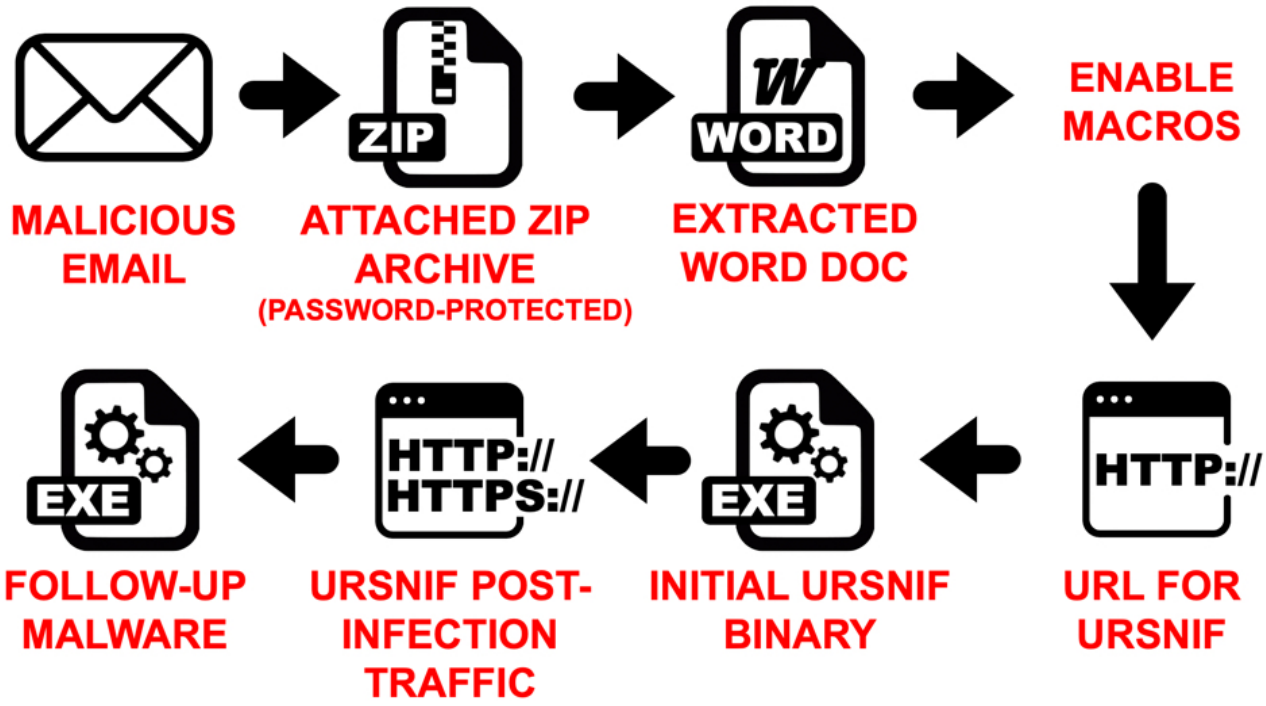
SANS ISC: German language malspam pushes Ursnif - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

Introduction

On Tuesday 2020-01-21, a wave of malicious spam (malspam) hit various recipients in Germany. Messages from this German malspam were email chains associated with infected Windows hosts, and these emails all had password-protected zip archives as attachments. A closer look revealed this malspam was pushing Ursnif.

