SANGFOR | SANGFOR SECURITY

XXX Company
Security Incident Report

October, 2019

Make IT Simpler, More Secure and Valuable

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: sales@sangfor.com | W.: www.sangfor.com

Document Details

Name	XXX Company Security Incident Report (October 2019)		
Version	V1.0		
ID	SFSS-MSS-IR0101		
Author	Sangfor MSS Team	**Issue Date**	XX-10-2019
Reviewed By	Sangfor MSS Team	**Review Date**	XX-10-2019
Classification	Confidential		
Limited To	· Sangfor Technologies Inc. · XXX Company		
Distribution Control	Sangfor Technologies Inc.: CREATE, MODIFY, READ	XXX Company: READ	

Version Change Record

Modified Date	Version	Description	Modified By
XX-10-2019	V1.0	Final Draft	Yue Fan

Disclaimer

SANGFOR

Table of Contents

1. Incident Overview

1.1 Overview

XXX Company noticed that OA Server was attacked by Phobos ransomware on XX October 2019 around 12pm noon. XXX and Sangfor were engaged to perform forensic investigation and assist in data recovery.

Reported By:	XXXXXXXX
Title / Role:	IT Security Manager

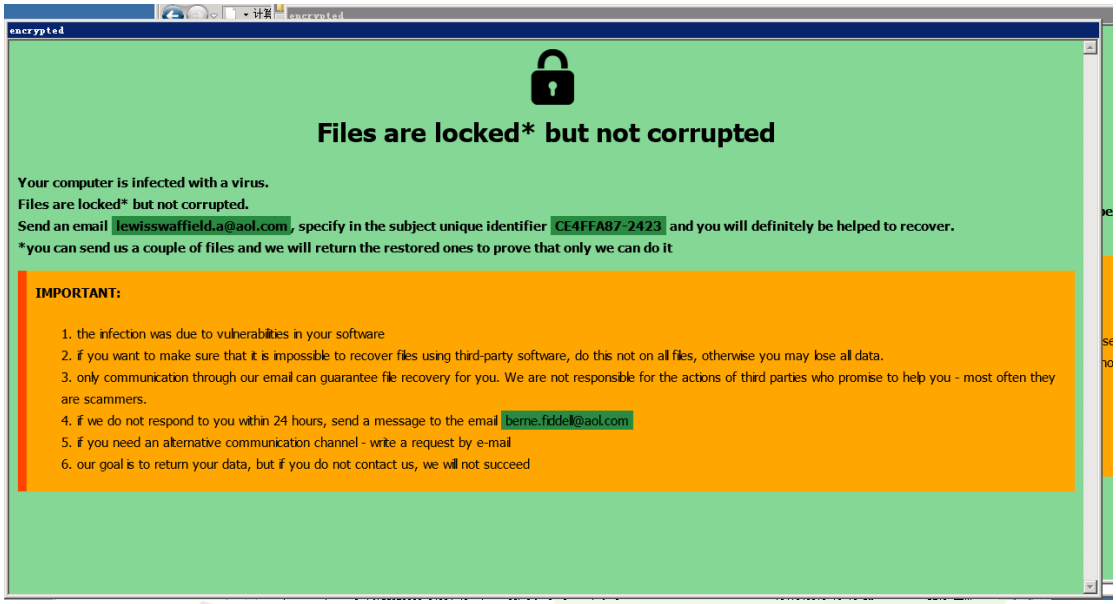
1.2 Technical Details

Affected Server:	Active Directory Server (10.0.0.20)
Server Functions:	Active Directory
Server Operating System:	Windows server 2008 R2
Ransomware Family:	Phobos
Ransomware Description:	Phobos is one of the ransomware that attacks Remote Desktop Protocol (RDP) connections. Once compromised the RDP service of the host, the files within the file system will be encrypted without the need of an Internet connection. Each file will be encrypted via individual initialization vector.

