# Adylkuzz

## How Peak Medical Was Cryptomined by the Best

Brian Ascani
Jennifer Gibbs
Oscar Ortega
Ed Gomez

Peak Medical Supplies

# Table of Contents

# 01 Introduction

This document summarizes our analysis of Adylkuzz and contains the following:

- Static Analysis
- Dynamic Analysis
- Summary of Functionality
- Containment Strategy
- Awareness Training

This analysis was performed using the static and dynamic analysis results furnished by Any.Run and VirusTotal and considers speculative analysis on containment strategies and awareness and training of employees.

# 02 Static Analysis

## 2.1 Synopsis of Executable

This section contains a summary of the uploaded executable files.

The file type is Win32 EXE and the size is 1.4 MB ( 1450500 bytes ). Reports of this malware started in April of 2017.

Below are the file names used in the execution:

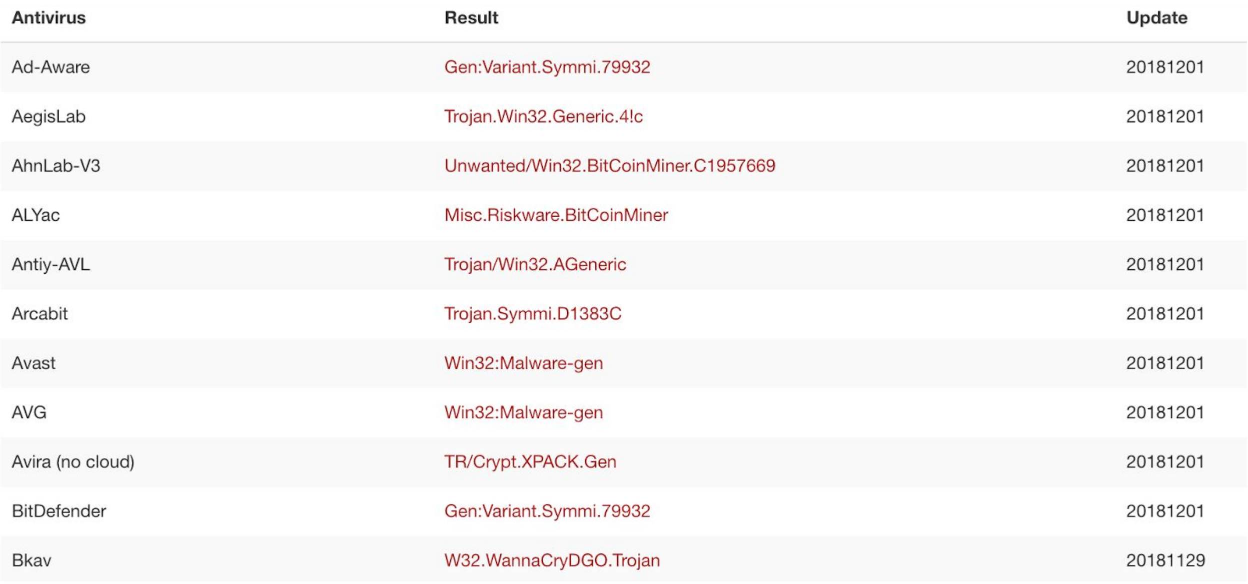
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf23.exe
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233.exe
adylkuz.exe
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233.bin
wuauser.exe
Adylkuzz.B spread via EBDP
Adylkuzz.B.Exe
170517-7.Ransom.CoinMiner.exe
wuauser.exe
Adylkuzz.B.exe
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf23

3.exe
3165616.exe
localfile~
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf23
3.vir.DNvir
test.exe
adylkuzz.exe
8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf23
3.exe

The analysis by any.run was completed on November 30, 2018.

The first submission was May 14, 2017 and last submitted on December 1, 2018.

