مرکز تخصصی

آپا دانشگاه کردستان

گزارش تهدیدات ماهانه(ماه‌های مارچ و آوریل)

فرشته کیاست

شماره سند: A97013

۱۳۹۷/۰۲/۱۹

www.cert.uok.ac.ir
apa@uok.ac.ir
087-33662932

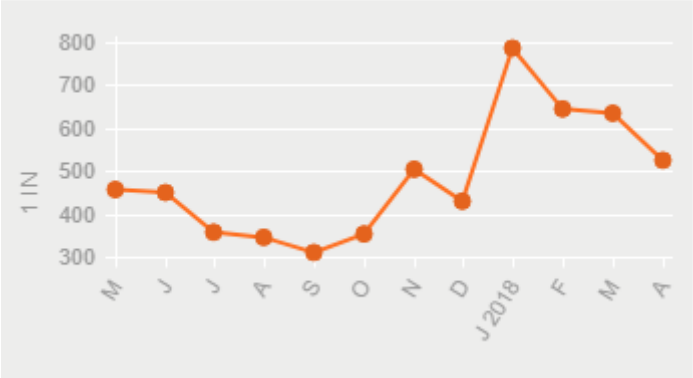
Symantec Security Response یک تیم جهانی از مهندسان امنیت، تحلیلگران تهدید و محققانی است که محتوای متنوعی را در مورد آخرین تهدیدات که سازمانها و کاربران نهایی را تحت تاثیر قرار می دهد، توسعه می دهد. در این گزارش مروری بر تهدیدات مربوط به بدافزارها، اسپم، حملات فیشینگ و رسانه اجتماعی و موبایل در چند ماه اخیر به ویژه ماه های مارچ و آوریل ارائه شده است. این گزارش بر گرفته از تحقیقات مرکز گزارش گیری تهدیدات امنیتی اینترنت (https://www.symantec.com/security-center/threat-report) است.

۱- Malware

تعداد ایمیل‌های حاوی بدافزار در ماه آوریل افزایش یافته و به یک در ۲۵۶ ایمیل رسید.

این تعداد در ماه ژانویه کمترین تعداد یعنی یک در ۷۸۶ ایمیل رسید.

کسب وکارهای کوچک با تعداد کارمندان یک تا ۲۵۰ دارای بالاترین میزان نرم افزارهای مخرب بودند. یعنی از هر ۳۷۲ ایمیل یک ایمیل حاوی بدافزار بود. در شکل ۱ نمودار تعداد ایمیل‌های مخرب در چند ماه اخیر نشان داده‌شده است. در شکل ۲ نمودار مربوط به ایمیل‌های حاوی بدافزار مربوط به صنایع مختلف آورده شده است



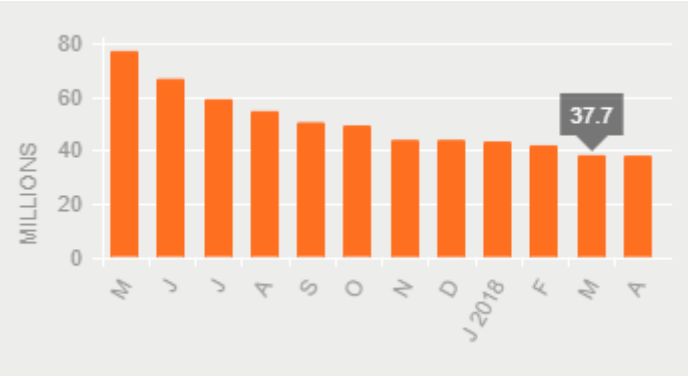
شکل ۱ نمودار ایمیل‌های حاوی بدافزار در ماه های اخیر

Rank	Industry	Apr '18 (1 in)	Mar '18 (1 in)
1	Mining	285	308
2	Agriculture, Forestr...	342	453
3	Manufacturing	383	466
4	Public Administratio...	446	574
5	Wholesale Trade	455	549

شکل ۲ نمودار ایمیل‌های حاوی بدافزار در صنایع مختلف

Company Size	Apr '18 (1 in)	Mar '18 (1 in)
1-250	372	488
251-500	385	484
501-1000	519	694
1001-1500	1005	1208
1501-2500	565	716

شکل ۳ نمودار ایمیل‌های حاوی بدافزار بر اساس اندازه سازمان



شکل ۴ نمودار تعداد بدافزارهای جدید

۲- Spam

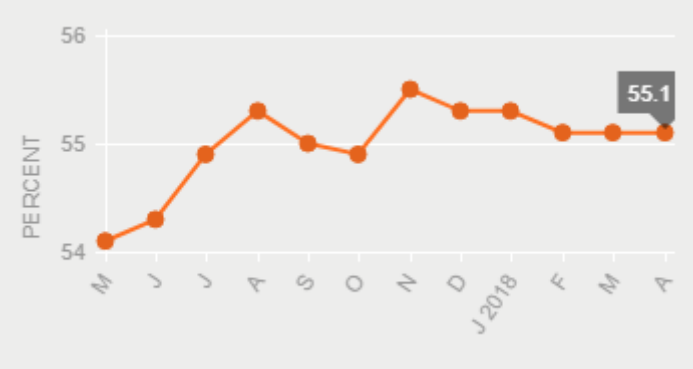
در دو ماه گذشته ۵۵ درصد اسپم های جهانی باقی مانده اند.

