CYBER FORENSIC FINAL CHALLENGE

Group-1 Presentation

Presenting by:
AKSHITH RAO- 00952448
AMANI PONNAM- 00863409
OLUWATOYOSI KEHINDE- 00836634
VINUSHA GOUD POTTOLLA-00941796
YADLAPALLI LAKSHMIDHAR- 00964282

INTRODUCTION

Digital forensic data loss inquiry of the HiTeK Company's exfiltration of private data.

The image files and network capture file were among the evidence that the responding agency had obtained.

The investigator applies the forensic methodology and document how the exfiltration happened.

SCENARIO

HiTek Company security engineers were managing a program to avoid data loss. The engineers have doubts about the possibility of important firm data being exfiltrated. As a result, two forensic images of two connected PCs and the network activity between them were made. The investigative team received these files and was entrusted with reviewing them in-order to determine whether or not data exfiltration had taken place within the HiTeK corporation.

Forensic Tools Used

1. Autopsy
2. Wireshark
3. John the Ripper
4. Kali Linux &Oracle Virtual Box
5. FTK Imager
6. fcrack zip

Identified Machines and IP Addresses

3 machines and multiple IP’s identified

1

Windows Machine
(Computer1.E01)
Hostname: DESKTOP-A8BOTBH
IPv4: 192.168.0.6

2

Ubuntu Virtual Machine Found within Windows Machine

3

Linux Server
(Computer2.E01)
Hostname: web-srv-02
IPv4: 192.168.0.8

Network Analysis

Wireshark and NetworkMiner were used for the analysis

- FTP connection between Windows machine & Linux server discovered
- Credentials for FTP server found in plaintext:

  User: webmaster

  Password: password

Linux server sent 2 zip files to Windows machine via FTP

- BusinessStrategy.zip
- Secrets.zip

Directories to files were then deleted on Linux server

Passwords/Credentials

7 passwords cracked

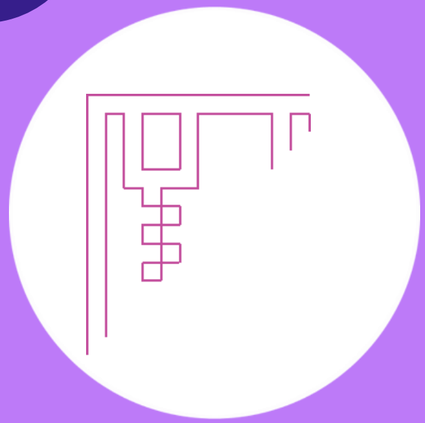
- 3 belong to Windows machine
- 2 to Ubuntu machine
- 2 to zip files

3 passwords found scattered within documents and files

- These passwords correspond with a site
- named www.crazywickedawesome.com
- Windows passwords stored in \Windows\System32\config\Sam
- Used Ophcrack to grab NTLM hashes & cracked them
- Ubuntu machine passwords stored in /etc/shadow as SHA256 hashes
- Used John the Ripper to crack passwords

  BusinessStrategy.zip = crazylongpassword

  Secrets.zip = VeryLongP@ssw0rd



Tables of Credentials

User Account	Password
tester	monkey
Carlson	12345
Johnathan	letmein
webmaster	password
cknight	popcorn

Login Details for www.crazywickedawesome.com

Usernames (www.crazywickedawesome.com)	Passwords	File Name	File Path
evilhenchman	MyP@ssw0rd!@#	Next-Character.docx	/Users/tester/Documents/Next-Character.docx
henchmen	P@ssw0rd!@#	grays.jpg	/Users/tester/Documents/grays.jpg
Laslow	FritoLay	MMC.exe	/Windows/MMC.exe

ComputerI.EOI

- Personally, examined the file to look into what transpired on the computer.
- Examining the browser history manually, the investigator discovered "Star Wars, CNN, emails of user esmith.hitek@gmail.com," which the machine had viewed.
- Determined the system's hostname.

  Found two email addresses and five distinct accounts.
- It was discovered that the SAM folder, which holds passwords and usernames, is encrypted.
- Discovered NTML hashes, which were then cracked to provide the usernames and passwords.

  Using Crackstation, I was able to crack the passwords.

