Noriben

Your Personal, Portable, Malware Analysis Sandbox

Brian Baskin
@bbaskin
github.com/Rurik

Origin Story

Nori-Ben:
Seaweed Lunch Box
Simplest “box” to make
Cheap
Minimal ingredients

Noriben

- Simple Malware Analysis Sandbox
  - Wrapper for Microsoft SysInternals Process Monitor (ProcMon)
  - Build a Sandbox VM with just:
    - Noriben.py
    - Procmon.exe
  - Optional:
    - Extra Procmon binary filters
    - YARA signature files
    - VirusTotal API Key
    - **Add new filters to the script**

Goals

- Quick malware analysis results
- Flexibility for open-ended runs (manually stopped analysis)
- Allow for user interaction
- Analysis of:
  - GUI apps
  - Command line args
  - Malware requiring debugging (Z-flags, code/mem altering)
  - Long sleeps (hours, days)

Focus

- Processes, File Activity, Registry Activity, Network Activity
- Log high level API calls while filtering out known noise
  - Thumbnail creation
  - Prefetch creation
  - Explorer registry keys (MRUs)
  - RecentDocs
  - Malware analysis tools (CaptureBat, IDA, FakeNet)
  - VMWare Tools
  - Java updater …

ZeroAccess

```
Processes Created:
==================
[CreateProcess] Explorer.EXE:1432 > "%UserProfile%\Desktop\hehda.exe"   [Child PID: 2520]
[CreateProcess] hehda.exe:2520 > "%WinDir%\system32\cmd.exe"    [Child PID: 3444]

File Activity:
==================
[CreateFile] hehda.exe:2520 > C:\RECYCLER\S-1-5-21-861567501-412668190-725345543-500\$fab110457830839344b58457ddd1f357\@
[MD5: 814c3536c2aab13763ac0beb7847a71f] [VT: Not Scanned]
[CreateFile] hehda.exe:2520 > C:\RECYCLER\S-1-5-21-861567501-412668190-725345543-500\$fab110457830839344b58457ddd1f357\n
[MD5: cfaddbb43ba973f8d15d7d2e50c63476] [YARA: ZeroAccess_Bin] [VT: 50/55]
[DeleteFile] cmd.exe:3444 > %UserProfile%\Desktop\hehda.exe

Registry Activity:
==================
[CreateKey] hehda.exe:2520 > HKCU\Software\Classes\CLSID\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InprocServer32
[SetValue] hehda.exe:2520 > HKCU\Software\Classes\CLSID\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\InprocServer32\ThreadingModel  =  Both
[SetValue] hehda.exe:2520 > HKCU\Software\Classes\CLSID\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InprocServer32\(Default)  =
C:\RECYCLER\S-1-5-21-861567501-412668190-725345543-500\$fab110457830839344b58457ddd1f357\n.

Network Traffic:
==================
[UDP] hehda.exe:2520 > google-public-dns-a.google.com:53
[UDP] google-public-dns-a.google.com:53 > hehda.exe:2520
[HTTP] hehda.exe:2520 > 50.22.196.70-static.reverse.softlayer.com:80
[TCP] 50.22.196.70-static.reverse.softlayer.com:80 > hehda.exe:2520
[UDP] hehda.exe:2520 > 83.133.123.20:53
```

