Alex Shah
EN.695.741.81.SP25 Information Assurance Analysis
Mod 1 Assignment 1 Part 1
January 26, 2025

SQLSlammer

The SQL Slammer worm leverages the CVE-2002-0649 vulnerability to buffer overflow the Resolution Service for MySQL Server 2000 and Microsoft Desktop Engine in order to remotely execute code and spread to other systems. The advisory pages from the 2002/2003 period give the worm different advisory numbers such as NVD NIST Page describing the CVE and lists the severity as “7.5 High”. Microsoft’s Security Bulletin names the vulnerability “Q323875” and calls the severity “Critical”. Bugtraq calls the vulnerability “#NISR25072002” with the Severity “Critical/Very High”. And Carnegie Mellon calls the vulnerability “VU#399260” and states the “severity metric” as “43.28”. There don’t appear to be variants listed on the advisory pages, and across the security advisories the description of the mechanism and affected software are the same, describing the same payload, while the name given to the vulnerability, identifying numbers, and severity score vary.

Advisories:
https://nvd.nist.gov/vuln/detail/CVE-2002-0649#vulnCurrentDescriptionTitle
https://www.cve.org/CVERecord?id=CVE-2002-0649
https://marc.info/?l=bugtraq&m=102760196931518&w=2
https://www.kb.cert.org/vuls/id/399260
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2002/ms02-039
https://seclists.org/fulldisclosure/2003/Jan/240

Propagation

The SQL Slammer worm infects a host running MS SQL or MSDE 2000 running with port 1434 open to UDP and executes a buffer overflow/overrun with the privileges of the SQL Service account from a flaw in the SQL Server Resolution Service. It then uses pseudo random number generation to get a new target to spread to, and sends the worm payload in a single packet to the same port (1434, UDP) on the target address to attempt to infect an unpatched host.

Detection
The Slammer code fits into a single packet and targets port 1434 on UDP where the SQL Server Resolution Service is expected to run. If traffic to that port is encountered, especially with a payload matching the Slammer worm, the infection attempt can be detected in logs and alerting software such as at the firewall. The service was patched, and it was recommended to block port 1434 to external connections to prevent infection, so unexpected traffic to that port would be detectable, and scanning the packet would reveal the payload. There don’t appear to be variants listed in the advisories, so detection would consist of analyzing traffic patterns and looking for the payload.

Further Sources
http://virus.wikidot.com/slammer

WannaCry

WannaCry ransomware exploits a vulnerability in Microsoft SMBv1 servers to execute remote code on a vulnerable system. The vulnerability is described as “High” or “Critical” by Microsoft and “High” by Nmap/Seclists and is denoted by CVE-2017-0144 and CVE-2017-0145 or Microsoft’s security advisory name “MS17-010”. There are many variants to the WannaCry payload as noted by the Tripwire article that over 12,000 variants had been detected with Sophos finding that 10 variants accounted for 3.4 million out of 5.1 million detected infection attempts. It was suggested that the variants were created by multiple groups for their own ransomware targeting purposes. There are multiple CVEs relating to the SMB vulnerability such as CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148 with CVE-2017-0144 and CVE-2017-0145 being the most commonly cited for the vulnerability in SMBv1 used to propagate WannaCry. The WannaCry ransomware is also given other names such as WannaCrypt, and Wcry and originates from the “EternalBlue” and similar malware that leverage the same exploits. Similar ransomware attacks with different names were launched with the same exploit such as NotPetya and BadRabbit.

Advisories
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0145

Propagation
The SMBv1 vulnerability allows remote execution on unpatched hosts running Microsoft operating systems. This allows an attacker to use an infected host to scan local devices and move laterally within a network, or using the devices to attempt to propagate to new networks by targeting a new IP on common SMB ports like 445 with a maliciously crafted packet that causes a buffer overflow and executes shellcode.

Detection
Some variants of the malware check for a kill switch domain before proceeding, so network calls to these hardcoded domains can provide evidence that a device is infected and should be isolated. Once the program has executed and encrypted local files, the ransomware makes itself known by demanding payment to decrypt. Later variants of the original checked for different hardcoded domains, which were registered by security research groups to prevent the spread of the ransomware by halting the program at the domain check. But later variants did not use the domain kill switch. Researchers also found methods to decrypt the data from flaws in Windows Encryption APIs and tools were created to subvert the ransom across variants. So network callouts to these domains can be detected and the processes that run the encryption can be detected as well from signature matching.

