بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

گزارش افزایش حملات ثبت شده به پورت ۲۳ در شبکه کشور

مرداد ۱۳۹۷

۱ مقدمه

بر اساس مشاهدات حسگرهای مرکز ماهر در شبکه کشور، در روزهای گذشته حجم حملات ثبت شده به پورت ۲۳ (telnet) افزایش چشمگیری داشته است. بر اساس بررسی‌های انجام شده، منشاء این حملات عمدتا تجهیزات IoT آلوده نظیر مودم‌های خانگی و به ویژه روترهای میکروتیک بوده و هدف آن نیز شناسایی و آلوده‌سازی تجهیزات مشابه است. مهمترین راهکار پیشگیری و مقابله با این تهدید، بروزرسانی firmware تجهیزات و مسدودسازی دسترسی به پورت‌های کنترلی از جمله پورت ۲۳ و ۲۲ است.

۱-۱ حملات IoT

تعداد حملات صورت گرفته بر روی دستگاه‌های IoT روز به روز در حال افزایش است. سطح پایین امنیت در بسیاری از این ابزارها، آنها را به هدف ساده‌ای برای حمله تبدیل می‌کند به طوری که بسیاری از قربانیان حتی متوجه آلوده شدن سیستم خود نمی‌شوند. هدف بسیاری از مهاجمین آلوده کردن یک سیستم IoT و اضافه کردن آن سیستم به شبکه بات است. بیشتر این بات‌نت‌ها برای ایجاد حمله DoS توزیع شده طراحی شده‌اند. در صورت عدم بروزرسانی دستگاه‌های IoT در هنگام نیاز، احتمال آلوده شدن دستگاه افزایش پیدا می‌کند.

انتشار این بدافزارها معمولا از طریق اسکن آدرس‌های IP و یافتن پورت‌های Telnet و SSH باز صورت می‌گیرد. در ادامه با استفاده از حمله Brute Force و یا استفاده از آسیب‌پذیری‌های شناخته شده ورود به سیستم صورت می‌گیرد. دستگاه‌های IoT از پردازنده‌ها و معماری‌های سخت افزاری مختلفی بهره‌می‌گیرند، به همین منظور توسعه‌دهندگان بدافزار برای اطمینان از اینکه برنامه آنها تعداد بالایی از این دستگاه‌ها را آلوده کند، فایل خود را برای معماری‌های مختلف آماده می‌کنند. در حملات مربوط به IoT معمولا ابتدا نوع پلتفرم دستگاه بررسی شده و پس از آن فایل اجرایی مربوطه در سیستم نصب می‌شود. پس از اجرای فایل باینری مخصوص دستگاه، اتصالی به یک سرور C&C برقرار شده و بات منتظر دستوری از بات‌مستر راه‌دور می‌ماند.

بیشترین معماری‌های مورد هدف عبارتند از x86، ARM، MIPS، PowerPC، SuperH و SPARC که بیشتر در ابزارهایی مانند روترها، مودم‌ها، دستگاه‌های NAS، سیستم‌های CCTV، سیستم‌های ICS و بسیاری ابزارهای IoT دیگر به کار می‌روند. بدافزار تولید شده با پوشش هر چه بیشتر معماری‌های مختلف، طیف گسترده ای از ابزارهای IoT را هدف می‌گیرد.

در ادامه جزییاتی از بدافزارهای ثبت شده بر روی پورت ۲۳ ارائه شده است که عمده این بدافزارها از خانواده‌ی Mirai می‌باشند.

نوع	تعداد بدافزار	سیستم هدف
ELF:FUp-B [Trj]	2	**لینوکس**
Linux.Siggen	5	**لینوکس**
Linux/Gafgyt.AMD	1	**لینوکس**
Miner	2	**لینوکس**
Dofloo	5	**لینوکس**
Linux.Ganiw	4	**لینوکس**
Mirai	24	**لینوکس**
DDoS.Linux.Agent	1	**لینوکس**
DDoS.Linux.Ddostf	3	**لینوکس**
Downloader.Linux.Tsunami	1	**لینوکس**
Downloader.Shell.Agent	6	**لینوکس**

بدافزار دسته ELF:FUp-B [Trj]

این بدافزار لینوکسی تنها توسط آنتی‌ویروس Avast شناسایی شده است.

نوع	نام بدافزار	هش
ELF:FUp-B [Trj]	Avast-Mobile#ELF:FUp-B [Trj]	43d45d6f24bda7869d608293b9cf17035e03fa2f0ab851f7702bd369d1462733
	Avast-Mobile#ELF:FUp-B [Trj]	f77132d7d21294305c6d994cd86869acf201475e9e155e1fd2f932e01d6fc41d

Linux.Siggen

این بدافزار تنها توسط آنتی‌ویروس DrWeb شناسایی شده است به احتمال قوی از سیستم قربانی برای ماینینگ استفاده می‌کند.