This malware has been active for about 19 months. The malware is still a risk for PC's that have not updated their OS which includes the patch for the vulnerability on port 445. The different anti-virus scanners determined this malware was a Trojan. Other anti-virus scanners labeled this malware as a coinminer and WannaCry. Interestingly enough Adylkuzz predates the WannaCry Ransomware.



| Antivirus | Result | Update |
|---|---|---|
| Ad-Aware | Gen:Variant.Symmi.79932 | 20181201 |
| AegisLab | Trojan.Win32.Generic.4!c | 20181201 |
| AhnLab-V3 | Unwanted/Win32.BitCoinMiner.C1957669 | 20181201 |
| ALYac | Misc.Riskware.BitCoinMiner | 20181201 |
| Antiy-AVL | Trojan/Win32.AGeneric | 20181201 |
| Arcabit | Trojan.Symmi.D1383C | 20181201 |
| Avast | Win32:Malware-gen | 20181201 |
| AVG | Win32:Malware-gen | 20181201 |
| Avira (no cloud) | TR/Crypt.XPACK.Gen | 20181201 |
| BitDefender | Gen:Variant.Symmi.79932 | 20181201 |
| Bkav | W32.WannaCryDGO.Trojan | 20181129 |

Figure 2.1: Examples of Anti-Virus Scan results.

## 2.2 Initial Behavior

The table below summarizes the initial activity generated by Adylkuzz upon upload to Any.Run's VM environment.

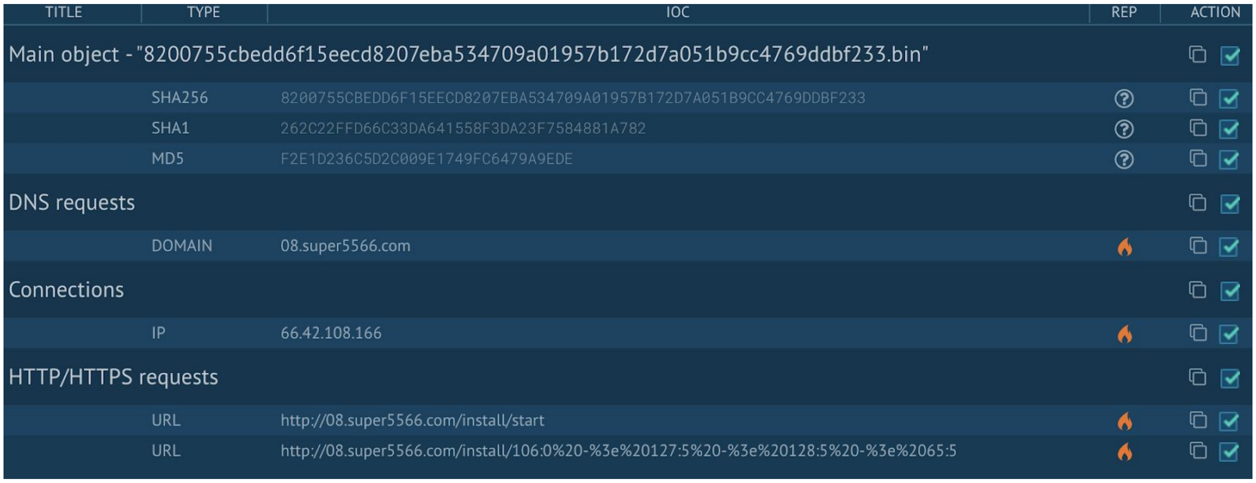
| Activity Type | Count |
|---|---|
| HTTP Requests | **2** |
| DNS Requests | **1** |
| Connections | **2** |
| Files Changed | **None** |

Figure 2.2: Table summarizing the initial activity generated by Adylkuzz.

While there were no files changed, the malware is being studied as a portable executable file. The Portable Executable (PE) format is a file format forexecutables, object code, DLLs, FON Font files, and others used in 32-bit and 64-bit versions of Windows operating systems. There were 12 different files used in the attack.

In addition, Any.Run reported the following threats.

