- **Formal SBAR report** (2 pages maximum)
  - `Executive Summary` (1 paragraph)
  - `Situation` (1 paragraph)
  - `Background` (1 paragraph)
  - `Assessment` (may be several paragraphs)
  - `Recommendation` (may be several paragraphs or a bulleted list)
- **Technical Appendix** (this section can be as long as necessary)

Use the file hash you discovered in the SIEM to hunt down additional (or corroborate previously-enumerated!) IOCs associated with the particular malware sample used in the previous task's watering hole incident and enrich your understanding of the incident that occurred.

Executive Summary:

The reinvestigation of a suspicious email sent to the CFO of AT-USA, has brought to light new findings that substantiate that this email was a part of an attack that did result in the successful execution of malware on an AT-USA device. The initial investigator, Boots, deemed the email harmless due to a benign link and no malicious attachments. However, this reinvestigation, utilizing SIEM logs, revealed a more complex situation. A drive-by-compromise attack, facilitated by the ciso[.]guide website, led to a Rig exploit kit delivering the Ramnit malware. ~~Several AT-USA devices were exposed, compromised, and or infected, challenging the original assumption that only one device was at risk.~~ As for the extent of compromise and infection, only two devices were compromised by the Rig EK (LAB-Win7-01, Daniel-PC), and one device infected with the Ramnit banking trojan (Daniel-PC). Adobe Flash likely served as the vulnerability exploited. The situation's containment status is uncertain, and mitigation efforts are unverified. Immediate recommendations involve quarantining and forensically examining affected devices. Concluding this summary, it is highly recommended that a ban of outdated/easily -exploitable browser plugins is put into place along with implementation of some built-in exploit protection in order to assist in the prevention of exploit kits and other forms of drive-by-compromises. These forms of prevention would allow employees to freely continue their day-to-day tasks without the worry of potential attack, providing much needed peace of mind.

Situation:

After a suspicious email was sent to the CFO of AT-USA (P. Brand), analyst Boots was originally tasked with investigating the incident. Having found the following: that the link in the email was a regularly visited site by AT-USA employees, no malicious binaries on the device, and no additional attachments were in the email - he determined that the email and the link it contained (www[.]ciso[.]guide[.]com) were benign; and that no other AT-USA devices had been compromised.

Background:

Assigned to me by Virgil, my task was to reinvestigate this incident and establish whether the reported email was legitimately benign (as previously determined by Boots). To do this, I was given access to and utilized SIEM logs, Boots' older SBAR report, and the originally-received email from the first previous investigation (which initially occurred on Friday December 29th, 2017 20:58 UTC).

Assessment:

Boots believed that the only threat vector was the spear phishing email itself and had surmised that the email posed no threat with P. Brand's device being the only workstation that needed to be examined - overlooking other AT-USA devices including one that had actually been compromised and infected.While the spear phishing email was a small component, the main attack vector in this incident was a drive-by-compromise (ciso[.]guide), which utilized a Rig exploit kit (vds[.]cs59923[.]timeweb[.]ru) to successfully deliver Ramnit malware to one AT-USA device. This was a part of a larger, watering hole attack, which exposed several devices other than P. Brand's (the original email recipient) to the threat of ciso[.]guide. It should also be noted that other employees received the spear phishing email as well (M. Land, D. Walker, S. Adams) and that, although P. Brand was targeted by the attacker's spear phishing email, he did not take the bait and did not visit ciso[.]guide during the time it was compromised. Additionally, Daniel *did* visit ciso[.]guide but *did not* receive the attacker's spear phishing email.

The following is a breakdown of the devices affected: 4 AT-USA devices (LAB-Win10-03, LAB-Win10-02, LAB-Win7-01, Daniel-PC) were exposed to the threat (Rig EK), 2 devices were compromised with malware executables (LAB-Win7-01 and Daniel-PC, and 1 device was infected by the Ramnit malware trojan (Daniel-PC). Users '\Daniel' and '\Waxwing' should be considered compromised as well.