نوع	نام بدافزار	هش
Linux.Siggen	DrWeb#Linux.Siggen.685	12d6f7971e5797e060621aa150eda78e814a3a9dab093f6e58d83cd94a71ced1
	DrWeb#Linux.Siggen.685	617233041f2011e400ec0ace47887f5e5d076e7ded89b4f8f36e4780efea6da0
	DrWeb#Linux.Siggen.685	9c3b289741c14e9e74a54d3cedc2157d2450c45730890caae4cbe143adc24efe
	DrWeb#Linux.Siggen.685	ab064c90cabe219ed71b6a465c7d2a11060ff50c8a4b03389a05db70d7e660ad
	DrWeb#Linux.Siggen.685	e4eab741f001cea55b4d8b3e3034147eb1804e4507798f2a61e76477154b46eb

Linux/Gafgyt.AMD

بدافزار Linux.Gafgyt یکی از بدافزارهایی است که بر روی سیستم‌های IoT مشاهده شده است. این بدافزار پس از نصب و متصل شدن به باتنت معمولا اقدام به حمله منع سرویس می‌کند. این بدافزار ممکن است وب‌سرورها یا روترهای دارای واسط وب CGI را مورد حمله قرار دهد. این بدافزار قادر به اجرای حمله Bruteforce بر روی روتر بوده و امکان استخراج اطلاعات از سیستم را دارد. نمونه بدست آمده از سنسور هانی پات مخصوص سیستمی با معماری ARM x86-64 است.

نوع	نام بدافزار	هش

Linux/Gafgyt.AMD	ESET-NOD32#a variant of Linux/Gafgyt.AMD	f67372717690857234af9dc69e9951bd008d617377f057bdd787ea5f52bb1252

Miner

این بدافزارها دسته ای از فایل های مخرب هستند که با انتقال به سیستم قربانی از توان پردازشی دستگاه استفاده کرده و اقدام به استخراج پول رمزپایه می‌کنند. بسیاری از دستگاه‌های IoT به دلیل امنیت پایین و عدم بروزرسانی به موقع در معرض این آلودگی‌ها قرار می‌گیرند. این دسته از بدافزارها ماینرهای مبتنی بر لینوکس هستند، که از طریق پورت ۲۳ منتشر شده اند.

نوع	نام بدافزار	هش
Miner	ESET-NOD32#Linux/CoinMiner.AR	783028f95b7f1ea7cb1ea2a29f09371708d6a154c9f4b72cc8bc213fc5b2e555
Miner	Kaspersky#not-a-virus:HEUR:RiskTool.Linux.BitCoinMiner.b	e651a05c9cb0bde4e8efa635f699ba3e186afd4ae4c42760e3d97ffa01d8c8ca

Dofloo

بدافزار Linux.Dofloo یک تروجان برای سیستم‌های مبتنی بر لینوکس است که بر روی سیستم‌های x86، ARM یا MIPS قابل اجرا است. این تهدید با نام AES DDoS نیز شناخته می‌شود، زیرا ارتباطات با C&C سرور توسط الگوریتم AES رمز شده اند. این تروجان یک Backdoor در دستگاه آلوده باز کرده و منتظر فرمان مهاجم راه دور می‌ماند. این بدافزار معمولا برای حملات DDoS استفاده می‌شود، ولی امکان جمع آوری اطلاعات درباره CPU، ترافیک شبکه و حافظه دستگاه آلوده و ارسال آنها به مهاجم را نیز دارد. این حمله نیز جز حملات شناسایی شده به دستگاه های IoT است. نمونه های شناسایی شده در هانی پات برای معماری Intel 80386 طراحی شده اند.

نوع	نام بدافزار	هش
Dofloo	Kaspersky#Backdoor.Linux.Dofloo.a	496f959c5a101d3ce26b927610fbe674cffcf14b4e51bd83c877a9d44b912d59
	Kaspersky#Backdoor.Linux.Dofloo.a	e6e28543f3e382d122f1c07c05a49f27f0a7910cf1cf34adb79363962b8b6e5c
	Kaspersky#Backdoor.Linux.Dofloo.a	5a8dbe7232c275130ef00e3a040344b6ccf2102866d24bb2f7b2d73630b36e07
	Kaspersky#Backdoor.Linux.Dofloo.b	fc519396d5c6fe71aa87bdcc2cc11635bc2db7a7f7c75f50670d9493cb528e59
	Kaspersky#HEUR:Backdoor.Linux.Dofloo .d	064ef9091cd000560ab87e9af55bc1d9ffdbd6770c0e37468a9d03251ab868c3

Linux.Ganiw

بدافزار Linux.Ganiw.A یک Backdoor و bot agent است که پلتفرم لینوکس را هدف قرار می‌دهد. بدافزار به یک سرور راه دور متصل شده و پس از شناسایی، اطلاعات سیستم را ارسال می کند و در مقابل دستوراتی را برای اجرا بر روی سیستم آلوده دریافت می کند. این بدافزار می تواند برای حملات DDoS مورد استفاده قرار گیرد.

