تحلیل جاسوس‌افزار لینوکسی GSpy

تاریخ گزارش: ۸ مرداد ۱۳۹۸

مقدمه

به تازگی آزمایشگاه امنیت کی‌پاد بدافزاری برای پلتفرم لینوکس در زیرساخت کشور جمهوری اسلامی ایران رصد و شناسایی کرده است که این بدافزار قابلیت‌های ویژه و منحصربفردی نسبت به نمونه‌های قبلی دارد. شایان ذکر است، در هنگام بررسی اولیه که توسط آزمایشگاه امنیت کی پاد صورت گرفت، این بدافزار توسط هیچ مکانیزم یا نرم‌افزار امنیتی قابل شناسایی نبود.

در حال حاضر نمونه بدافزارهای محدودی برای پلتفرم لینوکس شناسایی و گزارش شده‌اند، زیرا علاوه بر ساختار معماری پیچیده‌ای که کرنل سیستم‌عامل لینوکس دارد، قسمت اندکی از بازار سیستم‌های‌عامل شخصی را هم نسبت به دیگر سیستم‌های‌عامل به خود تخصیص داده است که این دو مورد موجب شده بود، مهاجمان توجه زیادی برای انجام عملیات‌های مخربانه متوجه این سیستم‌عامل نکنند. اکنون به نظر می‌رسد این راهبرد تغییر کرده است.

همچنین عموم بدافزارهایی که زیست‌بوم لینوکس را در گذشته هدف قرار داده بودند، متمرکز بر روی مباحثی با محوریت استخراج ارز رمزها[۱] برای مقاصد اقتصادی و باتنت‌ها برای انجام حملات منع سرویس توزیع شده[۲] بوده‌اند. در هر صورت، اخیرا آزمایشگاه امنیت کی‌پاد بدافزاری برای زیست‌بوم لینوکس رصد و شناسایی کرده است که برخلاف نمونه‌های قبلی، این بدافزار با محوریت جاسوسی از کاربران سیستم‌عامل لینوکس توسعه داده شده است و دارای ویژگی‌ها جدید و متنوعی است.

این بدافزار که توسط آزمایشگاه امنیت کی‌پاد «جاسوس‌افزار گنوم / Gnome Spyware» نامگذاری شده است، با محوریت تصویربرداری از دسکتاپ، سرقت فایل‌ها، ضبط صدا از میکروفون کاربر، سرقت کلیدهای فشرده شده، و اجرای پیلودهای مخرب بعدی خود این بدافزار در قالب یک افزونه برای گنوم توسط یک گروه روسی طراحی و پیاده‌سازی شده است.

شایان ذکر است، افزونه‌های گنوم[۳] به کاربران لینوکس این اجازه را می‌دهند که قابلیت‌ها و ویژگی‌های دسکتاپ لینوکس را توسعه و گسترش بدهند که توسعه‌دهندگان بدافزار جاسوس گنوم از این ویژگی برای توسعه و استقرار بدافزار خود سوء استفاده کرده‌اند. در ادامه به تحلیل عمیق و جزئیات این بدافزار لینوکسی پرداخته شده است

---

۱ Cryptocurrency mining attacks
۲ Distributed Denial of Service (DDoS)
۳ Gnome extension

مشخصات جاسوس‌افزار

در جدول زیر، مشخصات کلی بدافزار لینوکسی جاسوس‌افزار گنوم به صورت خلاصه آورده شده است. در ادامه، تحلیل این بدافزار که از خانواده جاسوس‌افزارها به شمار می‌رود، با جزئیات دقیق‌تری آورده شده است.

شناسه MD5	dcfc3cb0ca5ea83d835af6979a9b85c1
شناسه SHA-1	d11582903173e14c4ce41a3d2edfebdf5bf324c5
شناسه SHA-256	7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869
پلتفرم هدف	سیستم‌عامل لینوکس (Linux-based OS)
نوع بدافزار	جاسوس‌افزار «Spyware»
اسکریپت شناسایی	یارا: گیت‌هاب اسنورت: ندارد
توضیحات بدافزار	این بدافزار که توسط آزمایشگاه امنیت کی‌پاد «جاسوس‌افزار گنوم / Gnome Spy» نامگذاری شده است، با محوریت تصویربرداری از دسکتاپ، سرقت فایل‌ها، ضبط صدا از میکروفون کاربر، سرقت کلیدهای فشرده شده، و اجرای پیلودهای مخرب بعدی خود در قالب یک افزونه برای گنوم طراحی و پیاده‌سازی شده است.

فهرست

تحلیل بدافزار GSpy

همانطور که در ابتدا ذکر شد، جاسوس‌افزار پیچیده و پیشرفته GSpy به شکلی طراحی شده است که بتواند سیستم‌عامل لینوکس را هدف قرار بدهد. این اتفاق برای اولین بار برای پلتفرم و زیست‌بوم لینوکس در حال رخ دادن است، زیرا تا به الان برای این سیستم‌عامل جاسوس‌افزاری در این سطح توسعه داده نشده است.

یکی از دلایلی که مهاجمان و مجرمان سایبری به سیستم‌عامل لینوکس برای انجام حملات جاسوسی توجه اندکی کرده بودند، استفاده طیف اندکی از کاربران سیستم‌های شخصی از سیستم‌عامل لینوکس بود، اگر چه بالعکس سیستم‌های شخصی، سیستم‌عامل لینوکس بالاترین سطح استفاده را برای سرورها و تجهیزات نهفته را به خود اختصاص داده است.

از همین روی، عموماً سیستم‌عامل لینوکس به منظور اهداف اقتصادی با محوریت ماین ارزهای دیجیتالی یا استقرارسازی باتنت برای انجام حملات منع سرویس توزیع شده مورد هدف و حمله توسط مهاجمان و مجرمان سایبری قرار می‌گرفتند.

به همین دلیل، وجود و ظهور جاسوس‌افزاری برای این پلتفرم و زیست‌بوم نشان می‌دهد که استراتژی و راهبرد مهاجمان تغییر کرده است و به زودی سطح تهدیدات سایبری از نوع بدافزارها به صورت جدی به این زیست‌بوم هم خواهد رسید.

پیاده‌سازی و طراحی جاسوس‌افزار گنوم

بدافزار جدیدی که توسط آزمایشگاه امنیت کی‌پاد رصد و شناسایی شده است، نسبت به نوع بدافزارهای دیگری که پلتفرم لینوکس را هدف قرار داده بودند، دارای ویژگی‌ها بسیار جدیدتری است که با توجه به تحلیل‌های اولیه به نظر می‌رسد، توسط گروه روسی Gamaredon توسعه داده شده است.

What are GNOME Shell extensions?

GNOME Shell extensions allow customizing the default GNOME Shell interface and its parts, such as window management and application launching.

Each GNOME Shell extension is identified by a unique identifier, the uuid. The uuid is also used for the name of the directory where an extension is installed. You can either install the extension per-user in `~/.local/share/gnome-shell/extensions/<uuid>`, or machine-wide in `/usr/share/gnome-shell/extensions/<uuid>`.

To view installed extensions, you can use *Looking Glass*, GNOME Shell's integrated debugger and inspector tool.

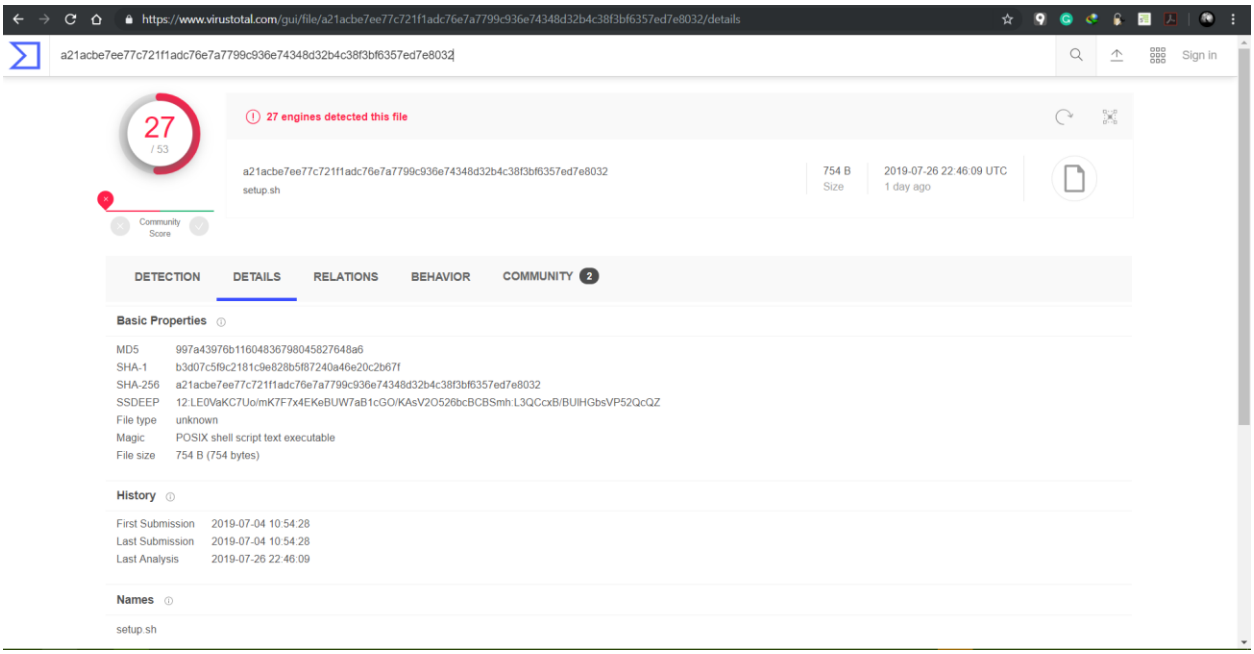
View installed extensions

1. Press Alt + F2, type in *lg* and press Enter to open *Looking Glass*.
2. On the top bar of *Looking Glass*, click Extensions to open the list of installed extensions.

