Malware Analysis CA1

Yogesh Anandhakumar
MSc Cyber Seurity
Dublin, Ireland

***Abstract*—This paper mainly discusses a completely isolated lab setup for a Malware analysis & analysis of the malware "DarkHotel". This will also give a detailed idea of how to create an isolated lab setup, tools & techniques for malware analysis. We will also be discussing the "Dark Hotel" malware's behavior and its damages. We will also discuss various types of Sandboxes, which can be used for malware analysis.**

Keywords—Malware, Analysis, Sandbox, DarkHotel, Lab Setup.

I. INTRODUCTION

Cybercriminals get sensitive data by employing sophisticated malware techniques. Malware can affect an individual, a group of individuals, or an organization's money and intellectual property. Malware can also stealthily and readily propagate from one computer to another.

Malware analysis is the process of reverse engineering a particular piece of malware to ascertain its source, functionality, and possible impact. Malware analysis is a crucial step in any penetration testing procedure since it allows us to obtain comprehensive information about the virus[1] . Following are the steps to prepare the testbed:

Step 1: Allocate a physical system for the analysis lab.
Step 2: Install a virtual machine (VMware, Hyper-V, etc.) on the system.
Step 3: Install guest OS on the virtual machine(s)
Step 4: Isolate the system from the network by ensuring that the NIC card is in the "host only" mode.
Step 5: Simulate Internet services using tools such as INetSim (https://www.inetsim.org)
Step 6: Disable "shared folders" and "guest isolation".
Step 7: Install malware analysis tools.
Step 8: Generate the hash value of each OS and tool.
Step 9: Copy the malware to the guest OS [2].

II. MALWARE LAB

A. Critical Analysis of Existing Sandboxes

Sandbox is a controlled and segregated environment, where a software can be installed and viewed without endangering the host system, especially potentially harmful code or untrusted programs. It functions as a virtual container that makes it possible for analysts, researchers, and security experts to safely examine the behaviour of files, programs, or code. Here we are using sandboxes mainly for analysis of "DarkHotel" malware. Below are the few sandboxes that are widely used by researchers.

TABLE I. SANDBOXES

Sandbox	*License*	*Mode of usage*	*Accepted File formats*
CrowdStrike Falcon	Licensed	Cloud-based/On-premises	The Falcon Sandbox supports PE files (.exe, .scr, .pif, .dll, .com, .cpl, etc.), Office (.doc, .docx, .ppt, .pps, .pptx, .ppsx, .xls, .xlsx, .rtf, .pub), PDF, APK, executable JAR, Windows Script Component (.sct), Windows Shortcut (.lnk), Windows Help (.chm), HTML Application (.hta), Windows Script File (*.wsf), Javascript (.js), Visual Basic (*.vbs, *.vbe), Shockwave Flash (.swf), Perl (.pl), Powershell (.ps1, .psd1, .psm1), Scalable Vector Graphics (.svg), Python (.py) and Perl (.pl) scripts, Linux ELF executables, MIME RFC 822 (*.eml) and Outlook *.msg files.
Any Run	Free/Licensed	Online	A wide range of file types including PDF, LNK, ZIP, RAR, Office documents, and others
Cuckoo	Free	On-premise	Analyze many different malicious files (executables, office documents, pdf files, emails, etc) as well as malicious websites under Windows, Linux, macOS, and Android virtualized environments.
Hybrid Analysis	Free	Online	Archives in one of the following formats with/without a password: ace, arj, 7z, bzip2, gzip2, iso, rar, rev, tar, wim, xz and zip.
Joe	Free/ Licensed	Cloud-based/On-premises	PE, PDF, ELF and Microsoft Office (.doc, .ppt, .xls, .docx, .pptx, .xlsx) files

B. VM Setup

Here I have installed VirtualBox as hypervisor, two VM's namely Kali Linux & Windows 11 on the hypervisor. Below is the detailed view of my VM setup:

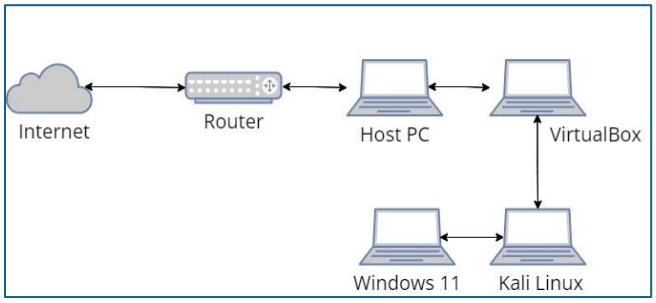

Fig. 1. Lab Setup

Network Configuration:

TABLE II. NETWORK CONFIGURATION

VM	*Adapter 1*	*Adapter 2*
Kali Linux	Bridged	Internal Network
Windows 11	Internal Network	-

Kali Linux VM:

Fig. 2. Kali VM Setup

Windows 11 VM:

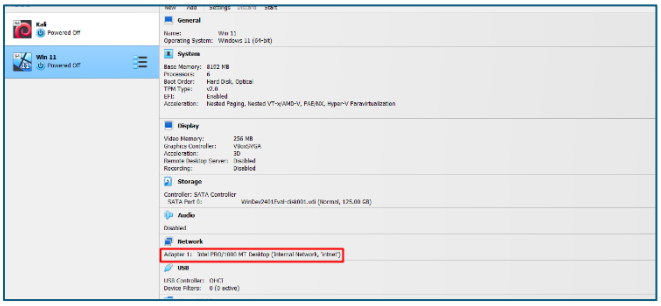

Fig. 3. Win 11 VM Setup

Here Windows 11 VM is the affected machine, which is isolated from the network by using Internal Network. Kali Linux VM is used for analyzing the malware in affected machine which is Win 11 VM. Kali Linux has been configured with two adapters, Bridged & Internal Network, where Bridged network will help the VM to connect to the internet & internal network is used to contact with the affected Win 11 VM.

C. *Software Tools*

The software tools installed for analyzing the malwares are listed below,

- Wireshark - It is a free and open-source packet analyzer software tool, which records and examines data packets as they pass through a network of computers. This is one of the most widely used packet analyzer globally and it serves a multitude of functions for network administrators, security experts, developers, and instructors, such as debugging network issues, assessing network security, packet capturing, etc.
- HashMyFiles – this tool produces the hash value of the file using various algorithms.
- Virus Total – this tool analyzes suspicious files or URLs.
- BinText - this tool can extract text from any kind of files & has the ability to find ASCII text, Unicode & Resource strings.
- PEid – this tool provides information about the windows executable files, which can also identify signatures associated with different packers & compilers.
- PE explorer - this tool allows to open, view & edit 32bit windows executable file types, such as exe, dll, etc.
- Dependency Walker – This tool will list all the dependent modules of exe files, gives us a hierarchical tree diagram and records all functions of each module exports & calls.
- Ghidra – this tool is an open-source reverse engineering tool.
- Process Monitor – this tool shows the real-time file system, registry & processes, or threads activity.

D. *Lab Testing*

The lab has been tested to confirm the isolation from the host machine by pinging the machines each other. Kali VM can contact Windows 11 VM via Internal Network adapter for analyzing the malware in it. Kali VM can also connect to the internet via Bridged adapter for analyzing the malware samples and files in the online sandboxes. Below are the screenshots,

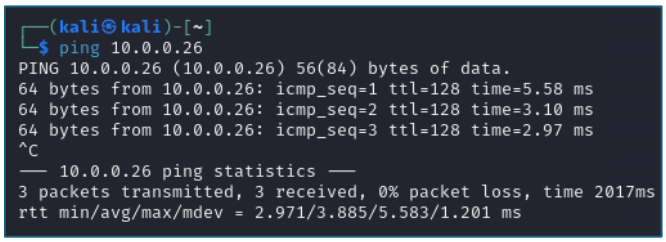

Fig. 4. Kali Linux VM to Windows 11 VM

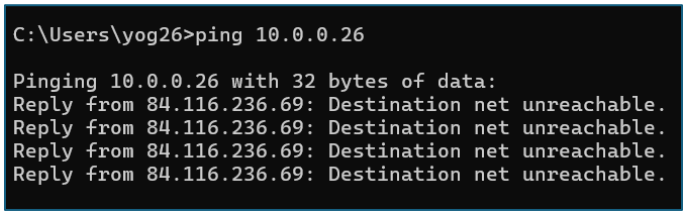

Fig. 5. Host Machine to Windows 11 VM

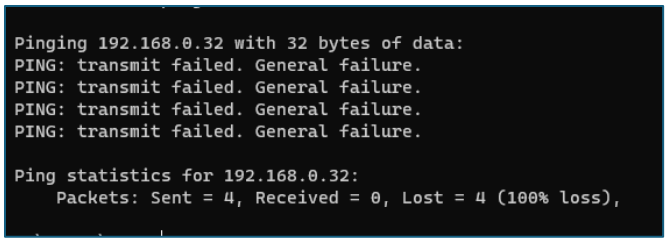

Fig. 6. Windows 11 VM to Host Machine

III. RESEARCH-BASED MALWARE ANALYSIS

A. Identification

The "DarkHotel" malware is a focused spear-phishing campaign that used malware and spyware to obtain private information from well-known people, especially business executives and other influential people. Because of its sophistication and persistence, Kaspersky Lab categorized it as an Advanced Persistent Threat (APT) [3], [4], [5], [6], [7].