نوع	نام بدافزار	هش
Linux.Ganiw	Kaspersky#HEUR:Backdoor.Linux.Ganiw.d	885fdc6be061dae3a95501f636924c1e7305684a468cd382ed8246e8bf84a5ff
	Kaspersky#HEUR:Backdoor.Linux.Ganiw.d	9282f80746ec95497deb554a1260a80a0bda445e8ea39cb8f8c8416075ed1e64
	Kaspersky#HEUR:Backdoor.Linux.Ganiw.d	dee03b7fd3954d0d653ef62cfd5f37711bae64e7fb31cc79ced4c5050d095f5c
	Kaspersky#HEUR:Backdoor.Linux.Ganiw.d	f5e21fa152932bc0637665337788eb6bc0e0eeb91ac0fe24f56e1347e54bca8c

Mirai

بدافزار میرای یکی از معروف ترین بدافزارهای IoT فعال در سطح جهان است. متن باز بودن کد این بدافزار باعث شده مهاجمین زیادی از قسمت های مختلف این کد برای توسعه بدافزارهای شخصی استفاده کنند.

نوع	نام بدافزار	هش
Mirai	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	b5d59a8c90183903002e1c4bde017ed2bfb9e755aab8d70e99cc06746d611f04
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	1e3d9a75cea9e8d7d6ffa5f6fd54b8d7126c89680b47e28406157987b39b05d2
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	a7a70052c41f4e56c6b7904314af842f2bbcc8e710ac3d3898ca7e308e8c132c
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	20ab765e26f914294c05ea94d094edfc54ce16fa04c01033fcab82129a0a4735
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	904a3a795c979d5bd82ac69ad4e9e251deb4729e29b4856c8b24c420c77c9eae
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	c9d4097fd39d04f2bf943f289c4467a1dcd98cbc6115d6d56c2c894082a257e0
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	4727173f50692b61709f9a30a4cbbfccede13e59976f3ce2ac433bdd9930c1c0
	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	f438dd2e40886d736da0242ebe0d00ed80bc326ef7592308b92fe048799af3d2

ff0431199a0aa95e24cd93ec758c69238914f8dc3d0487457893796063effeba	Kaspersky#HEUR:Backdoor.Linux.Mirai.b	
e676084f42899c213ebbdbf594dc9432beba8e2bb83a2e25fca6f7d855e7e3f2	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
24d79af69d0b071f6d58d01b86e5f75bb0f651aa1fa5de4da704d922bf71bfa4	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
a7b0fa9412e6b2abc551b6ecafcbfe802fa83fe3aa6fb98ebfc4406eb04bd19c	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
d5b066634c4ac598f93897cf53ed7646bc41aebf2d9ee67d02a18550d8a54132	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
f215029a8a9431143e359244a8421f9241f3db3bca12efc8a2449a1907fd0b06	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
e76ea97db82678fd7ee181b8f94fd6a9224b351ce4a60b8c1b09f0b2bf82b0a4	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
fcb05a75d4c2fe4bfd3aa70b3a18f988fb6d2c5317b09e4e601d3c772680f5d6	Kaspersky#HEUR:Backdoor.Linux.Mirai.ba	
0abdd43c666f1f7b05608e51a71c39da6cf8643a58cc8b3820d1fe09f4b7940b	Kaspersky#HEUR:Backdoor.Linux.Mirai.n	
4b1bddc6aa4a87793cc10da6e171aa67b5ba93cfd7bda9e341cb1ea52003a131	Kaspersky#HEUR:Backdoor.Linux.Mirai.n	
7419fe3a6e0667d6cdb6a70055436bc4636d2aa7f7d567a7b03336b2fcff14dd	Kaspersky#HEUR:Backdoor.Linux.Mirai.n	
08b11375ee43745b196c0fb6cb4dc075b96215f310cadc682081373c63fe7ea6	Kaspersky#HEUR:Backdoor.Linux.Mirai.n	
6616a8aa7cf8f1a6c2ba116a4184099b1522bd6863035476bf92afc1188473db	Kaspersky#HEUR:Trojan-Downloader.Linux.Mirai.d	
c4ae828d8e20b4c56e85dde21117e500c30729cc03d401058f6f831ee0197a92	Kaspersky#HEUR:Trojan-Downloader.Linux.Mirai.d	
88bbd1179076120e88169ea9fae02dcf8fb48db47fcc92421a9504146959fa4e	Kaspersky#HEUR:Trojan-Downloader.Linux.Mirai.d	
dd9b375bc3679513e722c1ee027f2e319cab6b235ebb0adfbaacbe29d1508739	Kaspersky#HEUR:Trojan-Downloader.Linux.Mirai.d	

