CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 15.05.2020 г.

Съдържание

Новият зловреден софтуер Ramsay може да открадне данни от air-gapped компютри

14 май 2020

С цел противопоставяне на уязвимостите, открити в свързаните с интернет машини, видяхме, че нараства използването на air-gapped компютри. Тези компютри са напълно изолирани от всяка външна мрежа, за да бъде повишена сигурността.

Въпреки това през последните няколко години видяхме air-gapped злонамереният софтуер да става все по-разпространен.

Този злонамерен софтуер позволява да бъдат откраднати различни документи, включително Word, PDF и Zip файлове, и след това обратно предадени на нападателите, въпреки че не е известно как точно става това предаване.

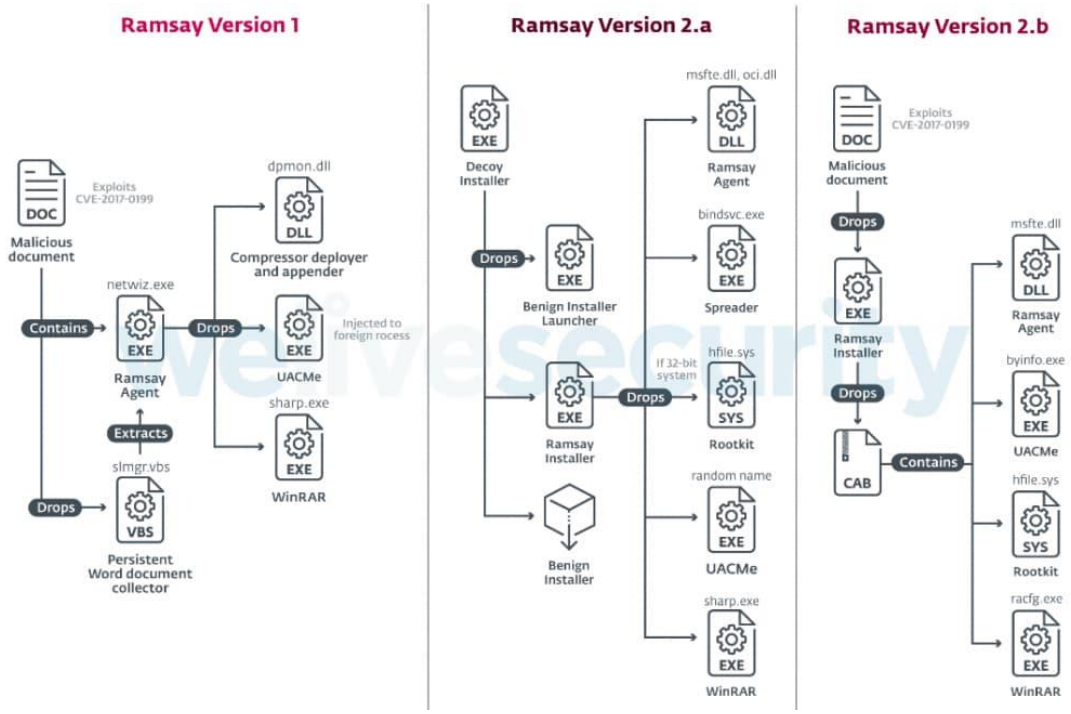
Зловреднният софтуер на име Ramsay има 3 различни версии, всяка от които е съставена на различни дати и функционира по различен начин:

1. Ramsay v1 - септември 2019

2. Ramsay v2.a - март 2020 г.

3. Ramsay v2.b - март 2020 г.

Във v1 зловреднният софтуер използва документи, които съдържат зловреден визуален основен скрипт, наречен „OfficeTemporary.sct“, вграден в JPG файл. Веднъж зареден, този скрипт отприщва „Ramsay agent“, оставяйки зловредния софтуер да свърши своята работа.



Изследователите смятат, че последвалите версии на Ramsay са по-сложни по своята същност. Те включват „компонент за разпространение“, който се използва за заразяване на преносими изпълними файлове (PE), които могат да бъдат открити както в преносими, така и в мрежови устройства.

За повече информация:

https://www.hackread.com/ramsay-malware-steal-data-air-gapped-computers/

Пачнали ли сте тези топ 10 рутинно експлоатирани уязвимости

15 май 2020

Американската агенция за сигурност в киберсигурността и инфраструктурата (CISA) призовава организациите да пачнат редица стари и нови софтуерни уязвимости, които рутинно се използват от киберпрестъпници.

Киберпрестъпниците продължават да използват обществено известни софтуерни уязвимости срещу широки целеви групи, включително организации от публичния и частния сектор. Експлоатацията на тези уязвимости често изисква по-малко ресурси в сравнение с 0-day експлоатация, за която няма налични пачове.

Най-често използваните уязвимости

Списъкът с десетте най-често експлоатирани недостатъка между 2016 и 2019 г. включва седем, засягащи предложенията на Microsoft (Office, Windows, SharePoint, .NET Framework), един засяга Apache Struts, един Adobe Flash Player и един Drupal.

Те са както следва:

- CVE-2017-11882
- CVE-2017-0199
- CVE-2017-5638
- CVE-2012-0158
- CVE-2019-0604
- CVE-2017-0143
- CVE-2018-4878
- CVE-2017-8759
- CVE-2015-1641
- CVE-2018-7600

На специалистите в областта на информационната сигурност се препоръчва да използват този списък заедно с подобен наскоро съставен от Recorded Future, който се фокусира върху десетте най-експлоатирани уязвимости от киберпрестъпниците през 2019 г.

В допълнение към всички тези недостатъци, CISA посочва още няколко, които са силно експлоатирани през 2020 г .:

CVE-2019-11510 (засяга Pulse Secure VPN сървъри)

CVE-2019-19781 (засяга устройствата Citrix VPN)

CISA предупреди организациите да проверят и за пропуски в техните конфигурации за сигурност на Microsoft Office 365.

Март 2020 г. доведе до рязка промяна - на работа от дома, която наложи за много организации бързо внедряване на облачни услуги за сътрудничество като

Microsoft Office 365. Нападателите се насочват към организации, чието прибързано внедряване на Microsoft O365 може да доведе до пропуски в конфигурациите за сигурност, което да ги направи уязвими на атака.

За повече информация:

https://www.helpnetsecurity.com/2020/05/13/routinely-exploited-vulnerabilities/