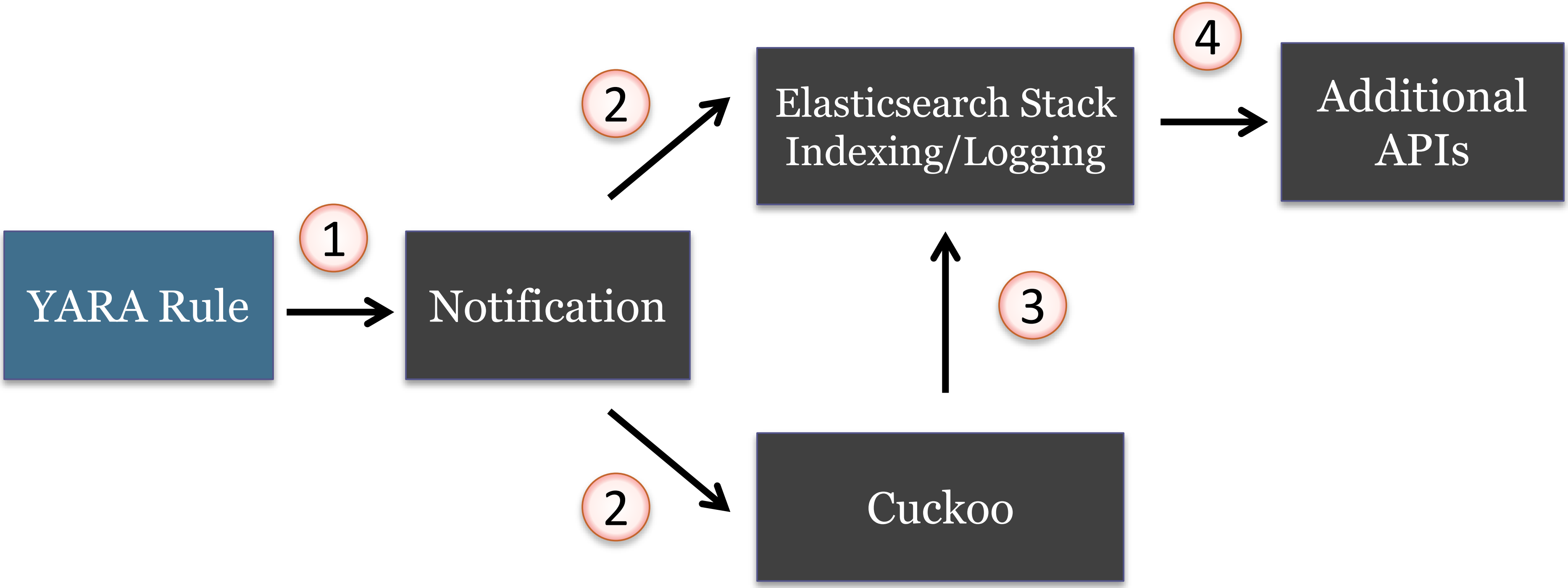
Tracking Threat Actors through YARA Rules and Virus Total

Kevin Perlow- Booz Allen Hamilton

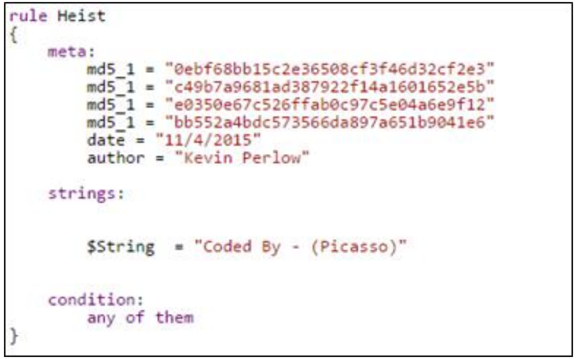
Allen Swackhamer- Target Corporation

Automation and Collection Workflow



YARA Rules - Purpose

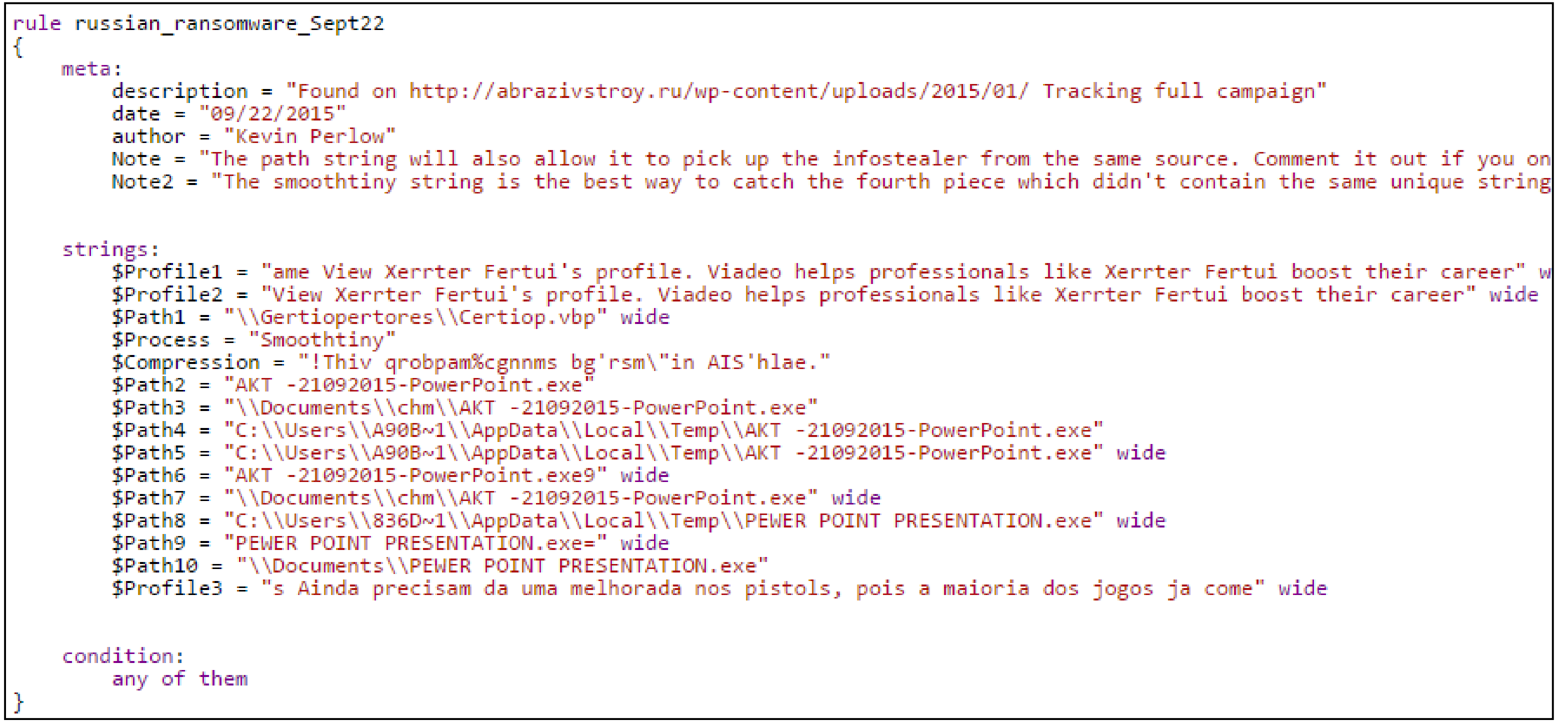
- Track Campaigns
  - Strings
  - Static Indicators
  - Compilation Artifacts
  - Opcode signatures
- Categorize Malware
  - Family / Variants



```
rule Heist
{
    meta:
        md5_1 = "0ebf68bb15c2e36508cf3f46d32cf2e3"
        md5_1 = "c49b7a9681ad387922f14a1601652e5b"
        md5_1 = "e0350e67c526ffab0c97c5e04a6e9f12"
        md5_1 = "bb552a4bdc573566da897a651b9041e6"
        date = "11/4/2015"
        author = "Kevin Perlow"

    strings:


        $String  = "Coded By - (Picasso)"


    condition:
        any of them
}
```

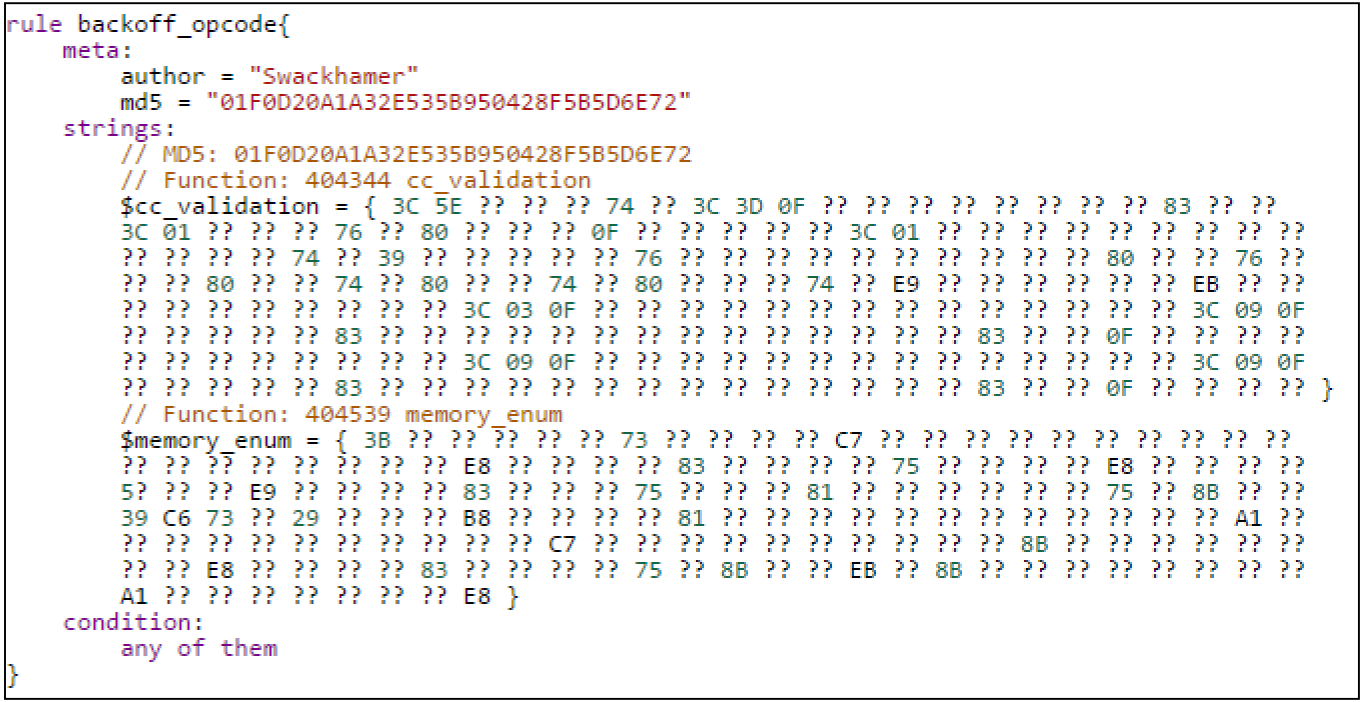
Basic YARA rule for tracking a crimeware crypter

