STAR
Research Journal

Available online at www.starresearchjournal.com (Star International Journal)
ENGINEERING
UGC Journal No: 63023

CYBER FORENSICS CASE STUDY ON SHAMOON VIRUS ATTACK

Dr. SREEJA MOLE. S. S[1], Dr.SUJATHA[2], K. SHILPA[3] & SHERIN. J[4]

[1]*Professor/HOD, Dept of ECE, CJITS, Janagon, India.*
[2]*Professor, Dept. of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Kuniamuthur, Coimbatore, Tamilnadu, India.*
[3,4]*PG Scholars, Dept. of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Kuniamuthur, Coimbatore, Tamilnadu, India.*

Abstract

Saudi Aramco is one of the largest producer, manufacturer and refiner of crude oilCompany in the world. The gulf countries economy is mostly based on the production and selling of crude oil and its products. The aim of this attack is to disrupt the production and supply of oil. On 15th august 2012, the Aramco was attacked by the virus name is called Shamoon. It will deletes the data on computer hard disks without crash or damage any hardware. 30000 workstations (i.e.,) 85% of Aramco systems was affected by shamoon attack and the company loses the million dollars of business. Shamoon is share others systems via the local area network of company. Systems infected by it rendered useless as most of the files, the Master Boot Record (MBR) and the partition tables are overwritten with garbage data. The overwritten data is lost and is not recoverable. In this paper explains the cyber forensics analysis of shamoon virus attack.

Keywords: Shamoon, Aramco, MBR, cyber forensics, cyber-attacks.

I. INTRODUCTION

Saudi-Aramco is a State owned Saudi Arabian American Oil Company, headquartered in Dhahran. It is the world largest exporter of petroleum products. In 2006, the corporation foiled a physical attack by al-Qaeda only to be hacked in 2012, resulting in a substantial loss of data on 30,000 computers by some Arab group. The advancement in computer technology and the role of the internet are breeding types of criminals, who can remain anonymous and wreck severe economic damage to individuals, corporations and states. Profiling the hackers, identifying and knowing their motive constitute an important step in mitigating their threats. U.S. considered the attack on Aramco with all the seriousness it deserved, and warned suspected countries, the readiness to go after groups and state criminals. American Cyber security experts were provided to undertake the forensic analysis and provide the necessary security tools to mitigate future cyber threats. Saudi- Arabian American Oil Co (Aramco), is owned by United States' companies, was nationalized by Saudi Arabia in 1988. It is the one of the world largest oil and gas producing and exporting the 40% of global petroleum needs. This has made the security of Aramco a major concern to both the Saudis and the Americans. On August 15th 2012, the Aramco network system was attacked. The shamoon virus infested more than 30, 000 hard drives of Windows-personal computers, and wiping off all information and installing pictures of American flag in flames. On the scene were no tracks of the hacker except for the hard drives, which had been wiped clean of data and replaced with the pictures of American flags in flames.

II. CYBER FORENCIS ANALYSIS

1. IDENTIFICATION

The Shamoon malware is identified by the detection W32/DistTrack, is a Trojan. Dropper malware that has exhibited extremely destructive behaviour. Systems infected by it rendered useless as most of the files, the Master Boot Record (MBR) and the partition tables are overwritten with garbage data. The overwritten data is lost and is not recoverable. The initial infection vector is as of yet unknown, but the malware has the capability of spreading via Admin$ shares. In August 2012, two foreign oil companies, Saudi Arabia's Saudi Aramco and Qatar's RAS Gas, reported infections as a result of W32/DistTrack. Although both companies reported there were no disruptions to oil and gas operations, tens of thousands of workstations were corrupted throughout the business networks of both companies. Due to the highly destructive functionality of the Shamoon "Wiper" module, organizations infected with the malware could experience operational impacts including loss of intellectual property and disruption of critical systems.

2. COLLECTION

The primary concern to the Oil and Natural Gas sector should be considerations of what impacts this malware could have to business operations, if the infection occurs and spreads. Although anti-virus

vendors rate the threat containment and removal as easy1, organizations should concentrate on the factthat this malware has been specifically targeted at their sector with the intent of destruction. The purpose of the malware is to destroy data, interrupt operations and cause overall harm to businesses within the Oil and Natural Gas sector. Organizations should consider impacts to all services, not just control systems, including finance, human resources, R&D, etc. Data loss from any of these departments could have impacts beyond the replacement of workstations, including loss of productivity, intellectual property, and personally identifiable information. All losses can result in lost revenue and could potentially incur significant costs to the business to regain or recreate corrupted data. Network breaches and data losses can also impact corporate reputations, and potentially investor confidence, leading to impacts on stock prices and additional loss of revenue.

