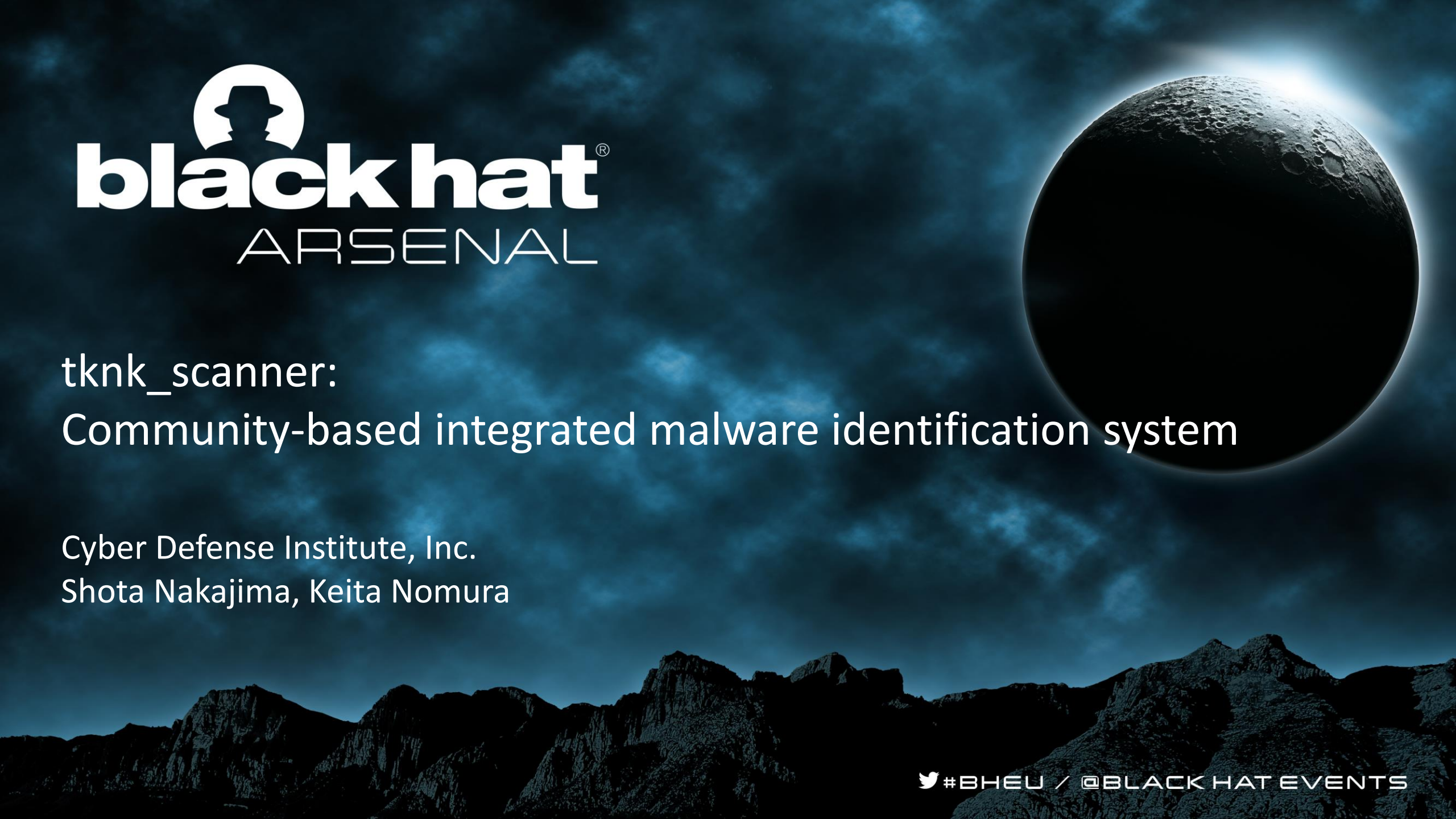

black hat®
ARSENAL
tknk_scanner:
Community-based integrated malware identification system
Cyber Defense Institute, Inc.
Shota Nakajima, Keita Nomura
#BHEU / @BLACK HAT EVENTS