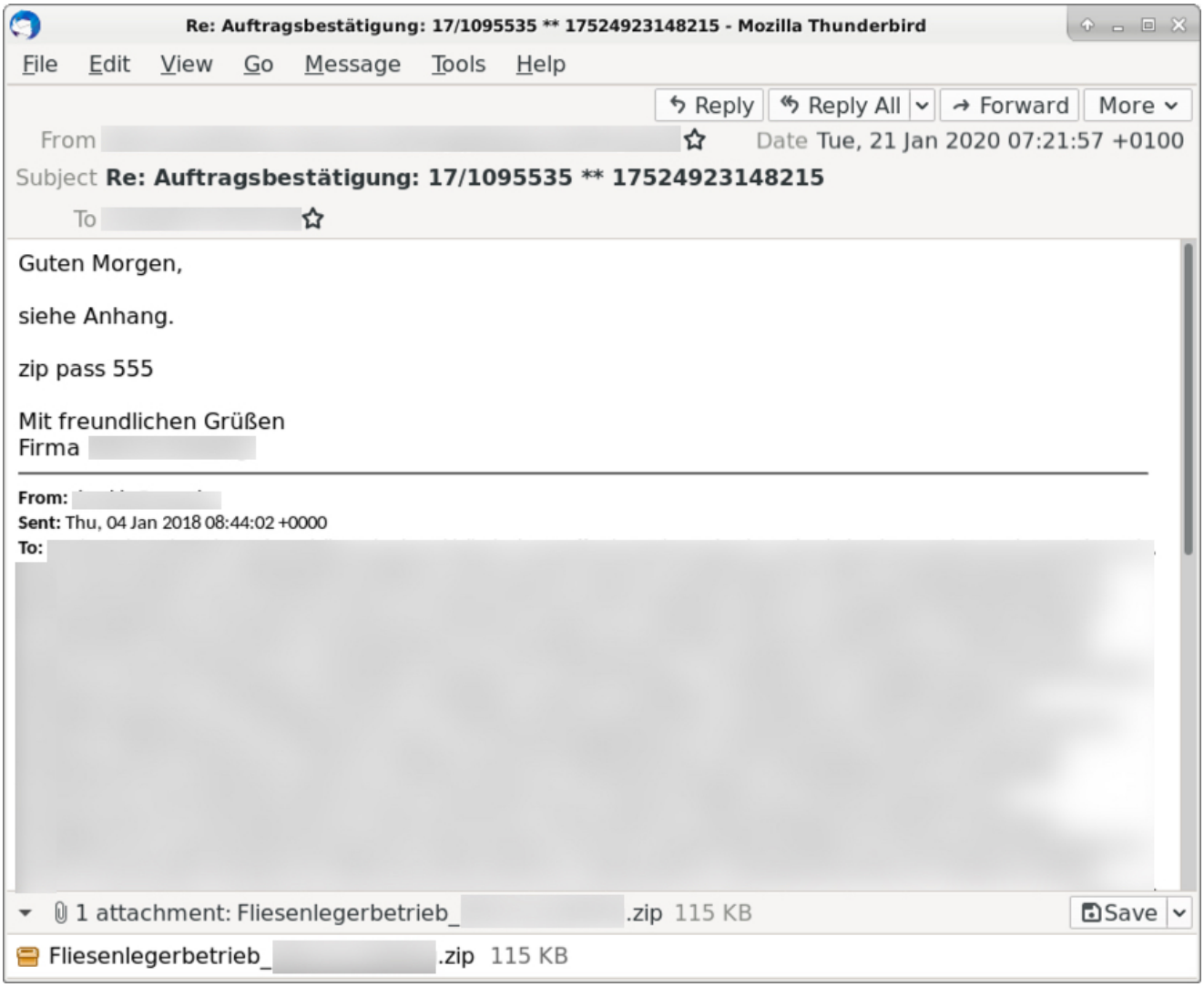
Today's diary reviews this malspam and an Ursnif infection from one of the attachments on Tuesday 2020-01-21.



