خبرنامه الکترونیکی ۶۵

مرکز تخصصی آپا دانشگاه سمنان

شماره شصت و پنجم، سال ششم، آبان ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

آموزش حمله به پروتکل ARP

با استفاده از ابزار Loki

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

مرکز آپا دانشگاه سمنان

"اگر فکر می‌کنید تکنولوژی به تنهایی می‌تواند مسائل امنیتی شما را حل کند، شما نه می‌دانید مسائل امنیتی چیست و نه می‌دانید تکنولوژی چیست!"

بروس اشنایر

رمزنگار آمریکایی و متخصص امنیت رایانه

فهرست

خبر

آموزش

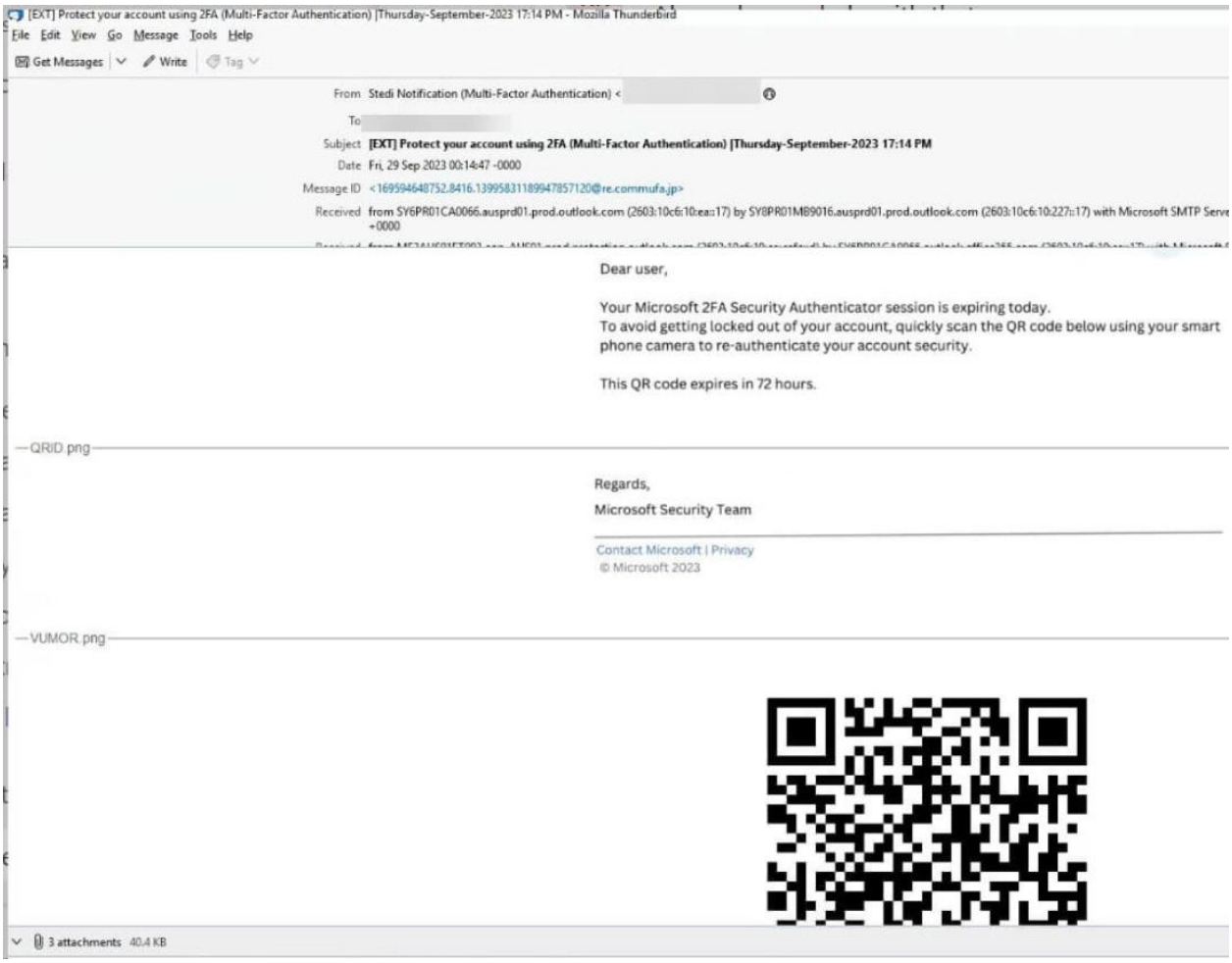
مرکز آپا دانشگاه سمنان

خبر

افزایش حملات فیشینگ
با بهره‌برداری از QRcode

کدهای QR، بارکدهایی دو بعدی هستند که می‌توانند داده‌های پیچیده از جمله URL، آدرس‌های ایمیل و شماره سریال را رمزگذاری کنند. آن‌ها به طور گسترده در حوزه‌های مختلف از جمله تبلیغات، بازاریابی و سیستم‌های پرداخت استفاده می‌شوند. کدهای QR در سال‌های اخیر به طور فزاینده‌ای محبوب شده‌اند و میلیون‌ها نفر برای پرداخت، اسکن منوها و دسترسی به اطلاعات از آن‌ها استفاده می‌کنند. این استفاده گسترده، آن‌ها را به هدفی جذاب برای مجرمان سایبری تبدیل کرده است. مهاجمان دو روش حمله برجسته را برای بهره برداری از کدهای QR ترجیح می‌دهند: Quishing و QRL-Jacking. از بین این دو نوع حمله، حملات Quishing به دلیل ماهیت گسترده خود در حال افزایش هستند.

در ماه‌های اخیر افزایش قابل توجهی در حملات فیشینگ کد QR مشاهده شده است. در این نوع از حملات از کدهای QR جهت فریب کاربران ناآگاه به منظور دسترسی به وب‌سایت‌های مخرب یا دانلود بدافزار استفاده می‌شود. به عنوان نمونه در یکی از این حملات، مهاجمان از طریق کد QR با استفاده از مهندسی اجتماعی، کاربران را به سایت‌های جمع‌آوری اعتبار هدایت می‌کند. ایمیلی که ادعا می‌شد از طرف مایکروسافت ارسال شده و حاوی یک کد QR بود برای کاربران ارسال شده بود. در این ایمیل ادعا می‌شد که احراز هویت چند عاملی مایکروسافت منقضی شده و کاربران باید مجددا احراز هویت کنند.



