

DC423 JULY MEETING

#HOMECON



AGENDA

- ▶ Intro to any new members
- ▶ Missing Defcon and our DC865 Neighbors
- ▶ BSIDESCHA
- ▶ Infrastructure Updates
- ▶ Cases of false attribution



DC423 JULY MEETING

INTROS



./ DC865

DC423 JULY MEETING

DC865





DC423 JULY MEETING

BSIDESCHA



INFRASTRUCTURE

I BLAME NATE & N01



INFRASTRUCTURE

- ▶ Server Rack
 - ▶ Two servers racked and connected
 - ▶ ESXI (still being built)
 - ▶ General Linux box
- ▶ Linode
 - ▶ Scripts (some could be ran from genral linux box when ready)
 - ▶ FOASS, Shodan Images can move to Linux box or here
 - ▶ Other purposes?
 - ▶ Things we can't lose due to power outages




INFRASTRUCTURE

▶ 19 days uptime

▶ **Network**

- Transfer/mo: 1000 GB
- Incoming: 667 MB
- Outgoing: 115 MB
- Total: 782 MB

You have used

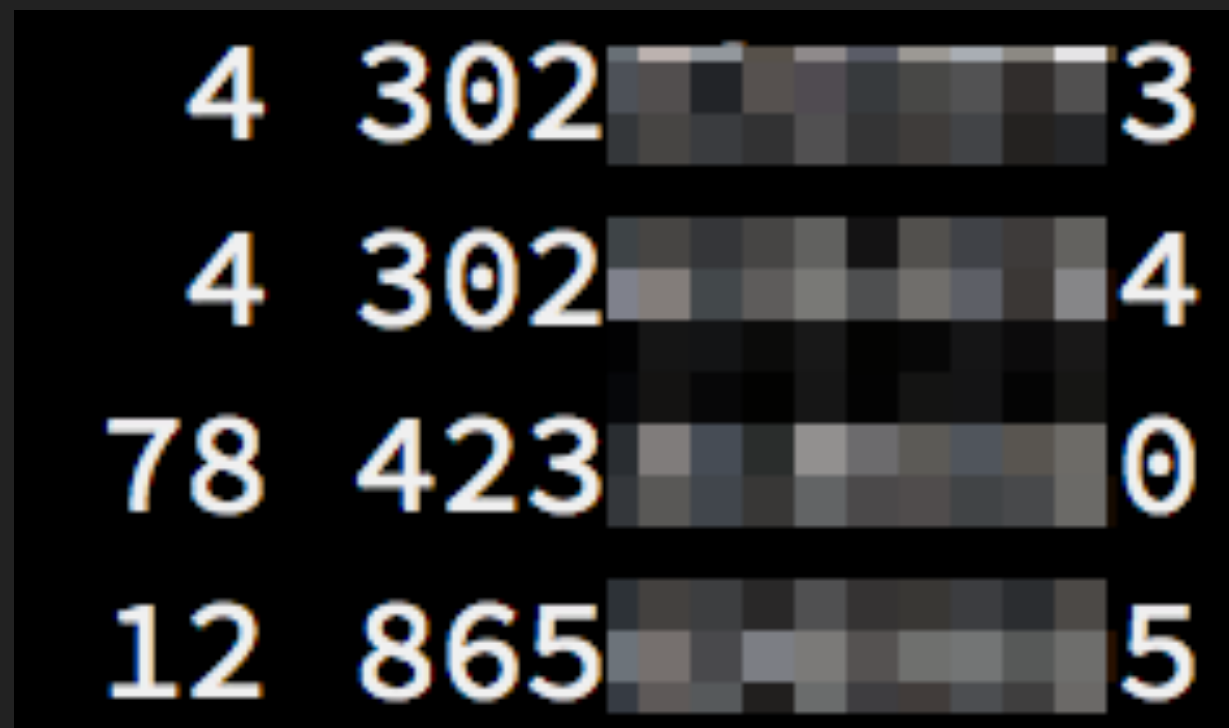
0% 

of your monthly transfer



INFRASTRUCTURE

- ▶ HC911 (NOW WITH TEXT MESSAGES)



INFRASTRUCTURE

► Weather Messages for Slack



This Afternoon APP 12:30 PM

A slight chance of showers and thunderstorms after 4pm. Mostly sunny, with a high near 93. Heat index values as high as 101. West wind 2 to 6 mph. Chance of precipitation is 20%. New rainfall amounts less than a tenth of an inch possible. ⚡



Tonight APP 12:30 PM ☆

A slight chance of showers and thunderstorms before 8pm. Partly cloudy, with a low around 74. Heat index values as high as 100. South southeast wind 1 to 5 mph. Chance of precipitation is 20%. New rainfall amounts less than a tenth of an inch possible. ⚡



INFRASTRUCTURE

► What else do YOU want to see?