تصویر ۱: توضیحات درباره افزونه پوسته گنوم[۱]

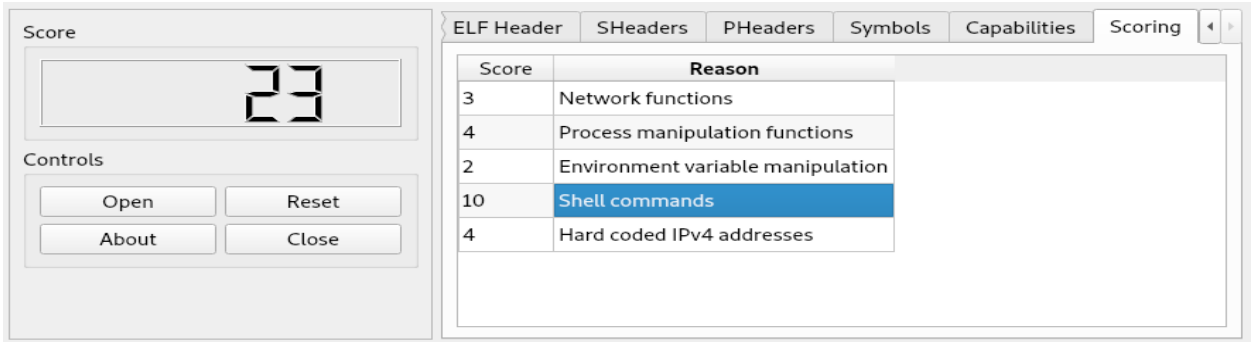
[۱] Gnome Shell Extension

شایان ذکر است، این جاسوس‌افزار لینوکسی توسط بخش کوچکی از مکانیزم‌ها و راه‌حل‌های نرم‌افزاری / سخت‌افزاری امنیتی قابل شناسایی و رصد است. اگرچه به نظر می‌رسد، بدافزار بارگزاری شده بر روی VirusTotal نسخه نهایی این جاسوس‌افزار نباشد، زیرا بدافزار دارای یک سری ویژگی از قبیل یک ماژول با محوریت کیلاگر است که کامل نشده‌اند، همچنین کامنت‌ها، سیمبول‌ها، متادیتاهای کامپایلر در این فایل وجود دارد که به صورت کلی در نسخه‌های نهایی بدافزارها نباید نمایش داده شود. از همین روی، به نظر می‌رسد توسعه‌دهندگان این بدافزار به اشتباه نسخه دیباگ را در پورتال VirusTotal بارگزاری کرده‌اند.

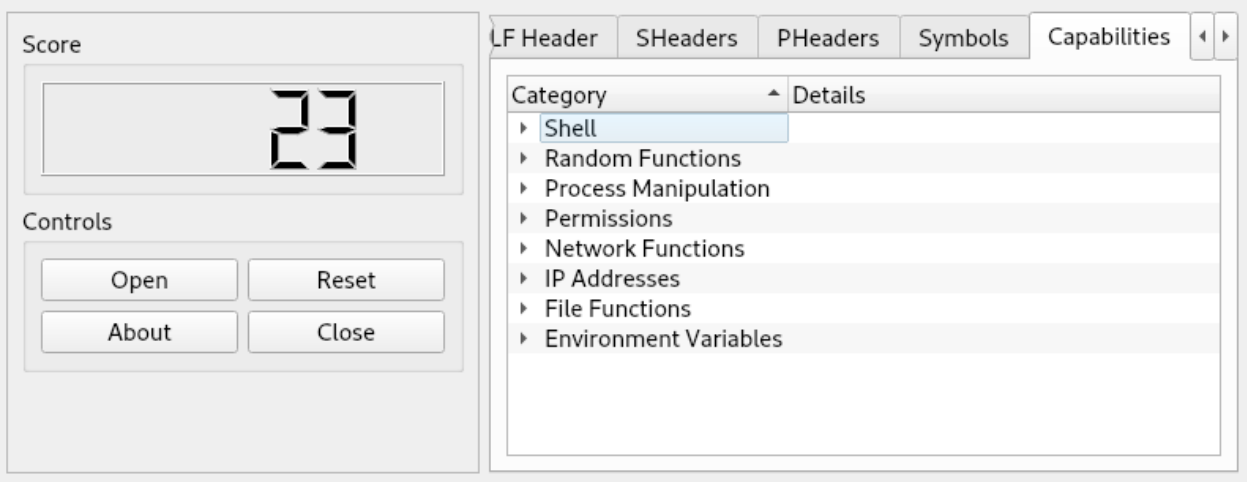


تصویر ۲: گزارش تحلیل بدافزار GSpy توسط VirusTotal

آزمایشگاه امنیت کی‌پاد این بدافزار را «جاسوس‌افزار گنوم / Gnome Spy» نامگذاری کرده است، زیرا این بدافزار از افزونه‌های گنوم برای آلوده کردن ماشین‌های لینوکسی استفاده می‌کند. افزونه‌های گنوم طراحی شده‌اند تا رابط پوسته گنوم و دیگر اجزای آن را سفارشی‌سازی کرد. قابلیت‌های این بدافزار شامل تصویربرداری از دسکتاپ، سرقت فایل، دریافت صداهای ضبط شده از میکروفون کاربر، و دانلود و اجرای پیلودهای بعدی این بدافزار است.



تصویر ۳: قابلیت‌های فایل اجرایی بدافزار



تصویر ٤: دسته‌بندی توابع توسط بدافزار مورد استفاده قرار گرفته است

در تصویر ۳ و ۴، قابلیت‌هایی که این بدافزار دارد، با تفکیک دسته‌بندی آن‌ها نمایش داده شده است که این قابلیت‌ها شامل ارتباطات تحت شبکه، دستکاری فایل سیستم، دستکاری پروسه‌های سیستمی، و مواردی از این دست می‌شود. بدافزار GSpy، اولین جاسوس‌افزاری است که علاوه بر قابلیت‌های ذکر شده در قسمت بالا، توانایی رفتار مانند یک درپشتی را هم بر روی سیستم دارد.

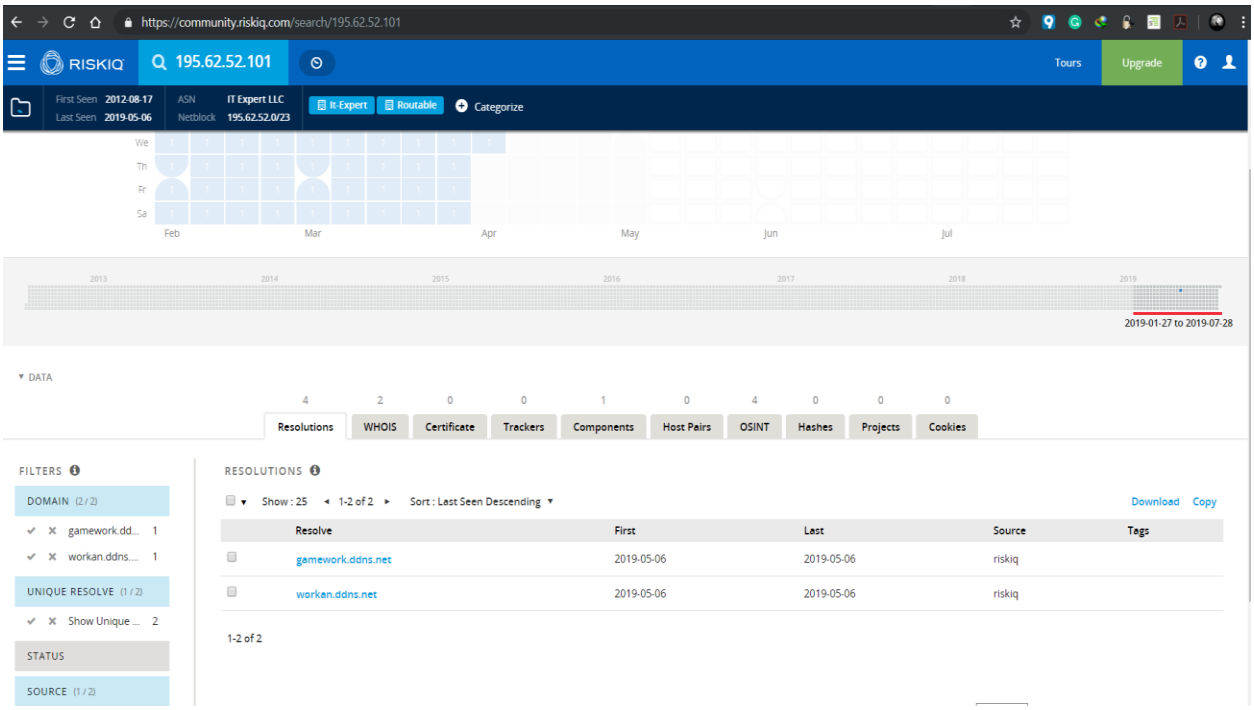
ارتباط بدافزار با گروه Gamaredon

با توجه به تحلیل ابتدایی که توسط آزمایشگاه امنیت کی‌پاد بر روی این بدافزار صورت گرفت، به نظر می‌رسد این بدافزار توسط گروه روسی Gamaredon توسعه داده شده است. این گروه تقریبا از سال ۲۰۱۲ فعالیت خود را شروع کرده است و به صورت عمده زیرساخت و افراد در کشور اوکراین را هدف قرار می‌دهد.

بردار حمله‌ای که این گروه برای هدف قرار دادن قربانیان خود مورد استفاده قرار می‌دهد، شامل حملات فیشینگ (پیوست‌های مخرب درون ایمیل) است و عموما از زیرساخت ارتباطی روسی برای توزیع بدافزارهای خودشان استفاده می‌کنند.