These attacks demonstrate the threats directed at oil and natural gas infrastructure and the need to maintain a high level of vigilance.Organizations deal with risk every day in meeting their business objectives. They may include financial risk, risk of failure of equipment, and personnel safety risk. These organizations have developed processes to evaluate risks associated with their business and to choose how to deal with those risks based on organizational priorities and both internal and external constraints.As Shamoon has demonstrated, organizations must also incorporate cyber security risk to the organization, including its business units, subsidiaries, related interconnected infrastructure and stakeholders, while recognizing the larger context of risk management. There are additional risks inherent in operating information technology and industrial control systems (ICS) or SCADA. A thorough understanding of the risks to network computing resources or from denial-of-service attacks, and the vulnerability of sensitive information to compromise is essential to an effective risk management program.

3. EXAMINATION

Three different hacker groups are have claimed responsibility for the shamoon virus attack on August 15th, 2012. 2000 servers and 30000 thousand computer systems was affected by the attack.

Arab Youth Group – one of the Iranian hacker group

Cutting Sword of Justice Group – Shamoon virus attack group

4. ANALYSIS

The analysis of Shamoon by Kaspersky Labs, it is similar type of wiper attack in Iran's oil ministry.Iran is one and only country to use wiper attacks and reverse-engineered attacks. The Saudi Arabian minister say some of Saudi Aramco employees are member of Hezbollah. Hezbollah members are hackers.

W32.Disttrack consists of several components:

- Dropper—the main component and source of the original infection. It drops a number of other modules.
- Wiper—this module is responsible for the destructive functionality of the threat.
- Reporter—this module is responsible for reporting infection information back to the attacker.

4.1 Dropper Component

The Dropper component performs the following actions:

- Copies itself to %System%\trksvr.exe
- Drops the following files embedded into resources:
- A 64-bit version of the dropper component: %System%\trksrv.exe (contained in the "X509" resource)
- Reporter component: %System%\netinit.exe (contained in the "PKCS7" resource)
- Wiper component: %System%\[NAME SELECTED FROM LIST].exe (contained in the "PKCS12" resource)

The name of the component is selected from the following list:

Caclsrv, certutl, clean, ctrl, dfrag, dnslookup, dvdquery, event, extract, findfile,clean, Fsutl, gpget, iissrv, ipsecure, msinit, ntx, ntdsutl, ntfrsutil, ntnw, power, rdsadmin, regsys, routemanRrasrv, sacses, sfmsc, sigver, smbinit, wcscript

- Copies itself to the following network shares:

  ADMIN$
  C$\\WINDOWS
  D$\\WINDOWS
  E$\\WINDOWS
- Creates a task to execute itself
- Creates the following service to start itself whenever Windows starts:
- **Service name:** TrkSvr
- **Display name:** Distributed Link Tracking Server
- **Image path:** %System%\trksvr.exe

4.2 Wiper Component

- The Wiper component includes the following functionality:
- Deletes an existing driver from the following location and overwrites it with another legitimate driver:
  %System%\drivers\drdisk.sys
- The device driver is a clean disk driver that enables user-mode applications to read and write to disk sectors. The driver is used to overwrite the computer's MBR but may be used for legitimate purposes.
- The file is digitally signed

- Executes the following commands that collect file names, which will be overwritten and writes them to *f1.inf* and *f2.inf*:

```
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i
download 2>nul >f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i
document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i download 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i picture 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i video 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i music 2>nul >>f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul  | findstr -i
desktop 2>nul >f2.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i desktop 2>nul >>f2.inf
dir C:\Windows\System32\Drivers /s /b /a:-D 2>nul >>f2.inf
dir C:\Windows\System32\Config /s /b /a:-D 2>nul | findstr -v -i
systemprofile 2>nul >>f2.inf
```

Figure I
Command used to select the file names

Files from the *f1.inf* and *f2.inf* will be overwritten with the JPEG image shown below. Overwritten files are thus rendered useless.

Figure II
Image used to overwrite files

- Finally, the component will overwrite the MBR so that the compromised computer canno longer start

The following string that points to the location of debug symbols was left in the Wiper component of this threat and gives an idea of where the component was located on the developer's computer:

C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb

4.3 Reporter Component

The Reporter component is responsible for sending infection information back to the attacker. Information is sent as a HTTP GET request and is structured as follows: http://[DOMAIN]/ajax_modal/modal/data.asp?mydata=[MYDATA]&uid=[UID]&state=[STATE]

The following data is sent to the attacker:

- [DOMAIN]—a domain name
- [MYDATA]—a number that specifies how many files were overwritten
- [UID]—the IP address of the compromised computer
- [STATE]—a random number

Threats with such destructive payloads are unusual and are not typical of targeted attacks. Symantec Security Response is continuing to analyze this threat and will post more information as it becomes available. Symantec customers are protected from this threat, which our security products detect as W32.Disttrack.