آمارها نشان می‌دهد که این نوع از حملات از ماه اوت تا سپتامبر سال 2023 میلادی افزایش 587 درصدی داشته است. همچنین در ماه اکتبر یک جهش ناگهانی در این نوع از حملات مشاهده شده است. شیوع حملات Quishing گواهی بر ماهیت در حال تکامل تهدیدات سایبری است.

توصیه‌های امنیتی

به منظور مقابله با حملات Quishing، هنگام مواجهه با کد QR در ایمیل‌ها، هوشیاری کاربران بسیار مهم است و اقدامات پیشگیرانه زیر توصیه می‌شود:

- قبل از اسکن QR کد، فرستنده اصلی ایمیل را بررسی کنید .
- از فناوری OCR (تشخیص کاراکتر نوری) برای ترجمه کدها به URL اصلی استفاده کنید.
- پیش نمایش URL کد QR را قبل از باز کردن آن بررسی کنید تا ببینید آیا درست به نظر می رسد یا خیر.
- اگر کد QR، شما را به وب‌سایتی هدایت می‌کند که اطلاعات شخصی یا اعتبارنامه‌های ورود را می‌خواهد بسیار محتاط باشید.

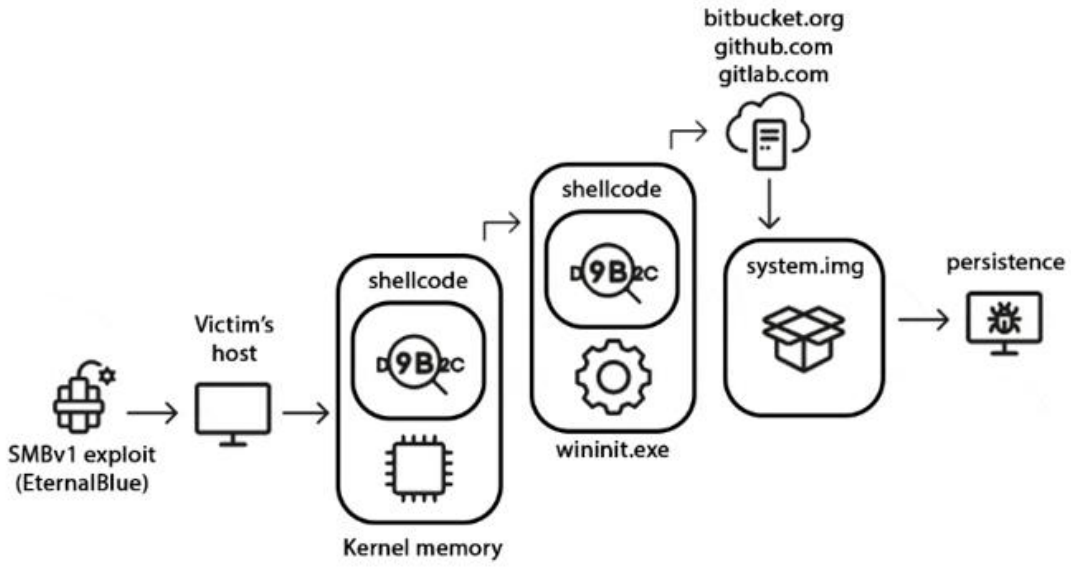
آلوده شدن بیش از یک میلیون سیستم ویندوزی و لینوکسی به

بدافزار خطرناک StripedFly

بدافزار StripedFly که پیش از این تصور می‌شد یک کریپتوماینر است در واقع یک پلتفرم جاسوسی پیچیده برای سیستم‌های ویندوزی و لینوکسی بوده است که می‌تواند در حملاتی از جمله حملات باج‌افزاری، جاسوس‌افزاری و حملات تهدید مانای پیشرفته[1] مورد استفاده قرار گیرد. این بدافزار در پنج سال فعالیت خاموش خود تاکنون بیش از یک میلیون سیستم ویندوزی و لینوکسی را آلوده کرده است. کسپرسکی این بدافزار را برای اولین بار در سال 2022 میلادی شناسایی کرد اما شواهدی وجود دارد که نشان می‌دهد این بدافزار فعالیتش را به عنوان ماینر ارز دیجیتال از سال 2016 میلادی آغاز کرده است. این بدافزار قابلیت‌های پیشرفته‌ای دارد که عبارتند از:

- سرقت کلمه عبور
- ذخیره اسکرین‌شات صفحه قربانی
- استفاده از روش پنهان‌سازی ترافیک ارتباطی مبتنی بر TOR
- به‌روزرسانی خودکار
- اکسپلویت سفارشی آسیب‌پذیری EternalBlue SMBv1
- و قابلیت‌های انتشار کرم‌گونه در شبکه

زنجیره آلودگی بدافزار StripedFly در شکل زیر نشان داده می‌شود. این بدافزار اولین بار با شناسایی شل‌کد مخربی که به پردازه WININIT.EXE تزریق شده بود، توسط کسپرسکی اعلام شد. WININIT.EXE فرآیند قانونی سیستم عامل ویندوز است که راه‌اندازی زیرسیستم‌های مختلف را کنترل می‌کند. پس از بررسی شل‌کد تزریق‌شده، مشخص شد که فایل‌های اضافی مانند اسکریپت‌های پاورشل از سرویس‌های قانونی مانند بیت باکت، گیت هاب و گیت لب دانلود و اجرا می‌شوند. بررسی‌های بیشتر مشخص کرد که سیستم‌های آلوده احتمالا برای اولین بار با استفاده از اکسپلویت سفارشی EternalBlue SMBv1 که کامپیوترهای در معرض اینترنت را هدف قرار می‌داد مورد نفوذ قرار گرفته‌اند. آخرین پیلود این بدافزار[2] از یک کلاینت شبکه TOR برای محافظت از شنود ارتباطات شبکه‌اش استفاده کرده است. همچنین قابلیت غیرفعال کردن پروتکل SMBv1و توزیع و آلوده‌سازی سایر سیستم‌های ویندوز و لینوکس درون شبکه هدف با استفاده از پروتکل‌های SSH و Eternal-Blue را دارد.