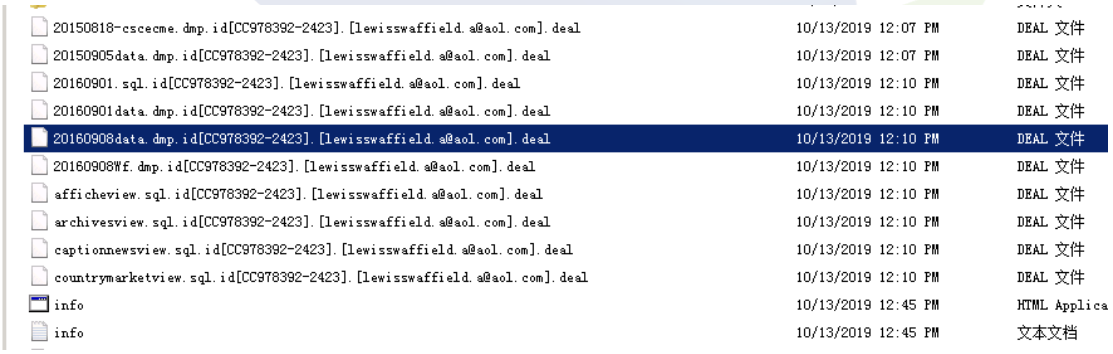
2. Incident Investigation Process

2.1 Abnomaly Observation

Readme file was noticed on the desktop.

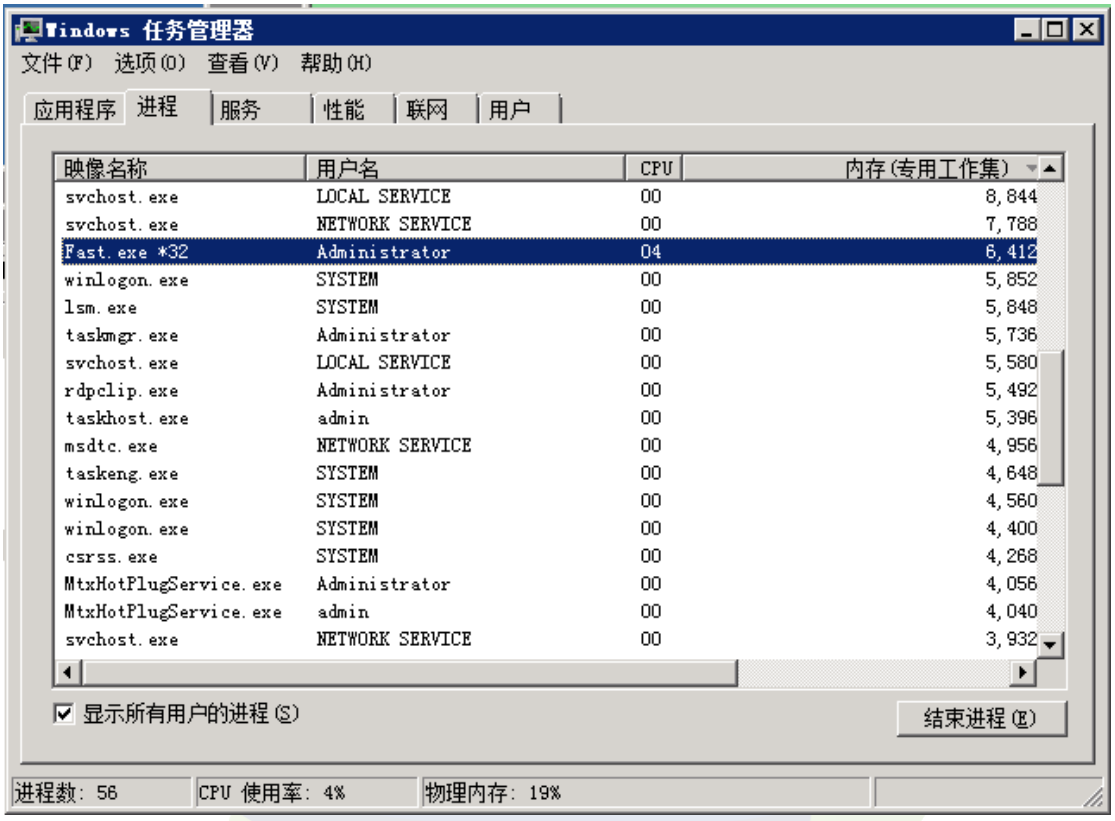


All files in the file system were encrypted and no longer readable.

