۱) مقدمه

گزارش پیش‌رو، به معرفی، تحلیل و شناسایی فعالیت بدافزاری موسوم به CPUMiner پرداخته‌شده است. پرداختن به این موضوع از آن‌جهت اهمیت دارد که تعداد قابل‌توجهی از سیستم‌های متعلق به زیرساخت‌های حیاتی کشور، به این بدافزار آلوده شده‌اند.

۲) معرفی برنامه

CPUMiner یک نرم‌افزار کاربردی است که بر روی کلاینت نصب شده و پس از برقراری ارتباط با سرورهای مشخص، تعدادی بلوک Hash دریافت می‌کند. سپس با استفاده از منابع خود (به‌خصوص CPU) اقدام به پویش و تلاش (اصطلاحاً Mining) برای شکستن و حدس زدن آن می‌کند. پس از انجام این عملیات، نتیجه به سمت سرور ارسال‌شده و در ازای آن، مبلغی (در واحد BitCoin) به کیف دیجیتالی کلاینت واریز می‌شود.

BitCoin واحد پول رایج در فضای مجازی و شبکه اینترنت است که برای اولین بار در سال ۲۰۰۹ معرفی شد. به این صورت که هر فرد یک کیف پول الکترونیکی (BitCoin Wallet) برای خود تعریف می‌کند که با شرکت کردن در فرآیندهای تولید و توزیع BitCoin -که اصطلاحاً Bitcoin Mining نامیده می‌شوند- می‌تواند بر مقدار موجود در این کیف بیافزاید.

به‌طور معمول، فرآیندهای Bitcoin Mining به این صورت است که افرادی موسوم به Minerها، مسئله‌ای (مانند برگرداندن پاسخ یک بلوک Hash شده) را در فضایی موسوم به Pool مطرح می‌کنند. کلاینت‌ها با اتصال به این Poolها (شکل ۱) و ارائه آدرس کیف پول خود، در صورت حل مسئله، تعدادی Bitcoin به دست خواهند آورد(شکل ۲).

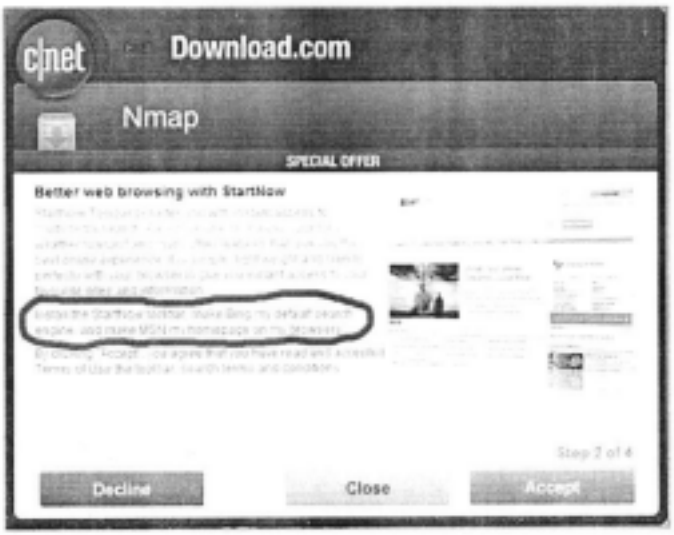
شکل ۱: نمونه‌ای از نحوه اتصال به Pool

شکل ۲: ارائه آدرس کیف پول دیجیتال جهت واریز BitCoin

فعالیت‌هایی به این شکل، زمانی جنبه امنیتی به خود می‌گیرد که هکرها، این برنامه را در سیستم‌های کاربران اینترنتی قرار می‌دهند تا با سوءاستفاده از منابع پردازشی آن‌ها اقدام به جمع‌آوری BitCoin نمایند. این برنامه بدون اطلاع و اجازه کاربر (PUP[1])، روی سیستم هدف بارگذاری شده و با هماهنگی و برقراری ارتباط با فرماندهی خود عملیات CPUMining اجرا می‌کند.