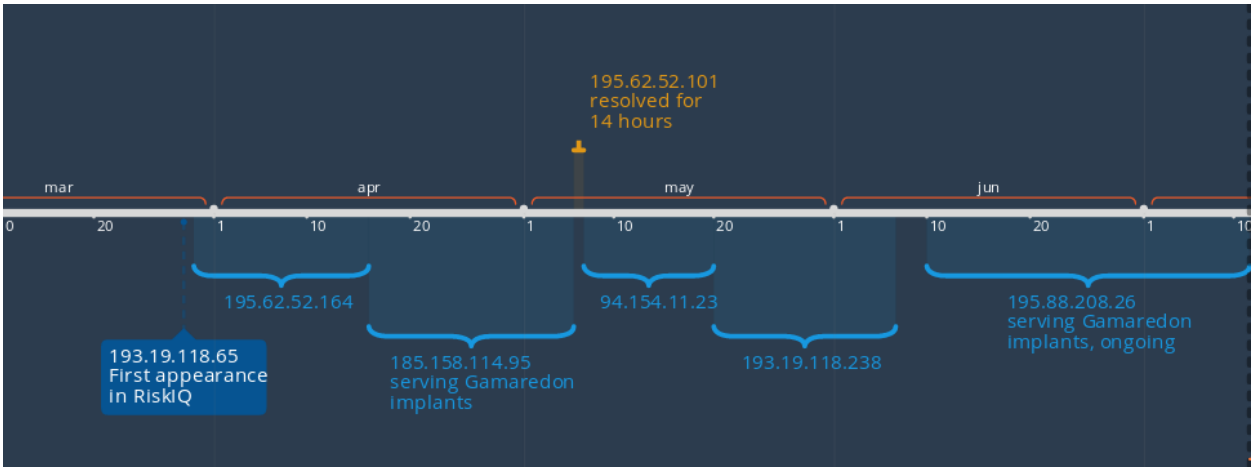
به نظر می‌رسد، با توجه به زیرساخت ارتباطی و قابلیت‌هایی که این بدافزار دارد، از قبیل تصویربرداری از دسکتاپ و سرقت صوت‌های ضبط شده و مواردی دیگر، بدافزار GSpy همچنین توسط این گروه توسعه داده شده باشد، زیرا مابقی بدافزارهای توسعه داده شده توسط این گروه، دارای معماری مشابه با این بدافزار بوده‌اند.

به عنوان مثال، بدافزار GSpy از یک میزبانی استفاده می‌کند که توسط گروه Gamaredon برای سالیان متمادی استفاده شده بود. آدرس اینترنتی (۱۹۵٫۶۲٫۵۲٫۱۰۱) سرور کنترل و فرماندهی جاسوس‌افزار GSpy دو ماه گذشته با دامنه‌های gamework.ddns.net و workan.ddns.net مورد ارجاع قرار می‌گرفت که مرتبط با گروه Gamaredon است.



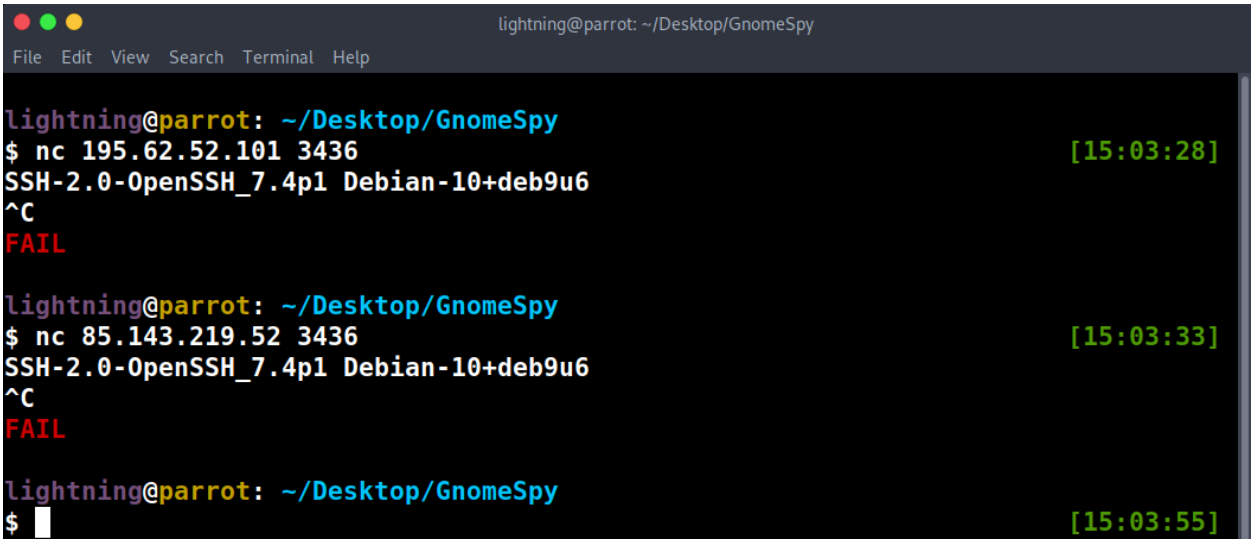
تصویر ۵: کوئری آدرس اینترنتی سرور کنترل و فرماندهی GSpy در پلتفرم RiskIQ

در تصویر ۶، از پلتفرم RiskIQ برای نگاشت و نمایش تاریخچه دامنه gamework.ddns.net استفاده کردیم که یافته‌های ما نشان می‌دهد جاسوس‌افزار GSpy بر روی یک آدرس IP عملیات انجام می‌داده است که توسط گروه Gamaredon دو ماه پیش در حال کنترل بوده است.



تصویر ٦: جدول زمانی DNS دامنه gamework.ddns.net

همچنین با بررسی‌هایی که بر روی زیرساخت کنترل و فرماندهی این بدافزار توسط تیم فنی شرکت کی‌پاد صورت گرفت، مشخص شد که زیرساخت کنترل و فرماندهی بدافزار GSpy در حال ارائه سرویس SSH روی پورت 3436 است. بعد از بررسی سرورهای کنترل و فرماندهی بدافزار GSpy، متوجه سرورهایی شدیم که سرویس SSH برای ارتباط با آن‌ها وجود دارند.



تصویر ۷: سرویس SSH ارائه شده بر روی پورت ۳۴۳۶

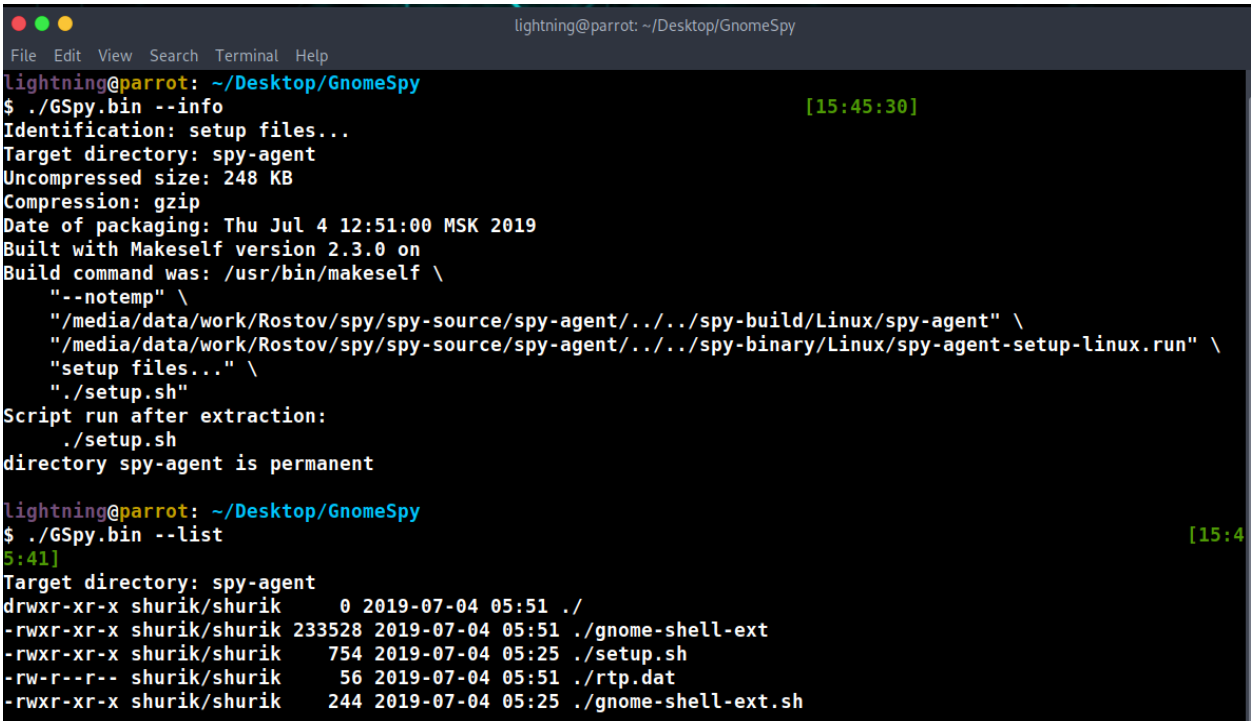
تحلیل فنی معماری و ساختار جاسوس‌افزار

این بدافزار در قالب اسکریپتی از نوع یک آرشیو خود استخراجگر[۱] در حال انتقال و توزیع است که توسط ابزار makeself ایجاد شده است. ابزار makeself.sh، یک اسکریپت کوچک است که می‌تواند یک فایل آرشیو فشرده استخراجگر از یک دیرکتوری ایجاد کند.

شایان ذکر است، فایل نهایی تولید شده توسط این ابزار با قالب .bin نمایش داده خواهد شد که می‌تواند به سادگی اجرا شود. در ادامه وقتی‌که فایل آرشیو از حالت فشرده در یک دیرکتوری موقت خارج شود، یک فرمان دلخواه برای راه‌اندازی نهایی فایل اجرا خواهد شد.

