EXECUTIVE SUMMARY

This incident was far more severe than previously thought, 2 AT-USA devices have been compromised with a banking Trojan binary file saved to their disks. The first compromise happened on LAB-Win7-01\s.adams at 12/29/2017 21:25:22 UTC. The second device was Daniel-PC\Daniel at 12/29/2017 23:05:04 UTC. An attacker has used the Rig Exploit Kit to deliver malware binaries containing the Ramnit Trojan through a Flash exploit. The malware has executed on Daniel-PC (Users: Daniel & Waxwing) at 12/29/2017 23:05:05 and has achieved persistence along with communication to its Command and Control server. Ramnit is a banking Trojan that is capable of exfiltrating sensitive data such as banking credentials and other passwords on the device. There are some simple, but effective recommended changes to prevent future attacks of similar nature. Adding detection for exploit traffic as well as adding Snort alerts to detect exploit traffic on top of C2 detection would take very little time and aid greatly in prevention. Also, implementing some internal policies such as disabling unapproved browser plugins, keeping plugins updated, and most importantly uninstalling Flash would greatly reduce the likelihood of a future Rig attack.

SITUATION

This investigation involves the AT-USA network. It is related to a previous investigation conducted by Boots. The incident started when the CFO of AT-USA(email: p.brand@at-usa.co) received an email that he flagged as suspicious. The task was assigned to me by Serper. I received a copy of Boots SBAR on the suspicious email.

BACKGROUND

The time of the reported incident was 12/29/2017 at 19:58 UTC. I was asked to re-work the open investigation and determine if the email sent to the CFO of AT-USA was benign and if any devices have been compromised. The evidence I was given was Splunk logs of AT-USA’s network, a copy of the original flagged email, and Boots SBAR. Serper has told me that the website is often visited by IT staff at AT-USA and that the email had no attachments. In Boots SBAR, his hypothesis was as follows: "This message appears to be benign, as no malicious binary was found on the device in question". He also recommended that the "device be put back into circulation and no further precautions or damage control is necessary at this time." Here was his reason for the investigation, "The CFO asked us to investigate an e-mail sent to him recently. This is one of an increased amount of reports of this nature that we have received of

late. He believes that it is suspicious, and as his position makes him a high-value target in our organization"

ASSESSMENT

The attack started with the email sent to p.brand on Dec. 29th, 2017 at 12:58:29. The email was directing him to a compromised website that was acting as a watering hole for the Rig Exploit Kit. Someone has compromised ciso[.]GUIDE by adding a redirection link within the page. The redirection link is an embedded iframe that sends the victim through a series of gates and then to the malware Landing page. A landing page is a server that a victim gets sent to and sends the malware back to the device. In this incident, the malware was the RIG exploit kit. A total of 4 company computers were exposed to the threat in this incident. They were exposed to the threat by connecting to the exploit kits' IP address. Once a computer connects to the EK's landing page, Rig will try one of the following attacks as needed: JavaScript, Flash, or VBScript-based attacks. After the 4 computers were connected to the malicious IP, RIG attempted to use a Flash exploit to download the malware payload to the devices. The 4 devices were the following, LAB-WIN7-01\s.adams, LAB-WIN10-03\m.land, Daniel-PC\Daniel, LAB-WIN10-02\d.walker. In this attack, they were successful at downloading the binary and compromising 2 AT-USA devices, LAB-Win7-01 and Daniel-PC.

The attacker is sending the Ramnit banking Trojan, capable of exfiltrating sensitive data including but not limited to banking credentials, browser cookies, personal data, and other passwords. Now that the malware is downloaded on 2 devices, it will attempt to execute. Before execution, the malware will run an analysis on the compromised machine and determine if it's compatible with one of the exploits and the malware campaign. It can also fail at any stage of execution due to numerous reasons. In this attack, it found one suitable computer to execute on, Daniel-PC/Daniel, and remains dormant on LAB-Win7-01. After the initial Rig EK's Bilo400.exe execution, the Ramnit software took over from here. It duplicated itself in multiple locations under different names on the device to establish persistence. Along with copying itself, Ramnit also does many registry modifications to avoid detection and gain further control. After only around 10 minutes of the initial Bilo400.exe execution, Ramnit made its first communication to its Command and Control (C2) server at 12/29/2017 23:16:35 UTC.

The C2 server for Ramnit is capable of receiving and storing data, along with sending commands or even more malware. A few days after the first user was infected, the malware was executed from within a second user on the same device, Daniel-PC/Waxwing. From the time of the first connection until 1/4/2018 16:40:50 UTC, the malware was sending and receiving information and commands from its C2 server. I do not have enough information to determine what exactly was stolen and sent back to the command server.

