



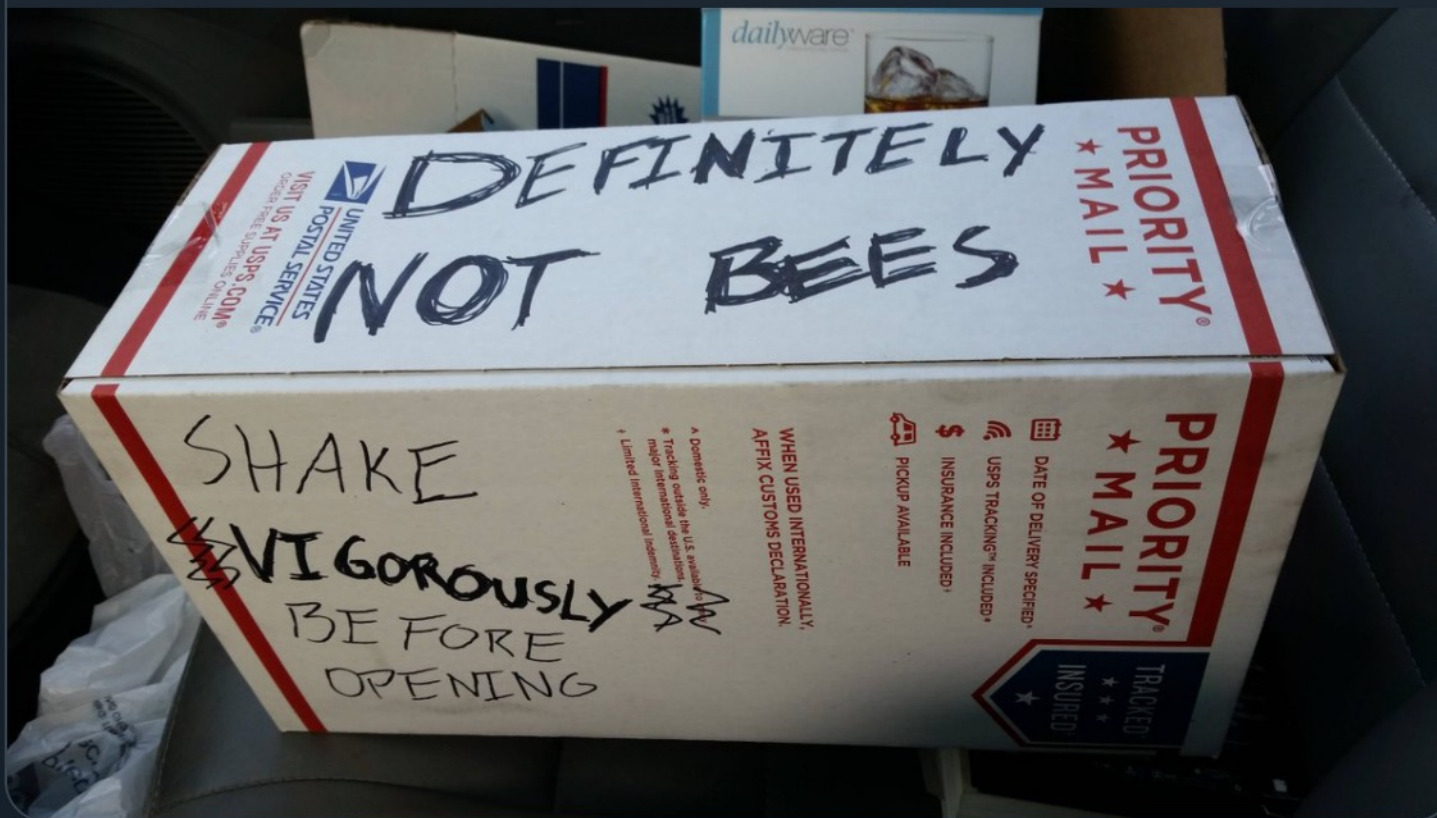
Jake Williams  
@MalwareJake



invoice.pdf.exe



WholesomeMemes @WholesomeMeme · 8h



6:04 PM · Jan 23, 2022 · Twitter for Android



# Software Reverse Engineering

COMP 272 | Spring 2022 | University of the Pacific | Jeff Shafer

## Build Your Own: Malware Analysis Lab

---

# KNOW YOUR MALWARE 101



Malware



# Dexter – December 2012

- Malware that steals credit card transactions from Windows-based POS systems (aka a card skimmer)
  - *POS = Point of Sale...*
- First seen: Mid December 2012

