بسمه‌تعالی

گزارش رسیدگی و پاسخگویی حمله‌ی سایبری به وب‌سایت‌ها و پورتال‌های خبری

در آستانه‌ی برگزاری راهپیمایی باشکوه ۲۲ بهمن‌ماه در روز شنبه مورخ ۲۱ بهمن‌ماه حدود ساعت ۲۰ الی ۲۲ اخباری در خصوص حمله به تعدادی از پورتال‌ها و وب‌سایت‌های خبری منتشر و باعث ایجاد نگرانی‌هایی در سطح جامعه شد. مرکز ماهر وزارت ارتباطات و فناوری اطلاعات موضوع را سریعا مورد بررسی قرار داده و اقدامات فنی لازم را در این خصوص بعمل آورد. جهت اطلاع و رعایت نکات مهم مطرح در این زمینه، توضیح اجمالی حمله فوق در گزارش حاضر آمده است.

وب‌سایت‌های خبری که مورد حمله قرار گرفته‌اند شامل: روزنامه‌ی قانون، روزنامه‌ی آرمان، روزنامه ستاره صبح بوده که در مرکز داده‌ی تبیان و مرکز داده شرکت پیشتاز میزبانی شده‌اند . گروه فنی مرکز ماهر اقدام به شناسایی نقاط اشتراک سیستم‌های هدف نموده و در این فرایند مشخص گردیده که تمامی این سامانه ها توسط یک شرکت و در بستر سیستم‌عامل ویندوز با سرویس‌دهنده‌ی وب IIS و زبان برنامه‌نویسی ASP.Net توسعه داده شده اند.

شرکت تولید کننده نرم افزار این سامانه ها مجری بیش‌از ۳۰ وب‌سایت خبری به شرح زیر در کشور می‌باشد که نفوذگران از این حیث به مجموعه اهداف مناسبی دست پیدا نمودند. تهدید اخیر کماکان برای این سایت ها وجود دارد و لازم است سریعا تمهیدات امنیتی مناسب را اعمال نمایند.

1- armandaily.ir

2- aminejameeh.ir
3- kaenta.ir
4- ghanoondaily.ir
5- asreneyriz.ir
6- sharghdaily.ir
7- ecobition.ir
8- karoondaily.ir
9- baharesalamat.ir
10- tafahomnews.com
11- bankvarzesh.com
12- niloofareabi.ir
13- shahrvand-newspaper.ir
14- etemadnewspaper.ir
15- vareshdaily.ir
16- bahardaily.ir
17- nishkhat.ir

18- sayeh-news.com
19- nimnegahshiraz.ir
20- shahresabzeneyriz.ir
21- neyrizanfars.ir
22- sarafrazannews.ir
23- tweekly.ir
24- armanmeli.ir
25- davatonline.ir
26- setaresobh.ir
27- noavaranonline.ir
28- bighanoononline.ir
29- naghshdaily.ir
30- hadafeconomic.ir

اقدامات فنی اولیه توسط مرکز ماهر به شرح زیر صورت پذیرفت:

- شناسایی دارایی های مرتبط با سامانه‌ها جهت تحلیل دقیق(در این زمینه متاسفانه مرکز داده تبیان هیچگونه همکاری را بعمل نیاورده است)
- از دسترس خارج نمودن سامانه‌های که مورد حمله قرار گرفته‌اند، جهت بازیابی و حذف تغییرات در محتوی پیام‌ها
- تغییر و یا غیرفعال سازی نام‌کاربری اشتراکی و پیش‌فرض در تمامی سامانه‌ها
- ایجاد یک Snapshot و همچنین یک کپی سالم و دست نخورده از سرویس‌دهنده‌های مجازی که مورد حمله قرار گرفته‌اند
- کپی کامل از تمامی فایل‌های ثبت وقایع بر روی سرویس‌دهنده‌های هدف

پس از دریافت فایل‌های ثبت وقایع از حملات انجام شده از سرویس‌دهنده‌ها با تحلیل و بررسی تاریخچه‌ی حملات و آسیب‌پذیری‌ها حجم بالایی از فایل‌ها مورد تحلیل و آنالیز قرار گرفت و آی‌پی مبدا حملات استخراج شد که شامل ۵ آی‌پی از کشورهای انگلستان ، آمریکا و بلغارستان بوده است.

جدول شماره‌ی ۱ – لیست آدرس‌های IP حمله کننده

ردیف	آدرس‌های IP حمله کننده	مبدا حمله	فراهم کننده‌سرویس
۱	93.155.130.14	Bulgaria	ITSERVICE09_GCN, AS47453

۲	212.113.128.230	United Kingdom	GYRON-AGG Gyron Internet Ltd, AS29017
۳	67.222.20.186	Seattle, Washington, United States	PrivateSystems Networks, AS63410
٤	162.223.90.211	United States, Wilmington	ColoUp, AS19084
٥	162.223.91.228	United States, Wilmington	ColoUp, AS19084

شواهد موجود در فایل‌های ثبت وقایع نشان می‌دهد که مهاجمان از دو روز قبل (از تاریخ 08/02/2018 الی 10/02/2018) پس از کشف آسیب‌پذیری‌های از قبیل انواع Injectionها، در تلاش جهت نفوذ با ابزارهای خودکار و نیمه‌خودکار جهت استخراج اطلاعات نظیر نام‌کاربری و کلمات عبور در پایگاه‌داده‌ی سامانه‌ها بوده‌اند. تمامی فعالیت‌ها و عملیات مخرب جهت کشف آسیب‌پذیری و نفوذ به سامانه‌ها، که متعلق به آدرس‌های IP حمله کننده استخراج و بررسی شد.

اقدامات اصلاحی انجام شده:

۱-تغییر نام کاربری و کلمه عبور پیش فرض راهبر سامانه در تمامی محصولات شرکت

توضیح مهم در این زمینه:

تمامی سایت های خبری مورد حمله دارای نام‌کاربری و کلمه‌ی عبور پیش‌فرض (*****) و یکسان توسط شرکت پشتیبان بوده‌است. همچنین در بررسی مشخص گردید که متاسفانه آدرس پست‌الکترونیکی راهبر ارشد سامانه با سطح دسترسی بالا برابر *****@gmail.com می‌باشد که نام‌کاربری و کلمه ی عبور استفاده شده در سایت‌ها نیز همان می‌باشد.این موارد نشان می‌دهد متاسفانه حداقل موارد امنیتی رعایت نشده است

۲-اطلاع رسانی به تمامی دارندگان و استفاده‌کنندگان محصول شرکت مورد هدف

۳-کشف ماژول‌ها و بخش‌های آسیب‌پذیر در سایت‌های مورد حمله و اطلاع به پشتیبان جهت وصله امنیتی سریع

۴-هشدارها و راهنمایی‌های لازم جهت حفاظت و پیکربندی و مقاوم‌سازی سرویس‌دهنده و فایل ثبت وقایع بر روی تمامی سرویس دهنده ها

۵-اقدامات لازم برای انجام آزمون نفوذپذیری بر روی تمامی بخش‌ها و ماژول‌های سامانه مشترک