User Accounts on Computer1.E01

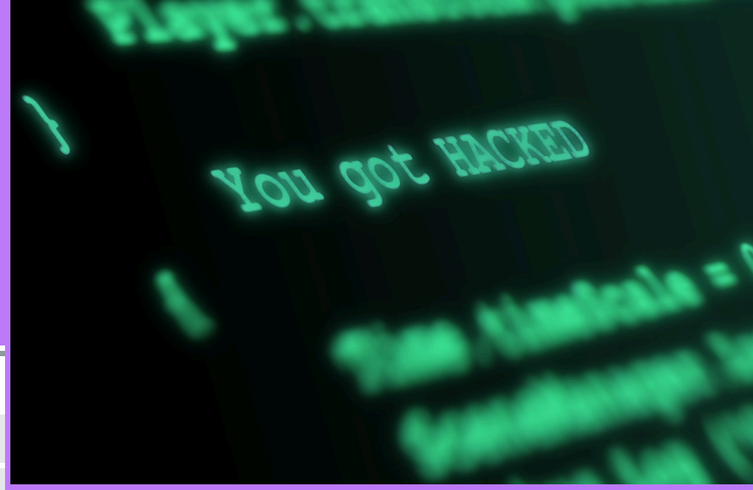
	Username	Password	Directory/Path to user accounts
	tester	monkey	/img_Computer1.E01/vol_vol3/Windows/System32/Config/SAM
	Carlson	123456	/img_Computer1.E01/vol_vol3/Windows/Users/Carson
	Jonathan	letmein	/img_Computer1.E01/vol_vol3/Windows/System32/Config/SAM
	Administrator	(No password found or disabled)	/img_Computer1.E01/vol_vol3/Windows/System32/Config/SAM
	Guest	(No password found or disabled)	/img_Computer1.E01/vol_vol3/Windows/System32/Config/SAM
	Default User	(No password found or disabled)	/img_Computer1.E01/vol_vol3/Users/Default
	Public	(No password found or disabled)	/img_Computer1.E01/vol_vol3/Users/Public

Stolen Credentials for www.crazywickedawesome.com

File Name	MD5 Hash	SHA256 Hash	File Path
grays.jpg	bf298fd9197b2fa17b227ddc71d61765	1a5c371340b9dda7880cc29284dca216df47d514351567c9e53a9498d9a5a276	Users/tester/Pictures/grays.jpg
	40a5f4a9ecc8bfe0d1ba13d8fb078cbe	637471bc8c21b39e3037e564c2e495fe0b88354acff6d78a6a0bf9dd22001847	Users/tester/Desktop/Installation Files/grays.png
MMC.exe	54e04095b1dea240a8c0778b4f34cab1	2b730c42d947f649682763886f47dd0a5c0d6bf6c4dc9d58810576714db10e2d	

List of Suspicious Files

File Name	Description	Data Sources	File Path
MMC.exe	An executable file that contains login details	Computer1.E01	img_Computer1.E01/vol_vol3/Windows/MMC.exe
BusinessStrategy.zip	An encrypted zip file	Computer2.E01	/img_Computer2.E01/vol_vol2/var/www/BusinessStrategy.zip
Secrets.zip	An encrypted zip file	Computer2.E01	/img_Computer2.E01/vol_vol2/var/www/Secrets.zip
veraCryptSetup.exe	An encrypted file software	Computer1.E01	Users/Carson/Desktop /VeraCryptSetup1.16.exe
a.zip	Contains a.txt files	Computer1.E01	vol_vol3/a.zip/a.txt
VMware-player-12.0.1-3160714.exe	VMware was installed in the system	Computer1.E01	Users/tester/Downloads /VMware-player-12.0.1-3160714.exe
DNSRecords.ods	A file that contains the IP address	Computer1.E01	Users/tester/Documents/DNSRecords.ods
ChromeSetup.exe	Chrome was installed in the system	Computer1.E01	Users/tester/Downloads/ChromeSetup.exe
grays.jpg	An image that contains login details	Computer1.E01	Users/tester/Desktop/grays.jpg
Projects.odt	Tells about accessories installation	Computer1.E01	Users/Carson/Documents/Projects.odt
shadow.bak	Linux log files that contained encrypted passwords	Computer2.E01	/img_Computer2.E01/vol_vol2/var/backups/shadow.bak
vmware.vmsg	An application that supports to change multiple languages	Computer1.E01	vol_vol3/Program Files(x86)/VMware/VMware Player/messages/ja/vmware.vmsg
access.log	Apache web log file	Computer2.E01	/img_Computer2.E01/vol_vol2/var/backups/access.log
X3fw-pxe.ncf	An encrypted file	Computer2.E01	/img_Computer2.E01/vol_vol2/lib/firmware/vxge/X3fw-pxe.ncf
X3fw.ncf	An encrypted file	Computer2.E01	/img_Computer2.E01/vol_vol2/lib/firmware/vxge/X3fw.ncf
vsftpd.log	FTP server log file	Computer2.E01	/img_Computer2.E01/vol_vol2/var/log/vs-ftpd.log