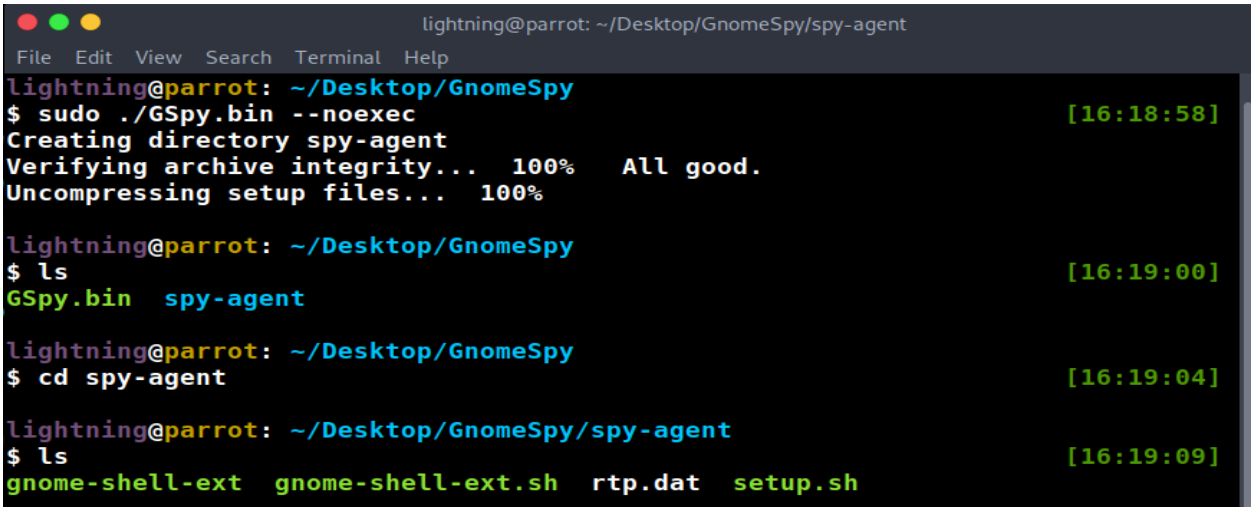
االبته نکته جالب هنگام تحلیل این بدافزار، عدم حذف متادیتا از فایل نهایی ایجاد شده توسط makeself است. اطلاعاتی از قبیل تاریخ ایجاد پکیج، مسیرهای توسعه، و نام‌ها کاملا موجود و قابل نمایش هستند. با توجه به تاریخی که در تصویر ۸ نمایش داده شده است، می‌توانید مشاهده کنید که این بدافزار اخیرا در تاریخ 4 July 2019 ایجاد شده است.

[۱] Self-extractable compressed archive



تصویر ۸: اطلاعات فایل GSpy.bin و محتویات درون پکیج آن

همانطور که در تصویر ۸ نمایش داده شده است، اسکریپت makeself به شکلی پیکربندی شده است تا بعد از خارج‌سازی پکیج از حالت فشرده فایل ./setup.sh را اجرا کند. البته با استفاده از دیگر آپشن‌های makeself می‌توانیم اسکریپت را به شکلی اجرا کنیم که فایل را از حالت فشرده استخراج کند، بدون اینکه فایل راه‌انداز آن یعنی setup.sh اجرا شود. در تصویر ۹ این مسئله نمایش داده شده است.



تصویر ۹: استخراج محتویات فایل BIN جاسوس‌افزار

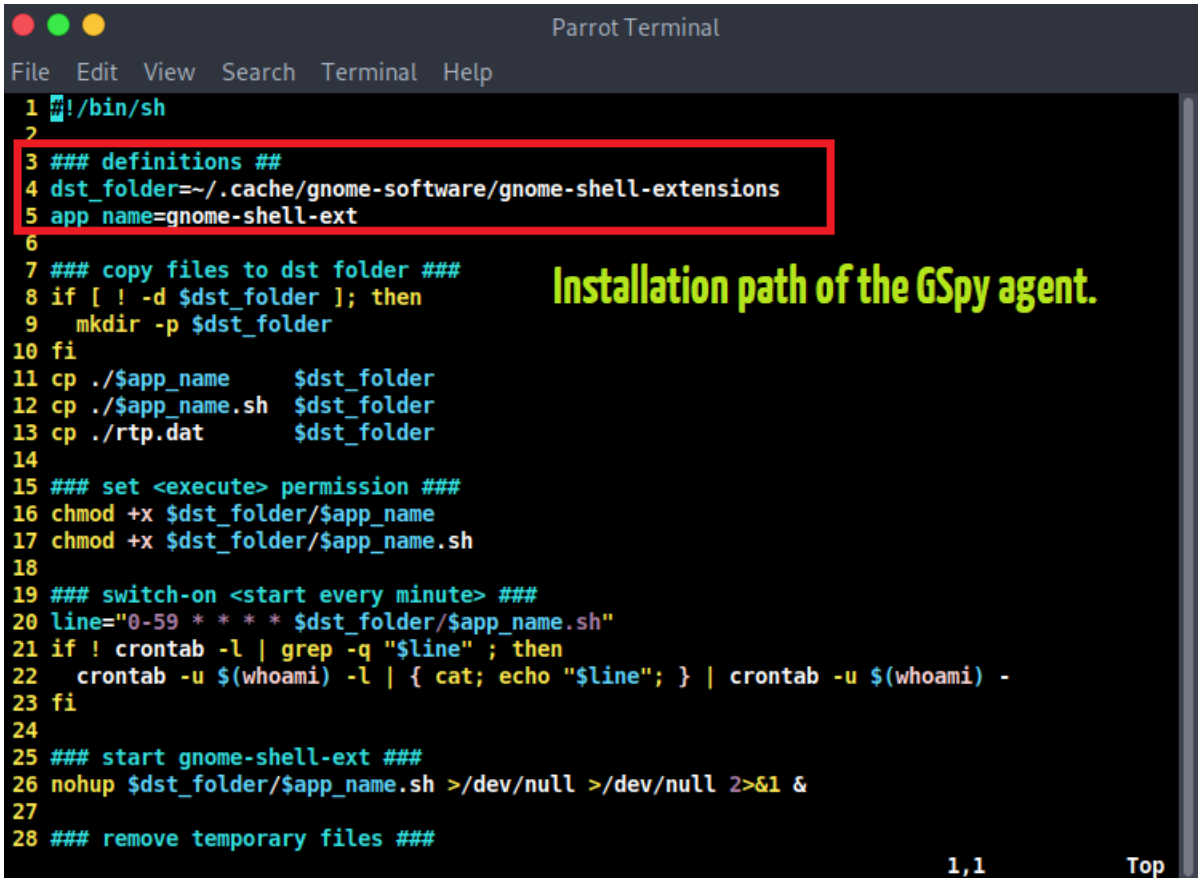
همانطور که مشاهده می‌کنید، بعد از استخراج محتویات از فایل bin.، چندین فایل در دیرکتوری spy-agent نمایش داده می‌شود که در زیر به ترتیب کلیات هدف این فایل‌ها تشریح شده است و در ادامه هم به جزئیات آن‌ها پرداخته خواهد شد:

۱. **gnome-shell-ext:** این فایل که در اصل یک فایل با قالب elf[۱] برای معماری پردازنده‌های ۶۴ بیتی می‌باشد، ایجنت اجرایی اصلی جاسوس‌افزار GSpy است.

۲. **gnome-shell-ext.sh:** این اسکریپت بررسی می‌کند که فایل بدافزار بر روی سیستم قربانی در حال اجرا است یا خیر. در نتیجه این بررسی اگر مشخص شود که بدافزار بر روی سیستم قربانی وجود ندارد، بعد از اجرای این اسکریپت فایل ایجنت بدافزار اجرا خواهد شد تا بر روی سیستم عملیات خود را از سر گیرد. این شل اسکریپت به شکلی مکانیزم ماندگاری[۲] عملکرد این بدافزار را تضمین می‌کند.

۳. **rtp.dat:** این فایل حاوی اطلاعات پیکربندی زیرساخت ارتباطی ایجنت جاسوس‌افزار gnome-shell-ext می‌شود. این فایل اطلاعاتی از قبیل آدرس سرور کنترل و فرماندهی، شماره پورت، شناسه ایجنت و دیگر اطلاعات مورد نیاز برای ایجنت را شامل می‌شود.

۴. **Setup.sh:** فایل نهایی در این دیرکتوری است که توسط خود makeself بعد از خارج‌سازی فایل بدافزار از حالت فشرده اجرا خواهد شد.

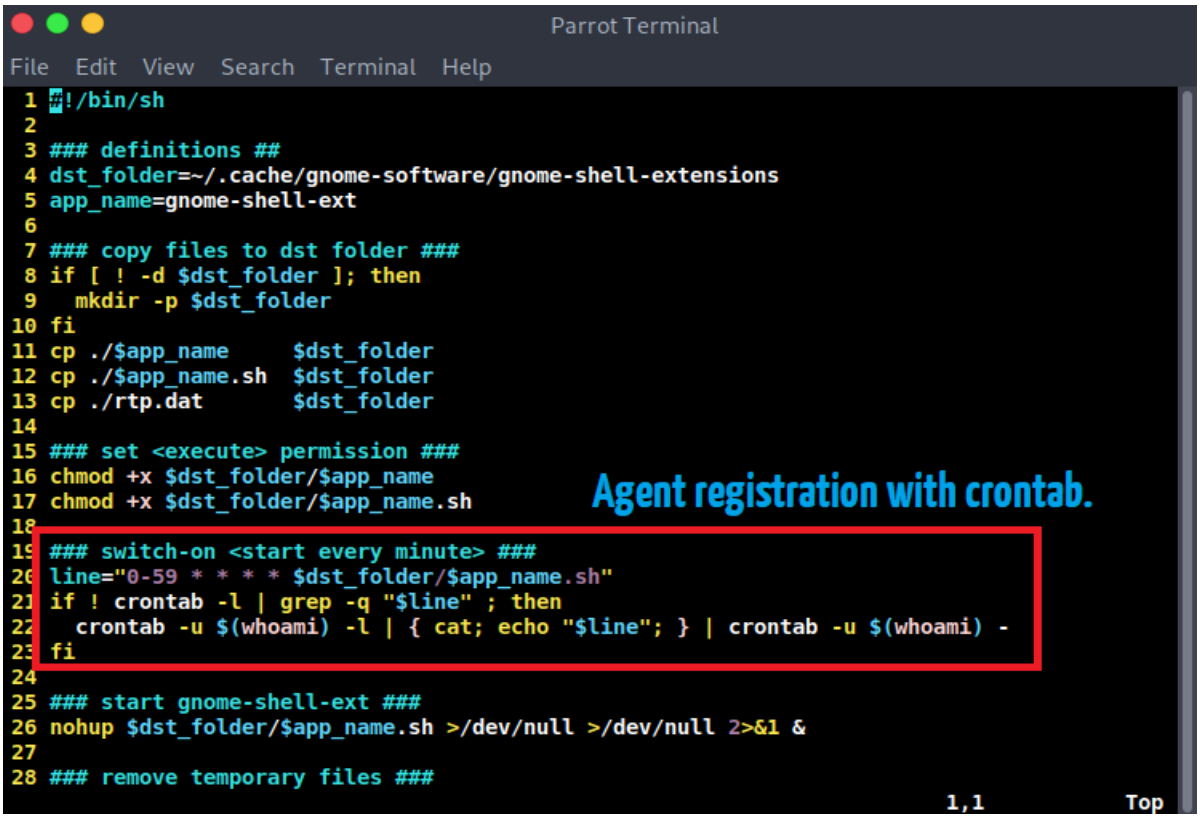


تصویر ۱۰: محل نصب ایجنت جاسوس‌افزار

[۱] Executable and Linkable Format

[۲] Persistence

همانطور که در تصویر ۱۰ نمایش داده شده است، بعد از اینکه فایل setup.sh توسط makeself اجرا شود، ایجنت جاسوس‌افزار در مسیر ~/.cache/gnome-software/gnome-shell-extensions/ نصب خواهد شد تا ایجنت بدافزار در قالب افزونه پوسته گنوم خود را پنهان کند زیرا افزونه‌های پوسته گنوم، اجازه می‌دهند کاربران سیستم‌عامل لینوکس دسکتاپ‌های مبتنی بر گنوم را دستکاری و به آن ویژگی‌های دلخواه اضافه کنند.