# Dexter

- Key capabilities
  - Code injection into `iexplore.exe`
  - Persistence via writing to Windows registry, and ensuring `iexplore.exe` restarts if stopped
  - Scan list of active processes and send to C2 server
    - *C2 = Command and Control*
  - Dump memory of POS programs and send to C2 server for data extraction

# Dexter – December 2012

- MD5 hashes of Dexter-*related* samples  
*(can be used to view analysis on malware websites or download executable)*
  - 8b27956f747791ef78faa52d2aca26a1
  - 2d48e927cdf97413523e315ed00c90ab
  - 70feec581cd97454a74a0d7c1d3183d1
  - f84599376e35dbe1b33945b64e1ec6ab
  - ed783ccea631bde958ac64185ca6e6b6
  
- **Why don't I have a single MD5 listed here?**

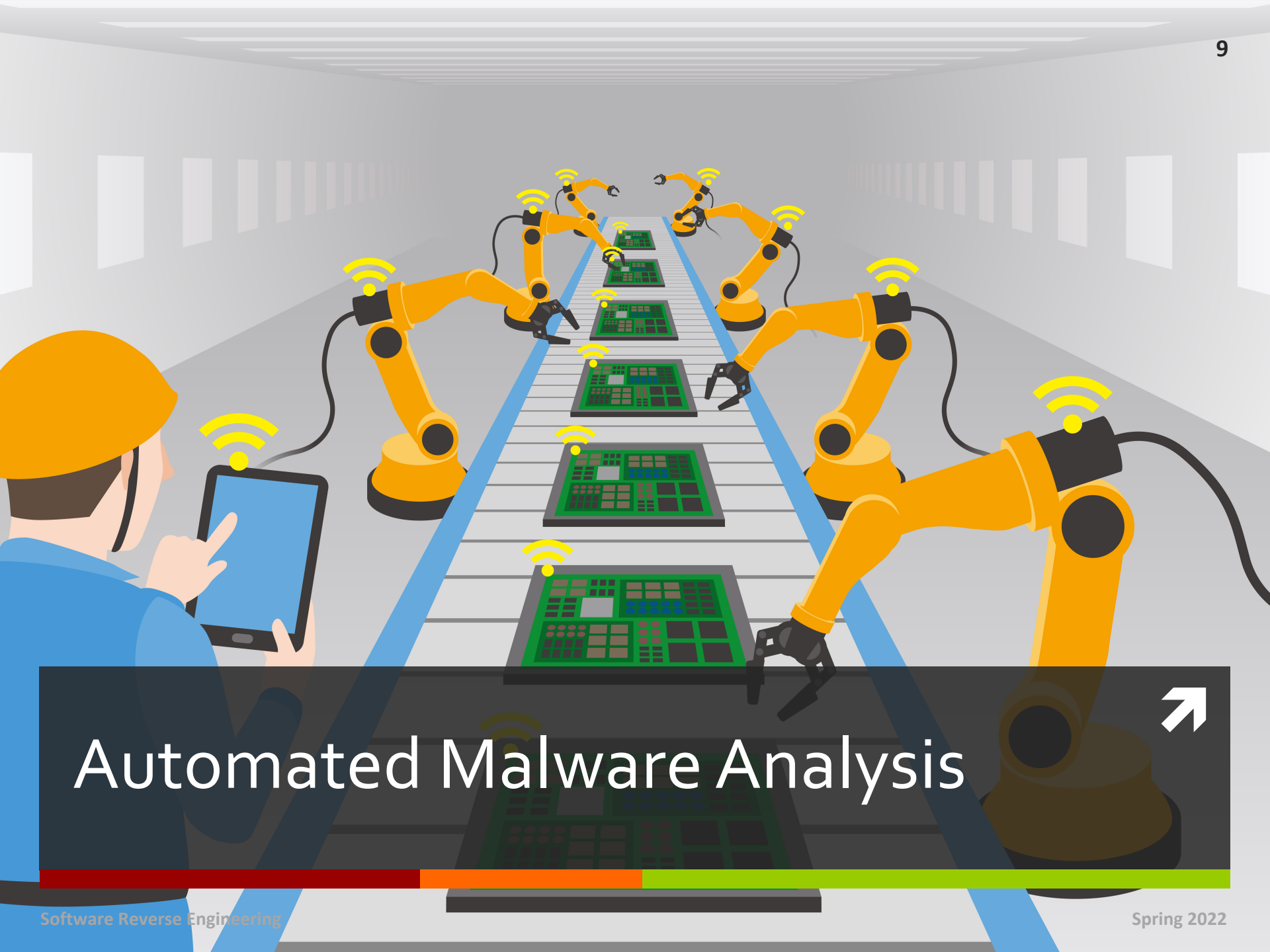
# Dexter

- <https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Dexter-Malware--Getting-Your-Hands-Dirty/>
- <https://www.secureworks.com/research/point-of-sale-malware-threats>
- <https://volatility-labs.blogspot.com/2012/12/unpacking-dexter-pos-memory-dump.html>
- Suspect this Dexter variant is being described:  
70feec581cd97454a74a0d7c1d3183d1



*Here's a  
binary.  
What  
does it  
do?*





# Automated Malware Analysis



# Automated Malware Analysis

- **Multi-AV scanners**
  - Does an anti-virus product think your sample is malicious? Check a bunch in parallel!
- **File Reputation**
  - Is this file a legitimate part of Windows, or OS X, or Adobe Acrobat, or Google Chrome, or ... ?
- **Malware Data Repositories**
  - Run static analysis on malware and view detailed results
- **Automated Sandbox**
  - What happens if the malware is run (“detonated”) in a controlled and monitored environment? What does it do?



## 44 engines detected this file

SHA-256 f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e  
 File name brbbot.exe  
 File size 74 KB  
 Last analysis 2017-11-07 09:54:05 UTC

