f**SOC Incident Report Team 2**

# Executive Summary

On **January 27, 2017**, Security Onion sensors detected suspicious web traffic associated with an exploit kit. Investigation confirmed the presence of the **RIG Exploit Kit** delivering **Cerber**

**ransomware** via a **drive-by download** attack. The infection chain originated from a

**compromised legitimate site** (homeimprovement.com) and redirected the user to malicious infrastructure, ultimately leading to ransomware execution.

This attack demonstrates a **multi-stage web exploitation flow** (Redirector → Exploit Kit → Flash exploit → Ransomware payload). The compromise lasted less than one minute but could have resulted in complete data encryption.

# Technical Findings

### Timeline

* + **Start:** 22:54:42
  + **End:** 22:55:28
  + **Duration:** < 1 minute.

### Attack Vector

* + User searched on **Bing** → clicked [www.homeimprovement.com.](http://www.homeimprovement.com/)
  + Site contained injected **JavaScript (dle\_js.js)** and hidden **iframe** → redirected to malicious host.
  + **RIG EK** delivered a **malicious Adobe Flash (SWF)** file.
  + Flash exploit executed → **Cerber ransomware** downloaded.

### Malware

* + **Exploit Kit:** RIG EK
  + **Malware family:** Cerber
  + **Delivery method:** Drive-by download via PseudoDarkLeech redirector.
  + **Files:** dle\_js.js, malicious SWF (signature CWS), Cerber payload.

# Indicators of Compromise (IOCs)

### Type Value

Malicious host retrotip.visionurbana.com.ve (139.59.160.143) Redirect server tyu.benme.com (194.87.234.129)

Check-in server 90.2.10.0

Cerber portal p27dokhpz2n7nvgr.1jjw2lx.top (198.105.151.50)

Referrer [www.homeimprovement.com/remodeling-your-kitchen-cabinets.html](http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html) Requested file dle\_js.js

Payload signature CWS → .swf (Adobe Flash) Exploit kit RIG EK

Malware Cerber ransomware

# Impact Assessment (specific to this lab)

* + **Data loss risk:** Cerber ransomware encrypts user files and demands ransom payment, making local data unusable.
  + **Business continuity:** Even though this was a lab case, a real infection could stop operations until backups are restored.
  + **Lateral movement risk:** Low – Cerber does not spread automatically, but multiple users could be infected if they visit the compromised site.
  + **Reputation:** Public exposure of employees clicking malicious links may harm organizational trust.
  + **Security posture gap:** The infection exploited **unpatched Adobe Flash**, highlighting outdated software risks.

# Recommendations (tailored to the lab)

1. **Patch Browsers & Plugins** – Disable/remove Adobe Flash (used by RIG EK). Apply latest browser and OS updates.
2. **Web Filtering** – Block access to known malicious domains (.top TLD, visionurbana.com.ve, tyu.benme.com).
3. **IDS/IPS Signatures** – Ensure detection rules for RIG EK and Cerber are up to date.
4. **Endpoint Protection** – Deploy anti-ransomware modules capable of blocking Cerber-like behavior.
5. **Backup Policy** – Maintain frequent ofline/immutable backups to mitigate ransomware impact.
6. **User Awareness** – Train employees to recognize suspicious redirects and avoid unsafe downloads.
7. **Threat Hunting** – Regularly review logs in Security Onion for EK-style patterns (redirects, SWF files, unusual DNS queries).

# Conclusion

**In conclusion**, this incident demonstrates the complexity and multi- stage nature of drive-by download attacks using exploit kits like RIG EK. Although this scenario was performed in a controlled lab environment, it highlights how quickly a user can become compromised through

malicious redirects and outdated plugins such as Adobe Flash. Effective mitigation requires a combination of timely patching, robust endpoint protection, proactive threat hunting, web filtering, and continuous user

awareness training. Adhering to these measures can significantly reduce the risk of malware infections and protect organizational assets from ransomware threats.

