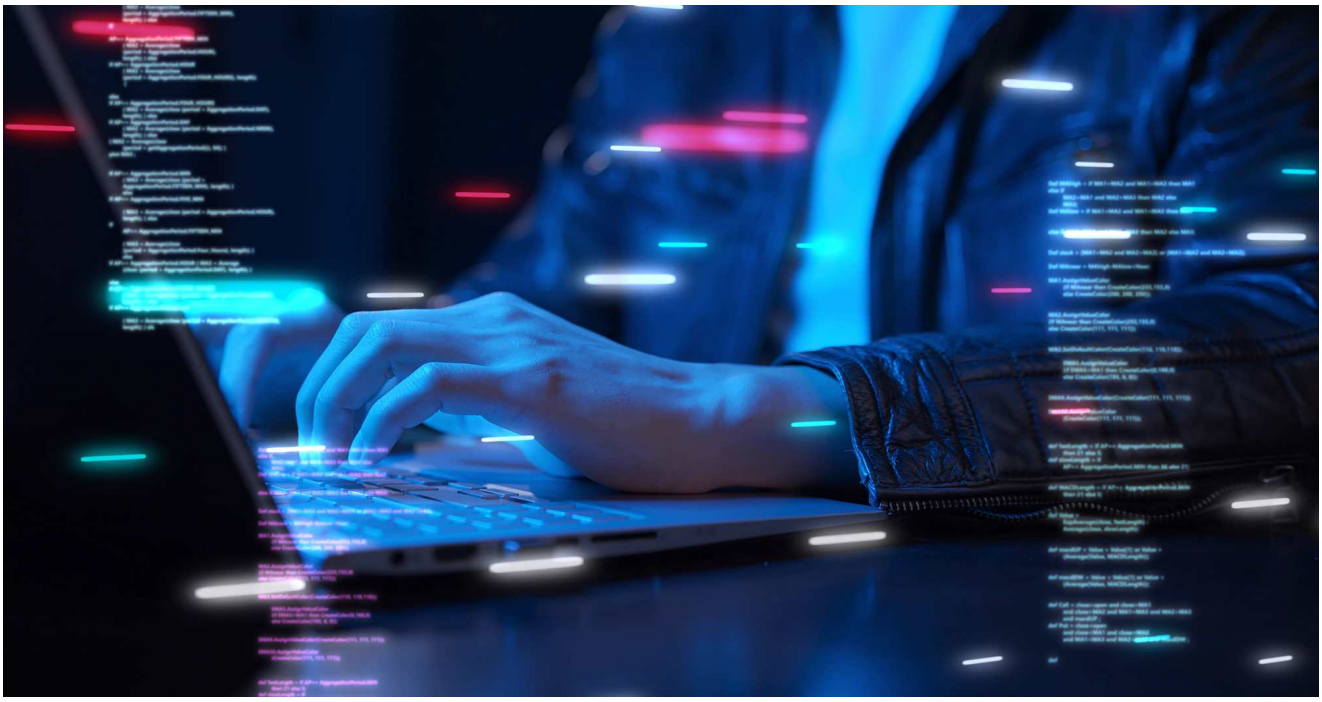
Hunting for Ursnif

bridewell.com/insights/news/detail/hunting-for-ursnif



Bridewell's Cyber Threat Intelligence (CTI) team have uncovered Ursnif infrastructure that has been used in campaigns during 2023, infrastructure which has seen extremely low detection, or no detection, by security vendors. Our team believe that this infrastructure has yet to be used by the operators of the Ursnif malware. This infrastructure can be linked together by the unique attributes of the C2 servers used by the operators, predominantly the SSL certificates. This report details the hunting process conducted by Bridewell CTI to uncover the Ursnif infrastructure.

Sign up to get instant Threat Intelligence Alerts

What is Ursnif?

Ursnif, or also known as Gozi, is a backdoor that was previously developed as a banking trojan which has had many forks and variants released over the years but now, following suit with other malware such as Emotet and Trickbot, focuses on facilitating ransomware and data exfiltration. The latest variant of Ursnif, known as LDR4, was first observed in June 2022 by Mandiant[1].

Recent Campaigns In January 2023, the DFIR report [2] documented an intrusion into an environment that begun with Urnsnif as the backdoor, that lead to the deployment of Cobalt Strike and ended with Data Exfiltration. Additionally, the threat actor used the legitimate RMM tools Atera and Splashtop. Ursnif was delivered in this instance via a malicious ISO file in a

phishing email to an end user. In March 2023, esentire reported on BatLoader dropping various second-stage payloads as part of a Google Ads campaign masquerading as popular tools such as Adobe Reader, Zoom and ChatGPT. The dropper would pull down payloads such as Redline information stealer as well as Ursnif. This activity was also followed up with Cobalt Strike in enterprise environments to facilitate further intrusion activity.

During 2023, there have been different documented initial access methods used to deploy Ursnif in to victim environments, such as through target phishing or malicious advertisements. Customers should be aware of this threat currently being used by threat groups to collate and exfiltrate data and support further payload delivery such as Cobalt Strike. Royal ransomware group, first observed in June 2022, have made frequent use of Ursnif to support data aggregation activities during their intrusions. This ransomware group is a financially motivated criminal group that has compromised multiple industry sectors including Critical National Infrastructure.

