بسمه‌تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

سیستم های لینوکس، هدف بدافزار جدید درب پشتی

گزارش بدافزار

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۴۰۲/۰۲/۲۷

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴

(۰۲۱) ۸۸۱۱۵۷۲۴

cert.ir

فهرست مطالب

۱ مقدمه

یک شکل کاملاً جدید و گزارش نشده از BPFdoor اخیراً توسط آزمایشگاه Deep Instinct کشف و مورد بررسی قرار گرفت. استفاده از Berkley Packet Filter، روشی غیرمعمول برای دریافت دستورالعمل‌ها و اجتناب از شناسایی توسط این بدافزار است که از محدودیت‌های فایروال در ترافیک ورودی فراتر می‌رود و از همین رو به BPFdoor نام‌گذاری شده‌است. این بدافزار به Red Menshen (Red Dev 18) مرتبط است.

۲ جزئیات آسیب‌پذیری

بدافزاری که اخیراً کشف شده است به نام BPFdoor، بیش از پنج سال است که به طور مخفیانه سیستم‌های لینوکس و سولاریس را مورد هدف قرار داده است. BPFDoor یک درب پشتی لینوکس/یونیکس است که به عوامل تهدید اجازه می‌دهد تا از راه دور به پوسته لینوکس متصل شوند تا به یک دستگاه آسیب‌دیده دسترسی کامل پیدا کنند. این بدافزار نیازی به باز کردن پورت‌ها ندارد، نمی‌توان آن را با فایروال‌ها متوقف کرد و می‌تواند به دستورات هر آدرس IP در وب پاسخ دهد، که آن را به ابزاری ایده‌آل برای جاسوسی شرکت‌ها و حملات مداوم تبدیل می‌کند.

۲-۱ BPFDoor سیستم های لینوکس را هدف قرار می‌دهد

برای ایجاد یک جایگاه پایدار و طولانی مدت در شبکه‌ها و محیط‌هایی که قبلاً نقض شده‌اند، BPFdoor یک درب پشتی منفعل، کمتر شناخته‌شده و مختص لینوکس است که در درجه اول تضمین می‌کند که مهاجم می‌تواند برای مدت طولانی پس از در معرض خطر قرار گرفتن، دوباره وارد یک ماشین آلوده شود.

BPFdoor در ابتدا به دلیل طراحی کاربردی و ظریف و تاکید زیاد بر مخفی‌کاری شناخته شد، که این امر، برای اطمینان از ماندگاری طولانی مدت عدم شناسایی، بسیار اهمیت دارد.

	"New stealthy" 2023 variant	"Old" 2022 variant
Encryption	Static library encryption	RC4 Encryption
Communication	Reverse-Shell	Bind shell and iptables
Commands	No hardcoded commands – all commands are sent through the reverse-shell	Hardcoded commands
Filenames	Not hardcoded	Hardcoded

شکل ۱. تفاوت بین نسخه‌های قدیمی و جدید BPFdoor

دستورات و نام فایل‌های این بدافزار به صورت سخت‌کدگذاری‌شده بود[1] و تا سال ۲۰۲۲ از رمزگذاری RC4، bind shell و iptables برای برقراری ارتباط استفاده می‌نمود.

نوع اخیری که توسط Deep Instinct مورد بررسی قرار گرفته است شامل ارتباطات معکوس پوسته ، رمزگذاری ایستای کتابخانه و تمام دستورات ارسال شده توسط سرور C2 است.

علاوه بر این، با حذف دستورات سخت‌کدگذاری‌شده، بدافزار توسط نرم‌افزارهای ضدویروسی که از تجزیه و تحلیل استاتیک، مانند تشخیص مبتنی بر امضا استفاده می‌کنند، کمتر کشف می‌شوند. این امر ظاهراً با فعال کردن طیف گسترده‌تری از مجموعه‌های دستوری، انعطاف‌پذیری بیشتری به بدافزار می‌دهد.

