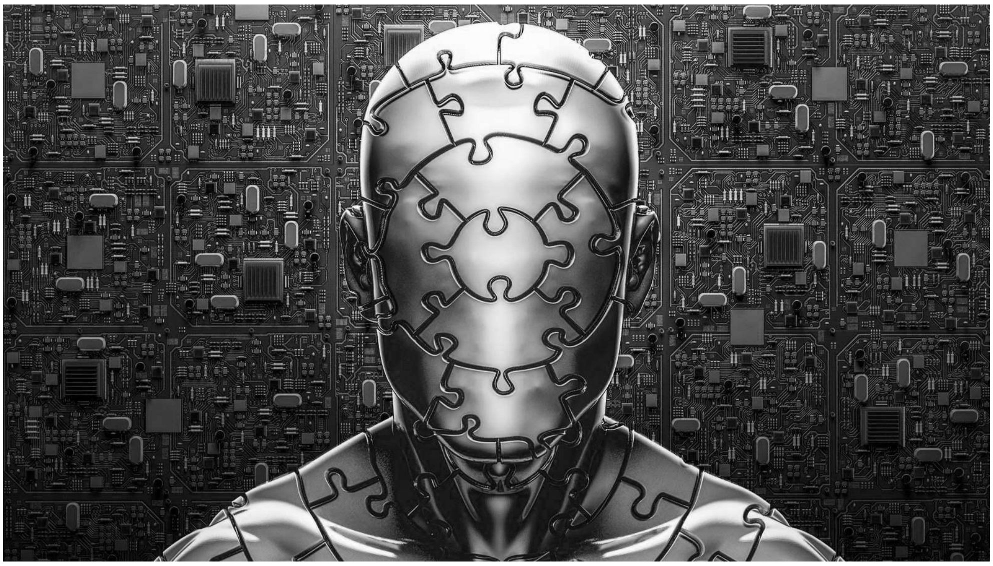
Russian state hackers lure Western diplomats with BMW car ads

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

July 12, 2023 03:01 PM 1



The Russian state-sponsored hacking group 'APT29' (aka Nobelium, Cloaked Ursa) has been using unconventional lures like car listings to entice diplomats in Ukraine to click on malicious links that deliver

APT29 is linked to the Russian government's Foreign Intelligence Service (SVR) and has been responsible for numerous cyberespionage campaigns targeting high-interest individuals across the globe.

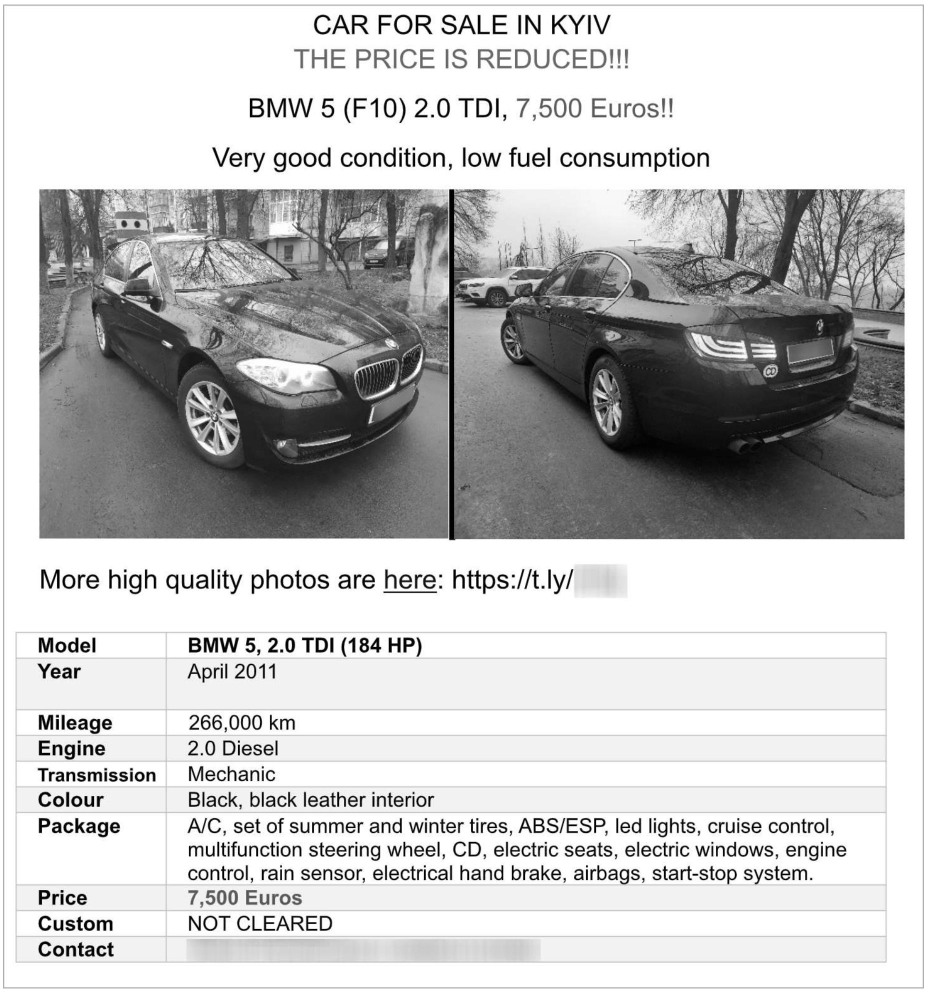
In the past two years, Russian hackers focused on NATO, EU (https://www.bleepingcomputer.com/news/security/russian-hackers-linked-to-widespread-attacks-targeting-nato-and-eu/), and Ukrainian targets, using phishing emails and documents with foreign policy topics, along with phony websites to infect their targets with stealthy backdoors (https://www.bleepingcomputer.com/news/security/russian-apt29-hackers-stealthy-malware-undetected-for-years/).

A report published today by Palo Alto Network's Unit 42 team (https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/) explains that APT29 has evolved its phishing tactics, using lures that are more personal to the phishing email recipient.

Luxury cars in Kyiv

In one of the most recent APT29 operations spotted by Unit 42, which started in May 2023, the threat actors use a BMW car advertisement to target diplomats in Ukraine's capital, Kyiv.

The sale flier was sent to diplomat's email addresses, mimicking a legitimate car sale circulated two weeks prior by a Polish diplomat preparing to leave Ukraine.



CAR FOR SALE IN KYIV

THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption

More high quality photos are here: https://t.ly/[redacted]

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	**7,500 Euros**
Custom	NOT CLEARED
Contact	[redacted]

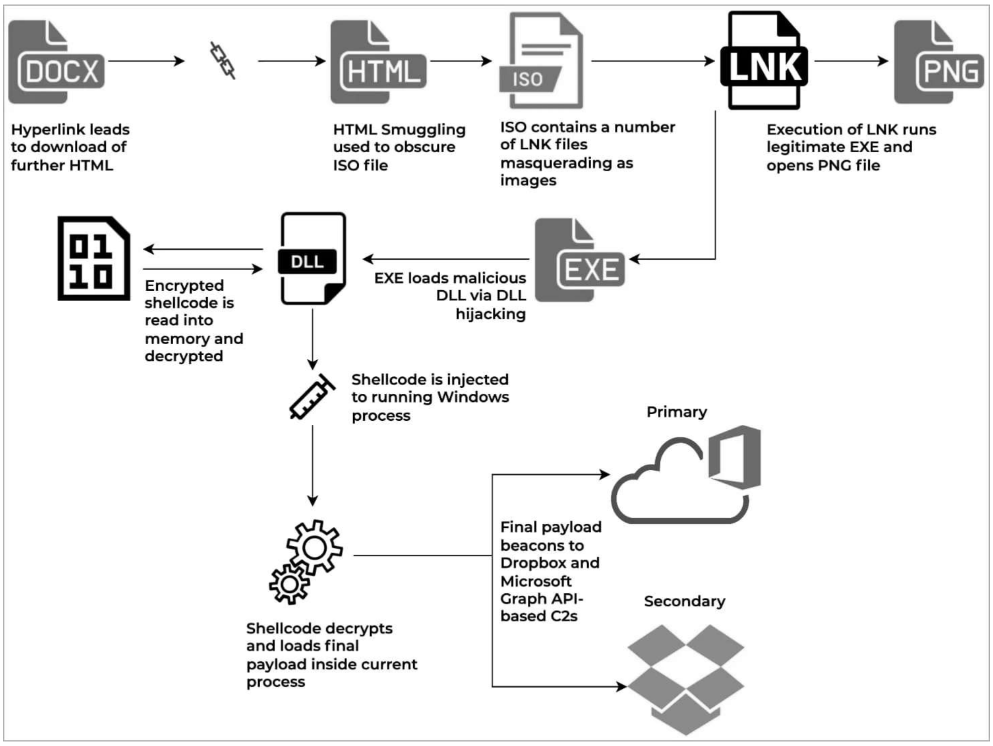
Malicious flyer sent by APT29 *(Unit 42)*

When the recipients click on the "more high-quality photos" link embedded in the malicious document, they are redirected to an HTML page that delivers malicious ISO file payloads via HTML smuggling.

HTML smuggling is a technique used in phishing campaigns that use HTML5 and JavaScript to hide malicious payloads in encoded strings in an HTML attachment or webpage. These strings are then decoded by a browser when a user opens the attachment or clicks a link.

Using this technique helps to evade security software as the malicious code is obfuscated and only decoded on rendering in the browser.

The ISO file contains what appears to be nine PNG images but are, in reality, LNK files that trigger the infection chain shown in the diagram below.


DOCX
HTML
ISO
LNK
PNG
Hyperlink leads to download of further HTML
HTML Smuggling used to obscure ISO file
ISO contains a number of LNK files masquerading as images
Execution of LNK runs legitimate EXE and opens PNG file
01
10
DLL
EXE
Encrypted shellcode is read into memory and decrypted
EXE loads malicious DLL via DLL hijacking
Shellcode is injected to running Windows process
Primary
Final payload beacons to Dropbox and Microsoft Graph API-based C2s
Secondary
Shellcode decrypts and loads final payload inside current process

Observed infection chain *(Unit 42)*

When the victim opens any of the LNK files posing as PNG images, they launch a legitimate executable that uses DLL side-loading to inject shellcode into the current process in memory.

Fake PNG files contained in the ISO archive *(Unit 42)*

Unit 42 reports that this campaign has targeted at least 22 of the 80 foreign missions in Kyiv, including those of the United States, Canada, Turkey, Spain, Netherlands, Greece, Estonia, and Denmark. However, the infection rate remains unknown.

Roughly 80% of the email addresses that received the malicious flyer were publicly available online, while APT29 must have sourced the other 20% through account compromise (https://www.bleepingcomputer.com/news/security/russian-hackers-compromise-embassy-emails-to-target-governments/) and intelligence collection.

Targeted embassies in Ukraine *(Unit 42)*

Another recent example of APT29's readiness to exploit real-world incidents for phishing is a PDF sent to the Turkish Ministry of Foreign Affairs (MFA) earlier in 2023, guiding humanitarian assistance for the earthquake that struck southern Turkey in February.

Unit 42 comments that the malicious PDF was likely shared among MFA's employees and forwarded to other Turkish organizations, as the attack took advantage of the excellent timing.

As the conflict in Ukraine persists and evolving developments within NATO threaten to alter the geopolitical landscape, Russian cyber espionage groups are expected to continue and even intensify their efforts to target diplomatic missions.

Related Articles:

Hackers target European government entities in SmugX campaign (https://www.bleepingcomputer.com/news/security/hackers-target-european-government-entities-in-smugx-campaign/)

CISA orders govt agencies to patch bugs exploited by Russian hackers (https://www.bleepingcomputer.com/news/security/cisa-orders-govt-agencies-to-patch-bugs-exploited-by-russian-hackers/)

Russian APT28 hackers breach Ukrainian govt email servers (https://www.bleepingcomputer.com/news/security/russian-apt28-hackers-breach-ukrainian-govt-email-servers/)

Asylum Ambuscade hackers mix cybercrime with espionage (https://www.bleepingcomputer.com/news/security/asylum-ambuscade-hackers-mix-cybercrime-with-espionage/)

An AI-based Chrome Extension Against Phishing, Malware, and Ransomware (https://www.bleepingcomputer.com/news/security/an-ai-based-chrome-extension-against-phishing-malware-and-ransomware/)

APT29 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/APT29/)

BMW (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/BMW/)

CYBER-ESPIONAGE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBER-ESPIONAGE/)

NOBELIUM (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/NOBELIUM/)

PHISHING (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/)

RUSSIA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RUSSIA/)

RUSSIAN INTELLIGENCE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RUSSIAN-INTELLIGENCE/)

(https://www.bleepingcomputer.com/author/bill-toulas/)

BILL TOULAS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/)

(MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM)
(HTTPS://TWITTER.COM/BILLTOULAS)

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

PREVIOUS ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/MICROSOFT/NEW-WINDOWS-11-BUILD-SHIPS-WITH-MORE-RUST-BASED-KERNEL-FEATURES/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/SONIC WARNS-ADMINS-TO-PATCH-CRITICAL-AUTH-BYPASS-BUGS-IMMEDIATELY/)

Comments

ranchhand_ (https://www.bleepingcomputer.com/forums/u/789552/ranchhand/)
- 11 hours ago

"HTML5 and JavaScript to hide malicious payloads"
...Another reason to run Noscript on your computer...

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

You may also like:

POPULAR STORIES

Microsoft rebrands Azure Active Directory to Microsoft Entra ID

(https://www.bleepingcomputer.com/news/microsoft/microsoft-rebrands-azure-active-directory-to-microsoft-entra-id/)

Microsoft July 2023 Patch Tuesday warns of 6 zero-days, 132 flaws

(https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2023-patch-tuesday-warns-of-6-zero-days-132-flaws/)

FOLLOW US:

[illegible]

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

VPN Buyer Guides (https://www.bleepingcomputer.com/vpn/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/) - Affiliate Disclosure (https://www.bleepingcomputer.com/affiliate-disclosure/)