تصویر ۱۱: محل نصب ایجنت بدافزار

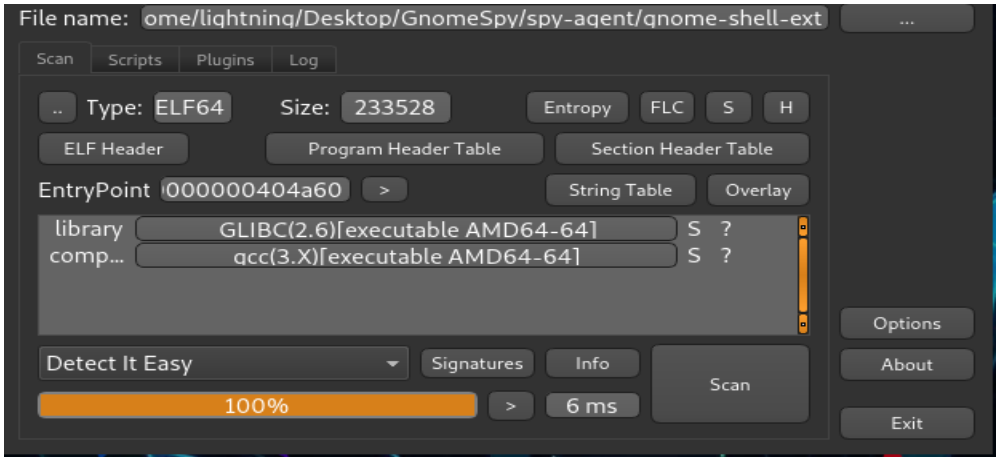
علاوه بر این، در تصویر ۱۱ مشاهده می‌کنید که جاسوس‌افزار برای اینکه ماندگاری در اجرا و تداوم عملیاتی به دست آورد، ایجنت gnome-shell-ext.sh را در قالب crontab رجیستر می‌کند تا هر دقیقه اجرا شود و در صورتی که بدافزار در حالت اجرا بر روی سیستم نبود، آن را مجدد بر روی سیستم بارگزاری و اجرا کند.

تحلیل استاتیک جاسوس‌افزار

با توجه به بررسی‌هایی که توسط آزمایشگاه امنیت کی پاد صورت گرفت، مشخص شد که ایجنت اصلی جاسوس‌افزار GSpy توسط زبان C++ برای معماری x64 پیاده‌سازی و نوشته شده است. همچنین ایجنت جاسوس‌افزار Gspy پک[۱] و

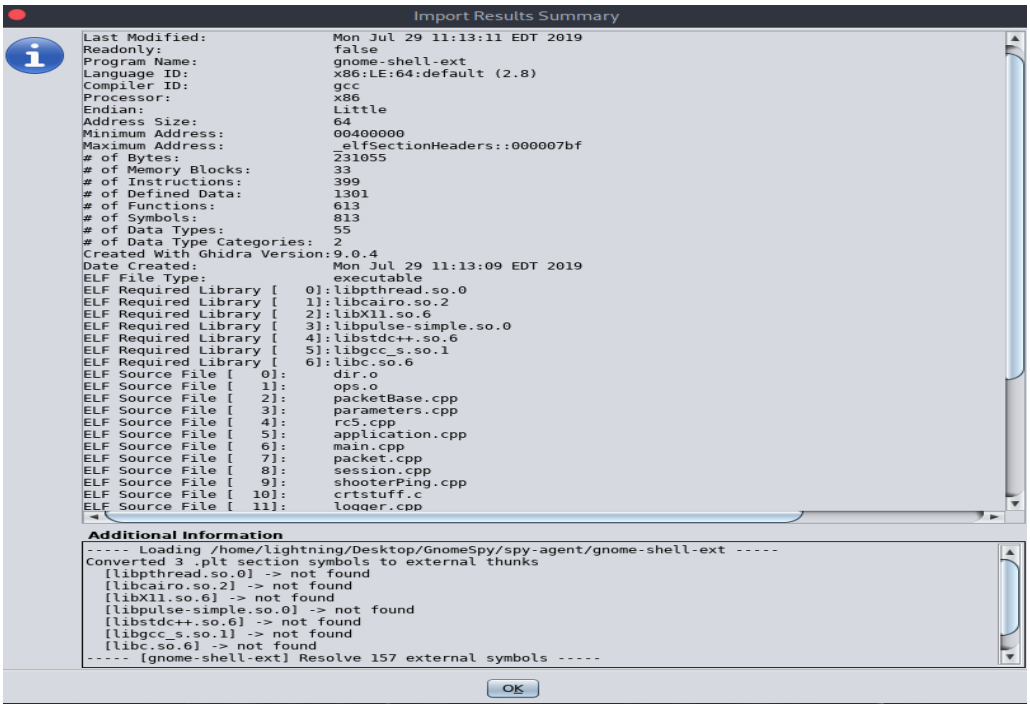
[۱] Packing

مبهم‌سازی[1] نشده است از همین روی تحلیل ساختار آن دشوار نخواهد بود. در تصویر ۱۲، جزئیات کامپایلر و پیاده‌سازی ایجنت جاسوس‌افزار نمایش داده شده است.



تصویر ۱۲: جزئیات پیاده‌سازی ایجنت جاسوس‌افزار

شایان ذکر است، بعد از دیزاسمبل فایل اصلی ایجنت جاسوس‌افزار، متوجه شدیم این بدافزار از طیف وسیعی از کلاس‌ها، ماژول‌ها و همچنین پارادایم برنامه‌نویسی شی‌گرایی بهره برده است. در تصویر ۱۳ اطلاعات کلی ایجنت جاسوس‌افزار GSpy به همراه ماژول‌های آن نمایش داده شده است.

