EBU

OPERATING EUROVISION AND EURORADIO

R 145

MITIGATION OF RANSOMWARE AND MALWARE ATTACKS

RECOMMENDATION

SOURCE: SP-MCS

Geneva
September 2016

Mitigation of Ransomware and Malware Attacks

EBU Committee	*First Issued*	*Revised*	*Re-issued*
SP-MCS	2016		

Keywords: Information Security, Cybersecurity, IT Security, ransomware, malware, exploit.

Recommendation

The EBU, considering that:

1. Media companies increasingly use Internet Services for media production.
2. The Cyberthreats of malware and ransomware are increasing in number and scope.
3. Typical broadcast systems use CIFS/SMB file shares in production workflows.
4. Critical damage may occur to media or production data if ransomware becomes active in media production environments and encryption of media and production-related files results.

Recommends that:

1. Security awareness training on correct handling of links and attachments included in e-mails is provided to all employees (especially on how to detect phishing attempts).
2. A robust and reliable backup and restore process is implemented; ransomware that is active on Clients or Servers shall not be able to touch these backups;
3. A policy on the accepted private use of company Internet resources and equipment is in place.
4. Access to network resources (e.g. file shares) is granted on a need-to-know basis. This can be effected by;
    a. Applying role based access controls to the file systems.
    b. Restricting write permissions on file servers as far as is possible.
    b. Separating network segments.
5. General security best practice is applied to IT-endpoints, including;
    a. Provisioning and installation of all relevant security-updates to corporate desktops (not just the operating system, but also internet browser, mail client, Java, Flash, etc.)
    b. Secure configuration of every internet connecting software (browser, mail, …)
    c. Installation of Antivirus and zero-day mitigation or intrusion prevention/detection software such as EMET or HIPS.
6. Security Information and Event Management (SIEM) technologies are used, focusing on detecting infections, attacks and suspicious communications.

Proven special technical strategies against ransomware and malware are described in the Annex.

Informative Annex overleaf.

Annex: Special technical strategies against ransomware and malware

1. Pre-Exploitation protection

a. Activate browser malicious URL filtering (e.g. IE Smart Screen Filter, Google Phishing and Malware Protection, Safari Fraudulent Site Protection, Firefox Phishing and Malware Protection)

b. If applicable additional browser extensions should be taken into account to block malicious websites and proactively block advertising networks that are often misused for malware distribution

c. Deploy URL filters that include malware protection (e.g. Proxy with Proxy AV). Be aware that SSL protected websites can only be scanned by AV if SSL-interception is performed.

d. Using sandbox technologies that opens email attachments and remove attachments based on behavioural analysis.

e. Filter all the following attachments on your mail gateway (also inside archives, such as ZIP): .exe, .bat, .ps1, .js, .jse, .scr, .com, .ocx, .jar, .vb, .vbs, .vbe, .bas, .ws, .wsf, .shs, .pif, .hta, .lnk. For High-Security-Environments also filter: .doc(x), .xls(x), .rtf

f. Deploy security gateways that can also detect and filter malicious attachments such as IPS.

2. Exploitation Protection

a. Deploy Anti-Exploit technologies such as Microsoft EMET[1] or Malwarebytes Antiexploit[2].

b. Harden your corporate desktops (at least the most valuable or threatened ones) with a micro virtualisation tool such as Bromium[3] ™

3. Post-Exploitation Protection

a. Disable macros in Microsoft Office files downloaded from the Internet. This can be configured to work in two different modes:

   i. Open downloaded documents in 'Protected View'

   ii. Open downloaded documents and block all macros

b. Disable execution of OLE objects (packager objects) via registry option PackagerPrompt key entry for Microsoft Office files. This can be configured to work in two different modes:

   i. Prompt from Office when user clicks, object executes

   ii. No prompt, Object does not execute

c. Disable Windows Script Host (WSH) on Windows.

d. Disable Powershell on Windows

e. Deploy Application Blacklisting or Whitelisting technologies.

   i. Application Blacklisting

   Block program executions (exe, com and scripts) for the %AppData%, %TEMP% and the user's

