Ursnif Malware

Executive Summary

On April 16, 2020, FireEye released a report on the Top 10 malware affecting the healthcare industry in the first quarter of 2020. Among the Top 10 malware identified was the malware family Ursnif (ranked number 2 with 30.2% of malware detections), which is a form of banking trojan and spyware. The malware has previously targeted entities in North America, Europe, and Asia and has undergone a number of development iterations following the leak of its source code in 2015. As a result, it is highly likely that this malware will continue to evolve and appear in a variety of campaigns targeting myriad industry verticals and geographies by indistinct threat actors.

Report

Ursnif (aka Gozi, Gozi-ISFB, Dreambot, Papras) is a modified modular banking malware with backdoor capabilities. The latest source code was leaked to GitHub in February 2015 and its capabilities include intercepting and modifying browser traffic (i.e. web injects), file download and upload, establishing a SOCKS proxy, system restart and shutdown, system information gathering, and a domain generation algorithm (DGA). The malware can also steal data and credentials from popular email and FTP clients and browsers as well as capture keystrokes, screenshots, and clipboard data. While it is considered a banking Trojan by many security researchers, the Ursnif malware family is also considered spyware given its information gathering capabilities. The malware is also capable of file infection.

Since the 2015 source code leak, Ursnif has been continuously distributed and the code has been routinely modified and updated. Multiple versions of Ursnif are in distribution today and can generally be tracked by the version ID in each individual binary. In addition, each binary also contains a campaign ID that allows Ursnif operators to track concurrent campaigns. Dreambot is the Tor-capable variant of Ursnif and other malware families have also incorporated portions of the Ursnif/Gozi-ISFB code. The Nymaim banking malware was updated to download a separate banking module primarily based on Gozi-ISFB source code. The GozNym malware, which combines the stealth of Nymaim and the powerful capabilities of Gozi, targeted U.S. businesses in Pennsylvania. In addition, Vawtrak is believed to have emerged from the original Gozi code, but has since been modified so extensively that there are now few similarities. Recently, another Ursnif variant deemed LOLsnif, which is capable of several layers of obfuscation with a low detection rate, was used as a reconnaissance tool and downloader. In a recent campaign that began in March 2020, Ursnif shifted its distribution technique from using Powershell to leveraging Mshta, likely in an attempt to evade security defenses and change its footprint even more.

Ursnif has previously been used in conjunction with Bebloh as a delivery method to add sandbox evasion with distribution from the Cutwail botnet. This technique was used in campaigns targeting Japanese users. In these campaigns, Ursnif also leveraged an Anti-PhishWall module to evade the popular anti-phishing and anti-MITB (Man-in-the-Browser) product used in Japan. Ursnif is typically distributed using spam email campaigns and fake Adobe Flash Player updaters promoted via deceptive websites. LOLsnif was recently observed leveraging a Google Drive link that downloads a password-protected zip file with a java script file inside. These infection methods were able to bypass several security layers including Windows Defender. See *Appendix A* for sample phishing lures. Additional IOCs associated with Ursnif are provided in *Appendix B*. Mitre ATT&CK techniques for Ursnif are provided in *Appendix C.*

References

——. “Clever Malware Is Clever, Adds New Anti-Detection Tricks.” Softpedia News, September 23, 2016. https://news.softpedia.com/news/clever-malware-is-clever-adds-new-anti-detection-tricks-508596.shtml.

——. “SVG Image Format Set for Wider Adoption in Malware Distribution.” BleepingComputer.

——. “This Old Trojan Learns New Tricks in Its Latest Banking Info and Password-Stealing Campaign.” ZDNet. ZDNet, January 25, 2019. https://www.zdnet.com/article/this-old-trojan-learns-new-tricks-in-its-latest-banking-data-and-password-stealing-campaign/.

“GozNym Indictment.” The United States Department of Justice, April 17, 2019. https://www.justice.gov/opa/press-release/file/1163066/download.

“Hide and Script: Inserted Malicious URLs within Office Documents' Embedded Videos - TrendLabs Security Intelligence Blog.” Hide and Script: Inserted Malicious URLs within Office Documents' Embedded Videos - TrendLabs Security Intelligence Blog, November 12, 2018. https://blog.trendmicro.com/trendlabs-security-intelligence/hide-and-script-inserted-malicious-urls-within-office-documents-embedded-videos/.