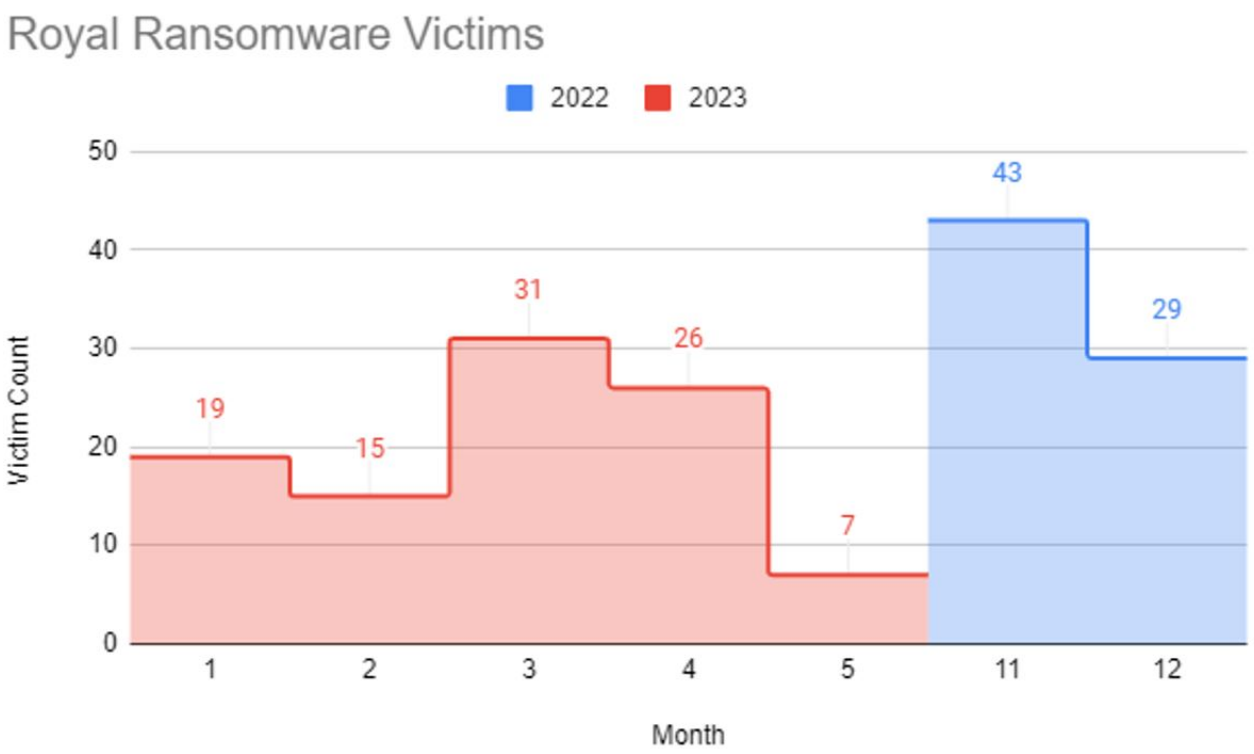
Executive Summary

As a result of our intelligence collection and analysis we identified 72 command and control servers associated with Ursnif malware, from our threat research the following points can be made:

- 23 of the 72 servers contained evidence of the Ursnif malware connecting to them.
- 6 are yet to be identified as Ursnif C2 servers.
- Detection remains extremely low with an average of 4.78 vendors detecting the C2 servers.
- 49 servers remain without any communicating files but match the Bridewell hunt rule.

[1] https://www.mandiant.com/resources/blog/rm3-ldr4-ursnif-banking-fraud

[2] https://thedfirreport.com/2023/01/09/unwrapping-ursnifs-gifts/



Key Takeaways

In March 2023, America's Cybersecurity & Infrastructure Security Agency published as report on the Royal Ransomware group stating that Royal uses:

"…malware tools and derivatives, such as Ursnif/Gozi, for data aggregation and exfiltration."

Royal Ransomware has been a prominent ransomware threat against global organisations since September 2022, regularly posting victims across multiple sector verticals to their leak site each month. Below is a graph detailing the total number per month. Ursnif is a tool utilised by the group during their intrusions and provided Cyber Threat Intelligence teams an opportunity to identify and track command and control infrastructure linked to this malware.

The use of Ursnif in their attack chain makes Ursnif a malware family worth hunting for, as such this report details the findings of the hunting activity conducted by Bridewell CTI.

Ursnif Hunt Process

Our research began when analysing some relatively new Ursnif IP addresses published by other security researchers. After conducting analysis, we observed notable features that could be leveraged to hunt for new IP addresses in the wild. The Ursnif IP addresses in question were communicating with C2 servers which had an SSL certificate with the following noticeable attributes: the issuer and subject fields.

SSL Certificate Issuer: C=XX, ST=1, L=1, O=1, OU=1, CN=*

SSL Certificate Subject: C=XX, ST=1, L=1, O=1, OU=1, CN=*

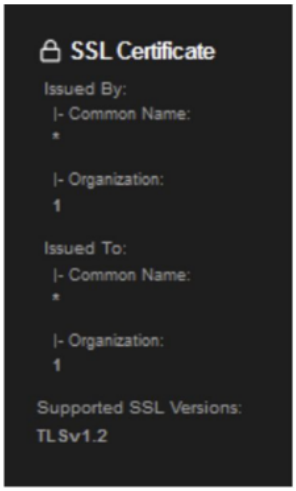


Figure 1. Example Ursnif SSL certificate

Working with this and other features that can be fingerprinted, we were able to identify 72 further servers of interest which matched our new Ursnif hunt rule.

