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. As for the extent of compromise and infection: two devices were compromised by the Rig EK (LAB-Win7-01, Daniel-PC), and one device was successfully 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). We were also given a memory and disk image of the infected host (Daniel-PC) to use for further analysis and investigation.

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) and successfully delivered Ramnit malware to two AT-USA devices (LAB-Win7-01 & Daniel-PC), with only one ultimately becoming infected. 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]

[2018-01-04 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:

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:

_____

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

_____

Registry Modifications:

Hive Location	Root Key	Key	Key Value	Key Data	Last Write Timestamp
vol_vol3/Windows/System	HKLM	Wow6432Node\Microsoft\Sec	FirewallOv	1	2017-12-29 23:15:03

32/Config/SOFTWARE		urity Center	erride		
vol_vol3/Windows/System32/Config/SOFTWARE	HKLM	Microsoft\Windows\CurrentVersion\Policies\System	EnableLUA	0	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SOFTWARE	HKLM	Wow6432Node\Microsoft\Security Center	AntiVirusOverride	1	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\wscsvc	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\wscsvc	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\WinDefend	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\WinDefend	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\MpsSvc	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\MpsSvc	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\wuauserv	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\wuauserv	Start	4	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	EnableFirewall	0	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	EnableFirewall	0	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	DoNotAllowExceptions	0	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	DoNotAllowExceptions	0	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	DisableNotifications	1	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SYSTEM	HKLM	ControlSet002\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	DisableNotifications	1	2017-12-29 23:15:03
vol_vol3/Windows/System32/Config/SOFTWARE	HKLM	Wow6432Node\Microsoft\Security Center	AntiVirusDisableNotify	1	2017-12-29 23:15:03
vol_vol3/Windows/System	HKLM	Wow6432Node\Microsoft\Sec	FirewallDi	1	2017-12-29 23:15:03

32/Config/SOFTWARE		urity Center	sableNotify		
vol_vol3/Windows/System 32/Config/SOFTWARE	HKLM	Wow6432Node\Microsoft\Security Center	UpdatesDisableNotify	1	2017-12-29 23:15:03
vol_vol3/Windows/System 32/Config/SOFTWARE	HKLM	Wow6432Node\Microsoft\Security Center	UacDisableNotify	1	2017-12-29 23:15:03
User_Daniel\NTUSER.DAT	HKCU	Software\Microsoft\Windows\CurrentVersion\Run	Run	Null (no value)	2017-12-29 23:16:32
User_waxwing\NTUSER.DAT	HKCU	Software\Microsoft\Windows\CurrentVersion\Run	Run	Null (no value)	2018-01-04 14:54:07
vol_vol3/Windows/System 32/Config/SOFTWARE	HKLM	Microsoft\Windows NT\CurrentVersion\Winlogon	Userinit	userinit.exe,C:\Users\Daniel\AppData\Local\guwayhtr\obommhdf.exe	2018-01-01 21:10:22
vol_vol3/Windows/System 32/Config/SOFTWARE	HKLM	Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	Userinit	userinit.exe,C:\Users\Daniel\AppData\Local\guwayhtr\obommhdf.exe	2017-12-29 23:15:05
User_waxwing\NTUSER.DAT	HKCU	Software\AppDataLow\0C3AFB06-FBAD-1ECB-E500-5F32E9340386	OboMmhdf	C:\Users\Waxwing\AppData\Local\guwayhtr\obommhdf.ex	2018-01-02 4:14:15
User_Daniel\NTUSER.DAT	HKCU	Software\AppDataLow\0C3AFB06-FBAD-1ECB-E500-5F32E9340386	OboMmhdf	C:\Users\Daniel\AppData\Local\guwayhtr\obommhdf.ex	2017-12-29 23:16:50

			e		
vol_vol3/Windows/System32/Config/SOFTWARE	HKLM	Wow6432Node\Microsoft\Windows NT\CurrentVersion	jfghdug_ooetvtgk	TRUE	2018-01-01 21:10:21