# Appendix – Lab Questions & Answers

## Part 1 – Kibana Investigation

**Q1: What is the time of the first detected NIDS alert in Kibana? A1:** Jan 27, 2017 - 22:54:43

**Q2: What is the source IP address in the alert? A2:** 172.16.4.193

**Q3: What is the destination IP address in the alert? A3:** 194.87.234.129

**Q4: What is the destination port in the alert? What service is this? A4:** 80, HTTP

**Q5: What is the classification of the alert? A5:** Trojan Activity

### Q6: What is the destination geo country name? A6: Russia

**Q7: What is the malware family for this event? A7:** Exploit\_Kit\_RIG

**Q8: What is the severity of the exploit? A8:** The signature severity is Major.

### Q9: What is an Exploit Kit (EK)?

**A9:** An Exploit Kit is an exploit that uses multiple websites and redirects to infect a computer with malware.

Exploit kits frequently use a drive-by attack to begin the campaign. In a drive-by attack, a user visits a website that appears safe, but attackers exploit vulnerabilities on the webserver to insert malicious HTML/JavaScript, often through an iFrame. This iFrame redirects the browser to malicious sites or downloads malware.

**Q10: What website did the user intend to connect to? A10:** [www.homeimprovement.com](http://www.homeimprovement.com/)

### Q11: What URL did the browser refer the user to? A11: ty.benme.com

**Q12: What kind of content is requested by the source host from ty.benme.com? Why could this be a problem?**

**A12:** The content is gzip. This could be a malware file requested for download. Because it is compressed, the contents are obfuscated, making it difficult to see what is inside.

### Q13: What are some of the websites that are listed in the HTTP - Sites section? A13:

* [www.bing.com](http://www.bing.com/)
* p27dokhpz2n7nvgr.1jw2lx.top
* homeimprovement.com
* tyu.benme.com
* [www.google-analytics.com](http://www.google-analytics.com/)
* api.blockcipher.com
* spotsbill.com
* fpdownload2.macromedia.com
* retrotip.visionurbana.com.ve

### Q14: Which of these sites is likely part of the exploit campaign? A14:

* p27dokhpz2n7nvgr.1jw2lx.top
* homeimprovement.com
* tyu.benme.com
* spotsbill.com
* retrotip.visionurbana.com.ve

### Q15: What are the HTTP - MIME Types listed in the Tag Cloud?

**A15:** *(not provided in your text – you want me to fill this in from lab analysis or leave blank?)*

## Part 2 – Investigate the Exploit with Sguil

### Q1: According to Sguil, what are the timestamps for the first and last of the alerts that occurred within about a second of each other?

**A1:** 22:54:42 to 22:55:28. The entire exploit occurred in less than a minute.

**Q2: According to the IDS signature rule which malware family triggered this alert? A2:** Malware\_family PseudoDarkLeech

### Q3: According to the Event Messages in Sguil what exploit kit (EK) is involved in this attack? A3: RIG EK Exploit

**Q4: Beyond labelling the attack as trojan activity, what other information is provided regarding the type and name of the malware involved?**

**A4:** Ransomware, Cerber

### Q5: By your best estimate looking at the alerts so far, what is the basic vector of this attack? How did the attack take place?

**A5:** The attack seems to have taken place by visiting a malicious web page.

### Q6: 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?

**A6:** The user issued a search on Bing with the terms *“home improvement remodeling your kitchen.”* The user clicked the [www.homeimprovement.com](http://www.homeimprovement.com/) link and visited that site.

**Q7: What kind of request was involved? A7:** HTTP/1.1 GET request

**Q8: Were any files requested? A8:** dle\_js.js

### Q9: What is the URL for the referer and the host website? A9:

* Referer: [www.homeimprovement.com/remodeling-your-kitchen-cabinets.html](http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html)
* Host: retrotip.visionbura.com.ve

### Q10: How was the content encoded? A10: gzip

**Q11: How many requests and responses were involved in this alert? A11:** 3 requests and 3 responses

### Q12: What was the first request?

**A12:** GET /?ct=Vivaldi&biw=Vivaldi.95ec

### Q13: Who was the referrer?

**A13:** [www.homeimprovement.com/remodeling-your-kitchen-cabinets.html](http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html)

**Q14: Who was the host server request to? A14:** tyu.benme.com

### Q15: Was the response encoded? A15: Yes, gzip

**Q16: What was the second request? A16:** POST /?oq=CEh3h8…. Vivaldi

**Q17: Who was the host server request to? A17:** tyu.benme.com

### Q18: Was the response encoded? A18: Yes, gzip

**Q19: What was the third request? A19:** GET /?biw=SeaMonkey.105….

### Q20: Who was the referrer?

**A20:** <http://tyu.benme.com/?biw>...

**Q21: What was the Content-Type of the third response? A21:** application/x-shockwave-flash

### Q22: What were the first 3 characters of the data in the response? A22: CWS

**Q23: What type of file was downloaded? What application uses this type of file? A23:** swf file, used by Adobe Flash

### Q24: How many files are there and what are the file types?

**A24:** There are three files. Two are .html files and one is a .swf file.

## Part 3: Use Wireshark to Investigate an Attack

### Q1: What website directed the user to the [www.homeimprovement.com](http://www.homeimprovement.com/) website? A1: Bing

**Q2: What is the HTTP request for?**

**A2:** A JavaScript file that is named *dle\_js.js*

### Q3: What is the host server?

**A3:** retrotip.visionurbana.com.ve

### Q4: What did VirusTotal tell you about this file?

**A4:** From the response, you can verify that the SWF is part of the RigEK exploit kit. 32 of 55 antivirus programs have rules that identify this hash as coming from a malware file.

### Q5: Are there any similarities to the earlier alerts?

**A5:** Yes, the alerts show GET, POST, and GET requests to *tyu.benme.com*.

### Q6: Are the files similar? Do you see any differences?

**A6:** Yes, two text/html files and a flash file. The file names are different.

**Q7: Is this the same malware that was downloaded in the previous HTTP session? A7:** Yes. The two hashes match even though the filenames are different.

### Q8: Why do they seem to be post-infection?

**A8:** All four alerts concern communication with the malware server.

**Q9: What is interesting about first alert in the last 4 alerts in the series? A9:** It sends a UDP code to a ransomware check-in server.

### Q10: What type of communication is taking place in the second and third alerts in the series and what makes it suspicious?

**A10:** They are DNS requests initiated from the local host; however, it is unlikely that they are the result of normal user activity. They must be sent by the malware file. The *.top* domain does not look like a valid domain name.

**Q11: What is the result of the URL search for the .top domain in VirusTotal? A11:** It is a malicious domain, that still triggers alerts.

**Q12: What are the filenames if any (last alert in the series)? A12:** Yes. EE7EA-D39….

## Part 4 – Examine Exploit Artifacts

### Q1: Can you find the two places in the webpage that are part of the drive-by attack that started the exploit?

**A1:**

* The script tag in the header loads the JavaScript file *dle\_js.js* from

### retrotip.visionurbana.com.ve.

* The iframe that loads content from **tyu.benme.com** is defined in the HTML body.

### Q2: What does the file (dle\_js.js) do?

**A2:** The JavaScript document.write() writes content to the webpage, creating an iframe that takes the user to a URI at **tyu.benme.com**.

**Q3: How does the code in the JavaScript file attempt to avoid detection? A3:** By splitting the end iframe tag into two pieces: </ifr' + 'ame>.

**Q4: What kind of file is the text/html file with *Vivaldi* in the filename? A4:** An HTML webpage.

**Q5: What are some interesting things about the iframe? Does it call anything? A5:** It is hidden. It calls a start() function.

### Q6: What does the start() function do?

**A6:** It writes to the browser window. It creates an HTML form and submits the variable NormalURL through POST. The NormalURL variable equals a URI at **tyu.benme.com**.

### Q7: What do you think the purpose of the getBrowser() function is?

**A7:** The getBrowser() function determines the type of browser that the webpage is displayed in.

### Q8: The EK used a number of websites. Complete the table below.

**URL IP Address Function**

[www.bing.com](http://www.bing.com/) N/A Search engine links to legitimate webpage [www.homeimprovement.com](http://www.homeimprovement.com/) 104.28.18.74 Malicious iFrame redirects to malicious site retrotip.visionurbana.com.ve 139.59.160.143 Executes malicious JavaScript

tyu.benme.com 194.87.234.129

Delivers malicious Adobe Flash file, exploit landing page

n/a 90.2.10.0 Cerber ransomware check-in server p27dokhpz2n7nvgr.1jjw2lx.top 198.105.151.50 Cerber ransomware page

### Q9: It is useful to “tell the story” of an exploit to understand what happened and how it works. Start with the user searching the internet with Bing.

**A9:**

The user searches with Bing for information on home improvements and clicks a link to [**www.homeimprovement.com**](http://www.homeimprovement.com/). This website has been compromised by a threat actor. A malicious JavaScript executes and downloads a malicious Adobe Flash file from **tyu.benme.com**. The Flash file runs and installs malware. After installation, the malware checks in with a

Command-and-Control (CnC) server