- **Name**: Danger: Connects to a CnC server.



| TITLE | TYPE | IOC | REP | ACTION |
|---|---|---|---|---|
| Main object - "8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233.bin" | | | | ⧉ ☑ |
| | SHA256 | 8200755CBEDD6F15EECD8207EBA534709A01957B172D7A051B9CC4769DDBF233 | ? | ⧉ ☑ |
| | SHA1 | 262C22FFD66C33DA641558F3DA23F7584881A782 | ? | ⧉ ☑ |
| | MD5 | F2E1D236C5D2C009E1749FC6479A9EDE | ? | ⧉ ☑ |
| DNS requests | | | | ⧉ ☑ |
| | DOMAIN | 08.super5566.com | 🔥 | ⧉ ☑ |
| Connections | | | | ⧉ ☑ |
| | IP | 66.42.108.166 | 🔥 | ⧉ ☑ |
| HTTP/HTTPS requests | | | | ⧉ ☑ |
| | URL | http://08.super5566.com/install/start | 🔥 | ⧉ ☑ |
| | URL | http://08.super5566.com/install/106:0%20-%3e%20127:5%20-%3e%20128:5%20-%3e%2065:5 | 🔥 | ⧉ ☑ |

Figure 2.3: Table summarizing Indication of Compromises

# 03 Dynamic Analysis

The results below were generated by executing a sample of Adylkuzz on Any.Run's hosted platform. The Dynamic Analysis will discuss privileges being used, version information, different protocols used over the network and any file modifications/additions taking place.

## 3.1 Process Environment

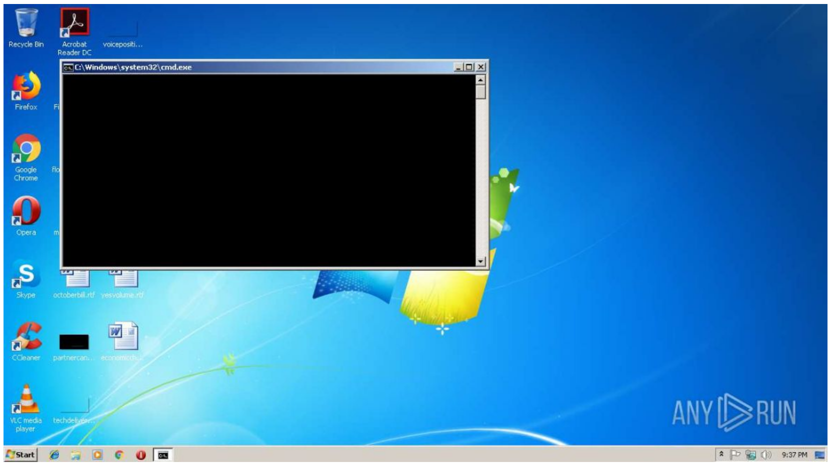
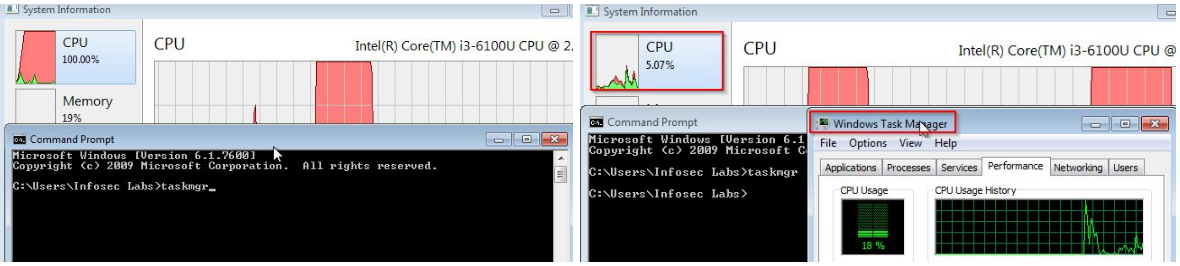


Figure 3.1: Showing the Initial Process of Adylkuzz running on the Any.Run VM by opening command lines in a Windows 7 environment.