Its Technical name was Trojan: Win32 / Tapaoux, Troj / Tapaoux - AD, Trojan. Tapaoux. Its point of origin was South Korea.

Primary targets are corporate tourists staying in opulent hotels, particularly in Asia and the US. The ransomware used a combination of spear-phishing emails and malware distribution via infected hotel Wi-Fi networks as its attack strategy.

The main techniques of this malware are,

- Phishing emails: These emails use social engineering techniques to fool recipients into opening attachments with malware or clicking on bogus links.
- Compromised Wi-Fi: Gaining access to hotel Wi-Fi networks to intercept and modify user traffic, possibly sending users to malicious websites or infecting them with malware.
- Malware: Installing backdoor Trojans that may take financial information, emails, and login passwords from compromised devices.

Senior corporate leaders are the target of assaults, which use fake digital certificates—created by factoring the weak public keys of genuine certificates—to trick victims into believing that software downloads that are requested are legitimate. Attackers target individual people who are visitors to luxury hotels, mostly in Asia and the US, by uploading malicious code to hotel servers. According to [8], the gang known by the names DarkHotel or Tapaoux has also been actively infecting users since 2007 through peer-to-peer networks and spear-phishing, then leveraging those attacks to load reverse engineering and key logger tools onto compromised endpoints. Numerous victims have been identified in Japan, China, Korea, and Russia. Attackers swiftly steal confidential data, including passwords and intellectual property, from victims' computers once they get access to them. They then destroy their equipment in the hopes of avoiding detection, preventing high-level victims from changing all of their account passwords. Bitdefender released further findings regarding Inexsmar, a variant of the DarkHotel virus that was intended to target political individuals rather than companies, in July 2017 [6] .

B. Analysis

Malware analysis is the process of reverse engineering a particular piece of malware to ascertain its source, functionality, and possible impact. The process of analysing a malware is Static analysis & Dynamic analysis [2].

Static analysis of the malware refers to processes like File fingerprinting, offline & online malware scanning, performing string search, identifying packing/obfuscation methods, finding the portable execution (PE) information [2].

Dynamic analysis steps include System baselining & Host Integrity Monitoring. System baselining is the process of capturing a snapshot of the system, which includes the information about the file system, registry, open ports, network activities, etc., at the beginning of malware investigation. Host Integrity monitoring refers to collecting a system snapshot both before and after analysis to see how the system has changed. It contains registry monitoring, network traffic analysis, log analysis, port monitoring, process monitoring, installation monitoring, etc [2].

DarkHotel employs a range of strategies, such as phishing attacks, zero-day vulnerabilities, and the deployment of malicious software like Trojan horses and keyloggers, to undermine the security of its targets. The gang has a history of fooling victims into disclosing personal information, including financial information and login credentials, by using malicious Wi-Fi networks and fake login pages. DarkHotel is known to steal confidential documents and other data from victims' devices once they have access to it. They may also install other software to maintain the hacked device infected. The gang has also been known to track a victim's activities and take additional login credentials by using their access to the victim's device.

1) Basic Properties:

- Hash: 89ec1f32e1bbf794c41fa5f5bc6869c0
- MD5: 89ec1f32e1bbf794c41fa5f5bc6869c0
- SHA-1: 9a1d038f3002484613bed1364cd8e55398a7b3aa
- SHA-256: 8d956e79689f2e34d66052f4a795440afd69e396f3f3f47802fcacea3e37d99d
- Vhash: 8ea071dcc39f9fae944f06d9121bc0df
- SSDEEP: 24576:9/ZsXn8TBAfZRyu/uFrlqg748EoUMogg1Xq7LovkBl/dOONHBr9cerbODho6M3Yx:9/eXnJfZRh/uFrlR74vrMogOXq7Lov+U
- TLSH: T118450253A5408C95FEFA4630F0FAA728C3F9364679EC686E0DCE290510B6689BD3954F
- File type: Office Open XML Document, document, MS office, text, word, docx,
- Magic: Microsoft Word 2007+
- TrID: Soft Maker Text Maker text Document (64.7%) Word Microsoft Office Open XML Format document (18%) Open Packaging Conventions container (13.4%) ZIP compressed archive (3%) Print Fox/Page fox bitmap (640x800) (0.7%)
- File size: 1.11 MB (1167495 bytes)[9]