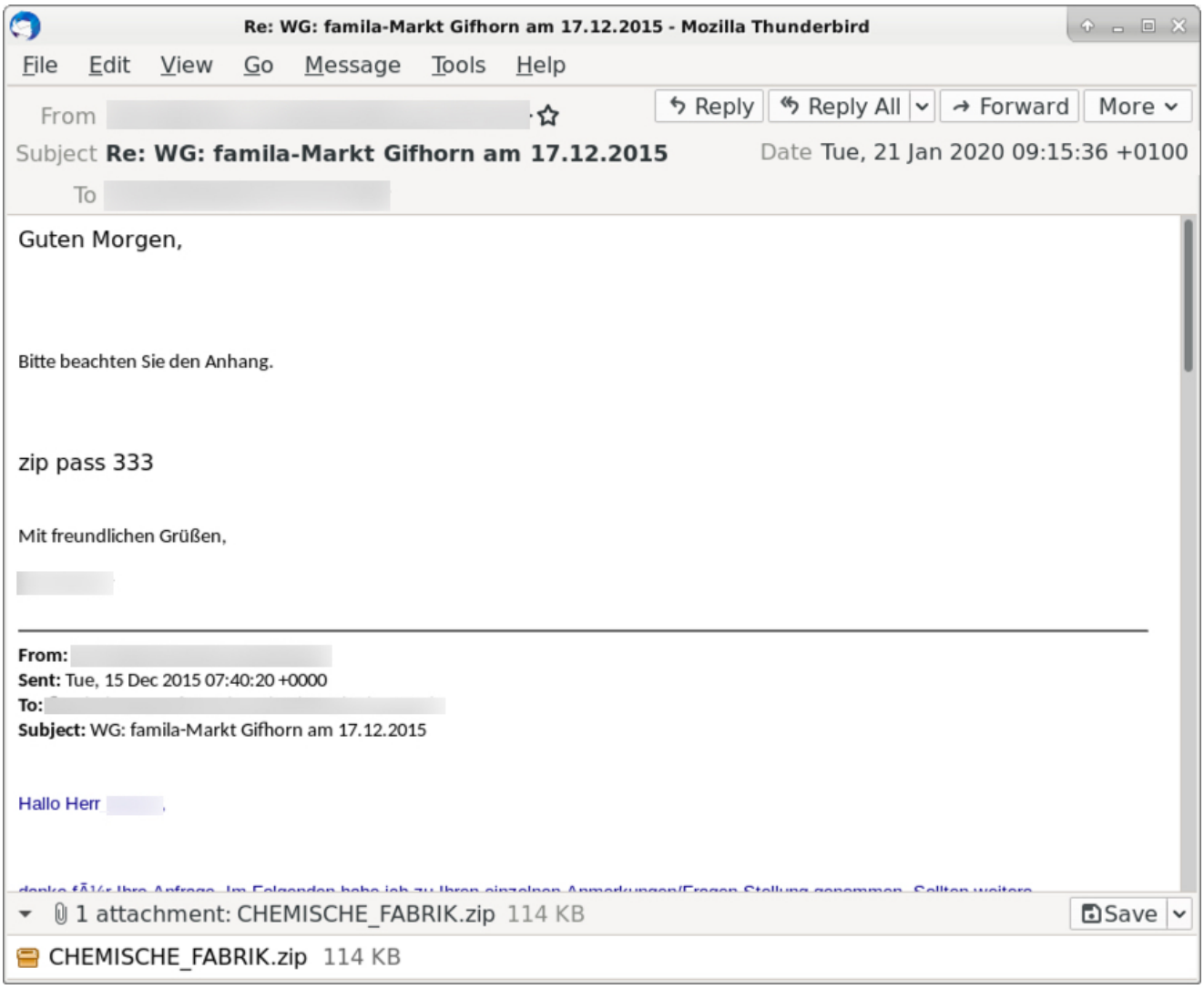
Shown above: Flow chart for an infection from this wave of German malspam.

The malspam

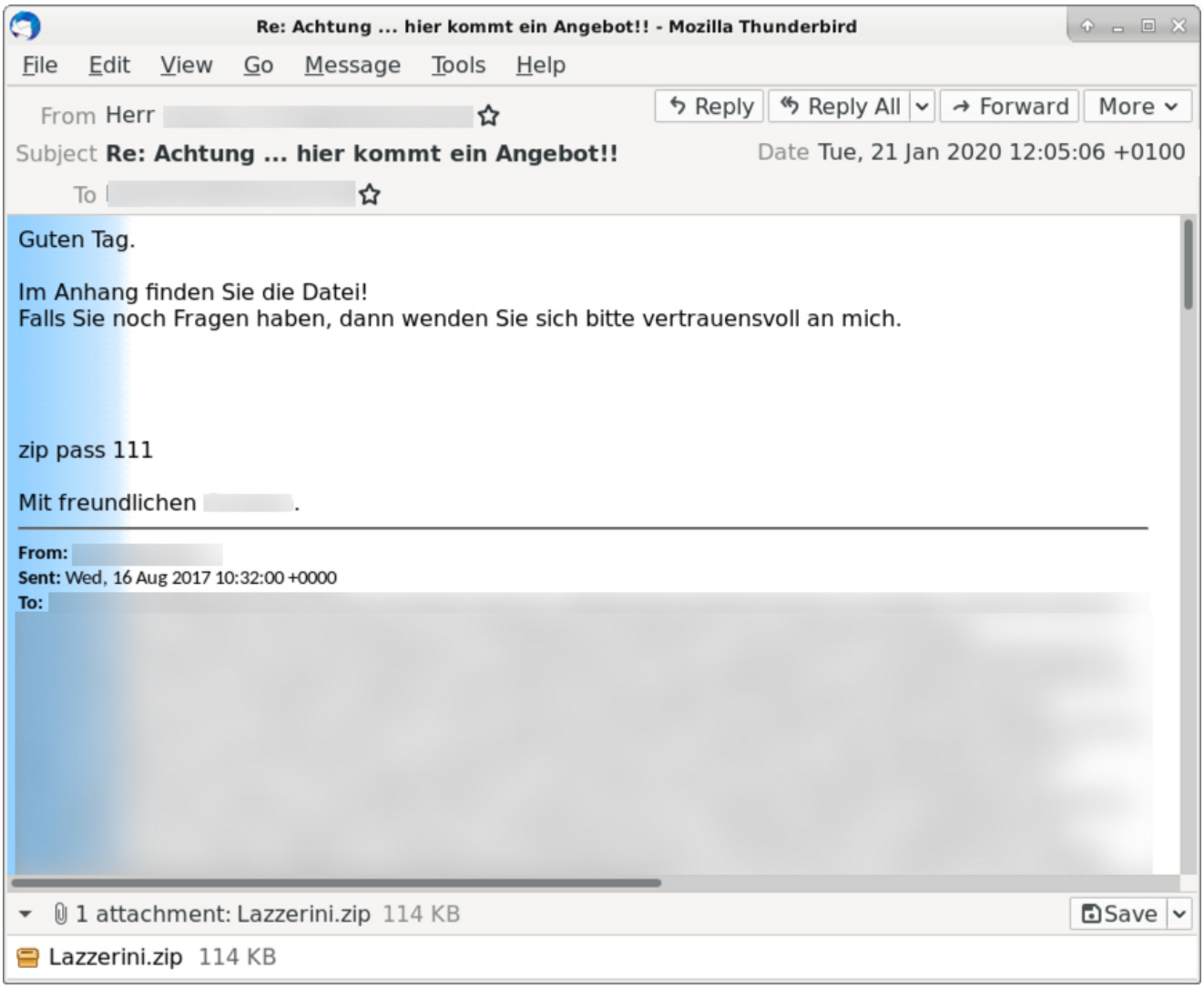
See the next three images for examples from this wave of malspam. Of note, this campaign often used ***777*** as the password for the attached zip archive. In this wave of malspam, we saw passwords ***111***, ***333***, and ***555***. Other passwords were probably used as well in examples we have not yet reviewed.



