INCIDENT REPORT

Organization	IEEE
Service	MSS-BAS
Severity Level	High
Impact Level	High
Vulnerability Level	High

IMMEDIATE THREAT CYBER ASSESSMENT

Files containing any type of malware are a real and immediate threat to every organization. Our intelligence team continuously collects these types of immediate threats and tests your organization against these real world attacks as they emerge. This report includes the new public breaches and exploits that were found and can potentially be used by hackers. These types of files should be filtered or contained immediately as they are the hottest threats used by hackers and cybercrime organizations around the world.

Outlook SMB-RTF Vulnerability

During the current immediate threat assessment our platform sent 4 emails containing the immediate threat in a number of variations and concealment levels. The results are divided into Direct and Indirect exposure.

Direct exposure: When an email containing the unconcealed immediate threat file manages to penetrate without being disarmed or modified.

Indirect exposure: When an email containing a concealed immediate threat file manages to penetrate without being disarmed or modified.

No exposure: When none of the emails containing the immediate threat manages to penetrate.

Simulation Summary

Risk Level	Sent	Penetrated
High	1	1
Medium	0	0
Low	3	3

Total Assessment: 4 / 4

DESCRIPTION

A remote attacker can exploit this vulnerability by sending an email containing an RTF file to a target victim. The RTF file contains a remotely hosted image file (OLE object) that is downloaded from the attacker-controlled SMB server. By tricking victims to preview the email with Microsoft Outlook, attackers could steal sensitive information, including users' Windows login credentials, without requiring any additional user interaction. Since MS Outlook will render the OLE content, it will initiate an automatic authentication procedure with the attacker's controlled remote server over SMB protocol using single sign-on (SSO), handing over the victim's username and NTLMv2 hashed version of the password. This could potentially allow the attacker to gain access to the victim's system.

RECOMMENDATION

The best thing one could do against this type of attack is not letting it through; it's always best to prevent it. Preventive/remediation measures include:

1. Apply the Microsoft update for CVE-2018-0950, if you have not yet (see MS updates in the following link: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/**CVE-2018-0950**). This will prevent automatically previewing the content of an email in MS Outlook.
2. Block the following ports: 445/tcp, 137/tcp, 139/tcp, along with 137/udp and 139/udp; used for incoming and outgoing **SMB sessions**.
3. Block NT LAN Manager (NTLM) Single Sign-on (SSO) authentication.
4. Educate users to be watchful and avoid downloading software from unknown sources. We recommend complementing this with the GLESEC MSS-BAS Phishing Vector.
5. Always use complex passwords that cannot be cracked easily even if their hashes are stolen. There exist a variety of Privilege Identity Manager (PIM) solutions for this, that are used to make sure credentials for regular and privilege users are always in compliance with company standards as an automatic process.
6. Keep the antivirus updated, this can help and it is one of the best practices in cyber security. This is however a necessary **but not sufficient condition.** We recommend that you utilize other non-signature based forensic and remediation technologies, preferably of low false-positives.
7. Erase the malware in case a user downloads it. Be aware that malware applications create a number of additional files; these also have to be eliminated.

For more information contact the GLESEC OPERATIONS CENTER.