44 / 68



Detection

Details

Community 1

### Basic Properties ⓘ

MD5 1c7243c8f3586b799a5f9a2e4200aa92  
 SHA-1 4db5a8e237937b6d7b435a8506b8584121a7e9e3  
 Authentihash 8cdecfb08525fa3a6854cfc2fcd12281e87ccd760183262b8b430e4f70dbc21e  
 Imphash 475b069fec5e5868caeb7d4d89236c89  
 File Type Win32 EXE  
 Magic PE32+ executable for MS Windows (GUI) Mono/.Net assembly  
 SSDeep 1536:b6sMD3H8V3jsUnHLiREsTbDV/480O4vh47483gLi9+LSG:b6srVzJiRrTHVORe75g4+LS  
 TRiD Win64 Executable (generic) (87.3%)  
 Generic Win/DOS Executable (6.3%)  
 DOS Executable Generic (6.3%)  
 File Size 74 KB

### Tags ⓘ

64bits

peexe

assembly

### History ⓘ

Creation Time 2015-02-25 06:12:18  
 First Seen In The Wild 2015-02-25 06:12:18  
 First Submission 2017-06-30 19:41:01  
 Last Submission 2017-09-23 22:39:07

<https://www.virustotal.com>

# brbbot.exe

Analyzed on January 23rd 2018 01:34:41 (CEST) running the *Kernelmode* monitor  
Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1  
Report generated by Falcon Sandbox v7.21 © Hybrid Analysis

**malicious**

Threat Score: 100/100  
AV Multiscan: 57%

Labeled as: [Ransom\\_Blocker.R011COOH217](#)  
Tagged as: [#ransomware](#)

[Link](#) [Twitter](#) [E-Mail](#)

- Incident Response
- Platform Intelligence
- Indicators
- File Details
- Screenshots (1)
- Hybrid Analysis (1)
- Network Analysis
- Extracted Strings
- Extracted Files (1)
- Notifications
- Community (0)

[Back to top](#)

- Sample (37KiB)
- Downloads
- External Reports
- Re-analyze
- Hash Not Seen Before
- No similar samples
- Report Abuse

## Incident Response

### Risk Assessment

- Persistence** Modifies auto-execute functionality by setting/creating a value in the registry
- Fingerprint** Reads the active computer name  
Reads the cryptographic machine GUID
- Network Behavior** Contacts 1 domain. View the [network section](#) for more details.