۲-۲ تجزیه بسته های جادویی

BPFDoor یک در پشتی غیرفعال است، به این معنی که می‌تواند به یک یا چند پورت برای بسته‌های ورودی از یک یا چند میزبان گوش دهد، که مهاجمان می‌توانند از آن برای ارسال دستورات از راه دور به شبکه در معرض خطر استفاده کنند. این بدافزار از یک فیلتر بسته Berkeley (BPF به نام درب پشتی) استفاده می‌کند که در رابط لایه شبکه کار می‌کند و می‌تواند تمام ترافیک شبکه را ببیند و بسته‌های ارسالی را به هر مقصدی ارسال کند. به دلیل موقعیت یابی آن در چنین سطح پایینی، BPF از قوانین فایروال تبعیت نمی کند.

BleepingComputer از کریگ رولند، بنیانگذار Sandfly Security، شرکتی که راه حلی بدون عامل برای محافظت از سیستم های لینوکس ارائه می دهد، آموخته است، این نسخه برای سیستم های لینوکس و Solaris SPARC دارد، اما می تواند به BSD نیز منتقل شود. محقق امنیتی کوین بومونت، که یک پست وبلاگی در

[1] hard-coded

BPFDoor منتشر کرد، به BleepingComputer گفت که اپراتورها از یک رمز عبور جادویی برای کنترل اعمال ایمپلنت استفاده می کنند. BPFDoor فقط بسته های ICMP، UDP و TCP را تجزیه می کند، آنها را برای یک مقدار داده خاص و همچنین یک رمز عبور برای دو نوع بسته اخیر بررسی می کند. چیزی که BPFDoor را متمایز می کند این است که می تواند هر پورتی را برای بسته جادویی نظارت کند، حتی اگر آن پورت ها توسط سرویس های قانونی دیگر مانند وب سرورها، FTP یا SSH استفاده شوند. اگر بسته‌های TCP و UDP داده‌های جادویی مناسب و رمز عبور صحیح داشته باشند، درب پشتی با اجرای یک فرمان پشتیبانی‌شده، مانند راه‌اندازی پوسته bind یا reverse، وارد عمل می‌شود. گفته‌شده که بسته‌های ICMP نیازی به رمز عبور ندارند، که اجازه می‌دهد اینترنت را برای اجرای ایمپلنت‌های BPFDoor با استفاده از عملکرد پینگ اسکن کند.

همچنین توانستند فعالیت BPFDoor را در شبکه‌های سازمان‌ها در مناطق جغرافیایی مختلف، به ویژه ایالات متحده، کره جنوبی، هنگ کنگ، ترکیه، هند، ویتنام و میانمار پیدا کنند. ۱۱ سرور Speedtest آلوده به BPFDoor را کشف کردند. همچنین بیان‌شده که مشخص نیست این ماشین‌ها چگونه در معرض خطر قرار گرفته‌اند، به‌ویژه که آن‌ها بر روی نرم‌افزار متن‌بسته کار می‌کنند.

۳-۲ دور زدن فایروال محلی

رولند در یک گزارش فنی جامع در مورد BPFDoor اشاره می کند که این بدافزار از برخی تاکتیک‌های هوشمندانه ضد فرار استفاده می‌کند. در حافظه سیستم قرار دارد و اقدامات ضدشناسایی و پاکسازی را به کار می‌گیرد (محیط فرآیند را پاک می‌کند، هرچند ناموفق، زیرا آن را خالی می‌گذارد)

فیلتر بسته برکلی (BPF) را بارگیری می‌کند و به آن اجازه می‌دهد تا در مقابل هر فایروال‌هایی که به صورت محلی در حال اجرا هستند کار کند تا بسته‌ها را ببیند. قوانین iptables را هنگام دریافت بسته مربوطه تغییر می دهد تا امکان ارتباط مهاجم از طریق فایروال محلی را فراهم کند. باینری را با نامی شبیه به یک شبح معمولی سیستم لینوکس بپوشاند. تغییر نام داده و خود را به صورت /dev/shm/kdmtmpflush اجرا می کند.