Figure 2. Shodan Results for the Bridewell Ursnif Hunt Rule

Hosting Infrastructure

Looking at the 72 servers, we can identify where they are geographically hosted and by which hosting providers:

Geographical Distribution - Top 3: Germany, Netherlands, Russia

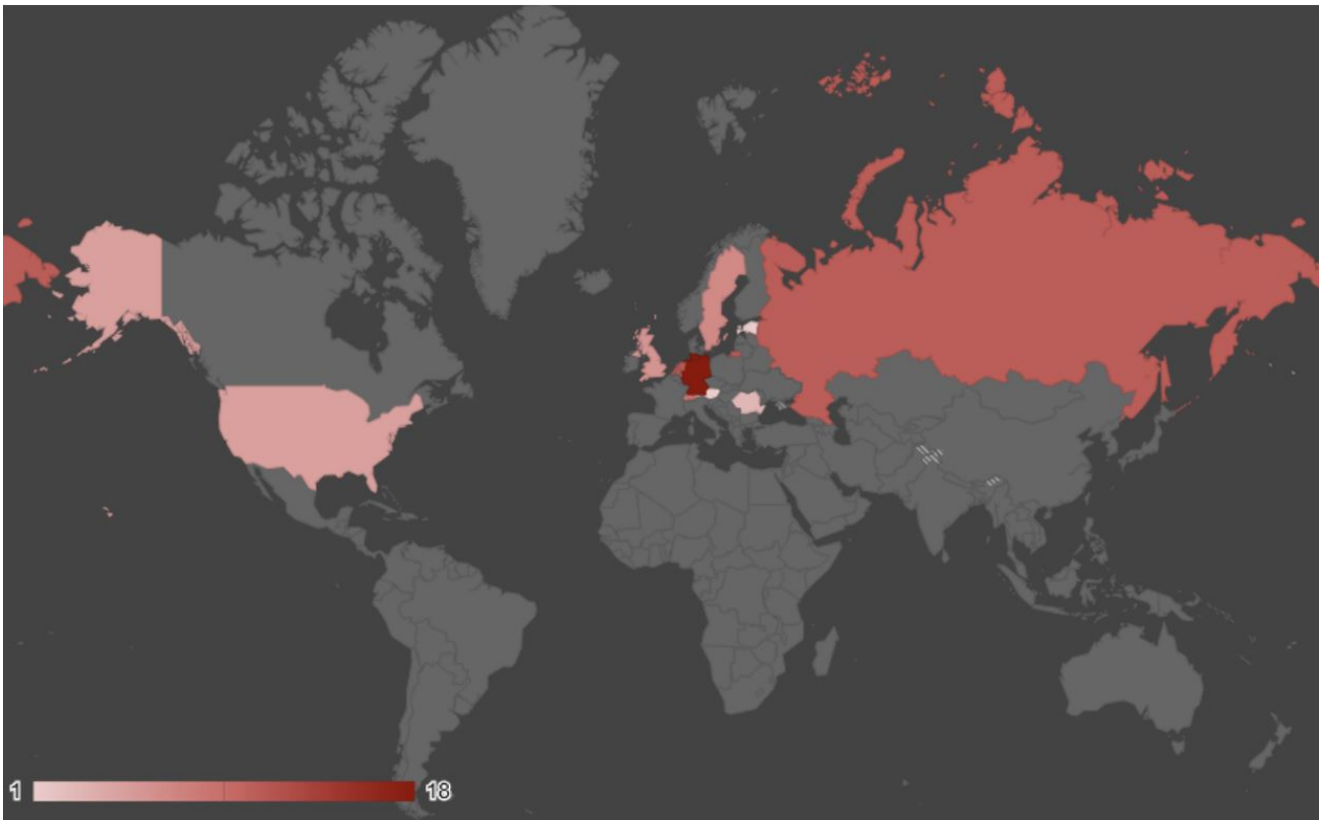


Figure 3. Geographical distribution of Ursnif C2 servers

Hosting Provider - Top 3: servinga GmbH, Datasource AG, GleSYS AB.