## Additional Context

### Platform Intelligence

**Associated SHA256s** c6745630a65c38aa182de51fccbb7280cb851c210501581cc0e0df3c420034fc

# Automated Malware Analysis

➔ **Strengths and Weaknesses of these tools used in Lab 1?**





# Automated Malware Analysis

- **Why might I not want to use these tools?**
- File may have sensitive data embedded in it – don't want to publicly release
  - Suggest looking up by hash instead of uploading file
- Attacker may be checking the major sites to see if they have been detected yet
  - Highly relevant for a *targeted* attack
  - Irrelevant for mass-market malware
  - Searching by hash may risk tipping off attacker
  - *You could run your own, private, automated tool set*
- Malware may be too well obfuscated and/or fail to do anything in automated sandbox

**Automated tools won't answer *all* of your questions**



Do it  
yourself





# Build Your Own: Malware Analysis Lab

Design Question: How do we  
*safely* and *successfully*  
examine and run malware?

# Build Your Own: Malware Analysis Lab

- **Should we use a physical machine?  
Should we use a virtual machine? (Pros/Cons?)**
  
- **Physical machine**
  - **Pros:** 100% fidelity, harder for malware to escape
  - **Cons:** Limited by number of physical computers available; Restoring state (either to pristine state or earlier state in middle of infection & analysis process) is inconvenient
    - Must image and restore full disk
    - PXE boot? Clonezilla? FOG?
  - *You may need to do this for certain malware, but not a common case*

# Build Your Own: Malware Analysis Lab

- **Should we use a physical machine?  
Should we use a virtual machine? (Pros/Cons?)**
  
- **Virtual machine**
  - **Pros:** Have as many virtual machines as you want; Snapshots make restoring state easy
  - **Cons:** Malware can *trivially* detect it is running in a VM. **Discuss...**
    - Does malware that steals business data or encrypts disks for ransom care in 2020?
    - Does malware that hijacks ATMs or industrial control systems care?

# VM Detection

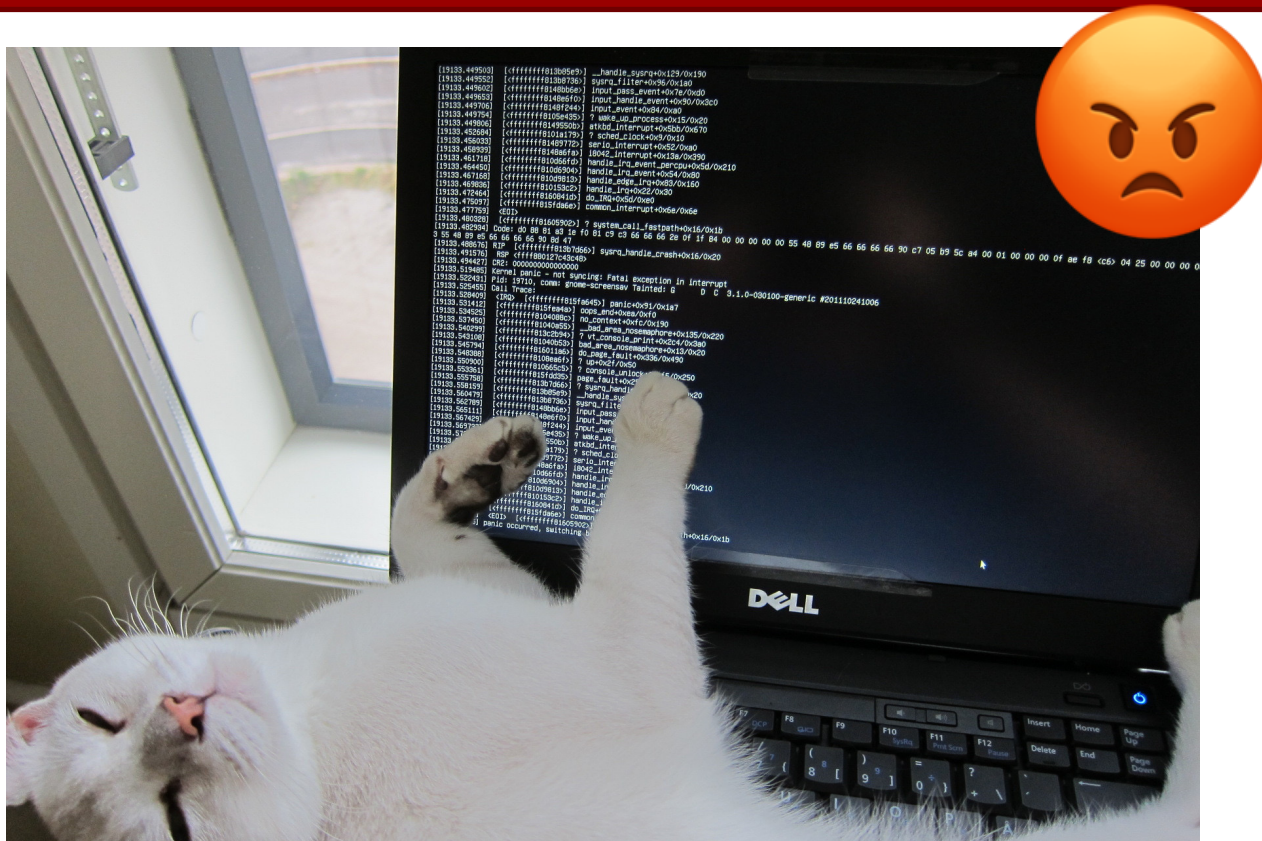
- **Q: Will the malware behave differently in a VM?**
- In 2022, with virtualization and cloud providers being universal, malware doesn't bother with detecting if it is being run in a VM
  - Lots of good data to steal is there!
  - *We can come up with specific (uncommon) scenarios where a malware author might care to write the code*
  - *Older malware (2006-2007) might care, back when VMs were new and infrequently used in business*
- **But, the attackers really care about being analyzed and will look for any signs of analysis tools**