تاریخ باینری (timestomping) را قبل از حذف به ۳۰ اکتبر ۲۰۰۸ تغییر می دهد.

رولند معتقد است که توضیحی برای زمان‌بندی، به‌عنوان یک تکنیک ضد شناسایی و پاکسازی در این مورد، می‌تواند این باشد که مهاجم ممکن است سعی کند از باینری در صورت عدم حذف آن محافظت کند.

محقق می گوید که هدف از تاریخ جعلی می‌تواند پنهان کردن بدافزار از جستجوی فایل‌های جدید در سیستم باشد. تغییر قوانین فایروال از اهمیت ویژه ای برخوردار است زیرا به مهاجمان اجازه می‌دهد تا از طریق ترافیکی که فایروال‌ها نمی‌توانند به عنوان مشکوک علامت‌گذاری کنند با درپشتی ارتباط برقرار کنند.

رولند توضیح می‌دهد که وقتی میزبان آلوده یک بسته ویژه BPFDoor را دریافت می‌کند، بدافزار نمونه جدیدی ایجاد می‌کند و قوانین محلی iptables را تغییر می‌دهد تا از میزبان درخواست‌کننده به پورت پوسته تغییر مسیر دهد. به عنوان مثال، ایمپلنت می تواند تمام ترافیک مهاجم را با استفاده از پورت TCP 443 (وب رمزگذاری‌شده) به پوسته هدایت کند. از منظر خارجی، ترافیک مانند ترافیک TLS/SSL به نظر می‌رسد، اما در واقع مهاجم در حال تعامل با یک پوسته ریشه از راه دور روی سیستم است. برای توضیح بیشتر، رولند می‌گوید که برای پوسته محلی، بدافزار پیکربندی «iptables» را تغییر می‌دهد تا تمام ترافیک وارد شده از مهاجم از طریق یک پورت قانونی به محدوده پورت تعریف‌شده در بدافزار هدایت شود. به این ترتیب، مهاجم می تواند یک اتصال را از طریق هر پورتی انتخاب کند، زیرا به پوسته پشت فایروال هدایت می‌شود.

۲-۴ دستورات و شناسایی

یکی دیگر از تحلیل‌های فنی BPFDoor توسط Tristan Pourcelot از شرکت اطلاعاتی درباره تهدید و پاسخ به حادثه ExaTrack، اشاره می‌کند که این بدافزار با نام‌های سخت‌کد متعددی ارائه می‌شود که با رشته‌های فرمان در بسته‌های مربوطه مطابقت دارد: justtryit، justrobot و justforfun برای ایجاد یک پوسته bind در پورت های ۴۲۳۹۱ تا ۴۲۴۹۱ سوکت یا sockettcp برای تنظیم پوسته معکوس به آدرس IP موجود در بسته