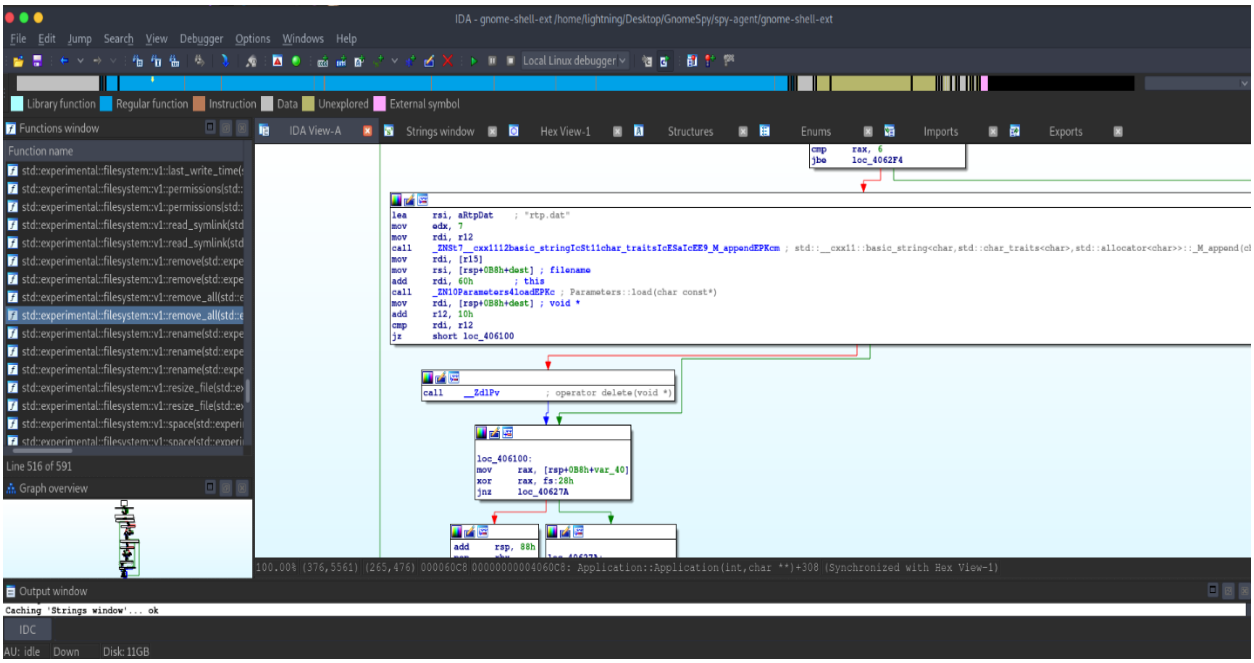


تصویر ۱۳: اطلاعات فایل اجرایی ایجنت جاسوس‌افزار

[1] Obfuscate

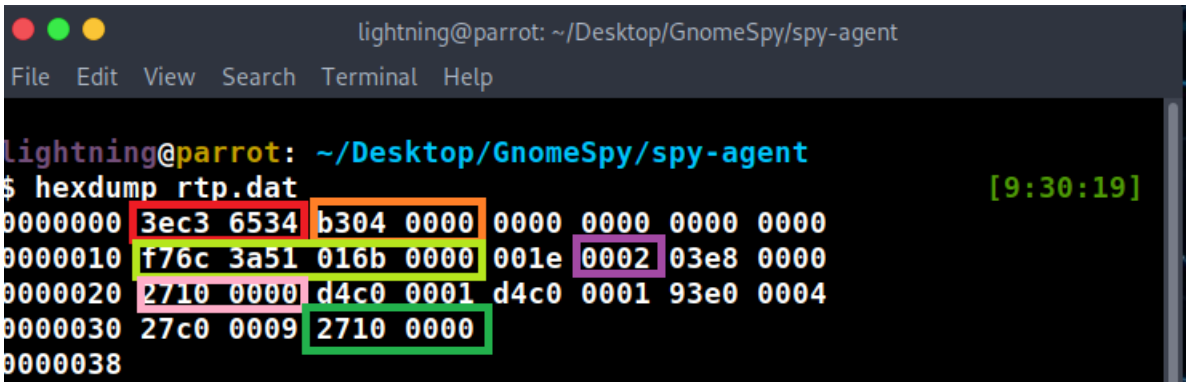
علاوه بر اینکه این بدافزار با C++ پیاده‌سازی شده است، توسعه‌دهندگان جزئیات پیاده‌سازی فایل نهایی بدافزار را حذف یا اصطلاحاً Strip نکرده‌اند، از همین روی در هنگام تحلیل دیزاسمبلی فایل اجرایی ایجنت بدافزار Gspy امکان این وجود داشت که با استفاده از سمبول‌های دیباگی که درون فایل اجرایی بدافزار وجود داشت، با سهولت بیشتری ساختار این بدافزار را تجزیه و تحلیل کرده و متوجه نیت پیاده‌سازی این فایل مخرب شویم.

به عنوان مثال، هنگامی که این بدافزار اجرا می‌شود، در مرحله اول یک پروسه جدید راه‌اندازی خواهد شد و در گام بعد محتویات فایل rtp.dat را خواهد خواند و آن را مستقیما در حافظه بارگزاری خواهد کرد. در تصویر ۱۴ بارگزاری این فایل نمایش داده شده است.



تصویر ۱۴: ساختار فایل دیزاسمبلی خواندن و بارگزاری فایل rtp.dat

همانطور که پیش از این ذکر شد، فایل rtp.dat شامل اطلاعات پیکربندی زیرساخت ارتباطی بدافزار از قبیل آدرس IP، شماره پورت، شناسه ایجنت، و ... خواهد شد. در تصویر ۱۵، ساختار این فایل در قابل هگزادسیمال نمایش داده شده است.



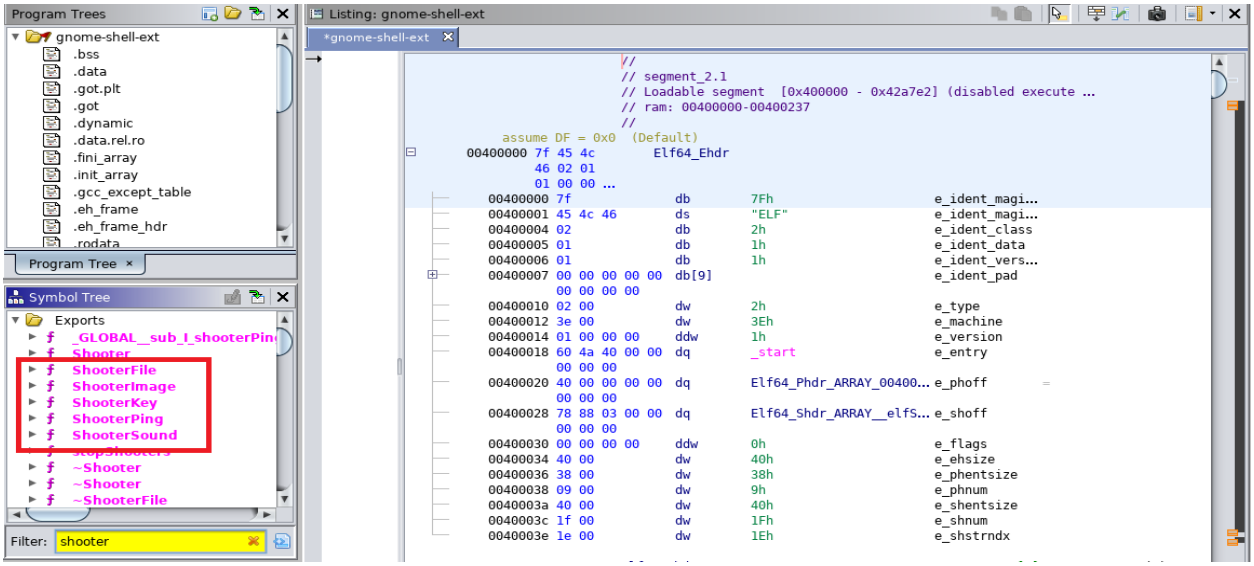
تصور ۱۵: ساختار هگزادسیمال فایل پیکربندی ایجنت جاسوس‌افزار

در جدول ۱، به تفکیک رنگ هر کادر در تصویر ۱۵، اطلاعات این فایل پیکربندی تجزیه و همچنین تشریح شده است. هر اطلاعات هر کدام از این فیلدها توسط ایجنت برای ارتباط با زیرساخت کنترل و فرماندهی بدافزار مورد استفاده قرار می گیرد.

شناسه	نمایش هگزادسیمال	نمایش دسیمال
آدرس سرور کنترل و فرماندهی	0xc3 0x3e 0x34 0x65	195.62.52.101
آدرس پورت	0x04 0xb3	1203
شناسه ایجنت	0xf7 0x6c 0x3a 0x51 0x01 0x6b 0x00 0x00	
اندازه پاکت‌ها	0x02 0x00	512
زمان تاخیر	0x10 0x27 0x00 0x00	4135
اندازه ضبط صدا	0x10 0x27 0x00 0x00	4135

جدول ۱: تفسیر اطلاعات درون فایل پیکربندی بدافزار

همانطور که در جدول ۱ نمایش داده شد، چند بایت ابتدایی فایل پیکربندی rtp.dat که در ابتدای اجرای ایجنت بدافزار خوانده می‌شود، آدرس سرور کنترل و فرماندهی این بدافزار است. علاوه بر این، ایجنت اصلی بدافزار GSpy شامل ۵ ماژول می شود که با عنوان کلی Shooter مورد ارجاع قرار می‌گیرند. در تصویر ۱۶ این ۵ ماژول در کادر قرمز نمایش داده شده‌اند:



تصویر ۱۶: ماژول‌های اصلی ایجنت بدافزار Gspy

هر کدام از این ماژول‌ها هدف مجزایی نسبت به یکدیگر دارند. در لیست زیر به صورت خلاصه هدف و رویکرد نهایی هر یک از ماژول‌های Shooter جاسوس‌افزار GSpy تشریح شده‌اند:

۱. **ماژول ShooterFile:** این ماژول با هدف پویش فایل سیستم ماشین هدف طراحی شده است، تا فایل‌هایی جدیدی که بر روی سیستم هدف ایجاد می‌شوند را دریافت و همچنین در ادامه بر روی زیرساخت کنترل و فرماندهی بدافزار بارگزاری کند. قابل ذکر است، این ماژول به صورت گزینشی یا Selective کار می‌کند، به این معنا که این ماژول دارای یک سری فیلتر است که در نتیجه بتواند فایل‌های مشخصی را پایش و سرقت کند.

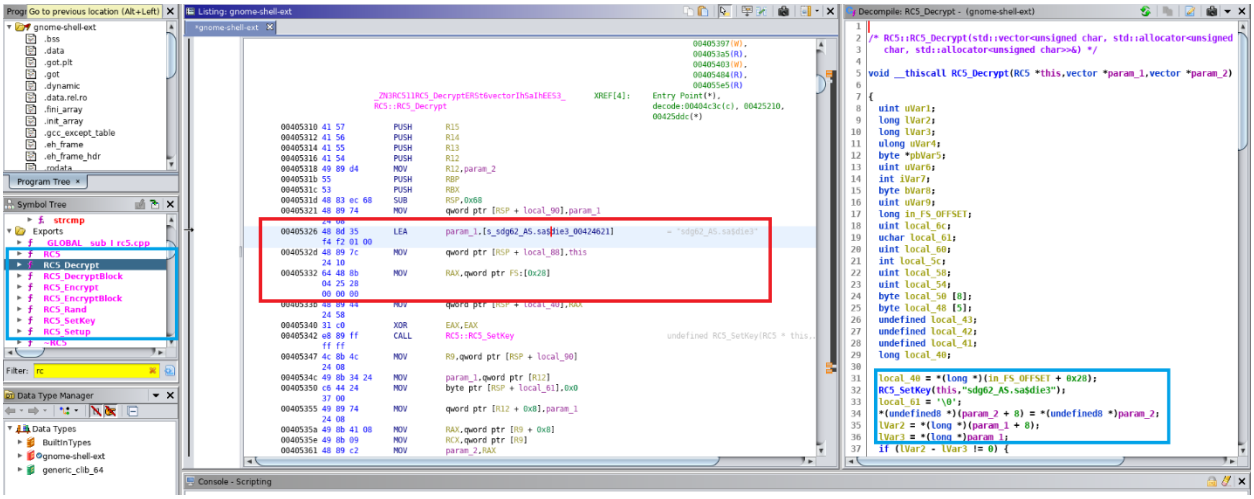
۲. **ماژول ShooterImage:** این ماژول با هدف دریافت تصاویر دسکتاپ و بارگزاری آن‌ها بر روی سرور کنترل و فرماندهی بدافزار طراحی و پیاده‌سازی شده است.

۳. **ماژول ShooterKey:** این ماژول با محوریت سرقت کلیدهای فشرده شده کیبورد توسعه داده شده است که در نسخه فعلی این بدافزار به صورت کامل پیاده‌سازی نگردیده است و همچنین توسط ایجنت مورد استفاده قرار نمی‌گیرد. به هر صورت، هدف این ماژول سرقت کلیدهای کیبورد قربانی را برعهده دارد تا در نهایت آن‌ها را به سرور کنترل و فرماندهی خود ارسال کند.