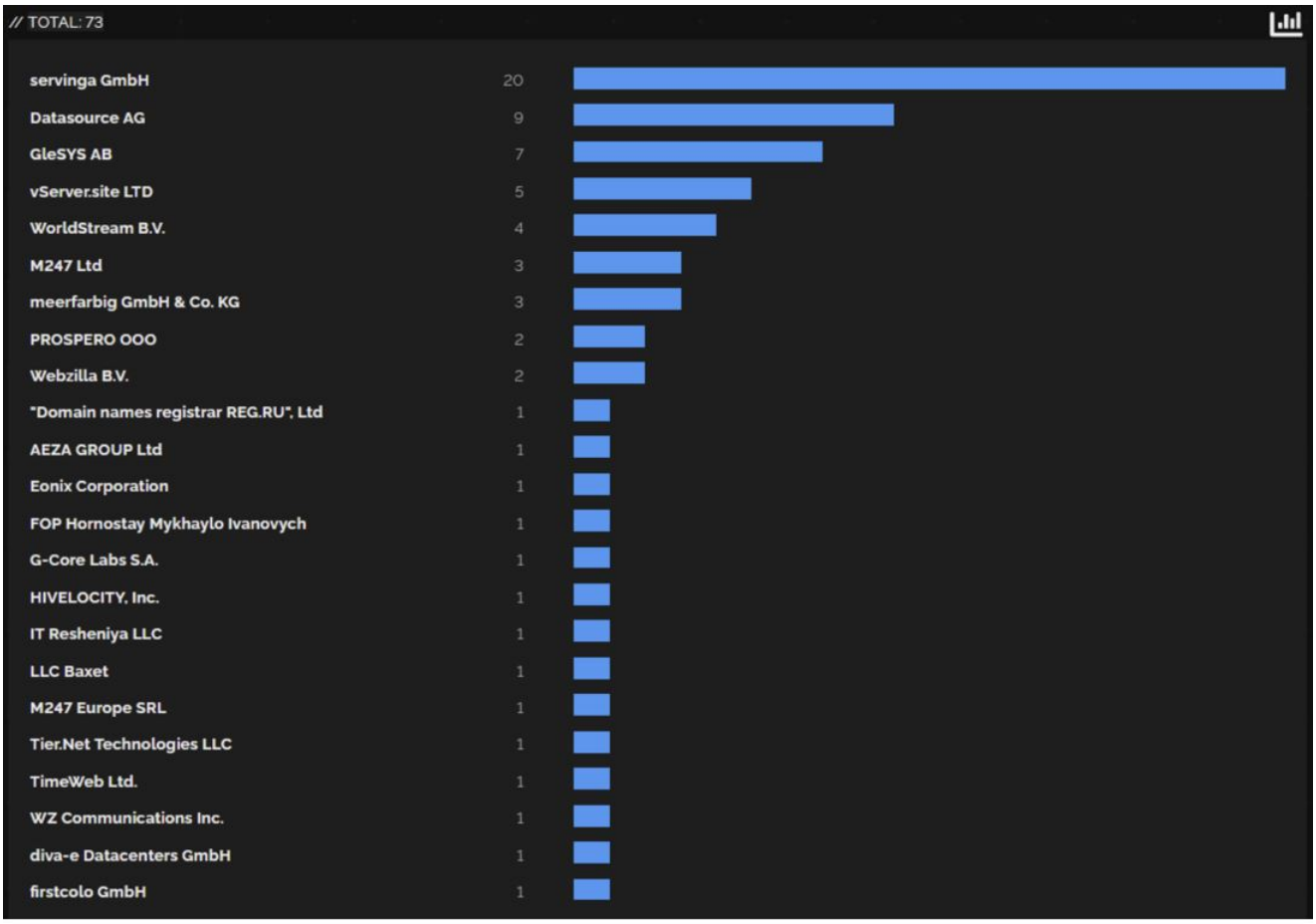


Figure 4. Hosting provider distribution of Ursnif C2 servers

In a report by Mandiant last year, they provided indicators of Ursnif C2's hosted on the ISP Stark Industries Solutions Limited, however it would appear now that the operators of Ursnif have completely migrated from this ISP and diversified amongst many ISPs, who have been associated with many other malware C2s.

Analysing the C2s

After analysing the 23 Ursnif C2 servers that have Ursnif communicating files, 6 have Ursnif files communicating but remain unreported and undetected as Ursnif C2's by Security vendors (at the time of writing this report):

95[.]46[.]8[.]157

193[.]164[.]149[.]143

79[.]133[.]124[.]62

45[.]11[.]181[.]117

92[.]38[.]169[.]142

31[.]214[.]157[.]31

We decided to investigate the IP addresses to understand whether the hunt rule was capturing Ursnif C2s and identifying other pivoting opportunities to enhance our hunt rules by looking at associated domains and hardcoded IPs communicating samples.

The most recently scanned IP in Shodan: 31.214.157[.]31 - Scanned 2023-04-30.

Virus Total Detections: 2/87

Analysing this IP in Virus Total, we can see two communicating files of Interest:

2023-04-12 - 112b84b09d2051376879f697f03190240132b87bbac0d069175bd3039d492f56

2023-03-18 - 282856a51245496390e8c06ed9fa3dff6171aabffa6132dec93a9b4a30b1e524 - MSICBE.tmp

Looking at MSICBE.tmp:

Virus Total Detections: 21/69

After pivoting around in VT, we can see the file's execution parent looks to be a malicious version of LibreOffice, 6ae710.msi.

Virus Total Detections: 3/41

The sample is configured to also beacon to IP 185.189.151[.]38 (tagged as ISFB by ThreatFox). This IP does not appear to be active anymore (not captured by our hunt rule), however by inspecting the scan history in Shodan we can see that the SSL cert with the same attributes matches our hunt rule in Jan 2023.

MSICBE.tmp also pulls down a DLL file:

(c.dll - 2d0f416aa030af708506fea815d4b268ba5a3bdd4680485a65c4cb112bc2ba7d) from 146.70.158[.]105.

Virus Total Detections: 1/88

Sample "92f56" also communicates with the same IP addresses.

