Anti-Ransomware Guide

Christopher M. Frenz & Christian Diaz

Version 1.6
12-September-2017

Executive Summary

Open up any newspaper or news site and an increasingly common headline is becoming "hospital held for ransom". While hospitals and other organizations often have downtime procedures that let them revert back to paper for dealing with power outages and other disasters, it is still a nightmare scenario to find your entire organization's IT infrastructure screeching to a halt all because someone clicked on a malicious link or opened a questionable email attachment. Moreover, many organizations have a significant number of legacy systems that make security a challenge and beyond very basic security provisions often do not have a corporate culture that is heavily focused on information security. This has left many organizations struggling with how to handle ransomware attacks. The below is meant to serve as a comprehensive defense in depth based checklist and guide to preventing ransomware from taking a foothold in your organization as well as ensuring the proper procedures are in place to deal with an actual ransomware outbreak in your environment. Given the prevalence of Windows systems as ransomware targets, the guide is geared towards a Windows environment but is designed to be product agnostic. Please note that the list is designed to be comprehensive and as such not all controls may be applicable to all environments.

Perimeter Protections:

These are your first line of defense as stopping a threat before it gains access to any of your systems or employees is always ideal.

Firewall:

While a firewall at the perimeter is probably already in place for most organizations, it is important to verify that your firewall is configured for egress filtering as well as ingress filtering. Ingress filtering controls what communications are allowed into the organization's network, while egress filtering controls what communications are allowed to leave the organization's network. Both egress and ingress access controls should be based on a least privilege model. Systems that do not need access to external information sources and systems should be blocked from communicating with external entities. A system without access to any external entities is far less likely to become an entry point for malware than an internet connected system. Moreover, in the event that a ransomware infection takes place it will not be able to phone home if proper egress filtering is in place. Logging should also be turned on on the firewall as repeated access attempts being logged to known malicious IP addresses can serve as an indicator of a problem.

Proxy Server/Web Filter:

As mentioned above, cutting systems off from the internet completely is a great defense where feasible, but the reality is that completely blocking internet on all systems is likely not feasible and would be a hindrance to business operations. Internet connected systems should be configured to go through a proxy server that allows for Web content to be filtered, with firewall rules ensuring that proxied Web access is the only means of egress for http and https connections. While a whitelisting approach to Web access is most ideal, organizations should at a minimum use their filtering appliance to block access to known malicious sites, spam/phishing sites, proxy avoidance sites, pornography, and all other categories of sites deemed unnecessary for normal business operations. It is also recommended, where feasible, that any website yet uncategorized by the vendor be blocked as there is a higher chance of such a site being malicious in nature than being a new valid business site. While it may be politically unpopular within many organizations, it is also strongly recommended to block access to personal email, file sharing sites, social media, instant messaging, and advertising networks at this level. Special exemptions for file sharing sites, social media, etc, can be added on an as needed basis. Prohibiting the

download of executable files (e.g. .exe, .scr, etc) onto endpoints should also be put in place. Many proxy servers/Web filtering appliances also have the ability to scan incoming web content with an AV engine. Where this is supported it is recommended that it be turned on and that where feasible a different AV engine than the one used internally used to enhance the likelihood that a signature exists for a relatively new threat. Web filters should be updated regularly to ensure that categorizations for malicious and other sites are always current.

In addition to the blocks stated above it is advised that Web traffic to the following top level domains be completely blocked as results from Spamhaus (https://www.spamhaus.org/statistics/tlds/) and BlueCoat (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems/) suggest that the majority of sites hosted on these TLDs are suspicious in nature:

Top Level Domain
.accountant
.biz
.click
.country
.cricket
.download
.gdn
.gq
.kim
.link
.party
.review
.review
.science
.stream
.tk
.top
.trade
.win
.work
.zip

SPAM Filter:

As a perimeter defense we are discussing SPAM filters that filter email before they hit your corporate mail server or if you are using hosted email ensuring that the SPAM filtering made available by your hosting provider is turned on. It is far better to block at the perimeter known SPAM, mail containing malicious links, and mail containing malicious attachments, that to let other internal layers of defenses handle it. It is also recommended to block any message that contains executable attachments such as .exe or .vbs files. For institutions that do not have any international presence it may also be advisable to block all emails coming from locations outside of North America and whitelisting any necessary exceptions. As with Web filtering software, SPAM filters should always be kept up to date

to ensure they have the latest block lists and that their AV engines have the latest signatures for analyzing attachments. Where feasible the AV engine used in the SPAM filter should be different than the AV engine used on endpoints where email will be accessed.