When the Adylkuzz payload is added to our system, it runs as Administrator giving it access to run all the processes it needs to mine coin from our computers. Initially, there are some fireworks with command lines popping up as seen in Figure 3.1 but after that it safely runs in the background and the only notice of infection would be general slowness and louder fan noises. The general slowness includes taking a long time for the operating system to load or long wait times for things to show up on the screen. This slowness comes from the malware's main malicious intent which is to use 100% of the CPU's processing power to mine the coin. We can see from Figure 3.2 below that Adylkuzz has a protective quality in that it will check if task manager is running. If the task manager is on, however, the miner will turn itself off to avoid detection and every minute it will look to turn itself back on.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Infosec Labs>taskmgr_
```

```
Microsoft Windows [Version 6.1
Copyright (c) 2009 Microsoft C

C:\Users\Infosec Labs>taskmgr

C:\Users\Infosec Labs>
```

Figure 3.2: When the Task Manager is not running, we can see 100% CPU usage, when the Task manager is on we can see that Adylkuzz is not using the CPU and percentage goes Back to normal and when it's off again, the miner turns back on and uses 100% usage.

## 3.2 Network Activity

After Adylkuzz runs netsh.exe, a specific type of network command line, to add firewall rules to the infected system, it obtains the public IP address of Peak Medical and uses it to attempt to connect to the hackers web server. Because our systems have never seen their IP address, it uses a protocol called DNS, which stands for Domain Name System, that links the target address with the domain. Specifically, this is going to link 66.42.108.166 to the address 08.super5566.com which is the hacker's domain.

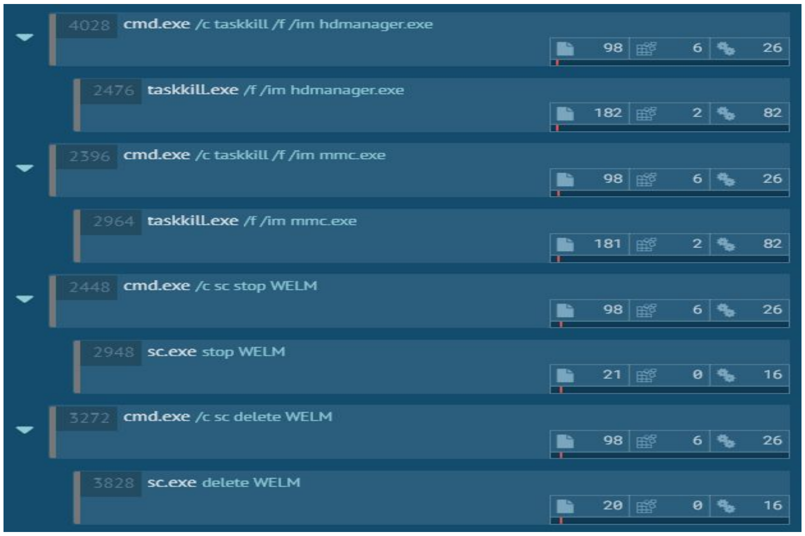
When the system knows the specific domain, it can use the HyperText Transfer Protocol (HTTP) which is a protocol that regulates how information is transferred on the World Wide Web. The protocol uses a command called GET which is fetching information from the HTML web server. The first GET request from Adylkuzz is going to ask for information from the subdirectory 08.super5566.com/install/start. The second is using the install subdirectory but is also using URL encoding which is a way of sending special characters in the address. The characters used include spaces and less than sign ( > ). Adding the characters to the /install subdirectory, the address says "install/106:0 -> 127:5 -> 128:5 -> 65:5."

| Request Type | Target Domain | Target IP Address | Reputation |
|---|---|---|---|
| DNS | 66.42.108.166 | 08.super5566.com | Malicious |
| HTTP GET | 66.42.108.166 | 08.super5566.com/install/start | Malicious |
| HTTP GET | 66.42.108.166 | http://08.super5566.com/install/106:0%20-%3e%20127:5%20-%3e%20128:5%20-%3e%2065:5 | Malicious |

Figure 3.3: Table describing DNS and HTTP protocols used by the cryptominer Adylkuzz.

The DNS request seen above in Figure 3.3 suggest that Adylkuzz is requesting the location of the attacker's command and control server. Once it is connected to the web server on port 80, it appears more software executables are going to be downloaded to mine the Monero coin because of the install and start subdirectories in the URL. Considering the potential nature of these addresses, they've been added to the reputation column as malicious.

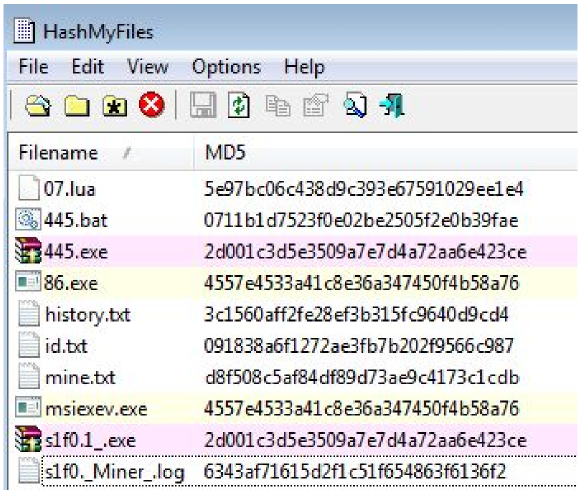
## 3.3 File System Modifications



