Contents

[**G0086 Stolen Pencil** 2](#_Toc179360210)

[**I. Introduction** 2](#_Toc179360211)

[**II. Tactics** 2](#_Toc179360212)

[**III. Techniques** 2](#_Toc179360213)

[**IV. Procedures** 3](#_Toc179360214)

[**V. Summary** 4](#_Toc179360215)

[**References** 6](#_Toc179360216)

## **G0086 Stolen Pencil**

## **I. Introduction**

Stolen Pencil, also known as Sharp Pencil or THALLIUM, is a North Korean-linked advanced persistent threat group that has been active since at least 2018. The group primarily focuses on academic institutions, specifically targeting individuals involved in research on North Korea, nuclear issues, and Korean unification. Their operations are characterized by a mix of cyber espionage and credential theft, with a particular emphasis on long-term intelligence gathering.

## **II. Tactics**

Stolen Pencil's tactical approach is characterized by

1. ***Targeted Phishing***

Heavy reliance on spear-phishing emails to gain initial access to target systems.

1. ***Credential Harvesting***

Strong focus on stealing login credentials for various services, particularly email accounts and academic resources.

1. ***Persistent Access***

Emphasis on maintaining long-term access to compromised accounts and systems for continuous intelligence gathering.

1. ***Social Engineering***

Use of sophisticated social engineering techniques to manipulate targets into compromising their security.

1. ***Low-sophistication Malware***

Deployment of relatively simple malware, often leveraging open-source tools.

## **III. Techniques**

This group uses a range of techniques in their operations

|  |  |
| --- | --- |
| Techniques | Descriptions |
| Spear-phishing Campaigns (T1566) | Use of tailored emails with malicious attachments or links, often mimicking academic communications or job offers. |
| Credential Phishing (T1566.002) | Development of convincing phishing pages mimicking legitimate login portals for academic institutions and email providers. |
| Remote Access Tools (RATs) | Deployment of custom and open-source remote access tools for system control and data exfiltration. |
| Keylogging (T1056.001) | Use of keyloggers to capture user credentials and other sensitive information. |
| Browser Extension Attacks | Deployment of malicious browser extensions to harvest data and maintain persistence |
| Command and Control (C2) Infrastructure | Use of compromised websites and legitimate cloud services for C2 communication (T1102.002). |
| Living off the Land (T1059) | Leveraging of legitimate system tools and PowerShell scripts for various malicious activities. |

## **IV. Procedures**

Stolen Pencil's typical attack chain follows this sequence

***1. Initial Access***

a. Highly targeted spear-phishing emails are sent to individuals in academic institutions.

b. Emails often contain links to credential phishing sites or malicious attachments.

***2. Credential Theft***

a. Victims are directed to convincing phishing pages that mimic legitimate login portals.

b. Stolen credentials are collected and used for further compromise.

***3. Execution and Persistence***

a. If malware is deployed, it's often a simple remote access tool or keylogger.

b. Persistence is established through methods like malicious browser extensions or scheduled tasks.

***4. Discovery***

a. The group conducts reconnaissance on compromised systems to identify valuable data and potential lateral movement paths.

***5. Lateral Movement:***

a. Stolen credentials are used to access other systems and accounts within the target institution.

***6. Collection and Exfiltration***

a. Sensitive documents, emails, and research data are identified and collected.

b. Data is exfiltrated, often through legitimate cloud services to avoid detection.

***7. Ongoing Operations***

a. Stolen Pencil maintains long-term access to compromised accounts for continuous intelligence gathering.

b. They regularly update their phishing sites and malware to evade detection.

## **V. Summary**

Stolen Pencil's operations offer a unique window into North Korea's cyber espionage priorities, particularly in the academic realm. Their targeting of researchers focused on North Korea, nuclear issues, and Korean unification clearly reflects the regime's strategic interests and information gathering priorities.

What's particularly interesting about Stolen Pencil is their approach to malware. Unlike other North Korean groups known for sophisticated tools, Stolen Pencil often opts for simpler, sometimes open-source solutions. This could be a deliberate tactic to avoid detection in academic settings where advanced malware might raise red flags. Their use of malicious browser extensions is a clever move, because it allows them to maintain a persistent presence and potentially bypass two-factor authentication. It shows that they understand their targets' work habits and environments.

The group's phishing campaigns demonstrate a deep grasp of academic culture, mimicking conference invitations or peer review requests. This level of social engineering, combined with their focus on long-term intelligence gathering, aligns with typical state-sponsored espionage patterns.

## **References**

1. Netscout Threat Intelligence. (2018). "STOLEN PENCIL Campaign Targets Academia." <https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia>

2. MITRE ATT&CK. (2024). "Stolen Pencil, G0086." <https://attack.mitre.org/groups/G0086/>