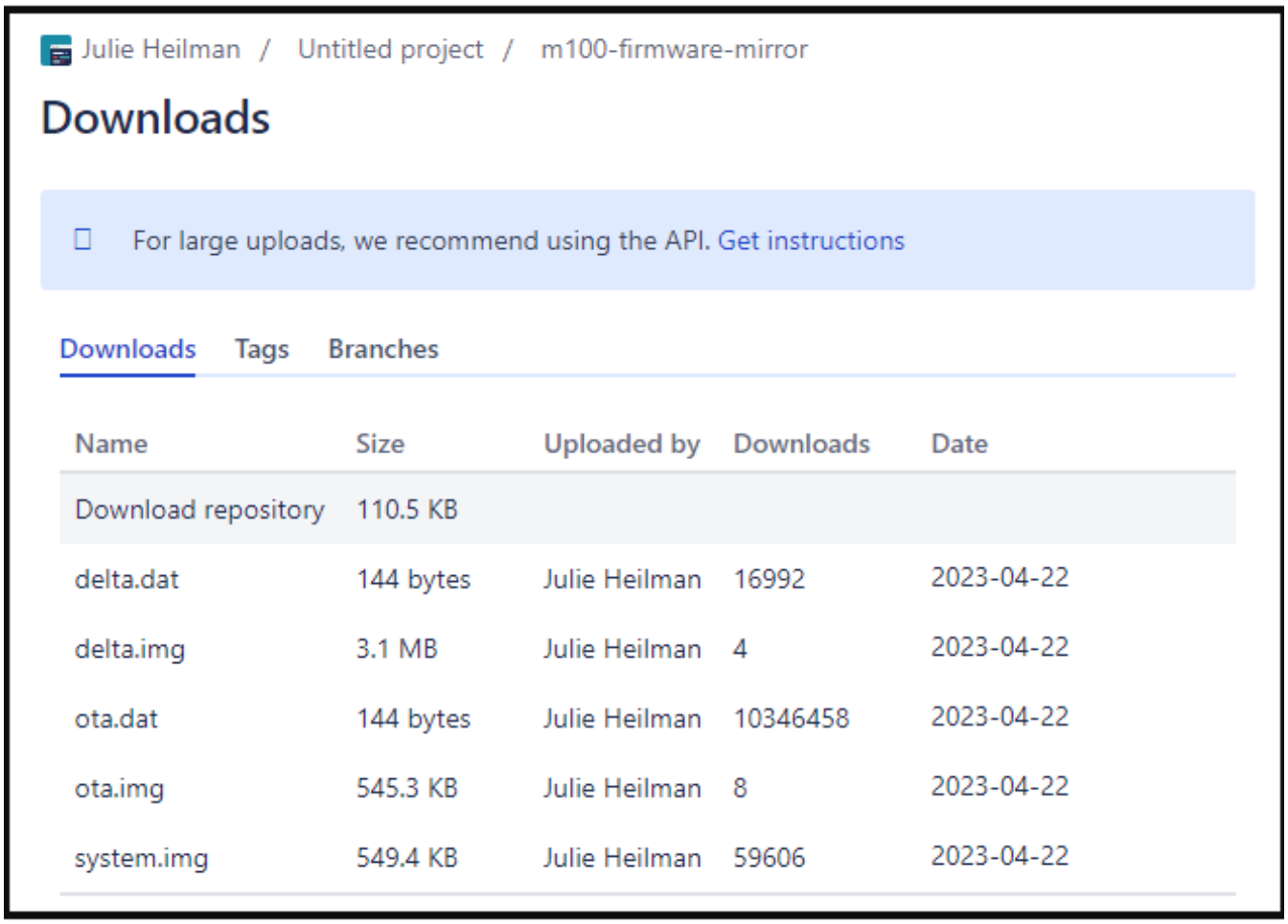


1-APT

2- system.img

StripedFly برای ماندگاری در سیستم‌های ویندوزی، رفتار خود را بر اساس سطح امتیازاتی که روی آن اجرا می‌شود و وجود پاورشل در سیستم تنظیم می‌کند. در صورت وجود پاورشل، اسکریپت‌هایی را برای ایجاد تسک‌های زمان‌بندی شده یا تغییر کلیدهای رجیستری ویندوز اجرا می‌کند. این کار باعث می‌شود که بدافزار پس از راه‌اندازی مجدد سیستم نیز اجرا شود. در صورت عدم وجود پاورشل، فایلی مخفی در دایرکتوری %AP-DATA% ایجاد می‌کند که حاوی کدی برای راه‌اندازی مجدد سیستم است. در سیستم‌عامل لینوکس، برای ماندگاری در سیستم سرویس "sd - pam" را برگزیده است. sd-pam سرویس systemd است که برای مدیریت ورود به سیستم استفاده می‌شود. بدافزار از این سرویس برای ایجاد سرویسی جدید استفاده می‌کند که پس از راه‌اندازی مجدد سیستم اجرا شود.

مخازن بیت‌باکت که پیلود نهایی را به سیستم‌های ویندوزی رسانده‌اند نشان می‌دهد که بین آوریل ۲۰۲۳ تا سپتامبر ۲۰۲۳، نزدیک به ۶۰ هزار سیستم آلوده شده است. این بدان معناست که StripedFly هم‌اکنون در حال توزیع بوده و شمار سیستم‌های آلوده در حال افزایش است. برآورد می شود که StripedFly از فوریه ۲۰۲۲ حداقل ۲۲۰ هزار سیستم ویندوز را آلوده کرده که تعداد بسیار قابل‌توجهی است. متاسفانه آمار قبل از آن در دسترس نیست. بدین ترتیب ممکن است Striped-Fly مدت‌ها قبل از سال ۲۰۲۲ وجود داشته و تعداد سیستم‌های آلوده بسیار بیشتر باشد. کسپرسکی تخمین می‌زند در پنج سال گذشته، بیش از ۱ میلیون سیستم با StripedFly آلوده شده‌اند.



