Using VirusTotal to Threat Hunt in Your Network

Brandon Levene, VirusTotal
Incident Response Consortium 2018, Arlington

HEAD OF APPLIED INTELLIGENCE

BRANDON LEVENE

Former SOC Analyst

Founding member of multiple Incident Handler, Incident Response, and Threat Research Organizations

Speaker at multiple BSides conferences and other, invite only, blue team events

Multiple threat focused publications

Alphabet Soup: OSCP, GCIH, GCIA, GPEN, GNFA, GCFA. Security+

Agenda

- Who is VirusTotal?
- What is VirusTotal Intelligence?
- Integrating VirusTotal in Your Investigations
- Investigative Use Cases
    - Alert Triage
    - IOC Expansion/Pivoting
    - Threat Hunting

VirusTotal

Who is VirusTotal?

- One of the world's largest malware intelligence services
  - 2+ Billion malware samples
  - 1 Million files uploaded per day
- Basic and advanced research capabilities
  - Crowdsourced verdicts (basic, free)
  - Threat hunting, investigation, relationship analysis (advanced, paid tiers)
- Powerful intelligence tools: YARA, Hunt, Graph
- Part of Chronicle, Alphabet's cybersecurity company

VirusTotal

What is VirusTotal Intelligence?

- VirusTotal Intelligence (VTI) sandboxing extracts behavioral and other signals
- VTI provides the ability to search through VT's dataset using:
    - Binary properties
    - Detection verdicts
    - Static properties
    - Behavior patterns
    - Submission metadata
- Access via web interface or APIs
- "I never knew I could do these things with VirusTotal!"

VirusTotal

Integrating VT in Your Investigations

- Attacker IOCs are never singular
- Attacks are never single stage
- Most malware wants, or needs, to reach out
- Use TTPs to pivot and **discover more** about who our attackers may be.

VirusTotal

01

INVESTIGATIVE USE CASE

ALERT TRIAGE

Alert Triage

Starting Point

- Piece of malware/URL/IP

What I Want To Know

- Context of my alert
- Explore associated metadata
- Related activity

VTI Approach

- VTI metadata

VirusTotal

Demo Time!

VirusTotal

02

INVESTIGATIVE USE CASE

IOC EXPANSION / PIVOTING

IOC Expansion / Pivoting

Starting Point	• Malicious domain
What I Want To Know	• Are there malicious subdomains? • Is this related to C2 activity? • What else is this domain linked to?
VTI Approach	• Graph + VTI Reports

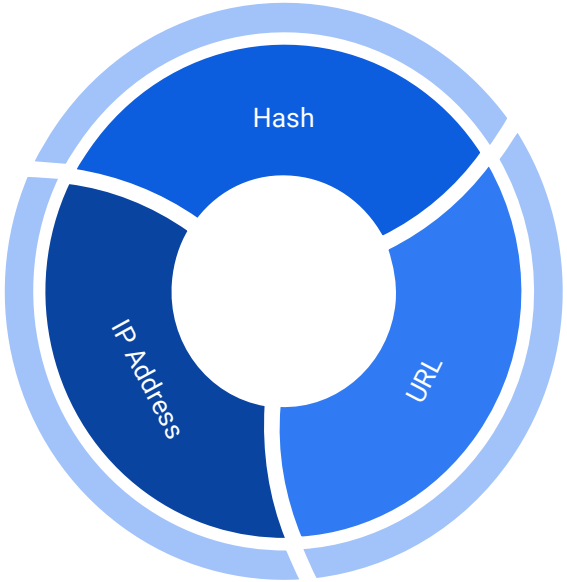
VirusTotal

Demo Time!

VirusTotal

Working Towards Better Defense

- Build context of alerts
- What else should I be looking for?
- Take indicators from one to many
- Collect multiple indicator types



VirusTotal

03

INVESTIGATIVE USE CASE

THREAT HUNTING

Threat Hunting

Starting Point	• Piece of malware/URL
What I Want To Know	• Are there other variants? • How old is my malware? • Are there other targets?
VTI Approach	• Retrohunt + YARA

VirusTotal

What is YARA?

