CISO.GUIDE FINAL REPORT

Rev B

Cyber Team 10

Authored by: S. Voss

TABLE OF CONTENTS

1 – EXECUTIVE SUMMARY 2
2 - SITUATION 3
3 – BACKGROUND 3
4 - ASSESSMENT 4
5 - RECOMMENDATIONS 6

1 – EXECUTIVE SUMMARY

P. Brand, the CFO of AT-USA received a suspicious email from the CISO.guide IT Support Team at 15:58 EST (20:58 UCT) on December 29th, 2017, and subsequently reported it.

Originally Boots investigated this report at the end of 2017 and determined it was a benign email and a false alarm.

The investigation was revisited as per a directive from Virgil.
It has since been determined that Boots' original assessment was wrong.

The email was sent out to lure AT-USA personnel to a legitimate website (www[.]ciso[.]guide) that has been frequently visited by the AT-USA IT staff prior to this email being received, and ultimately to an Exploit Kit (EK - Rig) landing page so a drive-by compromise could ossur. In turn, this EK would then send a payload malware (Ramnit) to devices that were not protected.

The investigation shows that four devices on their network interacted with this website with varying degrees of results.

Four devices exposed:

- *Daniel-PC*
- *LAB-Win7-01*
- *LAB-Win10-02*
- *LAB-Win10-03*

Of these four devices two were compromised by the EK (Rig).

- *Daniel-PC*
- *LAB-Win7-01*

Of these two, only Daniel-PC was infected with the Ramnit banking trojan malware.

The severity of this compromise is uncertain but could be considered troubling because Daniel-PC was manually infected. We're wrapping up the investigation now. Based on our analysis of the disk image, it's safe to say that Daniel-PC didn't seem to contain any sensitive information

Changes that can be easily implemented within AT-USA's infrastructure with minimal or no impact on employee productivity are, but not limited to:

- *Regularly update all browsers and plugins.*
- *Implement modern browsers with robust security features enabled.*
- *Ban the use of outdated or easily exploitable browser plugins (such as Flash or Silverlight).*
- *Implement various built-in exploit protection mechanisms*
    - *Windows Defender Exploit Guard (WDEG)*
    - *Enhanced Mitigation Experience Toolkit (EMET)*
- *Incorporate web-based content filtering*
    - *Script-blocking extensions*
    - *Adblockers*

2 - SITUATION

A suspicious email from the CISO.guide IT Support Team was received and subsequently reported by P. Brand, the CFO of AT-USA.

The email was a way to get AT-USA employees to a legitimate website (www[.]ciso[.]guide) that is frequently visited by the AT-USA IT staff.

Boots investigated and determined that the email didn't have any malicious attachments and that P. Brand's device was free of any suspicious and or malicious software, and that this was a false alarm. He did not investigate any further for other possible email recipients or compromised devices.

3 – BACKGROUND

The suspicious email reported by P. Brand was received at 2017-12-29 20:58 UTC
Originally Boots investigated this report at the end of 2017 and determined it was a benign email and a false alarm.

I've been tasked by Virgil to revisit this report and assessment and to confirm or refute Boots' findings of this email being benign and a false alarm, or was it in fact malicious, and if any other AT-USA devices were compromised and or infected.

I have been given the original suspicious email, Boots' SBAR, and access to all pertinent logs in the SEIM (email, bro, sysmon, av, cisco, and snort) to help and aid in the investigation.

4 - ASSESSMENT

The original assessment by Boots that this was a benign message and there was no malicious binary is wrong.

Also, P. Brand was not the only email recipient. S. Adams, M. Land, and D. Walker were also targeted.

This was more than a spearphishing attack, it was a drive-by compromise.
Ciso[.]guide is a watering hole website re-directing traffic to an EK (Rig) landing page.

Four devices were exposed.

- *Daniel-PC*
- *LAB-Win7-01*
- *LAB-Win10-02*
- *LAB-Win10-03*

Of these four devices two were compromised by the EK (Rig).

- *Daniel-PC*
- *LAB-Win7-01*

Of these two, only Daniel-PC was infected with the Ramnit banking trojan malware.

The timeline of the incident occurred between 2017-12-29 20:58:29 and 2018-01-04 16:40:49 UTC.

On 2017-12-29 20:58:29 UTC, a suspicious email, appearing to originate from support@ciso[.]guide, was reported by P. Brand. The investigation determined that the website linked in the email, ciso[.]guide, had been compromised and was being used as a watering hole to facilitate a drive-by compromise using (Rig EK).

During the period of compromise, any device that accessed ciso[.]guide was subsequently redirected to a Rig EK landing page (vds-cs59923[.]timeweb[.]ru). The EK was actively distributing the Ramnit banking trojan at the time of the attack.

There were four AT-USA employees (P. Brand, M. Land, D. Walker, S. Adams) who were recipients of the suspicious email.

Between 2017-12-29 21:24:23 and 23:37:03 UTC, three of the targeted employees (M. Land, D. Walker, S. Adams) accessed ciso[.]guide and were exposed to the threat. An employee using Daniel-PC (identified as Daniel) who hadn't received the email also navigated to ciso[.]guide. P. Brand did not visit the compromised website.

Each device was redirected to a (Rig EK) landing page after accessing ciso[.]guide. Of the four devices only two of these (LAB-Win7-01\s.adams, Daniel-PC\Daniel), were successfully compromised by the EK, likely through exploiting vulnerabilities in Adobe Flash Player.

Between 2017-12-29 21:26:28 and 21:47:16 UTC, four payloads (bilo439.exe, bilo494.exe, bilo161.exe, bilo467.exe) were delivered to LAB-Win7-01\s.adams. None of these payloads were executed, and LAB-Win7-01 remained uninfected.

