Malware Detection and Removal

Jake Smith
University of Virginia

Cybersecurity News Segment


EXIT
CYBER CUP


CNS@UVA
@cnsatuva
Following
Congrats to our team that competed in @ritsecclub's ISTS 17 for placing 2nd overall!
6:24 PM - 24 Feb 2019

[cs-ugrads] Georgia Weidman is speaking in the Penetration Testing course this Friday ... and you are invited!

I

Ibrahim, Ahmed (ai4z) to cs-ugrads@virginia.edu

Feb 25

Hello everyone,

You are invited to attend Georgia Weidman's talk, this Friday (3/1), as a guest speaker in the "Penetration Testing" course (starting at 2:30 pm in Rice 340). Georgia is the author of the "Penetration Testing: A Hands-On Introduction to Hacking" textbook which we are using in the first part of the "Penetration Testing" course. On Friday, she will talk about her penetration testing experience, how the real penetration testing environment is different from a classroom environment, and the art of writing penetration testing reports.

Disclaimer:

Only perform attacks on networks you own or are specifically authorized to. This information is for educational purposes only. The author is not liable for any misuse or damage.

NICE Challenge Portal

- Visit: https://portal.nice-challenge.com
- Sign-in with your username/password
  - Should have been emailed
  - Usernames look like virginia-jts5np
- Click Workspaces Available
- Malicious Malware (Complexity 1) -> Deploy

What is Malware?

- “software designed to disrupt, damage, or gain unauthorized access to a computer system”
  - -Dictionary.com
- Includes Virii, Worms, Trojans, Ransomware, RATs/Backdoors, and Droppers
- Compromises the computer’s integrity 😉

What is *not* Malware?

- Additional programs that provide some sort of functionality (ie a web server that just happens to be installed)
- Scanning, Remote Admin Tools are not inherently malicious (even if they can be abused)

Malware Objectives

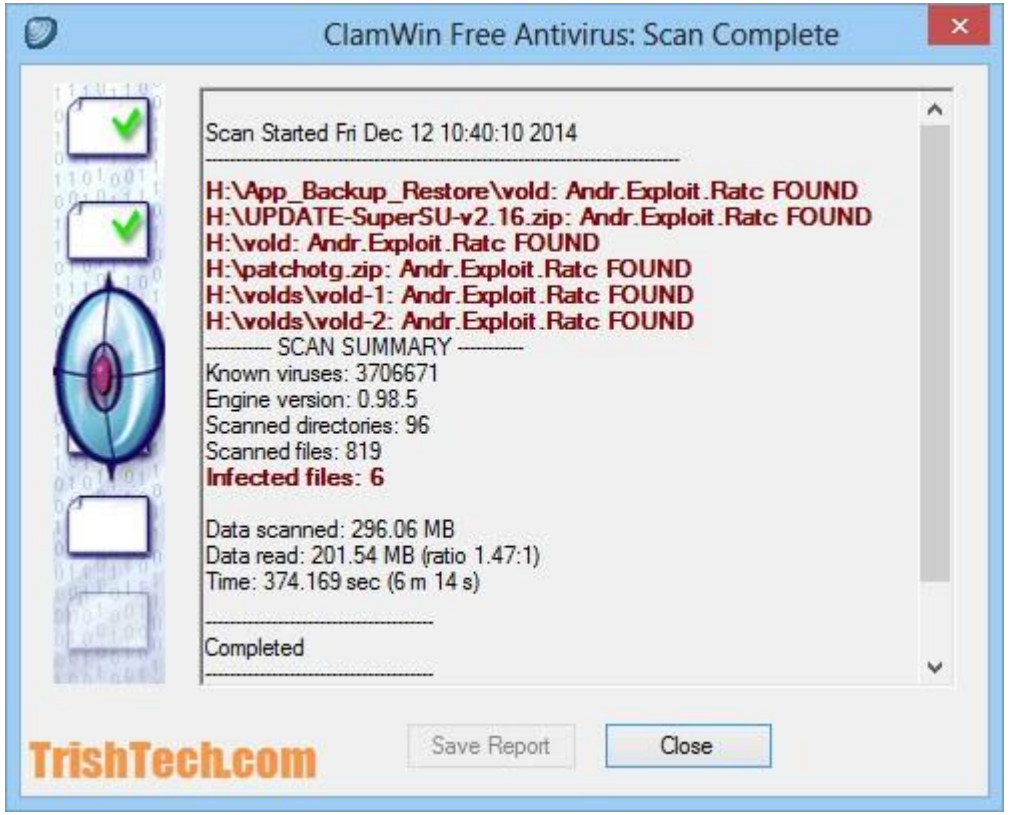
- Data: Intellectual Property, PII, PHI, Intelligence
- Dollars: Cryptocurrency, Financial Info
- Damage: Cause physical damage/harm, influence opinion