YARA Rules- Examples



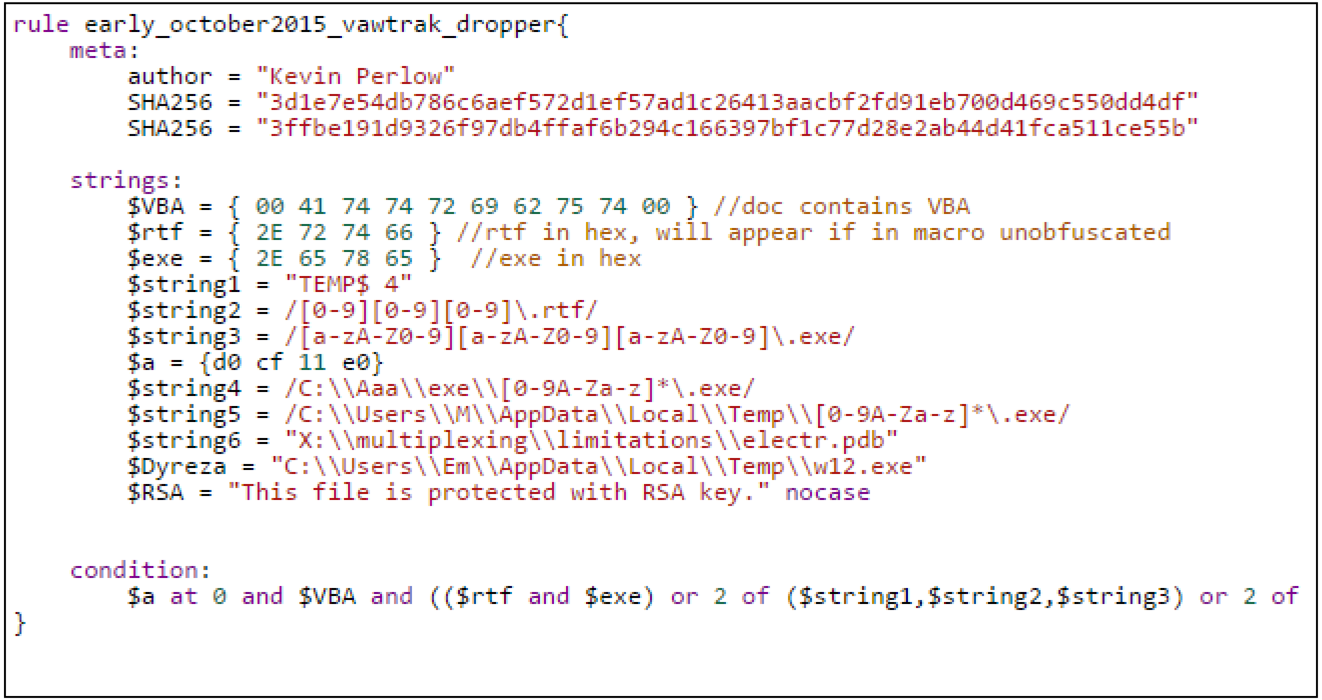
```
rule russian_ransomware_Sept22
{
    meta:
        description = "Found on http://abrazivstroy.ru/wp-content/uploads/2015/01/ Tracking full campaign"
        date = "09/22/2015"
        author = "Kevin Perlow"
        Note = "The path string will also allow it to pick up the infostealer from the same source. Comment it out if you on
        Note2 = "The smoothtiny string is the best way to catch the fourth piece which didn't contain the same unique string


    strings:
        $Profile1 = "ame View Xerrter Fertui's profile. Viadeo helps professionals like Xerrter Fertui boost their career" w
        $Profile2 = "View Xerrter Fertui's profile. Viadeo helps professionals like Xerrter Fertui boost their career" wide
        $Path1 = "\\Gertiopertores\\Certiop.vbp" wide
        $Process = "Smoothtiny"
        $Compression = "!Thiv qrobpam%cgnnms bg'rsm\"in AIS'hlae."
        $Path2 = "AKT -21092015-PowerPoint.exe"
        $Path3 = "\\Documents\\chm\\AKT -21092015-PowerPoint.exe"
        $Path4 = "C:\\Users\\A90B~1\\AppData\\Local\\Temp\\AKT -21092015-PowerPoint.exe"
        $Path5 = "C:\\Users\\A90B~1\\AppData\\Local\\Temp\\AKT -21092015-PowerPoint.exe" wide
        $Path6 = "AKT -21092015-PowerPoint.exe9" wide
        $Path7 = "\\Documents\\chm\\AKT -21092015-PowerPoint.exe" wide
        $Path8 = "C:\\Users\\836D~1\\AppData\\Local\\Temp\\PEWER POINT PRESENTATION.exe" wide
        $Path9 = "PEWER POINT PRESENTATION.exe=" wide
        $Path10 = "\\Documents\\PEWER POINT PRESENTATION.exe"
        $Profile3 = "s Ainda precisam da uma melhorada nos pistols, pois a maioria dos jogos ja come" wide


    condition:
        any of them
}
```

YARA Rules- Examples

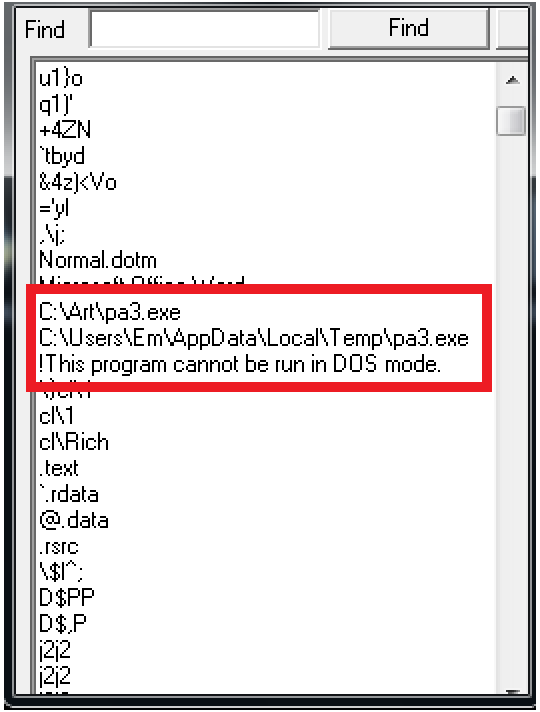


```
rule backoff_opcode{
    meta:
        author = "Swackhamer"
        md5 = "01F0D20A1A32E535B950428F5B5D6E72"
    strings:
        // MD5: 01F0D20A1A32E535B950428F5B5D6E72
        // Function: 404344 cc_validation
        $cc_validation = { 3C 5E ?? ?? ?? 74 ?? 3C 3D 0F ?? ?? ?? ?? ?? ?? ?? ?? 83 ?? ??
        3C 01 ?? ?? ?? 76 ?? 80 ?? ?? ?? 0F ?? ?? ?? ?? ?? 3C 01 ?? ?? ?? ?? ?? ?? ?? ?? ??
        ?? ?? ?? ?? 74 ?? 39 ?? ?? ?? ?? ?? 76 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 80 ?? ?? 76 ??
        ?? ?? 80 ?? ?? 74 ?? 80 ?? ?? 74 ?? 80 ?? ?? ?? 74 ?? E9 ?? ?? ?? ?? ?? ?? EB ?? ??
        ?? ?? ?? ?? ?? ?? ?? ?? 3C 03 0F ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 3C 09 0F
        ?? ?? ?? ?? ?? 83 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 83 ?? ?? 0F ?? ?? ?? ??
        ?? ?? ?? ?? ?? ?? ?? ?? 3C 09 0F ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 3C 09 0F
        ?? ?? ?? ?? ?? 83 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 83 ?? ?? 0F ?? ?? ?? ?? }
        // Function: 404539 memory_enum
        $memory_enum = { 3B ?? ?? ?? ?? ?? 73 ?? ?? ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
        ?? ?? ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 83 ?? ?? ?? ?? 75 ?? ?? ?? ?? E8 ?? ?? ?? ??
        5? ?? ?? E9 ?? ?? ?? ?? 83 ?? ?? ?? 75 ?? ?? ?? 81 ?? ?? ?? ?? ?? ?? 75 ?? 8B ?? ??
        39 C6 73 ?? 29 ?? ?? ?? B8 ?? ?? ?? ?? 81 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? A1 ??
        ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 8B ?? ?? ?? ?? ?? ??
        ?? ?? E8 ?? ?? ?? ?? 83 ?? ?? ?? ?? 75 ?? 8B ?? ?? EB ?? 8B ?? ?? ?? ?? ?? ?? ?? ??
        A1 ?? ?? ?? ?? ?? ?? ?? E8 }
    condition:
        any of them
}
```

YARA Rules- Examples

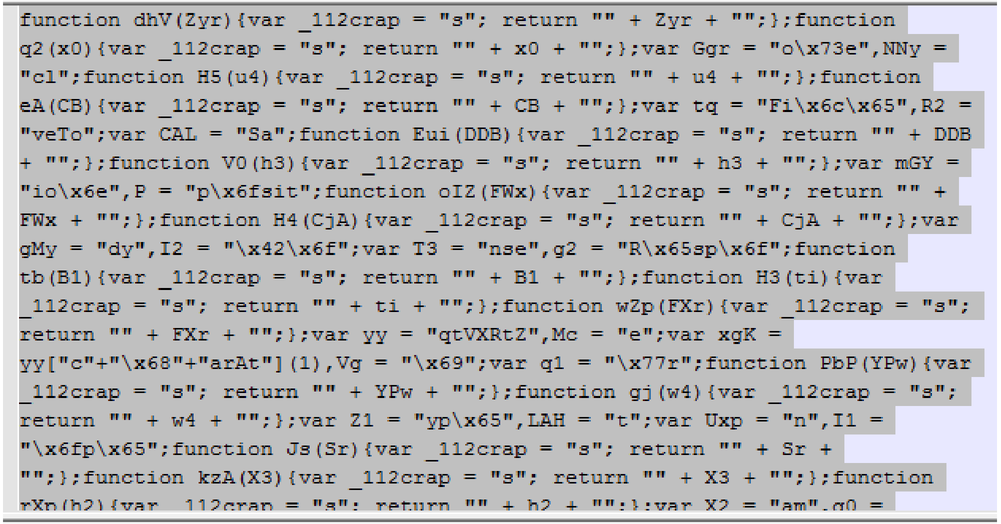


```
rule early_october2015_vawtrak_dropper{
    meta:
        author = "Kevin Perlow"
        SHA256 = "3d1e7e54db786c6aef572d1ef57ad1c26413aacbf2fd91eb700d469c550dd4df"
        SHA256 = "3ffbe191d9326f97db4ffaf6b294c166397bf1c77d28e2ab44d41fca511ce55b"

    strings:
        $VBA = { 00 41 74 74 72 69 62 75 74 00 } //doc contains VBA
        $rtf = { 2E 72 74 66 } //rtf in hex, will appear if in macro unobfuscated
        $exe = { 2E 65 78 65 }  //exe in hex
        $string1 = "TEMP$ 4"
        $string2 = /[0-9][0-9][0-9]\.rtf/
        $string3 = /[a-zA-Z0-9][a-zA-Z0-9][a-zA-Z0-9]\.exe/
        $a = {d0 cf 11 e0}
        $string4 = /C:\\Aaa\\exe\\[0-9A-Za-z]*\.exe/
        $string5 = /C:\\Users\\M\\AppData\\Local\\Temp\\[0-9A-Za-z]*\.exe/
        $string6 = "X:\\multiplexing\\limitations\\electr.pdb"
        $Dyreza = "C:\\Users\\Em\\AppData\\Local\\Temp\\w12.exe"
        $RSA = "This file is protected with RSA key." nocase


    condition:
        $a at 0 and $VBA and (($rtf and $exe) or 2 of ($string1,$string2,$string3) or 2 of
}
```