این بدافزار، به عنوان یک فایل اجرایی باینری یکپارچه با مولفه‌های قابل اتصال عمل می‌کند و به نظر می‌رسد با عملیات‌های حملات APT تطابق دارد. برخی از ماژول‌های این بدافزار عبارتند از:

- Configuration storage: پیکربندی بدافزار را به صورت رمزگذاری شده ذخیره می‌کند.
- Upgrade/Uninstall: به روز رسانی یا حذف را بر اساس دستورات سرور C2 مدیریت می‌کند.
- Reverse proxy: اجازه دسترسی از راه دور به شبکه قربانی را می‌دهد.
- Miscellaneous command handler: دستورات مختلف اعم از اجرای پاورشل و ذخیره اسکرین‌شات را اجرا می‌کند.
- Credential harvester: داده‌های حساس کاربران مانند کلمات عبور و نام‌های کاربری افراد را اسکن و جمع‌آوری می‌کند.
- Repeatable tasks : وظایف خاصی را تحت شرایط خاصی انجام می‌دهد، برای نمونه ضبط صدا.
- Recon module : اطلاعات دقیق سیستم را به سرور C2 ارسال می‌کند.
- SSH infector: از اعتبارنامه‌های SSH برای نفوذ به سیستم‌های دیگر استفاده می‌کند.
- SMBv1 infector: با استفاده از اکسپلویت سفارشی EternalBlue به سایر سیستم‌های ویندوز نفوذ می‌کند. این کار ممکن است با استفاده از آلودگی از طریق کرم‌ها باشد.
- Monero mining module : استخراج monero، در حالی که به عنوان فرآیند در chrome.exe استتار شده است.

حضور ماینر کریپتو Monero باعث انحراف افکاری عمومی برای ماهیت واقعی این بدافزار شده بود. در ابتدا StripedFly به عنوان یک بدافزار استخراج ارز دیجیتال در نظر گرفته می‌شد. این تصور ناشی از این واقعیت بود که بدافزار دارای ماینر Monero بود که از پردازنده سیستم آلوده برای استخراج ارز دیجیتال استفاده می‌کرد. با این حال، تحقیقات بیشتر نشان داد که StripedFly توانایی‌های دیگری نیز دارد. در گزارش کسپرسکی اشاره شده است که پیلود بدافزار شامل مولفه های مختلفی است که هر یک برای هدفی خاص طراحی شده‌اند. این مولفه‌ها به تفکیک اهدافشان عبارتند از:

- مولفه استخراج Monero؛
- مولفه سرقت اطلاعات؛
- مولفه بهره‌برداری از آسیب‌پذیری‌های سیستم؛
- مولفه اجرای حملات باج‌افزاری.

علت وجود مولفه استخراج Monero آن است که ارز دیجیتالMonero، تا اواسط سال 2018 به اوج ارزش خود رسید (542.33 دلار) ؛ این در حالی است که در سال 2017، 10 دلار بود. ارزش بالای ارز دیجیتال Mone-ro باعث می‌شود که استخراج این ارز برای مهاجمان جذاب باشد. لیکن وجود این مولفه برای بدافزار مزیتی دیگر داشت. کارشناسان امنیتی تاکید دارند که ماژول استخراج، عامل اصلی بود که باعث شد بدافزار، برای مدت طولانی قابل شناسایی نباشد. مهاجمان از مولفه استخراج Monero برای پنهان کردن فعالیت‌های مخرب خود استفاده می‌کردند.

آلوده شدن بیش از یک میلیون سیستم ویندوزی و لینوکسی به بدافزار خطرناک StripedFly

همچنین ارتباطاتی میان این بدافزار و باج افزار Thun-derCrypt شناسایی شد که نشان می‌دهد ممکن است هر دو بدافزار توسط یک گروه توسعه‌دهنده ایجاد شده باشند. متاسفانه این امر بیانگر آن است که مهاجمان می‌توانند از چندین بدافزار برای رسیدن به اهداف خود استفاده کنند.

با توجه به گستردگی بدافزار توصیه می‌شود سیستم خود را نسبت به وجود علائم آلودگی به این بدافزار بررسی نمایید.

ارتباط با سرور فرماندهی و کنترل:

gpiekd65jgshwp2p53igifv43aug2adacdebmuuri-34hduvijr5pfjad[.]onion ghtyqipha6mcwxiz[.]onion

ajiumbl2p2mjzx3l[.]onion

ارتباطات شبکه‌ای با:

bitbucket[.]org/JulieHeilman/m100-firmware-mir-ror/downloads/

bitbucket[.]org/upgrades/um/downloads/

bitbucket[.]org/legit-updates/flash-player/down-loads

gitlab[.]com/JulieHeilman/m100-firmware-mirror/raw/master/

gitlab[.]com/saev3aeg/ugee8zee/raw/master/

github[.]com/amf9esiabnb/documents/releases/download/

tcp://pool.minexmr[.]com:4444

tcp://mine.aeon-pool[.]com:5555

tcp://5.255.86[.]125:8080

tcp://45.9.148[.]21:80

tcp://45.9.148[.]36:80

tcp://45.9.148[.]132:8080

وجود فایل‌هایی با هش‌های زیر در سیستم:

system.img

b28c6d00855be3b60e220c32bfad2535

18f5ccdd9efb9c41aa63efbe0c65d3db

2cdc600185901cf045af027289c4429c

54dd5c70f67df5dc8d750f19ececd797

d32fa257cd6fb1b0c6df80f673865581

c04868dabd6b9ce132a790fdc02acc14

c7e3df6455738fb080d741dcbb620b89

d684de2c5cfb38917c5d99c04c21769a

a5d3abe7feb56f49fa33dc49fea11f85

35fadceca0bae2cdcfdaac0f188ba7e0

delta.dat

00c9fd9371791e9160a3adaade0b4aa2

41b326df0d21d0a8fad6ed01fec1389f

delta.img

506599fe3aecdfb1acc846ea52adc09f

6ace7d5115a1c63b674b736ae760423b

ota.dat

2e2ef6e074bd683b477a2a2e581386f0

04df1280798594965d6fdfeb4c257f6c

ota.img

abe845285510079229d83bb117ab8ed6

090059c1786075591dec7ddc6f9ee3eb

ThunderCrypt

120f62e78b97cd748170b2779d8c0c67

d64361802515cf32bd34f98312dfd40d

وصله سه آسیب‌پذیری روز صفرم از سوی مایکروسافت که به صورت فعال در حال بهره‌برداری بوده‌اند

مایکروسافت در به‌روزرسانی ماه اکتبر 2023 سه آسیب‌پذیری روز صفرم با شناسه‌های CVE-2023-36563، CVE-2023-41763 و CVE-2023-44487 در WordPad و Skype for Business که به صورت فعال در حال بهره‌برداری بوده‌اند را وصله کرده است.

شناسه CVE-2023-36563 یک آسیب‌پذیری در WordPad است که اگر مهاجم بتواند به سیستم کاربر دسترسی پیدا کند، قادر است با اجرای یک برنامه از پیش طراحی شده خاص، هش NTLM که رمز عبور رمزنگاری شده کاربران ویندوز است را دریافت کند و کنترل سیستم را به دست بگیرد. همچنین مهاجم می‌تواند سیستم کاربر محلی را از طریق باز کردن یک فایل مخرب، آلوده کند. مایکروسافت علاوه بر اعمال وصله برای این آسیب‌پذیری که در به‌روز رسانی ماه اکتبر ارائه شده است، توصیه می‌کند که مدیر سیستم، NTLM خروجی را بر روی SMB در ویندوز ۱۱ غیرفعال کند تا احتمال موفقیت بهره‌برداری از NTLM-relay را به حداقل برساند.

شناسه CVE-2023-41763 یک آسیب‌پذیری در Skype for Business است که باعث می‌شود مهاجم با ارسال یک درخواست خاص به سرور Skype for Business قربانی، اطلاعات حساس مانند آدرس IP و شماره پورت را به دست آورد. مایکروسافت اذعان دارد که این اطلاعات ممکن است منجر به دسترسی به شبکه‌های داخلی بوده و به عنوان یک آسیب‌پذیری ارتقاء سطح دسترسی شناخته شود.

شناسه CVE-2023-44487 یک آسیب‌پذیری در پروتکل HTTP/2 است که توسط مهاجمان برای انجام حملات DDoS با حجم بالا استفاده شده است. این آسیب‌پذیری که با نام Rapid Reset شناخته می‌شود، باعث مصرف منابع و افزایش بار پردازشی سرورهای HTTP/2 شده و ممکن است سرویس‌دهی آن‌ها را مختل کند. مایکروسافت وصله‌هایی را برای محصولات تحت تأثیر خود ارائه کرده است.

مایکروسافت به کاربران اکیداً توصیه کرده است که باید هرچه زودتر به‌روزرسانی ماه اکتبر ۲۰۲۳ را اعمال کنند و تنظیمات امنیتی سیستم‌های خود را مورد بازبینی قرار دهند. همچنین از باز کردن فایل‌های مشکوک پرهیز کنند.

ShellTorch

آسیب‌پذیری ShellTorch سرورهای هوش مصنوعی را در معرض اجرای کد از راه دور قرار می‌دهد

مجموعه‌ای از آسیب‌پذیری‌های بحرانی تحت عنوان ShellTorch در ابزار هوش مصنوعی متن باز TorchServe کشف شده‌اند که ده‌ها هزار سرور متصل به اینترنت را تحت تاثیر قرار می‌دهند. برخی از این سرورها متعلق به شرکت‌های بزرگ می‌باشند. TorchServe که توسط Meta و Amazon توسعه داده می‌شود یک ابزار محبوب برای مقیاس‌پذیری و ارائه مدل‌های چارچوب یادگیری ماشین PyTorch است.

این کتابخانه معمولاً توسط افرادی که در حوزه هوش مصنوعی فعالیت می‌کنند استفاده می‌شود و در کنار کاربران آکادمیک، شرکت‌های بزرگی مانند Amazon، Google، Azure، Tesla، OpenAI و Intel از آن استفاده می‌کنند. نقص‌های TorchServe توسط تیم تحقیقات امنیتی Oligo کشف شده‌اند که می‌توانند منجر به دسترسی غیر مجاز به سرور و اجرای کد از راه دور بر روی نمونه‌های آسیب‌پذیر شوند.

اولین آسیب‌پذیری از نوع پیکربندی نامناسب رابط مدیریتی API است که بدون تصدیق هویت قابل بهره‌برداری است و باعث می‌شود پنل تحت وب به جای localhost به طور پیش‌فرض به 0.0.0.0 تنظیم شود که آن را در دسترس درخواست‌های از راه دور قرار می‌دهد. از آنجایی که رابط کاربری نیازی به تصدیق هویت ندارد، این اجازه دسترسی نامحدود به هر کاربری را می‌دهد و می‌تواند برای بارگزاری مدل‌های آلوده از آدرس‌های خارجی مورد استفاده قرار بگیرد.

نقص امنیتی دوم که شناسه CVE-2023-43654 را به خود اختصاص داده و دارای شدت بحرانی 9.8 می‌باشد و یک آسیب‌پذیری جعل درخواست سمت سرور[1] است که منجر به اجرای کد از راه دور می‌شود. در حالیکه API مربوط به TorchServe دارای یک لیست از دامنه‌های مجاز به دریافت فایل‌های پیکربندی مدل‌ها از یک URL راه دور است، مشخص شده که به طور پیش‌فرض تمام دامنه‌ها مورد پذیرش هستند که این باعث به وجود آمدن نقض SSRF می‌شود و به مهاجمان اجازه خواهد داد مدل‌های مخرب خود را بارگزاری کرده و منجر به اجرای کد از راه دور بر روی سرور شوند.

سومین آسیب‌پذیری با شناسه CVE-2022-1471 دارای شدت بحرانی 9.8 می‌باشد و از نوع Java deserialization است که منجر به اجرای کد از راه دور می‌شود. به دلیل وجود deserialization غیر امن در کتابخانه SnakeYAML، مهاجم می‌تواند یک مدل با فایل مخرب YAML را بارگزاری کند که منجر به اجرای کد از راه دور شود.

1- SSRF

اگر یک مهاجم از این سه آسیب‌پذیری بهره‌برداری کند، به راحتی می‌تواند یک سیستم که نسخه آسیب‌پذیر TorchServe روی آن در حال اجرا است را تحت کنترل خود درآورد.