Defensive Response: Identification & Removal

Where might we find malware?
(on Windows, finding less sophisticated malware)

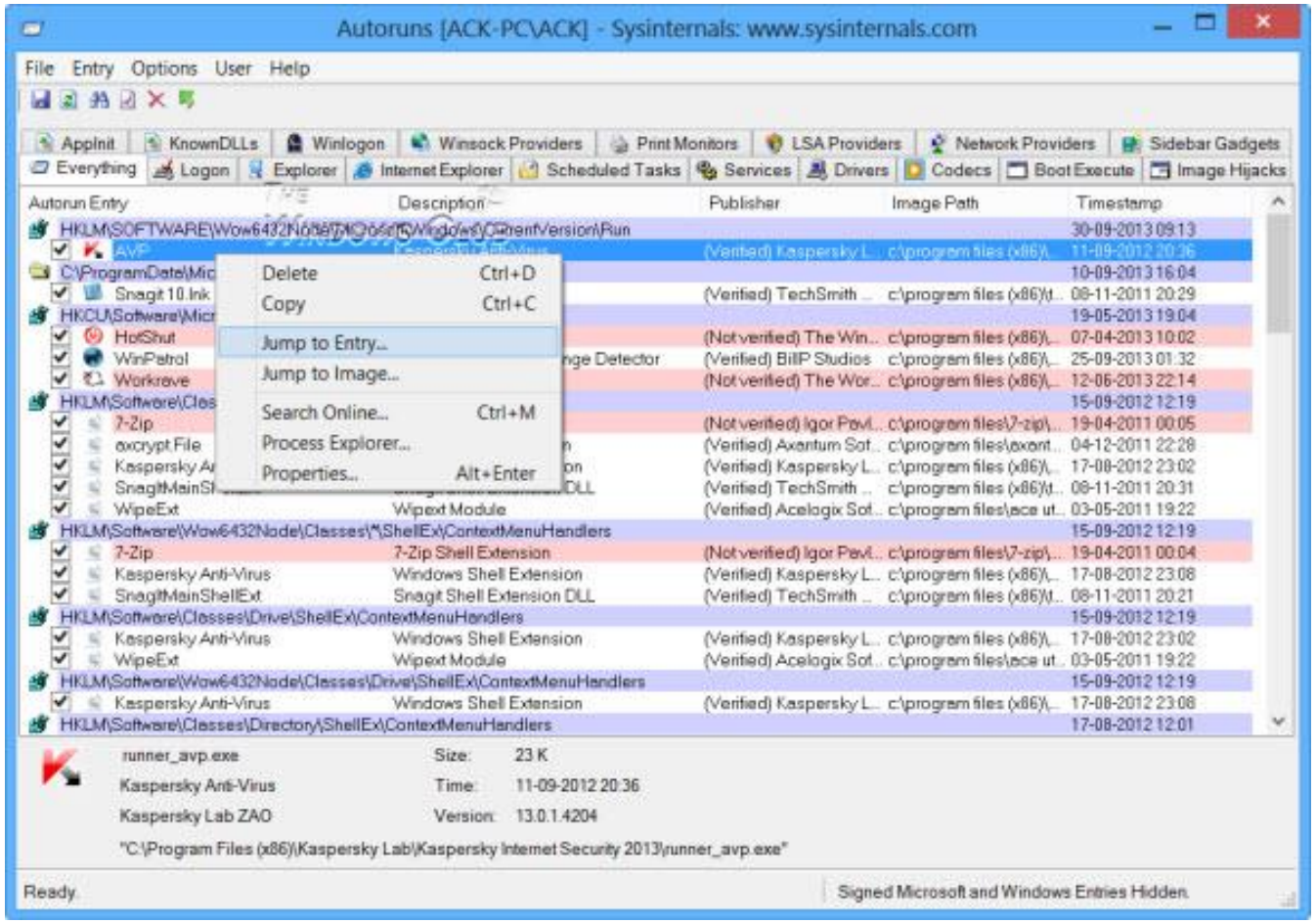
- Locations to examine
  - C:\Program Files and C:\Program Files (x86)
  - Hidden Folders (ie C:\ProgramData)
  - Installed Programs List
  - Registry Keys (scary)
- What else?