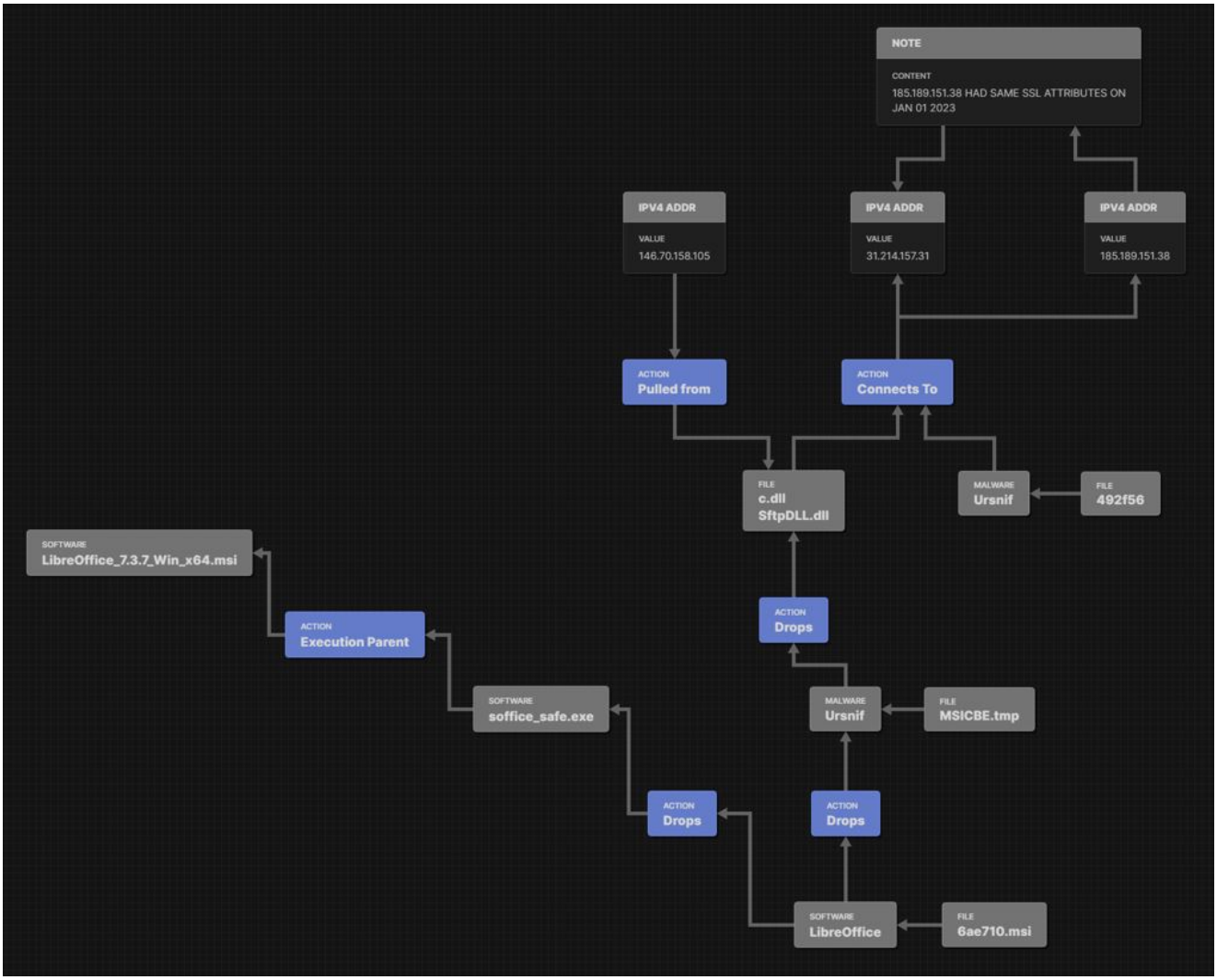


Figure 5. Relationship graph of Ursnif samples communicating with 185.189.151[.]38