Then I have analyzed the hash in Virus Total, the result is shown below,

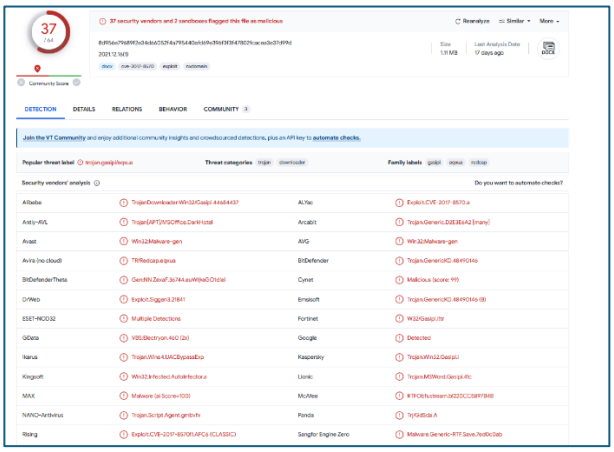

Fig. 7. Virus Total Scan result[9]

The first step of this attack is a multi-layered malicious document that defines an AltChunk element to load an embedded DOCX file. An additional malicious RTF file is loaded by an AltChunk element defined by the embedded DOCX file. Stage 2 involved a scriptlet file, whose first task was to deliver a list of active processes, encoded in Base64, to the configured C2 server. Then stage 3 was dropping the binaries. Then stage 4 was executing PowerShell scripts. Then stage 5, the .net dll turns as the downloader. The C2 server IP address was 23.111.184.119 [5].

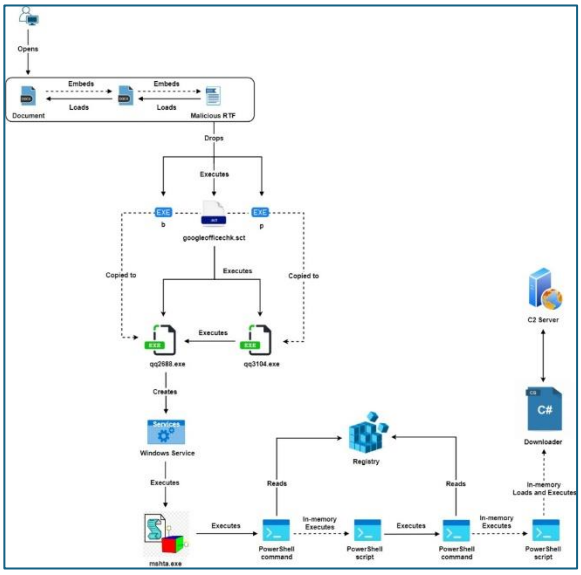

Fig. 8. Attack chain [5]

They discovered a pattern in the domain names and used passive DNS data to identify multiple domains hosted on the server with a fore mentioned IP address. Many domains were registered under false pretences of being political think tanks, government agencies, or educational institutions in China [4].

A table summarizing a few examples is provided below.

TABLE III. SPOOFED DOMAINS[5]

Domain name	***Target spoofed***
www.onlinesurvey.register.moe.edu.cn[.]servicenteasse.com	Ministry of Education, China
www.preview.maiil.caict.ac.cn.coremailxt[.]servicenteasse.com	Political think tanks of China
www.prevwdoc.mofcom.gov.cn.loginwebbauthh[.]servicenteasse.com	Beihang University in China
www.compliance.maill.buaa.edu.cn.coremailxt[.]servicenteasse.com	Ministry of commerce, China
www.compliance.maill.hit.edu.cn[.]coremailxt.servicenteasse.com	Harbin Institute of Technology
secureattch.nudt.edu.cn[.]coremailxt.servicenteasse.com	National University of Defence and Technology

Below are the messages left by the malware in the infected systems,

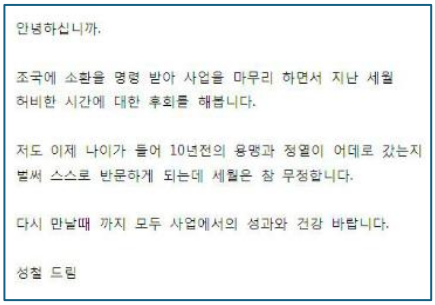

Fig. 9. Attackers Message [4], [5], [7], [10]

Fig. 10. Attackers Message [4], [5], [7], [10]

