НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

APT29 АТАКУЄ ПОСОЛЬСТВА, ВИКОРИСТОВУЮЧИ CVE-2023-38831

Резюме

У цьому звіті йдеться про кібератаку, організовану APT29, угрупованням, пов'язаним зі Службою зовнішньої розвідки росії (СЗР). Цілями цієї атаки були різні європейські країни, такі як Греція, Румунія, Італія, а також Азербайджан. Для проникнення в посольства цих країн APT29 використовувало нещодавно виявлену вразливість у WinRAR, ідентифіковану як CVE-2023-38831.

Цей звіт описує кампанію хакерів, тактики, методи та процедури зловмисників. APT29 майстерно використовувало нешкідливі приманки у вигляді привабливих фотографій і документів про продаж автомобілів BMW, які були бездоганно створені для заманювання жертв. Документи-приманки містили прихований шкідливий вміст, який використовував вразливість WinRAR, надаючи зловмисникам доступ до скомпрометованих систем.

Ця кампанія ілюструє еволюцію кіберзагроз та постійні спроби спонсорованих державами акторів скомпрометувати критично важливі об'єкти. Висновки цього звіту мають на меті підвищити обізнаність про складний ландшафт загроз, з якими стикаються дипломатичні місії та організації, що в кінцевому підсумку сприятиме проактивному підходу до посилення кібербезпеки.

Геополітичні наслідки

На початку вересня 2023 року сумнозвісне угрупування APT29, пов'язане з російським сзр, розпочало кібератаку, яка охопила посольства, міжнародні організації і навіть інтернет-провайдерів. Основна увага була зосереджена на дипломатичних акаунтах, причому Міністерства закордонних справ (МЗС) Азербайджану та Італії прийняло на себе основний удар. Крім того, серед численних мішеней також були посольства в Греції та Румунії, та поштові скриньки відомого грецького інтернет-провайдера Otenet. Список жертв розширився до найбільших міжнародних організацій, що підкреслює зухвалість і масштаби цієї кампанії.