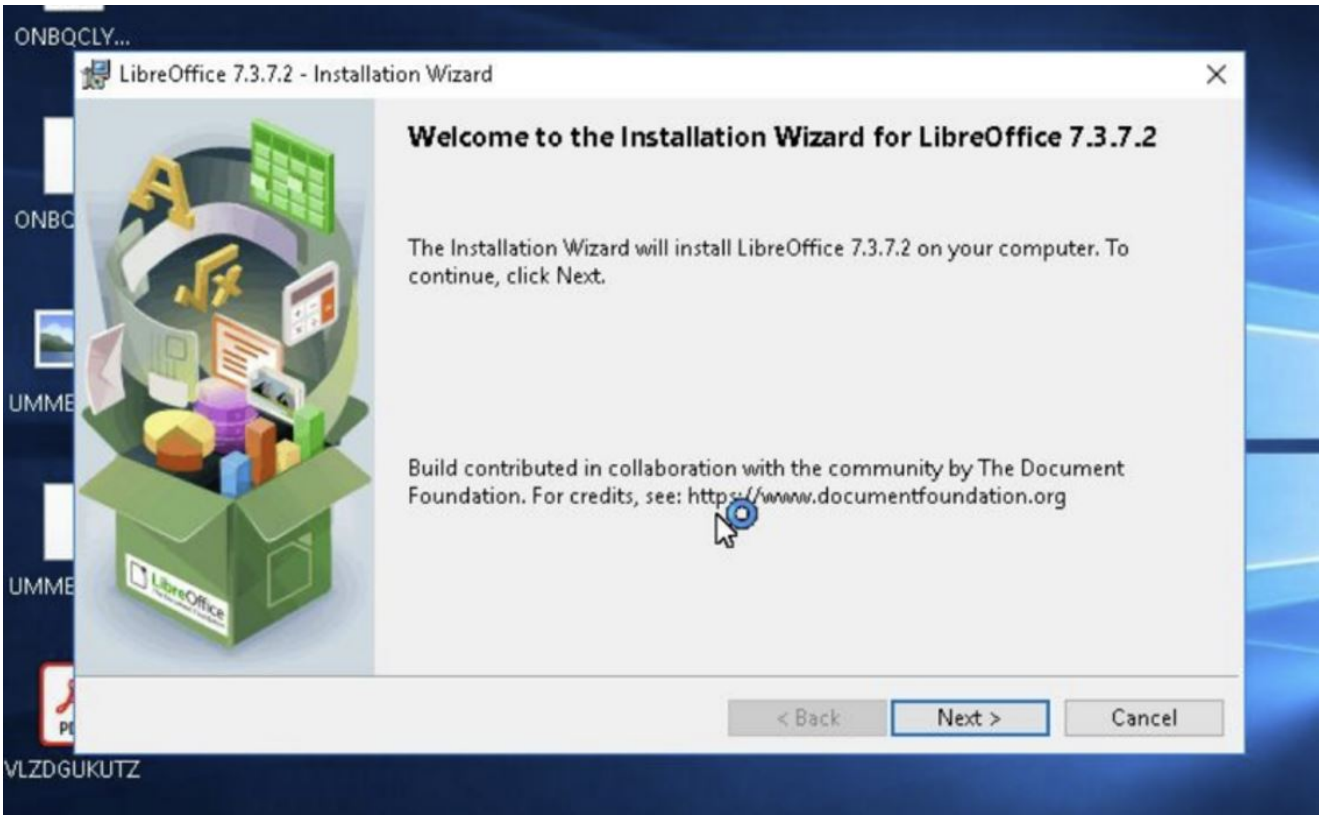


Figure 6. Installation of malicious LibreOffice file

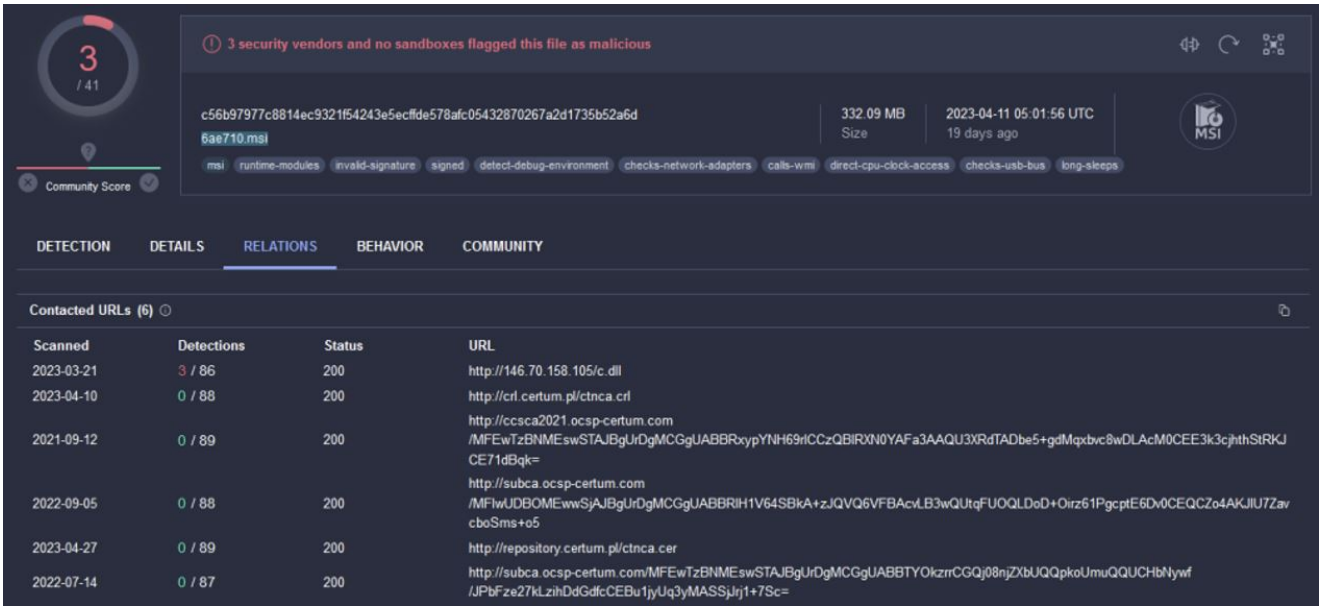


Figure 7. Virus Total Results for LibreOffice file.

Next on our result list was 31.214.157[.]160 - hosted on servinga GmbH, which was identified by Virus Total as Ursnif. From this we were able to pivot to a new hunt rule to identify additional unreported Ursnif C2 servers. This IP has a single .dll file called fxplugins.dll, communicating with it.

Virus Total Detections: 5/89

This file has connection attempts to the following IP addresses:

176.10.111[.]111

176.10.111[.]167

176.10.111[.]173

176.10.111[.]233

31.214.157[.]160

Several of these IP addresses are not captured by our current rule and to understand why, we built another hunt rule, this time pivoting from 176.10.111[.]167 using additional HTTP header information:

The results of this hunt: 55 servers

After deduplicating results against our first hunt rule, we are left with 7 servers that were not caught by the initial SSL hunt rule. This new rule also captures 176.10.111[.]111, one of the C2s used by the fxplugins.dll.

The new IP addresses:

176[.]10[.]111[.]111

91[.]241[.]93[.]152

77[.]91[.]86[.]116

45[.]147[.]200[.]47

62[.]3[.]58[.]57

45[.]155[.]250[.]55

92[.]38[.]169[.]142

Looking at these results further:

45.147.200[.]47 ← resolved from domains www.gameindikdowd[.]ru and jhgfdlkjhaoiu[.]su

Virus Total Detections: 1/87

The first domain has been tagged as ISFB.

Pivoting off the domain, gameindikdowd[.]ru we can see numerous files that have recently used it for C2 traffic.

Communicating Files (14)

Scanned	Detections	Type	Name
2023-01-25	47 / 70	Win32 EXE	20265db7b81ad779f7ccb51df644f0e0.virus
2023-04-04	60 / 69	Win32 EXE	control.exe
2022-11-13	54 / 70	Win32 EXE	c299063b9fc0cbc4521d9ecff2c76cdc.virus
2022-12-20	48 / 71	Win32 EXE	d7f8630ec6da9355b036c8f9a61079ca.virus
2023-01-22	40 / 70	Win32 EXE	c67db3f4ccb3e0c8fa34ad484930c8c3.virus
2023-01-13	55 / 70	Win32 EXE	control.exe
2023-03-22	54 / 69	Win32 EXE	bf3add49ceb633cdfc85bfa7dd747b1e.virus
2023-03-31	40 / 68	Win32 EXE	79e49252ad09ea8bf9e4c897ba20d259.virus
2023-01-27	46 / 70	Win32 EXE	control.exe
2023-01-19	58 / 70	Win32 EXE	main.exe
2023-01-30	43 / 70	Win32 EXE	16d292bb7e7aadcf3e570eb0516dacd7.virus
2023-03-07	58 / 69	Win32 EXE	control.exe.bin
2023-03-07	53 / 68	Win32 EXE	BethesdaNetHelper.exe
2023-01-12	53 / 70	Win32 EXE	7c7d4b4d407592197eb1e582bdbb4615.virus