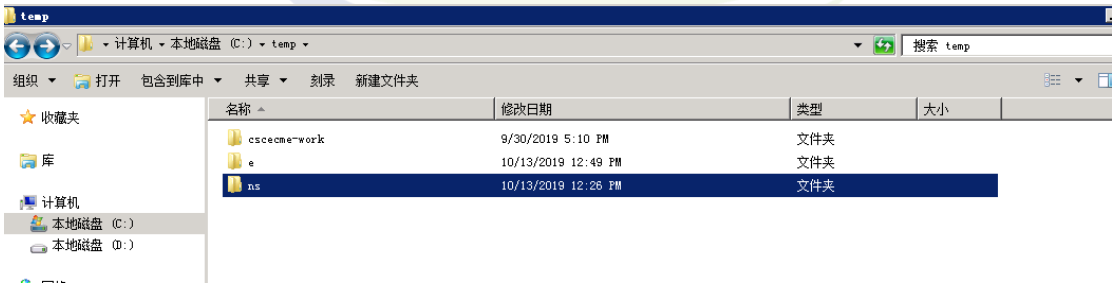


2.2 Investigation and Analysis Process

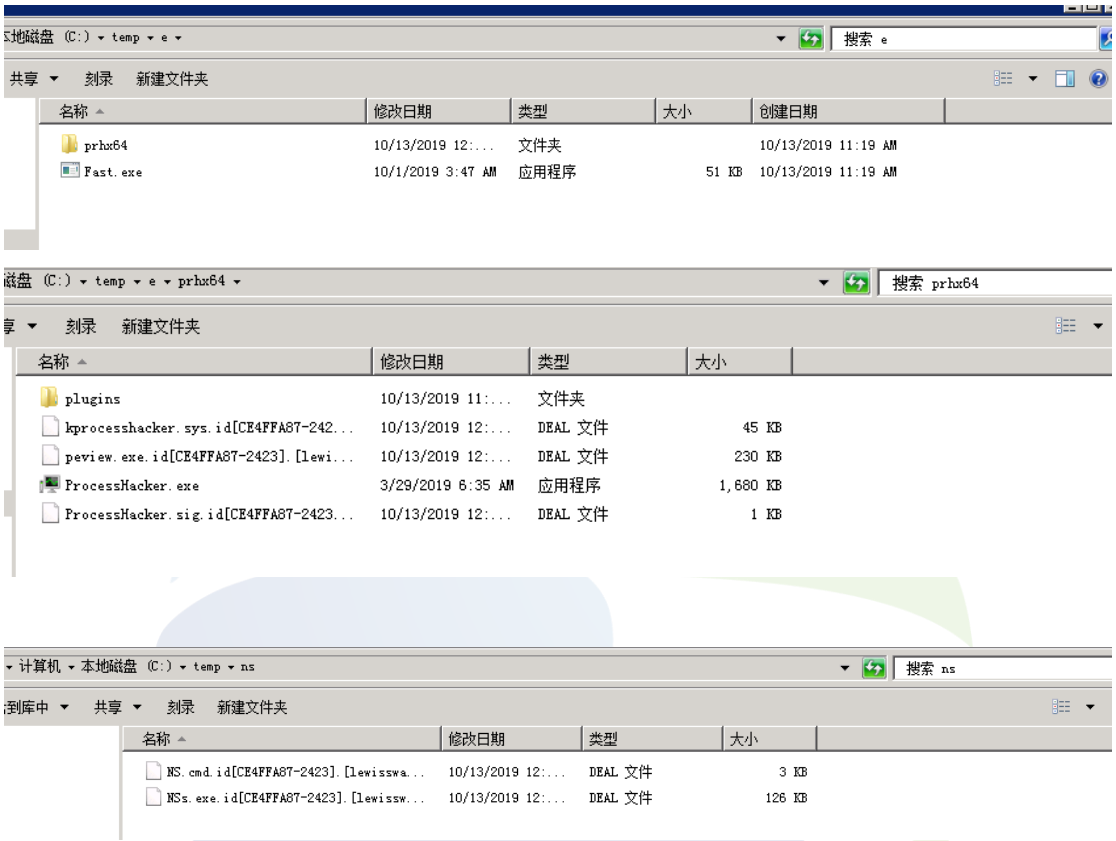
Investigated task manager of the host and identified unknown malicious process was running.