Network Defenses:

Defenses than can be deployed on the LAN to help detect and mitigate malware outbreaks.

DNS Sinkhole:

While connectivity to malicious sites is ideally blocked at the perimeter, an extra layer of defense against establishing connections to malicious sites can be added by creating a DNS sinkhole which will prevent connections to certain domains by giving out false information when a DNS request comes in for one of the domains in the sinkhole. As with perimeter defenses, preventing any system or person from accessing malicious content is always far preferable to mitigating it once it has been downloaded to or accessed by an endpoint. Ideally your sinkhole domain list will be from a different source than the one used on your Web filter to ensure more comprehensive coverage of malicious domains. A tutorial on creating DNS sinkholes on Windows DNS servers can be found at: https://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist

Network Segmentation:

Network Segmentation via VLANs and ACLs that control traffic between VLANs will not work to prevent a ransomware attack from gaining access to your systems, but will be invaluable if a malware infection is able to gain a foothold within your organization. Network segmentation can help to ensure that a malware infection, or other security issue, stays isolated to just the network segment the infected endpoint is on and does not spread through the entirety of the organization. It is particularly important for organizations that maintain legacy systems which are no longer able to receive security updates.

Virtual Machine Segmentation:

Just as the network segmentation discussed above is key in ensuring that the number of systems a malware infection can spread to is minimized, it is important to remember that many virtual machine communications take place across the back plane of a server and do not transverse standard network equipment like switches. For heavily virtualized environments it is advisable to deploy virtual machine segmentation technologies, such as VMware's NSX or Microsoft's HNV, to ensure that virtual machine communications can be controlled with network security mechanisms that are equivalent to that of physical systems.

Network Intrusion Detection System (NIDS):

Having a network IDS in place will likely not be a highly effective way of preventing malware from gaining access to your system as most are geared more towards detecting exploit attempts than malware, but a NIDS system can be used to alert to potential outbreaks since they can be used to alert if communication attempts are being made to malicious IP addresses such as command and control centers for botnets and key generation sites for ransomware tools. The earlier IT and infosec staff are alerted to the presence of malware outbreak, the better the chance there is at successfully containing the incident, and this is one such avenue of detection that can be employed. Depending on the deployment, NIDS systems may also help to pinpoint a system within the organization that is attempting to infect other systems.

Endpoint Protections:

Protections that exist on desktop PCs and other systems that users interface with.

Fully Patched and Updated:

Ransomware and other malware often use a variety of exploits to gain a foothold onto systems and ensuring that the OS and all applications on the system are fully patched and updated will minimize the number of ways that endpoints can be successfully exploited. With regards to ransomware keeping your email client, browser, and Flash fully updated is of critical importance. Organizations should have robust procedures in place for ensuring proper patch management and the routine patching of software.

No Unnecessary Applications and Services:

If an application does not exist on the system it cannot be exploited so ensuring that endpoint configurations also follow a least privilege model is an effective way of reducing the attack surface of endpoints. It is particularly advisable to not run Java and Flash on computers that do not require it.

No Administrative Rights:

Administrative rights should only be used for administrative tasks and normal computer usage should never be performed from an account with administrative privilege. This will prevent many types of malware from gaining a foothold as they users account may simply not have the proper permissions to "install" the malware.

Antivirus (AV):

Antivirus should be run on all endpoints and configured for on access scanning of files and other resources. Antivirus should be kept up to date and alerting should be configured to notify IT staff on any possible infections. It is important to remember that AV is largely signature based and, as such, can only effectively detect known threats. AV may not provide any protection against a novel virus or a new malware variant. Ideally this is a different vendor than one used to scan for viruses at the perimeter defense level.

Next Generation AV:

Antivirus solutions that signature-less in nature and as such have the potential to detect zero-day attacks and novel strains of malware. Next-gen AV uses methods like behavioral detection, machine learning, and cloud based file execution to try to identify exploit attempts and malware. Some Next-gen AV packages are certified under PCI-DSS as AV replacements but not all are. In many cases they can be used as a potential compliment to traditional AV.

Host Based Intrusion Detection/Prevention Systems (HIDS/HIPS):

These systems could be standalone or integrated into an endpoint protection solution from an AV vendor. They work to detect suspicious changes to critical system files, potential buffer overflows, and other potentially suspicious activity on endpoints. They may help to provide earlier insight into a possible outbreak and some have a limited ability to mitigate certain exploit attempts.

Web Filtering:

Many endpoint protection packages provide an additional means of filtering malicious Web content and it is advisable to turn these filters on as well, particularly if the recommended practice of using a different vendor for internal systems vs. the perimeter is followed. This will increase the chance that malicious Web content is blocked before a system or user has the ability to access it.