Oligo اعلام کرده که طی اسکن انجام شده جهت بررسی این آسیب‌پذیرها، ده‌ها هزار آدرس IP را شناسایی کرده است که در حال حاضر در برابر ShellTorch آسیب‌پذیر هستند که برخی از این سرورها متعلق به شرکت‌های بزرگ و بین المللی هستند.

محصولات تحت تأثیر

سه آسیب‌پذیری فوق الذکر که تحت عنوان Shell-Torch شناخته می‌شوند نسخه‌های 0.3.0 تا 0.8.1 TorchServe را تحت تاثیر قرار می‌دهند.

توصیه‌های امنیتی

جهت برطرف کردن این آسیب‌پذیری‌ها، کاربران باید به نسخه 0.8.2 از TorchServe به‌روزرسانی نمایند. این به‌روزرسانی آسیب‌پذیری CVE-2023-43654 را برطرف نمی‌کند ولی یک هشدار در خصوص SSRF به کاربر نمایش می‌دهد. در مرحله بعدی اطمینان حاصل کنید که کنسول مدیریتی دارای پیکربندی درست باشد. در فایل config.properties مقدار management_address باید به http://127.0.0.1:8081 تنظیم شود. این باعث می‌شود که TorchServe فقط از localhost در دسترس باشد. و در آخرین مرحله اطمینان حاصل کنید که با به‌روزرسانی دامنه‌های قابل اطمینان در فایل .config properties و قسمت allowed_urls سرور مدل‌ها را از دامنه‌های مجاز دریافت کند:

allowed_urls=https://s3.amazonaws.com/.*,
https://torchserve.pytorch.org/.*

Oligo یک ابزار برای بررسی آسیب‌پذیری ShellTorch در گیت‌هاب منتشر کرده که از طریق لینک زیر قابل دسترس می‌باشد:

https://github.com/OligoCyberSecurity/ShellTorch-Checker

مرکز آپا دانشگاه سمنان

"تمام چیزی که یک هکر می‌خواهد وجود تنها یک آسیب‌پذیری در سیستم شماست."

ویندو اسنایدر

افسر امنیت نرم افزار و دانشمند رایانه

مرکز آپا دانشگاه سمنان

آموزش

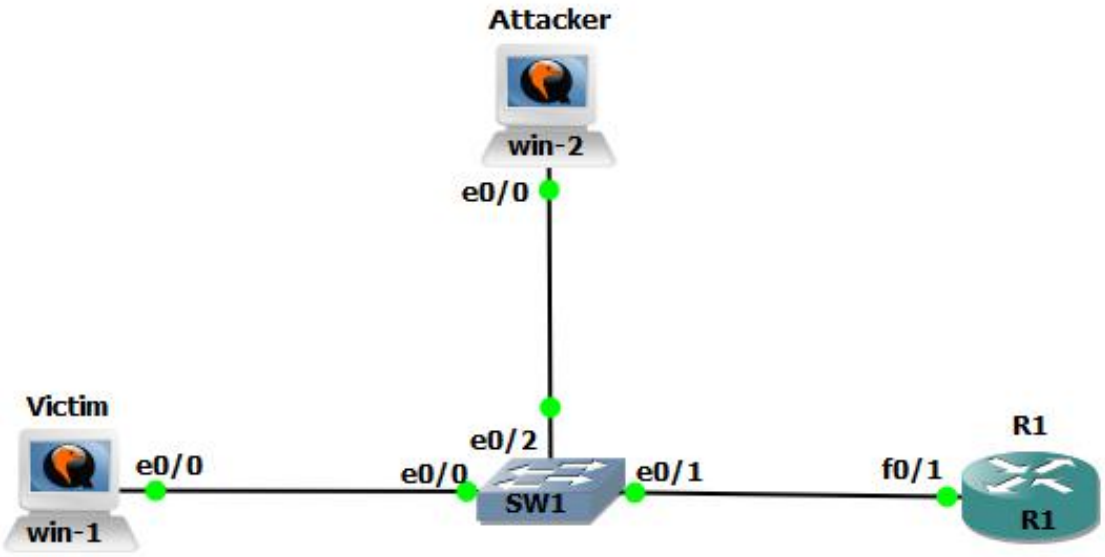
آموزش حمله به پروتکل ARP با استفاده از ابزار Loki

پروتکل ARP[1] عمل تبدیل IP به MAC را انجام می‌دهد. این پروتکل در لایه 2 شبکه فعال است و شیوه کار آن به این شکل است که یک سیستم برای به دست آوردن MAC مربوط به IP، بسته‌ی Broadcast تولید می‌کند. در این بسته یک Ip وجود دارد و سیستم‌های موجود در سطح شبکه، بعد از دریافت این بسته، درصورتی‌که دارای IP یکسانی با IP موجود دربسته باشند، MAC خود را به سمت سیستم ارسال‌کننده‌ی این درخواست می‌فرستند. برای اینکه هر بار این درخواست‌ها ایجاد نشود، نتایج در جدولی با عنوان ARP Cache ذخیره می‌شود و به‌این‌ترتیب جلوی هدر رفت ترافیک و پهنای باند گرفته خواهد شد. هر بار که این درخواست به سیستم‌ها برسد، جدولARP Cache خود را به‌روزرسانی می‌کنند و همین اتفاق باعث می‌شود که مهاجم بتواند تغییراتی در این جدول ایجاد کرده و از آن به نفع خود بهره ببرد. حملاتی تحت عناوین ARP Spoofing یا ARP Poisoning با استفاده از این پروتکل انجام می‌شود. به این شکل که مهاجم با استفاده از این پروتکل می‌تواند جدولCache ARP سیستم‌های موجود در شبکه را با اطلاعات نادرست پر کند و مسیر ترافیک‌های ارسالی را به سمت خود تغییر دهد.

ARP Spoofing

ARP Spoofing یکی از حملات MITM[2] است که در لایه 2 انجام می‌شود. در این حمله هکر با استفاده از ابزارهای موجود، آدرس MAC خود را به‌عنوان آدرس Gateway جا زده و به‌این‌ترتیب قادر خواهد بود تا اطلاعاتی که به مقصد Gateway ارسال می‌شوند را Sniff کند.

