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

CYBERSECURITY BULLETIN 2026-02

Understanding the Risk of Malicious Screensaver Files (.SCR)

Overview

Cybercriminals continue to develop new methods to bypass security systems and gain unauthorized access to organizations. A recent cyber threat involves the misuse of Windows screensaver files, commonly known as ".SCR" files, to spread malware and gain remote control of computer systems.

What is Happening?

Attackers are sending emails that appear legitimate, such as requests to review invoices, reports, or project documents. These emails contain links that lead users to download a screensaver file.

Although screensaver files are normally used to display animations on idle computers, they can also function as executable programs. This means they can run hidden malicious commands when opened.

Once the file is executed, it installs software that allows attackers to remotely monitor and control the infected computer without the user's knowledge.

How the Attack Works

1. The victim receives a phishing email containing a business-related message.

2. The email includes a link to download a screensaver (.SCR) file from an external storage website.
3. The user downloads and opens the file, believing it is safe.
4. The file secretly installs remote access software.
5. The attacker gains long-term access to the computer system.
6. The attacker may then steal sensitive information, spread malware across the network, or deploy ransomware.

Why This Threat is Dangerous

Many users do not recognize screensaver files as executable programs. Because of this, these files may bypass security controls and user suspicion. Attackers also use legitimate remote management tools, making their activity harder to detect.

If successful, this attack may lead to:

- Unauthorized access to sensitive data
- Financial loss
- System disruption
- Network-wide malware infection

Warning Signs to Watch For

Personnel should remain cautious if they encounter:

- Unexpected emails requesting urgent document review
- Download links from unknown or external storage websites
- Attachments or files ending in .SCR
- Requests involving unusual urgency or pressure
- Emails from unfamiliar senders posing as legitimate contacts

Recommendations

In this regard, AFP personnel are advised to follow these protective measures:

- Avoid downloading files from unknown or unverified sources
- Treat screensaver (.SCR) files as potentially dangerous programs
- Verify suspicious emails through official communication channels
- Use only approved and authorized remote access or monitoring tools
- Report suspicious emails, downloads, or system behavior immediately to cybersecurity personnel
- Avoid accessing non-work-related file hosting services using official devices

If you believe you have downloaded or opened a suspicious file:

- Immediately disconnect the device from the internet or network
- Do not attempt to investigate or delete files on your own
- Report the incident to your cybersecurity or ICT office
- Follow incident reporting procedures and chain of command

Conclusion

Cyber threats continue to evolve by exploiting unfamiliar file types and trusted tools to deceive users and bypass security defenses. Awareness and vigilance remain the strongest defense against these attacks. Personnel must remain cautious when opening files or links, especially those received through email or messaging platforms. By following established cybersecurity procedures and verifying suspicious communications, organizations can significantly reduce the risk of compromise and protect critical information systems.

Source: https://www.darkreading.com/application-security/attackers-use-screensavers-drop-malware-rmm-tools