SPAM Filtering:

As with Web filtering, SPAM filtering is also possible at the endpoint level and having a different filtering solution in place on endpoints can help to increase the odds that SPAM and malicious emails that bypass perimeter defenses are detected. This is critical since certain ransomware variants like Locky are commonly spread through malicious email attachments.

Disable Support for Macros:

Macros and other executable content can be embedded in documents used within office applications and PDF files. Odds are that most users in your organization have no legitimate need for such features and support for such features should be turned off by default.

Software Restriction Policies/AppLocker:

GPO policies can be set to blacklist certain applications from running and to blacklist applications from running in certain locations such as the AppData folder of a user's profile, which is a common malware target. Organizations can develop their own policies or use the anti-ransomware policies made available by organizations like Third Tier. As an alternative to GPO blacklists, the free CryptoPrevent utility can also be used to deploy software restriction policies to endpoints. Such policies are a nice compliment to AV software as they are not signature based and may prevent event novel malware variants from running successfully. Just be sure to test any such policies to ensure they do not interfere with any legitimate applications that are used within your environment. A better approach than blacklisting would be an application whitelisting approach, but this is more challenging and time consuming project in order to ensure that no critical applications are broken once only whitelisted applications are allowed to run.

Hosts file:

Hosts files are checked prior to DNS to resolve IP addresses and like DNS sinkholes can be used to prevent malicious domains from being properly resolved. In addition to other Web filtering mechanisms this could provide another layer of defense against a user or system potentially connecting to a malicious site.

Disable USB Access:

While not as common as Web and email based transmission vectors there have been variants of the CryptoLocker ransomware that have been known to spread via USB drives. Wherever feasible, USB drive access should be blocked.

Virtual Desktop Infrastructure:

If the organizations endpoints are virtualized an additional option for malware defense is to ensure that all VDI desktops are non-persistent and that the systems revert back to a predefined state after each

session. This ensures that any malware that infected a VDI desktop is eliminated once the users sessions ends, since the system reversion will restore the desktop to a "like new" pre-infection state.

Enhanced Mitigation Experience Toolkit (EMET):

EMET is a free utility released by Microsoft that helps to detect and prevent exploits that seek to take advantage of memory corruption. EMET is also a nice addition to techniques like AV, because it is not signature based and as such has a chance at stopping even novel malware and exploit attempts. Be sure to test EMET thoroughly before deploying though to ensure it does not interfere with any of the legitimate applications used in your enterprise. More information about EMET can be found at - https://technet.microsoft.com/en-us/security/jj653751 EMET is being made EOL in upcoming months, but will be replaced by Exploit Protection mechanisms built into the Windows Defender Security Center in Windows 10.

Local Administrator Password Solution (LAPS):

While the authors are not aware of any known ransomware variants that spread to other systems using pass the hash techniques, it is a common exploitable vulnerability present in many windows environments since the local admin password for each machine is common across all systems. LAPS randomizes the local admin password of systems and stores the passwords in Active Directory. It further allows for access controls to be put into place to control who can lookup these AD stored local admin passwords. LAPS thus makes it harder for attackers and potential worm like malware to move laterally through a breached organization. More information about LAPS can be found at - https://technet.microsoft.com/en-us/library/security/3062591.aspx

Application Sandboxing:

Application sandboxing is a method of isolating applications so that they only have access to a strict set of tightly controlled resources such as memory and disk space. Typically sandboxed applications are prevented from permanently committing any changes to disk. As such sandboxing application such as web browsers and their respective plugins can help to prevent certain forms of ransomware from impacting your system as the sandbox has the potential to keep the ransomware from accessing the files on your hard drive or network shares.

Disable SMBv1:

Many ransomware variants, including WannaCry, exploit vulnerabilities in the SMBv1 protocol. Modern versions of windows are capable of using the newer SMBv2 and/or SMBv3 protocols and in many cases SMBv1 can be safely disabled within your environment. In case other security vulnerabilities are discovered in the SMBv1 protocol having it disabled may provide a proactive security defense against future ransomware attacks. Microsoft has a guide for disabling SMBv1 available at https://blogs.technet.microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/. Please be sure to test this thoroughly before applying domain wide as older version of Windows and other legacy equipment may require SMBv1 to function properly.

Controlled Folder Access

A new feature being introduced in Windows 10 that will block unauthorized applications from making any changes to the contents of a protected folder.

https://blogs.windows.com/windowsexperience/2017/06/28/announcing-windows-10-insider-preview-build-16232-pc-build-15228-mobile

PayBreak

An interesting research project which has the potential to reverse the effects of a ransomware attack by recording the encryption keys used by the ransomware to encrypt each file. More information about the technique and tool developed by the researches is available at https://eugenekolo.com/static/paybreak.pdf.

