
/nsm/server_data/securityonion/rules/Shallot-eth1-1/downloaded.rules: Line 6696
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.1.101	65.32.5.111	4	5	0	64	61	0	0	128	12756

UDP	Source Port	Dest Port	Length	ChkSum
	1037	53	44	37646

```
F4 4A 01 00 00 01 00 00 00 00 00 00 07 63 68 65    .J...........che
63 6B 69 70 06 64 79 6E 64 6E 73 03 6F 72 67 00    ckip.dyndns.org.
00 01 00 01                                        ....
```

At the conclusion of the test, Microsoft Safety Scanner, a malware removal tool, was run to confirm the presence of Conficker on the infected computer. It showed that several versions were present.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: minbari-ibn1kvl.

Workgroup: WORKGROUP

For information on specific viruses, spyware, and other potentially unwanted software, click an entry.

Malware	Scan results
Worm:Win32/Conficker.A	Removed
Worm:Win32/Conficker.B!inf	Removed
Worm:Win32/Conficker.C	Removed
Worm:Win32/Conficker.gen!A	Removed

While tools are helpful, they are not perfect. They must be reviewed for effectiveness and adjusted as necessary. Additional signatures may need to be introduced or updated as malware changes over time.

4. Why Detection is Important?

As shown above, Conficker and MyDoom are two viruses that are still circulating in the wild many years after the initial outbreak. Although the command and control structure may be inert, Conficker infections continue to linger. Even if the command structure no longer remains, it can always be reconstructed in the future. Not only that, previous malware has been repurposed at a later date for a different use (Carman, 2015).

Reports show that tempting morsels of information offered on Wikileaks are sometimes infected with older versions of malware including MyDoom (Wieder, 2015). Chances are that newer versions of malware are more likely to be used on vulnerable systems, but that does not discount the older versions. While some virus creators previously designed the software to gain notoriety, today's malware often exists for more devious reasons. Infected computers may be conscripted into botnets for large scale processing or distributed denial of service (DDOS) attacks. Ransomware, often requiring Bitcoin as payment, is used to extort money from unsuspecting victims. However, detections reveal the older malware, such as MyDoom and Conficker, still persist and can be spread through various means such as email and innocuous network traffic.

XP is also still in use in many ATM's as well as in government agencies. To date, the upgrade to a newer platform has been slow. Lack of continued support on the part of Microsoft as well as lack of security controls may put these devices at risk.

Another platform often overlooked is Supervisory Control and Data Acquisition (SCADA). These systems include devices supporting infrastructure, such as electrical and nuclear, as well as medical devices. During the Conficker outbreak, many medical systems were compromised. Because SCADA systems are so important, they often include legacy systems. These systems are not likely to be removed or replaced quickly and will most likely be around for some time.

5. Protections

If an outdated or vulnerable device needs to be maintained, appropriate measures should be enabled to help protect the system. Anti-virus with real-time scanning should be installed on supported systems and up-to-date signatures maintained. At the very least, an alternate method such as a Live CD should be used on a regular basis. For systems that are connected to a network, an IDS or IPS is recommended. If there is traffic to and from the device, placement of a detection sensor, either inline or passive, will help detect possible intrusions.

For currently supported versions of software, it is always best to test and deploy patches on all systems as soon as possible. Since manufacturers often discontinue patching for older software, segregating the devices and implementing controls will provide protection. For instance, placing the vulnerable systems behind a firewall with limited access will go a long way to protect the system. Firewall rules should be carefully considered to prior to implementation to assess the risk presented to the systems. Along with this, careful consideration should be given to other systems in the same subnet.

Fifteen years later, one of the main ways of spreading malware is to take advantage of human weakness. Resisting phishing attempts is also important. Anti-malware software will help if an infection occurs. Also, remind employees, family members and friends to be vigilant and think before clicking links and opening attachments.

Turn off all unnecessary services on the devices (e.g. WINS or IPv6) that are not in use. By removing these, it reduces the open pathways into a system. For instance, SQL Slammer targeted devices with an open TCP port 1434. Systems that have this port open but no service that requires its use may become unfortunate victims. This is not only considered a best practice but is also covered under due diligence. A company also has legal and financial obligations to make every effort to protect the data. With the recent increase in data breaches, the federal government is also levying heavy fines on companies that do not properly protect customer data.

Businesses should perform an impact analysis to assess the potential damage if the system is lost. Can the system be rebuilt or recovered if they choose to do nothing? What if the system is already compromised? This should take into account the financial implications of the loss of data.

