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

isc.sans.edu/forums/diary/German+language+malspam+pushes+Ursnif/25732/

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.

3		Re: /	Auftrag	gsbestätigung	: 17/109	5535 ** 17	524923148215	- Mozilla Th	underbird		• - • ×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>M</u> essage	<u>T</u> ools	<u>H</u> elp					
							ゥ Re	ply 🦘 Re	eply All 🗸	→ Forward	More 🗸
Fro	om						☆	Date T	ue, 21 Jar	2020 07:21	:57 +0100
Subje	ect Re:	Auftra	igsbe	stätigung:	17/10	95535 *	** 1752492	3148215			
	То										
Guten Morgen,											
siehe	e Anhai	ng.									I
		-									I
zip p	ass 55:	0									I
Mit f	reundli	chen Gr	rüßen								I
	a										— I
From: Sent:	Гhu. 04 Ja	n 2018 08	:44:02 +	0000							I
To:											
- 0	1 atta	chment	: Flies	enlegerbetr	ieb_		.zip 115	KB			🖬 Save 🗸
😑 Fl	iesenle	gerbetr	ieb_		.zip	115 KB					

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

3			Re: V	VG: famila-Ma	rkt Gifho	rn am 17	12.2015	Mozilla T	hunderbi	ird		+ ×
<u>F</u> ile	<u>E</u> dit	View	<u>G</u> o	<u>M</u> essage	<u>T</u> ools	<u>H</u> elp						
Fro	m							ל Reply	や Rep	ly All 🗸	→ Forwa	ard More 🗸
Subie	ect Re	: WG: f	amila	-Markt Gif	horn a	m 17.1	2.2015		Date Tu	e. 21 la	n 2020 09	:15:36 +0100
	То									-, ,-		
Cuto	n Mor											
Gute	n Mor	gen,										
Bitte b	eachten	Sie den An	hang.									
zip p	ass 33	3										
Mit fre	undlich	en Grüßen,										
From:												
Sent:	Tue, 15 D	ec 2015 07	:40:20 +	0000								
Subje	t: WG: f	amila-Mark	ct Gifho	rn am 17.12.201	5							
Hallo	Herr											
danka	€Ā1/.e 160	o Apfrogo	Im Cola	ondon hoho ioh :	tu Ibran ai	ntolnon Ar	mortungo	Erogon Ct	ollung gond	mmon Cr	llton woitoro	
• 0	1 atta	chment	: CHEI	MISCHE_FAB	RIK.zip	114 KB						🖬 Save 🗸
😑 Cl	CHEMISCHE_FABRIK.zip 114 KB											

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

3			Re:	Achtung h	ier komn	nt ein Ang	ebot!!	- Mozilla Thu	underbird				+ - • ×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>M</u> essage	Tools	<u>H</u> elp							
Fro	m Her	r			습	,		ን Reply	🏷 Reply	All 🗸	~	Forward	d More 🗸
Subject Re: Achtung hier kommt ein Angebot!! Date Tue, 21 Jan 2020 12:05:06 +0									5:06 +0100				
	То			☆									
Gute	n Tag.												1
Im A Falls zip p Mit fr From: Sent: \ To:	Im Anhang finden Sie die Datei! Falls Sie noch Fragen haben, dann wenden Sie sich bitte vertrauensvoll an mich. zip pass 111 Mit freundlichen . From: Sent: Wed, 16 Aug 2017 10:32:00 +0000 To:												
- 0	1 attac	hment	: Lazz	erini.zip 114	1 KB		_						Save 🗸
😑 La	zzerini	zip 11	4 KB										

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 <u>here</u>, which contains infections from 2019. Of note, the follow-up malware for this Ursnif infection was another Ursnif variant.

(http.request or ssl.handshake.type == 1) and !(ssdp)								
Time Dst	Dst port	Host	Info					
→ 2020-01-21 21:18 80.85.157.246	80	emblareppy.com	GET /gunshu/lewasy.php					
2020-01-21 21:19 40.74.35.71	80	settings-win.data.micro	GET /images/EbUh8xIpG_					
2020-01-21 21:19 80.85.153.218	80	pzhmnbarguerite4819.com	GET /images/KnSeZFKNBI					
2020-01-21 21:20 40.74.35.71	80	settings-win.data.micro	GET /images/JyCc0SNuIc					
2020-01-21 21:21 95.169.181.33	80	n60peablo.com	GET /images/EHCYIyTPim					
2020-01-21 21:21 80.85.153.218	80	pzhmnbarguerite4819.com	GET /images/UkqxnMR2ns					
2020-01-21 21:22 40.74.35.71	80	settings-win.data.micro	GET /images/aC0UEXwrsE					
2020-01-21 21:22 95.169.181.33	80	n60peablo.com	GET /images/o3pphY9d6H					
2020-01-21 21:22 95.169.181.33	80	n60peablo.com	GET /favicon.ico HTTP/					
2020-01-21 21:22 95.169.181.33	80	n60peablo.com	GET /images/BZWCpvPGmC					
2020-01-21 21:22 95.169.181.33	80	n60peablo.com	GET /images/GOaMxLJBqk					
2020-01-21 21:23 40.74.35.71	443	settings-win.data.micro…	Client Hello					
2020-01-21 21:23 45.141.103.204	443	nk47yicbnnsi.com	Client Hello					
2020-01-21 21:23 104.193.252.15	7 80	104.193.252.157	GET /fonelsid.rar HTTP					
2020-01-21 21:24 45.141.103.204	443	nk47yicbnnsi.com	Client Hello					
2020-01-21 21:24 45.141.103.204	443	nk47yicbnnsi.com	Client Hello					
2020-01-21 21:24 216.58.206.14	80	google.com	GET / HTTP/1.1					
2020-01-21 21:24 172.217.22.68	80	www.google.com	GET / HTTP/1.1					
2020-01-21 21:29 80.249.145.116	80	limpopo.at	GET /images/0g4F36cKUx					
2020-01-21 21:29 109.175.7.8	80	estate-advice.at	GET /images/EIjW7fDwiX					
2020-01-21 21:29 5.56.73.146	80	sweetlights.at	GET /g32.bin HTTP/1.1					
2020-01-21 21:29 5.56.73.146	80	sweetlights.at	GET /g64.bin HTTP/1.1					
2020-01-21 21:30 5.56.73.146	80	estate-advice.at	POST /images/Pm9GzCvGa					
2020-01-21 21:30 5.56.73.146	80	estate-advice.at	POST /images/mkeqHuiYN					
2020-01-21 21:34 185.95.185.58	80	estate-advice.at	GET /images/zUU3QnWa9R					
2020-01-21 21:34 185.95.185.58	80	estate-advice.at	GET /images/murG2rwA81 *					

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.

Registry Editor – 🗆 🗙										
File Edit View Favorites Help										
Computer\HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\11FA388A-3C6C-6B5A-CED5-30CFE2D96473										
Computer\HKEY_CURRENT_USER\Software	are\AppDataLow\So Name (Default) (B01E9FCC-4 (B01E9FCC-4) (E3D1258E-E (E3D1258E-E)	ftware\Microsoft\11 Type REG_SZ REG_BINARY REG_BINARY REG_SZ REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_QWORD	.388A-3C6C-6B5A-CED5-30CFE2D96473 Data (value not set) b4 78 59 4f bd d0 d5 01 ee d8 f9 af b2 d0 d5 01 mshta "about: <hta:application><script></script></hta:application>							

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:

<u>c7f801c491d705cd5e6a202c7c5084874235e19b5505d8e0201111cb3789a9c8</u>

- 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 <u>here</u>.

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