CLICKFIX UNMASKED: KIMSUKY'S PSYCHOLOGICAL DECEPTION VIA POWERSHELL

Vairav Security News Report

Date: July 01, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Thirbam Sadak 148
Baluwatar, Kathmandu

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

In a chilling evolution of North Korean cyber operations, Genians Security Center (GSC) has exposed the APT group **Kimsuky's** renewed phishing and malware campaign dubbed **"ClickFix."** This highly deceptive attack chain tricks users into copying and executing PowerShell commands themselves under the pretense of fixing browser issues or accessing secured content. Seamlessly integrated into Kimsuky's long-standing **BabyShark** activity, ClickFix manipulates victims through trust, linguistic familiarity, and technical illusion.

ATTACK VECTOR & TECHNICAL HIGHLIGHTS

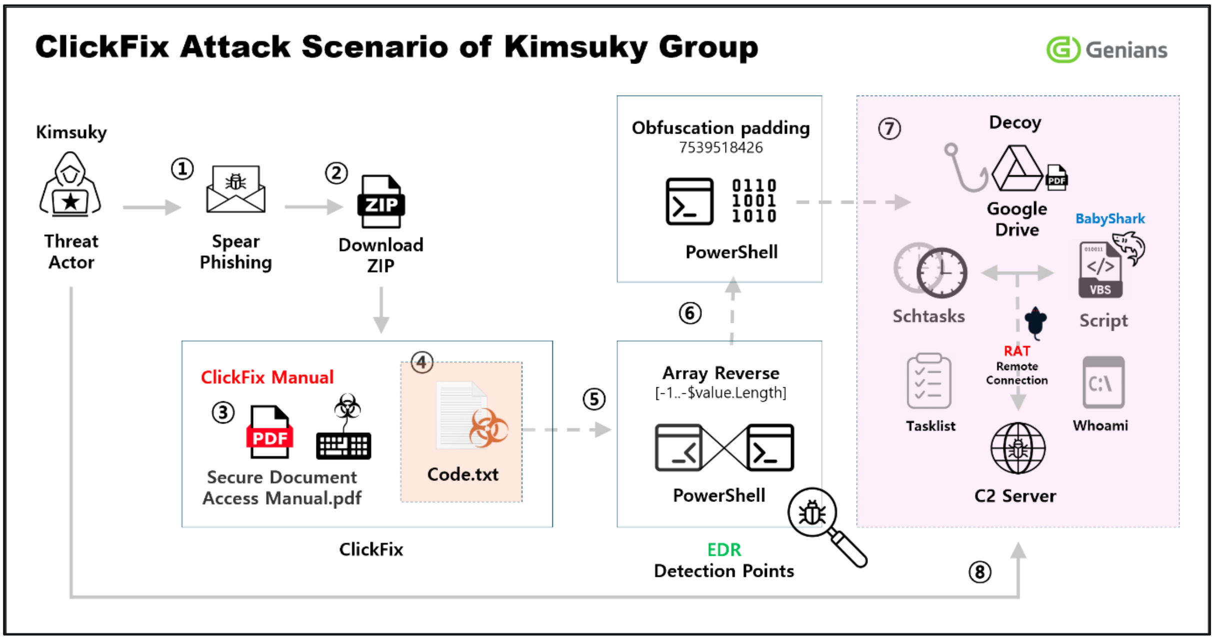
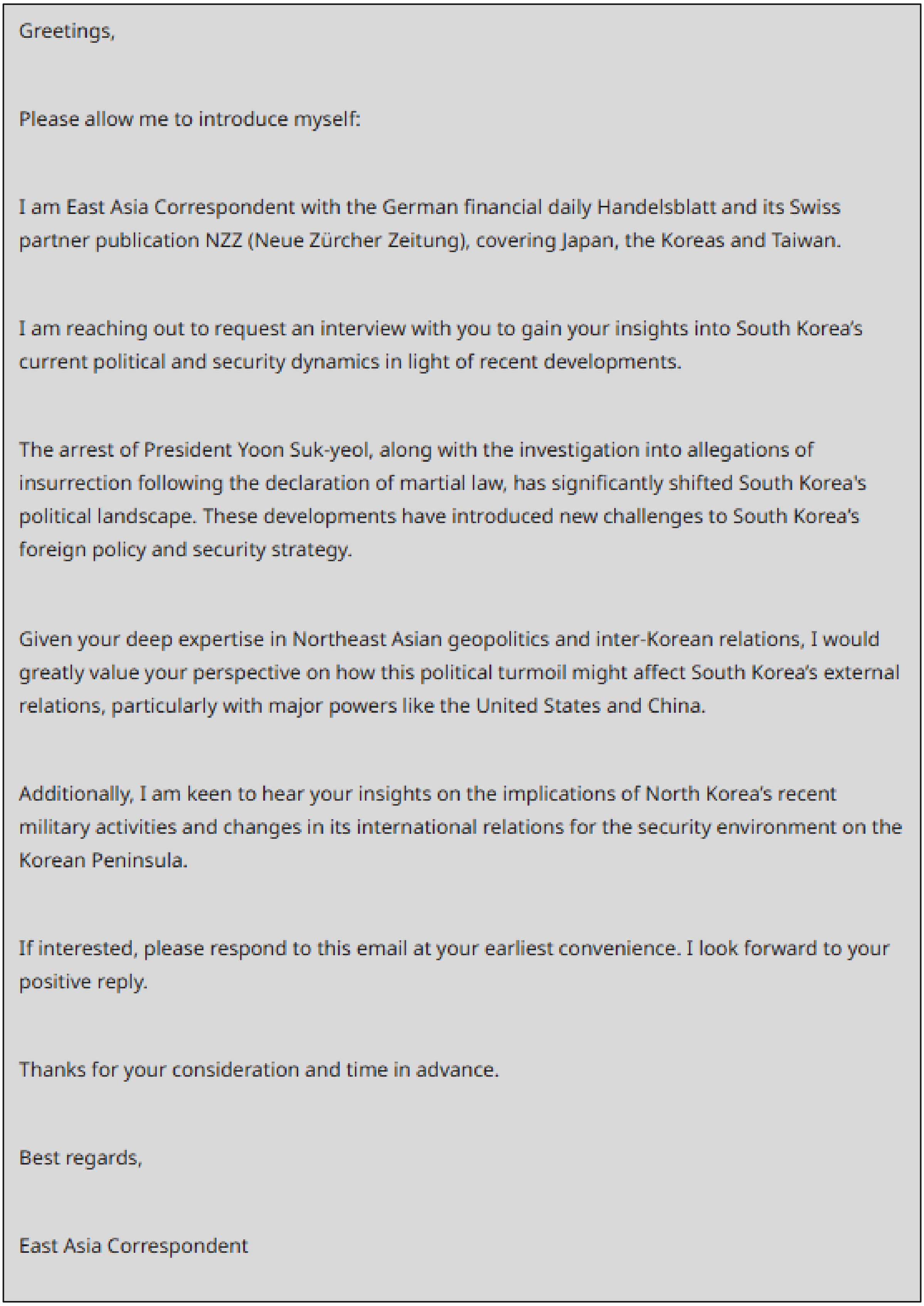