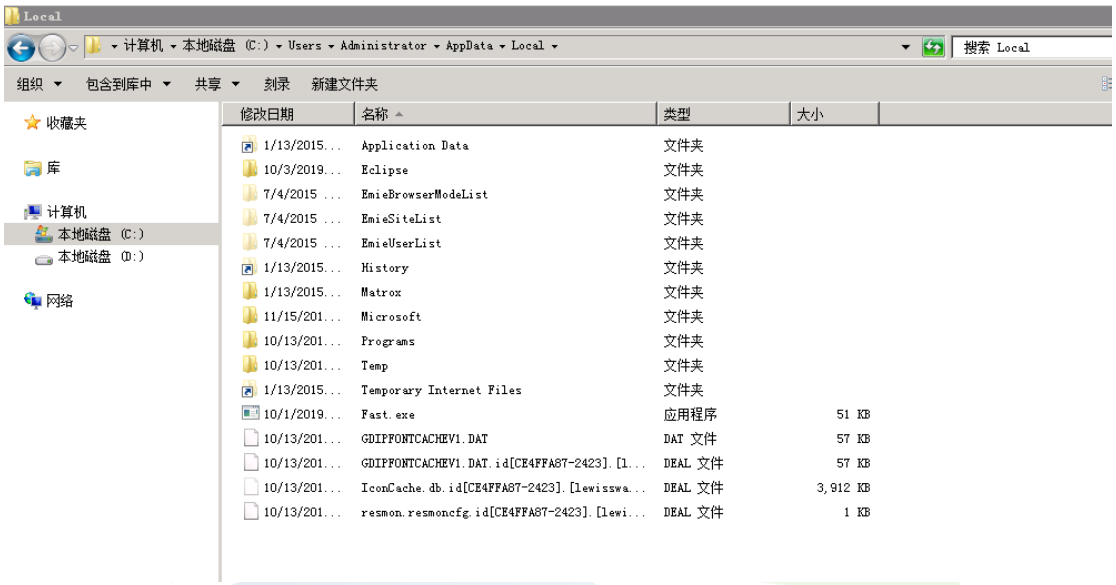
Located the folder location of the unknown process and files.



Relevant hacking tools and malicious hidden files installed by the attacker were identified.



The fast.exe was confirmed to be the ransom virus precursor.



2.3 Kill Chain Determination

The OA server was confirmed that it was the zero patient, first host within the network that affected by ransomware attack.

3. Post-Incident Process

After the ransomware attacks has occurred, Sangfor underwent two important actions on XXX company network in order to ensure the security assurance of the system and minimize the possibility and impact for malware lateral movement.