[1] Potentially Unwanted Program

شایع‌ترین روش برای انتشار برنامه CPUMiner استفاده از تکنیک Bundling است. به این صورت که برنامه یا کد مخرب در قالب برنامه‌های قانونمند توسط کاربر دانلود شده و بدون اطلاع آن، در پس‌زمینه شروع به فعالیت می‌کند. اخیراً بیشتر وب‌سایت‌های دانلود رایگان مانند Download.com و Softnic.com برخی برنامه‌های تبلیغاتی را با عناوینی نظیر "Download Managers"، "Download Client" یا "Installers" (که Miner در آن‌ها Bundle شده) برای درآمد اقتصادی به‌کار می‌گیرند (شکل ۳). البته این برنامه‌های اضافی به همراه برنامه درخواستی پیشنهاد و بارگیری می‌شوند. برای جمع‌بندی خلاصه‌ای از مطالب گفته‌شده حول این برنامه در جدول ۱ ارائه‌شده است.



شکل ۳: دریافت برنامه‌ای معتبر که کد مخرب در آن Bundle شده

جدول ۱: شناسنامه بدافزار

شناسنامه بدافزار	نام	CPU Miner
	سال کشف	
	روش انتشار	استفاده از تکنیک Bundling
	تأثیرات	دانلود کردن نرم‌افزارهای مخرب دیگر و اجرای آنها امکان سرقت اطلاعات از سیستم قربانی امکان دسترسی راه دور به سیستم قربانی کاوش بیت کوین

۳) شناسایی فعالیت

با توجه به اینکه برنامه CPUMiner به صورت عمومی قابل دسترس است[۲] و کاربردهای معمول دارد، شناسایی و گزارش تنها در موارد زیر حائز اهمیت است:

- برنامه به شکلی غیرقانونی و با استفاده از نفوذ یا آلوده‌سازی به سیستم هدف منتقل‌شده باشد.
- کاربری در داخل سازمان، با اطلاع آن را نصب کرده و در حال استفاده از آن است؛ که برخلاف سیاست‌های امنیتی سازمانی است. همچنین با توجه به این نکته که ثبت اطلاعات کاربر، سرقت و اشتراک‌گذاری این اطلاعات، جزو مشخصه‌های رفتاری این‌گونه برنامه‌هاست؛ امکان افشای اطلاعات سازمانی نیز مطرح می‌شود.

۳-۱) روش‌های شناسایی

در مراجع مختلف روش‌هایی برای شناسایی این‌گونه فعالیت‌ها در سطح شبکه ارائه‌شده است. نمونه‌ای شواهد شبکه‌ای به‌منظور شناسایی فعالیت CPUMiner عبارت‌اند از:

- به‌کارگیری سیستم تشخیص نفوذ (IDS)

مشخصات بسته‌های ترافیکی، کلمات کلیدی ارتباط و الگوهای مبادلاتی نمونه پارامترهایی است که می‌توان با آن‌ها قواعد طراحی کرده و در IDS قرار داد که امکان شناسایی را با درصد بالایی فراهم می‌کند.

- پالایش جریان‌های ترافیکی و فیلتر مبالات با سرورهای کنترل و فرماندهی شناخته‌شده

سرورهای کنترل و فرماندهی این برنامه‌ها توسط مراجع مختلف شناسایی و منتشر می‌شوند. با جستجوی در ترافیک، می‌توان ارتباط با این سرورها را شناسایی کرد.

روش‌های فوق مبتنی بر اطلاعات سطح شبکه است. در سطح میزبان نیز نشانه‌هایی از قبیل افزوده شدن افزونه‌های مرورگر، مصرف غیرمعمول منابع پردازشی مانند CPU -زمانی که کاربر دخیل نیست- وجود دارند.

۳-۲) شناسایی در شبکه زیرساخت‌های حیاتی

رصد و تحلیل مبادلات زیرساخت‌های حیاتی در مرکز افتا، شواهدی مبنی بر فعالیت این بدافزار در تعدادی از سازمان‌ها را نشان می‌دهد. این شواهد از اطلاعات سیستم تشخیص نفوذ و تحلیل جریان‌های ترافیکی -که با سرورهای Mining بوده- برگرفته‌شده است.

- رویدادهای امنیتی سیستم تشخیص نفوذ با مطابقت دادن امضای این بدافزار تولیدشده‌اند. به‌عنوان نمونه در شکل ۴ بخشی از بسته‌های این بدافزار ارائه شده است. آن‌چنان‌که در این تصویر مشاهده می‌شود، Agent مورداستفاده CPUMiner است. همچنین سایر پارامترهای مربوط به Login در این بسته قابل‌مشاهده است.