Background

- Sometimes we encounter unknown malware
  - Using Antivirus software or Virus Total, yara, etc.
  - However, the detection name may not be correct or may not be useful
- Do you want to analyze similar malware over and over?
  - We would like to do other fun jobs
  - Utilize past analysis results and published information

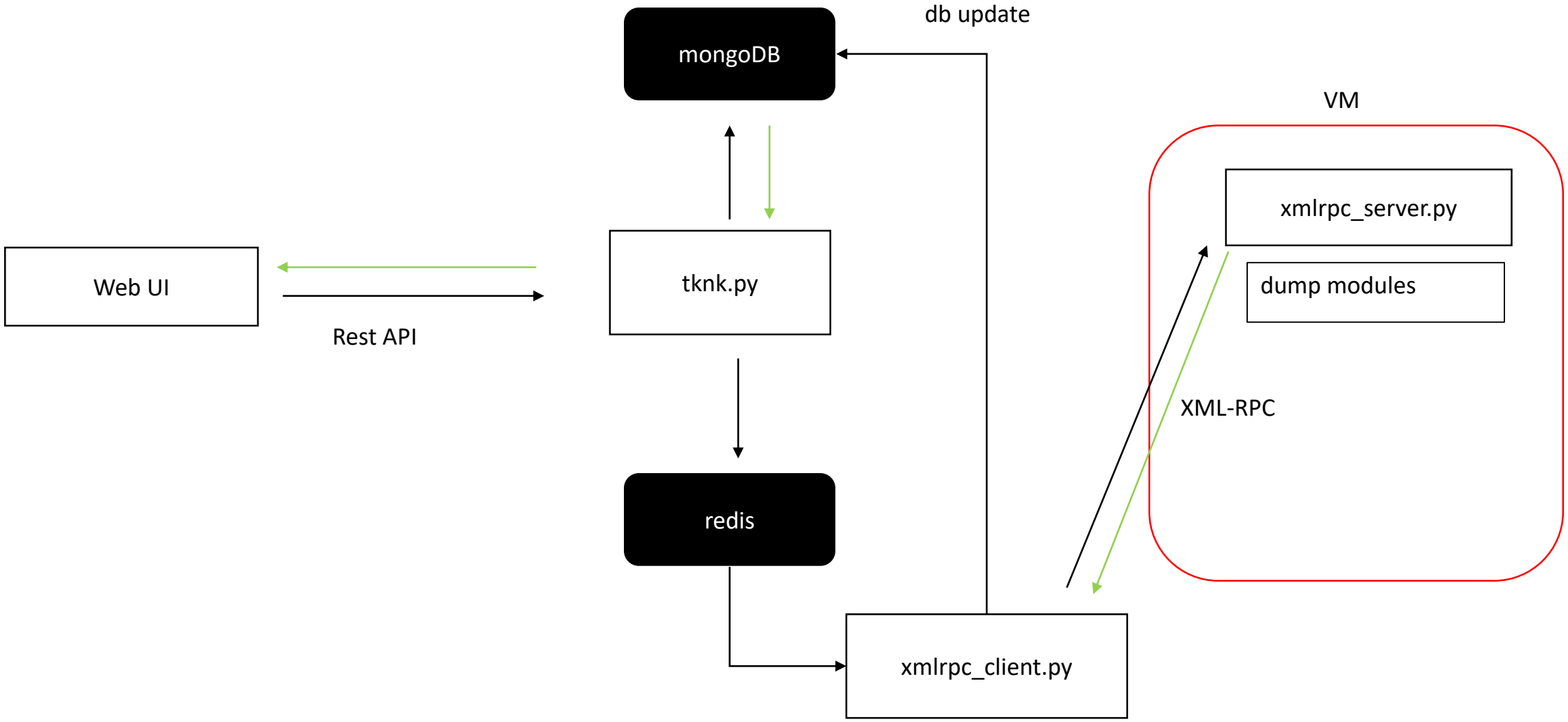
What is tknk_scanner

- Automatic identification and classification of malware
  - Scan the original malware code with yara
- Dumps original malware code
  - You can easily get the original code
- Community-based
  - Integrates multiple Open Source Software and free tools
- User-friendly Web-UI
  - Users can submit malware and check scan results using the Web-UI