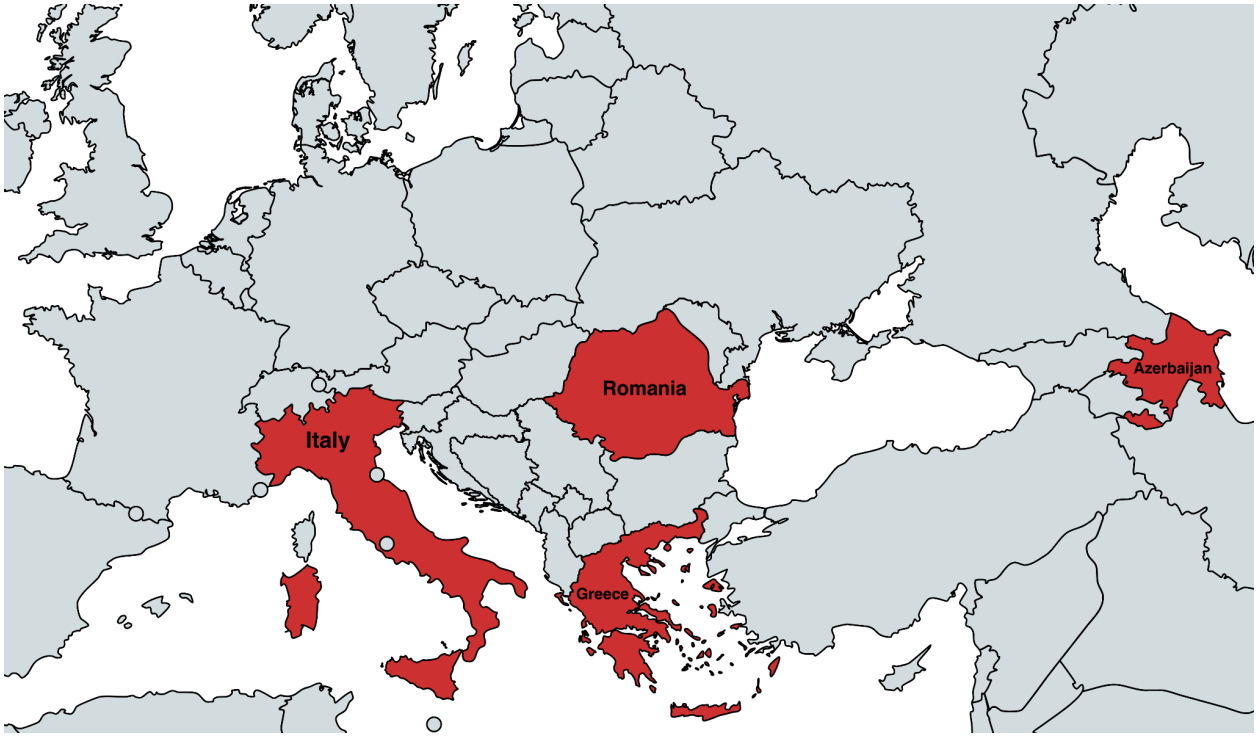

Рис.1 Карта країн з найбільшою кількістю атакованих установ.

Domain	Organization
@gccsg.org	Secretariat General of the Gulf Cooperation Council
@ec.europa.eu	European Commission
@unhcr.org	United Nations High Commissioner for Refugees
@unicef.org	United Nations International Children's Emergency Fund
@auf.org	Agence universitaire de la Francophonie
@francophonie.org	Organisation Internationale de la Francophonie (OIF)
@iom.int	International Organization for Migration
@worldbank.org	The World Bank
@selec.org	Southeast European Law Enforcement Center
@coe.int	Council of Europe
@euro.who.int	World Health Organization European Region

Таблиця.1 Список міжнародних організацій атаковані в рамках кампанії APT29

Серед кількох можливих мотивів, однією з найбільш очевидних цілей СЗР може бути збір розвідувальної інформації про стратегічну діяльність Азербайджану, особливо напередодні азербайджанського вторгнення в Нагірний Карабах. Варто зазначити, що країни-мішені – Азербайджан, Греція, Румунія та Італія – підтримують значні політичні та економічні зв'язки з Азербайджаном. Також Азербайджан нещодавно уклав угоду про закупівлю в Італії військових літаків, що стало рідкісним випадком постачання озброєнь західною країною.

Методологія атаки передбачала використання фішингових електронних листів, які містили приманки із зображенням продажу автомобілів BMW, – тактика, яку раніше використовувала APT29 під час атак на посольства в Києві. Ця кампанія складається з понад 200 цільових електронних адрес і підкреслює еволюцію кіберзагроз на міжнародній арені.

