باسمه‌تعالی

اینترنت اشیاء و ظرف‌های عسل

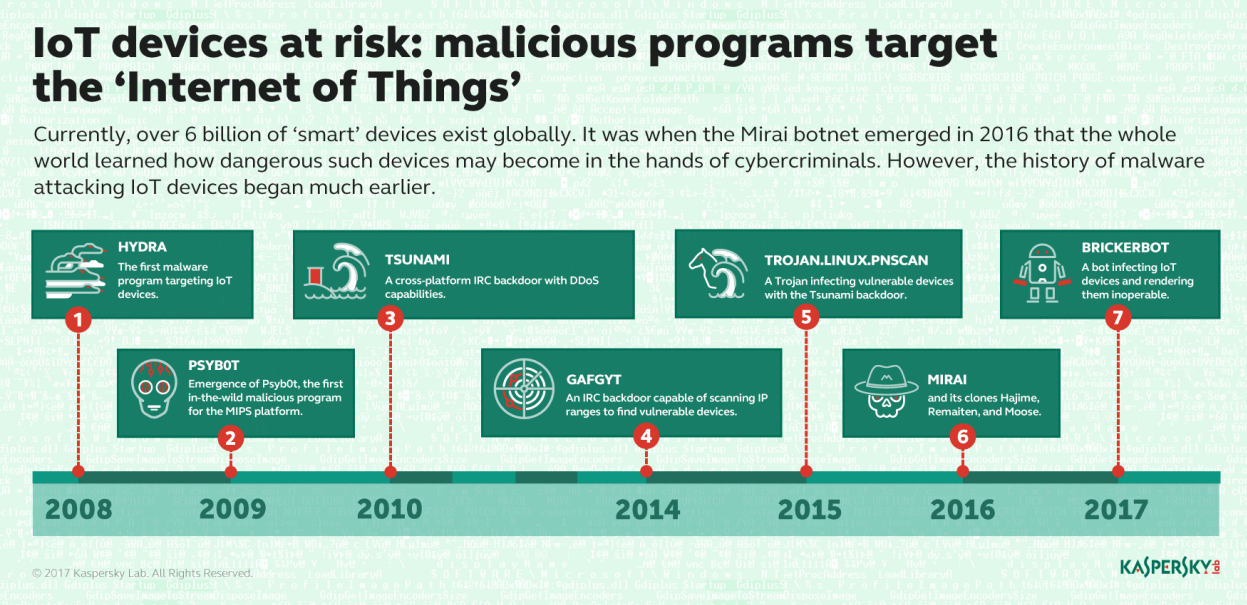
(تحلیل داده‌های گردآوری شده توسط تله‌های IoT

آزمایشگاه کسپرسکی)

۱ مقدمه

تعدادی از حوادث سال ۲۰۱۶ میلادی موجب شد تا موضوع امنیت در دستگاه‌ها و تجهیزاتِ IoT[1] (یا به عبارت دیگر تجهیزات هوشمند[2]) مورد توجه قرار گیرد. از جمله‌ی این حوادث می‌توان به حمله‌ی DDoS به هاست فرانسویِ OVH و همینطور DNS امریکاییِ Dyn اشاره کرد. این حمله‌ها با استفاده از بات‌نت‌های عظیمی متشکل از مسیریاب‌ها، دوربین‌های IP[3]، پرینترها و سایر تجهیزات صورت گرفتند.