Our Toolkit: ClamAV



- Free, Open-Source AV
- Primarily based on signatures

Our Toolkit: SysInternals Autoruns

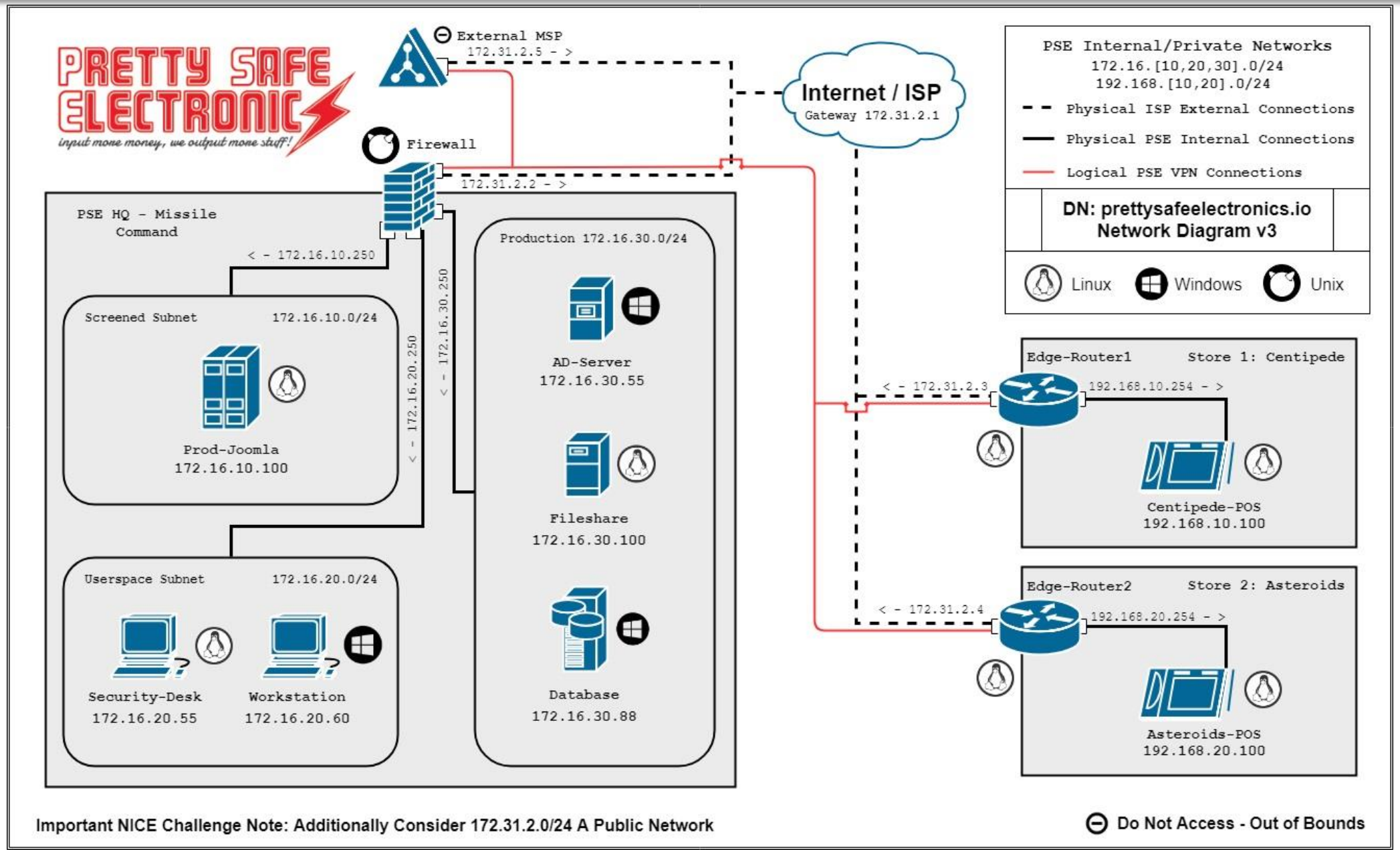


- Part of free SysInternals kit by Microsoft
- Lists automatically running things / detects non-signed things

The Scenario

- We've noticed that our Domain-Controller has had some unauthorized usage by one of our interns and is now exhibiting some odd behavior. We believe it to be some type of malware that is causing the odd behavior. We need you to find the malware and remove it in order to prevent further harm to our system.