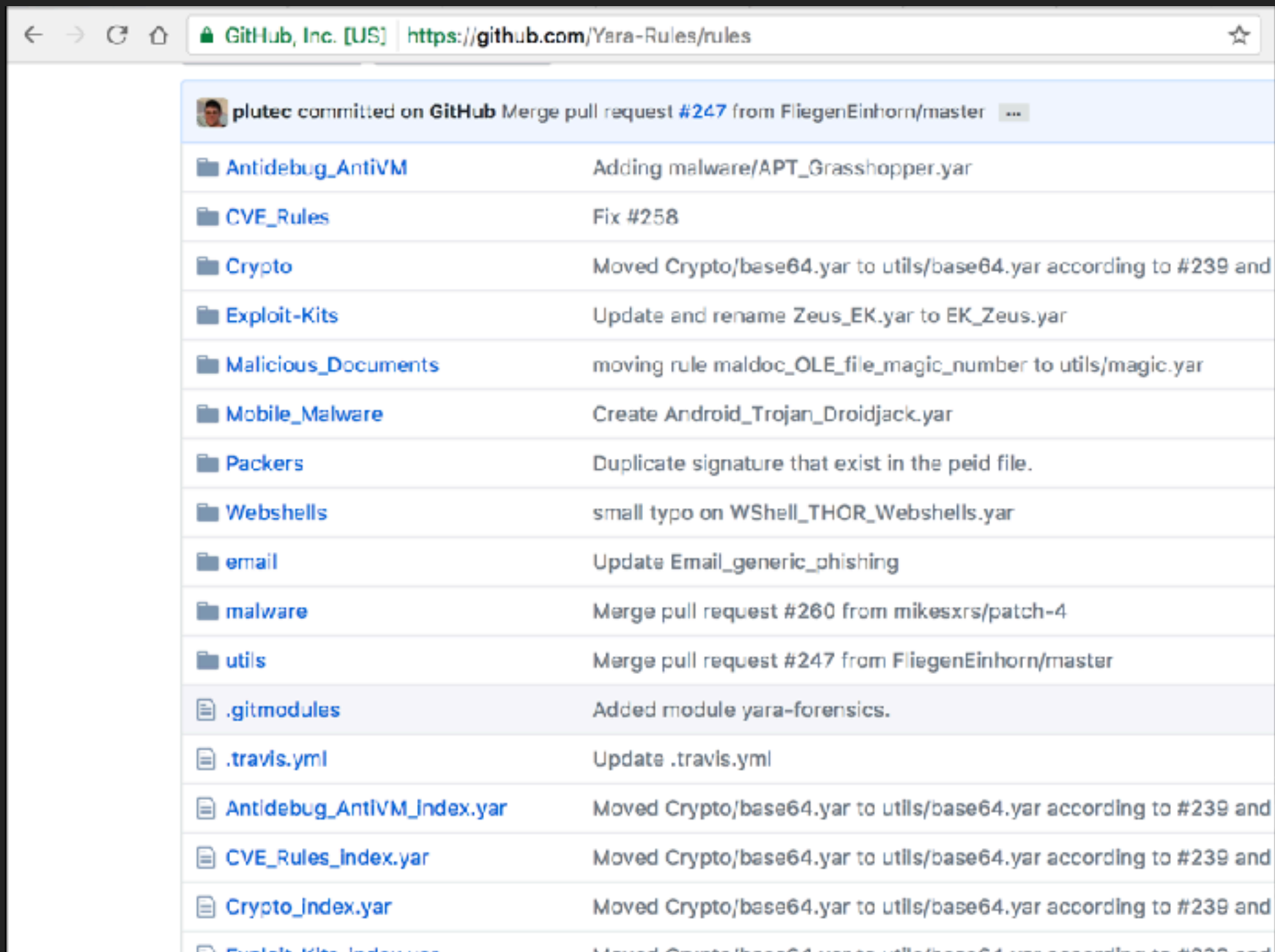


CASES OF FALSE ATTRIBUTION:

NEVER GOING TO GIVE YOU UP



RICK ROLL



A screenshot of a web browser displaying a GitHub commit page. The browser's address bar shows the URL <https://github.com/Yara-Rules/rules>. The commit is by user **plutec** and is titled "Merge pull request #247 from FliegenEinhorn/master". Below the commit message, a table lists the files changed in the commit. The files are organized into folders and individual files, with a brief description of the changes for each.

File	Change
Antidebug_AntiVM	Adding malware/APT_Grasshopper.yar
CVE_Rules	Fix #258
Crypto	Moved Crypto/base64.yar to utils/base64.yar according to #239 and
Exploit-Kits	Update and rename Zeus_EK.yar to EK_Zeus.yar
Malicious_Documents	moving rule maldoc_OLE_file_magic_number to utils/magic.yar
Mobile_Malware	Create Android_Trojan_Droidjack.yar
Packers	Duplicate signature that exist in the peid file.
Webshells	small typo on WShell_THOR_Webshells.yar
email	Update Email_generic_phishing
malware	Merge pull request #260 from mikesxrs/patch-4
utils	Merge pull request #247 from FliegenEinhorn/master
.gitmodules	Added module yara-forensics.
.travis.yml	Update .travis.yml
Antidebug_AntiVM_Index.yar	Moved Crypto/base64.yar to utils/base64.yar according to #239 and
CVE_Rules_Index.yar	Moved Crypto/base64.yar to utils/base64.yar according to #239 and
Crypto_Index.yar	Moved Crypto/base64.yar to utils/base64.yar according to #239 and
Exploit_Kits_Index.yar	Moved Crypto/base64.yar to utils/base64.yar according to #239 and

RICK ROLL

```
rule Havex_Trojan_PHP_Server
{
    meta:
        Author      = "Florian Roth"
        Date         = "2014/06/24"
        Description  = "Detects the PHP server component of the Havex RAT"
        Reference    = "www.f-secure.com/weblog/archives/00002718.html"

    strings:
        $s1 = "havex--></body></head>"
        $s2 = "ANSWERTAG_START"
        $s3 = "PATH_BLOCKFILE"

    condition:
        all of them
}
```