- Tool to assist malware researchers identify and classify malware
- Identify malware in string or binary patterns
- YARA rule = strings + condition
- Useful to catalog threat actors and associated IOCs

What is a YARA Rule?

```
sample-rule {

     strings:

          $a = “malicious_string”

          $b = {56 54 59}



     condition:

          $a or $b

}
```

INDICATORS

LOGIC

VirusTotal

Crafting a Custom YARA Rule

Malware family: **TinyPOS**

- PE file
- Typically < 7kb in size
- Built-in process whitelist/blacklist
- *OPTIONAL:* Built-in persistence
- *OPTIONAL:* Local file exfiltration

Crafting a Custom YARA Rule (2)

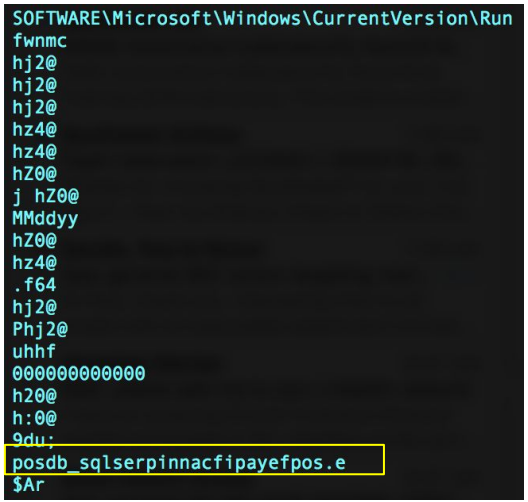
Malware family: **TinyPOS**

- PE file
- Typically < 7kb in size
- Built-in process whitelist/blacklist
- ~~*OPTIONAL:* Built-in persistence~~
- ~~*OPTIONAL:* Local file exfiltration~~

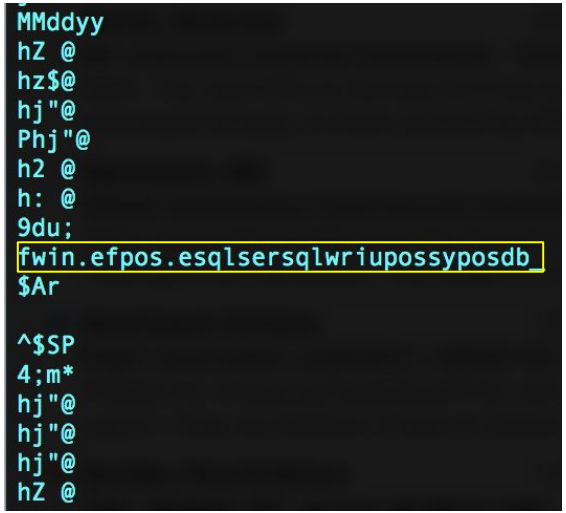
VirusTotal

Crafting a Custom YARA Rule (3)