1 Vulnerability Assessment

- Vulnerability assessment was conducted on internal network to identify the vulnerabilities and attack surface of internal hosts that could be exploited by the attacks
- Deep scanning and authenticated vulnerability assessment were performed on two servers that support critical business operations: Active Directory Server and File Server
- Unauthenticated vulnerability assessment was performed on the rest of the hosts within the network

2 Installation of Endpoint Secure

- Endpoint secure antivirus with latest virus signature database was installed and configured in each endpoints in the XXX company environment
- Active thorough scan was performed on each endpoints to verify the endpoints are not suffered from the ransomware attacks
- Active thorough scan was performed on each endpoints to identify any hidden malware that yet to be discovered

4. Conclusions

Multiple security vulnerabilities and risks were discovered upon the vulnerability scan on XXX company environment, as shown below:

- Server with default settings and lack of hardening
- Unpatched server
- Outdated software and applications
- Misconfigured system and application
- Unnecessary port listening and some were exposed to Internet

Due to the above security risks, vulnerabilities and inappropriate settings may allow an attacker to access the internal network from the Internet. Once gaining access to the internal network, an attacker can perform further enumeration and post-exploitation on the servers within the network. At this stage, an attacker can collect all sensitive information such as SAM files, passwords, company confidential information, and customer data. Not only that, an attacker can escalate his privileges to an administrative privileges. With administrative privileges, an attacker can install malware and backdoors on the system for remote access and persistence and console connections.

5. Gap Analysis

The gap analysis discovered during this security incident as shown below:

No.	Current Situation	Expected Situation	Recommended Mitigation Timeline
1	No backup on system that holding critical and important business data	Perform scheduled backup on system that holding critical and important business data.	1 month
2	No high availability on system that supporting critical business operation	Setup a passive server to ensure availability of the system that supporting critical business operation.	3 months
3	No network perimeter protection mechanism, such as firewall	Implement a firewall in external network perimeter to protect servers from external attacks and unauthorized access.	3 months
4	Lack of VLAN segregation	Implement VLAN segregation to separate servers based on roles and functions.	6 months
5	Lack of server hardening	Ensure servers are hardened before migrating into production environment and perform vulnerability assessment in a regular basis.	6 months

6. Post-Incident Improvement Recommendation

6.1 Overall Improvement Recommendation

1 Use VLAN segregation to ensure that all servers are separated based on the role and functionality of the servers

2 Perform server hardening before migrating to the production environment

3 Perform vulnerability assessments and penetration tests to identify possible threats and hidden risks on a regular basis

4 Perform server and network security product configuration reviews to ensure that all settings and configurations are in a secure manner

5 Ensure that the server, firmware and software are updated to the latest version on a regular basis

6 Ensure high availability and redundancy on servers that support critical business operation

7 Make sure business data is backed-up on a regular basis

8 Ensure no unnecessary ports are listening externally and exposed to Internet

6.2 System Hardening Recommendation

1. Ensure that network security devices are properly implemented and installed to protect against both internal and external threats
   - 1.1. **Firewall**: Protect the network perimeter from external threats and attacks (*NGAF*)
   - 1.2. **SSL-VPN**: Restrict unauthorized users from accessing the internal network (*NGAF*)
   - 1.3. **Antivirus**: Protect endpoints from both known and unknown malware and viruses (*Endpoint Secure*)
   - 1.4. **URL and Application Filtering**: Ensure only authorized URL and applications can be assessible by authorized employees (*NGAF*)

2. Ensure continuous monitoring of any possible attacks and threats, early detection and proactive response
   - 2.1. **Real Time Monitoring**: To continuously monitor for attack attempts, security incidents and events (*NGAF, Cyber Command*)

2.2. **Security Assessment**: Allow Managed Security Service Providers (MSSP) to assess the organization assets for vulnerabilities, threats and risks (*Vulnerability Assessment, Cyber Command*)

2.3. **Product Integration**: Should an attack attempt is discovered, an active response can be made automatically (*NGAF, Endpoint Secure, Cyber Command*)

2.4. **Incident Management**: Prepare standard operation procedures and incident management plans according to different scenarios (*Incident Response*)