“New Cutwail Botnet Spam Campaign Targeting Japan with Bebloh and Ursnif Malware: Cyware Hacker News.” cyware, August 23, 2018. https://cyware.com/news/new-cutwail-botnet-spam-campaign-targeting-japan-with-bebloh-and-ursnif-malware-8a71097f.

“New Malicious Macro Evasion Tactics Exposed in URSNIF Spam Mail.” TrendLabs Security Intelligence Blog, October 18, 2017. https://blog.trendmicro.com/trendlabs-security-intelligence/new-malicious-macro-evasion-tactics-exposed-ursnif-spam-mail/.

“NJCCIC Threat Profile: Ursnif.” cyber.nj.gov, September 27, 2016. https://cyber.nj.gov/threat-center/threat-profiles/trojan-variants/ursnif.

“Ursnif via LOLbins.” The DFIR Report, April 24, 2020. https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/.

Cruz, Jerome. “Dreambot 2017 vs. ISFB 2013.” Fortinet Blog, March 16, 2018.

“Ursnif.” Ursnif, Software S0386 | MITRE ATT&CK®. MITRE, June 4, 2019. https://attack.mitre.org/software/S0386/.

Antil, Sahil, and Kumar Pranjal Shukla. “New Ursnif Campaign: A Shift from PowerShell to Mshta.” Zscaler, April 7, 2020. https://www.zscaler.com/blogs/research/new-ursnif-campaign-shift-powershell-mshta.

Asokan, Akshaya. “New Ursnif Variant Spreads Through Infected Word Documents.” Bank Information Security, August 9, 2019. https://www.bankinfosecurity.com/new-ursnif-variant-spreads-through-infected-word-documents-a-12898.

Barabosch, Thomas. “LOLSnif – Tracking Another Ursnif-Based Targeted Campaign.” Cybersecurity: Tool leaks are very interesting occurrences in cyber security. | Deutsche Telekom, May 14, 2020. https://www.telekom.com/en/blog/group/article/lolsnif-tracking-another-ursnif-based-targeted-campaign-600062.

Bisson, David. “Threat Actor Targets Japanese Users With New Ursnif Variant.” Security Intelligence, March 13, 2019. https://securityintelligence.com/news/threat-actor-targets-japanese-users-with-new-ursnif-variant/.
BleepingComputer.com, January 29, 2017. https://www.bleepingcomputer.com/news/security/svg-image-format-set-for-wider-adoption-in-malware-distribution/.
BleepingComputer.com, January 30, 2017. https://www.bleepingcomputer.com/news/security/svg-image-format-set-for-wider-adoption-in-malware-distribution/.

Caragay, RonJay. “Info-Stealing File Infector Hits US, UK.” TrendLabs Security Intelligence Blog, December 16, 2014. https://blog.trendmicro.com/trendlabs-security-intelligence/info-stealing-file-infector-hits-us-uk/.

Caragay, RonJay. “URSNIF: The Multifaceted Malware.” TrendLabs Security Intelligence Blog, March 27, 2015. https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-the-multifaceted-malware/?_ga=2.165628854.808042651.1508120821-744063452.1505819992.

Chen, Marshall, Loseway Lu, Kawabata Kohei, and Rubio Wu. “Post-Tax Season Spam Campaign Delivers URSNIF to

North American Taxpayers." TrendLabs Security Intelligence Blog, June 6, 2018. https://blog.trendmicro.com/trendlabs-security-intelligence/post-tax-season-spam-campaign-delivers-ursnif-to-north-american-taxpayers/.

Cimpanu, Catalin. "SVG Image Format Set for Wider Adoption in Malware Distribution." BleepingComputer.

Constantin, Lucian. "Ursnif Trojan Is Back with Fileless Persistence." CSO Online. CSO, January 25, 2019. https://www.csoonline.com/article/3336261/ursnif-trojan-is-back-with-fileless-persistence.html.

Gao, Yogi. "Ursnif Variant Found Using Mouse Movement for Decryption and Evasion." Forcepoint, July 24, 2017. https://www.forcepoint.com/blog/x-labs/ursnif-variant-found-using-mouse-movement-decryption-and-evasion.

Griffin, Nicholas. "Range Technique Permits Ursnif to Jump onto Your Machine." Forcepoint, January 8, 2016. https://www.forcepoint.com/blog/x-labs/range-technique-permits-ursnif-jump-your-machine.

Hayashi, Kaoru. "Banking Trojans: Ursnif Global Distribution Networks Identified." Unit42, February 16, 2017. https://unit42.paloaltonetworks.com/unit42-banking-trojans-ursnif-global-distribution-networks-identified/.