Shown above: An example of the malspam from Tuesday 2020-01-21 (1 of 3).



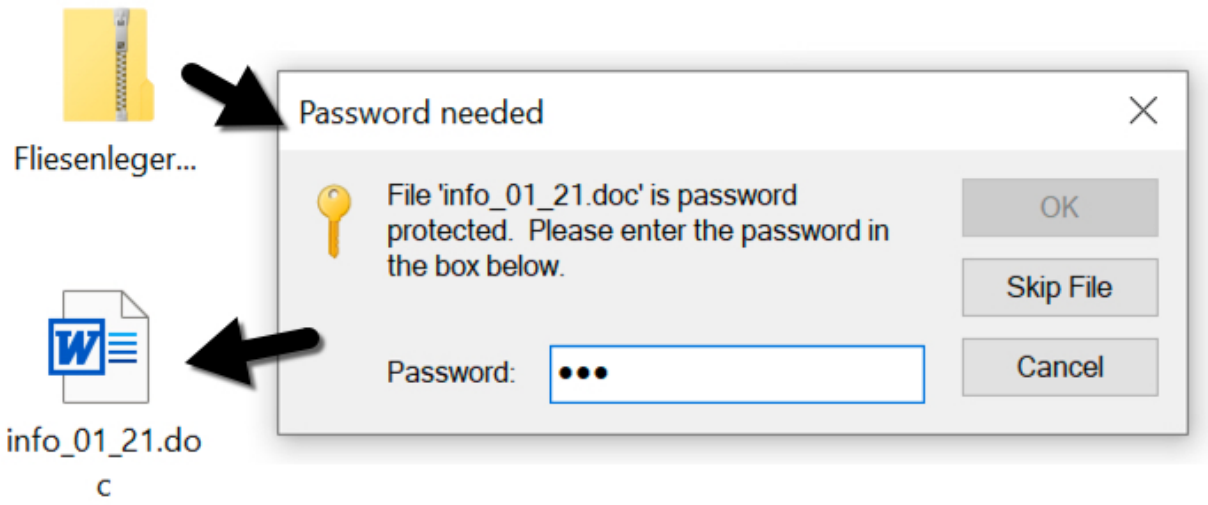
Shown above: An example of the malspam from Tuesday 2020-01-21 (2 of 3).