Figure 8. Ursnif communicating files

Looking at two recent files, control.exe (2023-04-04) and BethesdaNetHelper.exe (2023-03-07), we can identify additional domains used for C2 communications, including any active IP addresses that may not be detected by our hunt rules.

control.exe

gameindikdowd[.]ru

jhgfdlkjhaoiu[.]su

reggy505[.]ru - 109.94.209[.]203

Part of malicious AnyDesk campaign:

uelcoskdi[.]ru - 45.130.147[.]89 - caught by hunt rule

BethesdaNetHelper.exe

gameindikdowd.ru

iujdhsndjfks[.]ru - 45.130.147[.]89 - caught by hunt rule

reggy505[.]ru - 109.94.209[.]203

jhgfdlkjhaoiu[.]su, iujdhsndjfks[.]ru, gameindikdowd.ru domains are all referenced by esentire in their report. Additionally, the above screenshot aligns to the reference of a control.exe that is downloaded and decrypted by the BATLOADER malware in recent campaigns.

Apart from a single IP address, we were able to verify that we are capturing all the IP addresses resolved by these domains and can link these back to activity reported in open source.

Another example of an Ursnif C2 yet to be detected by most antivirus providers is 92.38.169[.]142:

Virus Total Detection: 1/87

A single communicating file called glcheck.exe has been detected as Ursnif on 2023-02-13 and 2023-04-04 - detected as Ursnif.

Virus Total Detection: 38/70

The file also communicates with 185.186.245[.]42 (captured by our hunt rule):

Virus Total Detection: 1/87

Which has the following domains resolving to it:

s28bxcw[.]xyz

8hak4j[.]xyz

dc3txd[.]xyz

2hrbjc[.]xyz

5icvzwz[.]xyz

These domains also have other IP addresses used for redundancy which are also captured by our hunt rule. 95.46.8[.]157 resolved by dantedbkoosov[.]site (3/87 VT) ← 361E.exe (58/70 VT, 2023-04-04) Detected as Ursnif (Product: Letasoft Sound Booster):

Virus Total Detection: 1/87

Findings

Results After conducting our analysis, just under 30% of the infrastructure detected our two hunt rules have files communicating with them that have been detected as Ursnif. Of the infrastructure identified as Ursnif C2's due to the communicating files, the average detection rate by security vendors in Virus Total is just 4.78. 71.3% of the IP addresses currently have

no communicating files. Based on the similarities in shared attributes and hosting providers, we believe there is high likelihood that these IP addresses will be used in the future by Ursnif operators.

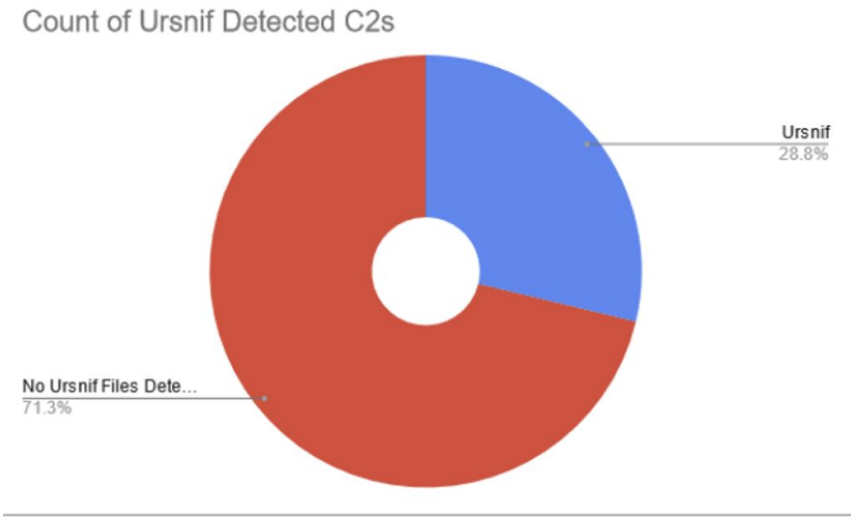


Figure 9. Proportion of identified servers having Ursnif-detected communicating files