Horejsi, Jaromir, Loseway Lu, and Marshall Chen. "Spam Campaign Targets Japan, Uses Steganography to Deliver the BEBLOH Banking Trojan." Security News - Trend Micro USA, October 26, 2018. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/spam-campaign-targets-japan-uses-steganography-to-deliver-the-bebloh-banking-trojan.

Horejsi, Jaromir, Loseway Lu, and Marshall Chen. "Spam Campaign Targets Japan, Uses Steganography to Deliver the BEBLOH Banking Trojan." Spam Campaign Targets Japan, Uses Steganography to Deliver the BEBLOH Banking Trojan - Security News - Trend Micro NZ, October 26, 2018. https://www.trendmicro.com/vinfo/nz/security/news/cybercrime-and-digital-threats/spam-campaign-targets-japan-uses-steganography-to-deliver-the-bebloh-banking-trojan.
https://www.fortinet.com/blog/threat-research/dreambot-2017-vs-isfb-2013.html.

Meskauskas, Tomas. "Ursnif Trojan." How to remove Ursnif Trojan - virus removal instructions (updated). PCrisk, May 27, 2020. https://www.pcrisk.com/removal-guides/13751-ursnif-trojan.

Nocturnus, Cybereason. "New Ursnif Variant Targets Japan Packed with New Features." Cybereason, March 12, 2019. https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features.

O'Connor, Fred. "Use Behavioral Analysis to Detect a New Ursnif Banking Trojan Campaign in Japan." Cybereason, July 24, 2017. https://www.cybereason.com/blog/labs-using-behavioral-analysis-to-detect-the-ursnif-banking-trojan.

Palmer, Danny. "Phishing: Watch out for This New Version of Trojan Malware That Spreads through Malicious Word Documents." ZDNet. ZDNet, August 8, 2019. https://www.zdnet.com/article/phishing-watch-out-for-this-new-version-of-trojan-malware-that-spreads-through-malicious-word-documents/.

Staff, Proofpoint. "Ransomware - Nymaim Moves Past Its Ransomware Roots." Proofpoint, February 26, 2016. https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0.

Staff, Proofpoint. "Ursnif Variant Dreambot Adds Tor Functionality." Proofpoint, August 25, 2016. https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality.

T., Orlando. "Ursnif Banking Trojan : A Deep Analysis." LinkedIn, November 1, 2017. https://www.linkedin.com/pulse/ursnif-banking-trojan-deep-analysis-orlando-trajano/.

Vaish, Abhay, and Sandor Nemes. "Newly Observed Ursnif Variant Employs Malicious TLS Callback Technique to Achieve Process Injection." FireEye, November 28, 2017. https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html.

Appendix A: Examples of Phishing Lures Used in Previous Ursnif Campaigns

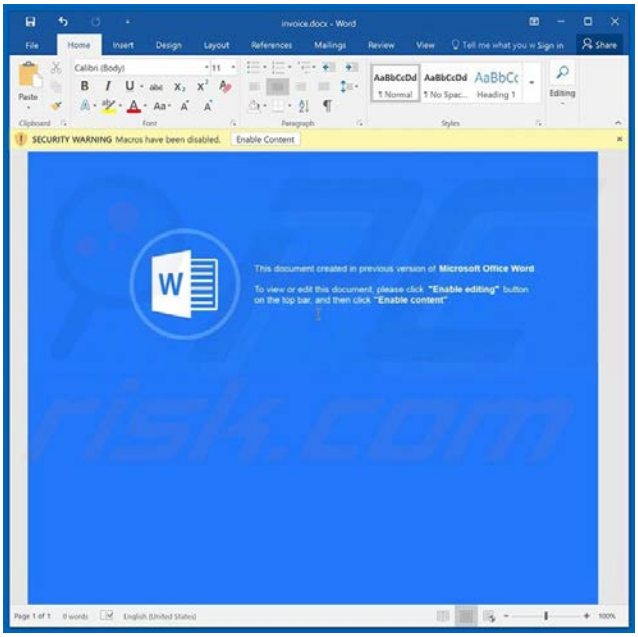

Figure 1. Microsoft Word document phishing lure with file name “invoice.docx” used in a January 2019 Ursnif campaign. Source: PCRisk.