Further Sources
https://www.tripwire.com/state-of-security/over-12000-wannacry-variants-detected-in-the-wild
https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/
http://virus.wikidot.com/wannacry

Duqu

Duqu and Duqu 2.0 are advanced persistent malware that use multiple exploits in Microsoft operating systems which also used advanced tactics to avoid detection. There are multiple exploits used which Microsoft names MS11-087, MS14-058, MS15-061, and MS14-068 for CVE's CVE-2011-3402, CVE-2015-2360, CVE-2014-4148, and CVE-2014-6324.

Advisories
https://www.cisa.gov/news-events/ics-alerts/ics-alert-11-291-01e

https://nvd.nist.gov/vuln/detail/CVE-2011-3402
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-087

https://nvd.nist.gov/vuln/detail/CVE-2015-2360
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-061

https://nvd.nist.gov/vuln/detail/CVE-2014-4148
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-058

https://nvd.nist.gov/vuln/detail/CVE-2014-6324

https://www.cisa.gov/news-events/alerts/2014/11/19/microsoft-windows-kerberos-kdc-remote-privilege-escalation

https://marc.info/?l=bugtraq&m=142350249315918&w=2
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms14-068

Propagation
Duqu does not spread on its own according to CISA. But it moves laterally within a network/Windows domain once an initial infection leads to elevated domain privileges. For example in a publication by Infosec Institute, a Duqu 2.0 attacker used spear phishing to target an individual at Kaspersky by email where a Word document attachment contained an exploit in TrueType font parsing. This gave access to an unprivileged domain user which was used to achieve domain administrator privileges from another exploit. This could then be used to infect other computers in the domain via Microsoft installer packages (.msi) sent remotely to the machines and started with Task Scheduler.

Detection
The malware runs in memory and writes no files to disk making detection difficult, but in the spear phishing example the target user's email inbox and web history had been erased, raising suspicions. Some variants, noted by Symantec in the Infosec Institute article, create a backdoor to multiple machines to retain persistence, and use stolen certificates from Foxconn/Hon Hair Precision to sign a driver. The compromised certificates and signed packages can be detected. The drivers were used in gateways and network devices to achieve access and prevent logging, which use premade passphrases which can be identified in malicious code as well as using cookie headers with hardcoded strings when sending messages to C&C servers. The code also connects to Microsoft URLs to get proxy addresses in order to indirectly connect to C&C servers. The malicious code also activated newly infected hosts with a hardcoded string over an SMB network pipe that can be detected. Variants of Duqu also hide their connection to the C&C server with encrypted data at the end of different image formats, and variants use different user agent strings. These various hardcoded strings, common URLs, and some

common hashes of packages and payloads can allow detection of the Duqu malware. These common addresses and hashes are enumerated through indicators of compromise such as files SecureLists released which can be used to prevent connections and distribution of related files in a network.

Further Sources
https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/
https://www.infosecinstitute.com/resources/malware-analysis/duqu-2-0-the-most-sophisticated-malware-ever-seen/

Flame

Flame is a large virus toolkit that uses several exploits on Microsoft's operating systems including ones previously seen in Stuxnet. Some were used in the initial infection such as by email or infected flash drives like CVE-2010-2568 which Microsoft calls MS10--046. And to move laterally with CVE-2010-2729 which Microsoft calls MS10-061.

Advisories
https://attack.mitre.org/software/S0143/
https://nvd.nist.gov/vuln/detail/CVE-2010-2568
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-046
https://nvd.nist.gov/vuln/detail/CVE-2010-2729
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-061

Propagation
Flame was likely spread through multiple ways and it contains multiple exploits for achieving initial infection such as by spear phishing over something like email or by infected flash drives or network devices. Once initial infection is achieved, there are several exploits that can be leveraged to move laterally like flaws in the print spooler service.

Detection
The user agent used in downloading some components is unique and can be used to identify communication by the malware. Being so large of a toolkit, there are many dll's and payloads that can be detected by the file hash though it can run in memory so this would have to be analyzed in memory dumps. The malware also makes registry changes that can be detected. Variants like Flame 2.0 have been discovered that use stronger encryption and obfuscation but the methods to detect the hashes of the files and detect processes and network activity remain the same.