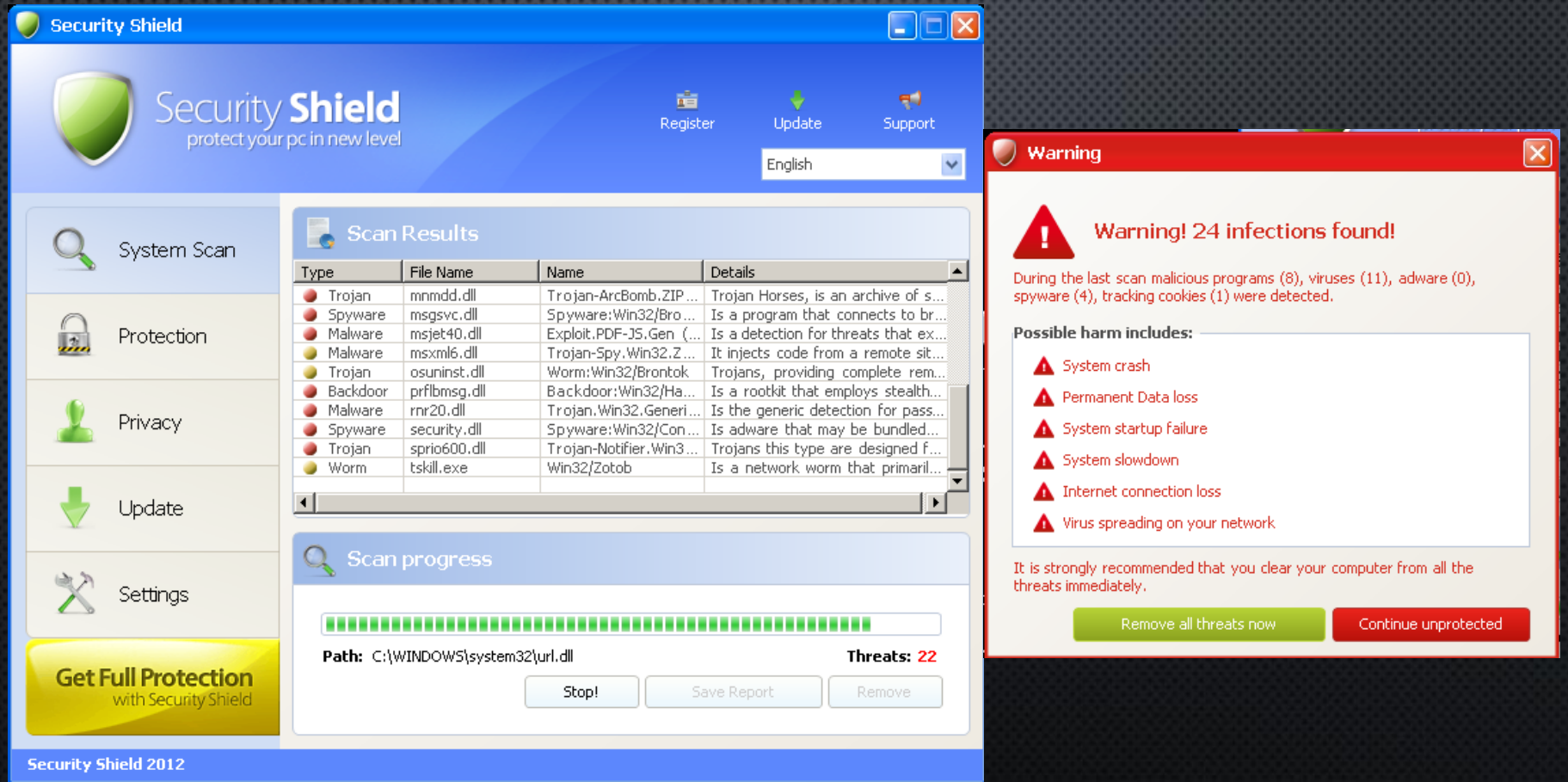
Upatre Campaign

```
Processes Created:
==================
[CreateProcess] python.exe:2752 > "malware\document.exe"    [Child PID: 3048]
[CreateProcess] document.exe:3048 > "malware\document.exe"  [Child PID: 3260]
[CreateProcess] document.exe:3260 > "%Temp%\nlibzar.exe"    [Child PID: 3632]
[CreateProcess] nlibzar.exe:3632 > "%Temp%\nlibzar.exe"     [Child PID: 4056]

File Activity:
==================
[CreateFile] document.exe:3260 > %Temp%\bwtBBCB.tmp  [MD5: fa32cacce112c18253a343c3fc41935a] [VT: Not Scanned]
[CreateFile] document.exe:3260 > %Temp%\nlibzar.exe  [MD5: 03721dc899125df9dba81f6d8d8997cf] [VT: 42/57]
[DeleteFile] nlibzar.exe:4056 > %UserProfile%\Desktop\MALWARE\document.exe
[CreateFile] nlibzar.exe:4056 > %UserProfile%\Local Settings\Temporary Internet
Files\Content.IE5\CROVKFGZ\suspendedpage[1].htm [MD5: 7acfe81f71e166364c90bfe156250da6] [VT: 0/56]
[DeleteFile] nlibzar.exe:4056 > %UserProfile%\Local Settings\Temporary Internet
Files\Content.IE5\0V0T0HC5\suspendedpage[1].htm

Network Traffic:
==================
[TCP] nlibzar.exe:4056 > 66.111.47.22:80
[TCP] 66.111.47.22:80 > nlibzar.exe:4056
[TCP] nlibzar.exe:4056 > 216.146.38.70:80
[TCP] 216.146.38.70:80 > nlibzar.exe:4056
[TCP] nlibzar.exe:4056 > 8.5.1.58:80
[TCP] 8.5.1.58:80 > nlibzar.exe:4056
```