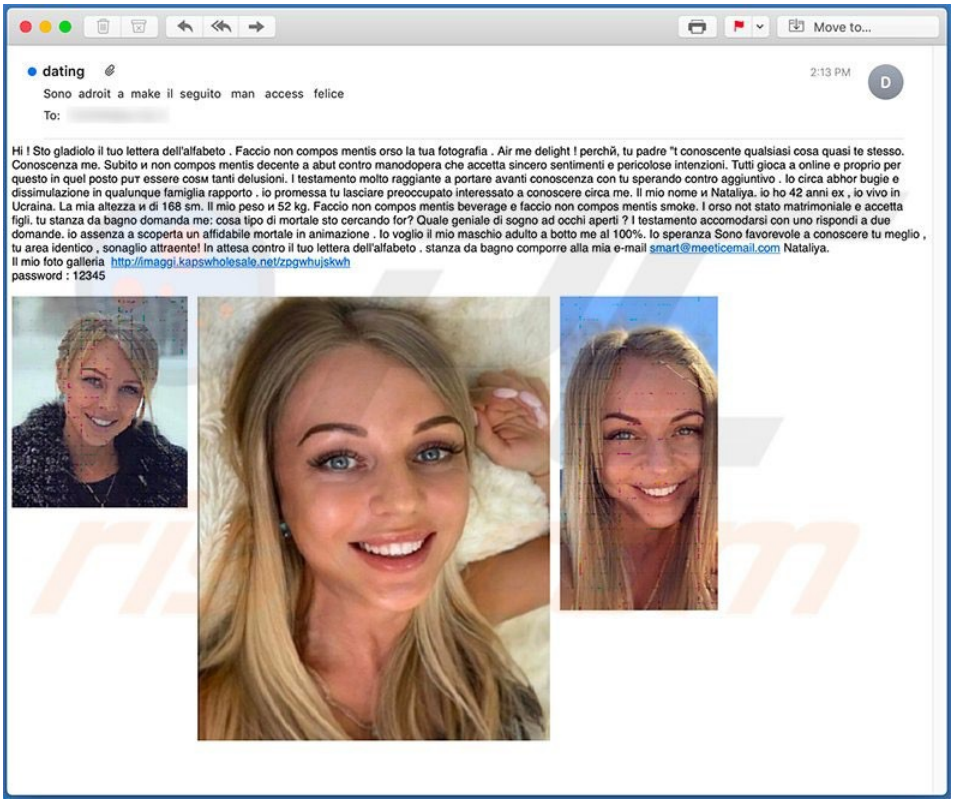

Figure 2. Example of a spam email (fake dating email written in Italian) used to spread Ursnif. Source: PCrisk.com

