Analyzing Ursnif's Behavior Using a Malware Sandbox

Date:
06/25/2019

Ursnif is a group of malware families based on the same leaked source code. When fully executed Urnsif has the capability to steal banking and online account credentials. In this blog post, we will analyze the payload of a Ursnif sample and demonstrate how a malware sandbox can expedite the investigation process.

Ursnif (also known as Gozi) is a banking Trojan that generally collects system activity, records keystroke data, and keeps track of network and

Access the VMRay Analyzer Report for Ursnif

This blog post will cover a behavioral analysis of a single Ursnif variant. It does not provide comprehensive insights into web injects, infrastructure or attribution. For additional Ursnif analysis see Appendix D.

OLSTEALER steals data from Outlook, including login information, and stores it in a local file. The internal name of the module is visible in Function log:

The contents of the created file appear as follows:

The IESTEALER module reads Internet Explorer history and passwords.

Table of Contents

Share With Others:

After stealing from Internet Explorer, the malware also looks for Thunderbird, though the name of the Thunderbird stealer module (TBSTEALER) did not explicitly appear.

System Info Gathering

Using built-in Windows system tools Ursnif gathers information about the system. The tools used are:

- *systeminfo.exe* – various info about the system including OS version, installed patches, domain, and basic hardware information
- *net view* – show network shares
- nslookup 127.0.0.1 – local IP
- *tasklist.exe /SVC* – Services
- *driverquery.exe* – Installed drivers
- (Installed software)*reg.exe query “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*
  reg.exe query “HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Data Exfiltration

Ursnif caches stolen data to the hard drive into temp files, compresses them into CAB files, and uploads them.

Steps followed to create the CAB:

1. The various stealer modules create files on the hard drive. Some use the*%TEMP%* directory, others use the random directory created earlier.

Tags : banking trojan, malware analysis

You May Also Like:

See All Post

Latrodectus: A year in the making

Read now

Healthcare Under Ransomware Attacks – Par…

Read now

Healthcare Under Ransomware Attacks – Par…

Read now

Subscribe to our Newsletter:

Email **Submit**

Solutions

- Alert Investigation for SOAR
- Alert Enrichment for EDR
- Incident Response
- Threat Hunting
- Threat Intel Extraction
- Detection Engineering
- User Reported Phishing

Products

- VMRay DeepResponse
- VMRay FinalVerdict
- VMRay TotalInsight
- Analyzer (Retired)
- Professional Services

Why VMRay

- VMRay Pricing
- VMRay Integrations
- VMRay Unparalleled
- VMRay Technologies
- Success Stories

Resources

- Blog
- Academy
- Glossary
- Malware Analysis Reports

MISSED THE HEADLINES?

WE'RE FEATURED IN:

Careers | Customer Support | Privacy Policy | Legal Information