FakeAV (Track Activity Per Button Clicked)



FakeAV (Track Activity Per Button Clicked)

```
Processes Created:
==================
[CreateProcess] python.exe:2376 > "C:\malware\FakeAV.exe"   [Child PID: 1556]
[CreateProcess] FakeAV.exe:1556 > "%WinDir%\system32\cmd.exe /c taskkill /f /pid 1556 & ping -n 3
127.1 & del /f /q C:\malware\FakeAV.exe & start C:\DOCUME~1\ADMINI~1\APPLIC~1\DPNCXX~1.EXE -f"
[Child PID: 1164]
[CreateProcess] cmd.exe:1164 > "taskkill /f /pid 1556 "   [Child PID: 1344]
[CreateProcess] cmd.exe:1164 > "ping -n 3 127.1 "     [Child PID: 2748]
[CreateProcess] cmd.exe:1164 > "C:\DOCUME~1\ADMINI~1\LOCALS~1\APPLIC~1\DPNCXX~1.EXE  -f"   [Child
PID: 776]

File Activity:
==================
[CreateFile] FakeAV.exe:1556 > %AppData%\dpncxxavk.exe  [MD5: 8915c6a007fb93b29709be2f428e5cae]
[DeleteFile] cmd.exe:1164 > C:\Malware\FakeAV.exe
[CreateFile] dpncxxavk.exe:776 > %AppData%\GDIPFONTCACHEV1.DAT  [File no longer exists]

Registry Activity:
==================
[RegDeleteValue] FakeAV.exe:1556 > HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\FakeAV
```