Further Sources
https://web.archive.org/web/20120528142705/http://www.crysys.hu/skywiper/skywiper.pdf
https://silascutler.com/uploads/Flame_2.0_Risen_from_the_Ashes.pdf

Stuxnet

Stuxnet targeted SCADA systems and exploited vulnerabilities in Microsoft operating systems and Siemens Step7 program. It was originally given the name "Rootkit.Tmphider" by VirusBlokada, Symantec called it "W32.Temphid" then "W32.Stuxnet". Exploits in Windows shortcuts go by MS10-046 and CVE-2010-2568 which were also used in Flame and others. It also uses MS10-073/CVE-2010-

2549 to elevate privileges on Windows. It propagates with MS10-061/CVE-2010-2729 print spooler exploit and MS08-067/CVE-2008-4250 Remote Procedure Call exploit.

Advisories
https://attack.mitre.org/software/S0603/
https://www.cisa.gov/news-events/ics-advisories/icsa-10-272-01
https://web.archive.org/web/20120104215049/http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-046
https://nvd.nist.gov/vuln/detail/CVE-2010-2568
https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-073
https://nvd.nist.gov/vuln/detail/CVE-2010-2549
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-061
https://nvd.nist.gov/vuln/detail/CVE-2010-2729
https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067
https://nvd.nist.gov/vuln/detail/CVE-2008-4250

Propagation
The worm was spread to air gapped systems by infected flash drives that contained a shortcut file with an exploit to execute its payload. It also uses exploits in the Print Spooler service and using an exploit in Remote Procedure Call to spread to and update other internal systems that wouldn't have internet access. Further propagation could be carried out by spreading to removable media or later it unintentionally spread to an employee device that later connected to the internet where it began to spread beyond its original scope.

Detection
With its rootkit capabilities and limited intent outside of specific control systems in the target SCADA systems, Stuxnet mostly propagates and hides which makes it hard to detect but the CISA advisory describes many indicators of compromise including payload hashes and which files are modified by the malware as well as their hashes. This lets infected users detect the files and changes in order to quarantine and remove the malware files and attempt to remove the rootkit. There were variants that were created to speed up the spread of the malware but the detection remains the same.

Opasrv

Opasrv takes advantage of a flaw in network shares to connect with only one character of the password. The Microsoft advisory names this MS00-072 and it is also called CVE-2000-0979. There are several variants that use the same exploit and mechanisms but may obfuscate through encryption or use different file names. The advisories for the vulnerabilities do not list variants that use the exploit but advisories on Opasrv itself such as f-secure list that there were several variants denoted by letters such as "Opasoft.A (Worm.Win32.Opasoft.a, Brasil)", "Opaserv.E (Worm.Win32.Opasoft.E, Opasoft.E)", "Opaserv.F (W32/Opaserv.worm.F, Trojan.Win32.KillWin.m, W32.Opaserv.K.Worm)", "Opaserv.G (W32/Opaserv.worm.G, Trojan.Win32.KillWin.m, W32.Opaserv.M.Worm)", "Opaserv.N (Worm.Win32.Opasoft.f)", and "Opaserv.O (Trojan.Win32.KillWin.n)". virus.Wikidot.com also notes a variant "Opaserv.S".

Advisories

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32%2FOpaserv

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2000/ms00-072

https://nvd.nist.gov/vuln/detail/CVE-2000-0979

https://marc.info/?l=bugtraq&m=97147777618139&w=2

https://www.f-secure.com/v-descs/opasoft.shtml

Propagation

The malware spreads to shared network devices and drives through an exploit in the Shared File and Printer service in Windows that is able to use one character of a password to authenticate. The process scans local devices on nearby and randomly generated subnets to attempt to find NETBIOS Name service running on ports 137 and 139 over UDP. Files are dropped into the network share and autorun files are modified to start the process at boot which spreads the worm.

Detection

Certain files and registry values can be detected as the trojan tries to propagate and install such as srcsvr.exe spreading to a network shared drive, as well as changes to registry values and system files to allow the trojan to start at bootup. Some variants also present the user with a message about their Windows license. Traffic on ports 137 and 139 by UDP can indicate that the worm is spreading through the network and multiple variants cause the device to restart or prevent restart that can be detectable symptoms of the infection. The variants use different names for some files and processes, as well as registry values. But the overall detection process and mechanisms remain the same.