Getty Images

# Life as a Malware Analyst

Remember, the malware authors are actively trying to subvert you



Snapshots!

Snapshots!

Snapshots!

Snapshots!

Snapshots!

**Don't be shy** with taking snapshots in your VM!

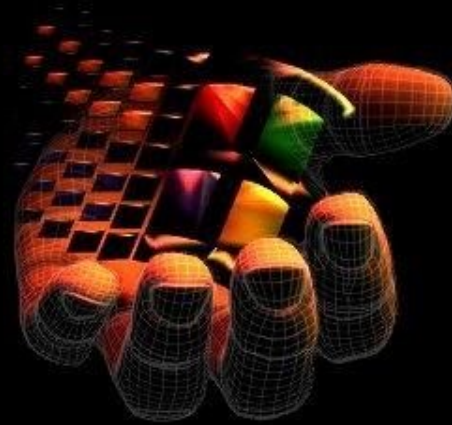
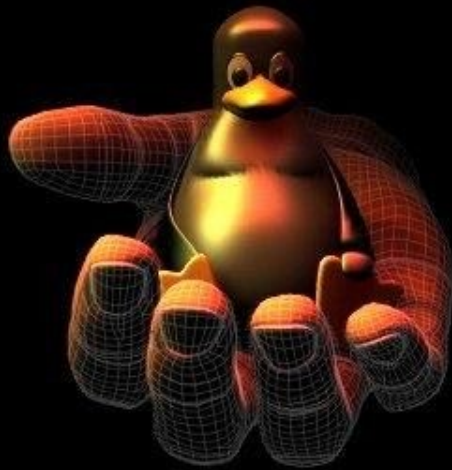
- Pristine uninfected state – restore to this **often!**
- Key points in the infection process  
*(imagine you're using a debugger, manually stepping through code, and editing variables on the fly to exercise code paths...)*
- Wherever you want to restore to without repeating your entire workflow from scratch...



