BREACH ATTACK SIMULATION
IMMEDIATE THREAT REPORT

Institute of Electrical and Electronics Engineers

June 2018

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

Table of Contents

GLESEC
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

About This Report

This report is a companion to the Monthly Operations & Intelligence Reports and is prepared once we receive notification that there is an "Immediate Threat". For more information you can review the dashboards of the GMP or if necessary contact us at the GLESEC Operation Centers (GOC).

Confidentiality

GLESEC considers the confidentiality of client's information as a trade secret. The information in this context is classified as:

- Client name and contact information
- System architecture, configuration, access methods and access control
- Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

GLESEC
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

BREACH ATTACK SIMULATION - IMMEDIATE THREAT REPORT

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.

MSS-BAS (e-mail vector)

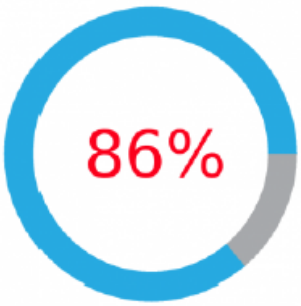
GLESEC carried out, as part of the MSS-BAS service contracted by your organization, a simulation with the latest threats located in the DeepWeb to-date.

7 tests were run in this simulation, of which, 6 were able to penetrate your organization's defenses. This simulation is based on the Adobe Flash player and Excel vulnerability CVE-2018-5002. The vulnerability uses .xls files as the way to execute remote code in the victim's computer.

Simulation Summary

Risk Level	Sent	Penetrated
High	1	0
Medium	0	0
Low	6	6

Total Assessment: 6 / 7



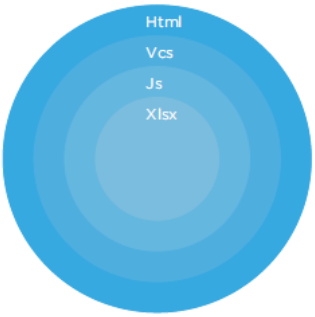
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

DESCRIPTION

The vulnerability exploit begins with a social engineering campaign online, with the theme of a salary adjustment. Users are prompted to download an excel file with information regarding the salary adjustment, once opened using a lesser known feature of executing Flash code in Office files, a SWF file is retrieved from the attacker's server, the transmission of this file is protected using an RSA+AES cryptosystem to protect the data payload and the symmetric key that decrypts the data payload. In this stage, the vulnerability has been exploited, due to the fact that despite the attachment appears as an xls file, the code is executed within a Flash container. The second stage of the threat occurs after the exploitation, the SVG downloaded, uses the same RSA+AES cryptosystem to download the final payload at the attacker's C&C server, which contains a shellcode that opens a backdoor in the victim's computer.

FILE STRUCTURE THAT WAS ABLE TO PENETRATE

Attack Name: Adobeflashplayerexcel(cve-2018-5002)XlsxJsVcsHtmlscript
Medium Risk
Indirect Vulnerability



A VCS file is a type of file contains information about an event or appointment, which can be imported into a calendar or scheduling program; saved in the vCalendar "Electronic Calendaring and Scheduling Exchange" format; includes the event date and time and other information about the event. Embedded within this one a VBS file is added which is a Virtual Basic script written in the VBScript scripting language; contains code that can be executed within Windows or Internet Explorer

via the Windows-based script host (Wscript.exe); may also use the .VB file extension. This VBS files executes another BAT file that basically can execute commands with the Windows Command Prompt (cmd.exe). It contains a series of line commands that typically might be entered at the DOS command prompt. BAT files are most commonly used to start programs and run maintenance utilities within Windows. To finally execute the malicious payload which was embedded within a IQY file that ultimately infects the device.

RECOMMENDATION

The best thing can be done against this type of attack is not letting it execute the payload and delete it immediately.

Preventive/remediation measures include:

1. Block/disable external content in Microsoft Office Excel. This can be done by following the next steps:
    a. In Excel, click the File tab.
    b. Click Options > Trust Center > Trust Center Settings, and then click External Content.
    c. Click the option that you want under Security settings for Data Connections:
        i. **Disable all Data Connections**.
        ii. Enable all Data Connections (not recommended).
        iii. Prompt user about Data Connections (not recommended).
2. Set attached files to open in protected view to stop any possibility of external content accidentally running. This can be done by following the next steps:
    a. In Word, **Excel** and/or PowerPoint click the File tab.
    b. Click Options > Trust Center > Trust Center Settings > Protected View > select the options:
    c. ✓ Enable **Protected View** for **Outlook attachments**
    d. ✓ Enable **Protected View** for files originating from the internet
    e. ✓ Enable **Protected View** for files located in **potentially unsafe** locations
3. Block “people.dohabayt.com” and “185.145.128.57” There are many ways this can be performed, depending on your Network Infrastructure. Most

commonly, one outbound and inbound Firewall **deny** rule can be added to and from this domain through ports 80 and 443.

4. Block/prevent from running all files listed on next section. This can be done using an antimalware tool or service with the capability to isolate and block/delete files that correspond to a specific hash value. Using Symantec Endpoint Protection, for example, the following steps are required:
    a. In Symantec Endpoint Protection Manager (SEPM), click Policies.
    b. Click Application and Device Control.
    c. Create a new Application and Device Control policy, or use an existing policy.
    d. Click your selected policy to edit it.
    e. Click Application Control.
    f. Click Add.
    g. Next to Apply this rule to the following processes, click Add.
    h. In the Process name to match field, type an asterisk (*).
    i. Click OK.
    j. Under Rules in the bottom left, click Add.
    k. Click Add Condition.
    l. Click Launch Process Attempts.
    m. Next to Apply to the following processes, click Add.
    n. In the lower right, click Options.
    o. Select Match the file fingerprint.
    p. Copy the **MD5** hash into the field for the fingerprint.
    q. Click OK.
    r. Click the Actions tab.
    s. Block: **Choose "Block Access."** You can enable logging under this option as well.
    t. Click OK.
    u. Ensure that the new rule is enabled and is set for production (test only logs) when you are ready to use it.
    v. Click OK.
    w. Click Yes to assign the policy.
    x. Check any client group to which the policy should apply.
    y. Click OK.
5. 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. *Contact us at GLESEC for more information on this.*

6. Execute and maintain a periodically data backup schedule.
7. Erase the malware in case a user downloads it. Be aware that malware applications create a number of additional files. All of these have to be eliminated. *Contact us at GLESEC for more information on this.*
8. Educate users to be watchful and avoid downloading software from unknown sources. *We recommend complementing this with the GLESEC MSS-BAS Phishing Vector.*

Block the following malicious file:

- Malicious Files:
  - SHA-256: **0b4f0d8d57fd1cb9b4408013aa7fe5986339ce66ad09c941e76626b5d872e0b5**
  - MD5: **c8aaaa517277fb0dbb4bbf724245e663**
  - File name: **basic_salary.xlsx**
  - File size: 85.25 KB
  - Last analysis: 2018-06-13 03:22:17 UTC

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com