# Advisory

## Increased Activity of SectorJ04 Group

aeCERT
One of Telecommunications Regulatory Authority (TRA) Initiatives
P O Box 116688, Dubai, United Arab Emirates (UAE)
www.aecert.ae | www.tra.gov.ae

Version: 1.0
Ref: ADV-19-049
Document Date: 04/09/2019

# Document Details

## Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained within this report, aeCERT and the TRA bear no liability or responsibility for any recommendations issued or inadvertent damages that could be caused by the recipient of this information.

Accessing third-party links in this advisory will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced.

## Contents

# Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about the SectorJ04 hacker group targeting different institution and organizations by sending spam email. The email spoofs trusted sources like Microsoft Office. The attack allows for the installation of backdoors to access the system and steal the account information, or distribute malware and ransomware to restrict access to the victim's system using encryption. The SectorJ04 hacker group has recently increased phishing activity across Asia and use different types of malwares and backdoors.

---

# Details

The SectorJ04 hacker group use spear phishing email attack which is also an email spoofing attack and targeted type of phishing. The hacking methods for the SectorJ04 group have changed through the years. The initial spam email was mostly sent with no content or messages, but the most recent emails started to include information like accounting data, images, and a new type of malware and backdoor.

The SectorJ04 group uses signed malware by adding valid digital signature in their malware, which allows it to pass the user account control and evade antivirus protection. The hacker group designed their own backdoor named ServHelper and FlawedAmmy RAT acting as a remote desktop agent and remote access trojan downloader; this is difficult to detect as it does not show in the list of running programs in the system.
In addition, the backdoor installs an email stealer, used to collect information stored in the registry by mail client such as protocol information – like Simple Mail Transfer Protocol and Internet Access Message Protocol – and also collects the email account information like username and password. It will then send the information to the attacker's server. As a last

step, the malware runs a self-deleting batch file to limit the forensic evidence on the infected pc.

The two main types of backdoors used by the hacker group are AdroMut and FlowerPippi: AdroMut being used to download the ServHelper and FlawedAmmy RAT; and FlowerPippi to act as a downloader and collect information like proxy setting, OS version, and administrator rights.

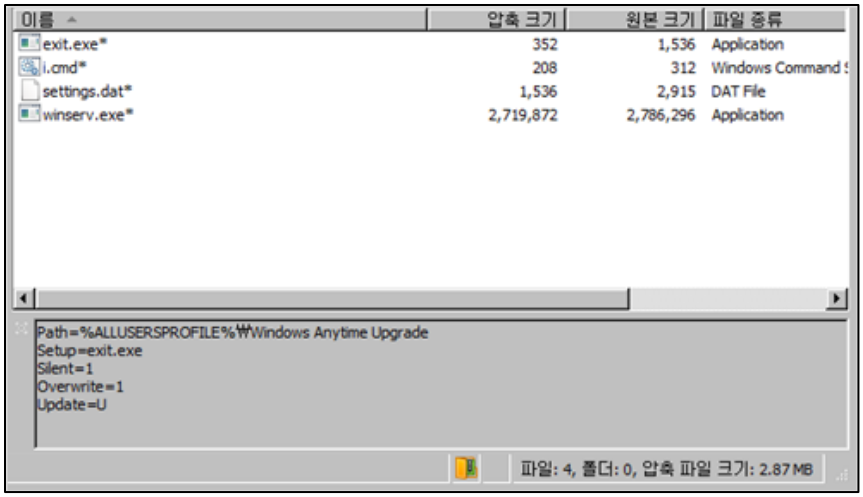
In 2019, the SectorJ04 hacker group started to expand and send spam emails to random companies. They have successfully hacked the Active Directory server by Microsoft and distributed the ransomware. The SectorJ04 hacker group used three types of malware attached in the malicious document.

The first type uses an encoded executable file: they used a Word or Excel file attached to the phishing email which downloads an MSI file using the hacker group server once the document run. The MSI file downloads the FlawedAmmy downloader and decodes it to install FlawedAmmy RAT to perform several functions such as using the attacker sever to decode encoded executable file downloader.

The second type use the MSI file in the malicious attachment to download an NSIS script to execute ServHelper to act as a backdoor.

The third type uses a self-extracting file downloaded by the MSI file. In addition, the file includes another self-extracting file that includes the RMS Remote Access Trojan. Each self-extracting file includes four files with the .exe extension.

The following figure shows that the second self-extracting file includes a file named “winserv.exe” which executes the RMS Remote Access Trojan with a DAT extension.




In June 2019, the SectorJ04 hacker group started to spread and send spam emails in different languages such as Arabic, Korean and Italian. The SectorJ04 group targeted governmental and financial institutions; the emails claim to be from Microsoft Office and include an HTML attachment or links to download malicious documents that install the backdoor.

---

# Indicators of Compromise

The list of indicators of compromise can be found by clicking here.

---

# Recommendations

**To avoid and mitigate the impact of an attack, we highly recommend the following:**

- Conduct awareness sessions for employees regarding phishing emails and fraud.
- Install a spam filter for emails and keep it up to date.
- Avoid clicking on malicious links or downloading suspicious files no matter how they seem legitimate or come from a legitimate source.
- Perform back-ups of your files frequently to an external drive to avoid having them encrypted.
- If your files are encrypted with a ransomware, always try to find a decryptor for it.
- Ensure that all systems are updated with the latest security patches.
- Report any suspicious emails/attachments to your IT/Security department.

---

# References

ThreatPost

Schneier on Security

ThreatRecon

---

# aeCERT Contact Info


P.O. Box 116688

Dubai, United Arab Emirates

Tel (+971) 4 777 4003

Fax (+971) 4 777 4100

Email incident[at]aeCERT.ae

Instagram @TheUAETRA

Twitter @TheUAETRA


For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to incident[at]aeCERT.ae