DDoS.Linux.Agent

این بدافزار در سایر آنتی ویروس ها با نام Xorddos شناخته می‌شود. این بدافزار یک Backdoor را بر روی کامپیوتر یا سیستم آلوده باز می کند. نام بدافزار به دلیل استفاده از رمزنگاری XOR در کد بدافزار و ارتباطات با C&C انتخاب شده

است. این بدافزار نسخه های گوناگونی برای معماری های x86 و ARM ارائه داده است. اصلی ترین اقدام بدافزار اجرای حمله DDoS است با این حال تروجان امکان دانلود و اجرای فایل، پاک کردن سرویس ها و نصب ماژول های دیگر را دارد.

نوع	نام بدافزار	هش
DDoS.Linux.Agent	Kaspersky#HEUR:Trojan-DDoS.Linux.Agent.g	f83cb2e114ef666439fb6545ce642e3ef51a785655fd0cd46fbd6b73885be601

DDoS.Linux.Ddostf

این بدافزار مبتنی بر لینوکس بوده و به منظور ایجاد حمله DDoS طراحی شده است، با این حال امکان انجام برخی کارهای دیگر از قبیل ارسال اطلاعات کاربر به مهاجم را نیز دارد.

نوع	نام بدافزار	هش
DDoS.Linux.Ddostf	Kaspersky#HEUR:Trojan-DDoS.Linux.Ddostf.a	4126e926732a38e1406a119c39585c9eaffe700911421cbf1b9532039b29ed08
	Kaspersky#HEUR:Trojan-DDoS.Linux.Ddostf.a	c0a7992ef58bb29f8c58b0670486233d0240cf2b5930372b2caf1e01b04e61a6
	Kaspersky#HEUR:Trojan-DDoS.Linux.Ddostf.a	43ae491b05e56f71b94fe8247ac2f30c95bb2946dc4f77691a960de3a0393480

Downloader.Linux.Tsunami

این بدافزار یک کرم است که از طریق سرویس تلنت بروی پورت ۲۳ منتشر شده و با استفاده از نام کاربری و گذرواژه های پرکاربرد سعی در نفوذ به سیستم را دارد. این بدافزار یک Backdoor در سیستم آلوده باز کرده و منتظر فرمان از سمت C&C می شود. دستگاه های آلوده به بات نت اضافه شده و برای حمله DDoS استفاده می شوند. نسخه های این بدافزار سیستم های IoT را هم مورد هدف قرار می دهند.

نوع	نام بدافزار	هش
Downloader.Linux.Tsunami	Kaspersky#HEUR:Trojan-Downloader.Linux.Tsunami.a	9baec7b29cdcebb949716bddf44754a47d6404f75d7f3a48350c7f69327019d8

Downloader.Shell.Agent

این بدافزار ، برنامه اجرایی مبتنی بر لینوکس است که عملیات ماینیگ انجام می دهد.

نوع	نام بدافزار	هش
	Kaspersky#HEUR:Trojan-Downloader.Shell.Agent.bf	36fc374823925e9d1c14bd41e282284111fbd345c8d9755974ea0e568f8ddbee

4f75eec50688856480316bb404ba90d33d5de43ded45066b5a3d9b3fb7cc8720	Kaspersky#HEUR:Trojan-Downloader.Shell.Agent.bf	Downloader.Shell.Agent
ab585ecaba6dc3022b4565cdbd125b520bf9c281f009f65e5d0170a4d65ff70b	Kaspersky#HEUR:Trojan-Downloader.Shell.Agent.bf	
12a51f899c8fab7c131b4b851cca0c84e95f31aadc86ce1198fae91126304127	Kaspersky#HEUR:Trojan-Downloader.Shell.Agent.bf	
7f4baf3bc359fe5679b76b2873ee5d3e474f6436bbb2f3027383ac87b9e2b590	Kaspersky#HEUR:Trojan-Downloader.Shell.Agent.bf	
0a4e4c573dd4481cdd62265031ee0e9abcd093d940f7d1cb1daeffddd0e97d0d	Kaspersky#HEUR:Trojan-Downloader.Shell.Agent.p	