برای پیاده‌سازی حمله ARP Spoofing ابتدا شکل 1 را در نرم‌افزار GNS3 رسم می‌کنیم و آدرس‌دهی‌های لازم را انجام می‌دهیم:



شکل1: سناریوی پیاده‌سازی حمله‌ی ARP Spoofing

1-Address resolution protocol
2-Men in the middle

در جدول زیر IP و MAC مربوط به هرکدام از سیستم‌های موجود در سناریو را خواهیم دید:

نام دستگاه	آدرس IP	آدرس MAC	GATEWAY
روتر R1	192.168.1.1	C2:01:16:7e:00:01	-
WIN-1	192.168.1.2	0c:4e:51:1a:88:00	192.168.1.1
WIN-2	192.168.1.100	0c:4e:51:be:c3:00	192.168.1.1

به‌طورکلی، برای پیاده‌سازی این حمله نیاز به واردکردن دستور خاصی در روتر نیست. اما باید دسترسی‌ها در شبکه برقرار باشد. در سناریوی بالا دستور زیر را جهت راه‌اندازی Gateway برای سیستم‌های درون شبکه وارد کنید و سپس مقدار Default Gateway سیستم‌ها را برابر با IP Address مربوط به R1 تنظیم کنید.

```
R1#
R1#
*Mar  1 00:09:39.039: %SYS-5-CONFIG_I: Configured from console by console
R1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface faste 0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

شکل2: دستورات مربوط به روتر R1

در ابتدا Arp Cache سیستم win-1 را قبل و بعد از ارسال بسته‌ی Broadcast می‌بینیم:

```
C:\Windows\system32>arp -a

Interface: 192.168.1.2 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Windows\system32>_
```

شکل3: بررسی ARP Cache

با استفاده از دستور arp، می‌بینیم که هنوز MAC مربوط به Gateway باقی سیستم‌های شبکه در جدول Win-1 وجود ندارد. برای اینکه روند کار پروتکل ARP را ببینیم gateway را ping می‌کنیم تا ارتباطی شکل بگیرد و پیغام‌های Broad-cast برای پیدا کردن Mac ارسال شود. در win-1 با استفاده از نرم‌افزار wireshark بسته‌های ARP را رصد می‌کنیم:

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=36ms TTL=255
Reply from 192.168.1.1: bytes=32 time=5ms TTL=255
Reply from 192.168.1.1: bytes=32 time=7ms TTL=255
Reply from 192.168.1.1: bytes=32 time=8ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 36ms, Average = 14ms

C:\Windows\system32>_
```

شکل 4: ارتباط با Gateway

با اجرای دستور بالا بسته‌ی Broadcast برای پیدا کردن MAC مربوط به Gateway در شبکه ارسال می‌شود. این بسته توسط نرم‌افزار Wireshark به شکل زیر قابل‌نمایش است:

```
ARP      42 Who has 192.168.1.1? Tell 192.168.1.2
ARP      60 192.168.1.1 is at c2:01:16:7e:00:01
ARP      60 192.168.1.1 is at c2:01:16:7e:00:01
```

شکل5: بسته‌ی Broadcast

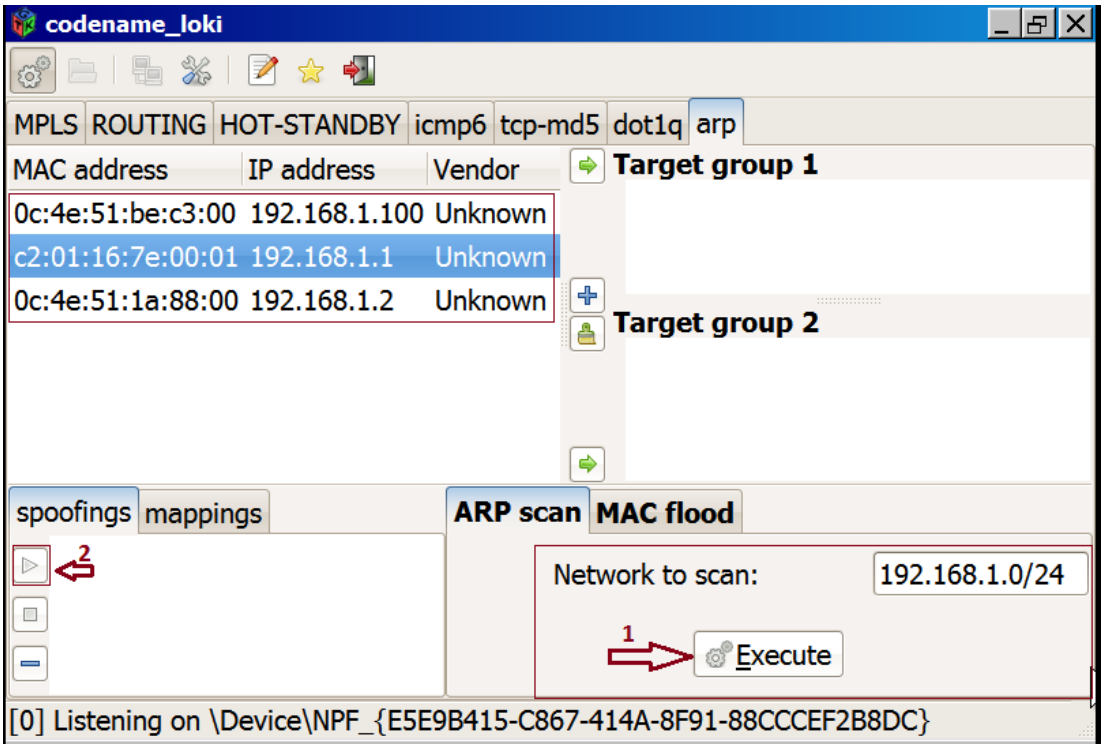
شکل بالا نشان می‌دهد که سیستم به دنبال MAC برای آدرس 192.168.1.1 است و پاسخی که دریافت می‌کند به‌وضوح نشان می‌دهد که این IP متعلق به کیست!