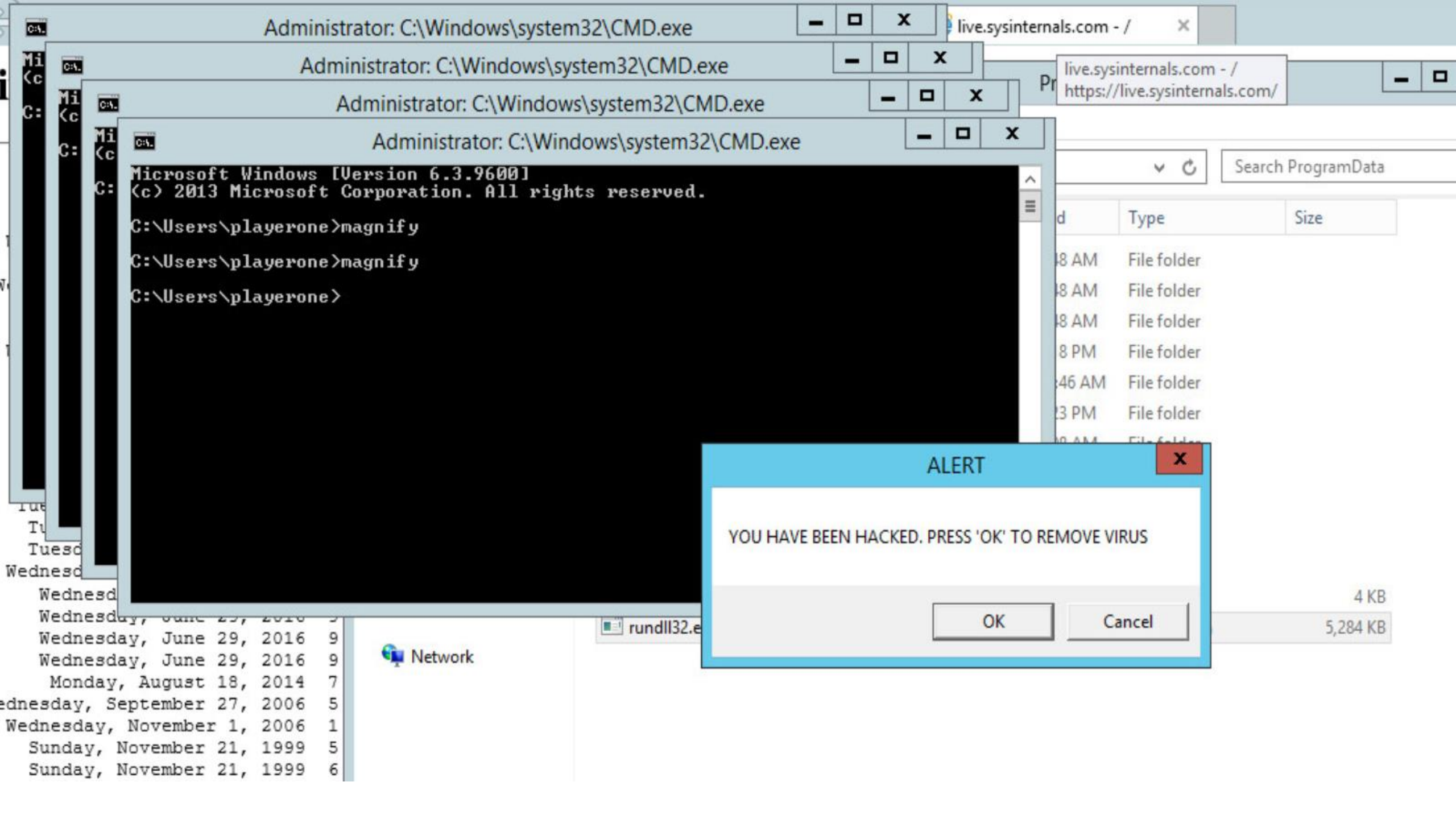
Network Topology



The Scenario (Continued)

- Two Goals:
  1. Malicious Malware Quarantined on Security-Desk
  2. All Instances of Windows Malware Removed

Let me know if you need help transferring the located malware to the Security-Desk Machine


Administrator: C:\Windows\system32\CMD.exe
Administrator: C:\Windows\system32\CMD.exe
Administrator: C:\Windows\system32\CMD.exe
Administrator: C:\Windows\system32\CMD.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\playerone>magnify
C:\Users\playerone>magnify
C:\Users\playerone>
live.sysinternals.com - /
live.sysinternals.com - /
https://live.sysinternals.com/
Search ProgramData
Type
Size
File folder
ALERT
YOU HAVE BEEN HACKED. PRESS 'OK' TO REMOVE VIRUS
OK
Cancel
Network
rundll32.e
4 KB
5,284 KB
Wednesday, June 29, 2016
Monday, August 18, 2014
Wednesday, September 27, 2006
Wednesday, November 1, 2006
Sunday, November 21, 1999
Sunday, November 21, 1999

When you find our your DC has been infected

When you find our your DC has been infected

Who ya gonna call?

Questions?

Sources

- NICE Challenge Portal
- Dictionary.com
- Various Internet Sources for the Pikachu Photos