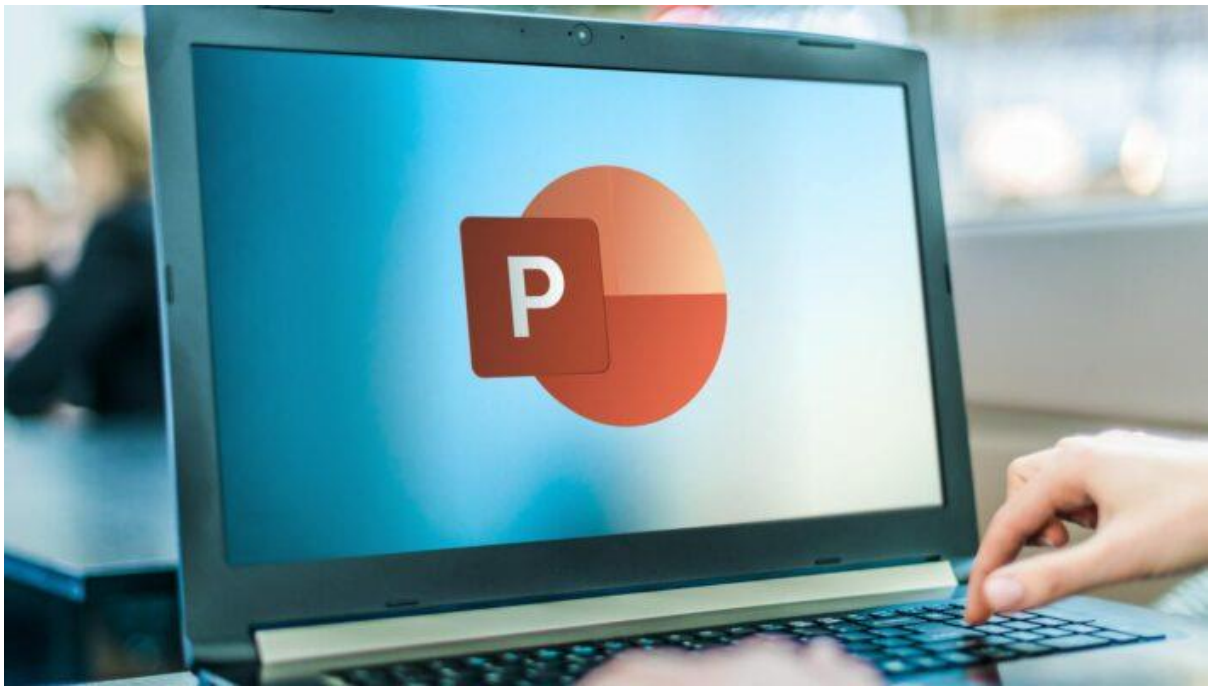
H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-14

POWERPOINT FILES FOR 'MOUSEOVER' MALWARE DELIVERY



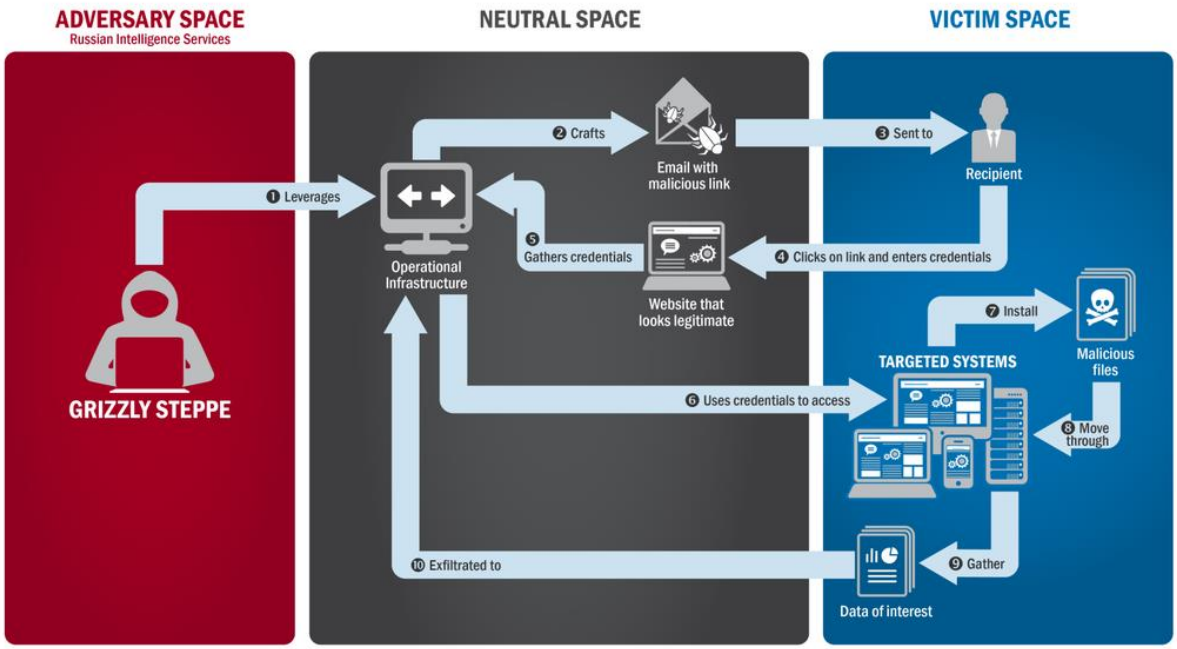
1. Background

Hackers believed to work for Russia have started using a new code execution technique that relies on mouse movement in Microsoft PowerPoint presentations to trigger a malicious PowerShell script. No malicious macro is necessary for the malicious code to execute and download the payload, for a more insidious attack. A report from threat intelligence company **Cluster25** says that **APT28** (a.k.a. 'Fancy Bear'), a threat group attributed to the Russian GRU (Main Intelligence Directorate of the Russian General Staff), have used the new technique to deliver the Graphite Malware.