[۲] Download link: https://github.com/pooler/cpuminer

```
{"method": "login", "params": {"login":
"46DXvzqHu64G6TftbF3QV42jSD99ME2ZDdGALoAxQa1mYWCRNLx57e6N2SyU9dgRKR2ZLcz
uK27tT4cG2uWdiakz928cbTu", "pass": "x", "agent": "cpuminer-multi/0.1"},
"id": 1}
```

شکل ۴ بخشی از بسته‌های مبادله شده

- این بسته‌های به سمت IPهایی از خارج از کشور هدایت شده‌اند که مربوط به سرورهای کنترل و فرماندهی سرویس‌های Mining است. با مراجعه به صفحه وب از این IPها وضعیت سرویس‌دهی آن‌ها قابل‌رؤیت است (شکل ۵).

شکل ۵ صفحه وب از سرورهای Mining که بیانگر وضعیت آن‌هاست

- درخواست‌های DNS برای ارتباط با دامنه‌های اینترنتی نیز نشان از ارتباط با دامنه‌هایی دارد که سرویس Pool ارائه می‌دهند. آن چنانکه در شکل ۶ مشاهده می‌شود، دامنه‌های Pool که سرورهای کنترل و فرماندهی این برنامه محسوب می‌شوند، بارها و در بازه زمانی بلندمدت بازبینی شده‌اند.

First Resolve	First Resolve	Domain	Resolved IP
2015-05-14 11:26:27.775	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.83.168.41
2015-05-14 11:26:27.775	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.129.44.156
2017-01-11 14:27:19.291	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.129.46.87
2015-05-14 11:26:27.775	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.129.46.191
2017-02-27 09:51:16.936	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.83.129.195
2017-04-05 00:18:44.491	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	62.210.29.108
2015-05-14 11:26:27.775	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.129.44.157
2017-06-15 18:22:32.208	2017-08-05 17:24:27.197	com.minexmr.pool	37.59.56.102
2017-06-21 01:50:56.606	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.114.218
2017-06-21 00:45:25.472	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.113.214
2017-06-21 00:45:25.472	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.113.168
2017-06-21 01:50:56.606	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.114.82
2017-07-04 02:27:12.639	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	51.15.145.187
2017-07-07 03:33:22.511	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.129.13.151
2017-07-07 03:33:22.511	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.83.189.246
2017-07-07 03:33:22.511	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.83.189.247
2017-07-07 03:33:22.511	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.129.13.124
2017-07-04 02:27:12.639	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	51.15.145.169
2017-07-04 02:27:12.639	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.229.214
2017-06-21 00:45:25.472	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.113.67
2017-07-04 02:27:12.639	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	163.172.229.213
2015-05-14 11:26:27.775	2017-08-05 18:04:27.512	fr.crypto-pool.xmr	212.83.168.39
2017-07-31 10:53:56.137	2017-07-31 10:53:56.137	com.wkery.xmr	51.15.145.169
2017-07-31 10:53:56.137	2017-07-31 10:53:56.137	com.wkery.xmr	212.83.189.247
2017-07-31 10:53:56.137	2017-07-31 10:53:56.137	com.wkery.xmr	163.172.113.67
2017-07-31 10:53:56.137	2017-07-31 10:53:56.137	com.wkery.xmr	212.129.44.157
2017-07-31 10:53:56.137	2017-07-31 10:53:56.137	com.wkery.xmr	163.172.113.214

1# Online Mining Server — Detected IP Range of Server#1
2# Online Mining Server — Detected IP Range of Server#2
3# Online Mining Server

شکل ۶ دامنه‌های ارائه‌دهنده سرویس Pool و IPهای ترجمه‌شده

۴) راهکارهای پیشگیری و پاک‌سازی

توصیه‌های امنیتی پیشگیری از آلودگی عبارت‌اند از:

در سطح میزبان:

- از بروز بودن آنتی‌ویروس‌ها و نرم‌افزارهای مورداستفاده مطمئن شوید.
- از تنظیمات امنیتی خود مطمئن شوید و هر چند وقت یک‌بار پویش آسیب‌پذیری را انجام دهید.
- آگاه کردن کاربران برای عدم کلیک بر روی لینک‌های مشکوک.
- بازنکردن ضمیمه‌های ایمیل‌های مشکوک
- جلوگیری از دانلود نرم‌افزارها از منابع نامعتبر

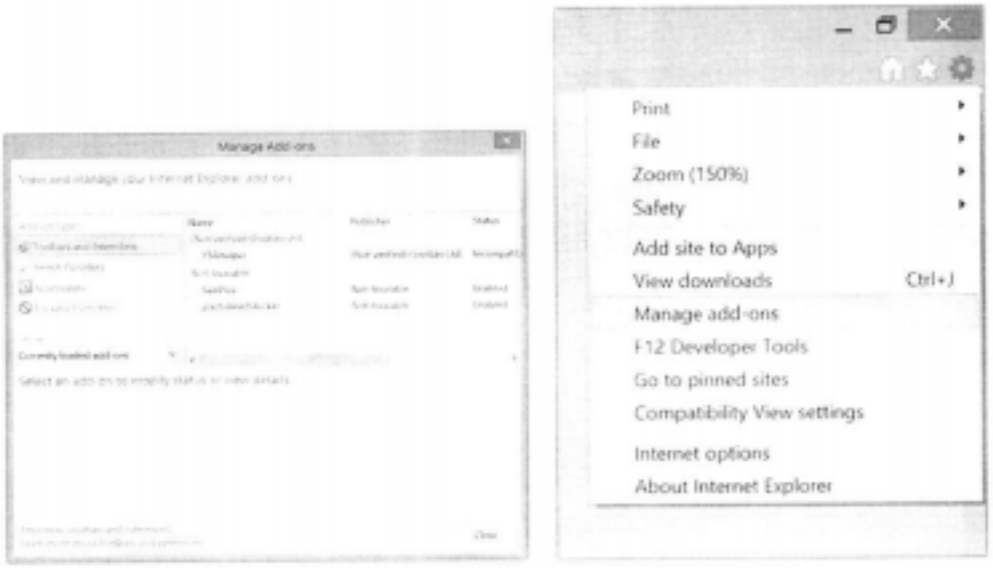
در سطح شبکه:

- استفاده از ضدویروس‌های تحت شبکه

برای پاک‌سازی این بدافزار از روی سیستم آلوده می‌توان از آنتی‌ویروس‌های معتبر و بروز نظیر Kaspersky و Symantec استفاده نمود. همچنین می‌توان در قسمت کنترل پنل، برنامه‌های نصب شده را مشاهده نمود و از این طریق برنامه را حذف کرد (شکل ۷).

شکل ۷: حذف از برنامه‌های نصب‌شده در کنترل پنل

همچنین برای پاک‌سازی سیستم باید به قسمت افزونه‌های مرورگرها مراجعه کرد و افزونه مربوط به CpuMiner را حذف نمود. برای مثال قسمت افزونه‌های مرورگر اینترنت اکسپلورر را مشاهده می‌کنیم و نحوه حذف نیز قابل انجام است (شکل ۸). در جدول خلاصه‌ای از راهکارهای پیشگیری و پاک‌سازی ارائه‌شده است.



شکل ۸. مدیریت افزونه‌ها در مرورگر اینترنت اکسپلورر

جدول ۲. راهکارهای پیشگیری و پاکسازی

راهکار پیشگیری	سطح شبکه	• استفاده از ضدویروس‌های تحت شبکه
	سطح میزبان	• به‌روز بودن نرم‌افزار ضدبدافزار نصب‌شده بر روی سیستم • آگاه کردن کاربران برای عدم کلیک بر روی لینک‌های مشکوک • باز نکردن ضمیمه‌های ایمیل‌های مشکوک • جلوگیری از دانلود نرم‌افزارها از منابع نامعتبر
راهکار پاک‌سازی	در سطح سیستم با استفاده از ابزار	• استفاده از آنتی‌ویروس‌های معتبر و بروز شده نظیر Kaspersky و Symantec و sophos
	بررسی پاک بودن سیستم	• استفاده از ابزارهای تحلیل ترافیک و بررسی وجود یا عدم وجود ترافیک شبکه‌ای به نام‌های دامنه در قسمت‌های پیشین