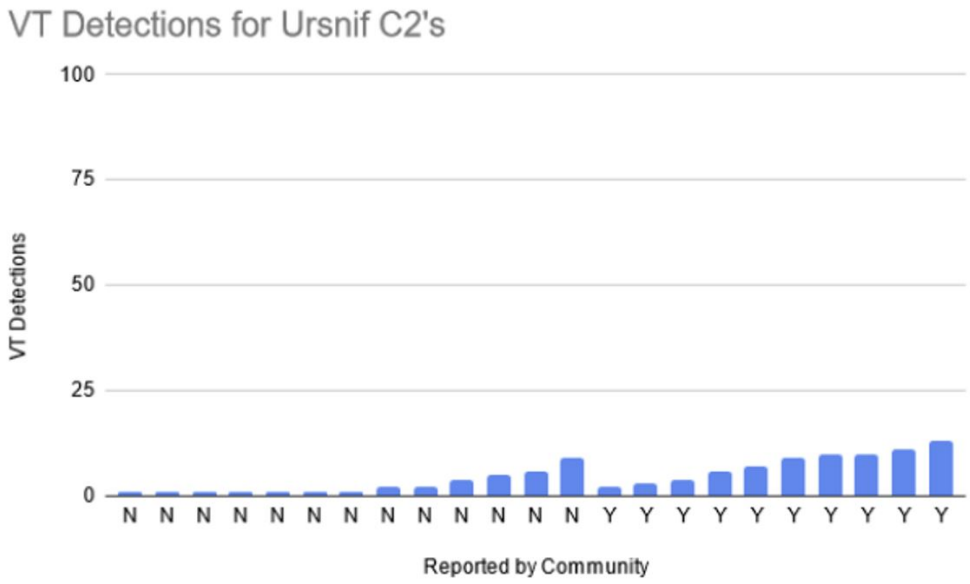


Figure 10. AV Detection rates of Ursnif C2 servers in Virus Total

Conclusion

Ursnif is a backdoor that is used by threat actors in campaigns that lead to ransomware and data exfiltration, posing a viable risk to organisations. The malware is delivered via malicious documents such as macro-enabled office docs or via malicious installers downloaded via Google Ad campaigns.

Bridewell proactively searches for Ursnif C2 infrastructure to protect their customer environments from threats by using a proactive research driven threat intelligence approach to security. As a result, Bridewell CTI provides valuable insight in to our SOC service whilst improving customer's security postures at both a strategic, operational and tactical level.

Ursnif is a longstanding malware that has pivoted from banking trojan to facilitating ransomware intrusions, particular for the Royal ransomware group. This malware communicates to C2 infrastructure, allowing CTI teams to track the operators usage, allowing defenders to respond in a timely manner to any detections within customer environments. Detecting these C2's provides an opportunity to mitigate the impact of ransomware intrusions before its too late.

Mitigation Strategies

To safeguard your organisation against Ursnif and similar threats, it is essential to:

Educate employees about the risks of opening attachments from unknown or suspicious senders.

Ensure that you have a robust application control policy that limits the execution of unauthorised applications from untrusted sources.

Ensure that your organisation uses updated antivirus software and firewalls to detect and prevent Ursnif infections.

Search for the Indicators of Compromise (IoCs) listed in the appendix and set up reference sets for detection within your organisation's security tools.

Implement a Managed Detection and Response (MDR) service to proactively monitor, detect, and respond to threats targeting your organisation.

Leverage a Vulnerability Management service to identify and support remediation of security weaknesses within your organisation's network and systems.

Incorporate a Cyber Threat Intelligence (CTI) services to stay informed of emerging threats and obtain tailored intelligence to enhance your organisation's cybersecurity posture.

Appendix 1 – References

https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/ursnif

https://www.mandiant.com/resources/blog/rm3-ldr4-ursnif-banking-fraud

https://thedfirreport.com/2023/01/09/unwrapping-ursnifs-gifts/

https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-ursnif

Appendix 2 – Indicators

C2 IPs

176[.]10[.]111[.]111

79[.]132[.]132[.]216

185[.]212[.]44[.]83

95[.]46[.]8[.]157

45[.]155[.]249[.]200

77[.]73[.]131[.]105

176[.]10[.]111[.]112

185[.]212[.]47[.]59

185[.]212[.]44[.]146

45[.]155[.]250[.]217

37[.]10[.]71[.]114

91[.]242[.]217[.]113

176[.]10[.]111[.]119

91[.]241[.]93[.]152

45[.]11[.]183[.]24

94[.]247[.]42[.]238

185[.]186[.]244[.]168

77[.]91[.]86[.]116

31[.]214[.]157[.]160

79[.]133[.]180[.]95

185[.]18[.]55[.]106

109[.]230[.]199[.]174

91[.]242[.]219[.]237

45[.]147[.]200[.]47

45[.]155[.]249[.]47

45[.]155[.]249[.]49

176[.]10[.]125[.]84

194[.]58[.]97[.]42

194[.]76[.]224[.]223

185[.]212[.]44[.]76

91[.]242[.]217[.]71

185[.]158[.]248[.]100

109[.]230[.]199[.]110

170[.]130[.]55[.]65

79[.]132[.]134[.]158

79[.]132[.]135[.]249

194[.]76[.]225[.]141

194[.]76[.]224[.]95

91[.]242[.]217[.]120

91[.]242[.]219[.]235

176[.]10[.]111[.]160

62[.]3[.]58[.]57

185[.]186[.]245[.]42

45[.]155[.]250[.]55

176[.]10[.]118[.]153

176[.]10[.]119[.]217

79[.]133[.]124[.]62

45[.]130[.]147[.]89

194[.]76[.]225[.]88

185[.]90[.]162[.]33

185[.]186[.]244[.]108

92[.]38[.]169[.]142

31[.]214[.]157[.]31

109[.]230[.]199[.]248

109.94.209[.]203

176[.]10[.]111[.]111

91[.]241[.]93[.]152

77[.]91[.]86[.]116

45[.]147[.]200[.]47

62[.]3[.]58[.]57

45[.]155[.]250[.]55

92[.]38[.]169[.]142

Domains

s28bxcw[.]xyz

8hak4j[.]xyz

dc3txd[.]xyz

2hrbjc[.]xyz

5icvzwz[.]xyz

gameindikdowd[.]ru

jhgfdlkjhaoiu[.]su

reggy505[.]ru

iujdhsndjfks[.]ru

reggy505[.]ru

jhzzj3[.]xyz

Register for instant alerts to Bridewell threat advisories or to speak with a member of our Cyber Threat Intelligence team.

Author

Joshua Penny

Senior Cyber Threat Intelligence Analyst

Joshua Penny is a CISSP certified Cyber Threat Intelligence Analyst with 5 years' experience working within CTI at Bridewell and previously within the education and research Sector.