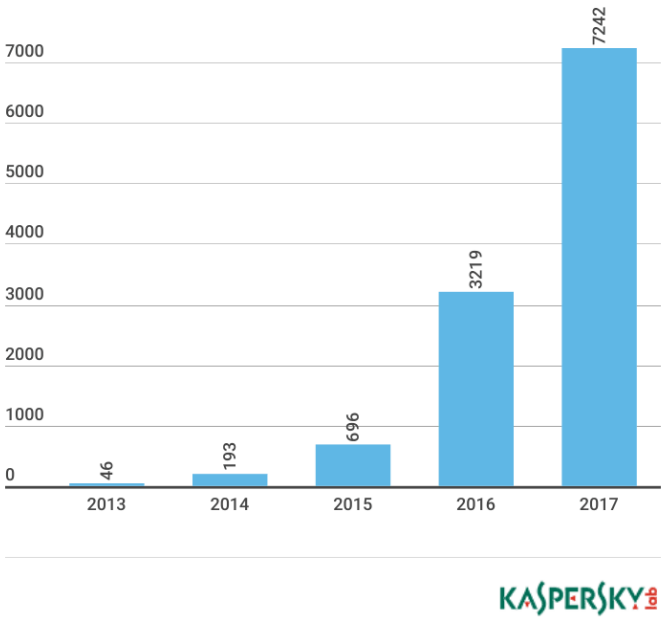
در سال گذشته همچنین بات‌نتِ غول‌آسایی متشکل از حدود ۵ میلیون مسیریاب شناسایی شد. به علاوه، هک شدنِ مسیریاب‌های شرکت آلمانیِ Deutsche Telekom پس از آلودگی تجهیزات مورد استفاده‌ی کلاینت‌های اپراتور به دستِ Mirai نیز از دیگر حوادث مهم بود. این هک‌ها صرفاً محدود به تجهیزات شبکه نبود و شامل مشکلات امنیتی در ظرف‌شویی‌های Miele و اجاق گازهای AGA نیز بود. مضاف بر اینها، کرمِ BrickerBot برخلاف کرم‌های مشابه خود تنها به آلوده کردنِ دستگاه‌های آسیب‌پذیر اکتفا نکرد، بلکه آنها را از کار انداخت.



شکل ۱ - تاریخچه‌ی بدافزارهای حمله‌کننده به تجهیزاتِ IoT

[1] Internet of Things devices
[2] smart devices
[3] IP camera

بنا بر آمارِ Gartner، هم‌اکنون ۶ میلیارد دستگاهِ IoT در دنیا وجود دارد. طبیعتاً چنین رقمِ بزرگ از تجهیزاتی که بالقوه آسیب‌پذیر هستند، توجه تبهکاران اینترنتی را به خود جلب می‌کند. تا ماه مِه ۲۰۱۷، مجموعه‌های گردآوری‌شده در Kaspersky Lab چندین هزار نمونه از بدافزارهای مختلف برای تجهیزاتِ IoT را شامل می‌شود که نیمی از آنها در سال ۲۰۱۷ کشف شده‌اند.



شکل ۲- تعداد بدافزارهای IoT کشف‌شده در سال‌های مختلف

۲ تهدیدات برای کاربران

اگر یک تجهیزِ IoT در شبکه‌ی خانگی فردی قرار داشته باشد که تنظیمات آن نامناسب بوده یا دارای آسیب‌پذیری باشد، آن فرد در معرض خطرات جدی قرار دارد. محتمل‌ترین سناریو آن است که دستگاه آسیب‌پذیر به عضویت یک شبکه باتنت در آید. این سناریو شاید بی‌ضررترین سناریو برای صاحب دستگاه باشد، چرا که سایر سناریوها خطرناک‌تر هستند. برای مثال، ممکن است تجهیزات خانگی برای انجام فعالیت‌های غیرقانونی مورد سوءاستفاده قرار گیرد، یا مثلاً یک تبهکار اینترنتی از تجهیزاتِ IoT جاسوسی کرده و سپس از صاحب آن اخاذی کند (چنین اتفاقاتی قبلاً در واقعیت رخ داده‌اند). نهایتاً ممکن است دستگاه از کار بیفتد که البته این مورد لزوماً بدترین اتفاق در بین سناریوهای مختلف نیست.

۳ مشکلات اصلی تجهیزات هوشمند

۳-۱ میان‌افزار

شرکت‌های سازنده‌ی تجهیزات، در انتشار آپدیت‌های میان‌افزار[۴] تجهیزات خود کند هستند. در بدترین حالت، سازندگان هیچ آپدیتی برای میان‌افزارها تولید نمی‌کنند. در بسیاری از تجهیزات اساساً امکانی برای آپدیت میان‌افزار تعبیه نشده است.