On 2017-12-29 23:05:04 UTC, a single payload (bilo400.exe) was manually delivered / implemented onto Daniel-PC\Daniel.

On 2017-12-29 23:14:33, the payload executed resulting in the infection of the device with the Ramnit banking trojan.

The Ramnit malware established persistence on Daniel-PC and initially connected to the Ramnit C2 server (ckkxyupextanlvcrdig[.]com) on 2017-12-29 23:16:34 UTC.

The last successful C2 connection occurred on 2018-01-02 05:39:55 UTC.
The final connection attempt, which was unsuccessful, occurred on 2018-01-04 16:40:49 UTC.

The Ramnit malware infected two user profiles on Daniel-PC (Daniel-PC\Daniel, Daniel-PC\Waxwing).

The severity of this compromise is uncertain but could be considered troubling at the very least because Daniel-PC was manually / deliberately infected.

Because we have a disk image of the contents of Daniel-PC that can be examined, and it doesn't appear to have anything of value to an attacker this case can be closed.

5 - RECOMMENDATIONS

Because Daniel-PC was manually / deliberately infected with the Ramnit malware which is a Trojan / Banking malware… an in-depth interview with Daniel and Waxwing should be conducted to understand what information Daniel-PC is privy to.

The severity of the attack is dependent on what information is being used / stored on the device but can be considered troubling at the very least because it was manually infected.

If possible, determine who was on the device at the time of the infection and why they would purposely infect the device?

A triage of the current situation:
AT-USA should be notified immediately that what was originally deemed as a false alarm, was in fact a compromise / breach.

The original SBAR created by Boots needs to be amended.

The following devices should be singled out for additional analysis and investigation.

- *LAB-Win7-01 - S. Adams*
  - *This device should be quarantined immediately and investigated. While it did not get infected by the malware Ramnit it was compromised by the Rig EK. It needs to have the undetonated payloads (bilo439.exe, bilo494.exe, bilo161.exe, bilo467.exe) removed.*
- *Daniel-PC – Daniel\Waxwing*
  - *This device has been infected by the malware (Ramnit) and needs to be quarantined immediately and ultimately reimaged.*
  - *Credentials for both Daniel and Waxwing need to be reset. This will extend beyond the login credentials for the device's user accounts. Any credentials used / entered in the browser could potentially be compromised.*

Changes that can be easily implemented within AT-USA's infrastructure are, but not limited to:

- *Regularly update all browsers and plugins.*
- *Implement modern browsers with robust security features enabled.*
- *Ban the use of outdated or easily exploitable browser plugins (such as Flash or Silverlight).*
- *Implement various built-in exploit protection mechanisms*
  - *Windows Defender Exploit Guard (WDEG)*
  - *Enhanced Mitigation Experience Toolkit (EMET)*
- *Incorporate web-based content filtering*
  - *Script-blocking extensions*
  - *Adblockers*

IMPROVED DETECTION||VISIBILITY FOR FUTURE SIEM INVESTIGATIONS

R3a DETECTION||VISIBILITY • Can you describe any general patterns associated with this attack that a rule could be built from that would automatically pick up on similar activity? Be specific about how you would define your rule so that it won't alert on false positives.

Set up rules for monitoring directories:

- Start Menu
    - Users
        - %USERPROFILE%
            - AppData
                - Local
                    - Temp
    - Windows
        - Prefetch

This won't eliminate ALL false positives but limit them, so time isn't wasted chasing everything.

R3b DETECTION||VISIBILITY • Identify the generic type of attack involved in this incident.

Winlogon.exe

- [EIGHT PSEUDO-RANDOM CHARACTERS].exe (obommhdf.exe)
    - [EIGHT PSEUDO-RANDOM CHARACTERS].exe (xwgrttjl.exe)
        - svchost.exe
        - svchost.exe
            - TRACERT.exe
        - sdbinst.exe

R3c DETECTION||VISIBILITY • Identify the characteristics of this generic type of attack.

Bilo[3 random digits].exe – Rig EK Payloads
[EIGHT PSEUDO-RANDOM CHARACTERS].exe – Random Executables
[EIGHT PSEUDO-RANDOM CHARACTERS].log – Downloaded files from Ramnit C2 server

R3d DETECTION||VISIBILITY • Identify the characteristic evidence of this type of attack, as you are able to currently see in the SIEM logs you have access to.

As per SANS Whitepaper:

- Able to identify certain registry entries and subkeys (below are some but not all):
  - FirewallOverride 1
  - FirewallDisableNotify 1
  - AntiVirusOverride 1
  - AntiVirusDisableNotify 1
- Able to see DLL's 1 and 2 showing communication with C2 Server.

Researching the hash: 08875f1b26f8cdaa139402559d6716dba973c8f9449decb19343fbf24a58d11f
As per VirusTotal, Hybrid Analysis, and AlienVault

Able to see multiple domains contacted globally:
China, Russian Federation, Netherlands, Czech Republic, Switzerland

[EIGHT PSEUDO-RANDOM CHARACTERS].exe (obommhdf.exe)
[EIGHT PSEUDO-RANDOM CHARACTERS].exe (xwgrttjl.exe)

The Ramnit malware established persistence on Daniel-PC and initially connected to the Ramnit C2 server

R3e DETECTION||VISIBILITY • Are there additional log sources (or configuration adjustments to existing sources) that would improve the visibility||detection of this type of attack in the SIEM? Make specific suggestions on what could be added or adjusted, if possible, to improve the efficacy of detecting and investigating this type of attack in the future.

Active Directory Logs – to provide information about user authentication and authorization.

Configuration adjustments:

- Adjust the configuration of existing log sources to improve the visibility and detection of this type of attack.
- Increase the level of detail in firewall logs or endpoint logs.
- Adjust the thresholds for generating alerts 1,2,3.