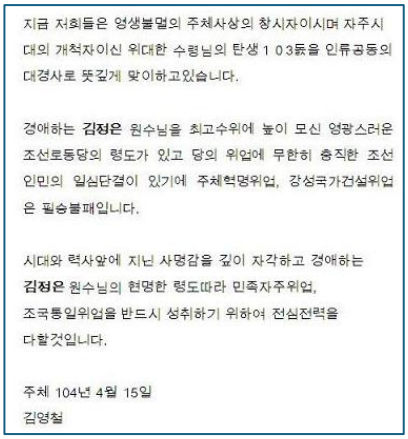

Fig. 11. Attackers Message[4], [5], [7], [10]

C. Conclusions

1) Summary of Findings:

The DarkHotel campaign is an alarming indication of the clever and enduring risks present in the digital world. Even though its peak activity seems to have passed, cybersecurity procedures must remain strong due to the strategies used and the possibility of new attacks of a similar nature. Travelers on business, especially those lodging in upscale hotels, are still susceptible to spear-phishing scams and malware spread via infected Wi-Fi networks. To accomplish its objectives, DarkHotel used a mix of malware installation, network manipulation, and social engineering. Risks can be reduced by putting robust cybersecurity measures into place, such as being aware of emerging threats and being cautious when utilizing public Wi-Fi. Organizations and people need to be on the lookout for changes in the threat landscape and adjust their security strategy accordingly. People and organizations can take precautions against future attacks by being aware of the strategies and objectives of threats such as DarkHotel.

2) Recommendations

The best way to safeguard your device from malwares like DarkHotel APT's is to use the hotspot on your mobile device to access the Internet rather than connecting to any public or untrusted networks, including hotel Wi-Fi networks, to be careful in visiting a webpage, to be careful in downloading or installing a file from untrusted sources.

If a system got infected by a malware, immediately isolate the machine from the network, take an image of the machine, start analysing using the image and the infected machine. So, we can have a clear idea of the malware's structure, behaviour, tricks, etc. Those will help us to find a way to defend those kinds of attacks in future Most important things need to be done in a network are, to strengthen the firewall by implementing strong rules, implementing proper access control mechanisms, using IDS, IPS, Antiviruses, wherever critical systems are present.

3) Next Steps

If I would download the DarkHotel malware, initially I would do the static analysis of the malware, like File Fingerprinting, local & online malware scanning, performing string search, identifying packing/obfuscation methods, finding the portable execution (PE) information. After completing static analysis & gathering results, I will move forward with dynamic analysis. Dynamic analysis steps include System baselining & Host Integrity Monitoring [2].

IV. References

[1] Palo Alto Networks, "Malware | What is Malware & How to Stay Protected from Malware Attacks - Palo Alto Networks," Palo Alto Networks. Accessed: Mar. 03, 2024. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-malware

[2] EC Council, "VitalSource Bookshelf: Certified Ethical Hacker (CEH) Version 12," EC Council. Accessed: Mar. 04, 2024. [Online]. Available: https://bookshelf.vitalsource.com/reader/books/9798885931144/pageid/1103

[3] "Global Research and Analysis Team A STORY OF UNUSUAL HOSPITALITY 2," 2014.

[4] K. L. Global Research & Analysis Team, "The Darkhotel APT | Securelist," Securelist. Accessed: Mar. 03, 2024. [Online]. Available: https://securelist.com/the-darkhotel-apt/66779/

[5] Zscaler, "New DarkHotel APT attack chain identified | Zscaler," Zscaler. Accessed: Mar. 03, 2024. [Online]. Available: https://www.zscaler.com/blogs/security-research/new-darkhotel-apt-attack-chain-identified

[6] Wikipedia, "DarkHotel - Wikipedia," Wikipedia. Accessed: Mar. 03, 2024. [Online]. Available: https://en.wikipedia.org/wiki/DarkHotel

[7] ZETTER KIM, "DarkHotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests | WIRED," WIRED. Accessed: Mar. 03, 2024. [Online]. Available: https://www.wired.com/2014/11/darkhotel-malware/

[8] Zetter Kim, "Dark Hotel | PDF | Malware | I Cloud," Scribd. Accessed: Mar. 03, 2024. [Online]. Available: https://www.scribd.com/document/265727486/Dark-Hotel

[9] Virus Total, "VirusTotal - File - 8d956e79689f2e34d66052f4a795440afd69e396f3f3f47802fcacea3e37d99d," Virus Total. Accessed: Mar. 03, 2024. [Online]. Available: https://www.virustotal.com/gui/file/8d956e79689f2e34d66052f4a795440afd69e396f3f3f47802fcacea3e37d99d/details

[10] F. Skopik and T. Pahi, "Under false flag: using technical artifacts for cyber attack attribution," *Cybersecurity*, vol. 3, no. 1, pp. 1–20, Dec. 2020, doi: 10.1186/S42400-020-00048-4/FIGURES/6.