۴. **ماژول ShooterPing:** این ماژول با هدف ارتباط با سرور کنترل و فرماندهی بدافزار طراحی شده است. بدافزار با استفاده از این ماژول فرمان‌های ارسالی از سمت سرور زیرساختی (مهاجم) را دریافت می‌کند.

۵. **ماژول ShooterSound:** این ماژول با هدف دریافت صداهای ضبط شده از میکروفون قربانی پیاده‌سازی و طراحی شده است. در نهایت بعد دریافت و ضبط صدا از میکروفون کاربر آن را بر روی سرور کنترل و فرماندهی بارگزاری خواهد کرد.

همانطور که تا به الان ذکر شده است، این بدافزار دارای ساختار ماژولار است که هر ماژول به صورت مجزا از بقیه در تردهای جدا اجرا می‌شود و همچنین دسترسی به منابع مشترک از قبیل فایل پیکربندی به واسطه موتکس‌ها محافظت شده است. قابل ذکر است، ماژول‌ها خروجی خود را رمزنگاری می‌کنند و در سمت سرور کنترل و فرماندهی هم رمزگشایی می‌کنند. الگوریتمی هم که برای رمزنگاری استفاده شده است، الگوریتم RC5 با کلید sdg62_AS.sa$die3 است که در تصویر ۱۷ نمایش داده شده است.



تصویر ۱۷: الگوریتم RC5 برای رمزنگاری اطلاعات

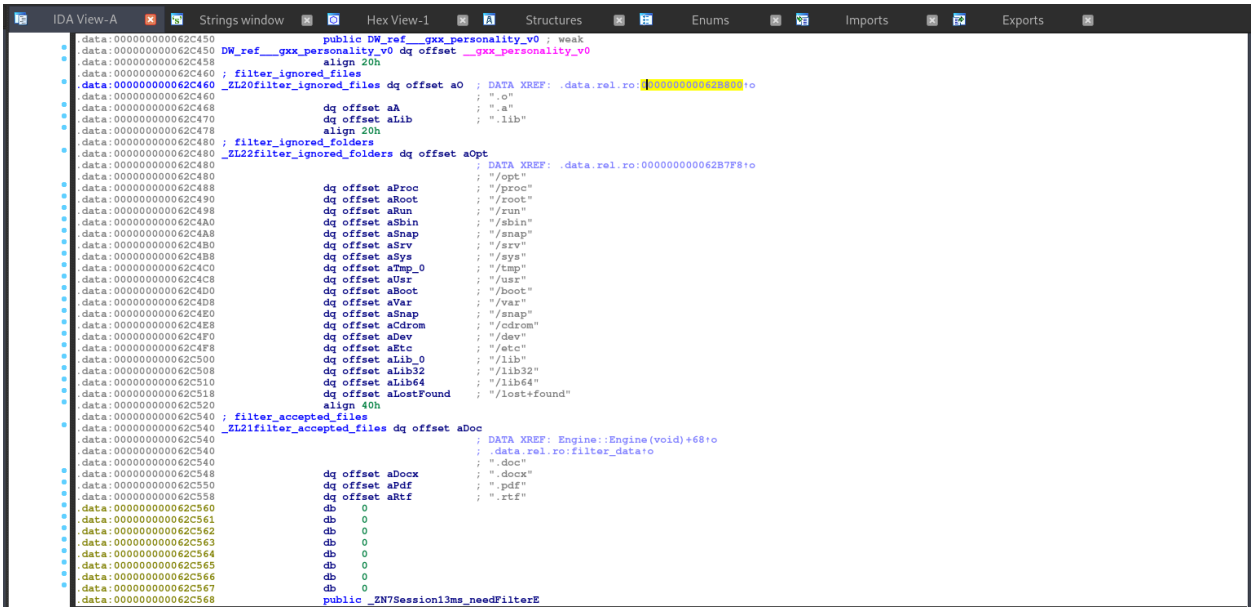
در ادامه هر ماژول از این بدافزار را به تفکیک مورد تحلیل قرار خواهیم داد که با ساختار پیاده‌سازی و جزئیات این بدافزار بیشتر آشنا شویم. در حالت کلی این بدافزار دارای ۵ ماژول است که هر ماژول با هدف مشخصی طراحی و پیاده‌سازی شده است. این ماژول‌ها در کنار هم دیگر هویت این بدافزار را تعریف می‌کنند.

ماژول ShooterPing

همانطور که پیش از این ذکر شد، ماژول ShooterPing وظیفه مدیریت ارتباط با سرور کنترل و فرماندهی بدافزار را بر عهده دارد. این ماژول وظایفی از قبیل دانلود و اجرای پیلودهای جدید جاسوس‌افزار، ایجاد فیلترهای جدید برای جستجو، دانلود ساختارهای پیکربندی جدید، انتقال اطلاعات ذخیره شده به سرور کنترل و فرماندهی بدافزار، و متوقف‌سازی ماژول‌های Shooter را بر عهده دارد. مابقی ماژول‌ها مبتنی بر زمان‌بندی که در فایل پیکربندی rtp.dat تعریف شده است، در یک بازه زمانی مشخص اجرا می‌شوند. شایان ذکر است، سرور کنترل و فرماندهی به واسطه ماژول ShooterPing توانایی کنترل این بازه زمانی در فایل پیکربندی rtp.dat را دارد.

ماژول ShooterFile

ماژول ShooterFile لیستی از فیلترها به منظور پویش فایل سیستم ماشین قربانی در قالب دو ساختار accepted_files، ignored_files و ignored_folders استفاده می‌کند و فایل‌ها / پوشه‌های مشخصی را نادیده می‌گیرد. در تصویر ۱۸ پوشه‌هایی که توسط این ماژول پویش نخواهند شد و همچنین فایل‌هایی که این بدافزار به صورت مشخص در جستجوی آن‌ها است، در قالب accepted_files و ignored_files و ignored_folders نمایش داده شده‌اند.

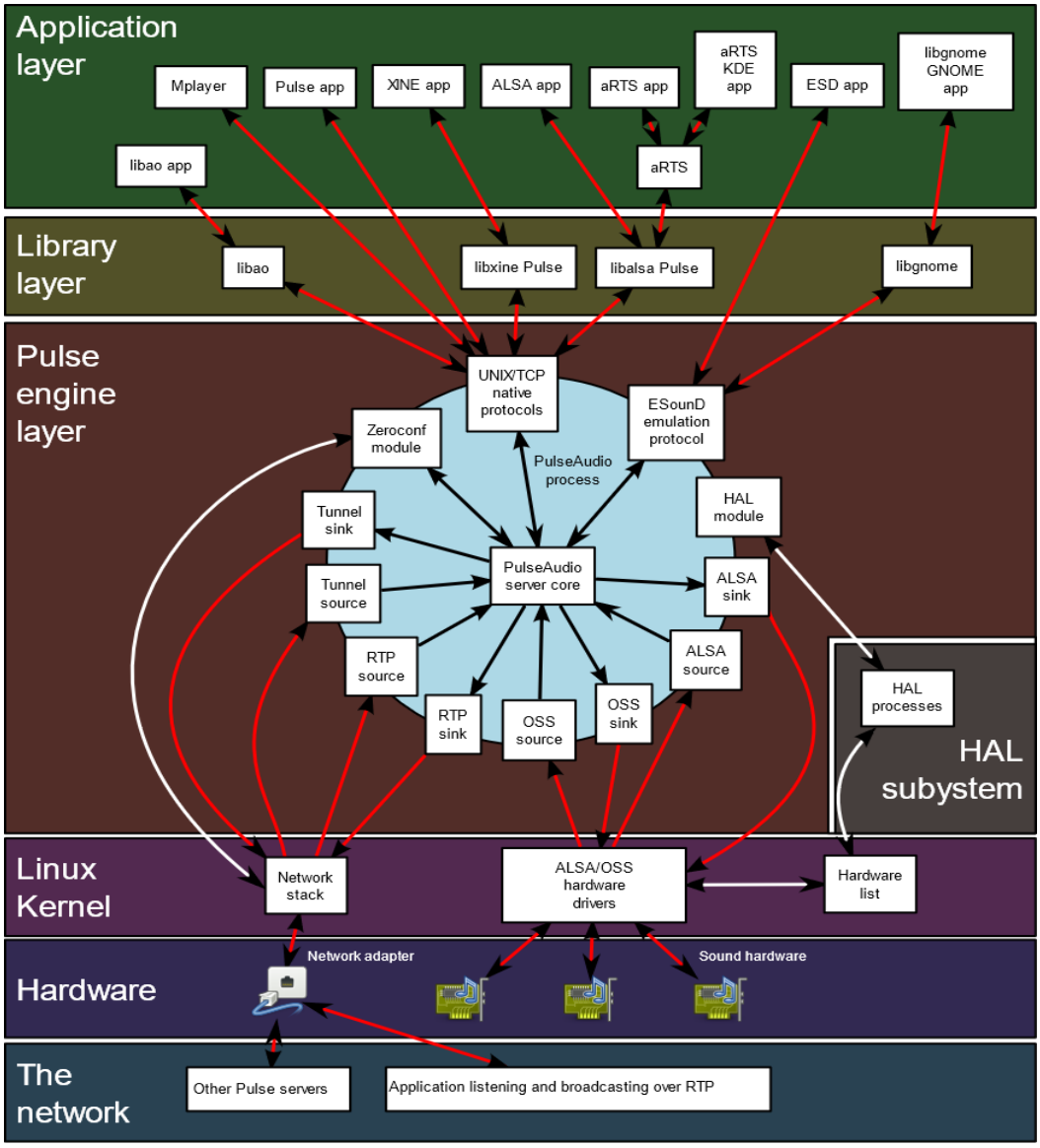


تصویر ۱۸: فیلتر پویش فایل ها

همچنین در تصویر ۱۸، قسمت filter_accepted_files مشخص شده است که این ماژول به صورت مشخص به دنبال فایل‌هایی با پسوند doc.، docx.، pdf. و rtf. است که برای جاسوس‌افزارها پایش این دست فایل‌ها طبیعی است.