# Build Your Own: Malware Analysis Lab

- **Should your VM images be Linux or Windows?  
(assume we have Windows malware to analyze)**
- **Yes**
- Need to run best tools for the job in whatever platform they are available in
- Windows: Dynamic analysis possible – you can run the malware
- Linux: Safer – no risk of accidentally running *Windows* malware





Linux / Windows

# Build Your Own: Malware Analysis Lab

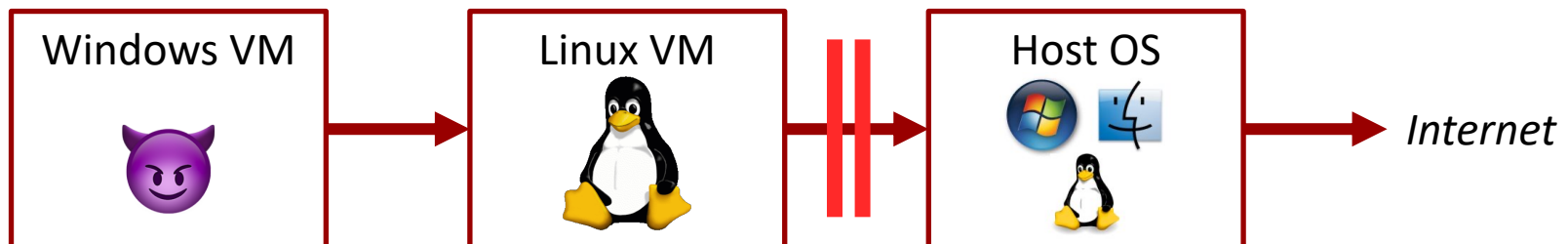
- **How do we ensure the virtual machines remain safely isolated?**
- Update the VM software often....  
Update the VM software often....  
Update the VM software often...  
*Give VMware all your money... \$\$\$*
- There are **zero-day vulnerabilities** and **escalation attacks** in hypervisors (VMWare, Virtual Box, Hyper-V)
  - **You must be running the latest supported virtualization software at all times**

# Build Your Own: Malware Analysis Lab

- **How do we isolate ourselves from the virtual machines?**
- Should I enable shared folders between my host and guest VM?
  - Ans: NO!
- Should I enable drag and drop between my host and guest VM?
  - Ans: Maybe? How paranoid are you?
- Should I use my guest VM for non-malware-analysis purposes?
  - Ans: NO!
- What is the most likely way of malware escaping?
  - Ans: **HUMAN ERROR**  
(e.g., having lots of windows simultaneous open and accidentally running malware in your *host*, not *guest VM*. Oops!)
  - Tip: Use an ugly background in your malware VM and train your mind – “I only run malware on the **fuchsia** background screen”

# Build Your Own: Malware Analysis Lab

- **How do I connect my VMs to the network?  
Do I connect them to the network? (Pros/Cons?)**
- Step 1: No network – See what the malware does
- Step 2: Configure Windows VM to route through Linux VM, and selectively enable protocols as needed during your investigation (OFF by default)



# Build Your Own: Malware Analysis Lab

- ➔ **Should the malware connect to the Internet through my business connection?**
- ➔ What will a malware author think if he checks on IP addresses making C2 requests and sees they are assigned to `MalwareExterminators.com` or `Security-consultants-r-us.com` instead of `TargetedMegaCorp.biz`?

## ➔ Options

- ➔ Tunnel through public VPN service
- ➔ Tunnel through private VPN via cloud provider
- ➔ Tunnel through TOR
- ➔ **Get a MiFi hotspot from Verizon 😊**

***Suspicious!  
Commonly  
blocked.***

*Odds of  
legitimate target  
vs researcher or  
law enforcement  
not in attacker's  
favor.*

# Build Your Own: Malware Analysis Lab

- Related Tip: Don't just use normal `wget` to fetch a suspicious file from a website
  - Any competent attacker will monitor their logs and pick out the user agent!
  - At a minimum, spoof a real user agent
  - *(You would never use a real web browser, since you want full control over the downloading process)*
  
- **General point: You don't want the attacker to know that you are investigating them for any serious *targeted* attack**



# Analysis Tools




# Build Your Own: Malware Analysis Lab

- **What tools do we need in the lab?**
- **Static property analysis** (program *not* running)
  - PEStudio, Strings, BinText, ...
- **Interactive behavioral analysis** (program *is* running)
  - Process Hacker, RegShot, Wireshark, API Monitor, ...
- **Code analysis/reversing (We ♥ Assembly)**
  - IDA Pro, Ghidra, x64dbg, OllyDbg, ...



# Pre-Lab

- **Download (see link in Canvas announcement):**  
Windows 10 x64 Reverse Engineering  
Malware.ova
- **Import OVA file into a new VM**
  - **Open Virtual Appliance**



Ready by  
Next Class