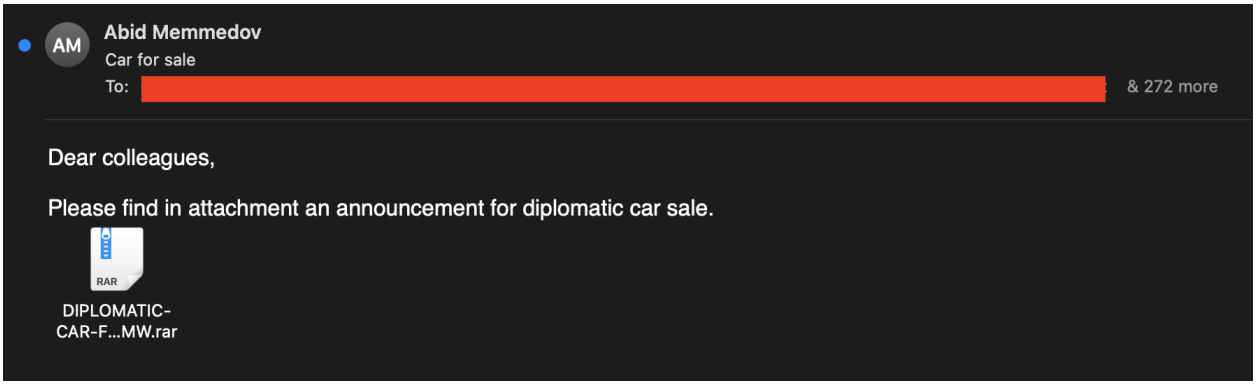

Рис.2 APT29 фішинговий лист з тематикою продажу автомобіля BMW

Старі та Нові Тактики

Використання теми продажу автомобілів BMW як приманки у фішингових атаках APT29 набула нового значення з розгортанням тематичного RAR-архіву "DIPLOMATIC-CAR-FOR-SALE-BMW.rar". Цей архів містить виявлену та використану у квітні 2023 року вразливість CVE-2023-38831. Вона пов'язана з неправильним поводженням з ZIP-архівами, які, на перший погляд, містять звичайні файли, такі як стандартні документи .PDF та папки з однаковими іменами.

Основна проблема прихована в архівах, куди зловмисники можуть непомітно вставляти папки зі схожими іменами. Коли користувач намагається отримати доступ до одного з файлів, ZIP-архів може містити папку з такою ж назвою, що приховує виконуваний вміст, який часто містить шкідливий код. При відкриванні файлу, система обробляє прихований шкідливий вміст у папці з однаковим ім'ям, що дозволяє виконання довільного коду.

В контексті цієї конкретної атаки виконується скрипт, який генерує PDF-файл із зображенням автомобіля BMW, виставленого на продаж. Одночасно у фоновому режимі завантажується і виконується сценарій PowerShell з сервера корисного навантаження наступного етапу. Очевидно, що зловмисники застосували нову техніку з'єднання зі шкідливим сервером, використовуючи безкоштовний статичний домен Ngrok для доступу до свого сервера, розміщеного на інстансі Ngrok.

DIPLOMATIC CAR FOR SALE

BMW | F10 5 Series Sedan 528i xDrive

Price	:	28.000 EUR
Year	:	2016
City	:	Ankara
Brand	:	BMW
Model	:	5 Series
Km	:	115000 KM
Fuel type	:	Benzin
Engine Power	:	258 hp
Color	:	Grey
Body Style	:	Sedan
Transmission	:	Automatic
Cylinder Volume	:	2000 cm³ (cc)
Specifications	:	ABS, Locks, Alarms, Driver Airbag, Passenger Airbag, Fog Shadow, Leather Seats

For more Information, please contact my email: a.memmedov@gmail.com

or give me a call (+90 5013347703)

Рис.3 «DIPLOMATIC-CAR-FOR-SALE-BMW.pdf» документ приманка

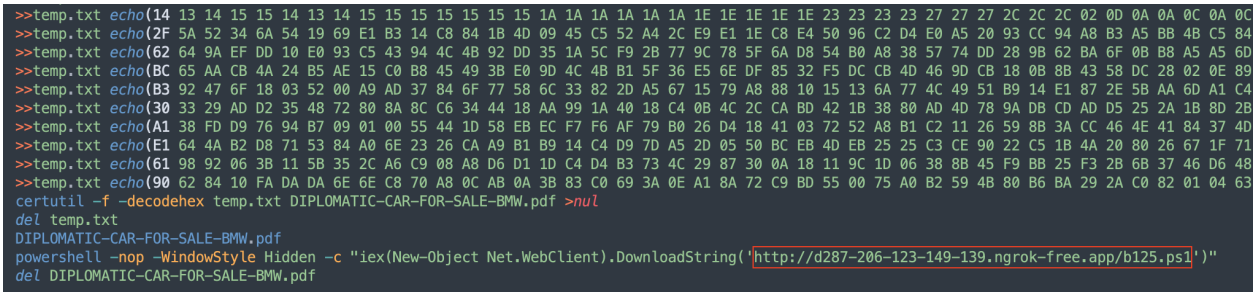

Рис.4 PowerShell скрипт, який створює .pdf документ приманку та завантажує наступний пейлоад з ngrok-free.app

Ngrok – це універсальний та крос-платформний інструмент, призначений для безпечного підключення портів локальної мережі до Інтернету за допомогою процесу, відомого як тунелювання. Однак під час кібероперацій Ngrok виконує іншу роль. Замість легітимного призначення, зловмисники почали використовувати Ngrok для зберігання свого наступного корисного навантаження PowerShell та встановлення прихованих каналів зв'язку.

Таким чином вони використовують безкоштовні статичні домени, надані Ngrok, як правило, у вигляді субдомену під назвою ngrok-free.app. Ці субдомени діють як дискретні та непомітні точки доступу для їхнього шкідливого корисного навантаження. Ця адаптація дозволяє зловмисникам маскувати свою діяльність і спілкуватися зі скомпрометованими системами, уникаючи при цьому виявлення. Використовуючи можливості Ngrok у такий спосіб, зловмисники можуть ще більше ускладнити зусилля фахівців з кібербезпеки та залишатися «під радаром», що ускладнює захист і ідентифікацію зловмисників.

CVE-2023-38831

Критична вразливість, ідентифікована як CVE-2023-38831, була виявлена в попередніх версіях програмного забезпечення WinRAR від RARLab, зокрема, випущених до версії 6.23. Вона становить значну загрозу, оскільки дозволяє зловмисникам виконати довільний код за допомогою спеціально створеного ZIP-архіву.

Основною причиною цієї уразливості є некоректна робота з ZIP-архівами, які містять, на перший погляд, звичайні файли, такі як .PDF або папки з однаковими іменами. Суть проблеми в тому, що зловмисники можуть вставити в ці архіви папки з однаковими іменами. Коли користувач намагається отримати доступ до одного з нешкідливих файлів, ZIP-архів може містити папку з такою ж назвою, яка містить виконуваний вміст, часто шкідливе програмне забезпечення або інший шкідливий код. Під час спроби користувача відкрити безпечний файл, система мимоволі обробляє шкідливий вміст однойменної папки, що призводить до виконання довільного коду.

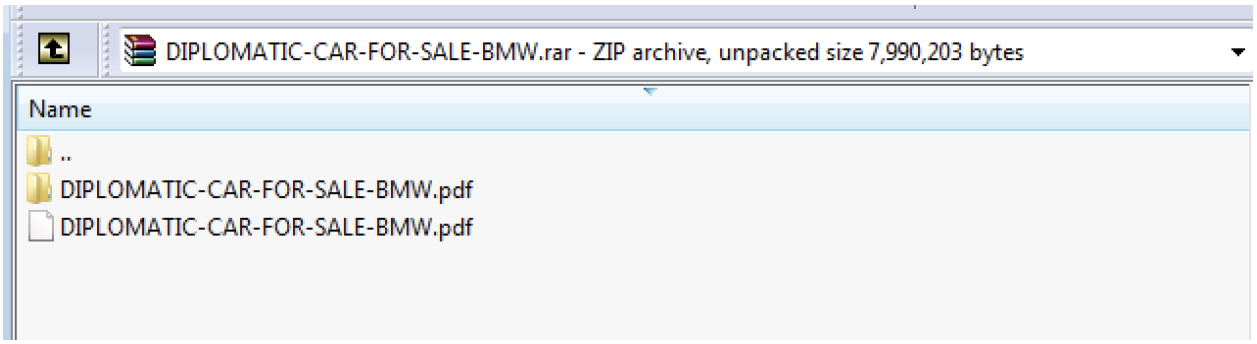

Рис.5 WinRAR архів, що експлуатує CVE-2023-38831

Ця вразливість активно використовувалась в реальних інцидентах. Ці атаки були зафіксовані в період з квітня по жовтень 2023 року. Зловмисники використовують цю вразливість для створення шкідливих ZIP-архівів і розповсюдження їх різними каналами, наприклад, у вигляді вкладень в електронних листах або на скомпрометованих вебсайтах. Користувачі, які відкривають ці, на перший погляд, безпечні файли, можуть несвідомо запустити виконання шкідливого коду, надаючи зловмисникам доступ до системи жертви та потенційно призводячи до низки згубних сценаріїв, включаючи крадіжку даних, компрометацію системи тощо. PoC цієї вразливості знаходиться у відкритому доступі.