A disaster recovery plan should also be considered and documented. If the system needs to be recovered, steps to ensure that the system is secured against further compromise should be included. Backups are an important part of disaster recovery planning. This helps ensure that some if not all of the data can be recovered and reduce the amount of downtime.

6. Conclusion

While viruses and worms pass into history, the general public tends to forget their existence. Klez, Melissa, and Sobig may not be a current threat to most systems, but others such as MyDoom and Conficker continue to outlast the memory of the non-security community. Although newer malware is developed, older versions continue to circulate and infect vulnerable, unprotected systems. Old tricks may resurface or be recycled and become harmful once more. Older software that is no longer supported by the manufacturer or community stays in use for various reasons, and it must remain protected utilizing techniques and tools of the trade.

IDS or IPS solutions can be useful in detecting and preventing the compromise of vulnerable systems. They must be properly configured and carefully reviewed on a regular basis to produce the best results. Utilizing data signatures and other methods, they can detect malware in transit and either log an alert or prevent the traffic from reaching the destination. They are not a panacea, but instead should be used to complement other tools such as firewall systems.

To facilitate the process, identify system vulnerabilities, assess the risk to the person or organization, and take steps to ensure that the data is safe. Carefully consider recovery actions and be prepared to use them. As part of this process, businesses should consider the legal and financial ramifications if the system is compromised.

Not unlike medical diseases, the spread of digital viruses and worms may slow down or go dormant only to be reawakened at a later date. It is important to be ever vigilant in security and remember tactics that may once again become useful to attackers.

References

Boutin, P. (2003, July 1). Slammed! *Wired*. Retrieved from http://www.wired.com/2003/07/slammer/

Carman, A. (2015, September 220. Repurposed malware and attack campaigns make a comeback. SC Magazine. Retrieved from http://www.scmagazine.com/arid-viper-returns-after-months-away/article/440127/

Conficker Working Group. (2011, January 29). Retrieved from http://www.confickerworkinggroup.org/wiki/

Danyliw, R., & Householder, A. (2001). CA-2001-19. Retrieved October 31, 2015, from http://www.cert.org/historical/advisories/CA-2001-19.cfm

Knowles, D., & Perriott, F. (2003, December 9). W32.Blaster.Worm. Retrieved November 15, 2015, from http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99

Leder, F., & Werner, T. (2009). *Know Your Enemy: Containing Conficker*. Retrieved from The Honeynet Project website: http://honeynet.org/papers/conficker

Longeray, P. (2015, November 13). Windows 3.1 Is Still Alive, And It Just Killed a French Airport. Retrieved November 15, 2015, from https://news.vice.com/article/windows-31-is-still-alive-and-it-just-killed-a-french-airport

Martel Police Body Camera Virus Found Embedded into Camera [Web log post]. (2015, November 12). Retrieved from http://www.goipower.com/?pageId=40

Meet Linux Viruses. (2012, July 26). Retrieved November 22, 2015, from http://www.unixmen.com/meet-linux-viruses/

Microsoft Security Intelligence Report (19). (2015). Retrieved from Microsoft website: http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf

Schneier, B. (2007, October 4). Gathering 'Storm' Superworm Poses Grave Threat to PC Nets. *Wired*. Retrieved from http://archive.wired.com/politics/security/commentary/securitymatters/2007/10/securitymatters_1004

Snort.Org. (n.d.). Retrieved from https://snort.org/

Unknown. (n.d.). Virus: W32/Melissa Description | F-Secure Labs. Retrieved October 31, 2015, from https://www.f-secure.com/v-descs/melissa.shtml

Vulnerability Summary for CVE-2003-0533. (2008, September 10). Retrieved November 15, 2015, from https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533

Xiao, K. (2015, September 25). W32.Mydoom.E | Symantec. Retrieved November 5, 2015, from http://www.symantec.com/security_response/writeup.jsp?docid=2015-092509-0009-99

Zetter, K. (2009, July 8). Lazy Hacker and Little Worm Set Off Cyberwar Frenzy. *Wired*. Retrieved from http://www.wired.com/2009/07/mydoom/

Wieder, J. (2015, March 30). Josh Wieder: Wikileaks Global Intelligence File Dump is Loaded With Malicious Software [Web log post]. Retrieved from http://www.joshwieder.net/2015/03/wikileaks-global-intelligence-file-dump.html