از ابتدای ماه فوریه نرخ کلی اسپم ۰,۰۷ بوده است.

بخش معدن در ماه آوریل ۵۸,۶ درصد تعداد اسپم را داشته است.

بخش های مالی، بیمه و املاک با نرخ ۵۷,۲ درصد اسپم در در رتبه دوم قرار دارند.

سازمان های با ۱۰۰۱ الی ۱۵۰۰ کارمند نیز بالاترین تعداد اسپم را داشته اند.



شکل ۵ نمودار درصد تعداد اسپم در ماه های اخیر

Rank	Industry	Apr '18 (%)	Mar '18 (%)
1	Mining	58.6	57
2	Finance, Insurance, ...	57.2	56.2
3	Public Administratio...	56.1	55.2
4	Manufacturing	55.9	56.2
5	Nonclassifiable Esta...	54.2	55.7

شکل ۶ درصد اسپم های جهانی در صنایع مختلف

Company Size	Apr '18 (%)	Mar '18 (%)
1-250	55.9	55
251-500	53.9	53.8
501-1000	54.5	54.5
1001-1500	56.5	56.7
1501-2500	54	53.9

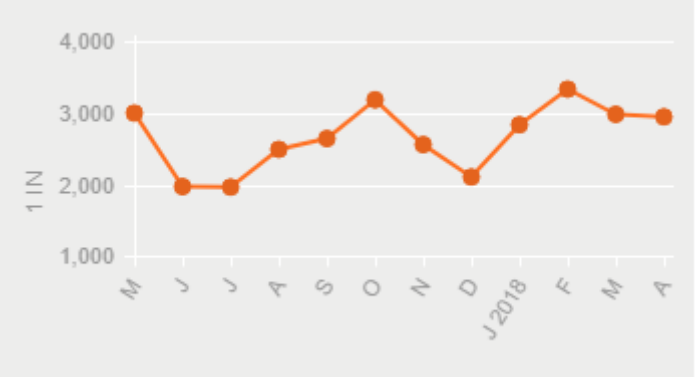
شکل ۷ درصد اسپم های جهانی در دو ماه گذشته بر اساس اندازه سازمان ها

۳- Fishing

نرخ فیشینگ در ماه آوریل به یک ایمیل در ۲۹۴۶ ایمیل رسید.

Mining دارای رتبه دوم فیشینگ با تعداد ایمیل ۱ در ۲۳۲۳ ایمیل بود.

کسب وکارهای کوچک با حداکثر ۲۵۰ کارمند در ماه آوریل دارای بیشترین تعداد فیشینگ بوده اند.



شکل ۸ نمودار ۱ ایمیل حاوی فیشینگ در n ایمیل

Rank	Industry	Apr '18 (1 in)	Mar '18 (1 in)
1	Agriculture, Forestr...	1802	1394
2	Mining	2323	2499
3	Manufacturing	2741	3749
4	Wholesale Trade	2744	3830
5	Nonclassifiable Esta...	2889	4192

شکل ۹ حملات فیشینگ در صنایع مختلف

Company Size	Apr '18 (1 in)	Mar '18 (1 in)
1-250	2510	2978
251-500	2700	3078
501-1000	3270	3989
1001-1500	5307	6433
1501-2500	3136	3086

شکل ۱۰ حملات فیشینگ در دو ماه اخیر بر اساس سایز سازمان‌ها

۴- رسانه اجتماعی و موبایل

کلاهبرداری های مربوط به انتشار رسانه های اجتماعی تقلبی در ماه آوریل به ۳۵,۵۶ رسیده است.

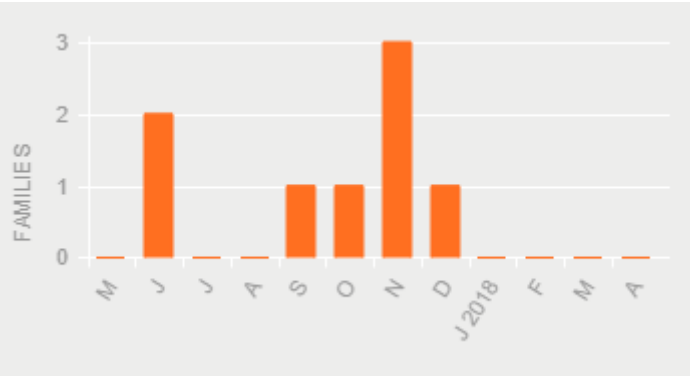
Manual Sharing در ماه آوریل به میزان ۲۸,۹۶ تا ۲۹,۹۴ کاهش یافته است.

Like Jacking در رتبه سوم از ۲۹,۱۴ درصد به ۲۹,۶۵ رسیده است.

در ماه آوریل هیچ خانواده جدیدی از تروجان های اندرویدی کشف نشده است.

Rank	Type	Apr '18 (%)	Mar '18 (%)
1	Fake Offer	38.56	10.49
2	Manual Sharing	29.94	58.9
3	Like Jacking	29.65	29.14
4	Fake App	1.05	0.69
5	Copy-Paste	0.21	0.14

شکل ۱۱ کلاهبرداری های رسانه اجتماعی



شکل ۱۲ خانواده های جدید از بدافزارهای اندروید