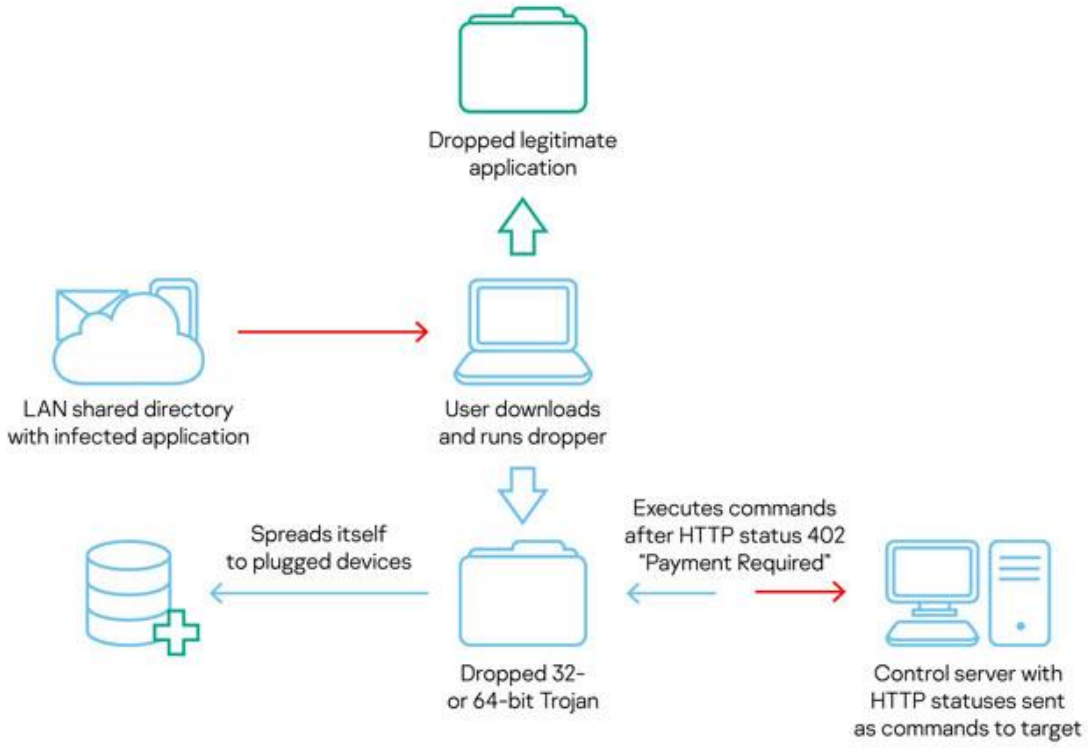
کدهای وضعیت HTTP فرمان می‌دهند که چگونه سیستم‌های هک شده، توسط یک بدافزار کنترل شوند.

نسخه‌ی جدیدی از تروجان دسترسی از راه دور (RAT) COMpfun در عمل کشف شده است که از کدهای وضعیت HTTP برای کنترل سیستم‌های قربانی که اخیراً در یک کمپین علیه نهادهای دیپلماتیک در اروپا مورد هدف واقع شده بودند، استفاده می‌کند.

تیم تحقیق، تجزیه و تحلیل جهانی در Kaspersky کشف کردند که بدافزار جاسوسی از طریق یک Dropper که خود را به عنوان یک اپلیکیشن ویزا جا می‌زند گسترش یافته است.

اولین بار در سال ۲۰۱۴ توسط G-Data ثبت شده است که، COMpfun سال گذشته پس از آنکه Kaspersky متوجه شد از این بدافزار برای جاسوسی از فعالیت مرورگر قربانی با اجرای حملات MitM در ترافیک رمزنگاری شده‌ی وب از طریق یک ترفند در مولد اعداد تصادفی مرورگر به نام PRNG گسترش قابل توجهی داشته است.



علاوه بر عملکرد به عنوان یک RAT کاملاً برجسته که قادر به ضبط کلیدهای فشرده شده‌ی صفحه کلید، تصاویر و استخراج داده‌های حساس است، این نوع جدید ازCOMpfun در قالب کد وضعیت HTTP، از هر دستگاه USB قابل جابجایی متصل به سیستم‌های آلوده، برای پخش بیشتر و دریافت دستورات از سرور تحت کنترل مهاجم استفاده می‌کند.

محققان می‌گویند: "ما یک پروتکل ارتباطی جالب C2 را با استفاده از کدهای نادر وضعیت HTTP /HTTPS مشاهده کردیم." " چندین کد وضعیت HTTP (422-429) از کلاس Client Error به Trojan اطلاع می‌دهد که اپراتورها قصد انجام چه کاری را دارند. پس از اینکه سرور کنترل وضعیت" Payment Required "(۴۰۲) را ارسال می‌کند، تمام این دستوراتی که از قبل دریافت شده‌اند، اجرا می شوند".

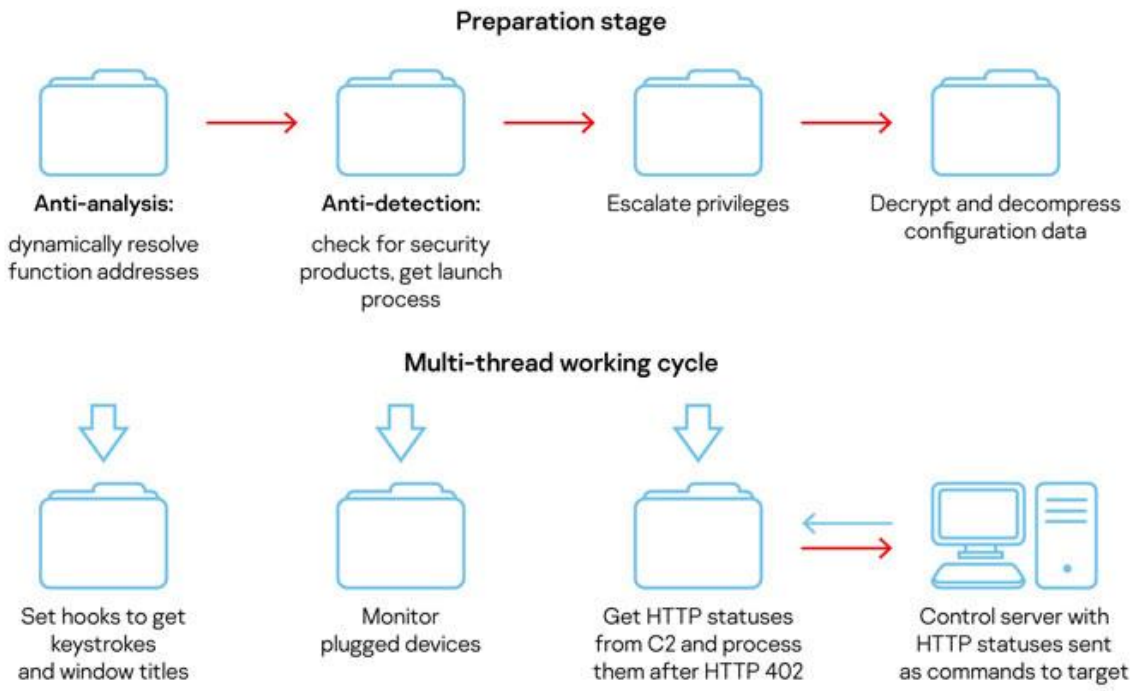
کدهای وضعیت HTTP پاسخ‌های استانداردی هستند که توسط یک سرور در پاسخ به درخواست مشتری از سرور، صادر شده اند. هدف از صدور دستورات از راه دور در قالب کدهای وضعیت، این است که در هنگام اسکن ترافیک اینترنت، هرگونه تشخیص فعالیت‌های مخرب را دور بزنید.

HTTP status	RFC status meaning	Corresponding command functionality
200	OK	Send collected target data to C2 with current tickcount
402	Payment Required	This status is the signal to process received (and stored in binary flag) HTTP statuses as commands
422	Unprocessable Entity (WebDAV)	Uninstall. Delete COM-hijacking persistence and corresponding files on disk
423	Locked (WebDAV)	Install. Create COM-hijacking persistence and drop corresponding files to disk
424	Failed Dependency (WebDAV)	Fingerprint target. Send host, network and geolocation data
427	Undefined HTTP status	Get new command into IEA94E3.tmp file in %TEMP%, decrypt and execute appended command
428	Precondition Required	Propagate self to USB devices on target
429	Too Many Requests	Enumerate network resources on target

C2 HTTP status code descriptions, including installation, USB propagation, fingerprinting, etc.

"نویسندگان کلید عمومی RSA و منحصر به فرد HTTP ETag را در داده‌های پیکربندی رمزنگاری شده نگه می‌دارند. این نشانگر ممکن است به دلایلی مانند ذخیره‌سازی محتوای وب همچنین برای فیلتر کردن درخواست‌های ناخواسته به C2 مانند مواردی که به جای اهداف از سمت اسکنر شبکه هستند، استفاده شود."

"برای استخراج داده‌های هدف به C2 از طریق HTTP / HTTPS ، این بدافزار از رمزنگاری RSA استفاده می‌کند و تروجان نیز برای مخفی‌کردن داده‌ها به صورت محلی، فشرده‌سازی LZNT1 و رمزنگاری یک بایت XOR را اجرا می‌کند".



با اینکه عملکرد دقیق نحوه‌ی تحویل اپلیکیشن ویزای مخرب به یک هدف مشخص نیست، Dropper در هنگام بارگیری، مرحله‌ی بعدی بدافزار را اجرا می‌کند که با استفاده از یک ماژول مبتنی بر وضعیت HTTP ، با سرور فرمان و کنترل (C2) ارتباط برقرار می‌کند.

محققان Kaspersky گفتند: "اپراتورهای بدافزار تمرکز خود را بر روی نهادهای دیپلماتیک و انتخاب یک برنامه مربوط به ویزا - که در یک فهرستی در شبکه محلی ذخیره می‌شود – به عنوان یک بردار اولیه‌ی آلودگی که به نفع آن‌ها کار می‌کرد، حفظ کردند".

"ترکیبی از یک رویکرد مرتبط با اهداف آن‌ها و توانایی تولید و اجرای ایده‌هایشان، مطمئناً باعث می‌شود که توسعه‌دهندگان COMpfun به یک تیم تهاجمی قوی تبدیل شوند."

منبع:

https://thehackernews.com/2020/05/malware-http-codes.html