EBU

OPERATING EUROVISION AND EURORADIO

R 145

MITIGATION OF RANSOMWARE AND MALWARE ATTACKS

RECOMMENDATION

SOURCE: SP-MCS

Geneva
September 2016

EBU

OPERATING EUROVISION AND EURORADIO

R 145

MITIGATION OF RANSOMWARE AND MALWARE ATTACKS

Внимание!
Данный перевод **НЕ** претендует на аутентичность
и может содержать отдельные неточности.
Оригинал документа на сайте https://tech.ebu.ch

ПРЕДУПРЕЖДЕНИЕ ПОСЛЕДСТВИЙ АТАК ВРЕДОНОСНЫХ И ВЫМОГАТЕЛЬСКИХ ПРОГРАММ

ИСТОЧНИК РЕКОМЕНДАЦИИ: SP-MCS

Женева
Сентябрь 2016

Предупреждение последствий атак вредоносных и вымогательских программ

Комитет EBU	*Первый выпуск*	*Переработка*	*Переиздание*

SP-MCS	2016		

Ключевые слова: Информационная безопасность, Кибербезопасность, IT безопасность, вымогательские программы, вредоносные программы, вредоносный код.

Рекомендация

EBU, учитывая, что:

1. Медиа компании все больше пользуются интернет-услугами для медиа производства.
2. Растет число и масштаб каберугроз от вредоносных и вымогательских программ.
3. Типичные вещательные системы использую т в производственных процессах общий каталог файлов CIFS/SMB.
4. Критические повреждения могут произойти в медиа или производственных данных, если вредоносная программа станет активной в среде медиа производства и в результатах шифрования медиа и производственных файлов.

Рекомендует:

1. Обучение мерам безопасности по корректному обращению со ссылками и приложениями к электронным письмам для всех сотрудников (особенно по обнаружению попыток фишинга).
2. Реализацию надежного процесса восстановления; вредоносные программы, активные в клиентах или серверах, не должны затрагивать эти резервы;
3. Политику приватного использования интернет-ресурсов и оборудования компании.
4. Предоставление доступа к сетевым ресурсам (например, общим каталогам) на основе служебной необходимости. Это может осуществляться посредством:
    a. Применения контроля доступа к файловым системам на базе ролей.
    b. Ограничения разрешения записи в файловых серверах по возможности.
    c. Разделения сегментов сети.
5. Применять передовую практику общей безопасности в конечных точках IT, включая;
    a. Обеспечение и установку всех необходимых обновлений систем безопасности в корпоративные компьютеры (не только операционная система, но и интернет-браузер, почтовый клиент, Java, Flash и т.д.)
    b. Безопасную конфигурацию каждой программы, подключенной к интернету (браузер, почта) Установку антивируса и предупреждения уязвимости нулевого дня или программ для предупреждения / обнаружения вторжений, например, EMET или HIPS.
6. Применять технологии управления информацией о безопасности и событиях (SIEM), сфокусированные на обнаружении заражений, атак и подозрительных коммуникаций.

Испытанные специальные технические стратегии против вредоносных и вымогательских программ описаны в Приложении.

Информативное приложение на обороте.

Приложение: Специальные технические стратегии против вредоносных и вымогательских программ

1. Защита до вторжений

a. Активируйте в браузере фильтрацию вредоносных URL (Например, IE Smart Screen Filter, Google Phishing and Malware Protection, Safari Fraudulent Site Protection, Firefox Phishing и Malware Protection)

b. При необходимости следует учитывать дополнительные расширения браузера для блокировки вредоносных веб-сайтов и сети с упреждающей блокировкой рекламы, которая часто используется для распространения вредоносных программ

c. Внедрите фильтры URL, которые включают защиту от вредоносных программ (например, Proxy с Proxy AV). Убедитесь, что веб-сайты с защитой SSL могут сканироваться только AV при выполнении SSL-перехвата.

d. Используйте технологии «песочницы», которые открывают приложения к электронным письмам и удаляют приложения на основе поведенческого анализа.

e. Фильтруйте все следующие приложения в своем почтовом шлюзе (а также внутри архивов, таких как ZIP): .exe, .bat, .ps1, .js, .jse, .scr, .com, .ocx, .jar, .vb, .vbs, .vbe, .bas, .ws, .wsf, .shs, .pif, .hta, .lnk. Для High-Security-Environments также фильтруйте: .doc(x), .xls(x), .rtf

f. Внедрите защитные шлюзы, способные также обнаруживать и фильтровать вредоносные приложения типа IPS.

