Mateusz Łąpieś ([mateusz.lapies@student.pk.edu.pl](mailto:mateusz.lapies@student.pk.edu.pl))

## Sprawozdanie – lab3

1. **What is the time of the first detected NIDS alert in Kibana?**January 27th 2017, 22:54:43.000  
   **What is the source IP address in the alert?**  
   172.16.4.193  
   **What is the destination IP address in the alert?**194.87.234.129  
   **What is the destination port in the alert? What service is this?**80, http  
   **What is the classification of the alert?**  
   High  
   **What is the destination geo country name?**Russia  
   **What is the malware family for this event?**Exploit\_Kit\_RIG  
   **What is the severity of the exploit?**  
   Major  
   **What is an Exploit Kit? (EK) Search on the internet to answer this question.**  
   An exploit kit or exploit pack is a type of toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities.  
   **What website did the user intend to connect to?**  
   <http://homeimprovement.com/remodeling-your-kitchen-cabinets.html>  
   **What URL did the browser refer the user to?**  
   tyu.benme.com  
   **What kind of content is requested by the source host from tybenme.com? Why could this be a problem? Look in the DST server block of the transcript too.**Zapytanie określa, że będzie akceptowane text/html, application/xhtml+xml, \*/\*  
   Natomiast odpowiedź zawiera typ text/html;charset=UTF-8  
   Stąd mogą być problemy ze specjalnymi znakami.  
   **What are some of the websites that are listed?  
   Obraz zawierający tekst, zrzut ekranu, ekran

   Opis wygenerowany automatycznie  
   Which of these sites is likely part of the exploit campaign?**tyu.benme.com  
   api.blockcypher.com  
   p27dokhpz2n7nvgr.1jw2lx.top  
   **What are the HTTP - MIME Types listed in the Tag Cloud?  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie**
2. **According to the IDS signature rule which malware family triggered this alert? You may need to scroll through the alert signature to find this entry.**PseudoDarkLeech  
   **According to the Event Messages in Sguil what exploit kit (EK) is involved in this attack?**trojan-activity **Beyond labelling the attack as trojan activity, what other information is provided regarding the type and name of the malware involved?  
     
   By your best estimate looking at the alerts so far, what is the basic vector of this attack? How did the attack take place?  
     
   What are the referer and host websites that are involved in the first SRC event? What do you think the user did to generate this alert?**Obraz zawierający tekst

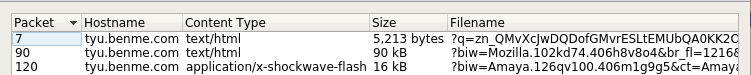
   Opis wygenerowany automatycznieUżytkownik prawdopodobnie wyszukał hasło w przeglądarce bing i otworzył stronę podaną w Host, która zawierała iframe.  
   **What kind of request was involved?**  
   Typ: GET  
   **Were any files requested?**  
   /engine/classes/**dle\_js.js  
   What is the URL for the referer and the host website?**Obraz zawierający tekst

   Opis wygenerowany automatycznie **How the content encoded?**gzip, deflate  
   **How many requests and responses were involved in this alert?**3  
   **What was the first request? Who was the referrer? Who was the host server request to?**Obraz zawierający tekst

   Opis wygenerowany automatycznie **Was the response encoded?**gzip  
   **What was the second request?** **Who was the host server request to? Was the response encoded?**Obraz zawierający tekst

   Opis wygenerowany automatycznie **What was the third request? Who was the referrer? What was the Content-Type of the third response? Type your answers here. What were the first 3 characters of the data in the response? The data starts after the last DST: entry.**Obraz zawierający tekst

   Opis wygenerowany automatycznie **What type of file was downloaded? What application uses this type of file?**Adobe Flash .swf  
   **How many files are there and what is the file types?**3 pliki, 2 html, 1 swf
3. **What website directed the user to the www.homeimprovement.com website?**bing.com  
   **What is the http request for? What is the host server?  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   What did VirusTotal tell you about this file?**Plik jest uznany za niebezpieczny.  
   **Are there any similarities to the earlier alerts?**Zapytania mają taką samą strukturę GET, POST, GET **Are the files similar? Do you see any differences?**Pliki również przypominają te z poprzedniego ataku  
   ****  
   **Is this the same malware that was downloaded in the previous HTTP session?**Tak  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
     
   **Why do they seem to be post-infection?** **What is interesting about first alert in the last 4 alerts in the series? What type of communication is taking place in the second and third alerts in the series and what makes it suspicious?**Pierwszy z czterech alertów zawiera połączenie UDP, kolejne dwa ma zapytania DNS, w obu przypadkach nie przypomina to zapytań w czasie próby infekcji. Ostatni zawiera połączenia TCP oraz http, które nawiązują do iframów, które zapewne są wstrzykiwane do stron, które odwiedza użytkownik.  
   **Go to virustotal.com and do a URL search for the .top domain used in the attack. What is the result?**  
   **Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   What are the filenames if any?**Jedynie plik html – EE7E-AD39-7D8C-080C-18BF%3fiframe&\_=1485557725652
4. **Can you find the two places in the webpage that are part of the drive-by attack that started the exploit?  
     
   What does the file do?** **How does the code in the javascript file attempt to avoid detection?**Skrypt dodaje do otwartego dokumentu iframe, który otwiera link do niebezpiecznej domeny, prawdopodobnie pobiera w ten sposób plik, który dokonuje infekcji.  
   **What kind of file it is?  
     
   What are some interesting things about the iframe? Does it call anything?  
     
   What does the start() function do?  
     
   What do you think the purpose of the getBrowser() function is?**