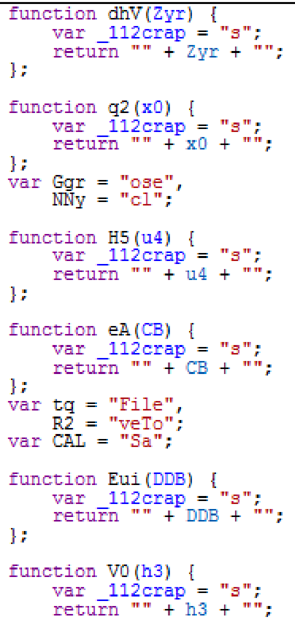


```
u1}o
q1}'
+4ZN
`tbyd
&4z}<Vo
='yl
.\j;
Normal.dotm
C:\Art\pa3.exe
C:\Users\Em\AppData\Local\Temp\pa3.exe
!This program cannot be run in DOS mode.
cl\1
cl\Rich
.text
`.rdata
@.data
.rsrc
\$l^;
D$PP
D$,P
j2j2
j2j2
```

YARA Rules- Case Study

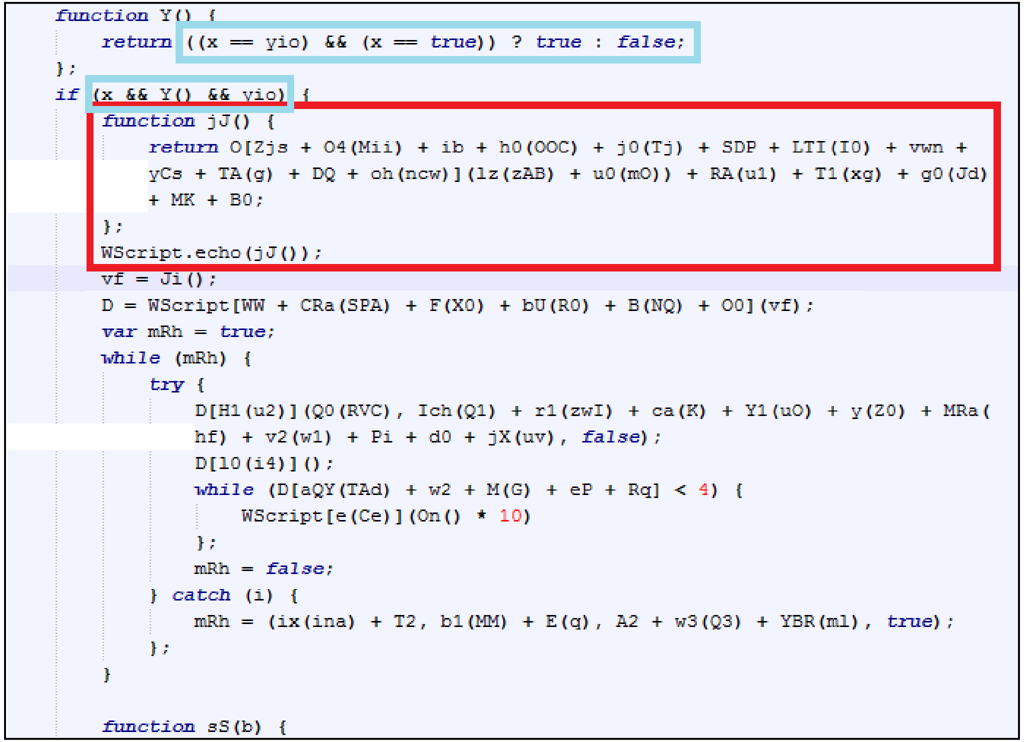


```
function dhV(Zyr){var _112crap = "s"; return "" + Zyr + "";};function
q2(x0){var _112crap = "s"; return "" + x0 + "";};var Ggr = "o\x73e",NNy =
"cl";function H5(u4){var _112crap = "s"; return "" + u4 + "";};function
eA(CB){var _112crap = "s"; return "" + CB + "";};var tq = "Fi\x6c\x65",R2 =
"veTo";var CAL = "Sa";function Eui(DDB){var _112crap = "s"; return "" + DDB
+ "";};function V0(h3){var _112crap = "s"; return "" + h3 + "";};var mGY =
"io\x6e",P = "p\x6fsit";function oIZ(FWx){var _112crap = "s"; return "" +
FWx + "";};function H4(CjA){var _112crap = "s"; return "" + CjA + "";};var
gMy = "dy",I2 = "\x42\x6f";var T3 = "nse",g2 = "R\x65sp\x6f";function
tb(B1){var _112crap = "s"; return "" + B1 + "";};function H3(ti){var
_112crap = "s"; return "" + ti + "";};function wZp(FXr){var _112crap = "s";
return "" + FXr + "";};var yy = "qtVXRtZ",Mc = "e";var xgK =
yy["c"+"\x68"+"arAt"](1),Vg = "\x69";var q1 = "\x77r";function PbP(YPw){var
_112crap = "s"; return "" + YPw + "";};function gj(w4){var _112crap = "s";
return "" + w4 + "";};var Z1 = "yp\x65",LAH = "t";var Uxp = "n",I1 =
"\x6fp\x65";function Js(Sr){var _112crap = "s"; return "" + Sr +
"";};function kzA(X3){var _112crap = "s"; return "" + X3 + "";};function
rXp(h2){var _112crap = "s"; return "" + h2 + "";};var X2 = "am",g0 =
```

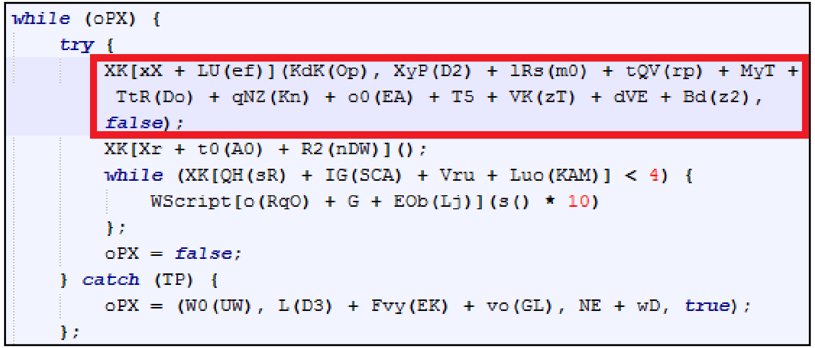


```
function dhV(Zyr) {
    var _112crap = "s";
    return "" + Zyr + "";
};

function q2(x0) {
    var _112crap = "s";
    return "" + x0 + "";
};
var Ggr = "ose",
    NNy = "cl";

function H5(u4) {
    var _112crap = "s";
    return "" + u4 + "";
};

function eA(CB) {
    var _112crap = "s";
    return "" + CB + "";
};
var tq = "File",
    R2 = "veTo";
var CAL = "Sa";

function Eui(DDB) {
    var _112crap = "s";
    return "" + DDB + "";
};

function V0(h3) {
    var _112crap = "s";
    return "" + h3 + "";
```

YARA Rules- Case Study



```
function Y() {
    return ((x == yio) && (x == true)) ? true : false;
};
if (x && Y() && yio) {
    function jJ() {
        return O[Zjs + O4(Mii) + ib + h0(OOC) + j0(Tj) + SDP + LTI(I0) + vwn +
        yCs + TA(g) + DQ + oh(ncw)](lz(zAB) + u0(mO)) + RA(u1) + T1(xg) + g0(Jd)
        + MK + B0;
    };
    WScript.echo(jJ());
    vf = Ji();
    D = WScript[WW + CRa(SPA) + F(X0) + bU(R0) + B(NQ) + O0](vf);
    var mRh = true;
    while (mRh) {
        try {
            D[H1(u2)](Q0(RVC), Ich(Q1) + r1(zwI) + ca(K) + Y1(uO) + y(Z0) + MRa(
            hf) + v2(w1) + Pi + d0 + jX(uv), false);
            D[l0(i4)]();
            while (D[aQY(TAd) + w2 + M(G) + eP + Rq] < 4) {
                WScript[e(Ce)](On() * 10)
            };
            mRh = false;
        } catch (i) {
            mRh = (ix(ina) + T2, b1(MM) + E(q), A2 + w3(Q3) + YBR(ml), true);
        };
    }

    function sS(b) {
```

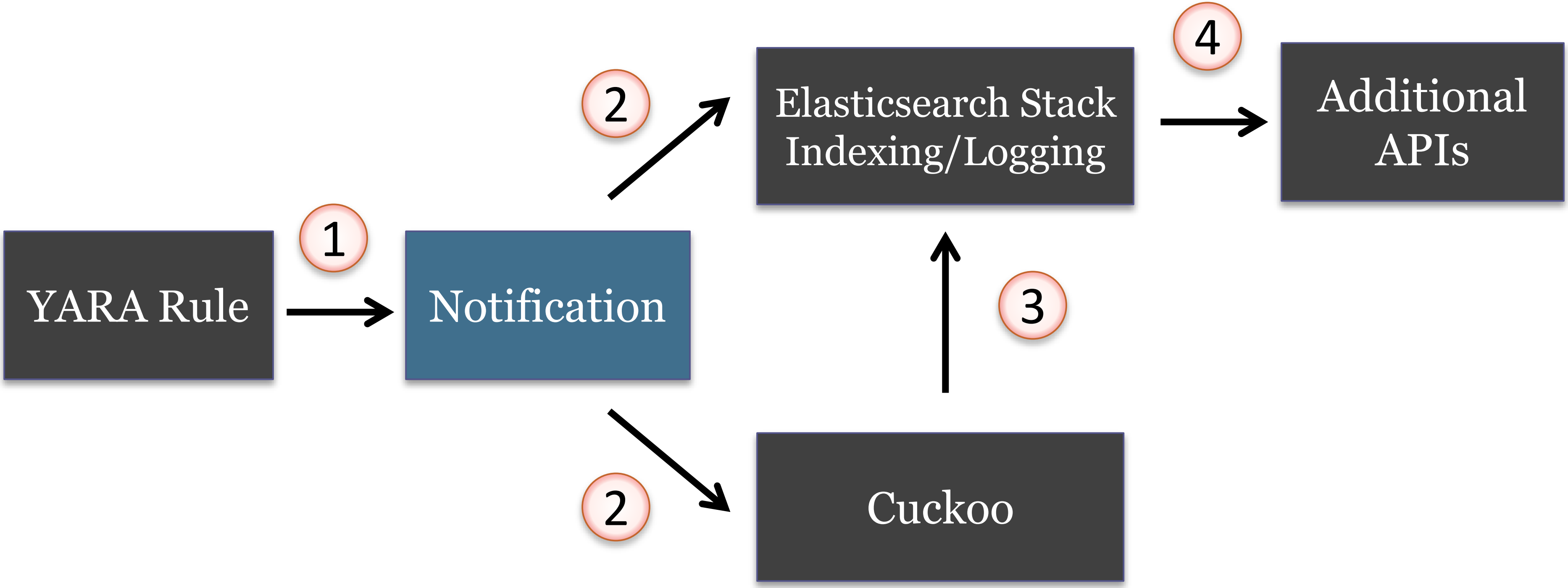


```
while (oPX) {
    try {
        XK[xX + LU(ef)](KdK(Op), XyP(D2) + lRs(m0) + tQV(rp) + MyT +
         TtR(Do) + qNZ(Kn) + o0(EA) + T5 + VK(zT) + dVE + Bd(z2),
        false);
        XK[Xr + t0(A0) + R2(nDW)]();
        while (XK[QH(sR) + IG(SCA) + Vru + Luo(KAM)] < 4) {
            WScript[o(RqO) + G + EOb(Lj)](s() * 10)
        };
        oPX = false;
    } catch (TP) {
        oPX = (W0(UW), L(D3) + Fvy(EK) + vo(GL), NE + wD, true);
    };
```

Left: the executable path being built.

