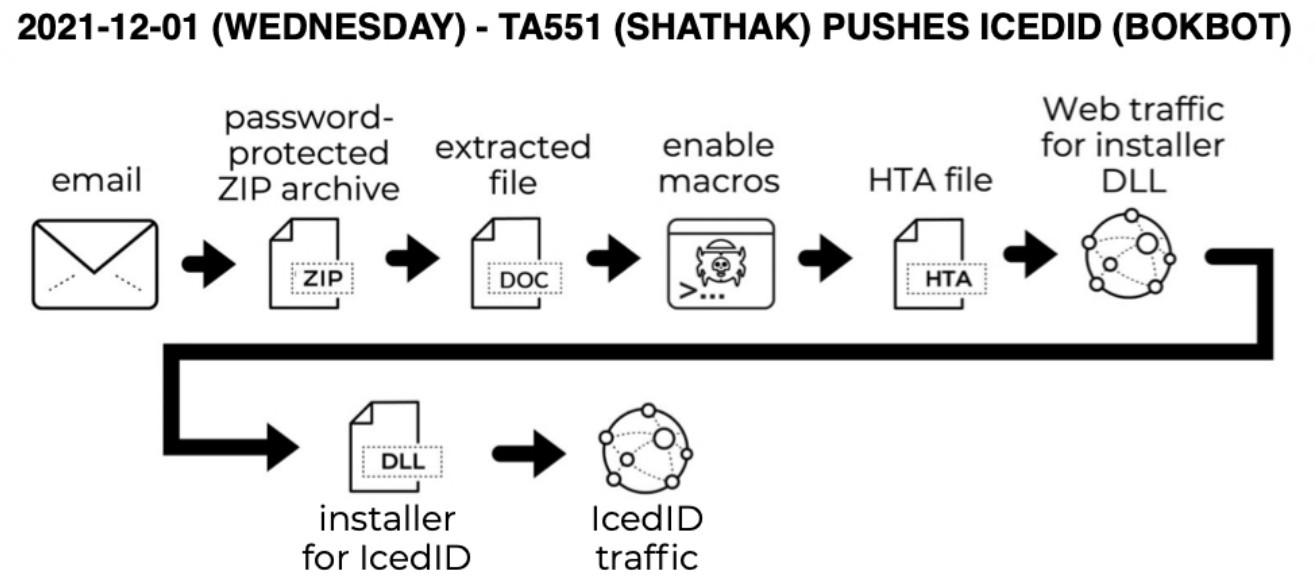
SANS ISC: TA551 (Shathak) pushes IcedID (Bokbot) - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

