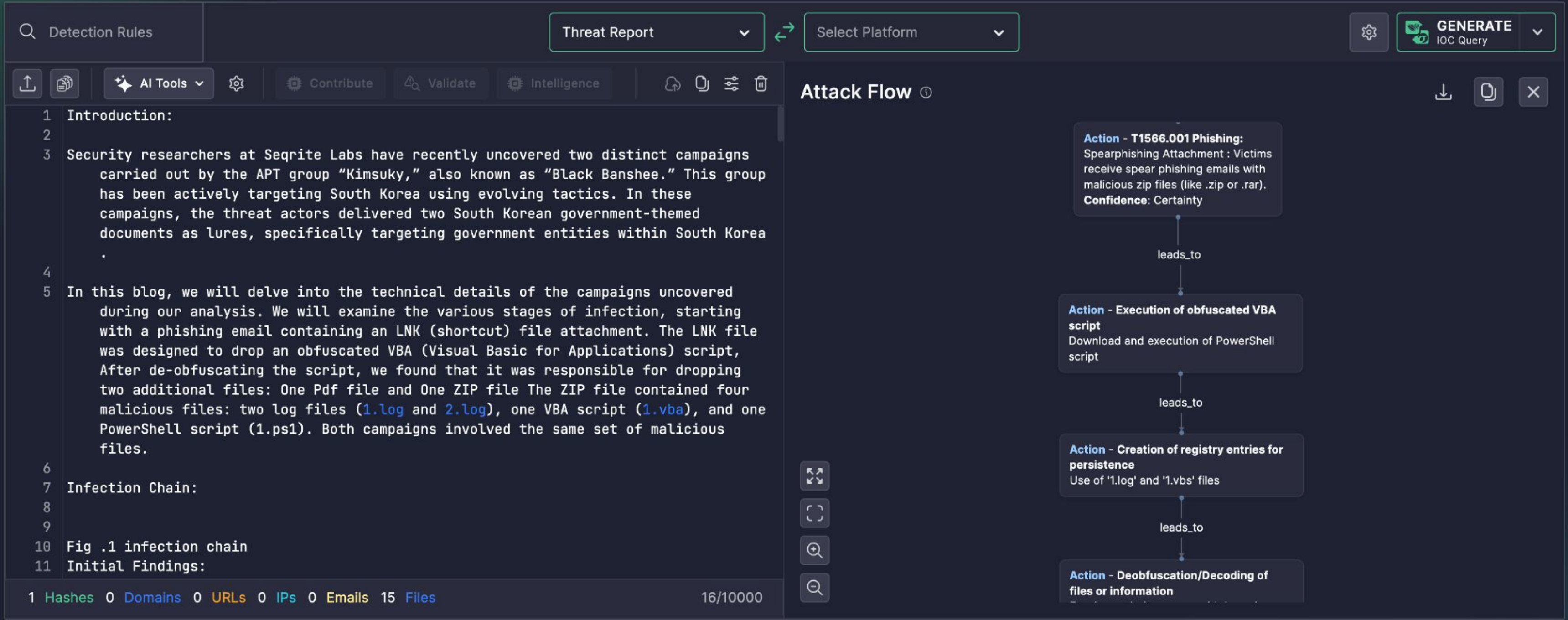
Attack Flow Generation with AI

Uncoder AI

Attack Flow Generation with AI

Released on April 16



Introduction:

Security researchers at Seqrite Labs have recently uncovered two distinct campaigns carried out by the APT group “Kimsuky,” also known as “Black Banshee.” This group has been actively targeting South Korea using evolving tactics. In these campaigns, the threat actors delivered two South Korean government-themed documents as lures, specifically targeting government entities within South Korea .

In this blog, we will delve into the technical details of the campaigns uncovered during our analysis. We will examine the various stages of infection, starting with a phishing email containing an LNK (shortcut) file attachment. The LNK file was designed to drop an obfuscated VBA (Visual Basic for Applications) script, After de-obfuscating the script, we found that it was responsible for dropping two additional files: One Pdf file and One ZIP file The ZIP file contained four malicious files: two log files (1.log and 2.log), one VBA script (1.vba), and one PowerShell script (1.ps1). Both campaigns involved the same set of malicious files.

Infection Chain:

Fig .1 infection chain
Initial Findings:

1 Hashes 0 Domains 0 URLs 0 IPs 0 Emails 15 Files 16/10000

Action - **T1566.001 Phishing: Spearphishing Attachment** : Victims receive spear phishing emails with malicious zip files (like .zip or .rar). **Confidence**: Certainty

leads_to

Action - **Execution of obfuscated VBA script**
Download and execution of PowerShell script

leads_to

Action - **Creation of registry entries for persistence**
Use of '1.log' and '1.vbs' files

leads_to

Action - **Deobfuscation/Decoding of files or information**

Attack Flow Generation with AI

Visualization can be a great help in understanding an attack. Uncoder AI analyzes the provided threat report of other description of malicious activities and visualizes it in the form of Attack Flow. For this purpose, Uncoder AI uses Llama 3.3 customized for detection engineering and threat intelligence processing, hosted at SOC Prime SOC 2 Type II private cloud for maximum security, privacy, and IP protection.

- Inspired by the open-source Attack Flow project to help defenders move from tracking individual adversary behaviors to tracking the sequences of behaviors that adversaries employ to move towards their goals
- Data doesn't leave SOC Prime's infrastructure
- Reduces the time to understand the attack. On average, generation takes about 2 minutes
- Visualized attack flows can directly inform detection rule logic by identifying TTP chains, enabling proactive defense without relying on IOCs
- When linked to existing telemetry or detection rules, it helps prioritize threats that map to known gaps or current alerts
- Machine-readable MMD export for easier integration with detection engineering workflows
- Gives engineers a visual depiction that aids communication with non-technical stakeholders, management, and executives