Top right: Similar sample- the GET request being made inside a try/catch function

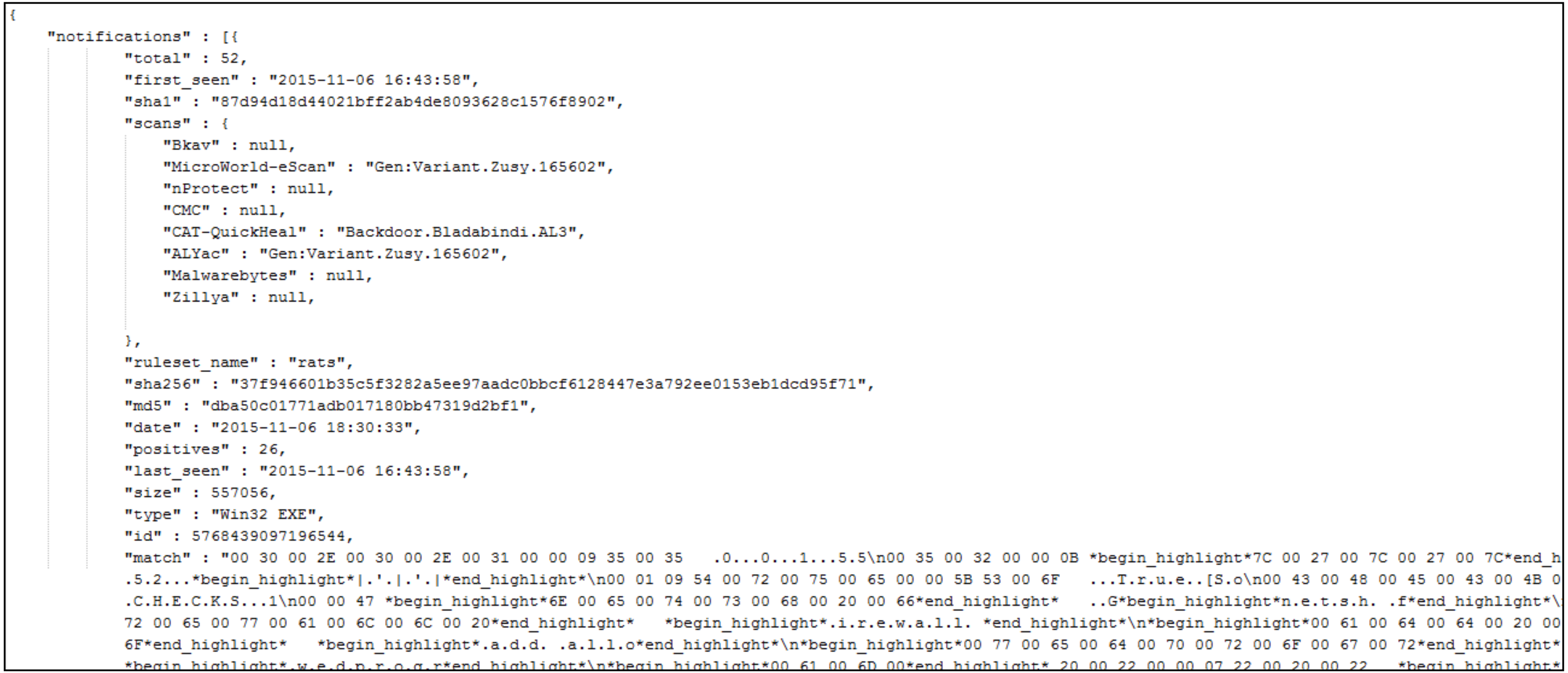
Automation and Collection Workflow



Notifications API

- VirusTotal or proprietary database
  - SMTP notifications
    - Pull via Python IMAP library
  - JSON notifications
    - Pull from REST API via Python requests library
    - Delete the alerts from VT after you process them
- Index and Parse into Elasticsearch

Sample VirusTotal Notification

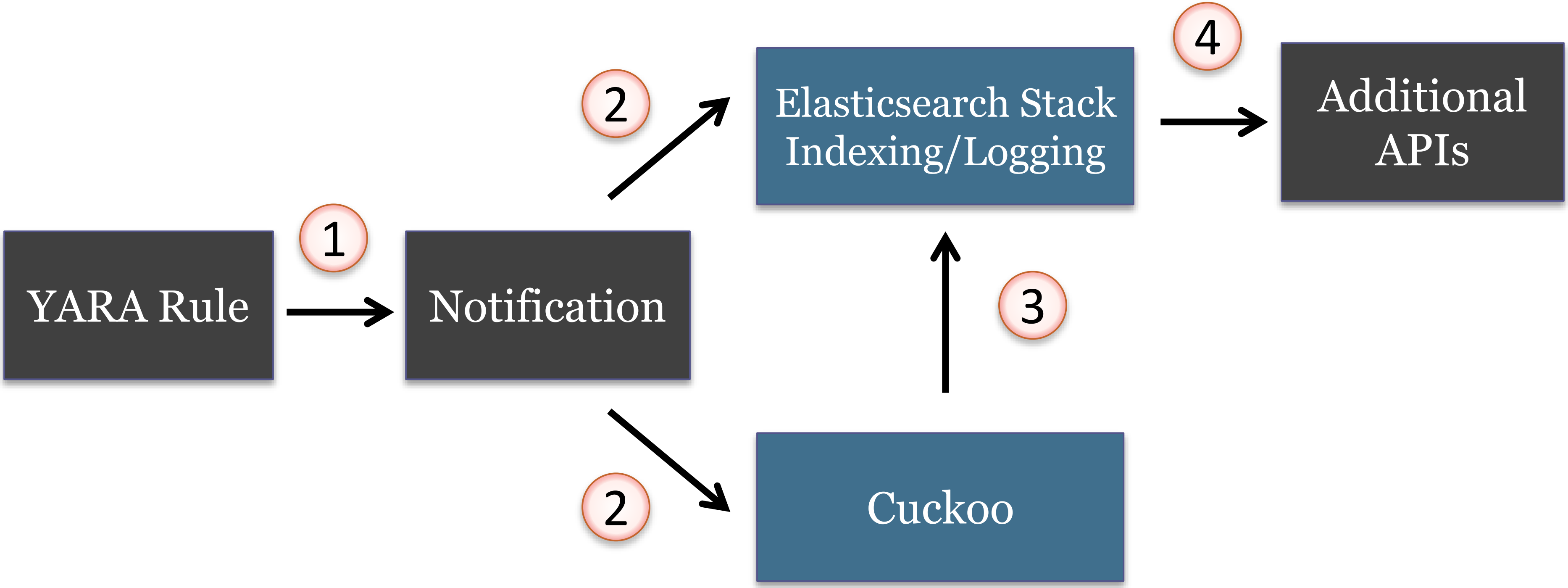


```
{
    "notifications" : [{
            "total" : 52,
            "first_seen" : "2015-11-06 16:43:58",
            "sha1" : "87d94d18d44021bff2ab4de8093628c1576f8902",
            "scans" : {
                "Bkav" : null,
                "MicroWorld-eScan" : "Gen:Variant.Zusy.165602",
                "nProtect" : null,
                "CMC" : null,
                "CAT-QuickHeal" : "Backdoor.Bladabindi.AL3",
                "ALYac" : "Gen:Variant.Zusy.165602",
                "Malwarebytes" : null,
                "Zillya" : null,

            },
            "ruleset_name" : "rats",
            "sha256" : "37f946601b35c5f3282a5ee97aadc0bbcf6128447e3a792ee0153eb1dcd95f71",
            "md5" : "dba50c01771adb017180bb47319d2bf1",
            "date" : "2015-11-06 18:30:33",
            "positives" : 26,
            "last_seen" : "2015-11-06 16:43:58",
            "size" : 557056,
            "type" : "Win32 EXE",
            "id" : 5768439097196544,
            "match" : "00 30 00 2E 00 30 00 2E 00 31 00 00 09 35 00 35   .0...0...1...5.5\n00 35 00 32 00 00 0B *begin_highlight*7C 00 27 00 7C 00 27 00 7C*end_h
            .5.2...*begin_highlight*|.'.|.'.|*end_highlight*\n00 01 09 54 00 72 00 75 00 65 00 00 5B 53 00 6F   ...T.r.u.e..[S.o\n00 43 00 48 00 45 00 43 00 4B 0
            .C.H.E.C.K.S...1\n00 00 47 *begin_highlight*6E 00 65 00 74 00 73 00 68 00 20 00 66*end_highlight*   ..G*begin_highlight*n.e.t.s.h. .f*end_highlight*\
            72 00 65 00 77 00 61 00 6C 00 6C 00 20*end_highlight*   *begin_highlight*.i.r.e.w.a.l.l. *end_highlight*\n*begin_highlight*00 61 00 64 00 64 00 20 00
            6F*end_highlight*   *begin_highlight*.a.d.d. .a.l.l.o*end_highlight*\n*begin_highlight*00 77 00 65 00 64 00 70 00 72 00 6F 00 67 00 72*end_highlight*
            *begin_highlight*.w.e.d.p.r.o.g.r*end_highlight*\n*begin_highlight*00 61 00 6D 00*end_highlight* 20 00 22 00 00 07 22 00 20 00 22   *begin_highlight*
```

IOC Extraction and Logging

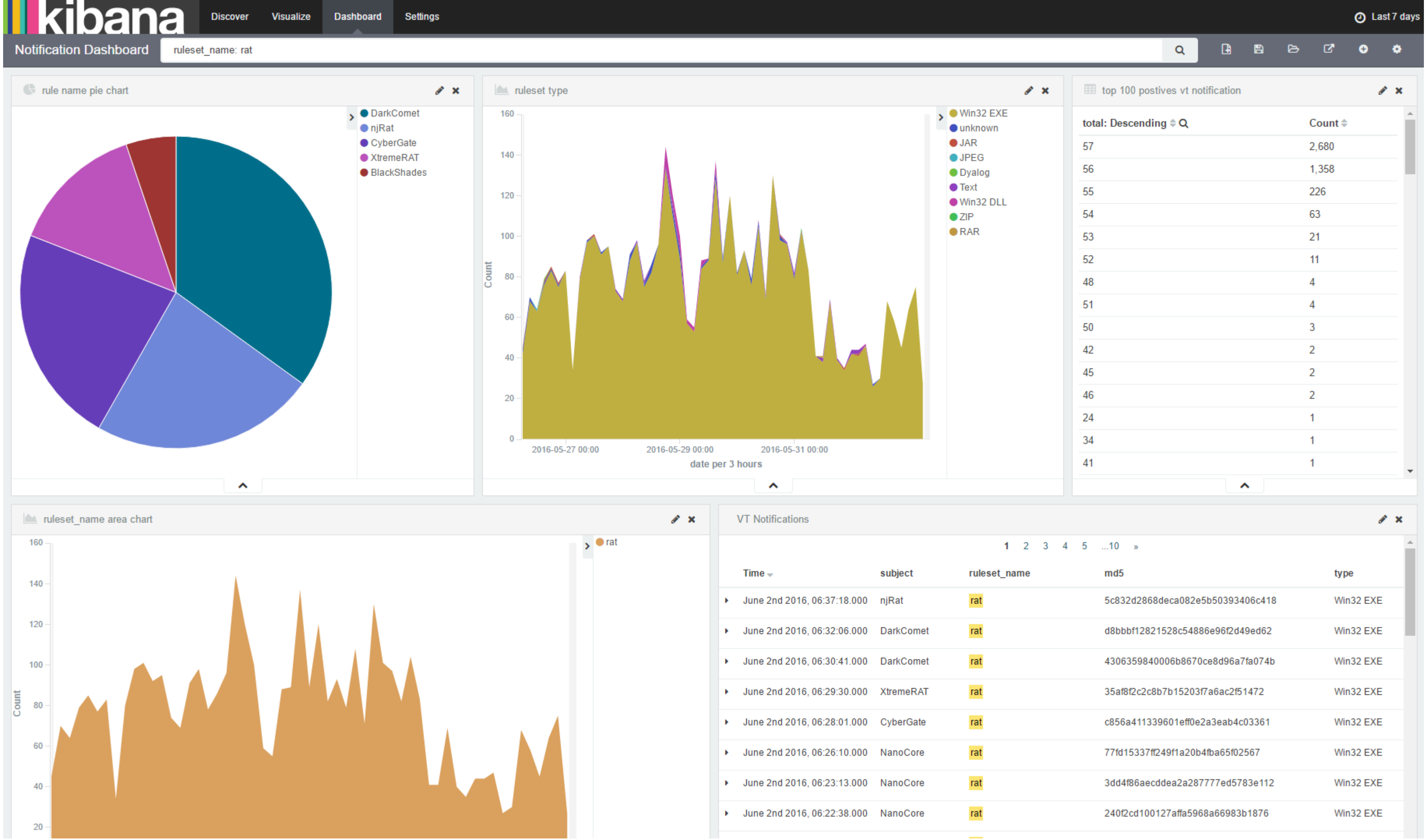
- Static Extraction
  - Configuration deobfuscation and parsing
  - Strings
  - Various obfuscation techniques (olevba)
  - FLOSS – Automated deobfuscation of strings
- Dynamic Extraction
  - Sandbox
    - Network
    - File system