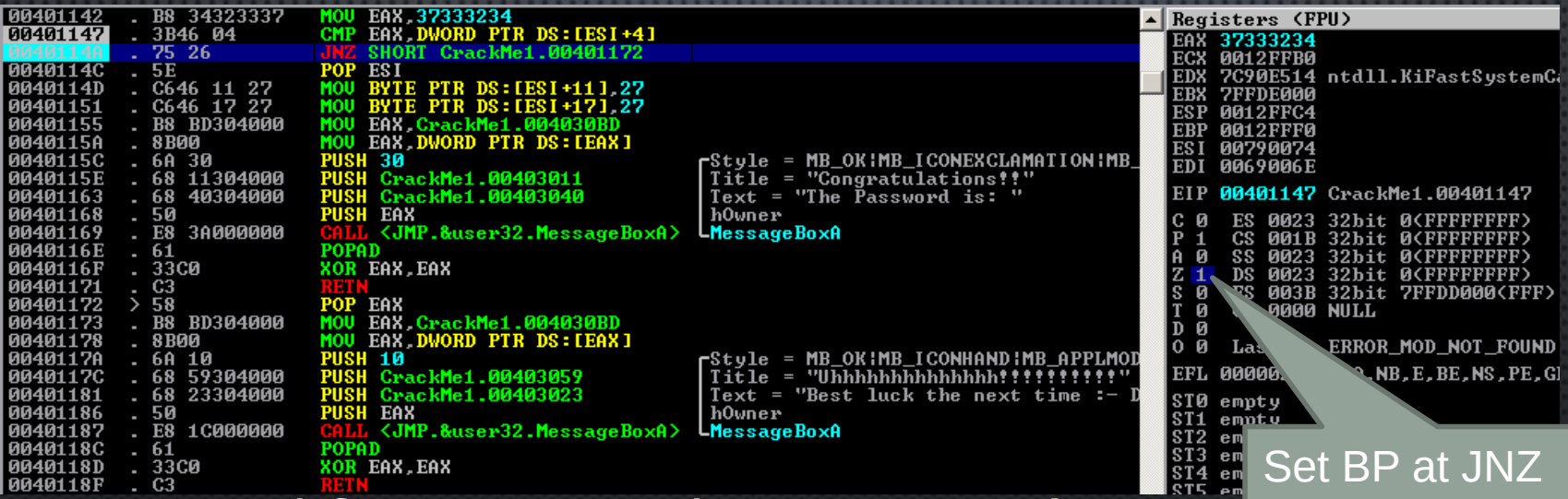
Command line (e.g. HTran)

```
Processes Created:
==================
[CreateProcess] cmd.exe:3024 > "htran"    [Child PID: 3924]
[CreateProcess] cmd.exe:3024 > "htran -h"    [Child PID: 3848]
[CreateProcess] cmd.exe:3024 > "htran -install"    [Child PID: 3688]
[CreateProcess] cmd.exe:3024 > "htran -start"    [Child PID: 4072]
[CreateProcess] services.exe:720 > "C:\Malware\htran.exe -run"    [Child PID: 268]

Registry Activity:
==================
[RegSetValue] services.exe:720 > HKLM\System\CurrentControlSet\Services\HTran\Type  =  272
[RegSetValue] services.exe:720 > HKLM\System\CurrentControlSet\Services\HTran\Start  =  2
[RegSetValue] services.exe:720 > HKLM\System\CurrentControlSet\Services\HTran\ImagePath  =
C:\Malware\htran.exe -run
[RegSetValue] services.exe:720 > HKLM\System\CurrentControlSet\Services\HTran\DisplayName  =  Proxy Service
[RegSetValue] services.exe:720 > HKLM\System\CurrentControlSet\Services\HTran\ObjectName  =  LocalSystem
[RegSetValue] htran.exe:3688 > HKLM\System\CurrentControlSet\Services\HTran\Description  =  HUC Socks5 Proxy
Service.
[RegSetValue] htran.exe:3688 > HKLM\System\CurrentControlSet\Services\HTran\Data\styk  =  0
[RegSetValue] htran.exe:3688 > HKLM\System\CurrentControlSet\Services\HTran\Data\sbpk  =  8009
[RegSetValue] htran.exe:3688 > HKLM\System\CurrentControlSet\Services\HTran\Data\schk  =  127.0.0.1
[RegSetValue] htran.exe:3688 > HKLM\System\CurrentControlSet\Services\HTran\Data\scpk  =  80
[RegSetValue] htran.exe:3688 > HKLM\System\CurrentControlSet\Services\HTran\Data\slpk  =  8009
```

Track activity per PID

Monitor Through Debugger



Set BP at JNZ
Toggle Z-Flag
…
Profit!

- Or modify memory during exec (e.g. inject decrypted data into memory)
- Noriben will just show process as “OllyDbg.exe” or “Immunity.exe”

Noriben Output

```
Processes Created:
==================
[CreateProcess] document.exe:3048 > "malware\document.exe" [Child PID: 3260]
[CreateProcess] document.exe:3260 > "%Temp%\nlibzar.exe" [Child PID: 3632]

File Activity:
==================
[CreateFile] document.exe:3260 > %TEMP%\bwtBBCB.tmp  [MD5: fa32cacce112c18253a343c3fc41935a] [VT: Not Scanned]
[CreateFile] document.exe:3260 > %TEMP%\nlibzar.exe  [MD5: 03721dc899125df9dba81f6d8d8997cf] [VT: 42/57]

Network Traffic:
==================
[TCP] nlibzar.exe:4056 > 66.111.47.22:80
[TCP] 66.111.47.22:80 > nlibzar.exe:4056
```

- Designed to be simple:
  - Show precise IOCs without much noise.
  - Easy to Copy/Paste into reports, signatures, alerts, code
- Can be an automated sandbox, works best alongside capable analyst
  - And Notepad++: double-click PID to highlight all

Options

- Pre-filter content using ProcMon Configuration (PMC) filters
  - Reduces logs from 500 MB to < 50 MB
- Import file MD5 white lists
- Generalize folder paths:
  - "C:\Users\Malware\AppData\Roaming" > %AppData%
  - "C:\Users\Malware\AppData\Local\Temp" > %Temp%