Concept

- We don’t want to analyze known malware manually and label it
- If malware is obfuscated, use debuggers or other techniques
  - We can expect to get appropriate result with yara scan from original code
- Malware works most of the time
  - Except: evasive malware and APT Malware
  - Original code of malware is copied in the memory
- It is useful to automatically obtain the original code in memory and automatically identify the malware

System Overview



Features

- Scan
  - Mode
    - hollows_hunter, procdump, scylla, diff
  - yara
    - With the rules you own
- Additional Information
  - python-magic
  - Detect it easy
    - Detect It Easy is a packer identifier
    - https://github.com/horsicq/Detect-It-Easy
  - avclass
    - *AVClass is a malware labeling tool.*
    - *You give it as input the AV labels for a large number of malware samples and it outputs the most likely family name for each sample that it can extract from the AV labels.*
    - https://github.com/malicialab/avclass

Scan

tknk_scanner Scan Recent

MD5, SHA-1 or SHA Search

Processing: 0 / Queued: 0

Code on Github

tknk_scanner

File:

Select file Browse

accept only PE binary

Scan Mode:

select dump tool

Running Time:

120

Upload

[Scan]hollows_hunter

- hollows_hunter developed by @hasherezade
  - https://github.com/hasherezade/hollows_hunter
- A process scanner detecting and dumping hollowed PE modules
  - Uses PE-sieve (DLL version)
- It has powerful features
  - *Recognizes and dumps variety of implants within the scanned process: replaced/injected PEs, shellcodes, hooks, and other in-memory patches*

```
HollowsHunter v.0.1.8
using: PE-sieve v.0.1.5.0

Optional:

---scan options---
/pname <process_name>
        : Scan only processes with given name.
/hooks  : Detect hooks and in-memory patches.
/shellc : Detect shellcode implants. (By default it detects PE only).
/loop   : Enable continuous scanning.

---dump options---
/imp    : Enable recovering imports. (Warning: it may slow down the scan)
/dmode <*dump_mode>
        : Set in which mode the detected PE files should be dumped.
*dump_mode:
        0 - autodetect (default)
        1 - virtual (as it is in the memory, no unmapping)
        2 - unmapped (converted to raw using sections' raw headers)
        3 - realigned raw (converted raw format to be the same as virtual)

---output options---
/ofilter <*ofilter_id>
        : Filter the dumped output.
*ofilter_id:
        0 - no filter: dump everything (default)
        1 - don't dump the modified PEs, but save the report
        2 - don't dump any files
/kill   : Kill processes detected as suspicious
/quiet  : Print only the summary and minimalistic info.

Info:
/help    : Print this help.
/version : Print version number.
---
```

[Scan]ProcDump

- Windows Sysinternals
- https://docs.microsoft.com/en-us/sysinternals/downloads/procdump
- Execute the following command
  - procdump.exe -t -ma PID
  - Write a dump when the process terminates or after a specified time
- Please note that the size of file is large

[Scan]Scylla

- Using Scylla - x64/x86 Imports Reconstruction
  - https://github.com/NtQuery/Scylla
- Only uploaded file is dumped
- Sometimes done not dump successfully
  - The entry point value has been changed
  - The process terminates

[Scan]diff

- Dump the newly created process after malware execution using procdump
  - Get process list with EnumProcesses
  - Dump process that exists only in process list after specified time
- Please note that size of dumped files are very large

Results

tknk_scanner Scan Recent

MD5, SHA-1 or SHA Search Processing: 0 / Queued: 0

Result

Success!