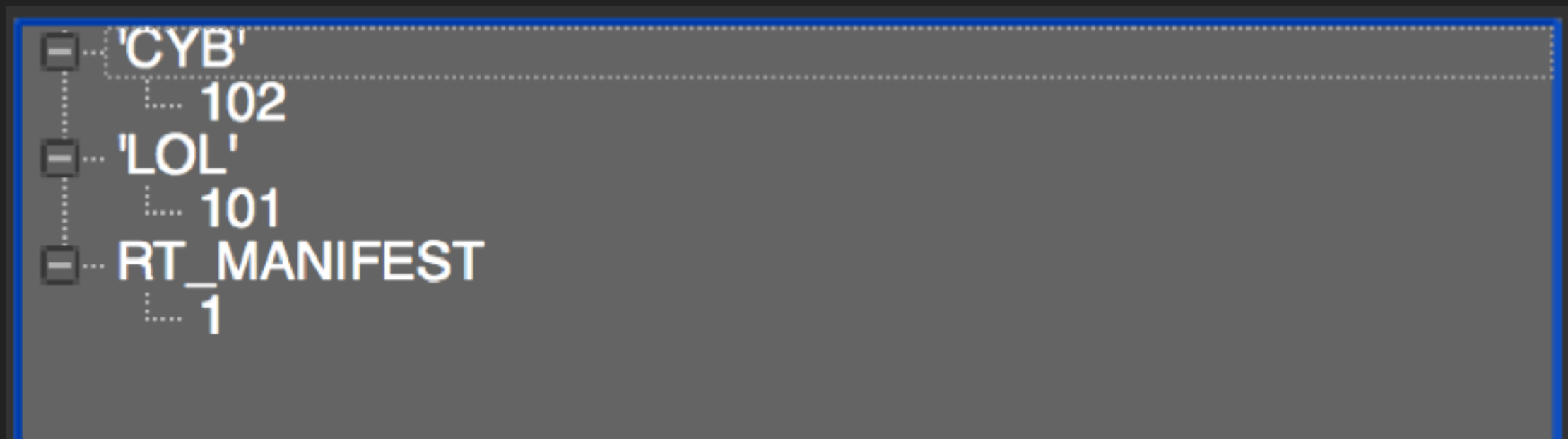
RICK ROLL

1401741d3	44	65	62	75	67	67	65	72	20	6F	72	20	74	6F	6F	6C	Debugger.or.tool
1401741e3	20	66	6F	72	20	6D	6F	6E	69	74	6F	72	69	6E	67	20	.for.monitoring.
1401741f3	64	65	74	65	63	74	65	64	21	21	21	00	00	00	00	00	detected!!!.....
140174203	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
140174213	00	00	00	00	00	00	00	00	00	00	00	90	00	00	00	00
140174223	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
140174233	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
140174243	00	00	00	00	00	00	00	00	00	00	90	FF	E0	E8	00	00 yàè..
140174253	00	00	5B	83	EB	05	EB	04	52	4E	44	0B	01	00	00	00	..[ë.ë.RND.....
140174263	00	00	00	00	00	00	00	00	00	00	00	18	10	00	00	10
140174273	00	00	00	00	00	00	00	00	00	00	00	00	10	00	00	00



RICK ROLL

- ▶ Wait a Second...