[1] https://support.microsoft.com/de-ch/kb/2458544

[2] https://de.malwarebytes.com/antiexploit/

[3] https://www.bromium.com/

download folder (for example with AppLocker[4] or Software Restriction Policies SRP[5]) and all their subfolders on Windows Systems. On macOS consider deploying Google Santa[6]. Be aware that there will be some false positives as there are few software products that also runs code within these folders. Blocking policy may also be implemented by disallowing unsigned software (Applocker and SRP on Microsoft Windows or Gatekeeper[7] and Ostiarius[8] on macOS). Depending on the operating system this might cause many false positives.

ii. Application Whitelisting[9]

Application Whitelisting can be implemented with technologies like Applocker and SRP on Microsoft Windows, Google Santa on macOS or third party applications. Usually a list of applications with hash values is created based on a running applications enumeration. The execution of programs is then globally limited to these applications. This approach will cause many false positives.

f. Show file extension in Explorer or Finder.

i. Windows

Set the registry key "HideFileExt" to 0 in order to show all file extensions in Windows, even of known file types. This helps avoiding cloaking tricks that use double extensions. (e.g. "not_a_virus.pdf.exe").

ii. macOS

Set Finder option "Show all filename extensions[10]"

iii. Discuss this topic in your user awareness trainings.

g. Enforce User Access Control (UAC) on all corporate windows desktops. Administrative users must confirm an action that requires elevated rights.

h. Remove and restrict administrative rights whenever possible. Malware can only modify files that users have write access to.

i. Activate the local firewall to restrict workstation to workstation communication.

j. Use software on your corporate desktops that allows the control of the execution of processes - sometimes integrated in Antivirus products. Free: AntiHook[11], ProcessGuard and System Safety Monitor on Windows and BlockBlock[12] on macOS.

k. Force extensions primarily used for infections on Windows to open up in Notepad rather than Windows Script Host or Internet Explorer.

l. Server-side file screening with the help of File Server Resource Manager.

m. Client-side file screening with the help of special screening tools such as Malwarebytes Anti-Ransomware[13] on Windows or Ransomwhere[14] on macOS.

---

[4] https://technet.microsoft.com/en-us/library/dd759117(v=ws.11).aspx

[5] https://technet.microsoft.com/en-us/library/ee791851(v=ws.11).aspx

[6] https://github.com/google/santa

[7] https://support.apple.com/en-us/HT202491

[8] https://objective-see.com/products/ostiarius.html

[9] http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm#applocker

[10] https://support.apple.com/kb/PH19072?viewlocale=en_US&locale=de_DE

[11] http://virus-protect.org/artikel/tools/antihook.html

[12] https://objective-see.com/products/blockblock.html

[13] https://blog.malwarebytes.com/malwarebytes-news/2016/01/introducing-the-malwarebytes-anti-ransomware-beta/

[14] https://objective-see.com/products/ransomwhere.html

n. Block connection attempts to command and control servers (e.g. via URL Filter, DNS Security or Botnet protection gateways).

o. Turn off autorun; stop network based worms from jumping from USB keys and network drives without changing company polices on Open Shares.

p. Turn on enhanced security in Adobe® Reader; protect your machines from attacks hidden in PDF files by hardening Adobe Reader.

q. Disable Network discovery on corporate desktops.

r. Disable RDP (Remote Desktop Protocol) as much as possible or isolate RDP on specific networks (Admin), as some ransomeware uses RDP infiltration.

s. DropBox / Google Drive/ OneDrive, etc. should not be "on" by default. These should only be started to sync data and then closed when this is completed, in accordance with a stated corporate information security policy.

t. Set browsers to ask users if they wish to activate plugins (Adobe flash, Adobe Reader, Java and Silverlight, etc.)

4. Detection Measures

a. Monitor suspicious process execution on the client (e.g. with Sysinternal Sysmon[15] on Windows or BlockBlock on macOS).

b. Centrally collect security related logfiles (Proxy events, EMET events, AV events, SRP/Applocker/Santa/Ostiarius/BlockBlock events, Sysmon events, …).

c. Make use of Security Information and Event Management Systems (SIEM)

5. Reaction

a. Implement adequate Security Incident Processes to handle detected infections.

b. If legal investigation is desired, follow chain of custody practices. External support might be essential for the forensic investigation.

[15] https://technet.microsoft.com/en-us/sysinternals/bb545027.aspx