نرم‌افزار داخل تجهیزات ممکن است خطاهایی داشته باشد که تبهکاران سایبری بتوانند از آنها سوءاستفاده کنند. برای مثال، تروجانِ PNScan (یا Trojan.Linux.PNScan) تلاش کرد تا با استفاده از یکی از آسیب‌پذیری‌های زیر، مسیریاب‌ها را هک کند:

- CVE-2014-9727 برای حمله به مسیریاب‌های Fritz!Box
- یک آسیب‌پذیری در HNAP[۵] و آسیب‌پذیریِ CVE-2013-2678 برای حمله به مسیریاب‌های Linksys
- ShellShock (CVE-2014-6271)

در صورت موفقیت از طریق هر یک از این آسیب‌پذیری‌ها، PNScan دستگاه مربوطه را با بک‌دورِ Tsunami آلوده می‌ساخت.

تروجانِ Persirai نیز از یک آسیب‌پذیریِ موجود در بیش از هزار مدل مختلف از دوربین‌های IP استفاده می‌کرد. در صورت موفقیت، این بدافزار می‌توانست کدهای دلخواه خود را از طریق سطح دسترسیِ اَبَرکاربر[۶] بر روی دستگاه اجرا کند.

یک روزنه‌ی امنیتیِ دیگر نیز در پیاده‌سازی پروتکلِ TR-069 وجود داشت. این پروتکل بدین منظور طراحی شده که اپراتور بتواند از راه دور تجهیزات را مدیریت کند. اساس این پروتکل بر SOAP بنا شده که از فرمتِ XML برای تبادل دستورات استفاده می‌کند. چندی پیش یک آسیب‌پذیری در درون تجزیه‌گرِ دستور[۷] تشخیص

---

[4] firmware
[5] Home Network Administration Protocol
[6] super-user
[7] command parser

داده شده بود و از این مکانیسمِ آلودگی در نسخه‌هایی از تروجانِ Mirai و همینطور Hajime استفاده شد. این روش همان روشی بود که تجهیزاتِ Deutsche Telekom آلوده شدند.

۲-۳ پسوردها، telnet و SSH

یک مشکل دیگر، پسوردهای از پیش تعیین شده توسط شرکتِ سازنده هستند. پسوردها ممکن است نه تنها برای یک محصول بلکه برای دسته‌ای از محصولات آن سازنده یکسان باشد. جدای از آن، این وضعیت آن‌چنان ادامه‌دار بوده که پسوردها به سادگی در اینترنت یافت می‌شوند (موضوعی که تبهکاران سایبری بسیار از آن استفاده می‌کنند). موضوع دیگری که کار را برای تبهکاران سایبری آسان‌تر کرده این است که پورت‌های telnet یا SSH در بسیاری از تجهیزاتِ IoT، از دنیای بیرون قابل دسترسی می‌باشد.

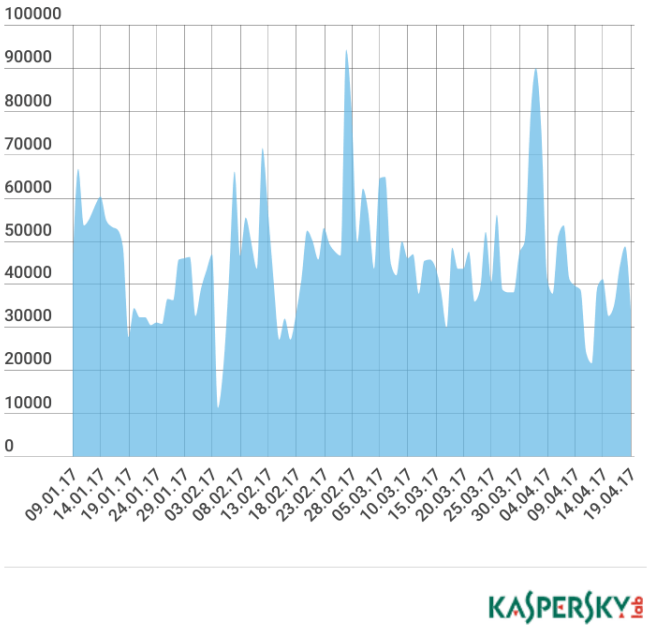
برای مثال، جدول زیر لیستی از ترکیباتِ نام/کلمه عبور است که یکی از نسخه‌های تروجانِ Gafgyt (یا Backdoor.Linux.Gafgyt) استفاده می‌کند:

لیست ترکیب‌های پیش فرض نام و کلمه عبور برخی از تجهیزات مختلف

username	password
root	root
root	–
telnet	telnet
!root	–
support	support
supervisor	zyad1234
root	antslq
root	guest12345
root	tini
root	letacla
root	Support1234

۴ آمار و ارقام

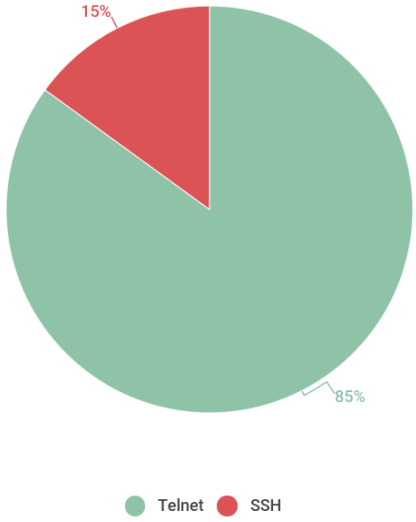
برای تهیه این گزارش، آزمایشگاه کسپرسکی چندین تله‌ی ظرف عسل[۸] ایجاد نموده که رفتار تعداد زیادی از تجهیزاتِ لینوکسی را تقلید می‌کند. این تله‌ها به اینترنت متصل شده‌اند تا اتفاقی که برای آنها میافتد مورد مشاهده قرار گیرد. این کار بسیار زود نتیجه داد: تنها پس از چند ثانیه، تلاش‌های اولیه برای اتصال به پورتِ telnet آغاز شد. پس از ۲۴ ساعت، ده‌ها هزار تلاش برای اتصال از طرف آدرس‌های یکتای IP انجام گرفت.



شکل ۳- تعداد تلاش‌ها برای حمله به تله‌های ظرف عسل از طرف آدرس‌های یکتای IP - ژانویه و آوریل ۲۰۱۷

در اکثر موارد، تلاش‌ها برای ایجاد ارتباط از طریق پروتکلِ telnet انجام گرفته و مابقی از SSH استفاده کرده‌اند.

[8] honeypot



شکل ۴ - توزیع حمله‌ها بر اساس نوع پورت ارتباطی - ژانویه و آوریل ۲۰۱۷

در جدول زیر لیستی از پراستفاده‌ترین ترکیب‌های لاگین/پسورد که برنامه‌های مخرب در هنگام تلاش برای ارتباط به پورت telnet استفاده کرده‌اند آورده شده است:

لیستی از پرکاربردترین ترکیب‌های لاگین/پسورد Telnet مورد استفاده نرم‌افزارهای مخرب

User	Password
root	xc3511
root	vizxv
admin	admin
root	admin
root	xmhdipc
root	123456
root	888888
root	54321
support	support
root	default
root	root
admin	password

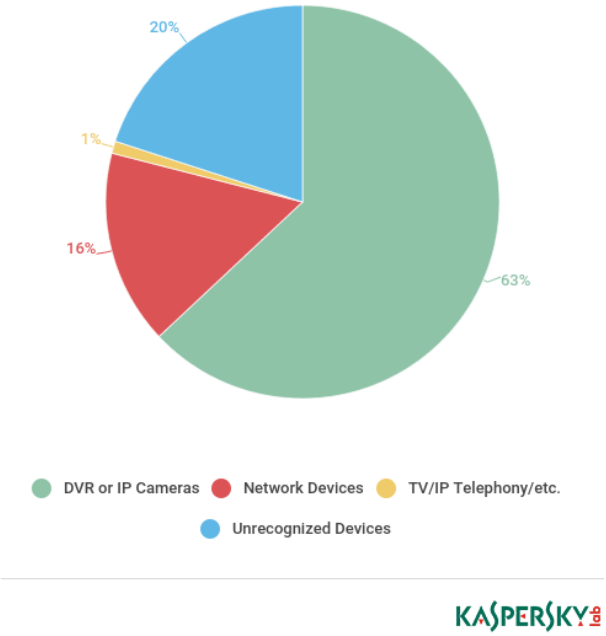
root	anko
root	
root	juantech
admin	smcadmin
root	1111
root	12345
root	pass
admin	admin1234