Time Range of Exposure to Rig EK:

[2017-12-29 21:24:12-23:16:10.787 UTC] Exposed: LAB-Win7-01, LAB-Win10-03, LAB-Win10-02, Daniel-PC are exposed to the Rig EK threat [via Ciso[.]guide]

Payload Delivery to LAB-Win7-01:

[2017-12-29 21:26:28.856-21:47:16.149 UTC] Payloads (bilo439.exe, bilo494.exe, bilo161.exe, bilo467.exe) are dropped onto LAB-Win7-01\s.adams; Malicious malware payloads are dropped onto the devices. [vds.cs59923.timeweb.ru, LAB-Win7-01]

bilo400.exe Payload on Daniel-PC:

[2017-12-29 23:14:33.073 UTC] Infection occurs: First payload 'bilo400.exe' is dropped on host Daniel-PC. Malicious Ramnit malware payload is dropped onto the device. [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:15:03.161 UTC] Malware executes: Daniel-PC has file 'obommhdf.exe' created from process 'bilo400.exe'. File is created from initial malware process, spreading infection. [vds.cs59923.timeweb.ru, Daniel-PC]

C2 Traffic:

[2017-12-29 23:16:34 UTC] C2 Traffic begins: Initial connection with C2 server. C2 server plays a central role in coordinating and executing malicious activities on the compromised devices, this is its initial connection. [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2018-01-02 05:39:55 UTC] Most recent successful connection with C2 server. C2 communication most likely denotes instructions for malicious activity. [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2018-01-08 16:40:49.938 UTC] Last attempted (but unsuccessful) connection with C2 server. Contact with the C2 server is halted, did they get what they were looking for? [ckkxyupextanlvcrdig[.]com, Daniel-PC]

It is fairly likely that Adobe Flash was the vulnerable application that was exploited in this attack, though further details and investigation is needed to confirm this (Internet Explorer and Silverlight are also on the suspect list).

To my current knowledge the threat has not been contained, and I have no evidence of

mitigations being put into place. It is also unknown at this time whether anything of value was exfiltrated.

There is currently insufficient information for a definitive assessment of severity. Although Daniel-PC did get infected, the situation could have been much worse had other workstations been infected as well. Further questioning and investigation is needed to determine whether Daniel-PC has access to sensitive business-related information which could result in business function disruption.

Recommendation:

The device 'Daniel-PC' should be considered compromised and infected. This device was compromised by the EK and the malware the EK distributed - given this information, it is my recommendation that this device be promptly quarantined, forensically imaged for additional evidence, and then reimaged.

Being compromised and infected, credentials on Daniel-PC should be reset as all credentials used and inputted on this device and its applications could be compromised as well.

LAB-Win7-01 should be also considered compromised by the EK, but not infected - recommendation would be to quarantine this device and remove undetonated payloads, reimaging not required. File names include: bilo467.exe, bilo161.exe, bilo494.exe, bilo439.exe.

Devices that were only exposed to the threat do not necessitate remediation.

- **Banning Outdated or Easily-Exploitable Browser Plugins**: Prohibit the use of vulnerable plugins like Flash or Silverlight. This would significantly reduce the attack surface for drive-by compromise threats.
- **Implementing Built-in Exploit Protection**: Utilize exploit protection strategies to intercept the exploit chain before it escapes the browser's sandbox.
- **Security applications** like Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET) can mitigate exploitation behavior.
- **Web-Based Content Filtering**: Implement some form of web-based content filtering to significantly reduce the likelihood of encountering drive-by compromises within the organization's devices.
- **Script blocking extensions** can prevent the execution of JavaScript commonly used during the exploitation process.
- **Adblockers** can help prevent malicious code served through ads from executing in the first place.
- **Keep browsers up-to-date:** the simple act of keep browsers and other applications regularly updated helps in preventing vulnerabilities

Technical Appendix:

Initial event: [2017-12-29 20:58:29 UTC] Spear phishing (S.P.) emails are sent
Final event: [2018-01-08 16:40:49.938 UTC] Last attempted C2 communication (unsuccessful)

[2017-12-29 20:58:29-20:58:31 UTC] Spear phish attack (begins): S.P. email sent to p.brand@at-usa.co, m.land@at-usa.co, d.walker@at-usa.co, and s.adams@at-usa.co . *AT-USA employees' personal emails are vulnerable to internal risk.* [daniel@mail.at-usa.co, LAB-Win10-04/10-03/10-02 & LAB-Win7-01]

[2017-12-29 21:24:12 UTC] Exposed: LAB-Win7-01\s.adams is exposed to the threat associated with ciso[.]guide. Host is vulnerable to a drive-by-compromise/other malicious redirects. [Ciso[.]guide, LAB-Win7-01]

[2017-12-29 21:26:28.856 UTC] Payload dropped: LAB-Win7-01\s.adams file ‘bilo439.exe’ is created. Malicious malware payload is dropped onto the device. [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:36:30.534 UTC] Payload dropped: LAB-Win7-01\s.adams file ‘bilo494.exe’ is created. Malicious malware payload is dropped onto the device. [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:46:21.166 UTC] Payload dropped: LAB-Win7-01\s.adams file ‘bilo161.exe’ is created. Malicious malware payload is dropped onto the device. [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:47:16.149 UTC] Payload dropped: LAB-Win7-01\s.adams file ‘bilo467.exe’ is created. Malicious malware payload is dropped onto the device. [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:40:33.974 - 21:55:53.103 UTC] Exposed: LAB-Win10-03 is exposed to the threat associated with ciso[.]guide. Host is vulnerable to a drive-by-compromise/other malicious redirects. [Ciso[.]guide, LAB-Win7-01]

[2017-12-29 22:50:07.951 - 23:10:11.405 UTC] Exposed: Daniel-PC is exposed to the threat associated with ciso[.]guide. Host is vulnerable to a drive-by-compromise/other malicious redirects. [Ciso[.]guide, LAB-Win7-01]

[2017-12-29 23:05:04 UTC] Infection occurs: First payload ‘bilo400.exe’ is dropped on host Daniel-PC. Malicious Ramnit malware payload is dropped onto the device. [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:15:03.161 UTC] Continued infection: Daniel-PC has file ‘obommhdf.exe’ created from process ‘bilo400.exe’. File is created from initial malware, spreading infection. [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:16:04.787 UTC] Continued infection: Daniel-PC has file ‘fgkhroxg.exe’ created from process ‘obommhdf.exe’. File is created from initial malware, spreading infection. [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:15:03.190 UTC] Malware binary stops: Last execution of malware binary occurs. Malware process execution has been successfully completed. [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:16:34 UTC] C2 Connection: Initial connection with C2 server. C2 server plays a central role in coordinating and executing malicious activities on the compromised devices, this is its initial connection. [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2017-12-29 23:16:10.787] Exposed: LAB-Win10-02 is exposed to the threat associated with ciso[.]guide. Host is vulnerable to a drive-by-compromise/other malicious redirects. [Ciso[.]guide, LAB-Win10-02]

[2018-01-02 05:39:55 UTC] Most recent successful connection with C2 server. C2 communication most likely denotes instructions for malicious activity. [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2018-01-08 16:40:49.938 UTC] Last attempted (but unsuccessful) connection with C2 server. Contact with the C2 server is halted, did they get what they were looking for? [ckkxyupextanlvcrdig[.]com, Daniel-PC]

External Hosts Involved:

Ciso[.]guide.com (IP: 35[.]196[.]138[.]220) - this is the watering hole that redirected traffic to the Rig EK landing page

Vds[.]cs59923[.]timeweb[.]ru (IP: 176[.]57[.]214[.]103) - this is the EK landing page for the Rig EK

Ckkxyupextanlvcrdig[.]com (194[.]87[.]109[.]183) - this is the malware’s C2 server used for communication

---