Further Sources

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32%2FOpaserv
https://www.f-secure.com/v-descs/opasoft.shtml
http://virus.wikidot.com/opaserv
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Opaserv-O/detailed-analysis
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32%2FOpaserv

Melissa

According to TrendMicro, Melissa goes by the names “W97M_MELISSA.FY (TrendMicro)”, “Email-Worm.VBS.Melissa.z (Kaspersky)” and “WM97/Meliss-Fam (Sophos_Lite)”. And Symantec calls it “W97M.Melissa.A”. There are a handful of variants that modify different files or contain different messages to trick users into opening the attachment such as “Assilem”, “Melissa.W (AKA Prilissa)”, and “Melissa.BG”. There aren’t any CVE numbers or vulnerabilities listed in the advisories, rather it

takes advantage of how macros work and betrays user trust in opening attachments or unknown files which launches a script.

Advisories

https://www.f-secure.com/v-descs/melissa.shtml

https://web.archive.org/web/20061110161357/http://www.symantec.com/security_response/writeup.jsp?docid=2000-122113-1425-99

https://www.trendmicro.com/vinfo/id/threat-encyclopedia/malware/W97M_MELISSA.FY

Propagation

The virus was sent by email, which when opened uses macros to send the virus to more recipients from the infected computer's Outlook email. The malicious email attachment uses a visual basic script to modify a template Word document and default macros where macros send the attachment to contacts in the infected systems Outlook mail system to infect more devices by email attachment. The malicious file can also be downloaded and run from the web.

Detection

The malicious email attachment or downloaded file can be detected by hash and the modified Word template file and modified macros can be detected as well in order to find that the device has been infected to send out the malicious attachment by email. The user would receive an email or obtain a file that would reveal the malicious script, as well as see outgoing mail to show that the file was sent out if the infection succeeded.

Further Sources

https://www.trendmicro.com/vinfo/id/threat-encyclopedia/malware/W97M_MELISSA.FY
https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519
http://virus.wikidot.com/melissa

Koobface

Koobface spreads by social engineering by prompting users to install a package such as a fake Adobe Flash installer, so there are no CVEs or vulnerabilities in the advisory pages. There are multiple fake installers or packages that users can run which aim to gather credentials for various social media platforms. The installers can target multiple platforms including Microsoft, Apple, and Linux operating systems. Which means there are many variants to run on the different platforms, to gather different credentials to spread, and multiple packages the variants can be hidden in to trick users. Variants different advisory and antivirus pages include "Worm:Win32/Koobface.gen!F", "Net-Worm.Win32.Koobface.a", "Net-Worm.Win32.Koobface.b", "WORM_KOOBFACE.DC", "W32/Koobfa-Gen", "W32.Koobface.D", and "OSX/Koobface.A".

Advisories

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Worm:Win32/Koobface.gen!F&threatid=2147631531

https://web.archive.org/web/20090512192108/http://www.us-cert.gov/current/archive/2009/03/04/archive.html#malicious_code_targeting_social_networking

https://web.archive.org/web/20081209011116/http://www.symantec.com/security_response/writeup.jsp?docid=2008-080315-0217-99

https://web.archive.org/web/20090815104342/http://www.symantec.com/security_response/writeup.jsp?docid=2009-080717-5930-99

Propagation

The worm spreads by malicious files or installer packages that trick users into installing what they believe to be legitimate programs or visiting legitimate links. The worm gathers credentials for various social media platforms to send messages to the user's contacts or post publicly which spreads the link or file to infect new hosts. It does this by checking for login cookies in browser directories to steal credentials. By spreading the link/file from user accounts, the user's friends are inclined to trust that the file was legitimate and so the primary spread was through social engineering and tricking users into believing that some software needed to be installed to view the linked videos or attachments.

Detection

The malicious payloads are packaged into installers such as pretending to be an Adobe Flash player update, which means common packages can be detected by antivirus software. The worm extracts and runs executable files such as within the Windows directory on Microsoft operating systems, and writes registry values to execute the worm at startup. These files and registry values can be detected to identify an infection. Depending on the variant and payloads, the worm may also serve ads or install other programs which would be indicators of an infection. While there are multiple variants, the primary vectors are social engineering to trick the user into installing software where variants target different operating systems and credentials to steal, so the extracted files, changed registry values, email/social posts, and errant software and popups would be similar across variants to detect.

Further Sources

https://en.wikipedia.org/wiki/Koobface
https://www.kaspersky.com/resource-center/definitions/what-is-the-koobface-virus