Automation and Collection Workflow



Elasticsearch Stack

- Elasticsearch & Kibana
  - Visualize Notification Trends
    - First Seen
    - Last Seen
    - Resubmissions
  - Export Data (Hash, Rule Name, Rule Set)
    - Pivot through additional API’s
    - Export to CSV/JSON or other consumable formats



total: Descending	Count
57	2,680
56	1,358
55	226
54	63
53	21
52	11
48	4
51	4
50	3
42	2
45	2
46	2
24	1
34	1
41	1

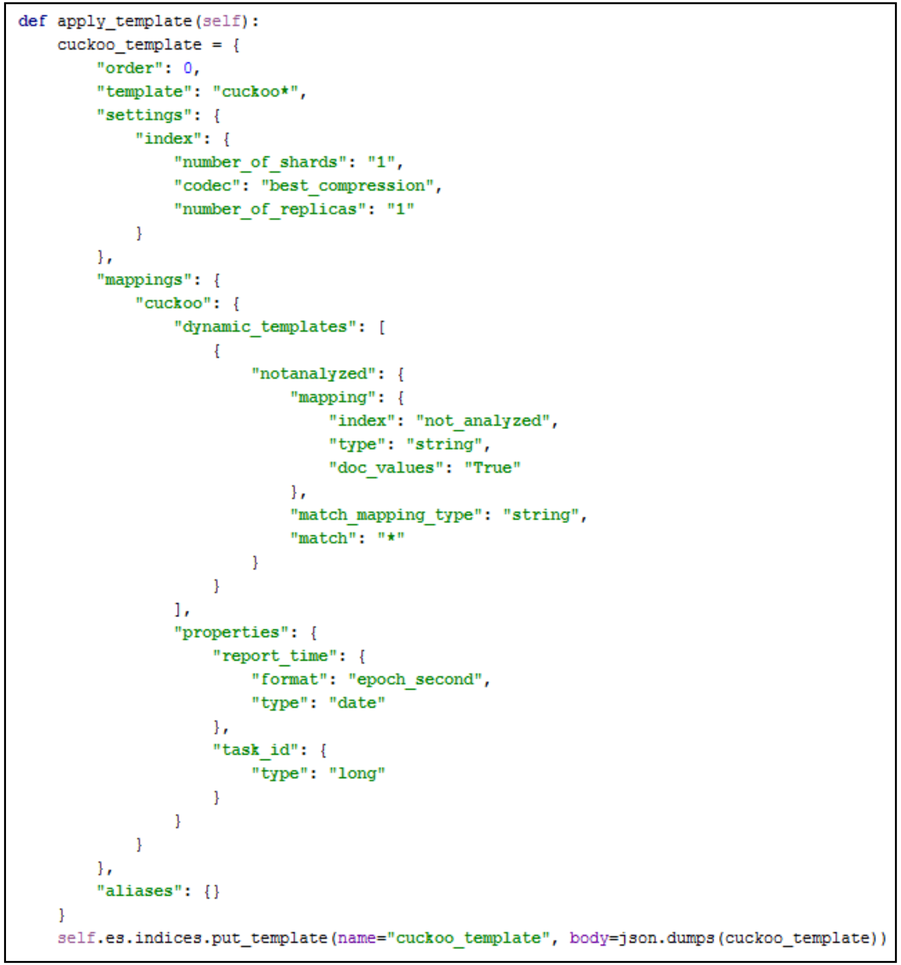
Time	subject	ruleset_name	md5	type
June 2nd 2016, 06:37:18.000	njRat	rat	5c832d2868deca082e5b50393406c418	Win32 EXE
June 2nd 2016, 06:32:06.000	DarkComet	rat	d8bbbf12821528c54886e96f2d49ed62	Win32 EXE
June 2nd 2016, 06:30:41.000	DarkComet	rat	4306359840006b8670ce8d96a7fa074b	Win32 EXE
June 2nd 2016, 06:29:30.000	XtremeRAT	rat	35af8f2c2c8b7b15203f7a6ac2f51472	Win32 EXE
June 2nd 2016, 06:28:01.000	CyberGate	rat	c856a411339601eff0e2a3eab4c03361	Win32 EXE
June 2nd 2016, 06:26:10.000	NanoCore	rat	77fd15337ff249f1a20b4fba65f02567	Win32 EXE
June 2nd 2016, 06:23:13.000	NanoCore	rat	3dd4f86aecddea2a287777ed5783e112	Win32 EXE
June 2nd 2016, 06:22:38.000	NanoCore	rat	240f2cd100127affa5968a66983b1876	Win32 EXE

Cuckoo Sandbox

- Automated Submission
  - Push notifications to Cuckoo on ingest from VT
  - Output IOCs (Domains, Files, Mutexs, etc…) back to Elasticsearch
- Customizable
  - Custom Elasticsearch reporting module
- Popular Sandboxes
  - VirusTotal
  - Malwr
  - Hybrid Analysis

Cuckoo Elasticsearch Index Template

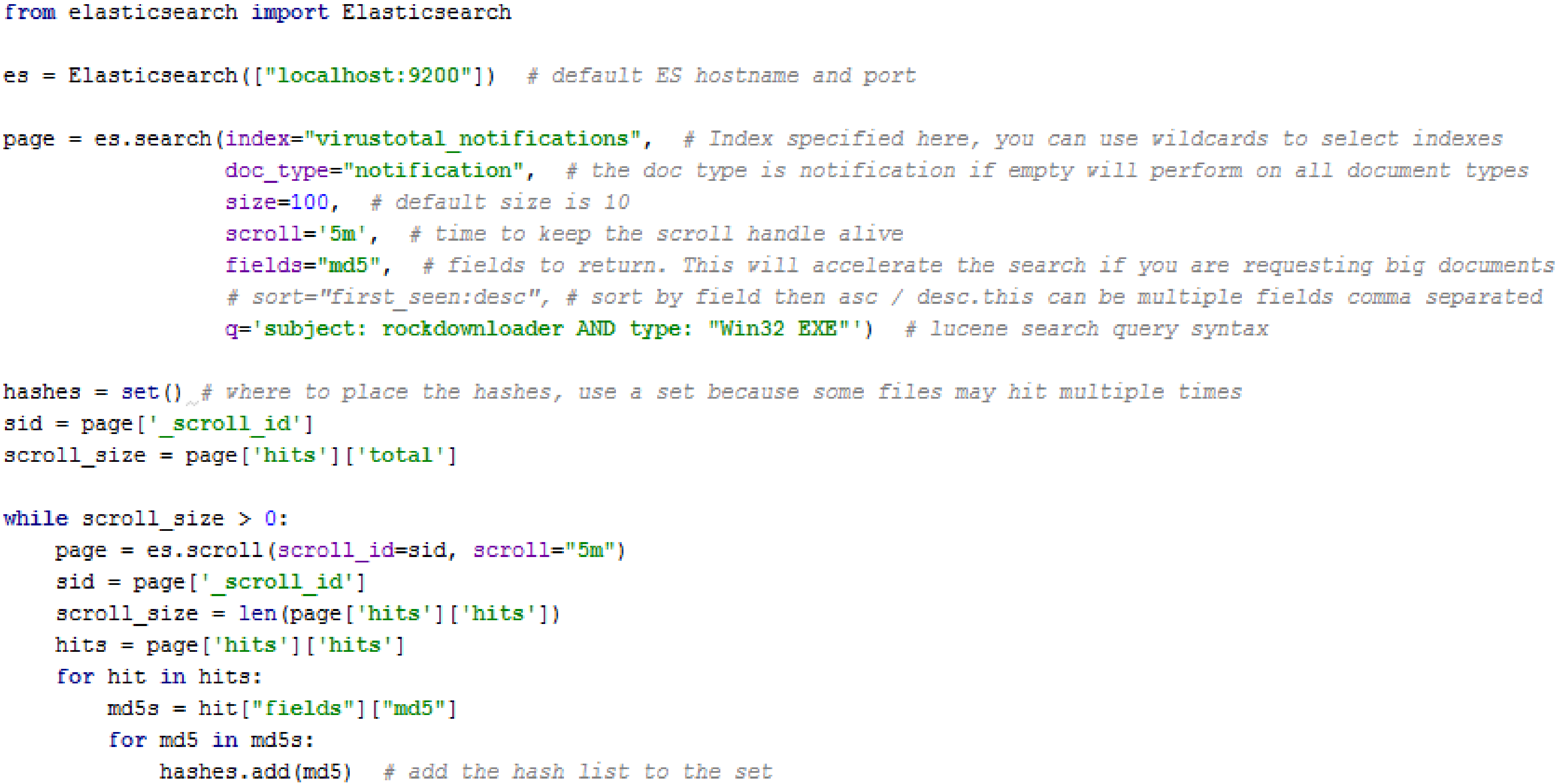
- Sets shard count to 1
- Compression to “best”
- Strings to “not_analyzed”
- task_id is an indexed field
- report_time is the date/time field