2. Защита во время вторжений

a. Внедрите технологии Anti-Exploit типа Microsoft EMET[1] или Malwarebytes Antiexploit[2].

b. Укрепите свои корпоративные компьютеры (по крайней мере, самые ценные или под наибольшей угрозой) инструментом микровиртуализации типа Bromium[3]™

3. Защита после вторжений

a. Отключите макросы в файлах Microsoft Office, скачанных из интернета. Это можно сконфигурировать для работы в двух режимах:

   i. Откройте скачанные документы в 'Protected View'

   ii. Откройте скачанные документы и заблокируйте все макросы

b. Отключите выполнение объектов OLE (объекты упаковщика) через опцию реестра Packager-Prompt key entry для файлов Microsoft Office. Это можно сконфигурировать для работы в двух режимах:

   i. Командная строка из Office, когда пользователь нажимает, объект выполняется

   ii. Без командной строки объект не выполняется

c. Отключите Windows Script Host (WSH) в Windows.

d. Отключите Powershell в Windows

e. Применяйте технологии Application Blacklisting или Whitelisting.

   i. Application Blacklisting

   Блокируйте выполнение программ (exe, com и скрипты) для %AppData%, %TEMP% и пользовательской папки загрузки (например, с помощью AppLocker[4] или Software Restriction Policies SRP[5]) и все их подпапки в Windows Systems. В macOS используйте Google Santa[6]. Имейте в

[1] https://support.microsoft.com/de-ch/kb/2458544
[2] https://de.malwarebytes.com/antiexploit/
[3] https://www.bromium.com/
[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

виду, что будут ложные результаты, т.к. некоторые программные продукты также запускают код в этих папках. Политику блокировки также можно реализовать путем запрета беззнакового ПО (Applocker и SRP в Microsoft Windows или Gatekeeper[7] и Ostiarius[8] в macOS). В зависимости от операционной системы это может вызвать много ложных результатов.

ii. Application Whitelisting[9]

Application Whitelisting можно реализовать технологиями типа Applocker и SRP в Microsoft Windows, Google Santa в macOS и сторонних приложений. Обычно создается список приложений с хеш-значениями на основе нумерации запущенных приложений. Выполнение программ тогда глобально ограничивается этими приложениями. Такой подход вызовет много ложных результатов.

f. Покажите расширение файлов в Explorer или Finder.

i. Windows

Установите ключ реестра "HideFileExt" на 0 для показа всех расширений файлов в Windows даже известных типов. Это поможет избежать маскировки с использованием двойных расширений (например, "not_a_virus.pdf.exe").

ii. macOS

Установите опцию Finder “Show all filename extensions”[10]

iii. Обсудите эту тему на обучении пользователей.

g. Включите User Access Control (UAC) во всех корпоративных компьютерах с Windows. Административные пользователи должны подтверждать действие, требующее расширенных прав.

h. По возможности удаляйте и ограничивайте административные права. Вредоносные программы могут изменять только файлы, к которым у пользователей есть доступ к записи.

i. Активируйте локальный файрвол для ограничения связи между рабочими станциями.

j. Используйте в корпоративных компьютерах программы, позволяющие контроль выполнения процессов – иногда интегрированные в антивирусные продукты. Бесплатные: AntiHook[11], ProcessGuard и System Safety Monitor в Windows и BlockBlock[12] в macOS.

k. Заставьте расширения, первично используемые для заражения в Windows, открываться в Notepad вместо Windows Script Host или Internet Explorer.

l. Фильтрация файлов со стороны сервера с помощью File Server Resource Manager.

m. Фильтрация файлов со стороны клиента с помощью специальных инструментов типа Malwarebytes Anti-Ransomware[13] в Windows или Ransomwhere[14] в macOS.

n. Блокируйте попытки соединения с командным и контрольным сервером (например, через URL Filter, DNS Security или защитные шлюзы Botnet).

o. Отключите автозапуск; остановите выскакивание сетевых «червей» из USB-ключей и сетевых накопителей, не меняя политики компании по Open Shares.

p. Включите расширенную защиту в Adobe® Reader; защитите свои машины от атак, скрытых в файлах PDF, укрепив Adobe Reader.

q. Отключите Network discovery в корпоративных компьютерах.

r. По возможности отключите RDP (Remote Desktop Protocol) или изолируйте RDP в специальных сетях (Admin), т.к. некоторые вредоносные программы используют несанкционированный доступ к RDP.

---

[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

s. DropBox / Google Drive/ OneDrive и т.д. не должны быть "on" по умолчанию. Они должны запускаться только для синхронизации данных и затем закрываться после ее завершения в соответствии с утвержденной политикой информационной безопасности компании.

t. Установите браузеры, чтобы они спрашивали пользователей, желают ли они активировать плагины (Adobe flash, Adobe Reader, Java, Silverlight и т.д.)

4. Меры обнаружения

a. Контролируйте выполнение подозрительных процессов в клиенте (например, с помощью Sysinternal Sysmon[15] в Windows или BlockBlock в macOS).

b. Централизованно собирайте журнальные файлы, связанные с безопасностью (события Proxy, EMET, AV, SRP/Applocker/Santa/Ostiarius/BlockBlock, Sysmon, …).

c. Используйте Security Information и Event Management Systems (SIEM)

5. Реагирование

a. Реализуйте адекватные процессы обнаружения нарушения безопасности для контроля вторжений.

b. При необходимости адвокатского расследования следуйте практике предварительного ареста. Для судебной экспертизы может потребоваться внешняя поддержка.

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