```
4028 cmd.exe /c taskkill /f /im hdmanager.exe      98   6  26
  2476 taskkill.exe /f /im hdmanager.exe          182   2  82
2396 cmd.exe /c taskkill /f /im mmc.exe            98   6  26
  2964 taskkill.exe /f /im mmc.exe                181   2  82
2448 cmd.exe /c sc stop WELM                       98   6  26
  2948 sc.exe stop WELM                            21   0  16
3272 cmd.exe /c sc delete WELM                     98   6  26
  3828 sc.exe delete WELM                          20   0  16
```

Figure 3.4: Adylkuzz using the command line to kill processes and stop and delete logs for tracking it.

While Adylkuzz does not show blatant modification like Wannacry Ransomware in which all the files are encrypted there is still malicious modifications running in the background. Right off the bat, taskkill.exe is going to end the process of hdmanager.exe and mmc.exe as well as stopping and deleting WELM. This initial activity seems to suggest that Adylkuzz is hiding from the Windows system itself by turning off process and add-in managers, and then stopping the Windows logging system and removing it. We can also see from Figure 3.4 that when taskkill program is being run there are parameters being set to forcefully shut down the program (/f) as well as to create an image of this event (/im).



| Filename | MD5 |
|---|---|
| 07.lua | 5e97bc06c438d9c393e67591029ee1e4 |
| 445.bat | 0711b1d7523f0e02be2505f2e0b39fae |
| 445.exe | 2d001c3d5e3509a7e7d4a72aa6e423ce |
| 86.exe | 4557e4533a41c8e36a347450f4b58a76 |
| history.txt | 3c1560aff2fe28ef3b315fc9640d9cd4 |
| id.txt | 091838a6f1272ae3fb7b202f9566c987 |
| mine.txt | d8f508c5af84df89d73ae9c4173c1cdb |
| msiexev.exe | 4557e4533a41c8e36a347450f4b58a76 |
| s1f0.1_.exe | 2d001c3d5e3509a7e7d4a72aa6e423ce |
| s1f0._Miner_.log | 6343af71615d2f1c51f654863f6136f2 |

Figure 3.5: Using HashMyFiles application we can see all added files from Adylkuzz and their hashes.

In Section 3.2, it was discussed that Adylkuzz will request files from the command and control server. We placed these files into the HashMyFiles program seen in Figure 3.5 above that will show a list of the programs and their MD5 hashes that can be added to the antivirus program. Even though we would like to know exactly what each file does, there isn't much information about the files specifically. However, we might be able to speculate their significance. The easiest one to pick out is the log created that will show the Monero mining process. Two programs are created with the name of 445, maybe this has to do with the server message block and possibly transferring files. There is an 86 executable, possibly referring to our processor type and running an instance of Adylkuzz based on it. The msiexev.exe is Microsoft process manager that might run the initial processes of the malware which would make sense why the task is killed later on trying to avoid detecting integral processes.

# 04 Summary

The malware installed on the infected PC uses the PC's resources to mine cryptocurrency.  The most prominent sign was the connection to a remote CnC Server (8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233.bin.exe, PID: 3492) The HTTP and DNS request are listed in Figure 3.3. Another sign was that the malware adds new firewall rules which are malicious to Peak Medical's systems.

# 05 Containment Strategy

## 5.1 Scope

Adylkuzz is considered one of the most severe and dangerous attacks employed by hackers. The attack is launched from several virtual private servers which constantly scan not only computers but also servers. The Adylkuzz malware threatens and minimizes the integrity of an organization's every day operation and poses long lasting liabilities within a network if not resolved immediately.

- Infects PC's in the Server message block (SMB v1) which is launched from several virtual private servers;