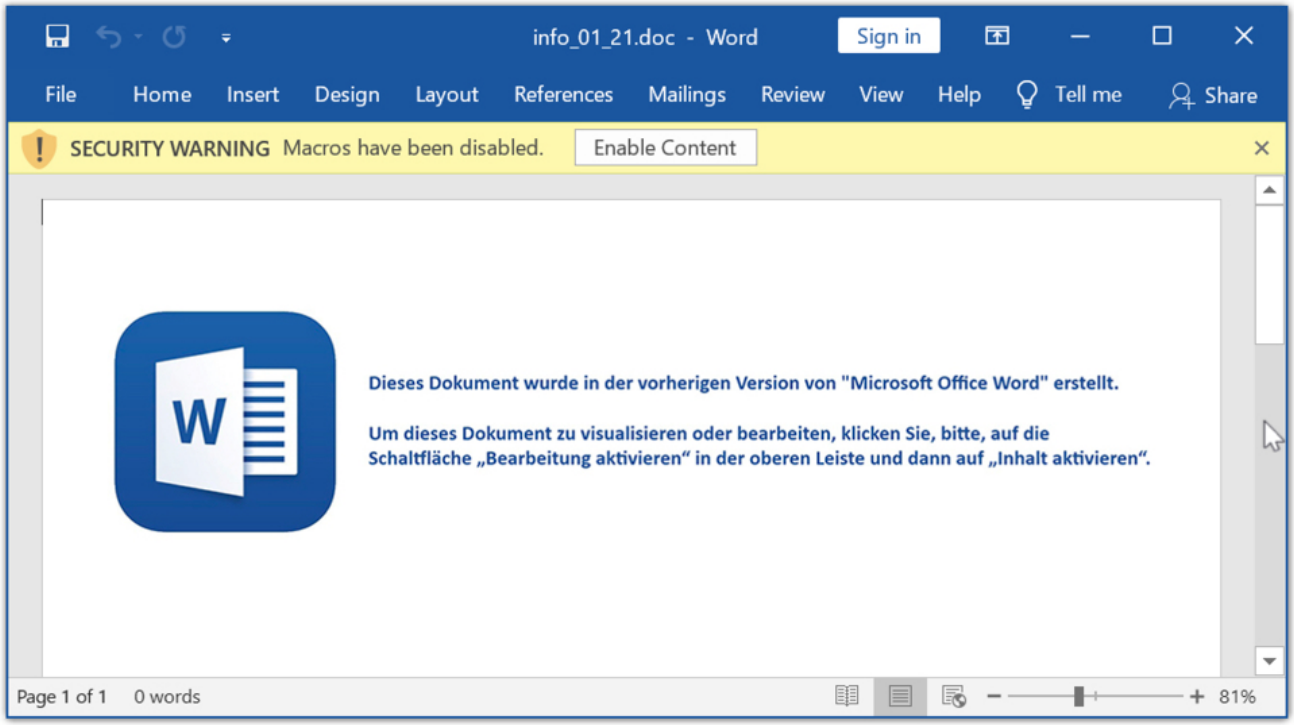
Shown above: An example of the malspam from Tuesday 2020-01-21 (3 of 3).

The attachments

Using the password from the email, you can extract a Microsoft Word document from the password-protected zip archive. The message in the Word document is in German, and it directs you to enable macros. All of the Word documents are named ***info_01_21.doc***. Of note, in recent versions of Microsoft Office, you must disable Protected Mode and bypass some other security features to enable macros and infect a vulnerable Windows host.



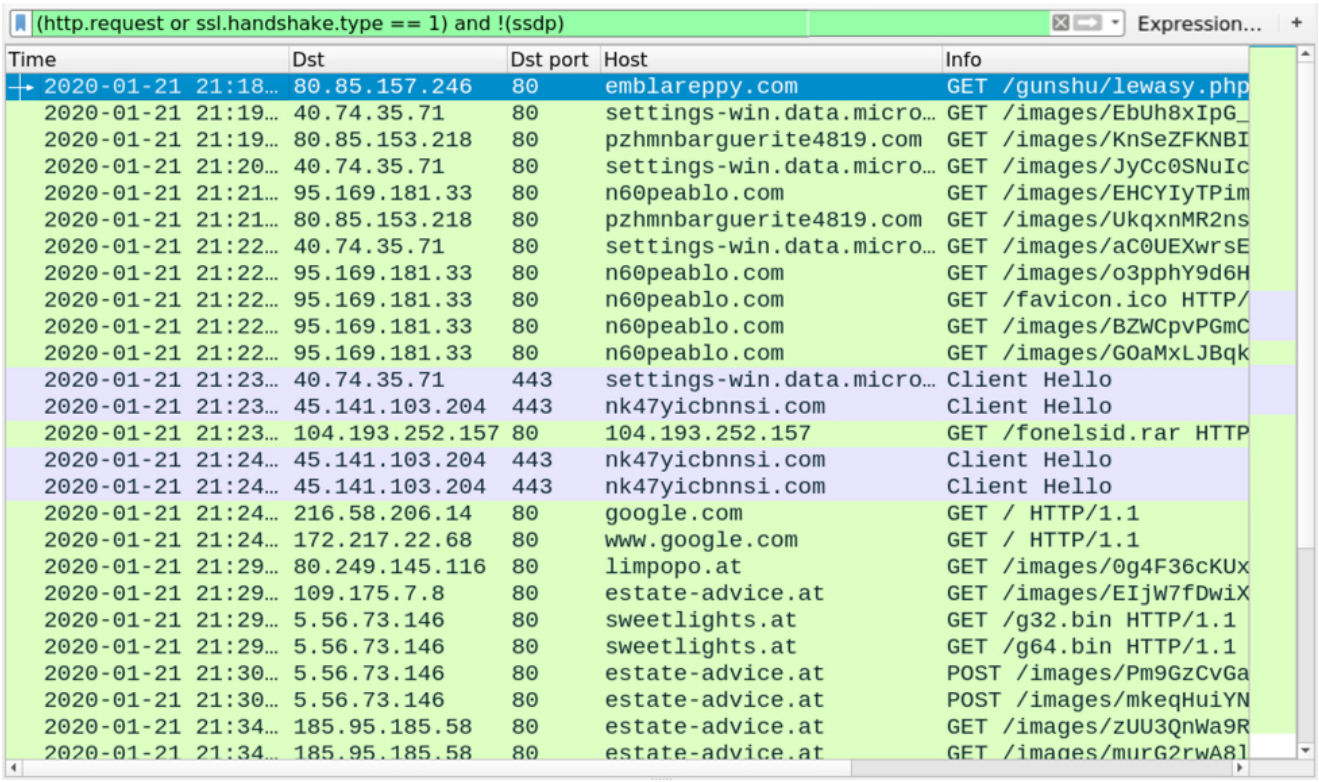
Shown above: Extracting a Word document from one of the password-protected zip archives.



