Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ЗАМЕСТНИК МИНИСТЪР-ПРЕДСЕДАТЕЛ ПО ЕФЕКТИВНО УПРАВЛЕНИЕ

№ 01.01-109
27.05. 2022 г.

НАРОДНО СЪБРАНИЕ
Вх.№ 47-254-06-1644
Дата 27 / 05 2022

15.49

ЧРЕЗ
ПРЕДСЕДАТЕЛЯ НА НАРОДНО СЪБРАНИЕ
Г-Н НИКОЛА МИНЧЕВ

ДО
НАРОДНИТЕ ПРЕДСТАВИТЕЛИ В
47-ТО НАРОДНО СЪБРАНИЕ
Г-ЖА ИННА ИВАНОВА И
Г-Н БЛАГОСВЕСТ КИРИЛОВ

На Ваш № 47-254-06-1644 от 20.5.2022 г.

УВАЖАЕМА ГОСПОЖО ИВАНОВА
УВАЖАЕМИ ГОСПОДИН КИРИЛОВ,

Във връзка с постъпил от Вас въпрос относно *„Кибератака срещу „Български пощи" ЕАД"*, Ви уведомявам за следното.

Информация за вектори на проведената атака - откъде е била входната точка - тип терминал, експлойт на ОС или на приложен софтуер, отворен файл, засегната инфраструктура и масиви от данни, вкл. какъв е обхватът на невъзстановяемите масиви, заедно с мостра от криптиран файл?

Инфраструктурата на „Български пощи" ЕАД включва Microsoft Windows Server 2019 Datacenter - Windows Server 2019 Hyper-V Failover Cluster. Виртуалната среда е конфигурирана и се управлява през System Center 2019 - Virtual Machine Manager Server. Създадени са виртуални сървъри за различни цели - домейн контролери, SQL сървъри, терминални сървъри, web сървъри, апликейшън сървъри, файлови сървъри, Exchange Server 2016 и т.н. Базите данни са реализирани на Microsoft SQL 2019. Сървърите SQL и файловите сървъри са конфигурирани в Guest Failover Clusters от виртуални машини, с цел отказоустойчивост.

Ransomware и други злонамерени програми се разпространяват главно чрез троянски коне, спам кампании, незаконни инструменти за активиране („кракове"), фалшиви актуализации и ненадеждни канали за изтегляне. Последните 2 години бяха забелязани масирани спам и фишинг кампании към мрежата на Български пощи ЕАД.

Предполагаем вектор на проведената атака - входната точка са 2600 броя физически и морално остарели работни станции с операционна система Windows XP и Windows 7, което създава предпоставки за пробив в сигурността на мрежата, като многократно е увеличен рискът за проникване в инфраструктурата на дружеството. На тези работни станции е невъзможно да се поддържа съвременен антивирусен софтуер, който ежедневно да се обновява. Използвана е и уязвимост в сигурността на Microsoft Exchange Server, която позволява на хакерите да имат достъп до вътрешни регистри на Windows, използвайки „cmdlets" на Microsoft Exchange. Това включва: права за дистанционно изпълнение на команди на PowerShell, пароли за потребителските акаунти и ключовете за тяхното декриптиране, и създаване на нов/използване на съществуващ администраторски акаунт.

В периода декември 31.12.2021 г.-03.01.2022 г. е имало глобален срив на Microsoft Exchange Server, който е прекъснал ползването на услугите и възстановяване им е предизвикало редица затруднения. Наложило се е прилагане на ъпдейт за Exchange Server, след който се е наблюдавало забавяне в работата му. Използван за нуждите на дружеството пощенски сървър е Exchange Server 2016 с Cumulative Update 3 (CU3). За смекчаване срещу ProxyShell, инсталациите на Exchange 2016 е трябвало да бъдат актуализирани поне до версията 2019 CU19, като актуализацията не е била осъществена поради старата информационна архитектура (домейн контролер Windows Server 2008R2).

Установено е използване на зловреден софтуер Mimikatz за компрометиране на потребителски идентификационни данни от злонамерени лица, за да получат неоторизиран достъп до системите на Windows. Чрез инструмента е придобита и модифицирана Администраторска парола на SQL administrator, чрез която е извършено криптиране на базите данни.

Повредените от криптовирус бази данни са с обем на базите от 2 TB и архив 1 TB.

Приложение: снимка „мостра" на криптирани файлове от заразената среда.

С УВАЖЕНИЕ,

ЗАМЕСТНИК МИНИСТЪР-ПРЕДСЕДАТЕЛ
ПО ЕФЕКТИВНО УПРАВЛЕНИЕ:

КАЛИНА КОНСТАНТИНОВА

AIA

Share View

› This PC › S2_SQL WEB DATA (D:) › MSSQL15.BGPOST_APP_DATA › MSSQL › DATA

Search DATA

Name	Date modified	Type	Size
Admin_Task_55.mdf.[AA6F3BD5].@Thomasdecryption	16.12.21 22:36	@THOMASDECRYPTION File	8 196 KB
BGPOST_Report.mdf.[AA6F3BD5].@Thomasdecryption	16.04.22 01:59	@THOMASDECRYPTION File	610 500 KB
BGPOST_ReportTempDB.mdf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:17	@THOMASDECRYPTION File	11 700 420 KB
IPSWebTrackingDb.mdf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:16	@THOMASDECRYPTION File	43 944 452 KB
KIP.mdf.[AA6F3BD5].@Thomasdecryption	18.03.22 14:04	@THOMASDECRYPTION File	31 677 700 KB
master.mdf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:17	@THOMASDECRYPTION File	5 508 KB
mastlog.ldf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:17	@THOMASDECRYPTION File	2 052 KB
model.mdf.[AA6F3BD5].@Thomasdecryption	16.12.21 22:36	@THOMASDECRYPTION File	8 196 KB
model_msdbdata.mdf.[AA6F3BD5].@Thomasdecryption	24.09.19 15:09	@THOMASDECRYPTION File	13 700 KB
model_msdblog.ldf.[AA6F3BD5].@Thomasdecryption	24.09.19 15:09	@THOMASDECRYPTION File	516 KB
model_replicatedmaster.ldf.[AA6F3BD5].@Thomasdecryption	24.09.19 15:09	@THOMASDECRYPTION File	516 KB
model_replicatedmaster.mdf.[AA6F3BD5].@Thomasdecryption	24.09.19 15:09	@THOMASDECRYPTION File	4 548 KB
modellog.ldf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:17	@THOMASDECRYPTION File	8 196 KB
MS_AgentSigningCertificate.cer.[AA6F3BD5].@Thomasdecryption	14.10.20 16:08	@THOMASDECRYPTION File	5 KB
MS_AgentSigningCertificateAA07C939-E80F-4E18-8D95-69AC76B4DC73.cer.[...	30.04.21 15:06	@THOMASDECRYPTION File	5 KB
MSDBData.mdf.[AA6F3BD5].@Thomasdecryption	15.04.22 23:16	@THOMASDECRYPTION File	22 212 KB
MSDBLog.ldf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:17	@THOMASDECRYPTION File	10 180 KB
POSTMONEYTRANSFER.mdf.[AA6F3BD5].@Thomasdecryption	16.04.22 02:17	@THOMASDECRYPTION File	51 302 340 KB
TRACE_Nomenclatures.mdf.[AA6F3BD5].@Thomasdecryption	16.04.22 00:03	@THOMASDECRYPTION File	519 273 476 KB

X00-413-1

:)

DATA (D:)

LOG (M:)

TEMP (S:)