جدول زیر نیز مربوط به ترکیب‌های لاگین/پسورد استفاده شده برای اتصال به پورت SSH است. می‌توان مشاهده کرد که این جدول کمی با جدول فوق تفاوت دارد.

لیستی از پرکاربردترین ترکیب‌های لاگین/پسورد SSH مورد استفاده نرم‌افزارهای مخرب

User	Password
admin	default
admin	admin
support	support
admin	1111
admin	
user	user
Administrator	admin
admin	root
root	root
root	admin
ubnt	ubnt
admin	12345
test	test
admin	<Any pass>
admin	anypass
administrator	
admin	1234
root	password
root	123456

در ادامه نگاهی به نوع تجهیزاتی که حملات از آنها نشأت می‌گیرد انداخته خواهد شد. آمار نشان می‌دهد که بیش از ۶۳ درصد از تجهیزات سرویس‌های DVR ارائه می‌نمایند (دوربین‌های IP) و ۱۶ درصد نیز گونه‌های مختلفی از تجهیزات شبکه و مسیریاب متعلق به همه‌ی سازنده‌های شناخته‌شده هستند. یک درصد هم تکرارکننده‌های وای‌فای و سایر سخت‌افزارهای شبکه، تیونرهای TV، تجهیزاتِ VoIP، نودهای خروج[9] در شبکه‌ی Tor، پرینترها و همینطور تجهیزاتِ مربوط به خانه‌های هوشمند هستند. حدود ۲۰ درصد از تجهیزات هم به طور صریح شناسایی نشدند.



شکل ۵ - توزیع مبدأِ حملات بر اساس نوع دستگاه - ژانویه و آوریل ۲۰۱۷

از سوی دیگر اکثر آدرس‌های IP که تلاش کردند با تله‌های ظرف عسل اتصال برقرار کنند، به درخواست‌های HTTP پاسخ می‌دادند. معمولاً هر آدرس IP توسط چند دستگاه استفاده می‌شود (از طریق NAT) و از این‌رو همواره دستگاهی که به درخواست‌های HTTP پاسخ می‌دهد لزوماً همان دستگاهی نیست که به تله‌ها حمله کرده است (هرچند که عمدتاً چنین است).

[9] exit node

پاسخ به هر درخواست، یک صفحه‌ی وب مانند کنترل پنل مربوط به یک دستگاه، صفحه نظارت[10]، تصاویر ویدیویی از یک دوربین یا ... بود که با استفاده از آن شاید بتوان نوع دستگاه را شناسایی کرد. در جدول زیر لیستی از هِدِرهایی آورده شده است که بیشترین تکرار را در بین این صفحات وب (که توسط تجهیزات حمله‌کننده بازگردانده شده‌اند) داشته‌اند:

لیست پرتکرارترین هدرهای پاسخ دریافتی

HTTP Title	Device %
NETSurveillance WEB	17.40%
DVR Components Download	10.53%
WEB SERVICE	7.51%
main page	2.47%
IVSWeb 2.0 – Welcome	2.21%
ZXHN H208N V2.5	2.04%
Web Client	1.46%
RouterOS router configuration page	1.14%
NETSuveillance WEB	0.98%
Technicolor	0.77%
Administration Console	0.77%
MΓidem – Inicio de sesiΓin	0.67%
NEUTRON	0.58%
Open Webif	0.49%
hd client	0.48%
Login Incorrect	0.44%
iGate GW040 GPON ONT	0.44%
CPPLUS DVR – Web View	0.38%
WebCam	0.36%
GPON Home Gateway	0.34%