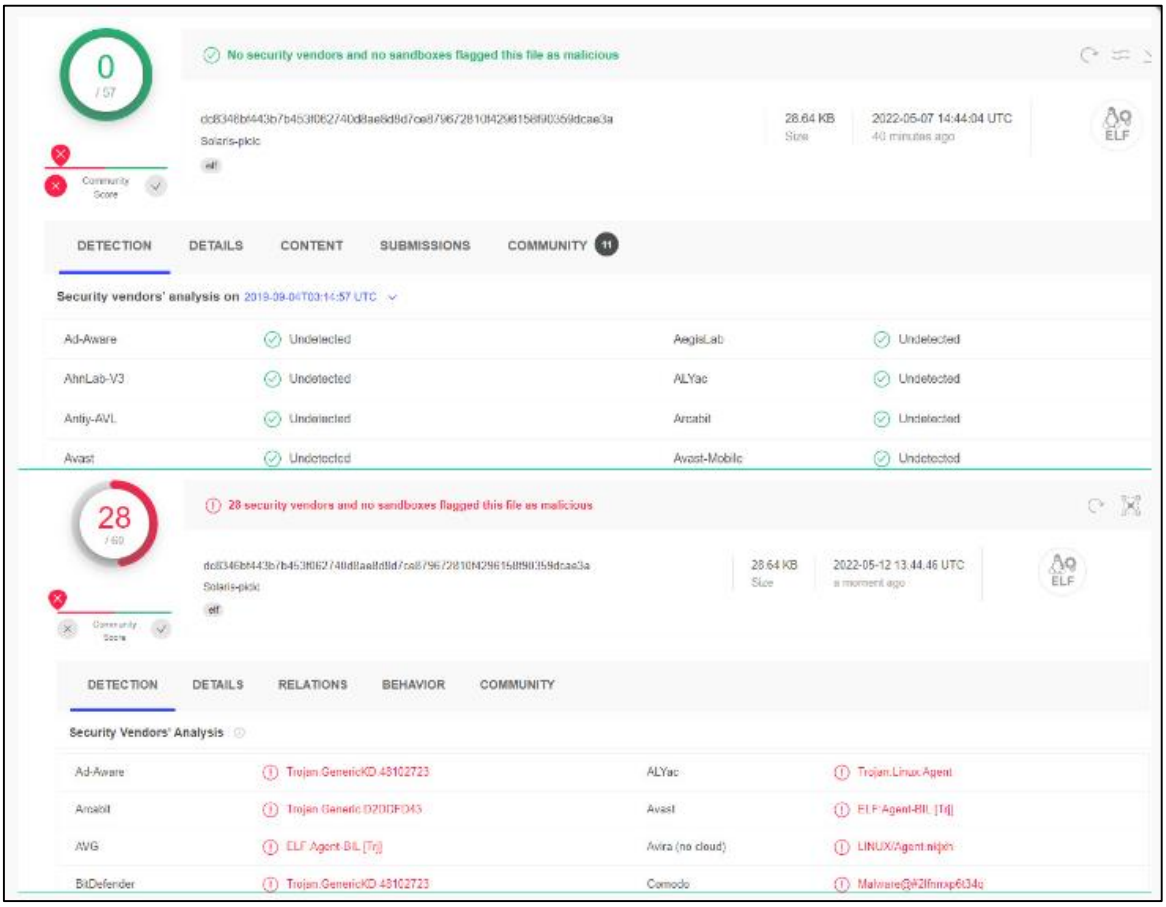
بخشی از تکنیک‌های BPFDoor برای فرار از تشخیص، تغییر نام باینری است تا با استفاده از گزینه‌های زیر به‌عنوان یک دیمون معمولی لینوکس ظاهر شود:

```
/sbin/udevd -d
/sbin/mingetty /dev/tty7
/usr/sbin/console-kit-daemon --no-daemon
hald-addon-acpi: listening on acpi kernel interface /proc/acpi/event
dbus-daemon --system
hald-runner
pickup -l -t fifo -u
avahi-daemon: chroot helper
/sbin/auditd -n
/usr/lib/systemd/systemd-journald
```

شکل ۲- دستورات و شناسایی

پورسلوت می‌گوید که عامل تهدید BPFDoor را به‌طور منظم به‌روزرسانی می‌کرد و هر نسخه را با نام‌های مختلف برای دستورات، فرآیندها یا فایل‌ها بهبود می‌داد. به عنوان مثال، انواع جدیدتر ایمپلنت از استفاده از کلمات کلیدی دستوری به هش MD5 تغییر مکان دادند، احتمالاً در تلاشی برای جلوگیری از تشخیص بی اهمیت بودند. حداقل ۲۱ نسخه از BPFDoor در حال حاضر بر روی پلت فرم اسکن ویروس توتال شناسایی شده است که اولین نسخه در آگوست ۲۰۱۸ ارائه شده است. در حالی که میزان تشخیص این ایمپلنت بهبود

یافت، به خصوص پس از انتشار یافته های Beaumont، Rowland و Pourcelot، بدافزار برای مدت طولانی عملاً نامرئی بود. یکی از انواع BPFDoor برای Solaris از سال ۲۰۱۹ حداقل تا ۷می امسال شناسایی نشد.