Whitelist Filters

- Simple to write!
- RegEx
- Just add to top of Noriben.py

```
cmd_whitelist = [r'%SystemRoot%\system32\wbem\wmiprvse.exe',
                 r'%SystemRoot%\system32\wscntfy.exe', ...

file_whitelist = [r'procmon.exe',
                  r'Thumbs.db$',
                  r'%SystemRoot%\system32\wbem\Logs\*', ...


reg_whitelist = [r'CaptureProcessMonitor',
                 r'HKCU\Software\Microsoft\.*\Window_Placement',
                 r'HKCU\Software\Microsoft\Internet Explorer\TypedURLs',
                 r'Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.doc',
                 r'Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs', ...
```

VirusTotal

- Query MD5 file hashes from VirusTotal
  - Requires Python-Requests library
  - API key in file “virustotal.api” (unless otherwise specified)
  - Transmits MD5 hashes ONLY (for now)
  - Raw results stored if debug (-d) is enabled:

```
[*] Writing 2 VirusTotal results to Noriben_10_Jul_15__19_24_48_028000.vt.json

[{"scan_id": "8e17d44a23c27f37be5eec94addd979560c0c0aec613750248c2306acacf527e-
1428647243", "sha1": "f0d23da00b382b33b343de8526eaae62df9b3049", "resource":
"03721dc899125df9dba81f6d8d8997cf", "response_code": 1, "scan_date": "2015-04-10
06:27:23", "permalink":
"https://www.virustotal.com/file/8e17d44a23c27f37be5eec94addd979560c0c0aec613750248c2306
acacf527e/analysis/1428647243/", "verbose_msg": "Scan finished, information embedded",
"sha256": "8e17d44a23c27f37be5eec94addd979560c0c0aec613750248c2306acacf527e",
"positives": 42, "total": 57, "md5": "03721dc899125df9dba81f6d8d8997cf", "scans":
{"Bkav":  ...
```

YARA

- Intakes a folder of YARA signatures
- Requires yara lib (from source, not pip)
- Soft fails on broken rules ☺
- Scans against every created, present file

Timeline Output (CSV)

- For automated sandbox analysis
- For knowing the timing/order of events

```
3:24:51,Process,CreateProcess,python.exe,2752,malware\document.exe,3048
3:24:51,Process,CreateProcess,document.exe,3048,malware\document.exe,3260
3:24:51,File,CreateFile,document.exe,3260,%UserProfile%\Local
Settings\Temp\bwtBBCB.tmp,fa32cacce112c18253a343c3fc41935a,,[VT: Not Scanned]
3:24:51,File,CreateFile,document.exe,3260,%UserProfile%\Local
Settings\Temp\nlibzar.exe,03721dc899125df9dba81f6d8d8997cf,,[VT: 42/57]
3:24:51,Process,CreateProcess,document.exe,3260,%Temp%\nlibzar.exe,3632
3:24:52,Process,CreateProcess,nlibzar.exe,3632,%Temp%\nlibzar.exe,4056
3:24:52,File,DeleteFile,nlibzar.exe,4056,%UserProfile%\Desktop\MALWARE\document.exe
3:24:52,File,CreateFile,nlibzar.exe,4056,%UserProfile%\Cookies\index.dat,ad8004807700f1d8d5ab6fa8c2935ef6,,
[VT: Not Scanned]
3:25:07,Network,TCP Send,nlibzar.exe,4056,66.111.47.22:80
3:25:07,Network,TCP Receive,nlibzar.exe,4056
3:25:07,File,CreateFile,nlibzar.exe,4056,%UserProfile%\Local Settings\Temporary Internet
Files\Content.IE5\0V0T0HC5\suspendedpage[1].htm,7acfe81f71e166364c90bfe156250da6,,[VT: 0/56]
3:25:15,Network,TCP Send,nlibzar.exe,4056,216.146.38.70:80
3:25:15,Network,TCP Receive,nlibzar.exe,4056
3:25:17,Network,TCP Send,nlibzar.exe,4056,8.5.1.58:80
3:25:17,Network,TCP Receive,nlibzar.exe,4056
```