This was a very serious attack. An attacker has targeted the AT-USA CFO with a banking Trojan through a drive-by compromise. Although they were not able to infect their target, they were able to fully compromise one device on the AT-USA network (Daniel-PC, Users: Daniel, Waxwing). I do not have enough information to determine if anything compromised was of value. As of this time, the threat has not been contained, and no mitigations have been put into place. Due to the specific malware sent, I believe the attackers were trying to exfiltrate some type of banking data. The main target(P.BRAND) was not infected, but another device on the network was and could be used to build and send a new attack that is capable of moving laterally on the network. Others might have been sent this email to avoid suspicion. I believe this was a targeted attack due to the email being sent to the CFO, and that AT-USA staff frequently visit ciso[.]GUIDE (a trusted site among AT-USA staff). The attacker was attempting to deliver Ramnit payloads to visitors of ciso[.]GUIDE through an Adobe Flash exploit using the RIG EK. I do not have enough information to determine if the attacker was successful at retrieving any important information. I believe this was part of a larger attack.

I found that Boot's hypotheses are incorrect because the message was not benign, and I have found evidence of at least one device, Daniel-PC, being fully infected. The attack originated from ciso[.]GUIDE, where an attacker has compromised the site and added a malicious redirection link.

RECOMMENDATION

- Daniel-PC(Daniel, Waxwing) has been fully infected and should be quarantined immediately to prevent any further loss of data or lateral movement.
- LAB-Win7-01(s.adams) also remains compromised due to multiple payloads being dropped on the disk. Although the payload has not been executed yet, it still has the possibility to do so at any time, so it should be treated similarly to Daniel-PC.
- The login credentials and banking credentials for the users' Daniel and Waxwing on Daniel-PC should be reset, along with any credentials stored on the device that were vulnerable during the attack.
- Due to the fact that we do not know what was stolen or sent in the attack, Daniel-PC(Daniel, Waxwing) should be signed out to have a forensic copy of the memory and hard drive taken.
- The users of Daniel-PC(Daniel, Waxwing) should be questioned about if any banking information is on the device to know what might have been stolen.
- A new investigation should be started by taking a forensic copy of the memory and hard drive on Daniel-PC(Daniel, Waxwing) to investigate what if anything was stolen during this attack.

Amendments: Boots SBAR had a few incorrect conclusions. "This appears to be a benign message" The message was not benign, the message was directing users to visit a compromised website being used as a watering hole to attempt to exploit users.

Network Configurations

- Adding Snort alerts to detect exploit traffic on top of C2 traffic would greatly reduce the chance for another attack achieving the same success of communication back to its C2 server. Right now, Snort is set up to only detect C2 traffic, which will only occur after a machine has been fully infected.
- Adding detection for exploit traffic could allow SOC and IT staff to quarantine the compromised devices before they can relay any information to a command server.

Host Recommendations

- For internal policies, ensure that all employee browsers and plugins are kept up to date and that Adobe Flash is uninstalled.
- Ensure that all employees Web Browsers are up-to-date to prevent VBScript based attacks
- User vigilance to use trusted sites and not click malicious links is a good way to prevent JavaScript attacks
- Disabling browser plugins for all employees unless approved by SOC/IT department. These fairly basic steps can greatly reduce the chance of exploits through browsers or plugins due to frequent security patches.

Future Prevention

The communication back to the control server, specifically the outbound traffic, can be monitored to detect malware variants using snort. This attack was carried out by the RIG EK delivering Ramnit payloads. The users were first exploited through a flash exploit from the watering hole ciso[.]GUIDE. The characteristics of an attack like this are a website being hacked so that malicious code can be added. That code redirects users through a series of gates that end up on the exploit kit's landing page. The landing page will send payload files that will attempt to execute and, if successful, communicate back to a C2 server.

Watering Hole:

ciso[.]GUIDE
35[.]196[.]138[.]220

C&C Server

Ckkxyupextanlvcrdig[.]com
194[.]87[.]109[.]183

Rig EK binary filenames:

LAB-Win7-01:
Bilo161.exe, Bilo439.exe, Bilo467.exe, Bilo494.exe
Daniel-PC:
Bilo400.exe

TECHNICAL APPENDIX

Ramnit/Rig SHA 256:
08875F1B26F8CDAA139402559D6716DBA973C8F9449DECB19343FBF24A58D11F.

All the files that need to be removed from Lab-Win7-01 are within
C:\Users\s.adams\AppData\Local\Temp\
C:\Users\s.adams\Desktop\