# Ursnif Banking Trojan Targets Germany and Italy

*Author: James Barnett*

## Overview

Between 23 and 24 January, security researcher Brad Duncan reported two separate malicious spam campaigns that used compressed Microsoft Word documents with malicious macros to deliver Ursnif malware.[1, 2]

## Customer Impact

Ursnif is a variant of the Gozi banking trojan that is capable of stealing credentials, cryptocurrency wallets, and email information. Upon infection, Ursnif injects its code into the Internet Explorer (IE) browser, then uses IE to manage communications with its command and control (C2), including follow-on downloads.

## Campaign Analysis

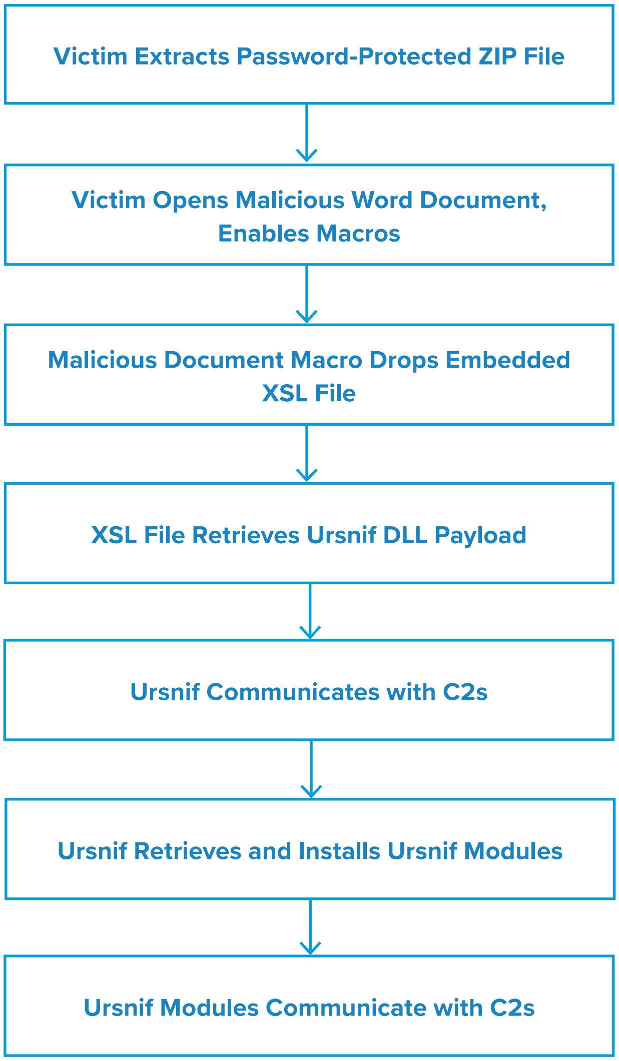
The Ursnif campaigns in this report used similar tactics to the Ursnif campaigns that Infoblox has reported in the past.[3, 4] Namely, they sent messages that appeared to be replies to existing email chains and asked the recipient(s) to open an attached ZIP file with a specific password.

These campaigns also continued the trend of Ursnif campaigns that target specific regions or languages: the emails and documents in the 23 January campaign were all written in German, while those in the 24 January campaign were written in Italian.

## Attack Chain

When the victim extracts and opens the malicious Word document contained within the password-protected ZIP file, they are presented with a message instructing them to enable macros. Once enabled, these macros drop an embedded XSL file that uses Javascript to download and activate an Ursnif DLL payload from a predetermined location.

When Ursnif is activated, it begins to steal user credentials and communicate with its C2s to exfiltrate information, receive further instructions, and download additional Ursnif modules that expand its capabilities.


Victim Extracts Password-Protected ZIP File
Victim Opens Malicious Word Document, Enables Macros
Malicious Document Macro Drops Embedded XSL File
XSL File Retrieves Ursnif DLL Payload
Ursnif Communicates with C2s
Ursnif Retrieves and Installs Ursnif Modules
Ursnif Modules Communicate with C2s

## Vulnerabilities & Mitigation

Emails in this campaign were designed using social engineering tactics to increase their effectiveness and likelihood of infecting victims with malware. As such, Infoblox recommends taking the following precautions to prevent these types of attacks from succeeding:

- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Block password-protected files, archives, or otherwise encrypted attachments until they can be deemed safe because email filters cannot decrypt and inspect their contents.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g. by phone or in person) before opening them.
- Do not enable macros in a Microsoft Office attachment, especially if the file's only apparent contents are directions to enable macros.

## Endnotes

1. http://malware-traffic-analysis.net/2020/01/23/index.html
2. http://malware-traffic-analysis.net/2020/01/24/index.html
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--26
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--48

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com

Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com