Shown above: An example of an extracted Word document.

The infection traffic

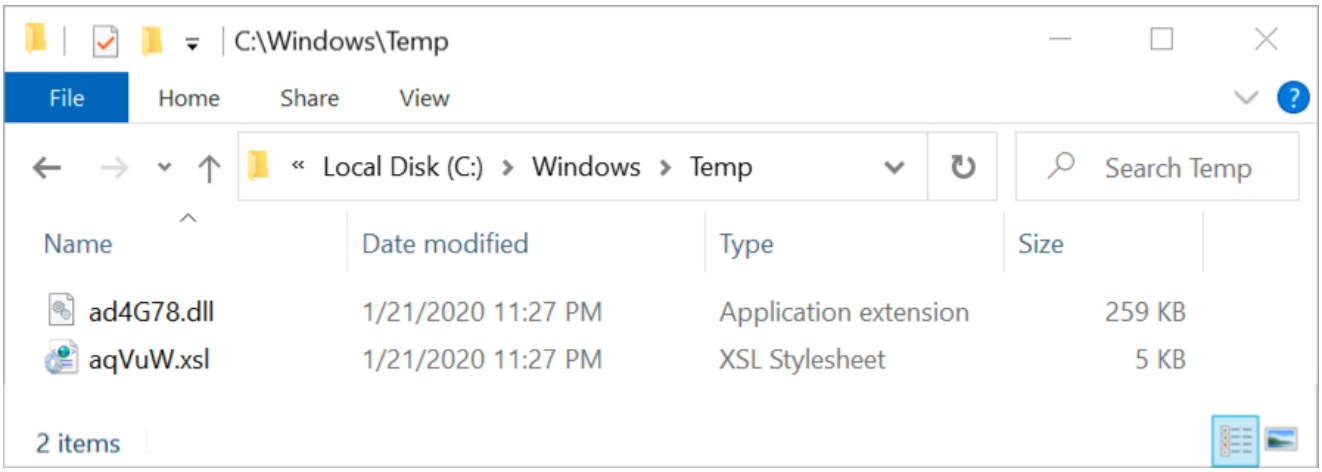
Infection traffic is typical for Ursnif infections in recent months. Other examples of Ursnif traffic can be found here, which contains infections from 2019. Of note, the follow-up malware for this Ursnif infection was another Ursnif variant.