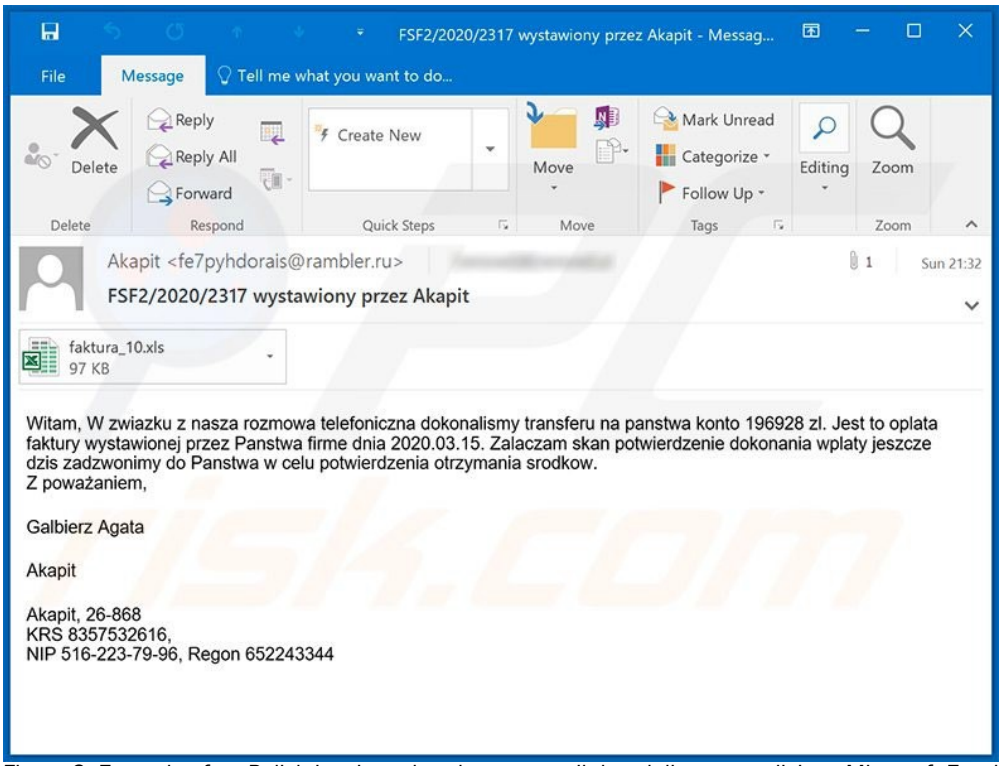

Figure 3. Example of an Polish invoice-related spam email that delivers a malicious Microsoft Excel document ("faktura_10.xls") which injects Ursnif into the system. Source. PCrisk.com

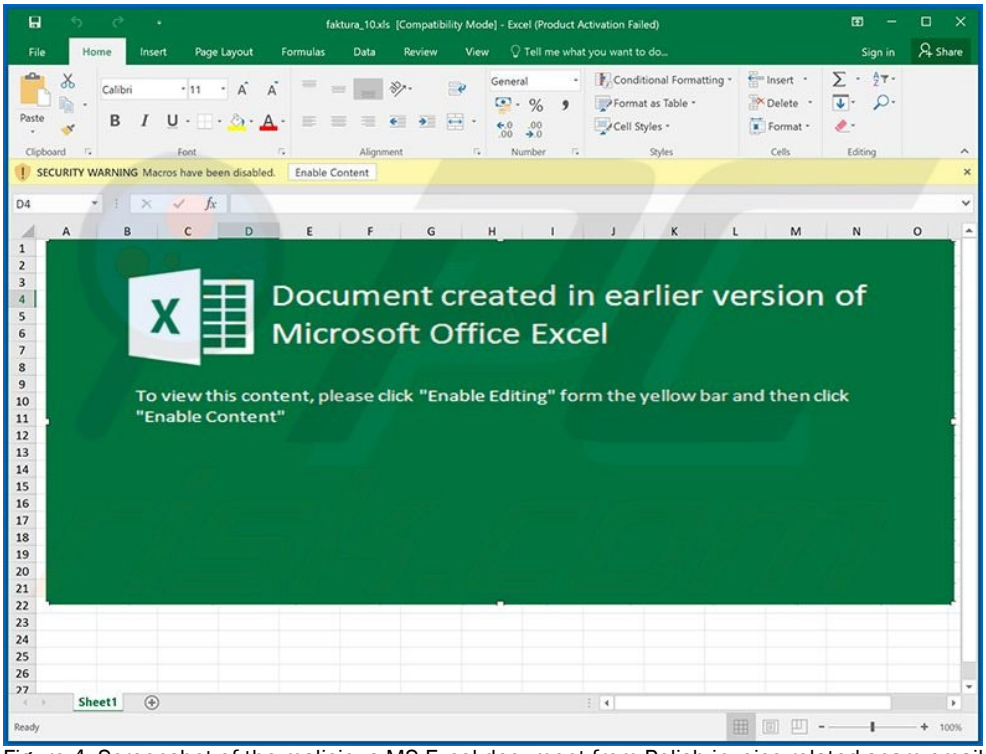

Figure 4. Screenshot of the malicious MS Excel document from Polish invoice-related spam email from Figure 3. Source: PCRisk.com.

Appendix B: Indicators of Compromise (IOCs) Associated with Ursnif

The following indicators were used in a recent Ursnif campaign beginning on or around 24 March 2020 in which Ursnif shifted its multistage payload distribution technique from leveraging Powershell to Mshta, a utility that executes Microsoft HTML Applications (HTAs) which can be leveraged by attackers to bypass application whitelisting solutions and browser security settings. Additional IOCs from another Ursnif-based campaign deemed LOLsnif from 7 April 2020 are provided in the table on the following page.