Figure 1: Attack Scenario

KEY ATTACK FEATURES

- **Initial Vector:** Spear-phishing emails disguised as interview requests or national security correspondence
- **Technique:** PowerShell commands obfuscated to appear as authentication codes or error fixes
- **Outcome:** Full system compromise, persistent access, and sensitive data exfiltration

CAMPAIGN DETAILS



Greetings,

Please allow me to introduce myself:

I am East Asia Correspondent with the German financial daily Handelsblatt and its Swiss partner publication NZZ (Neue Zürcher Zeitung), covering Japan, the Koreas and Taiwan.

I am reaching out to request an interview with you to gain your insights into South Korea's current political and security dynamics in light of recent developments.

The arrest of President Yoon Suk-yeol, along with the investigation into allegations of insurrection following the declaration of martial law, has significantly shifted South Korea's political landscape. These developments have introduced new challenges to South Korea's foreign policy and security strategy.

Given your deep expertise in Northeast Asian geopolitics and inter-Korean relations, I would greatly value your perspective on how this political turmoil might affect South Korea's external relations, particularly with major powers like the United States and China.

Additionally, I am keen to hear your insights on the implications of North Korea's recent military activities and changes in its international relations for the security environment on the Korean Peninsula.

If interested, please respond to this email at your earliest convenience. I look forward to your positive reply.

Thanks for your consideration and time in advance.

Best regards,

East Asia Correspondent

Figure 2: Contents of the Initial Phishing Email

GSC reports show Kimsuky deploying **ClickFix** via various lures:

- Fake Chrome error pages encouraging users to “fix” by copying malicious PowerShell commands.
- Spoofed job portals requiring “authentication” through embedded code.
- Fake CAPTCHA forms that launch reverse shells on execution.

One instance involved a phishing email impersonating a U.S. national security aide, asking the target to open a secure document. The document contained a scrambled PowerShell command such as:

```
$req_value=-join $value.ToCharArray()[-1..-$value.Length];
cmd /c $req_value;
exit;
```

Once executed, it established a connection to a **C2 server** and began harvesting data.

TOOLS & TACTICS OBSERVED

- Malicious VBS files delivered via pCloud
- Chrome Remote Desktop misuse for SSH access
- AutoIt-based data theft tools like *HncUpdateTray.exe*
- **C2 Infrastructure:** konamo[.]xyz, raedom[.]store, securedrive.fin-tech[.]com, kida.plusdocs.kro[.]kr
- **Hosting**: South Korea, U.S.-based servers; IP traces lead to China and Vietnam

While malware and infrastructure provide strong clues, **linguistic forensics** clinch the link:

- Use of North Korean vocabulary (e.g., “래일” for “내일”, “지령” for “command”)
- Consistent phishing structure, recurring PowerShell patterns
- Code reuse aligned with historic BabyShark operations

Kimsuky’s ClickFix proves that even basic Windows features can become potent tools for psychological warfare in cyberspace. As this campaign shows, the weakest link remains human trust, exploited not just by malware, but by the victim’s actions.

RECOMMENDATIONS

1. EDR Deployment: Deploy Endpoint Detection and Response (EDR) tools to monitor unusual command-line activity and script behavior.

2. PowerShell Restrictions: Limit PowerShell execution to administrative users and enforce logging policies.

3. Security Awareness Training: Simulate phishing attacks using real-world tactics to build resistance to psychological manipulation campaigns like ClickFix.

4. Browser Hardening: Disable browser-based script execution and extensions that can abuse clipboard access.

REFERENCES

https://securityonline.info/clickfix-unmasked-how-north-koreas-kimsuky-group-turned-powershell-into-a-weapon-of-psychological-deception/

https://www.genians.co.kr/en/blog/threat_intelligence/suky-castle

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar
Kathmandu, Nepal
Phone: +977-01-4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com
Website: https://vairavtech.com

VAIRAV TECH
CYBER DEFENDER