بدیهی است که تنها بخشی از تجهیزاتِ حمله‌کننده با استفاده از این تله‌های ظرف عسل قابل ردگیری است. برای تخمین اینکه از یک نوع دستگاه تقریباً چه تعداد در دنیا وجود دارند، سرویس‌های جستجوی مخصوص این کار مانند Shodan یا ZoomEye کمک‌کننده هستند. آنها می‌توانند رنج‌های IP را برای سرویس‌های تحت پشتیبانی اسکن کرده، آنها را شمارش کرده و نتایج را ایندکس کنند. برخی از هدرهایی که بیشترین تکرار را در

[10] monitoring

دوربین‌های IP، دستگاه‌های DVR و مسیریاب‌ها داشتند در ZoomEye مورد جستجو قرار گرفت. نتایج خیره‌کننده بود: میلیون‌ها دستگاه پیدا شد که به طور بالقوه امکان آلوده شدن به بدافزار را دارا بودند (و احتمالاً آلوده شده بودند).

تعداد آدرس‌های IP مربوط به تجهیزاتِ بالقوه آسیب‌پذیر (دوربین‌های IP و DVRها)

HTTP Title	Devices
WEB SERVICE	2 785 956
NETSurveillance WEB	1 621 648
dvrdvs	1 569 801
DVR Components Download	1 210 111
NetDvrV3	239 217
IVSWeb	55 382
Total	7 482 115

تعداد آدرس‌های IP مربوط به تجهیزاتِ بالقوه آسیب‌پذیر (مسیریاب‌ها)

HTTP Title	Devices
Eltex NTP	2 653
RouterOS router	2 124 857
GPON Home Gateway	1 574 074
TL-WR841N	149 491
ZXHN H208N	79 045
TD-W8968	29 310
iGate GW040 GPON ONT	29 174
Total	3 988 604

شایان ذکر است که تله‌های کار گذاشته شده نه تنها حمله‌هایی که از سخت‌افزارهای خانگیِ شبکه نشأت می‌گرفتند را ثبت کرده‌اند بلکه سخت‌افزارهای سازمانی نیز در میان آنها وجود دارد.

نکته‌ی آزاردهنده‌تر این است که در میان تمام آدرس‌های IP که منشأ حملات بوده‌اند، تعدادی از آنها میزبانِ سیستم‌های نظارتی و یا مدیریت تجهیزات با پیوندهای سازمانی و امنیتی هستند. برای مثال:

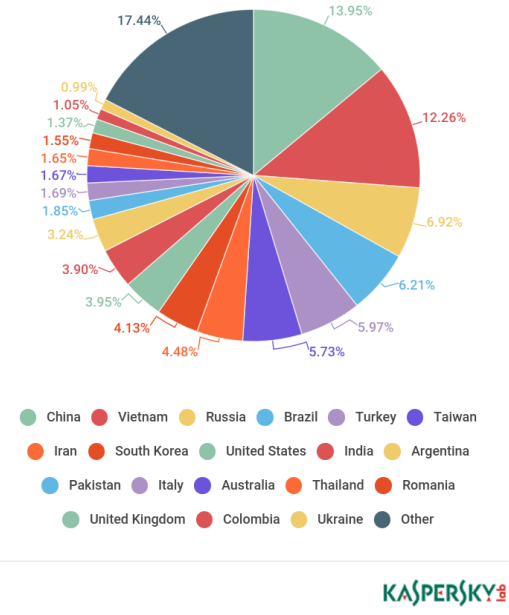
- تجهیزاتِ فروش در فروشگاه‌ها، رستوران‌ها و پمپ بنزین‌ها
- سیستم‌های دیجیتالیِ پخش تلویزیون

- سیستم‌های امنیت فیزیکی و کنترل دسترسی
- تجهیزات نظارتیِ زیست‌محیطی
- نظارت در یک ایستگاه زمین‌لرزه در بانکوک
- میکروکنترلرهای صنعتیِ قابل برنامه‌ریزی
- سیستم‌های مدیریت توان

نمی‌توان به طور قطع عنوان کرد که این‌گونه تجهیزات دچار آلودگی شده‌اند. با این حال، حمله‌هایی به تله‌های ظرف عسل مشاهده شده است که منشأ آن‌ها آدرس‌های IP استفاده شده توسط این تجهیزات هستند که نشان می‌دهد حداقل یک یا چند دستگاه در آن شبکه دچار آلودگی شده‌اند.