با بررسی دوباره‌ی جدول ARP Cache می‌بینیم که این اطلاعات در جدول درج‌شده است:

```
C:\Windows\system32>arp -a

Interface: 192.168.1.2 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c2-01-16-7e-00-01     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Windows\system32>_
```

شکل 6: اطلاعات جدول ARP Cache بعد از Broadcast

حـالا بـا اسـتفاده از نرم‌افـزار loki سـعی می‌کنیـم کـه MAC مربـوط بـه مهاجـم را بـا Gateway عـوض کنیـم و بـه ایـن شـکل مهاجـم می‌توانـد ترافیک‌هـا را بـه سـمت خـودش هدایـت کنـد. در مرحلـه اول بـا اجـرای نرم‌افـزار loki و انتخـاب کارت شـبکه‌ای کـه می‌خواهیـم حملـه روی آن انجـام شـود، دکمـه‌ی Execute را در بخـش ARP Scan می‌زنیـم تـا سیسـتم‌های موجـود در شـبکه را اسـکن کند(بخـش 1):



شکل 7: اجرای Loki

سـپس بـا زدن دکمهـی Spoof، در تمـام دسـتگاه‌هایی کـه اسـکن شـده‌اند، MAC مهاجـم جایگزیـن بقیـه MAC هـا می‌شـود و بـه ایـن شـکل حملـه اتفـاق میافتد(بخـش 2).

در ادامه تغییراتی که روی روتر و سیستم‌ها اتفاق افتاده را می‌بینیم:

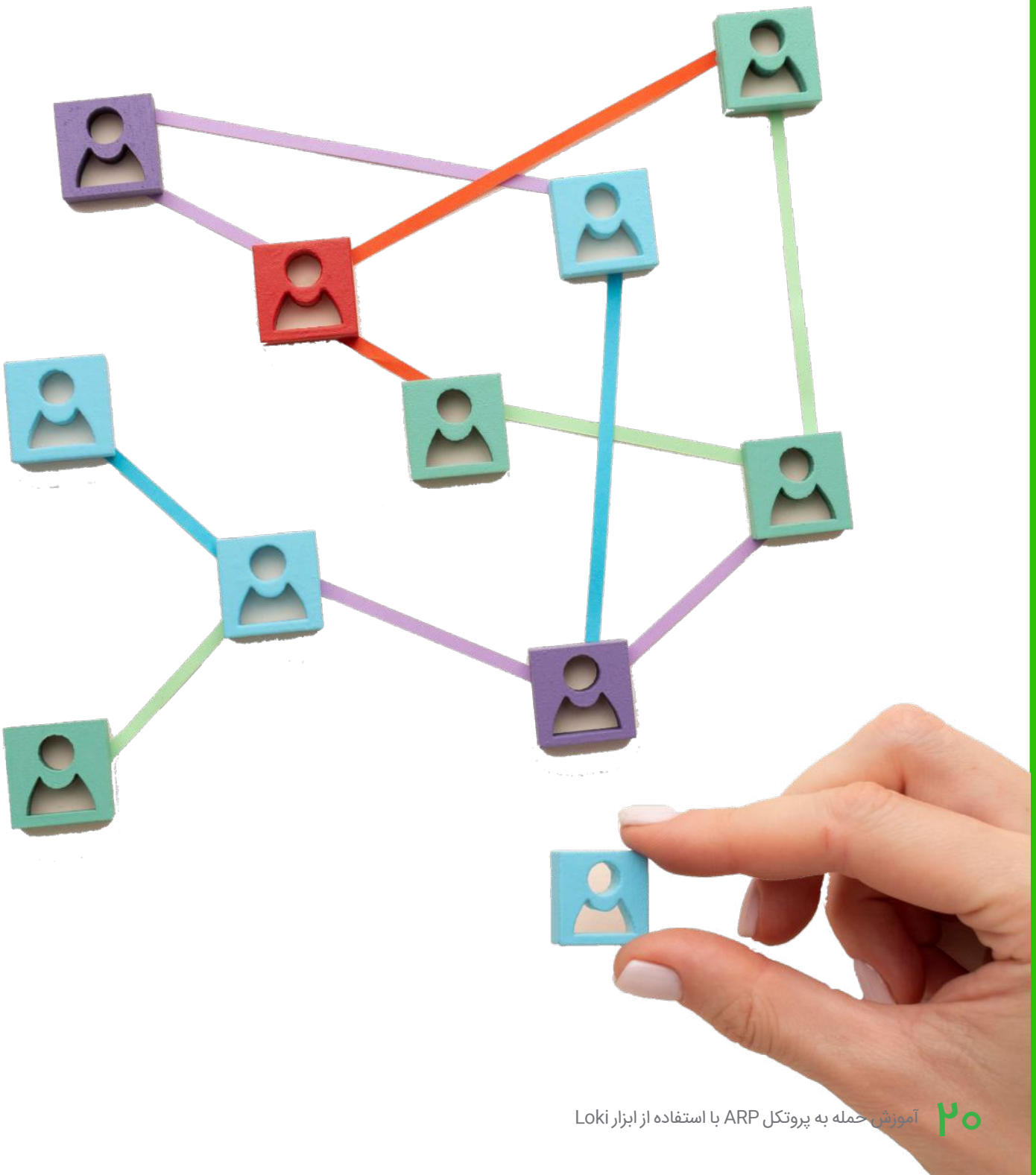
```
C:\Windows\system32>arp -a

Interface: 192.168.1.2 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           0c-4e-51-be-c3-00     dynamic
  192.168.1.100         0c-4e-51-be-c3-00     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Windows\system32>_
```

شکل 8: بررسی جدول ARP Cache سیستم بعد از انجام حمله

```
R1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   c201.167e.0001  ARPA   FastEthernet0/1
Internet  192.168.1.2            0   0c4e.51be.c300  ARPA   FastEthernet0/1
Internet  192.168.1.5            0   0c4e.51be.c300  ARPA   FastEthernet0/1
Internet  192.168.1.100          0   0c4e.51be.c300  ARPA   FastEthernet0/1
R1#
```

شکل 9: بررسی جدول ARP Cache روتر بعد از انجام حمله

با بررسی شکل‌های بالا پیداست که MAC مهاجم جایگزین تمام MACهای موجود در جدول ARP Cache شده است و این باعث تغییر جهت ترافیک به سمت سیستم حمله‌کننده خواهد شد.



تلاش ما
حفظ امنیت
شماست...