- Affected operating systems/services and versions: Any computer running windows XP/10 or less ; it attacks more specifically Windows operating systems. Servers / Computers running Microsoft OS are specifically vulnerable.

## 5.2 Severity

Adylkuzz occupies a computer in order to mine for cryptocurrency; specifically bitcoin; however, some infected users have suggested that the adware has been known to also mine for “Monero.’ The malware is installed without the user’s knowledge. Moreover, this type of malware does not ask for any type of money and does not lock any CPU’s internal data; however a potential computer will run slower and slower every day in order to mine for cryptocurrency (BItcoin / Monero). In addition, users will only notice their Windows machine running slowly and that they don’t have access to shared Windows Resources. Based on existing research it is unclear which windows machine will be targeted or when.

The following Figure 5.1 illustrates the impact on an idling host when the miner uses four threads to consume spare computing capacity. Over time, this performance load forces the host to work harder, which also generates higher energy costs.

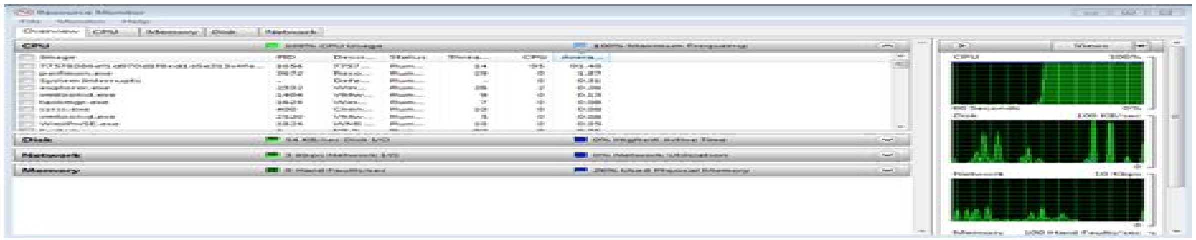


Figure 5.1: Showing Adylkuzz using 100% CPU usage.

## 5.3 Solution

The following strategies should be implemented in order to prevent any potential ‘Adylkuzz’ attack or should be used as general guidelines to respond to any potential threat to the Peak Medical company.

- Get patched against smb vulnerability
- Disable smb v1 (Microsoft Server Message Block on TCP 445
- Keep up to date in your windows patching
- Keep up to date with your antivirus
- Make sure all of your antivirus signatures are up to date
- Majority of antivirus vendors already have protection against this malware; using a firewall, especially a reputable one like Blue Coating will ensure traffic is being monitored, investigated, and appropriately blocked

Although cryptocurrency mining is legal, using a corporate system violates an organization's acceptable use and results in law enforcement action. The authorities should be involved for the unlawful use of processing power and consumption of Peak Medical's resources; our clients have noted surges in computing resources and effects on business-critical servers. This impact is amplified in large-scale infections.

# 06 Awareness Training

This section explains how end-users at Peak Medical can:

- Identify an infection by Adylkuzz
- Protect your data and isolate the infected machine
- Determine which organizational stakeholders to notify in the event of a compromise
- Protect computer and operating system from any damage due to virus.

## 6.1 Identification

Company computer users should be alert with the functions and performance of the operating systems being used. Employees should be alert and be aware if they begin to experience any of these following symptoms:

- Sudden and increasing speeds of computer fans. This could be done by simply monitoring the noise level surrounding the operating system, which usually emits a detectable noise if it begins to overheat.
- All programs and windows become noticeably slower. Experiencing lag in some programs can be a constant occurrence, in order to identify when a problem might be present, users should look for these cues: 1) Programs suddenly experiencing lag in unison with the system's fan working. 2) Programs that consistently ran smoothly, suddenly show signs of lag or extreme slowness. 3) That lag or slowness spreads from one function of the operating system to others, such as programs not responding and pointers moving at an extremely slow rate.
- Computer begins to overheat constantly and consistently. This method of identification involves monitoring users operating system for random influxes of temperature.