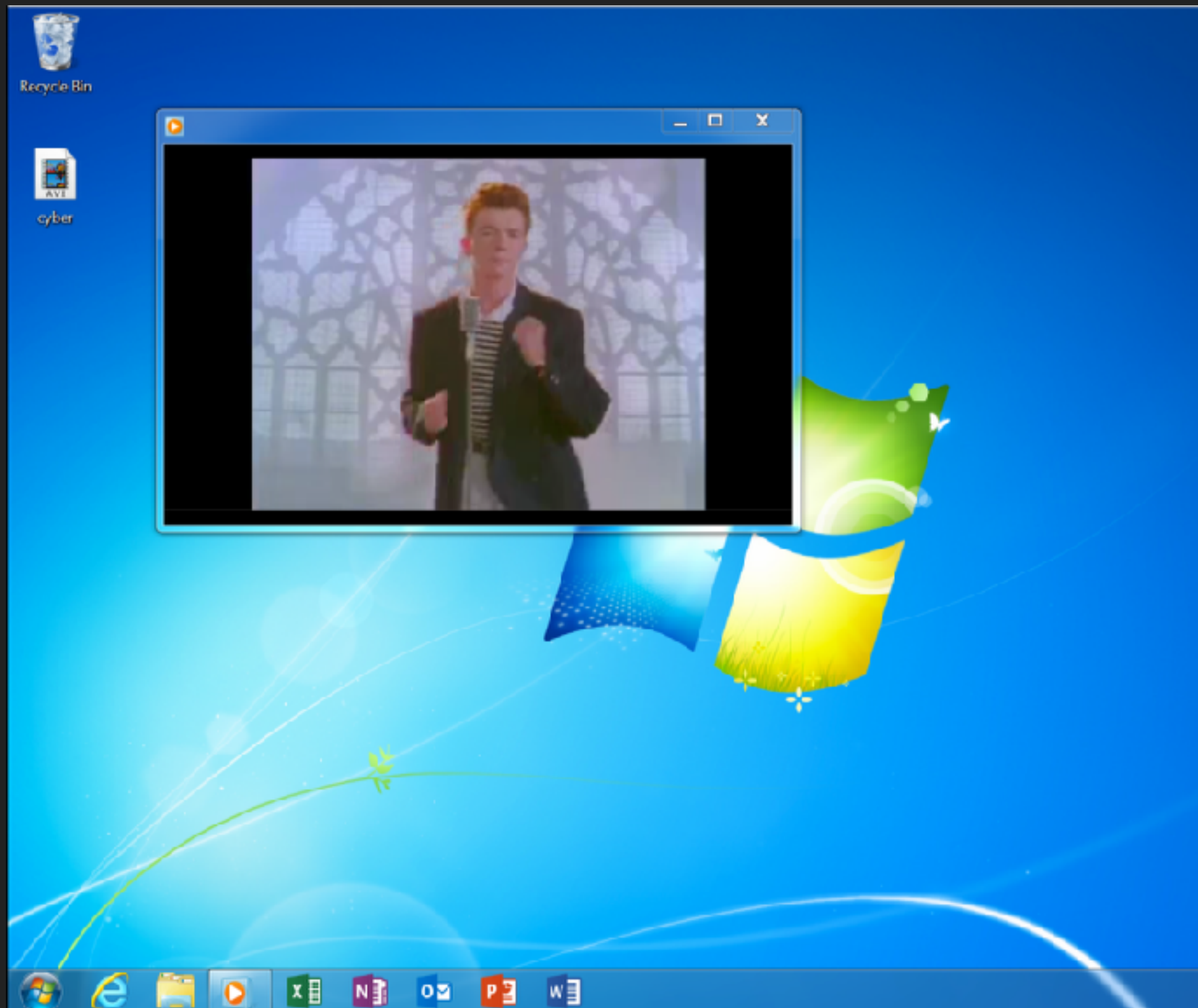
RICK ROLL

► Wait a Second...

```
if ( lpBuffer )
{
    ExpandEnvironmentStringsW(L"%temp%\\cyber.avi", &Dst, 0x208u); // drop and play the video file
    hFile = CreateFileW(&Dst, 0x120116u, 0, 0i64, 2u, 0x02u, 0i64);
    if ( hFile )
```



RICK ROLL



RICK ROLL

Search Hunting Clustering Statistics Help **New**

VirusTotal

6799845b

1 files found

File

827b2f
0dc730

Ad-Aware	Trojan.GenericKD.5096512	K7QW	Fiskware (004Ceff71)
AegisLab	Exploit.W32.Bypassuac	Kaspersky	Exploit.Win32.BypassUAC.brg
AhnLab-V3	Trojan.Win32.BypassUAC.C1947260	MAX	malware (ai score=81)
ALYao	Trojan.Agent.BypassUAC	McAfee	Artemis!0DC736990899
Antiy-AVL	Trojan.Win32.BT3Generic	McAfee-GW-Edition	Artemis!Trojan
Arcabit	Trojan.Generic.D4DCC10	MicroWorld-eScan	Trojan.GenericKD.5098512
Avast	Krile-5880	NANO-Antivirus	Exploit.Win64.BypassUAC.epomjh
AVG	Krile-5880	nProtect	Trojan-Exploit/W32.BypassUAC.2008064
AVware	Trojan.Win32.Generic!BT	Panda	Trj/Ci.A
Baidu	Win32.Backdoor.KewS.a	Qihoo-360	Win32/Trojan.ae7
BitDefender	Trojan.GenericKD.5096512	Rising	Backdoor.Pontoebl1.5637 (cloud:y2KuZFuJBRK)
CAT-QuickHeal	Exploit.BypassUAC	Sophos	Troj/DiaFox-A
ClamAV	Win.Trojan.Merong-1	Symantec	SecurityRisk.gen1
CrowdStrike	malicious_confidence_80% (D)	Tencent	Win32.Trojan.Gen.Klwk
Cyren	W64/Trojan.MHUX-6302	TrendMicro	JOKE_CYBERAVI
DrWeb	Trojan.Sggen7.22707	TrendMicro-HouseCall	JOKE_CYBERAVI
Emsisoft	Trojan.GenericKD.5096512 (B)	VBA32	Exploit.BypassUAC
F-Secure	Trojan.GenericKD.5096512	VIPRE	Trojan.Win32.Generic!BT
Fortinet	W32/BypassUAC.BRG!exploit	ViRobot	Trojan.Win64.S.Bypassuac.2008064
GData	Trojan.GenericKD.5096512	Zillya	Exploit.BypassUAC.Win32.314
Ikarus	Exploit.Win32.BypassUAC	ZoneAlarm	Exploit.Win32.BypassUAC.brg
K7AntiVirus	Riskware (0040eff71)		

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy