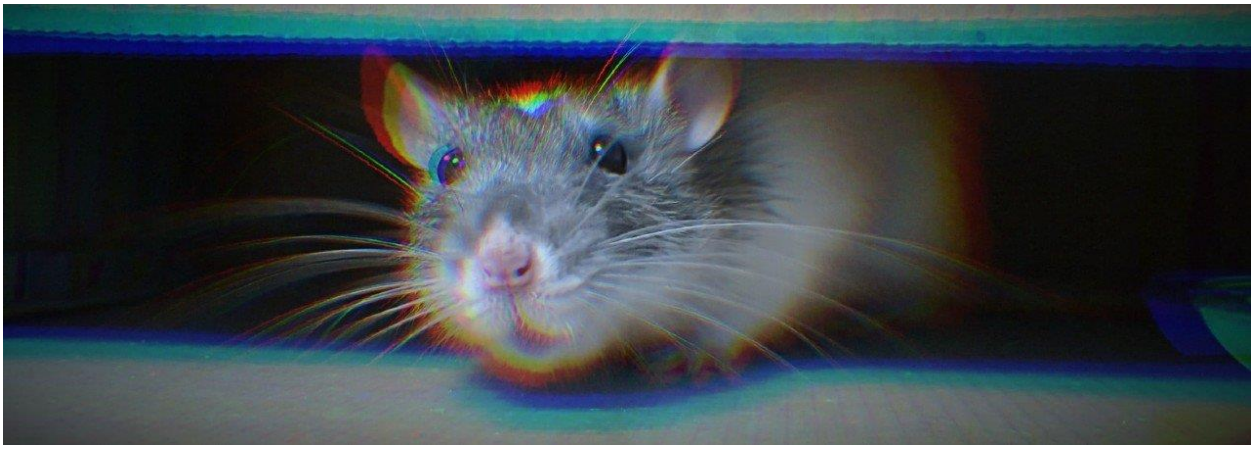
RATicate و انتشار بدافزارهای سرقت اطلاعات و RATهایی با اهداف سیستم‌های صنعتی



خلاصه‌ی خبر:

محققین امنیتی Sophos کشف کردند که حملات RATicat طی کمپین‌های انتشار متعدد شرکت‌های حقوقی مختلفی را مورد هدف قرار داده و در این راستا از دو زنجیر آلودگی که هردو مربوط به ایمیل‌های فیشینگ با اندکی تفاوت در نحوه‌ی استقرار آن‌ها، بهره جستند. Sophos با بررسی نمونه‌های جمع‌آوری شده دریافت که هر پنج کمپین انتشار فرآیند مشابهی را طی کرده و نتیجتاً عامل تهدید یکسان و مشترکی دارند، اما اینکه RATicat از شرکت‌های حقوقی و یا صنعتی جاسوسی می‌کند یا صرفاً به عنوان یک تأمین‌کننده‌ی اجاره‌ی بدافزار عمل می‌کند، معلوم نیست.

محققان امنیتی سوفوس (Sophos) گروه هکری را شناسایی کرده‌اند که از نصب‌کنندگان NSIS برای استقرار ابزارهای دسترسی از راه دور (RAT) و بدافزارهای سرقت اطلاعات، در حملات به شرکت‌های صنعتی سوءاستفاده کرده است.

سوفوس دریافت که از نوامبر ۲۰۱۹ تا ژانویه سال ۲۰۲۰، حملات RATicat شرکت‌های صنعتی در اروپا، خاورمیانه و جمهوری کره را به عنوان بخشی از پنج کمپین انتشار جداگانه هدف قرار داده‌اند، اگرچه محققان گمان می‌کنند که آن‌ها در دیگر کمپین‌های انتشار مشابه قبلی نیز دست داشته‌اند.

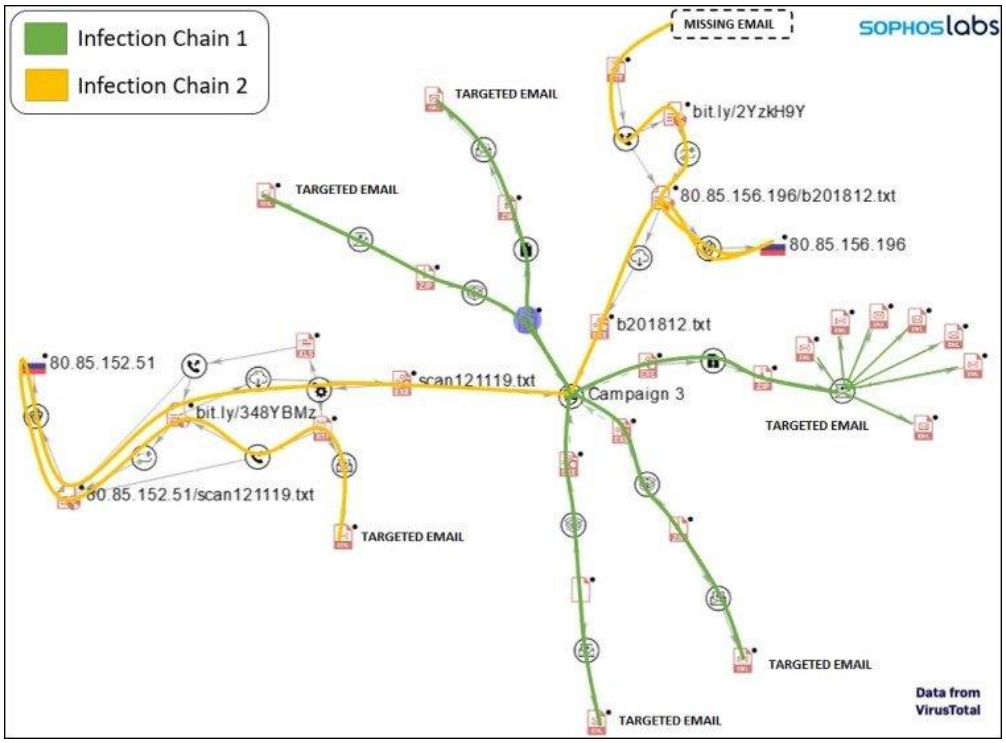
این کمپین‌های انواع مختلفی از نهادهای صنعتی، از شرکت‌های متمرکز بر تولید گرفته تا شرکت‌های سرمایه‌گذاری و شرکت‌های اینترنتی را مورد هدف قرار داده‌اند، از جمله:

- *تولیدکننده‌ی تجهیزات الکتریکی در رومانی؛*
- *یک شرکت مهندسی و خدمات ساخت و ساز در کویت؛*
- *یک شرکت اینترنتی کره‌ای؛*
- *یک شرکت سرمایه‌گذاری کره‌ای؛*
- *تولیدکننده‌ی تدارکات ساختمانی در بریتانیا؛*
- *انتشارات اخبار پزشکی در کره؛*
- *تولیدکننده‌ی کابل‌های برق و ارتباطات در کره.*
- *تولیدکننده‌ی تجهیزات چاپ و نشر سوئیسی؛*
- *یک شرکت پیک و حمل و نقل ژاپنی.*

زنجیره‌های آلودگی

برای آلوده‌کردن سیستم‌های هدف، مهاجمان از دو زنجیر آلودگی استفاده می‌کردند که هر دو مربوط به تحویل پی‌لود از طریق ایمیل‌های فیشینگ، با کمی تفاوت در نحوه‌ی استقرار آن‌ها بودند.

اولین زنجیر آلودگی از پیوست‌های مخرب UDF،ZIP و IMG استفاده می‌کند که حاوی نصب‌کننده‌های مخرب NSIS هستند، در حالی که دومی از اسناد XLS و RTF مشکوک برای دانلود نصب‌کننده‌ها از یک سرور از راه دور روی دستگاه‌های قربانیان استفاده می‌کند.



نصب‌کننده‌های NSIS (Nullsoft Scriptable Install System) از همان بارکننده‌ها استفاده کردند اما پیلودهای مخرب متفاوتی را رها کردند.

سوفوس می‌گوید: "ما دو سناریوی احتمالی را در نظر گرفتیم: یا بسته‌ی مخرب NSIS یک بسته‌بند عمومی است که در انجمن‌های زیرزمینی فروخته می‌شود؛ یا همان عامل تهدید است که از یک بارکننده سفارشی برای استقرار پی‌لودهای مختلف در انواع حملات خود، استفاده می‌کند".

نصب‌کننده‌های NSIS همچنین برای پنهان‌کردن بدافزار انتشار داده شده، مجموعه‌ای از فایل‌های ناخواسته - از تصاویر و فایل‌های کد منبع گرفته تا اسکریپت‌های پایتون – را بر روی سیستم هدف رها می‌کنند.

سوفوس گفت: "در طول تجزیه و تحلیل نمونه‌های جمع‌آوری شده چندین خانواده مختلف از RATها و infostealers را پیدا کردیم".

"این موارد شامل Lokibot، Betabot، Formbook و AgentTesla بودند. اما همه‌ی آن‌ها درحین اجرا همان روند چند مرحله‌ای را برای بازکردن بسته‌ها، دنبال می‌کردند".

یک عامل تهدید در چندین کمپین انتشار دست دارد

در کل، سوفوس دریافت که RATicat در پنج کمپین انتشار پی در پی دست دارد که مجموعه‌ای مشابه از پیلودها را آزاد می‌کند، فرمان و زیرساخت‌های کنترل را نیز به اشتراک می‌گذارد.

محققان دریافتند که " برخی از پیلودهای مختلف از هر کمپین (عمدتا Betabot، Lokibot، AgentTeslaو Formbook) یک C&C یکسان دارند" و اظهار داشتند که آن‌ها توسط یک عامل تهدید مشترک، هماهنگ شده‌اند.

"همچنین دسته‌بندی متمایزی از برنامه‌های زمانی کمپین وجود داشت که هیچ‌گونه همپوشانی بین آن‌ها وجود نداشت و این نشان می‌دهد که آن‌ها توسط همان عاملان تهدید به صورت سریالی اداره می‌شوند".

سوفوس همچنین کشف کرد: "بعضی از زیرساخت‌ها نیز در چندین کمپین مشترک بودند که نشان می‌دهد یک عامل مشترک در همه‌ی آن‌ها درگیر بوده است".

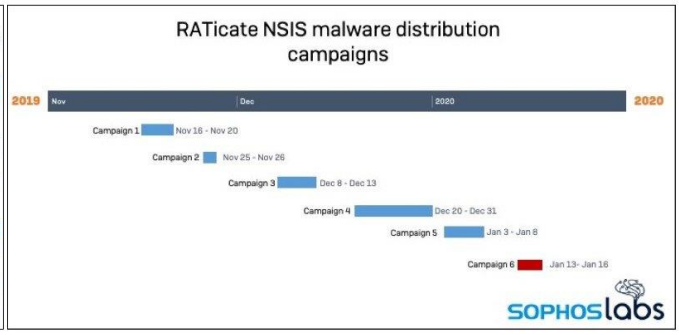
RATicate Campaign Relationships

Payloads Dropped

	Betabot	Lokibot	Formbook	Netwire	AgentTesla	Bladabindi	Remcos	Blackrat
Campaign 1	X	X	X	X				
Campaign 2	X		X			X	X	X
Campaign 3	X	X	X	X	X			
Campaign 4	X	X	X	X	X			
Campaign 5	X	X	X	X	X			

Shared C&C Infrastructure

	Campaign 1	Campaign 2	Campaign 3	Campaign 4	Campaign 5
Campaign 1	X	X	X		
Campaign 2	X	X	X	X	X
Campaign 3	X	X	X	X	X
Campaign 4		X	X	X	X
Campaign 5		X	X	X	X



جاسوسی شرکت‌های حقوقی یا ارائه دهنده‌ی MaaS

طبق گفته‌ی سوفوس، گروه RATicat به پیلودها و فریب‌های دیگری از جمله کاربران گمراه شده به‌وسیله COVID-19 روی آورده‌است و قربانیان بالقوه را به نصب بدافزار بر روی رایانه‌هایشان سوق دهد، که این موارد به عنوان یک سری از حملات کشف‌شده در مارس ۲۰۲۰ نشان داده شدند.

سوفوس گفت: "بر اساس رفتار آن‌ها، ما مطمئن نیستیم که گروه RATicat به جاسوسی شرکت‌ها می‌پردازد یا صرفاً به عنوان ارائه‌دهنده‌ی اجاره‌ی بدافزار به سایرین، عمل می‌کند".

"به سادگی می‌توان گفت که آن‌ها به منظور فراهم‌کردن دسترسی پولی به دیگران، بدافزارها را در شرکت‌های هدف رها می‌کنند، یا از بدافزارهای InfoStealer و RAT در راستای توزیع بدافزار، استفاده می‌کنند".

جزئیات بیشتر درباره‌ی کمپین‌های بدافزار RATicat و یک پیوند به لیستی از شاخص‌های خطر مربوط به کارزارهای آن‌ها در گزارش سوفوس موجود است.

منبع:

https://www.bleepingcomputer.com/news/security/raticate-drops-info-stealing-malware-and-rats-on-industrial-targets/