Computer2.E01

S.No	Username	Password	Directory/Path to user accounts
1	cknight	popcorn	/img_Computer2.E01/vol_vol2/home/cknight
2	webmaster	password	/img_Computer2.E01/vol_vol2/home/webmaster
3	jhathoway	(No password found or disabled)	/img_Computer2.E01/vol_vol2/home/jhathoway

Exfiltrated Files from HiTeK Company

IP Address	Hostname	MAC Address	Device Name
192.168.100.3	INTEL-CE-LINUX	d4:05:98:0f:ca:00	Arris Group Router
192.168.1.200	MICHAELS-AIRPORT	6c:70:9f:d4:b1:78	Apple
192.168.0.6	DESKTOP-A8BOTBH (Computer 1)	ec:f4:bb:8a:b4:fd	Dell
192.168.0.3	Katies-iPhone-2.local	18:f6:43:7f:32:00	Apple
192.168.0.9	XRY-PC	0c:84:dc:8e:01:c3	Hon Hai Precision
192.168.0.2	HP92C494.local	ec:9a:74:9c:c3:7c	HP
192.168.0.7	Ubuntu.local	00:0c:29:42:28:b8	VMWare
192.168.0.200	OXYGEN-PC	74:86:7a:2c:cb:46	Dell
192.168.0.8	web-srv-02 (Computer 2)	74:86:7a:2c:78:06	Dell
192.168.0.4	unknown.local	78:31:c1:c1:72:3c	Apple
192.168.0.1	N/A	d4:05:98:0f:ca:07	Arris Group Router
192.168.0.5	N/A	a0:63:91:80:bc:b6	Netgear
192.168.0.10	XRY-PC	74:86:7a:2c:cb:ae	Dell

Hashes

File Name	MD5 Hash	SHA1 Hash
Computer1.E01	19ce67619688a8be7e98fb7c2e659817	8666553e0d5ad9e340f9d22490844451e973d10f
Computer1.E02	53ff8a7c786e36824118ccdf5d13cb01	4eb10332a7876e39d8153624d7d365b67ccf6630
Computer1.E03	0b38a0e41c5b65aa320f1d02647800e6	b7d9f4d5fab03e30c21a2bb845bb6052c38b480a
Computer1.E04	f5297dc535f91666a6dbc34aaca330b0	32d20dfd9218cc03dd6ac2a936aa1d8192613a91
Computer1.E05	73c2a071afec76079f7eb9fa64409332	fff112b45673b759d950ff0fa8e240adfbf5cd77
Computer1.E06	f729bf6a150e881222cb93178db12d0f	5d1b4c35a28edd43d48ae2c2a290f89a055632c8
Computer1.E07	82359df946afb8a48e3cf0d5f0b1dde6	7493f7b667f2f305452bb3fd874688c6923eda9e
Computer1.E08	1c6b0be65195109c77d18436e2846eeb	85e88b711c089fe8635a68e68438e32bf3790ac3
Computer2.E01	afbed0b48ea057343ab84d0d7a1d140a	b02bbdb5bb422743b6bc5ea61531427b7e9f67a3
network.pcapng	8754862e479eb1e93eaa72d79e12e84d	03acc1be064b52523755b67fe566f789c1f5ee2c
BusinessStrategy.zip	c05fc707175f4e09201ac80d9c774d1f	3c16de12b6ddc828c88a2dbc40ea701ce29e589d
Secrets.zip	1142df97fd45fa8ea57f02cc51b457e9	e548d41084ecd6a9e4aec2106a96c807fdb7a8d6
SAM	a51701d7e4f78902e6586d3799dbc178	afd67eb7e19decbbd79c2633b0b15fa230563f99
SYSTEM	b40c6acd32c1e9a41fc55ede67a4848b	bfe729681b373e232aac43b959668bc51c417989
SVCHOST.EXE-6A349820	1bda1eb8239ad2d508e47d968cb6a767	28c989dd84f1ee855282e6a6102128d94ade2373
Next-character.docx	983d234db7a9d3d4e51697c2796031d4	46da9bd2423763cf67b4d1facd77b8645a962e5c

CONCLUSION

Sensitive information was in fact exfiltrated from the network. It's possible that someone within the company had been misusing their authority or had figured out weak passwords, extracting private information to provide to HiTeK's rivals. By employing stronger passwords throughout the whole company and keeping an eye on who is authorized to access certain areas of the network, this might have been avoided.

THANK YOU!