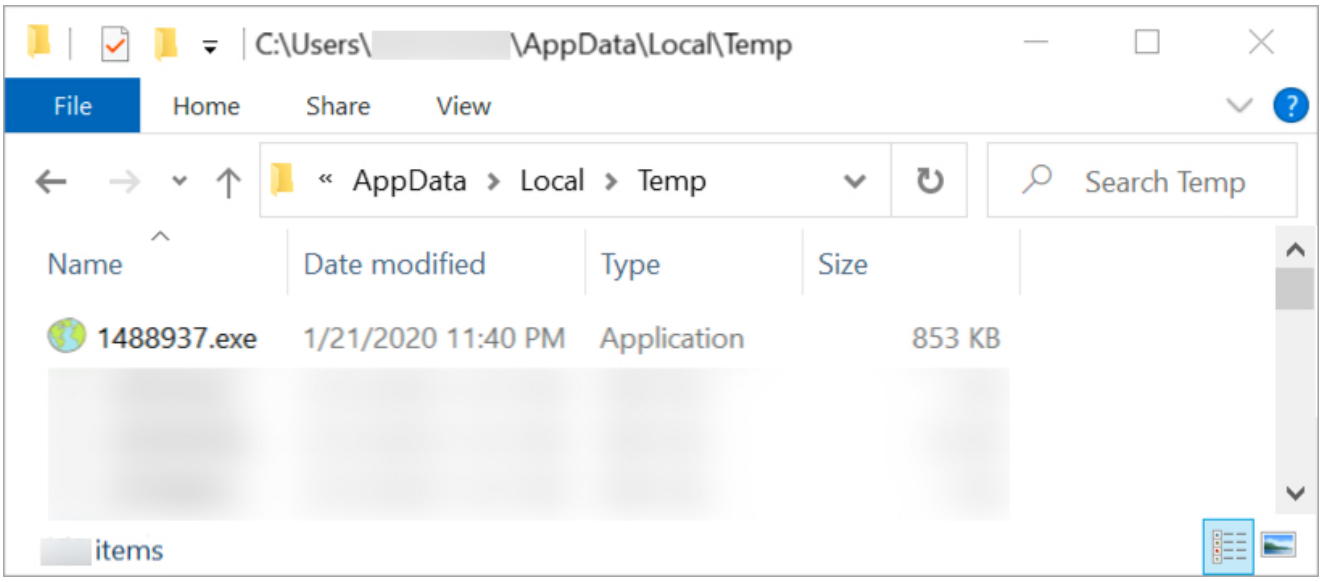
Shown above: Traffic from an infection filtered in Wireshark.

Forensics on an infected Windows host

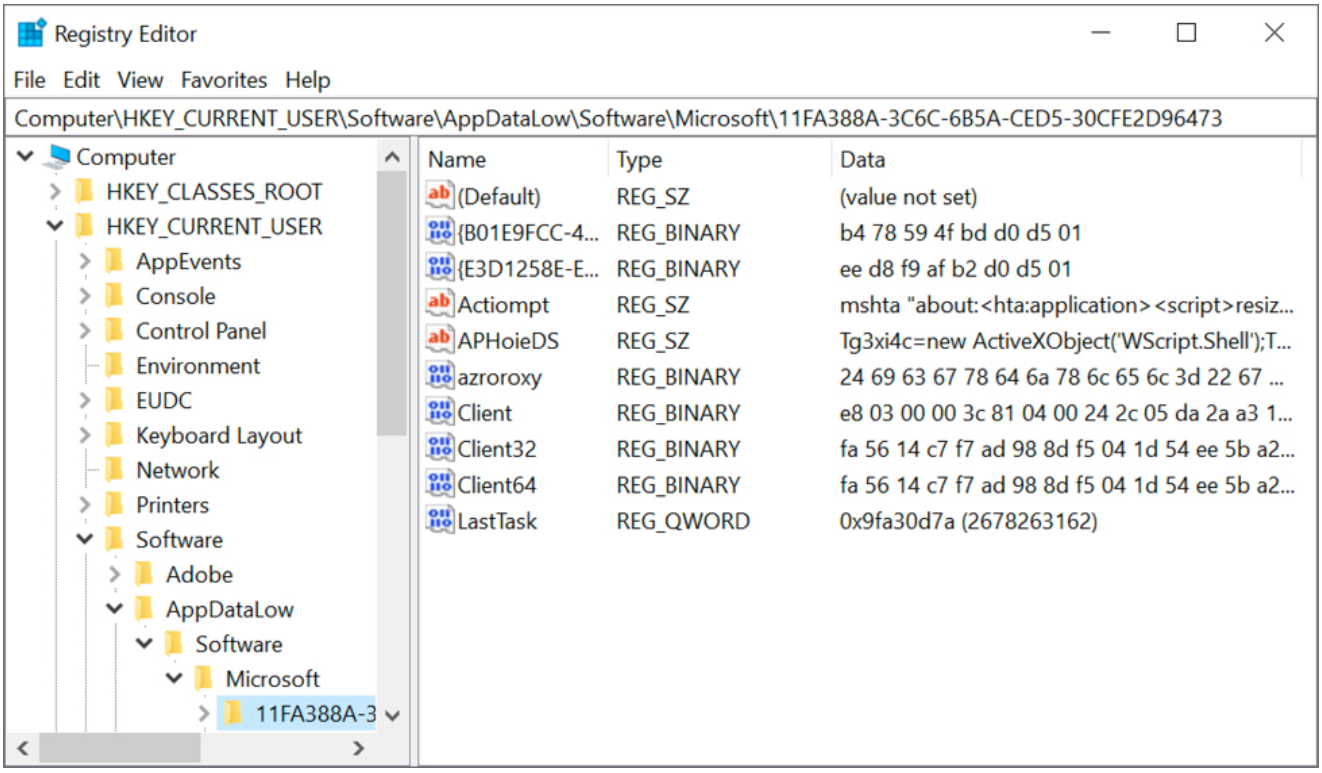
The infected windows host contained artifacts commonly seen with these type of Ursnif infections. See the images below for details.