شکل ۳- گزارش Virus Total

در برخی موارد، ردیابی‌ها عمومی هستند و به اشتباه نوع سولاریس فوق را به عنوان بدافزار لینوکس علامت‌گذاری می‌کنند، اگرچه این یک باینری لینوکس نیست. تریستان پورسلوت می‌گوید در حالی که BPFDoor از تکنیک‌های جدید یا پیچیده استفاده نمی‌کند، اما همچنان توانسته برای مدت طولانی مخفی بماند. این را می‌توان با این واقعیت توضیح داد که فناوری نظارت بر بدافزار در محیط های لینوکس به اندازه ویندوز رایج نیست. کریگ رولند موافق است که این یک مشکل بزرگ است. حتی اگر نظارت وجود داشته باشد، مردم نمی دانند به دنبال چه چیزی بگردند یا از روش اشتباه برای یافتن بدافزار لینوکس استفاده کنند.

برخی از مدیران از هش های رمزنگاری برای اسکن سیستم برای بدافزار یا فایل های مخرب استفاده می کنند. این به خوبی کار نمی‌کند زیرا کوچکترین تغییر در فایل منجر به یک هش جدید می‌شود. به‌علاوه EDR (تشخیص و پاسخ نقطه پایانی) می‌خواهد عامل‌ها را از همه جا بارگیری کند و عامل‌ها لینوکس را خراب می‌کنند، بنابراین آن‌ها اغلب انتخاب خوبی نیستند.

۳ محصولات تحت تأثیر

وقتی BPFDoor در ابتدا اجرا می‌شود، یک فایل زمان اجرا را در "var/run/initd.lock/" قفل می‌کند، خود را به‌عنوان یک فرآیند فرزند[۲]فعال می‌کند، و سپس به خود دستور می‌دهد تا سیگنال‌های سیستم‌عامل مختلف را که باعث قطع شدن آن می‌شوند، نادیده بگیرد.

Signal Number	Signal Name	Signal Description
1	SIGHUP	SIGHUP ("signal hang-up") is a signal sent to a process when its controlling terminal session is closed.
2	SIGINT	SIGINT ("signal interrupt") is a signal sent when a user interrupts a program (Ctrl + C)
3	SIGQUIT	SIGQUIT is a signal sent to terminate a process.
13	SIGPIPE	SIGPIPE is a signal sent when a pipe breaks.
17	SIGCHLD	SIGCHLD is a signal sent when a child process exits.
21	SIGTTIN	SIGTTIN is a signal sent to a process attempting to read from the same terminal session and is blocked.
23	SIGTTOU	SIGTTOU is a signal sent to a process attempting to write to the same terminal session and is blocked.

شکل 4= سیکنال‌های سیستم عامل که بدافزار قرار است نادیده بگیرد

برای نظارت بر ترافیک ورودی برای یک دنباله بایت "جادویی" ("x44x30xCDx9Fx5Ex14x27x66")، بدافزار یک بافر حافظه را اختصاص داده و یک سوکت شنود بسته را راه‌اندازی می‌کند.