- Msiexev.exe and wuauser.exe are identified in the Task Manager. If any employee happens to catch these files installing or being installed on their system, they should immediately follow the quarantine procedures  stated in this report. If caught early enough, the amount of damage may be limited to a single system or possibly prevent any damage from happening. This all depends on active awareness of their operating system and safe operating habits.

The only way to prevent an infection such as this would be to provide adequate training to all employees. Each employee should have a basic familiarity with the working components of both the Software and Hardware. With this knowledge on hand, they will be able to spot system irregularities such as overheating, unresponsiveness and maybe even be able to spot unknown files downloaded into their system. With that being said, the best defense would be developing safe habits involving their computer system, such as never downloading from unknown persons and verifying with others before downloading files.

## 6.2 Quarantine and Response

If an employee suspects something abnormal with their systems or identifies any or all of the symptoms stated above, they should immediately close all programs and shut down their computer and proceed to contact with their I.T. Department. So as they may begin to:

- Identify if any virus is affecting current system.
- If so, isolate and exterminate the virus.
- For example, if your malware made a GET request to the server 64.42.108.166, you should tell your users to disconnect from the network, and recommend setting a firewall rule that blocks all traffic to/from that IP.

## 6.3 Escalation

If any of these conditions are met for Identification, employees should immediately follow these procedure:

- Disconnect from all networks and proceed to shut their machines down if possible
- Notify both the Security team and I.T. Department immediately, so they can become aware of a possible intrusion and infection.
- The nature of this program allows it to run unidentified for some time, so it must be stressed to take note of the current conditions of the system.

As stated before, the best defense against this type of trojan and all trojans in general is prevention. Proper education in safe operating habits is paramount for the financial success of the company, all it takes is one system to penetrate the whole network. Managers should remind employees to practice safe habits when using their operating systems repeatedly.

# References

1. https://app.any.run/tasks/79528004-1cb3-4b6e-9c3d-24acd7ea6812
2. https://any.run/report/8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233/79528004-1cb3-4b6e-9c3d-24acd7ea6812
3. https://www.hybrid-analysis.com/sample/8200755cbedd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddbf233?environmentId=100
4. https://www.null0x4d5a.com/2017/05/behavioral-analysis-of-adylkuzz.html
5. https://lazarusalliance.com/crypto-mining-malware/
6. https://exchange.xforce.ibmcloud.com/collection/Adylkuzz-Currency-Miner-e9910d60bf99c5f37f0dbdbcfd4fbb6e
7. https://www.symantec.com/connect/blogs/adylkuzz-crytocurrency-miner-not-next-wanna
8. cry
9. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
10. https://blog.avast.com/meet-adylkuzz-cryptocurrency-mining-malware-spreading-using-the-same-exploit-as-wannacry
11. https://threatpost.com/wannacry-shares-code-with-lazarus-apt-samples/125718/
12. https://lazarusalliance.com/crypto-mining-malware/
13. https://www.youtube.com/watch?v=bxGxfLm0V00
14. https://www.youtube.com/watch?v=zKizx80w4Rk
15. https://www.youtube.com/watch?v=KeZ8MbJupjA
16. https://www.youtube.com/watch?v=-T0SjvIo910
17. https://www.joesandbox.com/analysis/96371/0/pdf
18. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/taskkill
19. https://www.google.com/search?q=what+is+portable+executable+file%3F&rlz=1C5CHFA_enUS805US808&oq=what+is+portable+executable+file%3F&aqs=chrome..69i57j0l2.13266j1j7&sourceid=chrome&ie=UTF-8