У серпні 2023 року дослідники ESET виявили ще одну фішингову кампанію, яку приписують **Sednit APT**, що використовує вразливість CVE-2023-38831 в WinRAR. Sednit, також відомий як APT28, – це група зловмисників, тісно пов'язана з російською військовою розвідкою ГРУ. Підхід Sednit полягав у використанні електронних листів з приманками, які стосувалися порядку денного Європейського парламенту. Це була прорахована кампанія, оскільки основними цілями були політичні структури в Європейському Союзі та Україні.

Тривожна тенденція використання вразливості CVE-2023-38831 хакерськими групами російських спецслужб свідчить про її зростаючу популярність. Організаціям та фахівцям з безпеки потрібно зберігати пильність та бути проактивними у захисті від кіберзагроз. Користувачам WinRAR вкрай важливо оновити своє програмне забезпечення до версії 6.23 або новішої, яка містить необхідні виправлення для усунення цієї критичної вразливості. Крім того, дотримання обережності при відкритті файлів, отриманих з невідомих джерел або ненадійних місць, є додатковим рівнем захисту від потенційної експлуатації цієї вразливості. Поінформованість про кібербезпеку та своєчасне оновлення програмного забезпечення мають вирішальне значення для підтримання стійкого захисту від таких загроз.

Висновки

У цьому звіті йдеться про кампанію, організовану APT29, угрупованням, пов'язаним з російською розвідкою. Їхні цілеспрямовані атаки на посольства, зокрема в Азербайджані, Греції, Румунії та Італії, дають новий погляд на еволюцію ландшафту загроз.

Одним з найбільш очевидних геополітичних мотивів цих атак є отримання розвідувальної інформації, особливо щодо дій Азербайджану в Нагірному Карабасі. Це чітке нагадування про те, що кібершпигунство є інструментом державного управління, і його вплив поширюється на різні регіони та сектори.

Цю кампанію особливо примітною робить синтез старих і нових методів. APT29 продовжує використовувати тему приманки у вигляді виставленого на продаж автомобіля BMW – тактику, яка застосовувалась в минулому. Однак використання вразливості CVE-2023-38831 WinRAR, що є новим підходом, свідчить про їхню здатність адаптуватися до мінливого ландшафту загроз. До того ж використання зловмисниками сервісів Ngrok для встановлення прихованого зв'язку підкреслює їхнє бажання залишатися непоміченими.

Крім того, поширеність подібних методів серед російських хакерських груп підкреслює, що організаціям необхідно серйозно ставитися до заходів безпеки. Впровадження суворих практик кібербезпеки, постійне інформування про найновіші вразливості та розвиток культури обізнаності з питань кібербезпеки є життєво важливими для захисту від цих складних і постійних загроз.

Індикатори Компрометації

Type	Value
filename	NEAS.f78ee3005ca9f0e78a9dd136fc69afe7c06d69d1fc6218bc9e7eb3adec045977zip.zip
md5	3b641b7e68b671da6497d10f773dcf7c
sha-1	37c619b18ba52956c249551587b955e7b2066b73
sha-256	f78ee3005ca9f0e78a9dd136fc69afe7c06d69d1fc6218bc9e7eb3adec045977
filename	payload_1.ps1
md5	2b9812a7793c3fe0f171456acd9edf02
sha-1	448047b975175cb9c1e8b36036324835a9e9943e
sha-256	5d6bfb8fd1102273ef489060219293f8da796d07e8b2872efbda55050512b71f
filename	Car for sale.eml
md5	ff7d1fb202bac38345be8cf267fa6688
sha-1	3da35178fb0b3a8ef51b78a07c719658a628d722
sha-256	eec902a61886198a8e48ac862fabeecd628f2fa4122b78a0d7d6ee5c256ae724
url	http://d287-206-123-149-139.ngrok-free.app/b125.ps1
domain	d287-206-123-149-139.ngrok-free.app
email address	a.menmedov@outlook.com