[۲] Child process

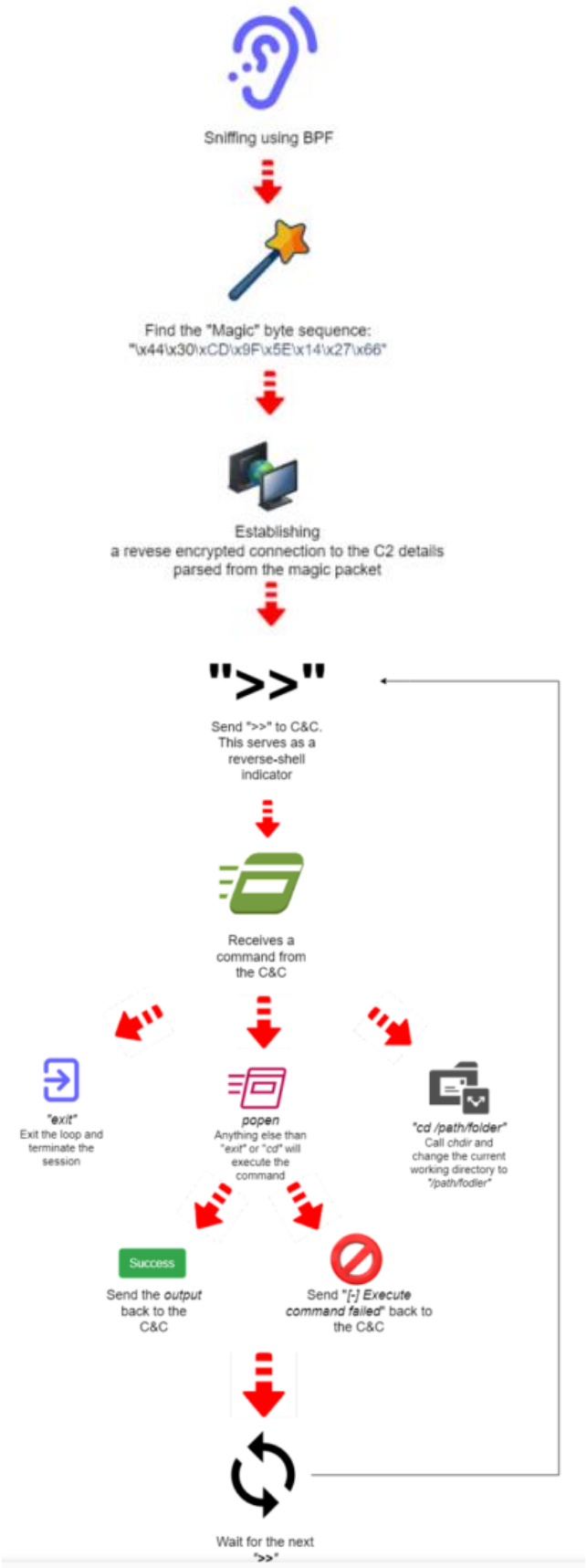
```
while ( 1 )
{
  while ( 1 )
  {
    while ( (DWORD)recvfrom(fd_sock, recved_buff, 0x10000, 0, 0, 0) < 0 )
      ;
    v8 = recved_buff[14];
    ++packet_counter;
    v9 = 4 * (v8 & 0xF);
    if ( v9 > 0x13 )
    {
      v10 = (DWORD)&recved_buff[v9 + 14];
      if ( 4 * ((unsigned byte)recved_buff[v9 + 26] >> 4) > 0x13 )
      {
        v11 = _byteswap_ulong(*(DWORD *)&recved_buff[v9 + 22]);
        if ( _byteswap_ulong(*(DWORD *)(v10 + 4)) == 0x4430CD9F && v11 == 0x5E142766 )
          break;
      }
    }
  }
}
```

شکل ۵- به دنبال دنباله بایت جادویی

برای خواندن فقط ترافیک UDP، TCP و SCTP از طریق پورت‌های 22(ssh)، 80(HTTP) و 443(HTTPS)، BPFDoor در این مرحله، یک فیلتر بسته Berkley را به سوکت متصل می‌نماید.

BPFDoor به قدری آهسته اجرا می‌شود که محدودیت‌های فایروال در رایانه در معرض خطر، بر این فعالیت شنود تأثیری نخواهند گذاشت.

بدافزار یک پوسته معکوس ایجاد می‌کند و پس از اتصال به C2 منتظر دستوری از سرور می‌ماند.



شکل ۶- نمودار عملیاتی

محققان این‌گونه نتیجه‌گیری نمودند که: BPFdoor با این نسخه اخیر، شهرت خود را به عنوان یک بدافزار بسیار مخفی و غیرقابل شناسایی حفظ می‌کند.

۴ منابع خبر

[1] https://cybersecuritynews.com/bpfdoor-targeting-linux-systems/

[2]https://www.bleepingcomputer.com/news/security/bpfdoor-stealthy-linux-malware-bypasses-firewalls-for-remote-access/