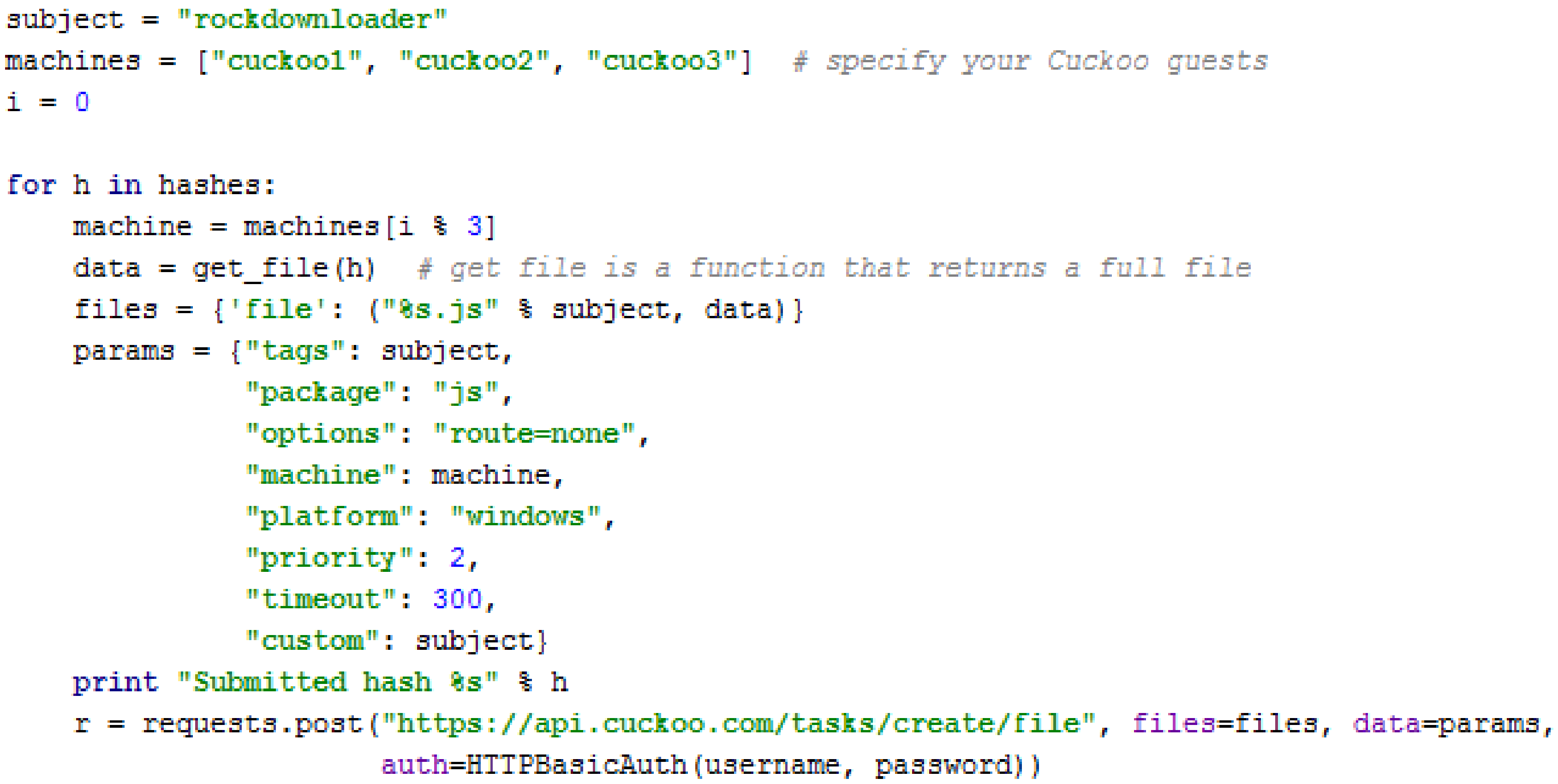
```
def apply_template(self):
    cuckoo_template = {
        "order": 0,
        "template": "cuckoo*",
        "settings": {
            "index": {
                "number_of_shards": "1",
                "codec": "best_compression",
                "number_of_replicas": "1"
            }
        },
        "mappings": {
            "cuckoo": {
                "dynamic_templates": [
                    {
                        "notanalyzed": {
                            "mapping": {
                                "index": "not_analyzed",
                                "type": "string",
                                "doc_values": "True"
                            },
                            "match_mapping_type": "string",
                            "match": "*"
                        }
                    }
                ],
                "properties": {
                    "report_time": {
                        "format": "epoch_second",
                        "type": "date"
                    },
                    "task_id": {
                        "type": "long"
                    }
                }
            }
        },
        "aliases": {}
    }
    self.es.indices.put_template(name="cuckoo_template", body=json.dumps(cuckoo_template))
```

Back to the Elasticsearch Stack

- Collect Cuckoo IOCs
  - Track by Domain, IP, Country
  - Files written to disk
  - Command line called
  - Normalization of A/V Data



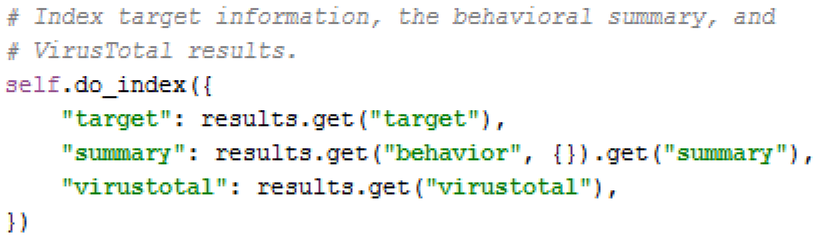
```python
from elasticsearch import Elasticsearch

es = Elasticsearch(["localhost:9200"])  # default ES hostname and port

page = es.search(index="virustotal_notifications",  # Index specified here, you can use wildcards to select indexes
                 doc_type="notification",  # the doc type is notification if empty will perform on all document types
                 size=100,  # default size is 10
                 scroll='5m',  # time to keep the scroll handle alive
                 fields="md5",  # fields to return. This will accelerate the search if you are requesting big documents
                 # sort="first_seen:desc", # sort by field then asc / desc.this can be multiple fields comma separated
                 q='subject: rockdownloader AND type: "Win32 EXE"')  # lucene search query syntax

hashes = set() # where to place the hashes, use a set because some files may hit multiple times
sid = page['_scroll_id']
scroll_size = page['hits']['total']

while scroll_size > 0:
    page = es.scroll(scroll_id=sid, scroll="5m")
    sid = page['_scroll_id']
    scroll_size = len(page['hits']['hits'])
    hits = page['hits']['hits']
    for hit in hits:
        md5s = hit["fields"]["md5"]
        for md5 in md5s:
            hashes.add(md5)  # add the hash list to the set
```



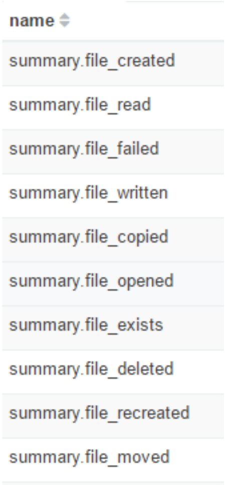
```
subject = "rockdownloader"
machines = ["cuckoo1", "cuckoo2", "cuckoo3"]  # specify your Cuckoo guests
i = 0

for h in hashes:
    machine = machines[i % 3]
    data = get_file(h)  # get file is a function that returns a full file
    files = {'file': ("%s.js" % subject, data)}
    params = {"tags": subject,
              "package": "js",
              "options": "route=none",
              "machine": machine,
              "platform": "windows",
              "priority": 2,
              "timeout": 300,
              "custom": subject}
    print "Submitted hash %s" % h
    r = requests.post("https://api.cuckoo.com/tasks/create/file", files=files, data=params,
                      auth=HTTPBasicAuth(username, password))
```

Cuckoo Summary

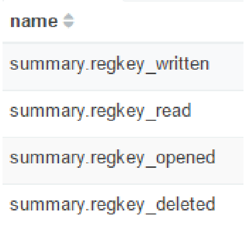
- Files
- Registry
- Mutex
- Directory
- Resolved Hosts
- Connected Hosts
- Command Line
- DLL Loaded
- WMI Query
- Target File - Hash
- Target File - Name
- Target File - Type
- VirusTotal Signatures



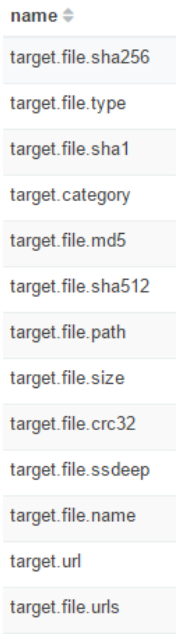
```
# Index target information, the behavioral summary, and
# VirusTotal results.
self.do_index({
    "target": results.get("target"),
    "summary": results.get("behavior", {}).get("summary"),
    "virustotal": results.get("virustotal"),
})
```



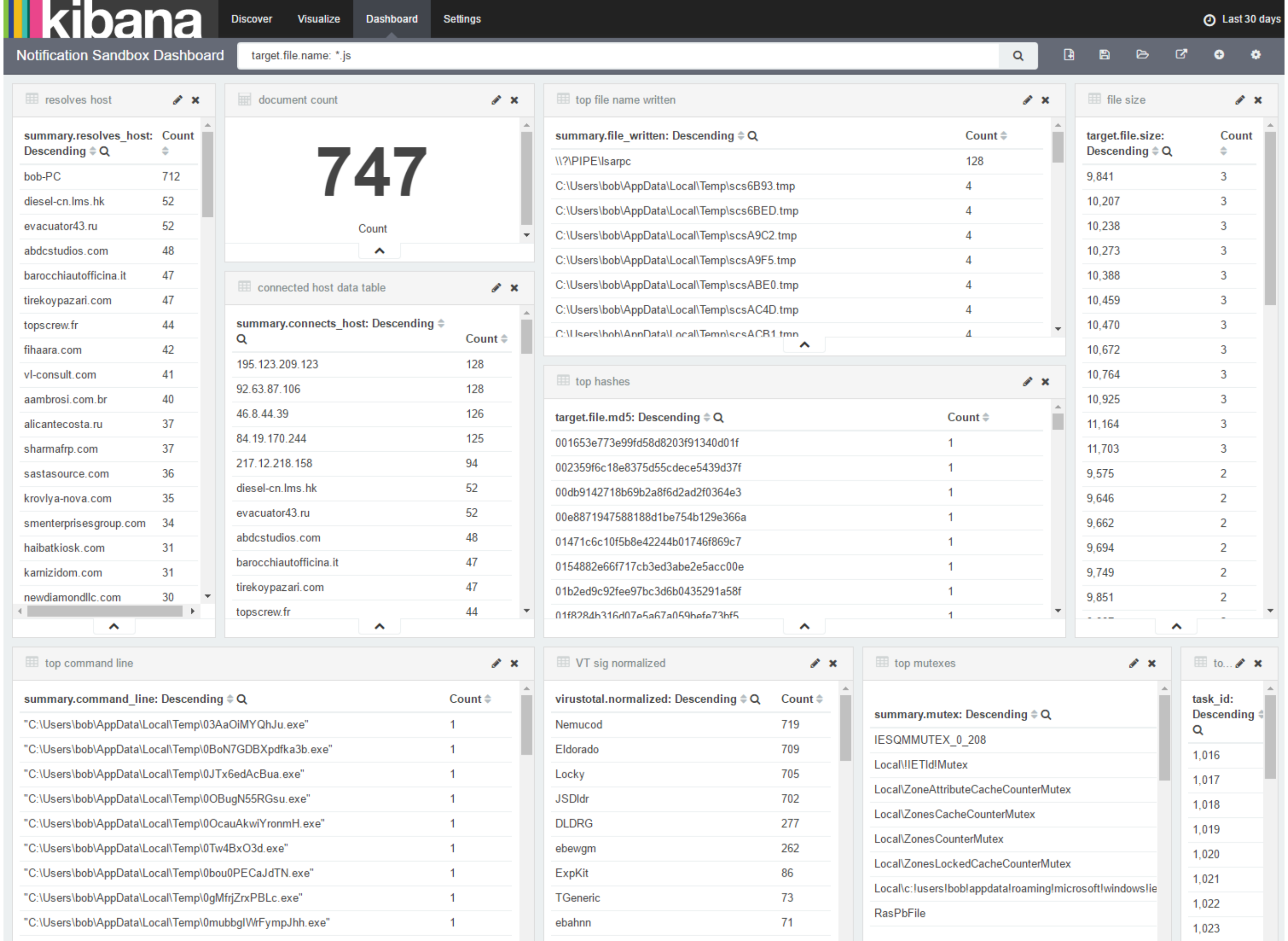
name
summary.file_created
summary.file_read
summary.file_failed
summary.file_written
summary.file_copied
summary.file_opened
summary.file_exists
summary.file_deleted
summary.file_recreated
summary.file_moved



name
summary.regkey_written
summary.regkey_read
summary.regkey_opened
summary.regkey_deleted



name
target.file.sha256
target.file.type
target.file.sha1
target.category
target.file.md5
target.file.sha512
target.file.path
target.file.size
target.file.crc32
target.file.ssdeep
target.file.name
target.url
target.file.urls