Mode	hollows_hunter
Detail	Detected with yara rule!
Running Time	20
Timestamp	2018-12-03T19:39:22.487168
Download dumped file	Download

Submit File

EXE

VirusTotal Found

File Name	crypts.exe
Size	208.9KB
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	e7f2d9dad77cc34a7711be1967293c9a
SHA-1	9164e9d0c1e8e5efdc14f6845d692cf2e6609944
SHA-256	510be7c75e4bc710fca908519006502545a2d3586f5f0c08abdc27ed832b60cc

AV Class	high 2 genkryptik 2 gandcrypt 2
DIE Indicators	PE: library: MFC(4.2)[-] PE: compiler: Microsoft Visual C++(6.0)[msvcrt] PE: linker: Microsoft Linker(6.0)[EXE32]
Detect Rules	No rule detects

Dump Files

File Name	Size	Detect Rule
400000.WerFault.exe	142.3KB	GandCrab

Recent

tknk_scanner Scan Recent MD5, SHA-1 or SHA Search Processing: 0 / Queued: 0

Recent

FileName	Size	Mode	Run Time	Detect Rules	VirusTotal	Timestamp	Results
OlympicDestroyer.exe	1.9MB	hollows_hunter	60	OlympicDestroyer_Gen2 ccrewQAZ	Found	2018-12-03T19:24:14.762423	Result
193.exe	524.3KB	hollows_hunter	120	Emotet win_geodo_a2	Found	2018-12-03T19:21:47.148719	Result
34e6ca7fcd9b02405980bd6a92e20b8f972b0988e90576135c4ce12216f12f7e.exe	835.6KB	hollows_hunter	120	Ursnif_Device	Found	2018-12-03T19:19:19.802513	Result
2018-11-17-Emotet-malware-binary-updated.exe	847.9KB	hollows_hunter	120		Found	2018-12-03T19:17:42.232198	Result
crypts.exe	208.9KB	hollows_hunter	20	GandCrab	Found	2018-12-03T19:16:52.430744	Result
netwire1.exe	188.4KB	hollows_hunter	120	MAL_unspecified_Jan18_1 Suspicious_BAT_Strings Malicious_BAT_Strings win_netwire_g1	Found	2018-12-03T19:14:23.858761	Result
samsamRansomware.exe	47.1KB	hollows_hunter	120	NETexecutableMicrosoft SamSam_Ransomware_Latest	Found	2018-12-03T19:11:55.571558	Result

Jobs

tknk_scanner Scan Recent MD5, SHA-1 or SHA Search Processing: 1 / Queued: 2

Current

File Name	Mode	Running Time	Status
34e6ca7fcd9b02405980bd6a92e20b8f972b0988e90576135c4ce12216f12f7e.exe	hollows_hunter	120	

Queued

File Name	Mode	Running Time	Status
193.exe	hollows_hunter	120	
OlympicDestroyer.exe	hollows_hunter	60	

Finished

File Name	Mode	Running Time	Status
netwire1.exe	hollows_hunter	120	Results
crypts.exe	hollows_hunter	20	Results
2018-11-17-Emotet-malware-binary-updated.exe	hollows_hunter	120	Results

Limitations

- tknk_scanner does not include yara rules
  - You can download the public yara rule
  - https://github.com/Yara-Rules/rules
- Matching yara rule does not exist
  - Please write your own yara rule and share it
- Dump fails
  - Try manual analysis
- tknk_scanner is not …
  - Sandbox
    - Using **Cuckoo Sandbox**
  - Antivirus scanner
    - Using **IRMA**

Thank you!!

Any Questions?

https://github.com/nao-sec/tknk_scanner

Twitter: @nao_sec

personal account

@PINKSAWTOOTH

@nomuken