مرکز تخصصی
آپا دانشگاه کردستان

گزارش وضعیت امنیتی ایران و جهان در ماه گذشته

هادی گلباغی

شماره سند: A97006

۱۳۹۷/۲/۸

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

گزارش وضعیت امنیتی ایران و جهان در ماه گذشته

گزارش تاریخ : ۱۴ مارس تا ۱۳ آوریل

با توجه به افزایش شدید حملات سایبری در طی یک سال گذشته و لزوم آمادگی و اتخاذ راهبردی مناسب در مقابل این حملات برای نفوذ به سامانه‌های حساس کشور، تهیه گزارش‌های امنیتی در خصوص آسیب‌پذیری‌های کشف شده بصورت هفتگی و ماهانه و اطلاع‌رسانی ضروری به نظر می‌رسد. بسیاری از تهدیداتی که در سطحی وسیع در جهان گسترش پیدا کرده‌اند در ابتدا تهدیداتی در سطحی کوچک بوده‌اند که می‌شد با اطلاع‌رسانی صحیح و به موقع از انتشار آن جلوگیری به عمل آورد. با بررسی تهدیدات هفتگی و ماهانه و گزارش آن تا حد زیادی می‌توان چشم‌اندازی از تهدیدات آینده داشت و تمهیداتی را پیش از جدی شدن آن رخداد و تهدید، اتخاذ کرد.

در ماه گذشته نکاتی بسیار مورد توجه قرار گرفت و بعضاً موجبات ایجاد تخریب را ایجاد کرده‌اند. یکی از این موارد آسیب‌پذیری‌های بسیار حساس و بحرانی کشف شده از شرکت سیسکو و دروپال بوده که نیازمند نصب وصله‌های امنیتی متعددی در این ماه گذشته بوده‌اند. همچنین گوگل کروم نیز آسیب‌پذیری‌های چندگانه‌ای را با ارائه وصله‌های امنیتی بر طرف نمود که در مواردی حساس نیز بوده‌اند. نکته‌ای در ماه گذشته بیشتر نمود پیدا کرد و باید بسیار مورد توجه قرار گیرد مدنظر قرار دادن وصله‌های امنیتی منتشر شده و نصب فوری آن‌ها در اسرع وقت است که سرعت بهره‌بردای و تخریب از طریق آسیب‌پذیری‌های منتشر شده با سرعت بسیار بیشتری نسبت به گذشته در حال انجام است و با نصب وصله‌های امنیتی منتشر شده روزانه تا حد بسیاری می‌توان از این موارد پیشگری نمود.

این گزارش در چند بستر تهیه می‌شود که حوزه‌های آن به صورت زیر می‌باشد.

- **Local Infections**
- **Web threats**
- **Network Attacks**
- **Exploited Vulnerability**
- **Spam**

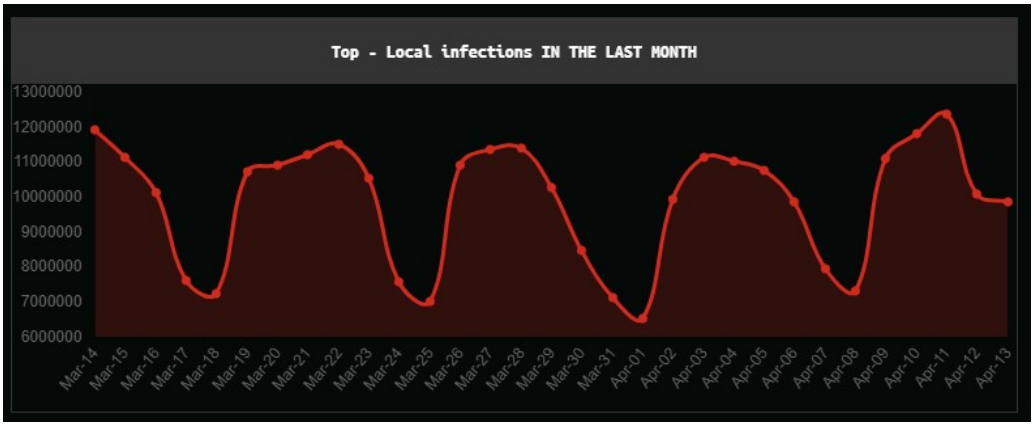
- **Infected mail**
- **On-Demand Scan**
- **Botnet activity**

همچنین گزارش در دو بخش طبقه‌بندی شده است که بخش اول مربوط به گزارش جهانی و بخش دوم ایران را پوشش داده است.

بخش اول: گزارش جهانی

❖ Local Infections

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

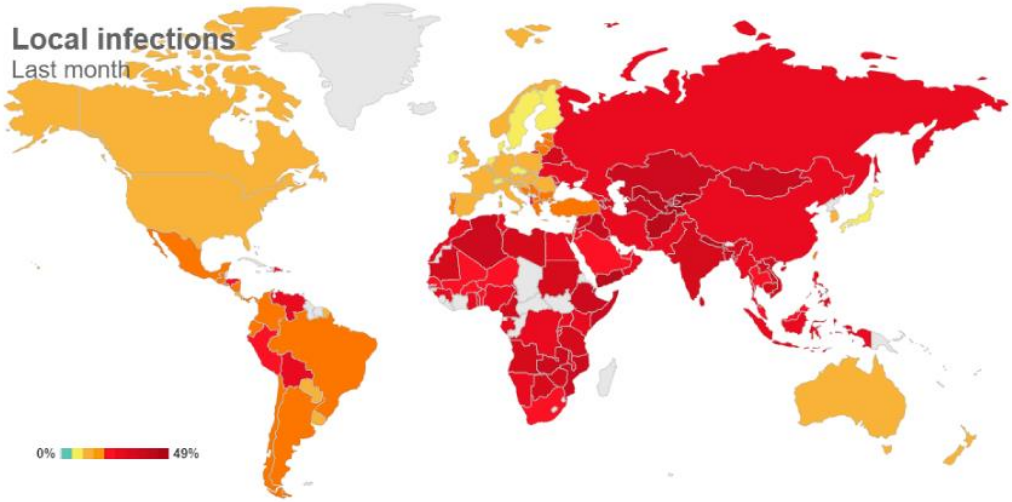
Top - Local infections IN THE LAST MONTH

1	DangerousObject.Multi.Generic	19.99%
2	HackTool.Win32.KMSAuto.c	7.69%
3	Trojan.Script.Generic	6.74%
4	Trojan.WinLNK.Starter.gen	4.63%
5	Trojan.WinLNK.Agent.gen	3.34%
6	Trojan.WinLNK.Runner.jo	2.66%
7	Trojan.Win32.AutoRun.gen	2.5%
8	Trojan.Win32.Agent.qwgdrf	2.18%
9	Trojan.JS.Miner.m	2.15%
10	Trojan.Win32.Generic	1.67%

در این لیست **DangerousObject.Multi.Generic** دارای بیشترین نرخ رشد در یک ماه گذشته بوده که خود یک نرم‌افزار مخرب است که توسط مرکز **KL Cloud Technologies** شناسایی شده و این نوع نام گذاری معمولا برای نمونه‌هایی است که هنوز طبقه‌بندی روی آن انجام نشده است. یک مورد دیگر **HackTool** است که دارای فروانی ۷,۶۹ درصد بوده که خود یک برنامه است که برای ایجاد یک کاربر جدید در لیست بازدیدکنندگان مجاز سیستم استفاده می‌شود و اطلاعات و ردپاهای حضور کاربر غیر مجاز را در سیستم پنهان می‌کند. این برنامه همچنین برای تجزیه و تحلیل و جمع آوری بسته‌های شبکه برای انجام اقدامات مخرب استفاده می‌شود و هنگام راه‌اندازی حملات بر روی کامپیوترهای محلی و یا راه دور، کاربران مضر از برنامه **HackTool** استفاده می‌کنند. یک مورد دیگر **Trojan.Script.Generic** بوده است که یک بدافزار از نوع تروجان می‌باشد که یک برنامه مخرب است که به منظور جاسوسی به

صورت الکترونیکی از کاربران فعال طراحی شده است (شامل ورودی صفحه کلید، گرفتن عکس از صفحه، گرفتن لیست فعالیت‌های برنامه‌ها و غیره). اطلاعات جمع‌آوری شده به وسیله ابزار مختلف از جمله ایمیل، **FTP** و **HTTP** (با ارسال اطلاعات در یک درخواست) به فرد مهاجم جرایم سایبری فرستاده می‌شود.

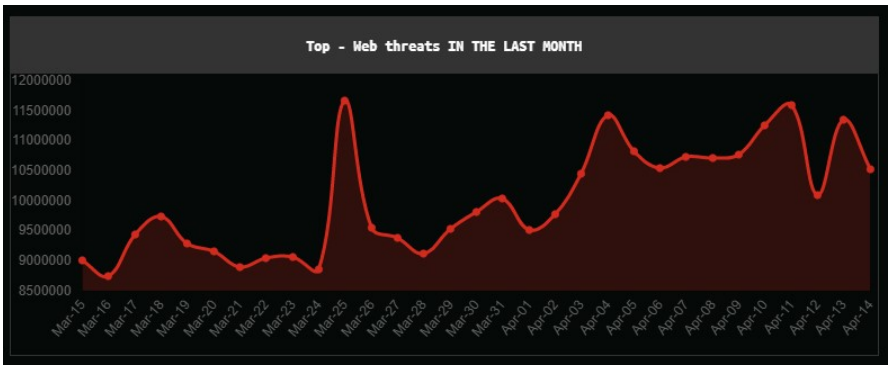
کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.



WORLD		
1	Tajikistan	47.85%
2	Kyrgyzstan	44.67%
3	Afghanistan	42.85%
4	Nepal	41.89%
5	Uzbekistan	40.66%
6	Yemen	39.45%
7	Ethiopia	39.1%
8	Rwanda	38.72%
9	Somalia	38.61%
10	Mongolia	38.47%
11	Djibouti	37.73%
12	Algeria	36.46%
13	Iraq	36.43%
14	Bangladesh	36.36%
15	Zambia	36.27%
16	Mozambique	35.89%
17	Kazakhstan	34.89%
18	Vietnam	34.1%
19	Angola	34.07%
20	Belarus	33.62%

❖ Web threats

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.

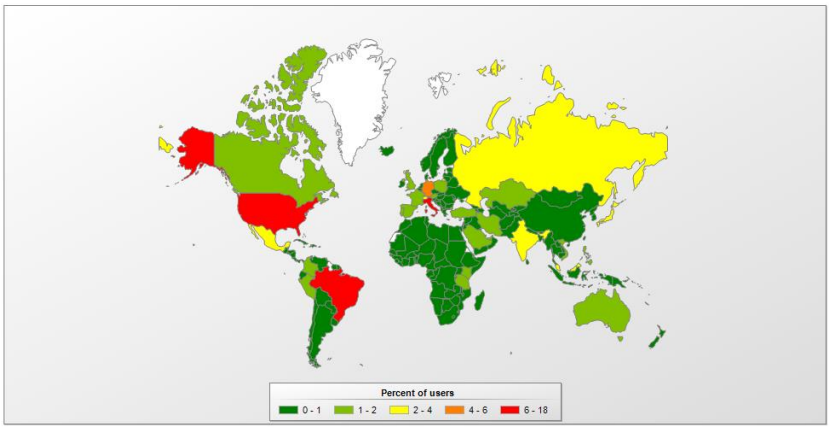


همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

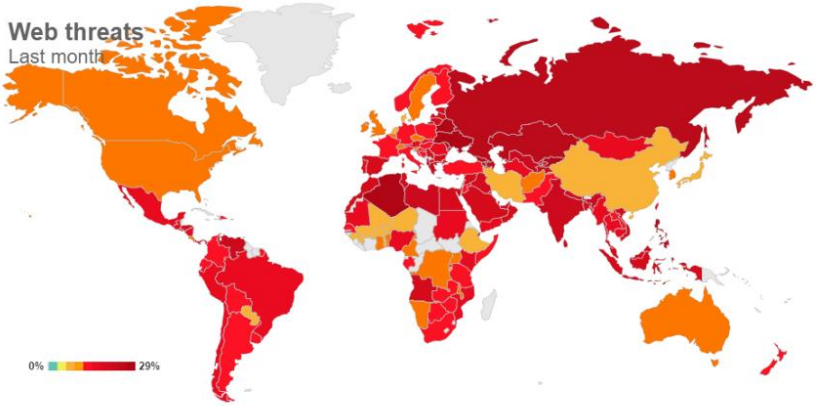
Top - Web threats IN THE LAST MONTH

1	Trojan.Script.Generic	50.46%
2	Trojan.Script.Miner.gen	16.04%
3	Trojan.Script.Agent.gen	9.1%
4	Trojan.JS.Miner.m	6.43%
5	Trojan-Clicker.HTML.Iframe.dg	2.9%
6	Trojan.JS.Miner.o	1.94%
7	Trojan.Win64.Shelma.a	1.6%
8	Trojan.JS.Agent.eak	1.23%
9	Trojan.JS.Agent.ebo	0.86%
10	Packed.Multi.MultiPacked.gen	0.53%

در این لیست موارد **Trojan.Script.Generic**، **Trojan.Script.Miner.gen** و **Trojan.JS.Miner**در بخش قبل مورد بررسی قرار گرفته‌اند. مورد **Trojan.Script.Agent.gen** یک نمونه عمومی از خانواده اسکریپت‌های جاوا اسکریپت یا اسناد **.doc/.docx** که شامل ماکروهای **VBA** است. این اسکریپت دیگر بدافزارها را دانلود و اجرا می‌کند که اغلب اوقات داده‌های کاربران را رمزگذاری می‌کند. شکل زیر گستردگی این اسکریپت در سطح جهان را نشان می‌دهد.



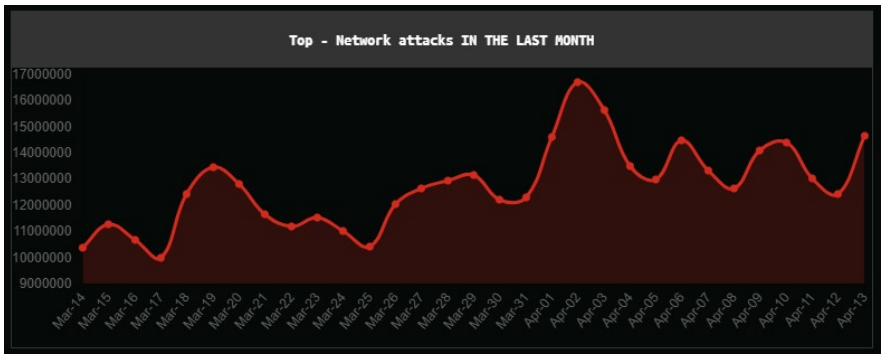
کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.



WORLD		
1	Ukraine	27.92%
2	Belarus	27.78%
3	Algeria	27.27%
4	Armenia	26.91%
5	Moldova	26.81%
6	Kyrgyzstan	25.89%
7	Azerbaijan	24.49%
8	Russia	23.92%
9	Georgia	23.68%
10	Kazakhstan	23%
11	Philippines	22.79%
12	Albania	22.23%
13	Greece	21.65%
14	Venezuela	21.21%
15	Qatar	21%
16	Djibouti	20.89%
17	Uzbekistan	20.76%
18	India	20.39%
19	Tajikistan	20.33%
20	Libya	19.79%

❖ Network Attacks

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Network attacks IN THE LAST MONTH

1	Intrusion.Win.MS17-010.o	12%
2	Bruteforce.Generic.RDP	4.16%
3	Bruteforce.Generic.Rdp.a	3.55%
4	Intrusion.Win.NETAPI.buffer-overflow.exploit	1.46%
5	DoS.Generic.SYNFlood	0.52%
6	Intrusion.Win.MS17-010.e	0.3%
7	DoS.Win.IGMP.Host-Membership-Query.exploit	0.11%
8	Intrusion.Win.CVE-2017-7269.cas.exploit	0.1%
9	Intrusion.Win.DCOM.exploit	0.1%
10	Scan.Generic.TCP	0.09%

نفوذ از طریق **Intrusion.Win.MS17-010** هنوز هم دارای بیشترین نرخ رشد در ماه گذشته بوده است. سوء استفاده از این آسیب‌پذیری باعث نفوذ به برنامه‌های کاربردی، خدمات و سیستم‌عامل‌های آسیب‌پذیر و یا به طور نادرست پیکربندی شده، از طریق شبکه از راه دور به منظور اجرای کد دلخواه و انجام فعالیت‌های غیر مجاز شده است. **SMB** پروتکل شبکه است که به طور گسترده برای اشتراک فایل و چاپگر و دسترسی از راه دور سرویس‌ها مورد استفاده است. این مورد تلاش برای نفوذ از طریق این آسیب‌پذیری است و بهره‌برداری موفق از آن باعث اجرای کد از راه دور بر روی سیستم هدف خواهد شد و باعث می‌شود مهاجم بدافزاری را بارگذاری کرده و آن را به سایر میزبان‌های آسیب‌پذیر شبکه انتشار دهد. باج‌افزارهای **WannaCry** و **ExPetr** از این نوع آسیب‌پذیری برای حمله استفاده کرده‌اند.

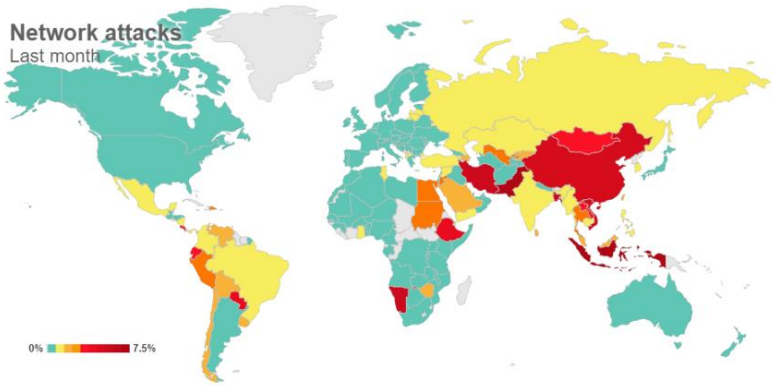
در رده بعدی نرخ بالای رشد در ماه گذشته **Bruteforce.Generic.RDP** بوده است که یک روش حمله برای حدس رمز عبور و یا کلید رمزگذاری است که شامل تلاش سیستماتیک تمام ترکیبات احتمالی

از کاراکترها تا یک مورد صحیح پیدا شود. برای رمزهای با طول بیشتر یک راه حل جایگزین حملات دیکشنری

است که به صورت موثری تری می‌تواند عمل کند. این حملات به مهاجم اجازه می‌دهد که از اعتبار یک کاربر معتبر سوء استفاده کند. همچنین **RDP** یک پروتکل اختصاصی مایکروسافت است که برای کاربر یک محیط گرافیکی را برای اتصال به یک کامپیوتر دیگر تحت شبکه فراهم می‌کند.یک حمله **Bruteforce.Generic.RDP** به منظور پیدا کردن رمز عبور و شناسه **RDP** یک کاربر با چک کردن تمامی حالات ممکن رمز انجام می‌گیرد. این حملات اگر موفقیت آمیز باشد به مهاجم امکان دسترسی از راه دور به سیستم میزبان را می‌دهد.

در این بخش ایران جزو پنج کشور با نرخ بالای رشد بوده است که نیازمند دقت و بررسی بیشتر برای عدم ایجاد مشکلات حساس در آینده است.

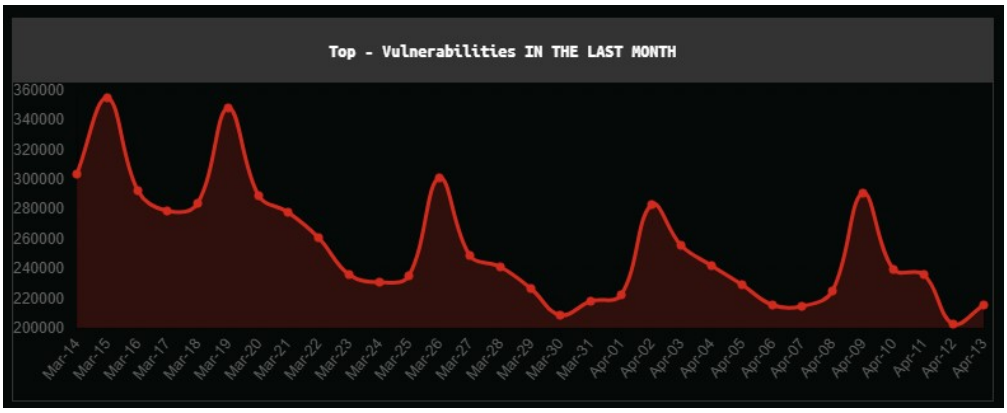
کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.



WORLD		
1	Pakistan	7.38%
2	Indonesia	6.84%
3	Namibia	5.96%
4	Bangladesh	5.28%
5	Iran	5.05%
6	Vietnam	4.4%
7	China	4.38%
8	Paraguay	4.38%
9	Ethiopia	3.86%
10	Laos	3.52%
11	Mongolia	3.32%
12	Costa Rica	3.32%
13	Ecuador	3.2%
14	Peru	3%
15	Dominican Republic	2.98%
16	Egypt	2.84%
17	Uzbekistan	2.63%
18	Venezuela	2.5%
19	Thailand	2.42%
20	Sudan	2.35%

❖ Exploited Vulnerability

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



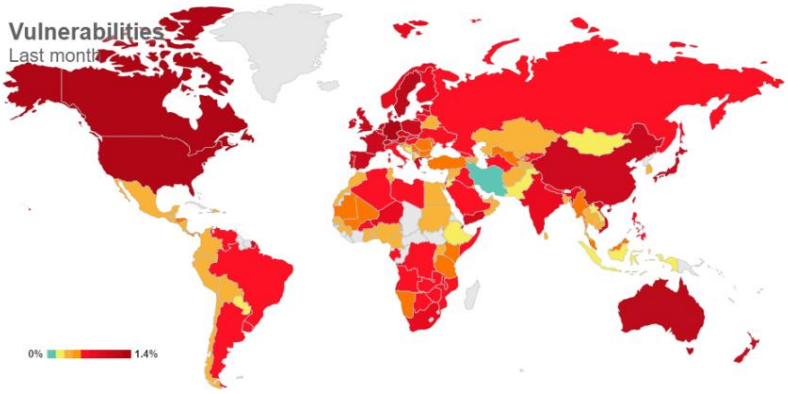
همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Vulnerabilities IN THE LAST MONTH

1	Exploit.Win32.ShadowBrokers.ae	10.24%
2	Exploit.Win32.CVE-2017-11882.gen	9.14%
3	Exploit.Win32.ShadowBrokers.z	5.62%
4	Exploit.Win64.ShadowBrokers.c	5.59%
5	Exploit.Win32.ShadowBrokers.aa	5.56%
6	Exploit.Win64.ShadowBrokers.d	5.54%
7	Exploit.Win32.ShadowBrokers.ad	5.54%
8	Exploit.Win32.ShadowBrokers.ab	5.5%
9	Exploit.MSOffice.CVE-2017-0199.h	3.63%
10	Exploit.MSOffice.Oleink.a	3.27%

در این بخش **Exploit.Win32.ShadowBrokers** که نسخه‌های مختلف آن دارای بیشترین نرخ رشد در این ماه بوده‌اند و اغلب مهاجمین برای نفوذ به سیستم‌های کاربران قربانی از این اکسپلویت‌ها استفاده می‌کنند که اخیرا بسیار دارای رشد بوده است. در رده‌های دیگر از میزان نرخ رشد در این لیست نوع اکسپلویت **Exploit.Win32.CVE-2017-11882.gen** است که با دقت به میزان رشد آن می‌توان پیش‌بینی که در طی هفته‌ها و ماه‌های آینده بسیار با نرخ بالایی رشد داشته باشد.

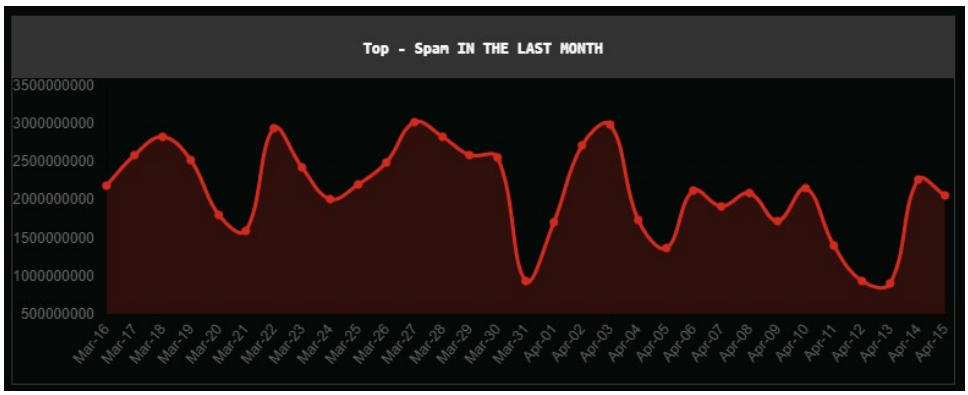
کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.



WORLD		
1	Germany	1.42%
2	United States	1.34%
3	Canada	1.3%
4	Switzerland	1.21%
5	Sweden	1.21%
6	Australia	1.21%
7	Estonia	1.08%
8	United Kingdom	1.07%
9	Japan	1.05%
10	Netherlands	1.05%
11	Austria	1.05%
12	China	1.03%
13	Poland	1%
14	Spain	0.97%
15	New Zealand	0.96%
16	Djibouti	0.96%
17	Czech Republic	0.95%
18	Ireland	0.89%
19	Portugal	0.88%
20	Niger	0.87%

❖ Spam

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.

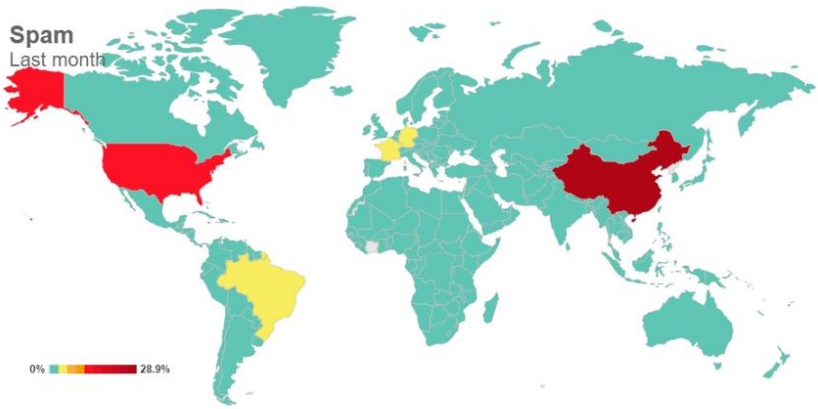


همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Spam IN THE LAST MONTH	
1 Shikari	84.99%
2 Analysis of Formal Attributes	10.58%
3 Linguistic Analysis	3.55%
4 Other	0.26%
5 Graphical Content Analysis	0.23%
6 Cloud Detection	0.23%
7 Signature Analysis	0.09%
8 Enforced Anti-Spam Update Service	0.06%

در ماه گذشته هرزنامه‌های **Shikari** و **Analysis of formal Attributes** به صورت کلی نزدیک به ۹۶ درصد از هرزنامه‌ها را تشکیل داده‌اند که می‌توان با اطلاع‌رسانی صحیح از گسترش آلودگی آن ممانعت کرد.

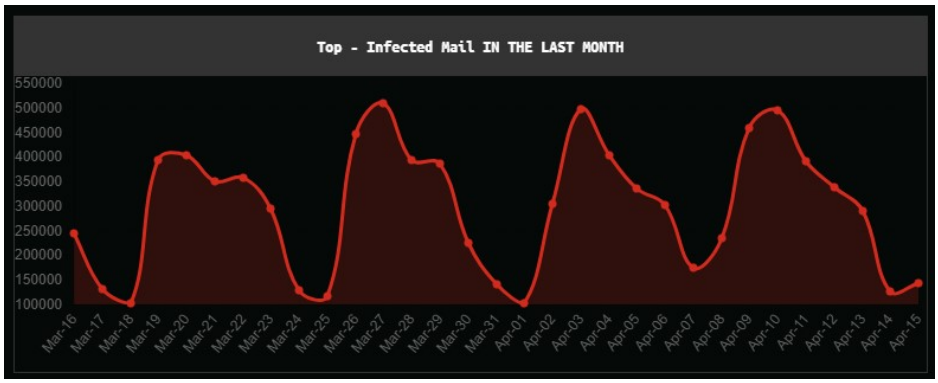
کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.



WORLD	
1 China	27.38%
2 United States	14.94%
3 Germany	4.33%
4 Brazil	3.4%
5 Russia	2.81%
6 Vietnam	2.77%
7 India	2.41%
8 Singapore	2.35%
9 Turkey	2.12%
10 Romania	1.71%
11 United Kingdom	1.62%
12 Italy	1.59%
13 Japan	1.38%
14 South Africa	1.35%
15 Netherlands	1.33%
16 Canada	0.88%
17 Belgium	0.87%
18 South Korea	0.84%
19 Argentina	0.81%
20 Malaysia	0.75%

❖ Infected mail

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Infected Mail IN THE LAST MONTH

1	Exploit.Win32.CVE-2017-11882.gen	7.3%
2	Trojan-Downloader.Win32.Furl.gen	5.55%
3	Worm.Win32.WBVB.vam	4.79%
4	Trojan-Downloader.Script.Generic	4.04%
5	Backdoor.Java.QRat.gen	3.33%
6	DangerousObject.Multi.Generic	3.05%
7	Trojan.Script.Generic	2.92%
8	Trojan-Downloader.JS.SLoad.gen	2.18%
9	Trojan-Downloader.BAT.Powedon.gen	1.91%
10	Backdoor.Win32.Phds.a	1.83%

در بخش ایمیل‌های آلوده نیز استفاده از اکسپولیت‌های مختلف در این لیست با نرخ بالایی رشد داشته‌اند. همچنین **Trojan-Downloader** برای دانلود برنامه‌های مخرب از جمله تروجان‌ها و تبلیغ افزارها و اجرای خودکار آن‌ها باعث ایجاد تخریب در سیستم قربانی خواهد شد. این نوع برنامه‌ها اغلب در وب سایت‌هایی که نشانی از فعالیت‌های تخریبی دارند یافت نشده و در سایت‌های بازی آنلاین و فعالیت‌های عادی و روتین یافت می‌شوند که حالت مشکوکی ندارند.

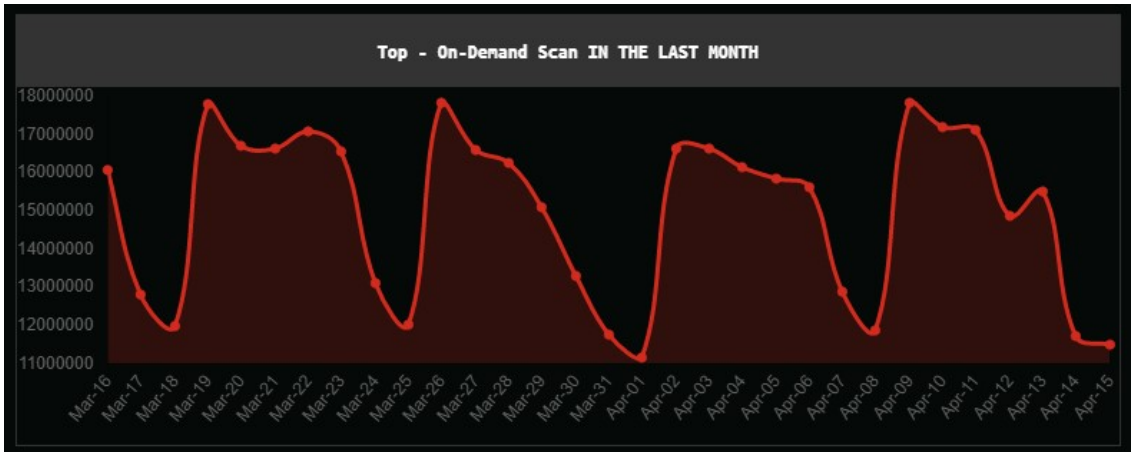
مورد دیگر **Worm.Win32.WBVB.vam** است که یک نوع کرم می‌باشد که شبکه‌های کامپیوتری را از راه دور جستجو کرده و خود را در دایرکتوری‌ها کپی می‌کند و قابلیت درسترسی از نوع خواندن یا نوشتن و یا هر دو را به دست می‌آورد. همچنین این نوع کرم در شبکه جستجو کرده و تلاش می‌کند تا دسترسی کاملی به سخت افزار و دیسک سخت رایانه‌ها پیدا کند. به علاوه اینکه یکی از ویژگی‌های این دسته به صورتی است که کرم‌هایی بنا به هر دلیلی به عنوان مثال برای تخریب در دستگاه‌های تلفن همراه نباشند، این دسته آن موارد را نیز پوشش می‌دهد.

کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.

WORLD		
1	Croatia	5.47%
2	United Arab Emirates	5.45%
3	Macedonia	5.37%
4	Cyprus	4.91%
5	Serbia	4.33%
6	Zimbabwe	4.26%
7	Greece	4.1%
8	Qatar	4.03%
9	Estonia	3.99%
10	Bangladesh	3.88%
11	Bulgaria	3.83%
12	Lebanon	3.82%
13	Bosnia and Herzegovina	3.77%
14	Slovenia	3.59%
15	Lithuania	3.56%
16	South Africa	3.41%
17	Mauritius	3.38%
18	Bahrain	3.26%
19	Luxembourg	3.17%
20	Brazil	3.05%

❖ On-Demand Scan

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - On-Demand Scan IN THE LAST MONTH		
1	Trojan.Script.Generic	3.42%
2	DangerousObject.Multi.Generic	2.86%
3	Trojan.Win32.EquationDrug.gen	1.78%
4	Trojan.Win64.EquationDrug.gen	1.32%
5	Trojan.Multi.GenAutorunReg.a	1.27%
6	HackTool.Win32.KMSAuto.l	1.12%
7	HackTool.Win32.KMSAuto.k	1.1%
8	HackTool.MSIL.KMSAuto.ba	1.03%
9	Trojan.Multi.GenAutorunBITS.a	1.01%
10	HackTool.Win32.KMSAuto.m	0.97%

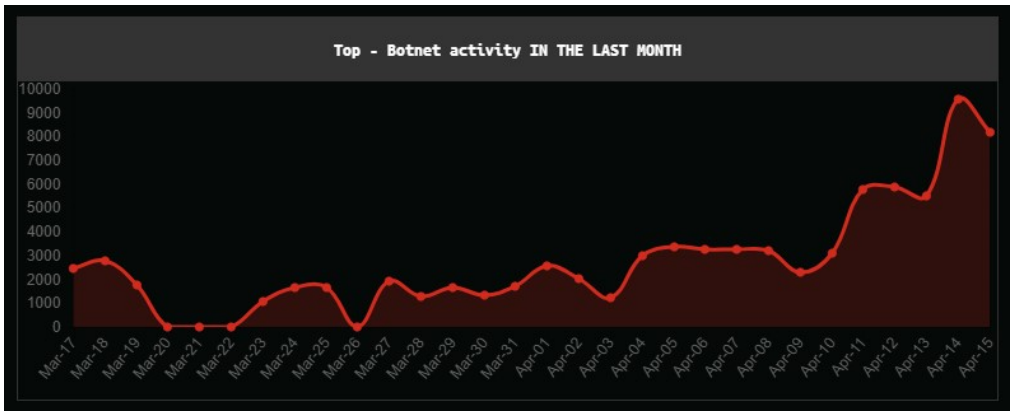
در این بخش میزان تقاضای اسکن نشان داده شده است که نمونه‌های مختلف با درصد بالای نرخ رشد وجود ندارند و از دسته‌های مختلفی برای این بخش استفاده شده است که هر کدام از آن‌ها در بخش‌های قبلی به صورت کامل توضیح داده شده‌اند.

کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.

WORLD		
1	Nepal	54.29%
2	Afghanistan	54.27%
3	Mongolia	53.4%
4	Somalia	51.45%
5	Yemen	50.6%
6	Laos	49.8%
7	Tajikistan	49.74%
8	Rwanda	49.6%
9	Kyrgyzstan	48.91%
10	Djibouti	47.97%
11	Iraq	47.25%
12	Armenia	47.23%
13	Vietnam	46.64%
14	Bangladesh	46.46%
15	Algeria	46.03%
16	Kazakhstan	45.82%
17	Libya	44.43%
18	Ethiopia	43.88%
19	Uzbekistan	43.62%
20	Cambodia	43.48%

❖ Botnet activity

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



همان‌طور که در نمودار نیز مشخص است در ماه گذشته با گذشت زمان رشد بالایی را در این بخش شاهد بوده‌ایم که انتظار می‌رود برای آنیده نزدیک نیز این رشد ادامه داشته باشد و اقدامات پیش‌گیرانه و اطلاع‌رسانی صحیح در این خصوص باید مدنظر قرار بگیرد.

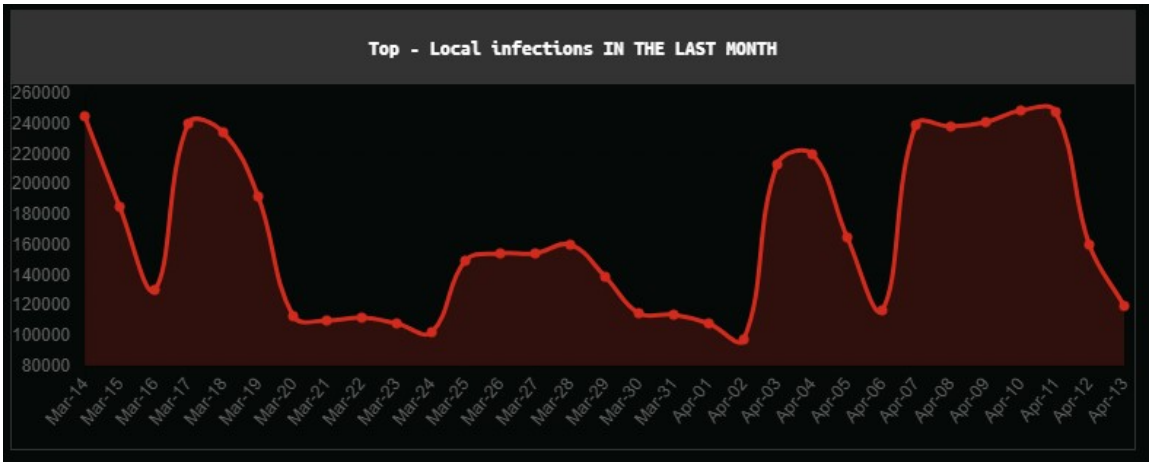
کشورهایی که بیشترین آمار را در این بخش دارند به صورت زیر است.

WORLD		
1	China	67340
2	United States	9044
3	South Korea	1823
4	Canada	379
5	Vietnam	259
6	United Kingdom	247
7	Taiwan	221
8	Romania	162
9	Germany	158
10	Russia	92
11	Mexico	53
12	Netherlands	51
13	Brazil	44
14	Belarus	36
15	Belize	31
16	Australia	27
17	Japan	25
18	Italy	25
19	Ukraine	24
20	Ireland	16

بخش دوم: گزارش ایران

❖ Local Infections

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



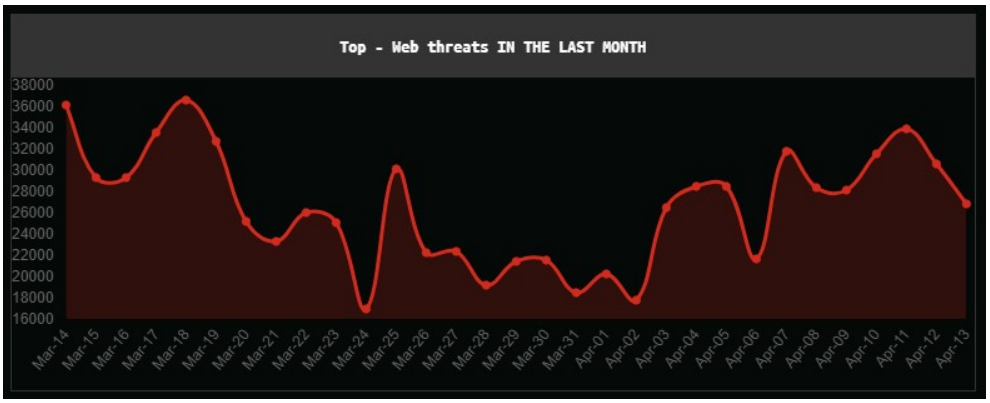
همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Local infections IN THE LAST MONTH

1	DangerousObject.Multi.Generic	20.48%
2	Trojan.WinLNK.Starter.gen	9.5%
3	Trojan-Ransom.Win32.Blocker.jaic	7.78%
4	HackTool.MSIL.KMSAuto.bl	7.53%
5	HackTool.Win32.Kiser.fnbel	6.04%
6	Trojan.WinLNK.Runner.jo	5.89%
7	Trojan.Script.Generic	3.18%
8	Trojan.AndroidOS.Hiddapp.bn	3.02%
9	Trojan.WinLNK.Agent.gen	2.79%
10	Trojan.JS.Miner.m	2.61%

❖ Web threats

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



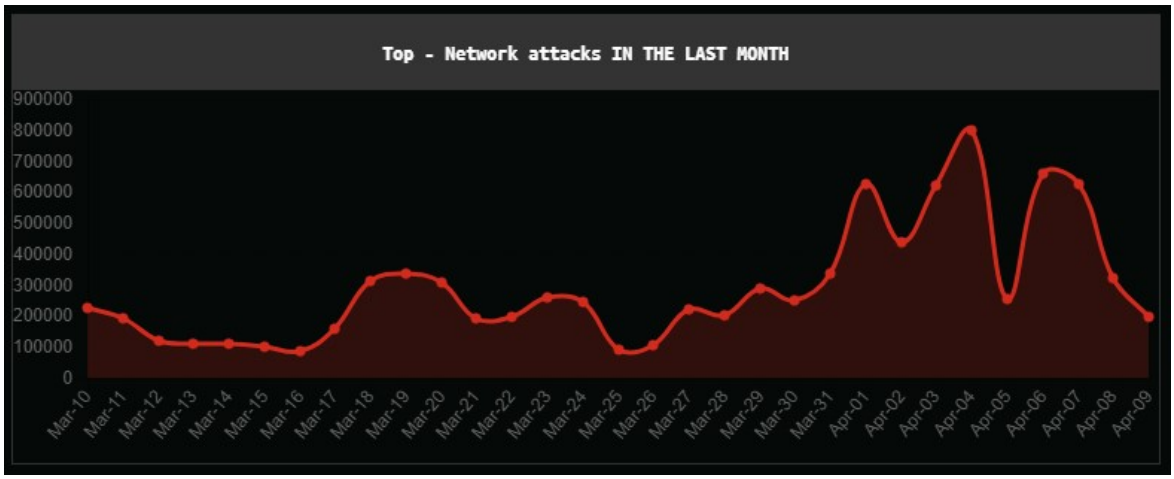
همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Web threats IN THE LAST MONTH

1	Trojan.Script.Generic	81.09%
2	Trojan.JS.Agent.eak	9.09%
3	Trojan.Script.Miner.gen	3.93%
4	Trojan-Clicker.HTML.Iframe.dg	2.3%
5	Trojan.JS.Miner.m	1.37%
6	Trojan.JS.Agent.dvu	0.23%
7	Packed.Multi.MultiPacked.gen	0.21%
8	Trojan.JS.Miner.o	0.12%
9	DangerousObject.Multi.Generic	0.11%
10	Backdoor.Win32.Phny.a	0.08%

❖ Network Attacks

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.

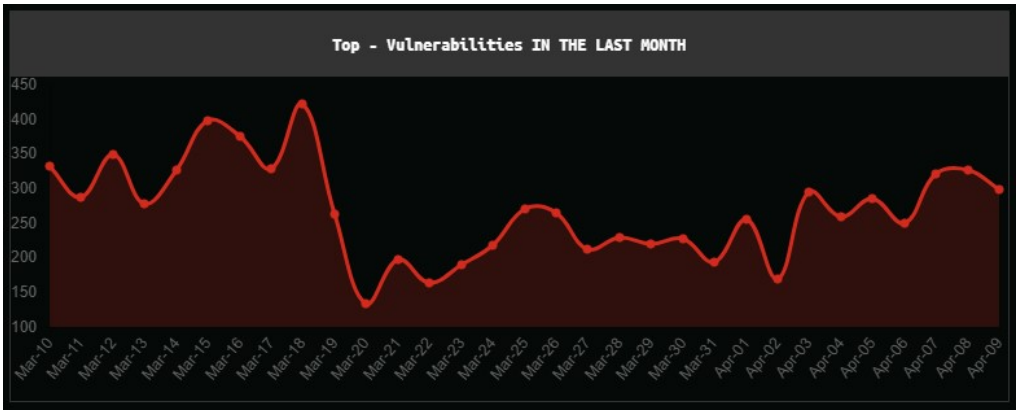


همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Network attacks IN THE LAST MONTH		
1	Bruteforce.Generic.Rdp.a	6.13%
2	Intrusion.Win.MS17-010.o	4.75%
3	Bruteforce.Generic.RDP	4.23%
4	Intrusion.Win.NETAPI.buffer-overflow.exploit	0.95%
5	Intrusion.Generic.CVE-2017-10271.exploit	0.19%
6	Intrusion.Generic.FTPD.PASS.buffer-overflow.attack	0.16%
7	Intrusion.Win.CVE-2017-7269.cas.exploit	0.14%
8	Intrusion.Win.MS17-010.e	0.07%
9	Intrusion.Win.MS17-010.p	0.06%
10	Intrusion.Win.MS17-010.cf	0.03%

❖ Exploited Vulnerability

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.

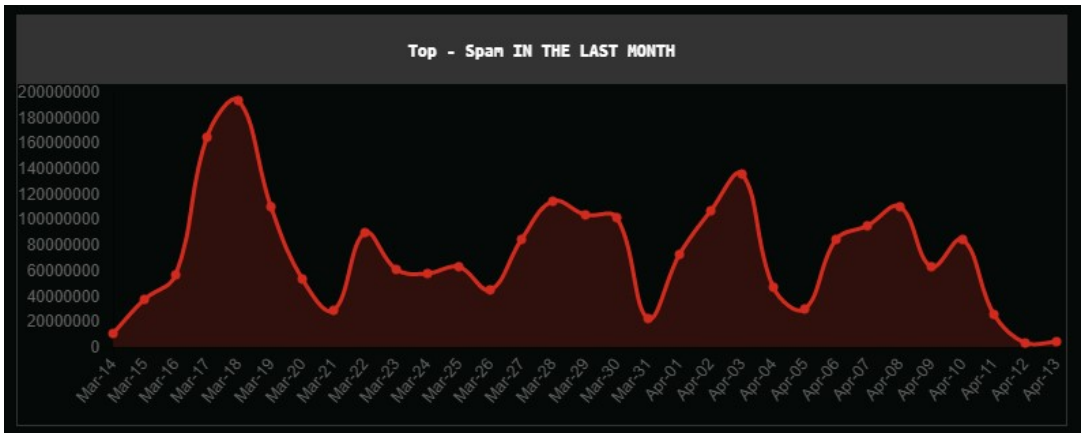


همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Vulnerabilities IN THE LAST MONTH		
1	Exploit.Win32.CVE-2017-0213.a	26.74%
2	Exploit.Win32.CVE-2017-11882.gen	15.05%
3	Exploit.MSOffice.CVE-2017-8570.a	10.02%
4	Exploit.AndroidOS.Lotoor.cc	3.81%
5	Exploit.AndroidOS.Lotoor.bm	2.8%
6	Exploit.AndroidOS.Lotoor.bk	2.28%
7	Exploit.MSOffice.CVE-2017-11882.a	2.23%
8	Exploit.Script.Blocker	2.01%
9	Exploit.AndroidOS.Lotoor.bg	2.01%
10	Exploit.AndroidOS.Lotoor.be	1.66%

❖ Spam

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



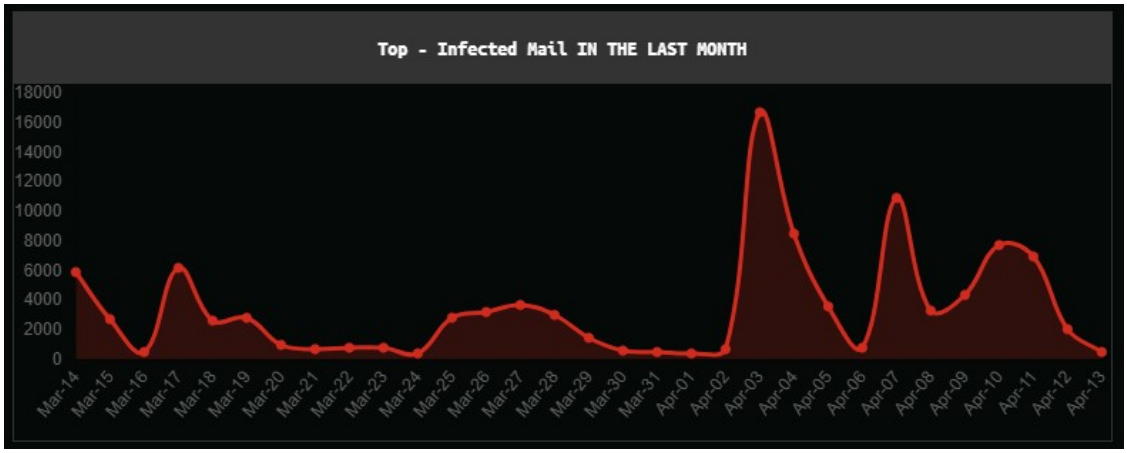
همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Spam IN THE LAST MONTH

1	Shikari	97.04%
2	Analysis of Formal Attributes	2.31%
3	Linguistic Analysis	0.58%
4	Enforced Anti-Spam Update Service	0.03%
5	Signature Analysis	0.02%
6	Graphical Content Analysis	0.01%
7	Other	0.01%
8	Cloud Detection	0.01%

❖ Infected mail

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.

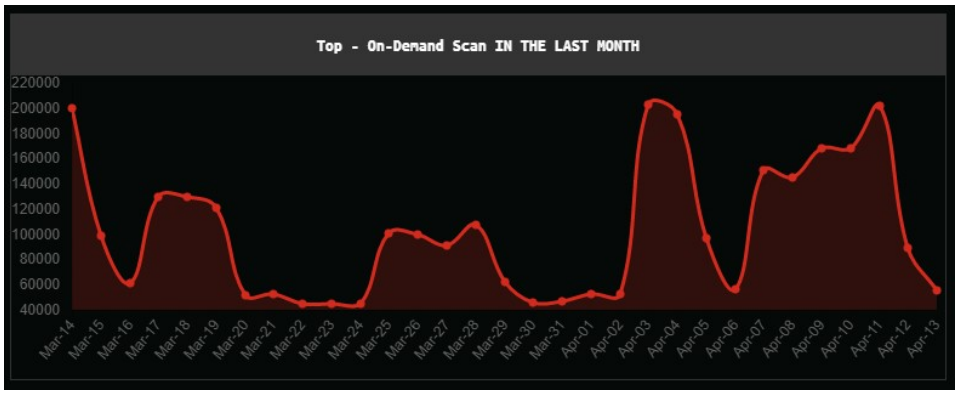


همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - Infected Mail IN THE LAST MONTH		
1	Exploit.Win32.CVE-2017-11882.gen	9.81%
2	Trojan.MSIL.Crypt.vho	6.64%
3	Backdoor.Java.QRat.gen	4.75%
4	Worm.Win32.WBVB.vam	2.96%
5	Trojan.Script.Generic	2.96%
6	Trojan-Downloader.Script.Generic	2.92%
7	Trojan-Downloader.Win32.Furl.gen	2.92%
8	Exploit.MSOffice.CVE-2017-8570.a	2.65%
9	Trojan.HTML.Fraud.gen	2.51%
10	Trojan-PSW.Win32.Chisburg.aizi	2.47%

❖ On-Demand Scan

آمار در این بخش در ماه گذشته بصورت نمودار زیر است.



همچنین بیشترین موارد تهدیدات در این بخش به صورت زیر است.

Top - On-Demand Scan IN THE LAST MONTH		
1	HackTool.MSIL.KMSAuto.bl	7.88%
2	DangerousObject.Multi.Generic	6.25%
3	Trojan-Ransom.Win32.Blocker.jaic	4.31%
4	Trojan.Multi.GenAutorunReg.a	3.41%
5	Trojan.Win32.EquationDrug.gen	3.17%
6	Trojan.Script.Generic	3.11%
7	HackTool.MSIL.KMSAuto.d	2.98%
8	Trojan.JS.Miner.m	2.9%
9	Trojan.Win64.EquationDrug.gen	2.09%
10	Trojan.WinLNK.Starter.gen	1.97%

❖ Botnet activity

در این بخش در ماه گذشته برای ایران گزارشی ارائه نشده است.

منابع :

1. https://cybermap.kaspersky.com/
2. https://securelist.com/statistics/
3. https://www.cisecurity.org/
4. https://www.us-cert.gov/