Shown above: Artifacts in seen the C:\Windows\Temp directory after enabling macros.



Shown above: Follow-up malware found on the infected Windows host.



Shown above: Update to the Windows registry caused by Ursnif to keep it persistent on the infected host.

Indicators of Compromise (IoCs)

Infection traffic from the initial Ursnif infection:

- 80.85.157[.]246 port 80 - ***emblareppy[.]com*** GET /gunshu/lewasy.php?l=ambobi9.cab
- port 80 - ***settings-win.data.microsoft[.]com*** - GET /images/*[long string]*.avi
- 80.85.153[.]218 port 80 - ***pzhmnbarguerite4819[.]com*** - GET /images/*[long string]*.avi
- 95.169.181[.]33 port 80 - ***n60peablo[.]com*** - GET /images/*[long string]*.avi

- port 443 - ***settings-win.data.microsoft[.]com*** - HTTPS traffic
- 45.141.103[.]204 port 443 - ***nk47yicbnnsi[.]com*** - HTTPS traffic

Request for the follow-up malware:

104.193.252[.]157 port 80 - ***104.193.252[.]157*** - GET /fonelsid.rar

Infection traffic caused by the follow-up malware (another Ursnif variant):

- port 80 - ***google[.]com*** - GET /
- port 80 - ***www.google[.]com*** - GET /
- DNS queries for ***onionpie[.]at*** - no response from the server
- DNS queries for ***tahhir[.]at*** - no response from the server
- 80.249.145[.]116 port 80 - ***limpopo[.]at*** - GET /images/*[long string]*
- 109.175[.]7.8 port 80 - ***estate-advice[.]at*** - GET /images/*[long string]*
- 5.56.73[.]146 port 80 - ***sweetlights[.]at*** - GET /g32.bin
- 5.56.73[.]146 port 80 - ***sweetlights[.]at*** - GET /g64.bin
- 5.56.73[.]146 port 80 - ***estate-advice[.]at*** - POST /images/*[long string]*
- 185.95.185[.]58 port 80 - ***estate-advice[.]at*** - GET /images/*[long string]*
- 80.249.145[.]116 port 80 - ***limpopo[.]at*** - POST /images/*[long string]*
- 51.223.47[.]15 port 80 - ***estate-advice[.]at*** - POST /images/*[long string]*

Malware info:

SHA256 hash:
957573dc5e13516da0d01f274ab28a141dddc8b6609fa35fde64a4900cb793e6

- File size: 127,243 bytes
- File name: info_12_21.doc
- File description: Word doc with macro for Ursnif

SHA256 hash: 05ec03276cdbb36fdd8433beca53b6c4a87fa827a542c5d512dcbb2cf93023c9

- File size: 3,651 bytes
- File location: C:\Windows\Temp\axsUG8.xsl
- File description: XSL file dropped by Word macro

SHA256 hash:
c7f801c491d705cd5e6a202c7c5084874235e19b5505d8e0201111cb3789a9c8

- File size: 265,216 bytes
- File location: hxxp://emblareppy[.]com/gunshu/lewasy.php?l=ambobi9.cab
- File location: C:\Windows\Temp\aaNuLh.dll
- File description: Ursnif DLL file retrieved using XSL file

- DLL note: "C:\Windows\System32\rundll32.exe" c:\Windows\Temp\aaNuLh.dll,DllRegisterServer

SHA256 hash:
df824e3e5bb15c7b74d5e8a021f3cbcd867100a02399b9c383488c660ae920b4

- File size: 873,472 bytes
- File location: hxxp://104.193.252[.]157/fonelsid.rar
- File location: C:\Users*[username]*\AppData\Local\Temp*[random digits]*.exe
- File description: Follow-up malware, another Ursnif variant
- File location note: binary returned from fonelsid.rar URL was encoded/encrypted as it was sent over the network

Final words

A pcap of the infection traffic, the associated malware and artifacts, and some malspam examples can be found here.

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