Notification Sandbox Dashboard

target.file.name: *.js

resolves host

summary.resolves_host: Descending	Count
bob-PC	712
diesel-cn.lms.hk	52
evacuator43.ru	52
abdcstudios.com	48
barocchiautofficina.it	47
tirekoypazari.com	47
topscrew.fr	44
fihaara.com	42
vl-consult.com	41
aambrosi.com.br	40
alicantecosta.ru	37
sharmafrp.com	37
sastasource.com	36
krovlya-nova.com	35
smenterprisesgroup.com	34
haibatkiosk.com	31
karnizidom.com	31
newdiamondllc.com	30

document count

747

Count

connected host data table

summary.connects_host: Descending	Count
195.123.209.123	128
92.63.87.106	128
46.8.44.39	126
84.19.170.244	125
217.12.218.158	94
diesel-cn.lms.hk	52
evacuator43.ru	52
abdcstudios.com	48
barocchiautofficina.it	47
tirekoypazari.com	47
topscrew.fr	44

top file name written

summary.file_written: Descending	Count
\\?\PIPE\lsarpc	128
C:\Users\bob\AppData\Local\Temp\scs6B93.tmp	4
C:\Users\bob\AppData\Local\Temp\scs6BED.tmp	4
C:\Users\bob\AppData\Local\Temp\scsA9C2.tmp	4
C:\Users\bob\AppData\Local\Temp\scsA9F5.tmp	4
C:\Users\bob\AppData\Local\Temp\scsABE0.tmp	4
C:\Users\bob\AppData\Local\Temp\scsAC4D.tmp	4
C:\Users\bob\AppData\Local\Temp\scsACB1.tmp	4

top hashes

target.file.md5: Descending	Count
001653e773e99fd58d8203f91340d01f	1
002359f6c18e8375d55cdece5439d37f	1
00db9142718b69b2a8f6d2ad2f0364e3	1
00e8871947588188d1be754b129e366a	1
01471c6c10f5b8e42244b01746f869c7	1
0154882e66f717cb3ed3abe2e5acc00e	1
01b2ed9c92fee97bc3d6b0435291a58f	1
01f8284b316d07e5a67a059befe73bf5	1

file size

target.file.size: Descending	Count
9,841	3
10,207	3
10,238	3
10,273	3
10,388	3
10,459	3
10,470	3
10,672	3
10,764	3
10,925	3
11,164	3
11,703	3
9,575	2
9,646	2
9,662	2
9,694	2
9,749	2
9,851	2

top command line

summary.command_line: Descending	Count
"C:\Users\bob\AppData\Local\Temp\03AaOiMYQhJu.exe"	1
"C:\Users\bob\AppData\Local\Temp\0BoN7GDBXpdfka3b.exe"	1
"C:\Users\bob\AppData\Local\Temp\0JTx6edAcBua.exe"	1
"C:\Users\bob\AppData\Local\Temp\0OBugN55RGsu.exe"	1
"C:\Users\bob\AppData\Local\Temp\0OcauAkwiYronmH.exe"	1
"C:\Users\bob\AppData\Local\Temp\0Tw4BxO3d.exe"	1
"C:\Users\bob\AppData\Local\Temp\0bou0PECaJdTN.exe"	1
"C:\Users\bob\AppData\Local\Temp\0gMfrjZrxPBLc.exe"	1
"C:\Users\bob\AppData\Local\Temp\0mubbglWrFympJhh.exe"	1

VT sig normalized

virustotal.normalized: Descending	Count
Nemucod	719
Eldorado	709
Locky	705
JSDldr	702
DLDRG	277
ebewgm	262
ExpKit	86
TGeneric	73
ebahnn	71

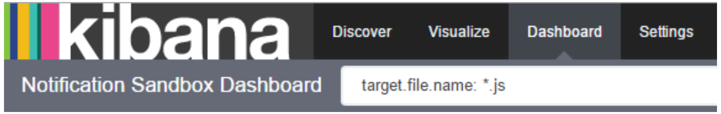
top mutexes

summary.mutex: Descending
IESQMMUTEX_0_208
Local\!IETld!Mutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\c:!users!bob!appdata!roaming!microsoft!windows!ie
RasPbFile

to...

task_id: Descending
1,016
1,017
1,018
1,019
1,020
1,021
1,022
1,023

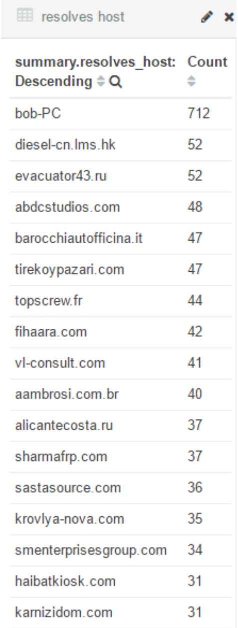
Lucene Search Query Syntax



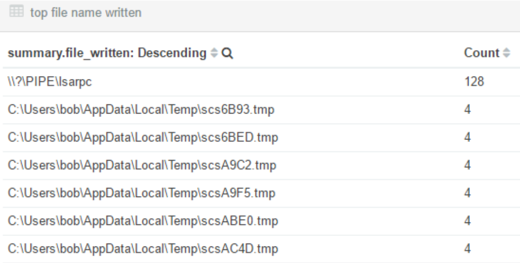
Notification Sandbox Dashboard

target.file.name: *.js

List of hosts and files written aggregated with count

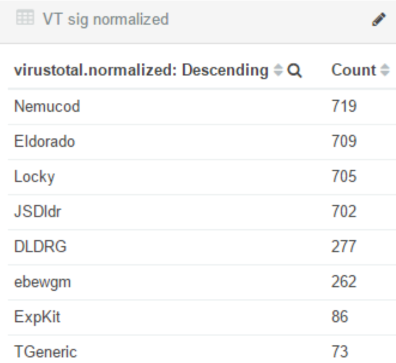

resolves host

summary.resolves_host: Descending	Count
bob-PC	712
diesel-cn.lms.hk	52
evacuator43.ru	52
abdcstudios.com	48
barocchiautofficina.it	47
tirekoypazari.com	47
topscrew.fr	44
fihaara.com	42
vl-consult.com	41
aambrosi.com.br	40
alicantecosta.ru	37
sharmafrp.com	37
sastasource.com	36
krovlya-nova.com	35
smenterprisesgroup.com	34
haibatkiosk.com	31
karnizidom.com	31


top file name written

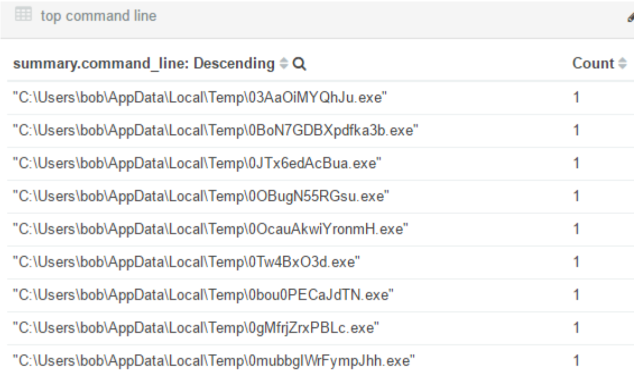
summary.file_written: Descending	Count
\\?\PIPE\lsarpc	128
C:\Users\bob\AppData\Local\Temp\scs6B93.tmp	4
C:\Users\bob\AppData\Local\Temp\scs6BED.tmp	4
C:\Users\bob\AppData\Local\Temp\scsA9C2.tmp	4
C:\Users\bob\AppData\Local\Temp\scsA9F5.tmp	4
C:\Users\bob\AppData\Local\Temp\scsABE0.tmp	4
C:\Users\bob\AppData\Local\Temp\scsAC4D.tmp	4

Normalized AV signatures from VT


VT sig normalized

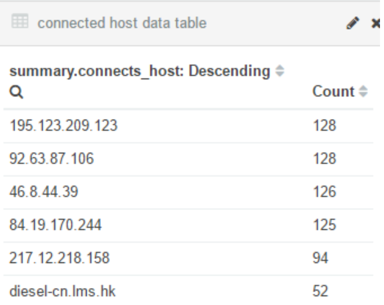
virustotal.normalized: Descending	Count
Nemucod	719
Eldorado	709
Locky	705
JSDldr	702
DLDRG	277
ebewgm	262
ExpKit	86
TGeneric	73

Command line called by malware

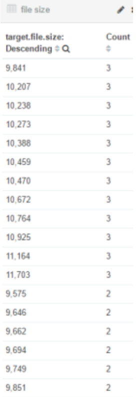

top command line

summary.command_line: Descending	Count
"C:\Users\bob\AppData\Local\Temp\03AaOiMYQhJu.exe"	1
"C:\Users\bob\AppData\Local\Temp\0BoN7GDBXpdfka3b.exe"	1
"C:\Users\bob\AppData\Local\Temp\0JTx6edAcBua.exe"	1
"C:\Users\bob\AppData\Local\Temp\0OBugN55RGsu.exe"	1
"C:\Users\bob\AppData\Local\Temp\0OcauAkwiYronmH.exe"	1
"C:\Users\bob\AppData\Local\Temp\0Tw4BxO3d.exe"	1
"C:\Users\bob\AppData\Local\Temp\0bou0PECaJdTN.exe"	1
"C:\Users\bob\AppData\Local\Temp\0gMfrjZrxPBLc.exe"	1
"C:\Users\bob\AppData\Local\Temp\0mubbglWrFympJhh.exe"	1

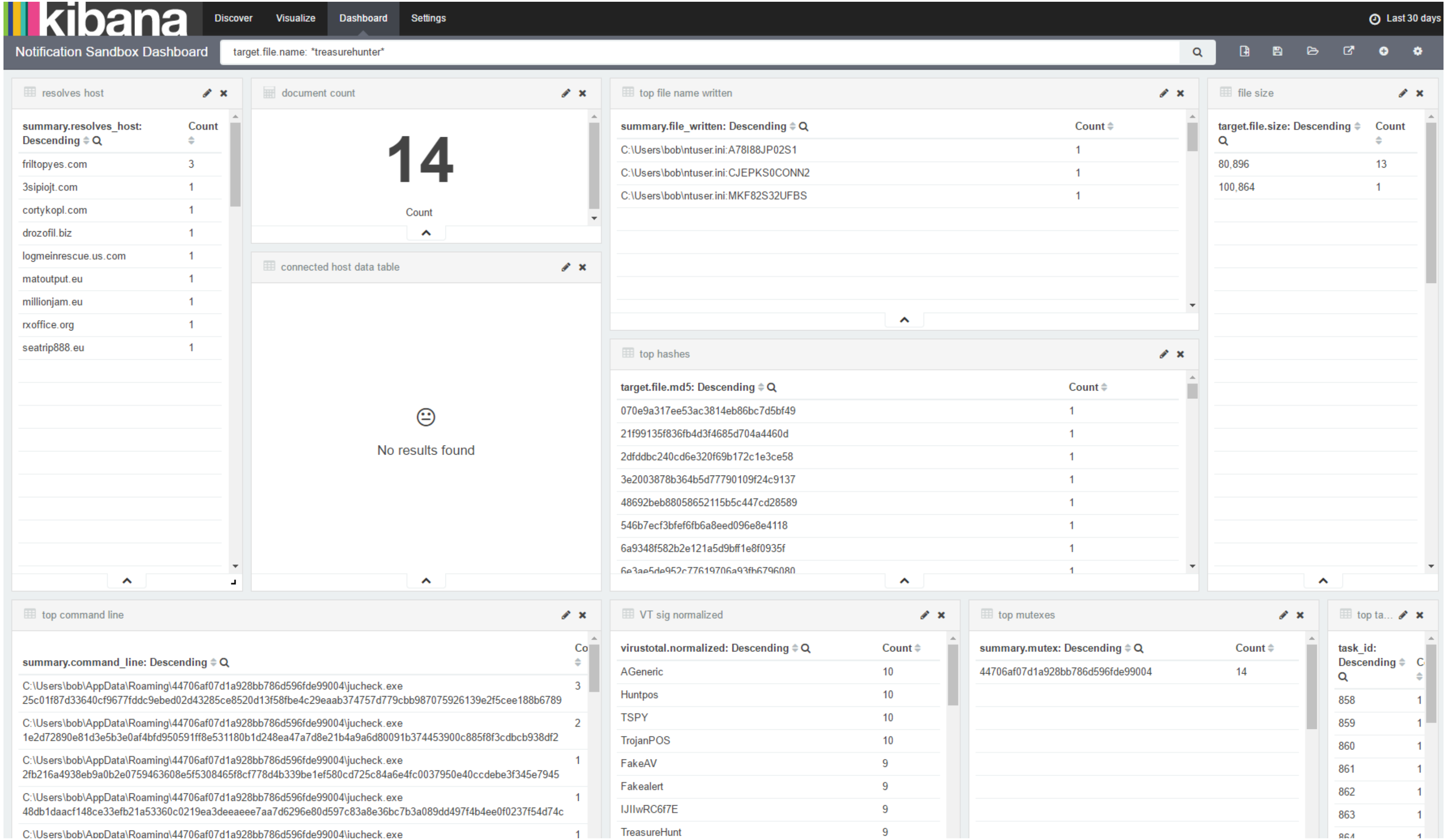
File size and hosts connected to


connected host data table

summary.connects_host: Descending	Count
195.123.209.123	128
92.63.87.106	128
46.8.44.39	126
84.19.170.244	125
217.12.218.158	94
diesel-cn.lms.hk	52


