www.glesec.com
GLESEC

BREACH ATTACK SIMULATION IMMEDIATE THREAT REPORT

Institute of Electrical and Electronics Engineers

May 2018

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

Info@glesec.com
www.glesec.com

Table of Contents

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.

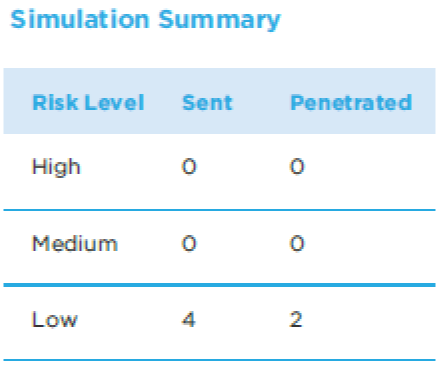
BREACH ATTACK SIMULATION - IMMEDIATE THREAT REPORT

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)

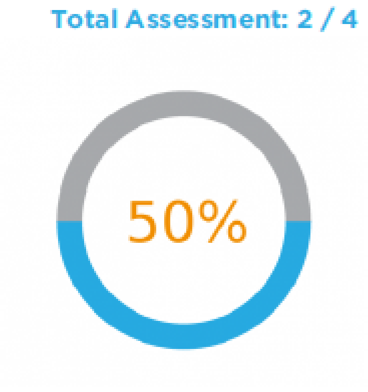
GLESEC carried out, as part of the MSS-BAS service contracted by your organization, a simulation with the latest threats located in the DeepWeb to-date.

As a result of the 4 types of tests of this simulation we found that 2 was able to successfully penetrate your organization's defenses. This test is associated with extension (.IQY), this type of file contains a URL and other parameters for making a query over the Internet. They can be opened with Microsoft Excel.



Simulation Summary

Risk Level	Sent	Penetrated
High	0	0
Medium	0	0
Low	4	2

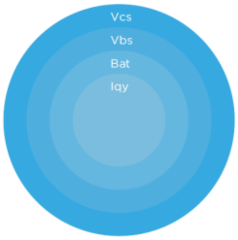


DESCRIPTION

The IQY attack starts off with a phishing email spread by the Necurs botnet with the subject of "Unpaid invoice [random numbered]" pretending to come from random names at the victim's email domain. This email contains an IQY file attachment, which eventually after a series of actions in the download chain delivers the "Flawed Ammy" Remote Access Trojan. IQY is basically a simple text file with a url that when opened in Excel, will download the payload at the attacker's C&C. Since this IQY file has no malicious content it will bypass all antiviruses. The "Flawed Ammy" trojan is aimed to steal user's sensitive information including but not limited to financial details, user credentials + passwords for email and social media accounts.

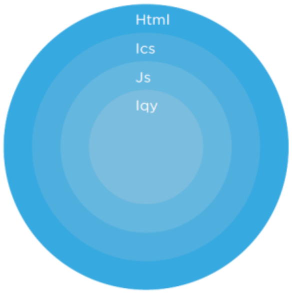
FILE STRUCTURE THAT WAS ABLE TO PENETRATE

Attack Name: IqyexcelwebqueryIqyBatVbsVcs
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.

Attack Name: IqyexcelwebqueryIqyJsIcsHtmlscript
Medium Risk
Indirect Vulnerability



A HTML file is a type of file that is coded in HTML that can be displayed in a web browser. It is used to format text, tables, images, and other content that is displayed on a webpage. HTML files are widely used on the web as most pages within static websites have an ".html" extension. From this one, an ICS file is referenced, which is a calendar file saved in a universal calendar format used by several email and calendar programs, including Microsoft Outlook, Google Calendar, and Apple Calendar. It enables users to publish and share calendar information on the web and over email. ICS files are often used for sending meeting requests to other users, who can import the events into their own calendars. This ICS file is used to execute JavaScript instructions in web pages which finally starts the IQY file with the malicious payload.

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 “http://clodflarechk.com/” domain. 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 known malicious files such as:

- ❖ Malicious Files:
  - o SHA-256: **05660c8d652fb9df8dab6a5705e3e2243b215ad5354000961feaebc07ed89ad9**
  - o MD5: **3a86ffce06d029730ad89cb233079d64**
  - o File name: **2.dat**
  - o File size: 170 B
  - o Last analysis: 2018-05-28 18:40:50 UTC
- ❖ Malicious File:
  - o SHA-256**:** **ebce76b8efff3a0568aa2b07d5fba8f21fe3dd6f56bfad0a77194a494b634079**
  - o MD5: **08bb85f5bff52d2605ddd8a19a5465fd**
  - o File name: **1.dat**
  - o File size: 309 B
  - o Last analysis: 2018-05-30 08:11:13 UTC

- Malicious File:
  - SHA-256 **f4b6b0c8787ea344ce9f68f5d506a5d6cc7447114b3dcdbb6d0207372054dfe2**
  - MD5: **172bc98dbe0f6c4ac59857c071cd8673**
  - File name: **data.xls**
  - File size: 123.5 KB
  - Last analysis: 2018-05-30 08:15:35 UTC

- Malicious File:
  - SHA-256: **bab69fb29c167451608f0840ede9dfb4c3c52fa0da5f38089ac7f2afbd94d867**
  - MD5: **418aa2d43b1e4a841d4769463b12fa3b**
  - File name: **dSNNRdBKAWSo.exe**
  - File size: 644 KB
  - Last analysis: 2018-05-30 12:45:10 UTC

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

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

Info@glesec.com
www.glesec.com