

## 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 سریعاً 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 سامانه‌ها توسط یک شرکت و در بستر سیستم‌عامل ویندوز با سرویس‌دهنده‌ی وب IIS و زبان برنامه‌نویسی ASP.Net توسعه داده شده‌اند.

شرکت تولید کننده نرم افزار این سامانه‌ها مجری بیش از 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 سایت‌ها وجود دارد و لازم است سریعاً تمهیدات امنیتی مناسب را اعمال نمایند.

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

- 18- [sayeh-news.com](http://sayeh-news.com)
- 19- [nimnegahshiraz.ir](http://nimnegahshiraz.ir)
- 20- [shahresabzeneyriz.ir](http://shahresabzeneyriz.ir)
- 21- [neyrizanfars.ir](http://neyrizanfars.ir)
- 22- [sarafranzannews.ir](http://sarafranzannews.ir)
- 23- [tweekly.ir](http://tweekly.ir)
- 24- [armanmeli.ir](http://armanmeli.ir)
- 25- [davatonline.ir](http://davatonline.ir)
- 26- [setaresobh.ir](http://setaresobh.ir)
- 27- [noavaranonline.ir](http://noavaranonline.ir)
- 28- [bighanoonline.ir](http://bighanoonline.ir)
- 29- [naghshdaily.ir](http://naghshdaily.ir)
- 30- [hadafeconomic.ir](http://hadafeconomic.ir)

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

- شناسایی دارایی های مرتبط با سامانه ها جهت تحلیل دقیق (در این زمینه متاسفانه مرکز داده تبیان هیچگونه همکاری را بعمل نیاورده است)
  - از دسترس خارج نمودن سامانه های که مورد حمله قرار گرفته اند، جهت بازبانی و حذف تغییرات در محتوی پیام ها
  - تغییر و یا غیرفعال سازی نام کاربری اشتراکی و پیش فرض در تمامی سامانه ها
  - ایجاد یک Snapshot و همچنین یک کپی سالم و دست نخورده از سرویس دهنده های مجازی که مورد حمله قرار گرفته اند
  - کپی کامل از تمامی فایل های ثبت وقایع بر روی سرویس دهنده های هدف
- پس از دریافت فایل های ثبت وقایع از حملات انجام شده از سرویس دهنده ها با تحلیل و بررسی تاریخچه ی حملات و آسیب پذیری ها حجم بالایی از فایل ها مورد تحلیل و آنالیز قرار گرفت و آی پی مبدا حملات استخراج شد که شامل ۵ آی پی از کشورهای انگلستان و آمریکا بوده است.

جدول شماره ی ۱ – لیست آدرس های IP حمله کننده

ردیف	آدرس های IP حمله کننده	مبدا حمله	فراهم کننده سرویس
۱	93.155.130.14	United Kingdom	ITSERVICE09_GCN, AS47453

GYRON-AGG Gyron Internet Ltd, AS29017	United Kingdom	212.113.128.230	۲
PrivateSystems Networks, AS63410	Seattle, Washington, United States	67.222.20.186	۳
ColoUp, AS19084	United States, Wilmington	162.223.90.211	۴
ColoUp, AS19084	United States, Wilmington	162.223.91.228	۵

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 نام کاربری 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 سایت‌های خبری مورد حمله دارای نام کاربری 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 نام کاربری و کلمه‌ی 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