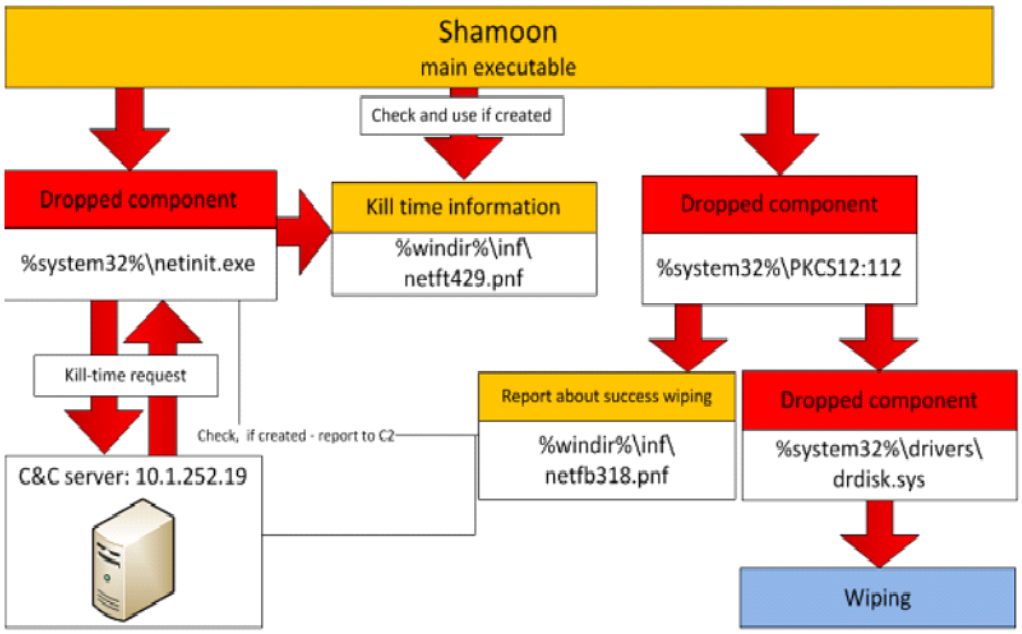

Figure III
Shamoon virus attack overview

Execute the following commands to generate a list of files that will be overwritten and write the path of the files to f1.inf and f2.inf

```
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i download 2>nul >f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i download 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i picture 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i video 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i music 2>nul >>f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i desktop 2>nul >f2.inf
dir C:\Users\ /s /b /a:-D 2>nul | findstr -i desktop 2>nul >>f2.inf
dir C:\Windows\System32\Drivers /s /b /a:-D 2>nul >>f2.inf
dir C:\Windows\System32\Config /s /b /a:-D 2>nul | findstr -v -i systemprofile 2>nul
>>f2.inf
```

The file listed in f1.inf and f2.inf will be overwritten using a JPEG file embedded on the module. The file can be easily extracted using foremost:

- $foremost –v sfmsc.xex –v –T
- The file is part of an image found in the internet showing a burning US flag.

Figure IV
Burning US Flag

The wiper module uses the driver to overwrite the MBR so the system cannot boot anymore. Here summarize the analysis assessment of shamoon virus attack.

III. SUMMARY

Type of attack – automation level malicious attack
Effect – minor level
Scope – high
Target – infect and destroy the data in computer system.
Vulnerability – security weakness. It contains the vulnerabilities are

- One SAP controlled all services
- Network and security specialists are IT company staffs
- Few employees are Hezbollah members

Iran is the centre of this attack. It is the only nation to access the original wiper virus. The Hezbollah, Arab Youth Group and Cutting Sword of Justice involve the hacktivist attack.

IV. CONCLUSION

The main reason for this attack is to disrupt the production and supplies of crude oil and its products to down the billion dollar business. The attacker gain a single system for launch, control, and command to the other systems connected in Local Area Network. The aim of this attack is destroy the system files. Saudi Aramco takes few weeks to renew the services. And also restore its network and recover the data losses, disabled workstation. Shamoon did not cause any physical damages it affects only the risk assessment in global infrastructure. After this attack Saudi Aramco add a new security mechanisms to avoid the cyber-attacks.

V. REFERENCES

1. Bronk, C., & Tikk-Ringas, E. (2013). Hack or attack? Shamoon and the Evolution of Cyber Conflict.
2. Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). World War C: Understanding nation-state motives behind today's advanced cyber attacks. *Technical Report, FireEye*.
3. Dehlawi, Z., & Abokhodair, N. (2013, June). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In *Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on* (pp. 73-75). IEEE.
4. Gamero-Garrido, A. M. (2014). Cyber Conflicts in International Relations: Framework and Case Studies. *Browser Download This Paper*.
5. Alalwan, N., Alzahrani, A., & Sarrab, M. (2013). Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey. *ICoFCS 2013*, 33.
6. Clayton, B., & Segal, A. (2013). *Addressing cyber threats to oil and gas suppliers*. Council on Foreign Relations.