The threat actor lures targets with a PowerPoint (.PPT) file allegedly linked to the Organization for Economic Co-operation and Development (OECD), an intergovernmental organization working towards stimulating economic progress and trade worldwide. Inside the PPT file there are two slides, both featuring instructions in English and French for using the Interpretation option in Zoom video-conferencing app. The PPT file contains a hyperlink that acts as a trigger for launching a malicious PowerShell script using the **SyncAppvPublishingServer** utility. This technique has been documented since June 2017. Multiple researchers explained at the time how the infection works without a malicious macro nested inside an Office.

Based on the metadata found, Cluster25 says that the threat actor targets entities in the defense and government sectors of countries in the European Union and Eastern Europe and believe that the espionage campaign is ongoing.

2. How the Graphite Malware works?



Graphite malware's purpose is to allow the attacker to load other malware into system memory.

When opening the lure document in presentation mode and the victim hovers the mouse over a hyperlink, a malicious PowerShell script is activated to download a JPEG file from a Microsoft OneDrive account. The JPEG is an encrypted DLL file (lmapi2.dll), that is decrypted and dropped in the 'C:\ProgramData\' directory, later executed via rundll32.exe. A registry key for persistence is also created for the DLL.

Next, lmapi2.dll fetches and decrypts a second JPEG file and loads it into memory, on a new thread previously created by the DLL. Cluster25 details that each of the strings in the newly fetched file requires a different XOR key for deobfuscation. The resulting payload is Graphite malware in portable executable (PE) form.

Graphite abuses the Microsoft Graph API and OneDrive to communicate with the command and control (C2) server. The threat actor accesses the service by using a fixed client ID to obtain a valid Authentication (**OAuth2)** token. Graphite then queries the Microsoft GraphAPIs for new commands by enumerating the child files in the check OneDrive subdirectory, the researchers explain.

If a new file is found, the content is downloaded and decrypted through an AES-256-CBC decryption algorithm, then the malware allows remote command execution by allocating a new region of memory and executing the received shellcode by calling a new dedicated thread.

3. Significant Attacks

a. Russian Military Intervention in Ukraine

According to CrowdStrike from 2014 to 2016, the group used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. They distributed an infected version of an Android app whose original purpose was to control targeting

data for the D-30 Howitzer artillery. The app, used by Ukrainian officers, was loaded with the X-Agent spyware and posted online on military forums. CrowdStrike initially claimed that more than 80% of Ukrainian D-30 Howitzers were destroyed in the war, the highest percentage loss of any artillery pieces in the army (a percentage that had never been previously reported and would mean the loss of nearly the entire arsenal of the biggest artillery piece of the Ukrainian Armed Forces.

b. International Olympic Committee

On January 10, 2018, the "Fancy Bears Hack Team" online persona leaked what appeared to be stolen International Olympic Committee (IOC) and U.S. Olympic Committee emails, dated from late 2016 to early 2017, were leaked in apparent retaliation for the IOC's banning of Russian athletes from the 2018 Winter Olympics as a sanction for Russia's systematic doping program. The attack resembles the earlier World Anti-Doping Agency (WADA) leaks. It is not known whether the emails are fully authentic, because of Fancy Bear's history of salting stolen emails with disinformation. The mode of attack was also not known, but was probably phishing.

c. Norwegian Parliament Attacks

In August 2020 the Norwegian Storting reported a significant cyberattack on their e-mail system. In September 2020, Norway's foreign minister, Ine Marie Eriksen Søreide, accused Russia of the attack. Norwegian Police Security Service concluded in December 2020 that "The analyses show that it is likely that the operation was carried out by the cyber actor referred to in open sources as APT28 and Fancy Bear," and that "sensitive content has been extracted from some of the affected email accounts."

4. Recommendations

Protect yourself from these kinds of malware delivery and execution, and other similar threats by following these tips:

a. **Application whitelisting** of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.

b. **Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with ‘extreme risk’ security vulnerabilities within 48 hours. Use the latest version of applications.

c. **Configure Microsoft Office Macro Settings** to block macros from the Internet, and only allow vetted macros either in ‘trusted locations’ with limited write access or digitally signed with a trusted certificate.

d. **User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

e. **Automated Dynamic Analysis of Email and Web Content** run in a sandbox, blocked if suspicious behavior is identified (e.g. network traffic, new or modified files, or other system configuration changes).

f. **Email Content Filtering**. Whitelist allowed attachment types (including in archives and nested archives). Analyze/sanitize hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.

g. **Web content filtering**. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.

h. **Deny Direct Internet connectivity.** Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.

i. **Operating System Generic Exploit Mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).

j. **Server Application Hardening** especially Internet-accessible web applications (sanitize input and use TLS not SSL) and databases, as well as applications that access important (sensitive/high-availability) data.

k. **Operating System Hardening** (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality (e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD).

l. **Control Removable Storage Media and Connected Devices**. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices.

m. **Block Spoofed Emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organization's domain.

n. **User Education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.

o. **Antivirus Software** with up-to-date signatures to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.

p. **TLS Encryption** between email servers to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://www.bleepingcomputer.com/news/security/hackers-use-powerpoint-files-for-mouseover-malware-delivery/*
- *https://www.zdnet.com/article/trellix-finds-onedrive-malware-campaign-targeting-govt-officials-in-western-asia/*
- *https://www.linkedin.com/pulse/mitigation-strategies-prevent-malware-delivery-vladimir-nikolov*
- *https://en.wikipedia.org/wiki/Fancy_Bear*