۵ جغرافیای دستگاه‌های آلوده

با نگاهی به توزیع جغرافیاییِ آدرس IP دستگاه‌هایی که به تله‌های ظرف عسل حمله کردند، آمار شکل زیر به‌دست آمده است:



شکل ۶ – تفکیک آدرس IP تجهیزات حمله‌کننده بر اساس کشور – ژانویه و آوریل ۲۰۱۷

همان‌طور که پیشتر عنوان شد، اکثر تجهیزاتِ آلوده از نوع دوربین‌های IP و DVRها هستند. بسیاری از آن‌ها در کشورهای چین و ویتنام و همینطور روسیه، برزیل، ترکیه و سایر کشورها قرار دارند.

۱-۵ توزیع جغرافیایی آدرس IP سرورهایی که بدافزارها از آنجا به تجهیزات دانلود شده‌اند

تا مدت زمانی که از سال ۲۰۱۷ گذشته است، بیش از دو میلیون تلاش برای هک و بیش از ۱۱ هزار آدرس IP یکتا توسط شرکت Kaspersky ثبت شده است که از آن‌ها بدافزارهایی برای تجهیزاتِ IoT دانلود شده است.

در جدول زیر این آدرس‌های IP بر اساس ده کشورِ بالای لیست تفکیک شده‌اند.

لیست تفکیکی ده کشور برتر از نظر میزبانی سرورهای بدافزار IoT

Country	Unique IPs
Vietnam	2136
Taiwan, Province of China	1356
Brazil	1124
Turkey	696
Korea, Republic of	620
India	504
United States	429
Russian Federation	373
China	361
Romania	283

اگر کشورها را بر اساس تعداد دانلودها مرتب کنیم، نتیجه‌ای متفاوت از جدول قبلی به‌دست خواهد آمد.

لیست تفکیکی ده کشور برتر از نظر تعداد مرتبه دانلود از سرورهای بدافزار IoT

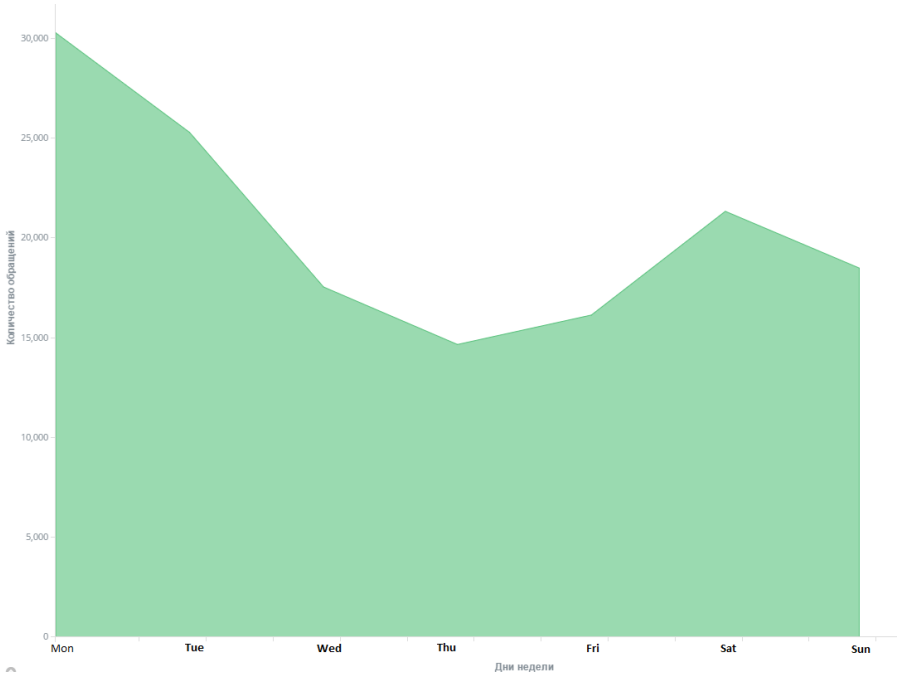
Country	Downloads
Thailand	580267
Hong Kong	367524
Korea, Republic of	339648
Netherlands	271654
United States	168224
Seychelles	148322