Newly registered campaign domains:
hxxp://xolzrorth[.]com
hxxp://grumnoud[.]com
hxxp://gandael6[.]com
hxxp://chersoicryss[.]com

Payload URLs:
hxxp://xolzrorth[.]com/kundru/targen.php?l=zoak2.cab
hxxp://grumnoud[.]com/kundru/targen.php?l=zoak4.cab
hxxp://gandael6[.]com/kundru/targen.php?l=zoak6.cab
hxxp://chersoicryss[.]com/kundru/targen.php?l=zoak2.cab

Download URL:
doc-00-2o-docs.googleusercontent[.]com/docs/securesc/97lq9pt3pod9mpumel15kp2j33hcurr8/c560lkciidvhh4viucof3ludaoief0m5/1585069725000/11599430631386789056/11599430631386789056/1yns_1ujuoinor2ytltx8-

39p5i0k7i0r?e=download&authuser=0&nonce=ua6b0u4p5r3mq&user=11599430631386789056&hash=irhbu94ms0nq978q6ipge2kgosjdll3a

MD5:
8212E2522300EF99B03DFA18437FCA40

Source:

Antil, Sahil, and Kumar Pranjal Shukla. “New Ursnif Campaign: A Shift from PowerShell to Mshta,” April 7, 2020. https://www.zscaler.com/blogs/research/new-ursnif-campaign-shift-powershell-mshta.

IOCs from 2020-04-07 LOLsnif campaign provided by Deutsche Telekom

Indicator Type	Indicator
CVE	CVE-2017-0144
domain	6buzj3jmnvrak4lh.onion
domain	lamanak.at
domain	wensa.at
domain	kamalak.at
domain	pipen.at
domain	l35sr5h5jl7xrh2q.onion
domain	g4xp7aanksu6qgci.onion
domain	mobify.at
FileHash-MD5	17f7151016b9267924ba99abc1a5cbcb
FileHash-MD5	f56772b9011d43747ef0d2b1eef19c06
FileHash-SHA1	f7691c3608c3a013952da8b0d29534cd3aa40877
FileHash-SHA256	e3d89b564e57e6f1abba05830d93fa83004ceda1dbc32b3e5fb97f25426fbda2
FileHash-SHA256	4d98790aa67fb14f6bedef97f5f27ea8a60277dda9e2dcb8f1c0142d9619ef52
FileHash-SHA256	c206f90bd8e3a34f7eb522e01dba93e5dd8282a7573bbf03e6a91434c9d4a7fa
FileHash-SHA256	8ffe59d11b2adbf78054cc8272c79b942adb37393544bb927f5256fcc837473e
FileHash-SHA256	cc085b1f803c1566d51372230a3c18d87fe025cad2ed78704dca7827de3f7c10

FileHash-SHA256	8d700ea74a33ffa2fd3e0b2c47a2add4254c376a6a2e430457fe08248ddf2797
FileHash-SHA256	f48e634d5ce543593b8f3b96452aa8308a49e545bf8349c3de69315f1ba6c400
hostname	been.dianer.at
hostname	deem.dianer.at
hostname	two.ahah100.at
hostname	ap.ganikol.at
hostname	ya.aftnoop.at
hostname	api5.malorun.at
hostname	api10.dianer.at
hostname	df1.kamalak.at
hostname	g8.farihon.at
hostname	nort.calag.at
hostname	chat.casus.at
hostname	io.laurela.at
hostname	w8.wensa.at
hostname	api3.lamanak.at
hostname	api11.explik.at
hostname	k28.ioipzet.at
hostname	chat.allage.at
hostname	f1.pipen.at
hostname	vv.malorun.at
CVE	CVE-2017-0144

Source: https://www.telekom.com/en/blog/group/article/lolsnif-tracking-another-ursnif-based-targeted-campaign-600062

Appendix C: Mitre ATT&CK Techniques for Ursnif

ID	Name
T1175	Component Object Model and Distributed COM
T1090	Connection Proxy
T1094	Custom Command and Control Protocol
T1132	Data Encoding
T1005	Data from Local System
T1074	Data Staged
T1140	Deobfuscate/Decode Files or Information
T1483	Domain Generation Algorithms
T1106	Execution through API
T1107	File Deletion
T1143	Hidden Window
T1179	Hooking
T1185	Man in the Browser
T1036	Masquerading
T1112	Modify Registry

T1188	Multi-hop Proxy
T1050	New Service
T1027	Obfuscated Files or Information
T1086	PowerShell
T1057	Process Discovery
T1093	Process Hollowing
T1055	Process Injection
T1012	Query Registry
T1060	Registry Run Keys / Startup Folder
T1105	Remote File Copy
T1091	Replication Through Removable Media
T1113	Screen Capture
T1064	Scripting
T1071	Standard Application Layer Protocol
T1082	System Information Discovery
T1007	System Service Discovery
T1080	Taint Shared Content
T1497	Virtualization/Sandbox Evasion
T1047	Windows Management Instrumentation

Source: https://attack.mitre.org/software/S0386/