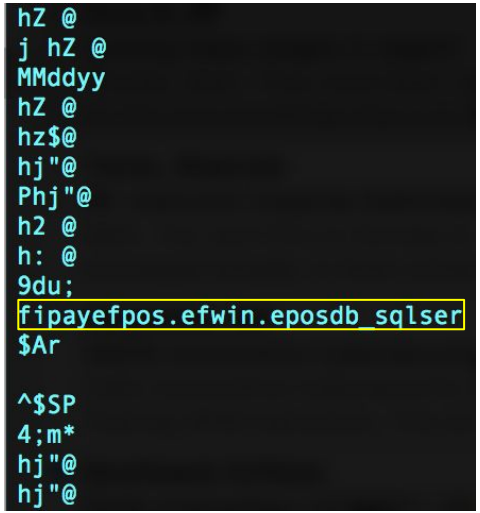
Sample #1



Sample #2



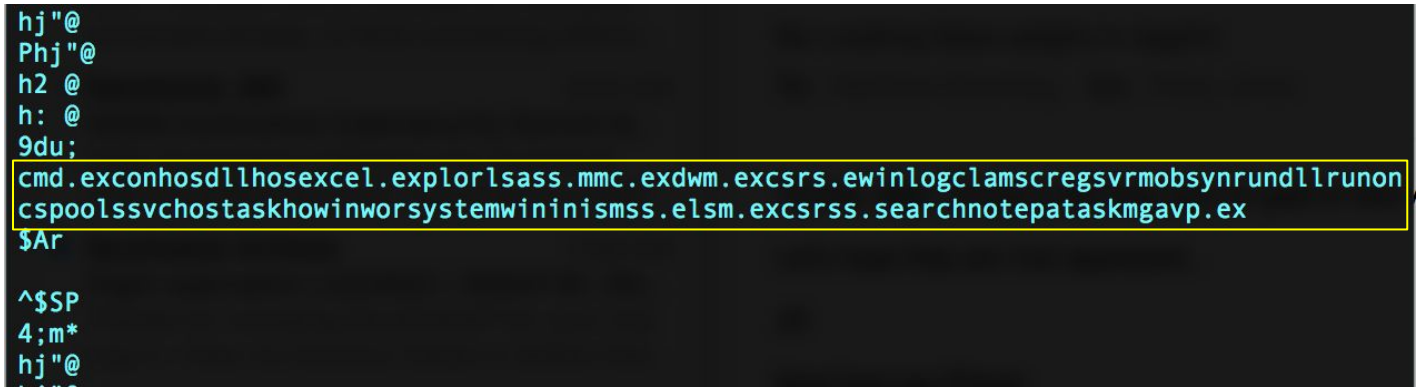
Sample #3



VirusTotal

Crafting a Custom YARA Rule (4)

Sample #4



VirusTotal

Crafting a Custom YARA Rule (5)

```
strings:

      $s1 = "fipayefpos.efwin.eposdb_sqlser"

      $s2 = "posdb_sqlserpinnacfipayefpos.e"

      $s3 = "fwin.efpos.esqlsersqlwriupossyposdb_"

      $s4 =
"cmd.exconhosdllhosexcel.explorlsass.mmc.exdwm.excsrs.ewinlogclamscregsvrmobsynrundll
runoncspoolssvchostaskhowinworsystemwininismss.elsm.excsrss.searchnotepataskmgavp.ex"
```

VirusTotal

Crafting a Custom YARA Rule (6)

```
strings:

      /* White Lists */

      $s1 = "fipayefpos.efwin.eposdb_sqlser"

      $s2 = "posdb_sqlserpinnacfipayefpos.e"

      $s3 = "fwin.efpos.esqlsersqlwriupossyposdb_"



      /* Black List */

      $s4 =
"cmd.exconhosdllhosexcel.explorlsass.mmc.exdwm.excsrs.ewinlogclamscregsvrmobsynrundl
lrunoncspoolssvchostaskhowinworsystemwininismss.elsm.excsrss.searchnotepataskmgavp.e
x"
```

VirusTotal

Crafting a Custom YARA Rule (7)

```
strings:

      /* White Lists */

      $s1 = "fipayefpos.efwin.eposdb_sqlser"

      $s2 = "posdb_sqlserpinnacfipayefpos.e"

      $s3 = "fwin.efpos.esqlsersqlwriupossyposdb_"



      /* Black List */

      $s4 = "cmd.exconhosdllhosexcel.explorlsass."
```

VirusTotal

Crafting a Custom YARA Rule (8)

```
rule POS_Sample

{

      strings:

         $s1 = "fipayefpos.efwin.eposdb_sqlser"

         $s2 = "posdb_sqlserpinnacfipayefpos.e"

         $s3 = "fwin.efpos.esqlsersqlwriupossyposdb_"

         $s4 = "cmd.exconhosdllhosexcel.explorlsass."

      condition:

         uint16(0) == 0x5a4d and filesize < 8KB and any of ($s*)

}
```

VirusTotal

Demo Time!

VirusTotal

Takeaways

- Use VTI to gain context of alerts
- Pivot from one to many
- Build out attacker IOCs
- Search for historical malware context

Better network defense

VirusTotal

Thank you.

info@virustotal.com
/in/blevene
virustotal.com/learn

VirusTotal

- Basic Malware Research
- Crowdsourced Files
- Aggregated AV Verdicts

VirusTotal Intelligence

- Advanced Malware Research
- API Integrations
- Expanded Information
- Relationship Visualization
- Hunting
- YARA Rules