France	68648
Honduras	36988
Italy	20272
United Kingdom	16279

به نظر می‌رسد که تفاوت در این دو جدول به دلیل وجود سرورهای ضدگلوله[11] در بعضی از این کشورها می‌باشد، بدین معنی که انتشار بدافزار بسیار سریع‌تر و آسان‌تر از آلوده‌سازی تجهیزاتِ IoT می‌باشد.

۲-۵ توزیع فعالیت حمله بر اساس روزهای هفته

در حین بررسی فعالیت باتنت‌های IoT، برخی پارامترهای عملیاتیِ آنها نیز مورد تحقیق قرار گرفته است. مشخص شده که در بعضی روزهای خاص از هفته، فعالیت‌های مخرب (همچون اسکن، حمله به پسورد و تلاش برای اتصال) دچار افزایش می‌شود.



شکل ۷ - توزیع حمله‌ها بر اساس فعالیت در روزهای مختلف هفته

به نظر می‌رسد که دوشنبه‌ها برای تبهکاران سایبری نیز روز پرکاری است. توضیح خاصی برای تفسیر این رفتار عجیب یافت نشده است.

[11] bulletproof server

۶ نتیجه‌گیری

افزایش تعداد بدافزارهایی که تجهیزات IoT را هدف قرار داده‌اند و همین‌طور حوادث امنیتی مشابه نشان می‌دهد که امنیت در تجهیزات هوشمند موضوعی بسیار جدی است. سال ۲۰۱۶ نشان داد که این تهدیدات نه صرفاً انتزاعی بلکه بسیار واقعی هستند. رقابت فعلی در بازارِ DDoS، تبهکاران سایبری را وادار کرده تا برای انجام حملات قدرتمندتر به منابعی جدید رو بیاورند. باتنتِ Mirai نشان داد که می‌توان از تجهیزات هوشمند بدین منظور استفاده کرد. در حال حاضر میلیاردها تعداد از این تجهیزات در دنیا وجود دارد و بنا بر پیش‌بینی تحلیل‌گران شرکت‌های مختلف، این تعداد در سال ۲۰۲۰ به ۲۰ الی ۲۵ میلیارد خواهد رسید.

در پایان، تعدادی راه‌کار به منظور حفظ امنیت تجهیزات در برابر آلودگی ارائه شده است:

۱. اجازه‌ی دسترسی به دستگاه خود را از خارج از شبکه‌ی محلی ندهید، مگر آنکه واقعاً نیازمندِ این موضوع باشید.
۲. تمام سرویس‌های شبکه که نیازی به آنها ندارید را غیرفعال کنید.
۳. اگر دستگاهی دارای یک پسوردِ از پیش تعیین‌شده و غیر قابل تغییر بوده و یا یک اکانت از پیش تعیین‌شده و مشخص دارد که نمی‌توان آن را غیرفعال کرد، تمامی سرویس‌های مورد استفاده‌ی آنها در شبکه را غیرفعال کرده و یا دسترسی به آنها از خارج از شبکه‌ی محلی را غیرممکن سازید.
۴. قبل از استفاده از دستگاه، پسورد را تغییر داده و از یک پسورد جدید و قوی استفاده کنید.
۵. میان‌افزار تجهیزات خود را به طور مرتب به نسخه‌های جدیدتر (در صورت وجود) به‌روزرسانی کنید.

در صورت پیروی از این چند راه‌کار ساده، می‌توان از درصد زیادی از بدافزارهای حال حاضرِ IoT مصون ماند.