# Article information:

APT28 Targets Ukrainian Government Entities with Fake "Windows Update" Emails
<https://thehackernews.com/2023/05/apt28-targets-ukrainian-government.html>

# Article summary:

1. APT28, a Russian nation-state hacking group, has been targeting Ukrainian government entities with fake "Windows Update" emails.

2. The phishing campaign involves impersonating system administrators of the targeted government entities using fake Microsoft Outlook email accounts created with the employees' real names and initials.

3. The Computer Emergency Response Team of Ukraine (CERT-UA) is recommending that organizations restrict users' ability to run PowerShell scripts and monitor network connections to the Mocky API to prevent these attacks.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article reports on a warning from the Computer Emergency Response Team of Ukraine (CERT-UA) about cyber attacks targeting Ukrainian government entities by Russian nation-state hackers, specifically APT28. The phishing campaign involves fake "Windows Update" emails containing instructions in Ukrainian to run a PowerShell command under the pretext of security updates. The script collects system information and exfiltrates it via an HTTP request to a Mocky API. The emails impersonate system administrators using fake Microsoft Outlook email accounts created with employees' real names and initials.

The article provides some context for the attacks, including recent ties between APT28 and attacks exploiting now-patched security flaws in networking equipment, as well as credential harvesting operations and exploitation of a critical privilege escalation flaw in Microsoft Outlook. It also mentions a multi-stage phishing attack that leverages a macro-laced Word document supposedly from Ukraine's Energoatom as a lure to deliver the open source Havoc post-exploitation framework.

Overall, the article appears to be well-sourced and informative, providing details on the specific tactics used in the phishing campaign and contextualizing them within broader trends in Russian hacking activity. However, there are some potential biases or missing points of consideration worth noting.

Firstly, while the article notes that CERT-UA is recommending organizations restrict users' ability to run PowerShell scripts and monitor network connections to the Mocky API, it does not provide any further analysis or discussion of these recommendations. It would be helpful to know more about why these measures are effective or necessary.

Secondly, while the article cites cybersecurity firm Recorded Future's report earlier this year suggesting that Russian intelligence agencies have an established relationship with cybercriminal threat actors, it does not provide any counterarguments or alternative perspectives on this claim. It would be useful to know if other experts disagree with this assessment or have different interpretations of the evidence.

Finally, while the article provides some context for recent Russian hacking activity targeting Ukraine and other European countries, it does not explore the broader geopolitical context or potential motivations for these attacks. For example, it would be interesting to know if there are any ongoing political tensions or conflicts between Russia and Ukraine that might be driving this activity.

Overall, while the article provides a useful overview of the APT28 phishing campaign targeting Ukrainian government entities, there are some potential biases and missing points of consideration worth noting.

# Topics for further research:

* Geopolitical tensions between Russia and Ukraine
* APT28 cyber espionage group
* PowerShell script security measures
* Russian intelligence agencies and cybercriminals
* Exploitation of Microsoft Outlook vulnerabilities
* Havoc post-exploitation framework

# Report location:

<https://www.fullpicture.app/item/a390dda860cd549afdd9a0968a6c6cbc>