ماژول ShooterAudio

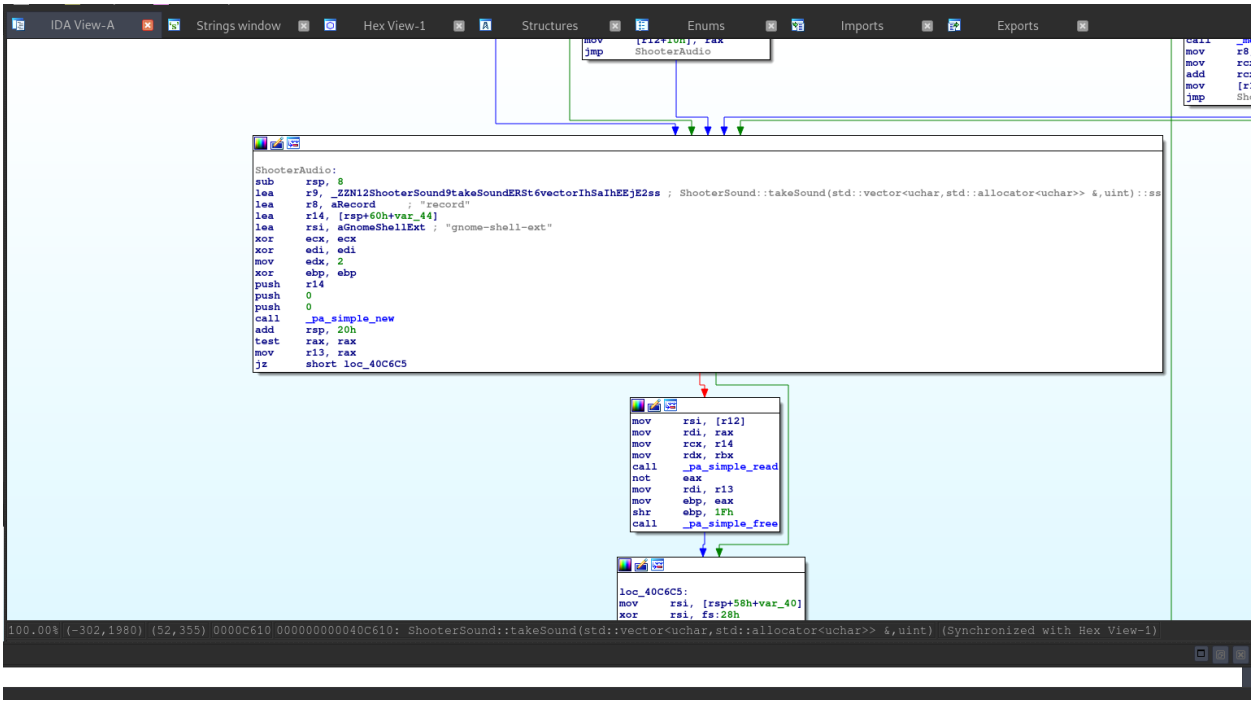
ماژول ShooterAudio برای دریافت صداهای ضبط شده توسط میکروفون بر روی پلتفرم لینوکس از PulseAudio استفاده می‌کند. نرم‌افزار PulseAudio در اصل مانند یک سرور برای صوت[1] عمل می‌کند، به شکلی که یک پروسه در پس‌زمینه می‌تواند ورودی صوتی را از یک یا چندین منبع دریافت کند و سپس آن را به دیگر منابع مانند کارت‌های صوتی، سرورهای PulseAudio و یا دیگر پروسه‌ها مسیردهی مجدد یا به عبارت دیگر ارسال کند.



تصویر ۱۹: فلوچارت اجرایی PulseAudio

[1] Sound Server

از آنجایی که این بدافزار از فایل پیکربندی rtp.dat برای راه‌اندازی و عملیات ایجنت خود استفاده می‌کند، مبتنی بر اطلاعاتی که در فایل پیکربندی تعریف شده است، ماژول ShooterAudio، در هر بار تلاش خود فایل‌های صوتی به اندازه ۸۰۰۰۰ بایت ضبط می‌کند. از همین روی، این ماژول صداها را فقط برای یک بازه زمانی اندکی ضبط می‌کند که این موجب خواهد شد عملا این ماژول فعال نباشد، مگر اینکه توسط سرور کنترل و فرماندهی اندازه ضبط صوت افزایش پیدا کند.



تصویر ۲۰: ماژول ShooterAudio

ماژول ShooterImage

این ماژول هدف تصویر برداری از دستکاپ را برعهده دارد. توسعه دهندگان این جاسوس افزار، برای تصویربرداری از دستکاپ از کتابخانه Cairo استفاده کرده اند که یک کتابخانه متن باز است. این ماژول ابتدا یک ارتباط با سرور Xorg Display ایجاد می کند که پشتیبان دسکتاپ Gnome است. در ادامه برای اینکه بتواند از دسکتاپ تصویر برداری کند، از کتابخانه Cairo و مجموعه توابع Surface آن برای ایجاد تصاویر PNG استفاده خواهد کرد. در تصویر ۲۱، نمونه ای رابط های ارائه شده توسط این کتابخانه نمایش داده شده است.

cairo_surface_write_to_png_stream ()

```
cairo_status_t
cairo_surface_write_to_png_stream (cairo_surface_t *surface,
                                   cairo_write_func_t write_func,
                                   void *closure);
```

Writes the image surface to the write function.

Parameters

surface	a cairo_surface_t with pixel contents
write_func	a cairo_write_func_t
closure	closure data for the write function

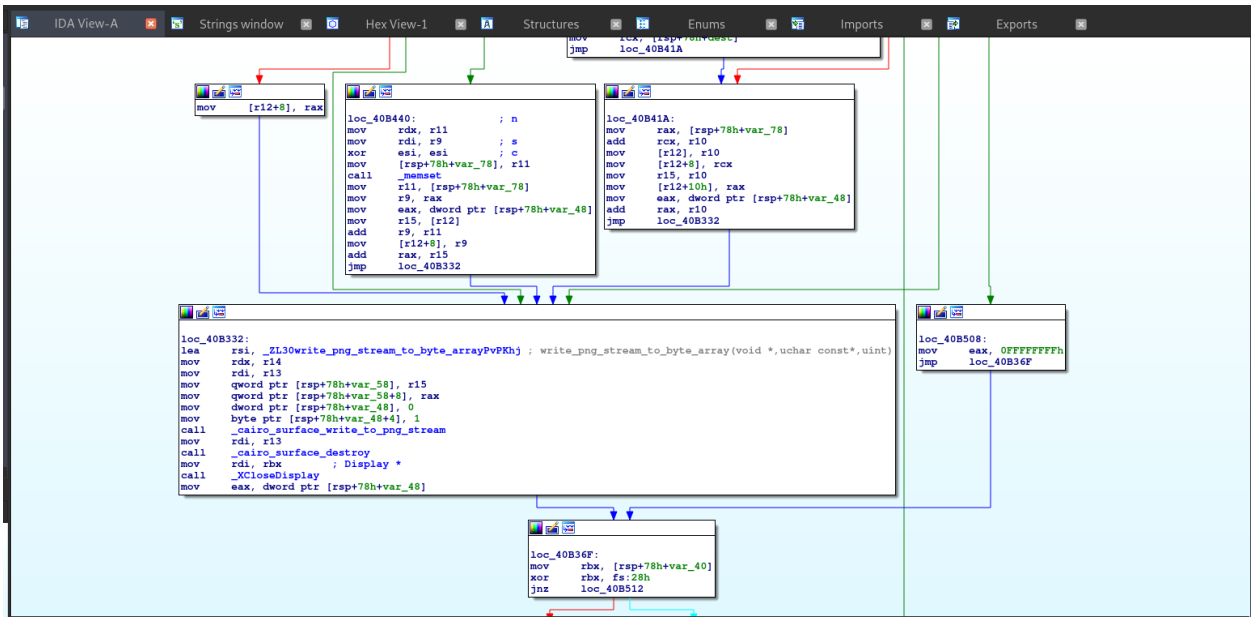
Returns

CAIRO_STATUS_SUCCESS if the PNG file was written successfully. Otherwise, CAIRO_STATUS_NO_MEMORY is returned if memory could not be allocated for the operation, CAIRO_STATUS_SURFACE_TYPE_MISMATCH if the surface does not have pixel contents, or CAIRO_STATUS_PNG_ERROR if libpng returned an error.

Since: 1.0

تصویر ۲۱: تابعی از کتابخانه Cairo

همچنین در تصویر ۲۲، ساختار دیزاسمبلی شده این ماژول را مشاهده می‌کنید که ببرخی از توابع متعلق به کتابخانه Cairo را برای کار با تصاویر گرافیکی فراخوانی کرده است و در نهایت هم تابع XCloseDisplay را فراخوانی می‌کند.



تصویر ۲۲: فرخوانی توابع Cairo

نتیجه‌گیری

جاسوس‌افزار گنوم از هر نظر برای مبحث امنیت زیرساخت‌های ارتباطی کشور جمهوری اسلامی ایران اهمیت راهبردی دارد، زیرا این بدافزار، اولین جاسوس‌افزاری است که با قابلیت‌های منحصربفردی از قبیل سرقت فایل، صوت، تصاویر و ... برای پلتفرم لینوکس توسعه داده شده است.

اگر چه به نظر می‌رسد، نسخه فعلی که از این بدافزار انتشار پیدا کرده است، نسخه آزمایشی باشد و در آینده نسخه‌های عملیاتی و خاص این بدافزار انتشار پیدا کنند. از همین روی، پیش از اینکه سامانه‌های زیرساختی کشور مورد حمله این بدافزار قرار بگیرند، باید گام‌هایی به منظور حفظ یکپارچگی و عملکرد آن‌ها برداشته شود.

نشانه نفوذگر «IOC»

Name:	Hash
Samples:	a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032 82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7 7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869
URLs	clsass.ddns.net kotl.space
Ips	185.158.115.44 195.62.52.101 185.158.115.154

جدول ۳: نشان نفوذ «IOC»