بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

کمپین هکری در کمین محصولات Citrix Netscaler

گزارش خبری

نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۴۰۲/۰۷/۲۲
طبقه‌بندی سند ..... عادی

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

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

۱ شرح خبر

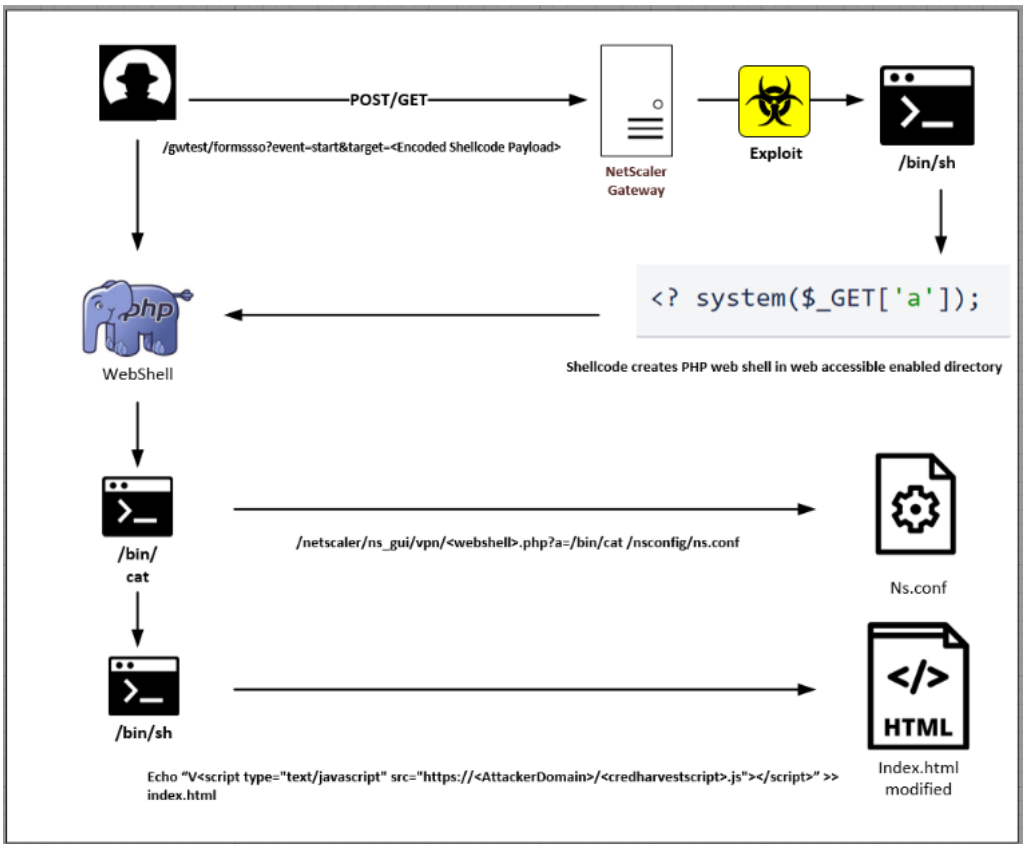
مهاجمان کمپینی در مقیاس بزرگ تشکیل داده‌اند که با سوء استفاده از آسیب‌پذیری اخیر Citrix NetScaler، CVE-2023-3519، اطلاعات ورود کاربران را به سرقت می‌برد. این آسیب‌پذیری که در ماه جولای گزارش شده است برای مهاجم احراز اصالت‌نشده امکان اجرای کد از راه دور و دسترسی غیرمجاز به اطلاعات ورود کاربران نسخه‌های NetScaler زیر را می‌دهد:

- NetScaler ADC و NetScaler Gateway نسخه‌های ۱۳,۱ و قبل از ۱۳,۱-۴۹,۱۳
- NetScaler ADC و NetScaler Gateway نسخه‌های ۱۳,۰ و قبل از ۱۳,۰-۹۱,۱۳
- NetScaler ADC و NetScaler Gateway نسخه‌های ۱۲,۱ تا آخر
- NetScaler ADC 13.1-FIPS (نسخه‌های قبل از ۱۳,۱-۳۷,۱۵۹)
- NetScaler ADC 12.1-FIPS (نسخه‌های قبل از ۱۲,۱-۵۵,۲۹۷)
- NetScaler ADC 12.1-NDcPP (نسخه‌های قبل از ۱۲,۱-۵۵,۲۹۷)

این آسیب‌پذیری تا اوایل ماه آگوست منجر به تسخیر ۶۴۰ سرور Citrix شد و تا اواسط این ماه، تعداد موارد حمله به ۲۰۰۰ سرور افزایش یافت. گزارش X-Force IBM نشان می‌دهد که با وجود هشدارهای متعدد برای به‌روزرسانی دستگاه‌های Citrix، سطح حمله هنوز هم بسیار قابل‌توجه است و هکرها شروع به سوءاستفاده از CVE-2023-3519 برای تزریق جاوا اسکریپت کرده و اعتبارنامه‌های ورود به سیستم کاربران را در ماه سپتامبر به سرقت بردند.

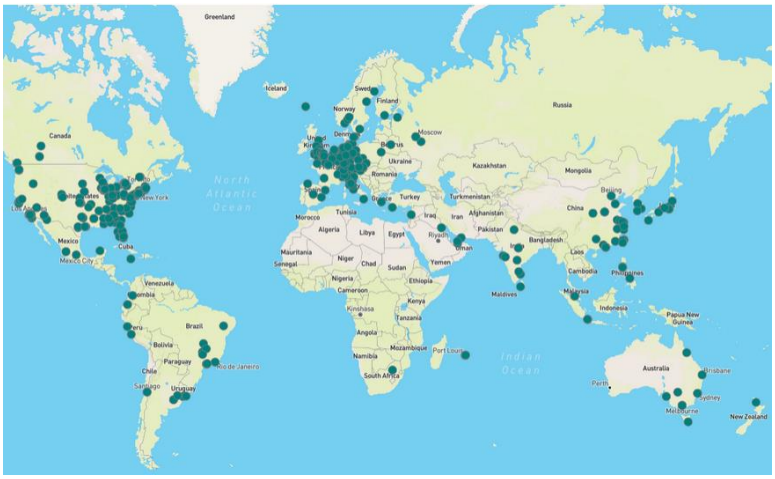
این کمپین سرقت اطلاعات برای اولین بار حین بررسی یکی از کلاینت‌ها که در فرایند احراز هویت در دستگاه NetScaler دچار کندی شده بود شناسایی شد. پس از تحقیقات بیشتر مشخص شد که مهاجمان از آسیب‌پذیری CVE-2023-3519 برای تزریق کد جاوا اسکریپت مخرب به صفحه ورود index.html دستگاه Citrix NetScaler استفاده کرده‌اند. حمله با یک درخواست وب آغاز می‌شود که از دستگاه‌های آسیب‌پذیر NetScaler برای نوشتن یک وب‌شِل ساده PHP در "netscaler/ns_gui/vpn/" سوءاستفاده می‌کند. مهاجمان از این وب‌شِل برای جمع‌آوری داده‌های پیکربندی از فایل "ns.conf" استفاده می‌کنند. سپس

مهاجمان، کد HTML مورد نظر خود را به فایل "index.html" اضافه می‌کنند که وظیفه دریافت و اجرای فایل جاوا اسکریپت راه دور را برعهده دارد. شکل ۱ زنجیره حمله را نشان می‌دهد. آخرین قطعه کد جاوااسکریپت برای جمع‌آوری اطلاعات ورود است. نهایتاً، اطلاعات جمع‌آوری‌شده از طریق یک درخواست HTTP POST به مهاجمان منتقل می‌شود.



شکل ۱. زنجیره حمله

عوامل تهدید چندین دامنه از جمله jscloud[.]ink، jscloud[.]live، jscloud[.]biz، jscdn[.]biz و cloudjs[.]live را برای کمپین ثبت کرده‌اند. X-Force تقریباً ۶۰۰ آدرس IP منحصربه‌فرد را برای دستگاه‌های NetScaler شناسایی کرد که صفحات ورود به سیستم آنها برای تسهیل عملیات سرقت اطلاعات ورود تغییر داده شده بودند. بیشتر قربانیان در ایالات متحده و اروپا قرار دارند، اما سیستم‌های در معرض خطر در سراسر جهان پراکنده‌اند. نقشه پراکندگی حملات در شکل ۲ نمایش داده شده است.



شکل۲. نقشه قربانیان

به منظور پیشگیری از این حمله لازم است در اولین فرصت نسخه‌های آسیب‌پذیر NetScaler ADC و NetScaler Gateway به روز رسانی شود.

۲ منبع خبر

- https://www.bleepingcomputer.com/news/security/hackers-hijack-citrix-netscaler-login-pages-to-steal-credentials/