NAS Server:

Most organizations have shared drives hosted on some form of NAS device that can have shares that are affected by ransomware. The protection mechanisms listed below are in addition to all of the protection mechanisms, such as fully patched, AV, etc, described under endpoint protection.

File Permissions:

A common principle in information security is that of least privilege whereby individuals should only have access to what is required to do their jobs and no more. Unfortunately with regards to network shared drives it is not uncommon for many organizations to experience scope creep with regards to permissions over time. IT is not always properly informed when an employee is transferred to a new department or in some other ways changes roles within an organization. This often results in permissions being added for the new role, but the no longer needed permissions of the old role remaining in place. While it is a good security practice in general to remove unnecessary access permissions, given the spike of ransomware attacks now is a very pertinent time for organizations to audit access permissions on all file shares and ensure that least privilege is being enforced. It is will be significantly more difficult for a malware infection to encrypt files if the user does not have access to the files in the first place. Thus, while this control may not help prevent a ransomware attack, it can go a long way towards mitigating how much data in your organization is impacted.

Shadow Copies:

While some newer ransomware variants have some ability to prevent data restoration from shadow copies having point in time snapshots of your data can provide a quick way of restoring data in many cases. Windows supports taking point in time snapshots of storage data and the ability to roll back to previous point in time versions of files.

Virtual Machine Snapshots:

Virtualization of server infrastructure is quite common and it is also possible to protect against ransomware by taking regularly scheduled virtual machine snapshots that will allow you to roll the virtual machine state back to a previous point in time. This can provide an alternate recovery option in the case a ransomware attack hits.

Data Inventory:

Having a data inventory which maps out what type of data is present in each share is highly beneficial at it can help you to triage your recovery and remediation priorities. Moreover, strains of malware that threaten to dox victims are also appearing. Having a clear sense of what data was encrypted or

otherwise effected by the malware, will help the organization to better assess the threat of doxing.

SIEM and Log Management:

Firewalls, servers, IDS devices, Web filters, endpoints, etc all generate log data which may provide clues to a malware outbreak. Having a SIEM solution monitor and process these logs may help to provide an early indication of a possible malware outbreak and as such may help to improve upon response times. Having this data centrally collected may also help in the analysis of it if a root cause analysis later needs to be performed.

Backup:

In case an attacks hits, recovering from a ransomware attack will take the presence of proper backup and recovery plans.

Backup and Recovery Plan:

The organization should have a well-defined recovery point and recovery time objective for each asset, which will help them to determine the proper backup technologies and procedures for their particular environment. There should be clearly documented policies and procedures in place for describing backup schedules, how data is supposed to be backed up or recovered, who is responsible for backups and recovery, etc. It also pays to have employees cross trained in this area.

Storage Snapshots:

In most large environments, server storage is often housed on a SAN and most modern SAN appliances let you retain one or more snapshots of your storage volumes. Storage snapshots should be configured so that if necessary a volume can be rolled back to a previous state that was snapshotted prior to the outbreak. The frequency of snapshots should be determined according to your organizations predetermined recovery point and recovery time objectives.

Offline Backups:

While technologies like real time replication between SANs or data centers are great for business continuity purposes, they are not much use in recovering from a ransomware attack as the encrypted versions of files will be rapidly replicated to other locations as well. To successfully restore data from backup following a ransomware event backups should be taken in a pull only manner and stored offline to ensure that backup data does not become encrypted and unrecoverable as well. While not as sexy as many newer disk based backup systems, tape can still serve as an ideal backup medium for storing multiple historical point in time snapshots of data from within an environment. Backup frequency should be determined according to your organizations predetermined recovery point and recovery time objectives.

Testing of Backup and Recovery:

Disaster recovery plans are often put to the wayside until disaster actually strikes which can be a big mistake. Backup and recovery should be successfully tested on a routine schedule to ensure that all systems are working properly and that staff members are knowledgeable enough to actually operate the systems. You do not want to wait to find out that a critical server was not being backed up properly after a ransomware attack or other disaster occurs. Routine testing will also improve the recovery time in the event that a disaster actually does strike.

Awareness Training:

Despite many protection mechanisms, the reality is that it is still possible for a malicious email or malicious link to get through and find itself presented to a user. In this case, while AV, software restriction policies, and other endpoint defenses may still protect you the best defense is a well-educated user capable of recognizing a suspicious email and reporting it to the IT department for investigation in a timely manner. The sooner such suspicious communications are reported, the sooner they can be blocked at the perimeter, AV companies contacted to create signature, and other defenses deployed to help stop the spread of the threat throughout the organization.