file size

target.file.size: Descending	Count
9,841	3
10,207	3
10,238	3
10,273	3
10,388	3
10,459	3
10,470	3
10,672	3
10,764	3
10,925	3
11,164	3
11,703	3
9,575	2
9,646	2
9,662	2
9,694	2
9,749	2
9,851	2



Notification Sandbox Dashboard

target.file.name: *treasurehunter*

resolves host

summary.resolves_host: Descending	Count
friltopyes.com	3
3sipiojt.com	1
cortykopl.com	1
drozofil.biz	1
logmeinrescue.us.com	1
matoutput.eu	1
millionjam.eu	1
rxoffice.org	1
seatrip888.eu	1

document count

14

Count

connected host data table

No results found

top file name written

summary.file_written: Descending	Count
C:\Users\bob\ntuser.ini:A78I88JP02S1	1
C:\Users\bob\ntuser.ini:CJEPKS0CONN2	1
C:\Users\bob\ntuser.ini:MKF82S32UFBS	1

top hashes

target.file.md5: Descending	Count
070e9a317ee53ac3814eb86bc7d5bf49	1
21f99135f836fb4d3f4685d704a4460d	1
2dfddbc240cd6e320f69b172c1e3ce58	1
3e2003878b364b5d77790109f24c9137	1
48692beb88058652115b5c447cd28589	1
546b7ecf3bfef6fb6a8eed096e8e4118	1
6a9348f582b2e121a5d9bff1e8f0935f	1
6e3ae5de952c77619706a93fb6796080	1

file size

target.file.size: Descending	Count
80,896	13
100,864	1

top command line

summary.command_line: Descending	Co
C:\Users\bob\AppData\Roaming\44706af07d1a928bb786d596fde99004\jucheck.exe 25c01f87d33640cf9677fddc9ebed02d43285ce8520d13f58fbe4c29eaab374757d779cbb987075926139e2f5cee188b6789	3
C:\Users\bob\AppData\Roaming\44706af07d1a928bb786d596fde99004\jucheck.exe 1e2d72890e81d3e5b3e0af4bfd950591ff8e531180b1d248ea47a7d8e21b4a9a6d80091b374453900c885f8f3cdbcb938df2	2
C:\Users\bob\AppData\Roaming\44706af07d1a928bb786d596fde99004\jucheck.exe 2fb216a4938eb9a0b2e0759463608e5f5308465f8cf778d4b339be1ef580cd725c84a6e4fc0037950e40ccdebe3f345e7945	1
C:\Users\bob\AppData\Roaming\44706af07d1a928bb786d596fde99004\jucheck.exe 48db1daacf148ce33efb21a53360c0219ea3deeaeee7aa7d6296e80d597c83a8e36bc7b3a089dd497f4b4ee0f0237f54d74c	1
C:\Users\bob\AppData\Roaming\44706af07d1a928bb786d596fde99004\jucheck.exe	1

VT sig normalized

virustotal.normalized: Descending	Count
AGeneric	10
Huntpos	10
TSPY	10
TrojanPOS	10
FakeAV	9
Fakealert	9
IJIlwRC6f7E	9
TreasureHunt	9

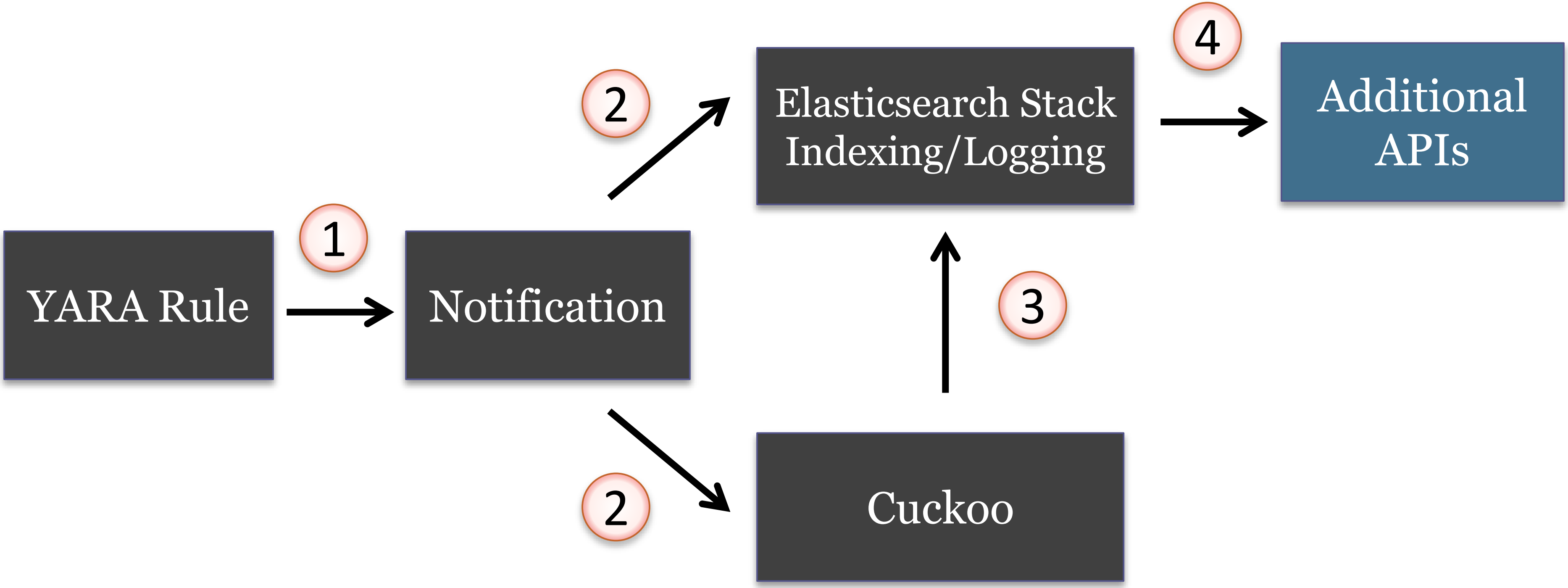
top mutexes

summary.mutex: Descending	Count
44706af07d1a928bb786d596fde99004	14

top ta...

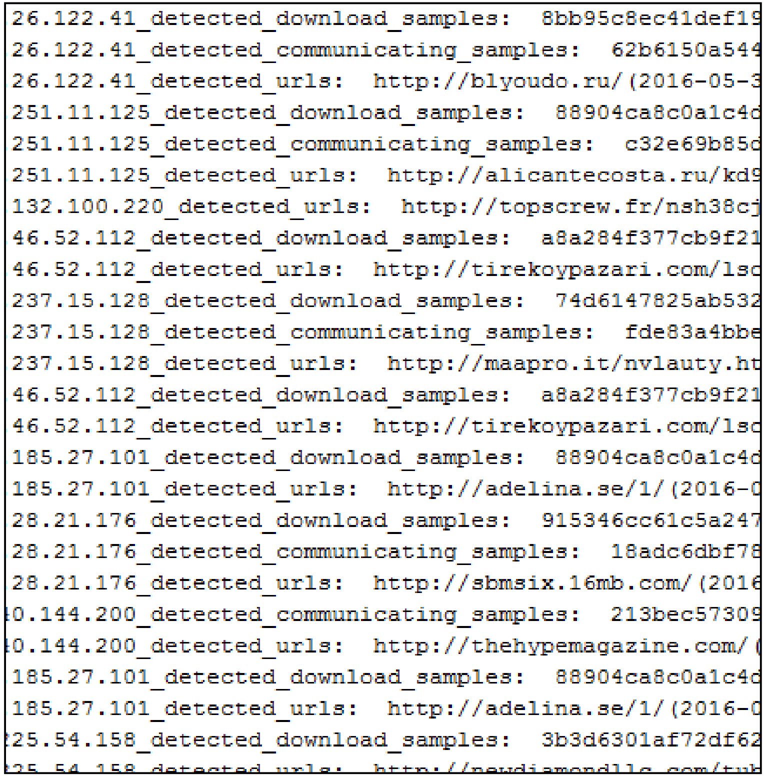
task_id: Descending	C
858	1
859	1
860	1
861	1
862	1
863	1
864	1

Automation and Collection Workflow



Additional APIs

- VirusTotal
  - Parent objects
    - Emails
    - Zip Files
  - Network Infrastructure
- CentralOps
  - Whois
  - Physical Address
- PassiveTotal
  - PassiveDNS
  - Historical Records



```
26.122.41_detected_download_samples:  8bb95c8ec41def19
26.122.41_detected_communicating_samples:  62b6150a544
26.122.41_detected_urls:  http://blyoudo.ru/(2016-05-3
251.11.125_detected_download_samples:  88904ca8c0a1c4d
251.11.125_detected_communicating_samples:  c32e69b85d
251.11.125_detected_urls:  http://alicantecosta.ru/kd9
132.100.220_detected_urls:  http://topscrew.fr/nsh38cj
46.52.112_detected_download_samples:  a8a284f377cb9f21
46.52.112_detected_urls:  http://tirekoypazari.com/lsc
237.15.128_detected_download_samples:  74d6147825ab532
237.15.128_detected_communicating_samples:  fde83a4bbe
237.15.128_detected_urls:  http://maapro.it/nvlauty.ht
46.52.112_detected_download_samples:  a8a284f377cb9f21
46.52.112_detected_urls:  http://tirekoypazari.com/lsc
185.27.101_detected_download_samples:  88904ca8c0a1c4d
185.27.101_detected_urls:  http://adelina.se/1/(2016-0
28.21.176_detected_download_samples:  915346cc61c5a247
28.21.176_detected_communicating_samples:  18adc6dbf78
28.21.176_detected_urls:  http://sbmsix.16mb.com/(2016
0.144.200_detected_communicating_samples:  213bec57309
0.144.200_detected_urls:  http://thehypemagazine.com/(
185.27.101_detected_download_samples:  88904ca8c0a1c4d
185.27.101_detected_urls:  http://adelina.se/1/(2016-0
25.54.158_detected_download_samples:  3b3d6301af72df62
25.54.158_detected_urls:  http://newdiamondllc.com/tuk
```

Recap

- Built YARA rule for one dropper
- Identified 700+ files
- Automated analysis via Cuckoo
- Logging via Elasticsearch and Visualization with Kibana
- Additional pivoting via API
- Source code: https://github.com/swackhamer

Questions?