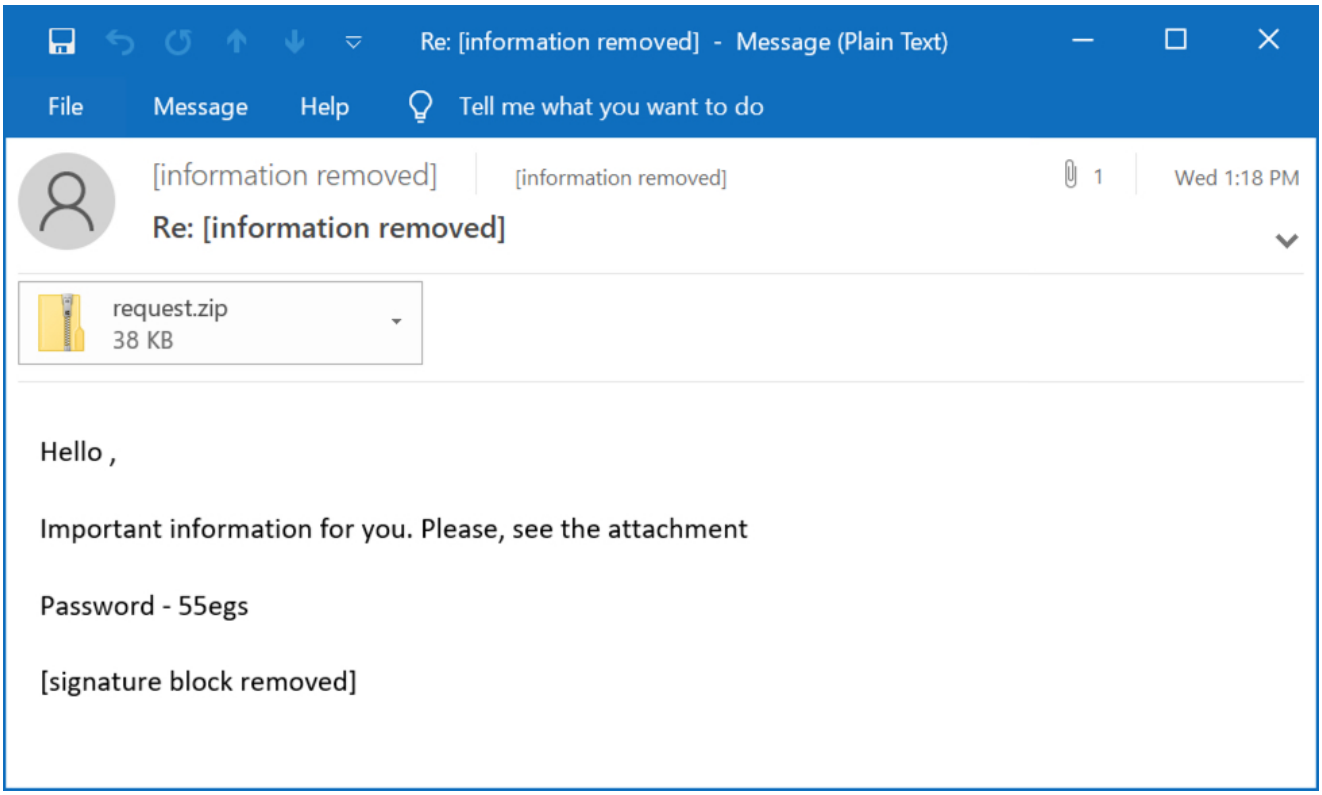
Introduction

TA551 (also known as Shathak) represents a threat actor behind malspam that has pushed different families of malware over the past few years. So far this week, TA551 is pushing IcedID (Bokbot).



Shown above: Flow chart for this infection.

Images from an infection



Shown above: Screenshot from a TA551 email with sensitive information removed.

Indicators of Compromise (IOCs)

The infection process was similar to my previous diary about TA551 from August 2021, but this time it delivered IcedID instead of BazarLoader.

Associated malware:

SHA256 hash:
d68fb04c96e925efcdb3484669365bed0cda22a272e486e99a43f9626019d31c

- File size: 38,958 bytes
- File name: request.zip
- File description: Password-protected zip archive attached to email
- Password: 55egs

SHA256 hash: 0a42f6762ae4f3b1d95aae0f8977cde6361f1d59b5ccc400c41772db0205f7c5

- File size: 34,322 bytes
- File name: charge_12.01.2021.doc
- File description: Word doc with macros for IcedID

SHA256 hash: c7f40608ce8a3dda25c13d117790d08ef757b07b8c2ccb645a27a71adc322fb2

- File size: 3,342 bytes
- File location: C:\Users*[username]*\Documents\youTube.hta

- File description: HTA file dropped after enabling Word macros

SHA256 hash: d54a870ba5656c5d3ddfab5f7f325c2fb8ee256b25e2872847c5ff244bc6ee6e

- File size: 257,672 bytes
- File location: hxxp://winrentals2017b[.]com/tegz/*[long string of characters]*/cab3?ref=*[long string of characters]*
- File location: C:\Users\Public\dowNext.jpg
- File description: Installer DLL for IcedID
- Run method: regsvr32.exe *[filename]*

SHA256 hash: cfc202b44509f2f607d365858a8218dfdc6b26f8087efcc5e46f4fef9ab53705

- File size: 341,898 bytes
- File location: C:\Users*[username]*\AppData\Roaming\ReliefEight\license.dat
- File description: license.dat data binary used to run persistent IcedID DLL

SHA256 hash:
c340ae2dde2bd8fbae46b15abef0c7e706fe8953c837329bde409959836d6510

- File size: 116,224 bytes
- File location: C:\Users*[username]*\AppData\Roaming\{24DB904E-86F7-2F2C-B7C1-85D8BBCE1181}\Miap\Giowcosi64.dll
- File description: persistent IcedID DLL
- Run method: rundll32.exe *[filename]*,DllMain --giqied="*[path to license.dat]*"

IcedID traffic:

- 143.204.155[.]37 port 443 - ***aws.amazon[.]com*** - HTTPS traffic
- 87.120.254[.]190 port 80 - ***normyils[.]com*** - GET / HTTP/1.1
- 87.120.8[.]98 port 443 - ***baeswea[.]com*** - HTTPS traffic
- 91.92.109[.]95 port 443 - ***bersaww[.]com*** - HTTPS traffic

Final words

IcedID can be followed by Cobalt Strike when an infected host is part of an Active Directory (AD) environment. These types of infections can deliver ransomware as a final payload in real-world environments.

But decent spam filters and best security practices can help you avoid IcedID. Default security settings in Windows 10 and Microsoft Office 2019 should prevent these types of infections from happening.

Brad Duncan
brad [at] malware-traffic-analysis.net

Brad

433 Posts
ISC Handler
Dec 3rd 2021