IoT Malware:

IoT malware like Mirai and Brickerbot have illustrated the potential for IoT devices to be compromised the same as any other network enabled computing device. The following controls are not a comprehensive list of IoT security controls, but a list of the security controls most likely to aid in the prevention, mitigation, and remediation of a ransomware attack. This section will just cover controls that apply to the IoT devices themselves. Network controls, etc., such as network segmentation, are critical to proper IoT security, but are covered in other sections.

No Default Credentials:

To date the most common vector for the compromise of IoT devices has been the use of default credentials, such as in the case of Mirai where a list of 62 username and password pairs was used to compromise hundreds of thousands of devices. Simply put, changing the password of your IoT device from the default will help to prevent many current malware strains that target IoT devices.

Account Lockout:

Given the prevalence of IoT malware that uses password guessing attacks, configuring account lockout policies, wherever possible, can help stop many IoT malware variants. Access should be restricted after 3 or more failed attempts.

Spare Copy of Firmware:

In case a device is infected having a spare copy of the devices firmware or a way to reset the device to a like new state can be essential to returning the device to a functional state.

Backup Configuration:

Related to the above control, having all custom configurations and settings backed up can be critical to speedily restoring a device to a functional state.

Restricted Management Interface: Management interfaces should be separate from any Internet facing interfaces wherever possible and the management interface placed on an isolated network segment. Admin access should be restricted to the management interface wherever feasible.

Update Mechanisms: All IoT devices should be configured to regularly receive updates and to ensure that the devices are always running the latest firmware version available.

Vulnerability Management:

All organizations should implement a comprehensive vulnerability management program that is designed to identify all information systems (endpoints, servers, IoT, etc) that are not fully patched and that do not comply with organizationally defined security policies. The program should include provisions for performing corrective actions within a finite period of time with the goal of reducing the organizations attack surface as time goes on. Vulnerability management initiatives should include provisions for continuous monitoring so vulnerabilities can be identified and mitigated as they arise.

Incident Response:

While hopefully all of the above defenses keep incidents to a minimum, organizations need to be prepared for the reality that no matter how controls are in place a ransomware incident is always a possibility.

Incident Response Plans:

One of the worst things an organization can do is wait until an incident occurs to begin to think about how to deal with one. Organizations should have a clear cut plan in place that defines how they will react to an incident and who will be responsible for what actions during the detection, containment, eradication, and recovery phases. It is also important all staff are made aware of the plan and are trained to respond appropriately and effectively. For organizations without any sort of incident response plan in place, a good starting resource is https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Mock Incidents:

When an incident occurs the best way to mitigate the damage is to detect and contain the incident as quickly as possible. The best way to do this is to routinely test your incident response plan to see how people within your organization respond to a mock incident. While there are many mock incidents that could be conducted some recommended starting ones would include a phishing campaign against employees and a simulated malware outbreak, which can be safely done using an EICAR test string.

Data Recovery:

If disaster hits it is better to be able to recover your data and applications from a pre-incident backup than via decryption since this will better help to ensure a clean system going forward, but that may not always be possible. If you find yourself the victim of ransomware, and are stuck without a backup, it may pay to check out the site nomoreransom.org which offers ransomware variant detection based on the upload of a sample file and also hosts the decryption keys for the variants Wildfire, Chimera, Teslacrypt, Shade, Coinvault, Rannoh, and Raknhi.

Insurance:

An increasing number of companies are transferring some of their cyber risks to insurance carriers by taking out policies against data breaches. Some insurance companies now provide policies or provisions within policies that particularly deal with ransomware attacks. Companies in heavily targeted industries may want to consider taking out policies that cover such attacks or determining if their existing policies will cover ransomware attacks.

Indicators of Compromise:

Indicators of compromise can be useful in determining if a system has been exposed to or effected by malware. A nice resource on indicators of compromise for various ransomware variants can be found here: http://goo.gl/b9R8DE

Acknowledgements

Thanks to Adrian Sanabria for raising awareness of PayBreak.

Changelog:

Version 1.1 – Added Sections on Data Recovery, Insurance, and Indicators of Compromise
Version 1.2 – TLD block recommendations added to Proxy Server/Web Filter section
Version 1.3 – Sections on Next-Gen AV and Data Inventory added
Version 1.4 – Added sections on IoT Security and Vulnerability Management
Version 1.5 – Added sections on disabling SMBv1
Version 1.6 – Updated EMET section and added sections on Controlled Folder Access and Paybreak.