SANGFOR

CASE STUDY

Sangfor Incident Response (IR)

Well-known Vehicle Dealers

The information contained in these documents is strictly confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Sangfor Technologies Inc.

Executive Summary

Location: Indonesia	**Employees:** >500
Industry: Retail	**Date & Time:** July 2020

Customer Background

This customer is one of the most well-known vehicle dealers in Indonesia, operating in Jakarta and West Java. As a vehicle retailer, they didn't pay much attention to cyber security.

When they suffered a ransomware attack, they found they had no way to recover from it - leading them to Sangfor for help.

Overview

6 server applications were unavailable and were encrypted. The ransomware was confirmed to be Crysis through the content of the ransomware information and the encryption suffix. There is no public decryption tool at this time.

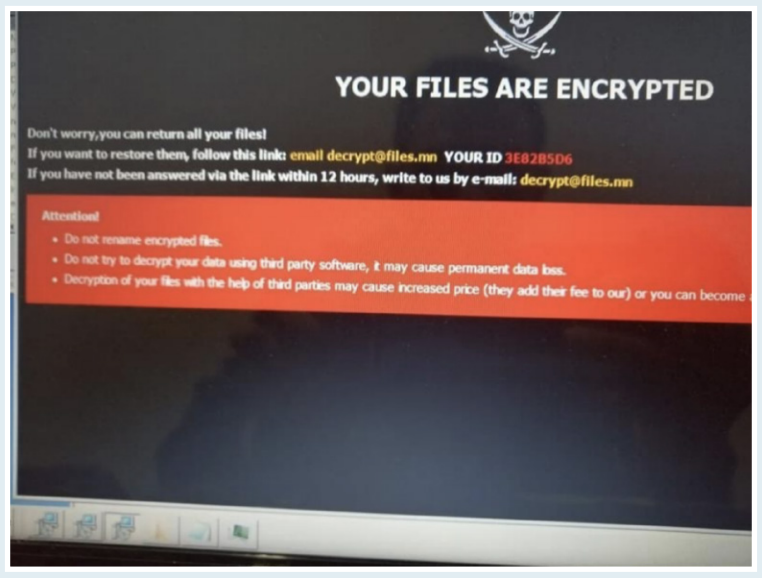
• Technical Details

Affected Server	Server (88.88.XX.XXX, 88.88.XX.XXX, etc.)
Server Functions	Database servers, etc.
Server Numbers	6 servers (5 virtual machines, 1 physical machine)
Ransomware Family	CrySis
Incident Description	The server was attacked by ransomware, encrypting the files with the suffix "ROGER". The ransomware family is CrySis, and there was no public decryption tool. The attack method was to manually run the ransomware file after a successful RDP brute force attack. The Sangfor Security Team traced back the external network invasion to IP 10.100.X.XXX.

Incident Response Process

• Anomaly Observation

Readme file was noticed on the desktop.



YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, follow this link: email decrypt@files.mn YOUR ID 3E82B5D6
If you have not been answered via the link within 12 hours, write to us by e-mail: decrypt@files.mn

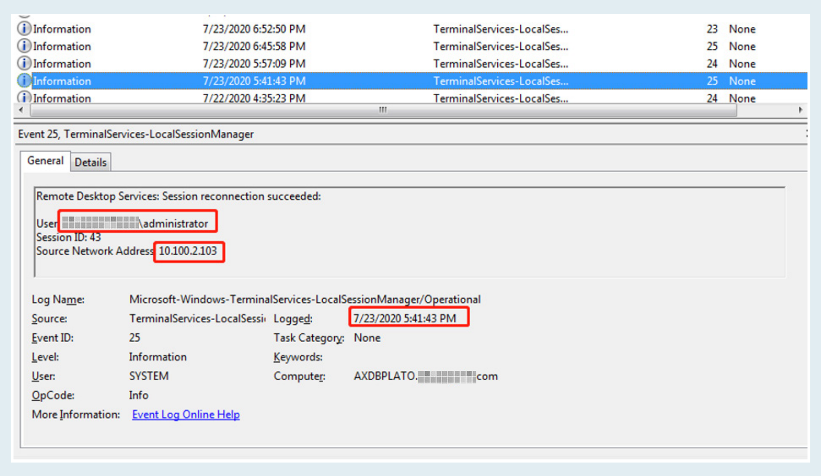
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become

• Investigation and Analysis Process

The investigation log found that there was an RDP login record at 5:41:43 pm on July 23, 2020, with the login IP of 10.100.X.XXX. Thelogin account was XXXXXXX\administrator.

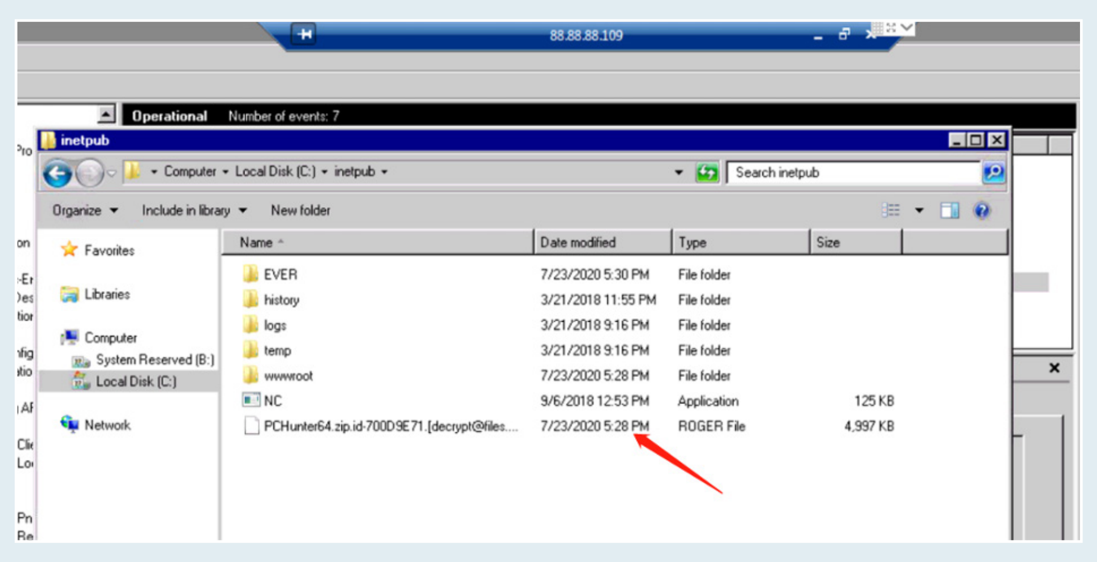
They believe that the hacker logged in through 10.100.X.XXX and executed his ransomware file:



```
Information    7/23/2020 6:52:50 PM    TerminalServices-LocalSes...    23  None
Information    7/23/2020 6:45:58 PM    TerminalServices-LocalSes...    25  None
Information    7/23/2020 5:57:09 PM    TerminalServices-LocalSes...    24  None
Information    7/23/2020 5:41:43 PM    TerminalServices-LocalSes...    25  None
Information    7/22/2020 4:35:23 PM    TerminalServices-LocalSes...    24  None

Event 25, TerminalServices-LocalSessionManager

Remote Desktop Services: Session reconnection succeeded:

User [redacted]\administrator
Session ID: 43
Source Network Address 10.100.2.103

Log Name:          Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source:            TerminalServices-LocalSessi  Logged:         7/23/2020 5:41:43 PM
Event ID:          25                           Task Category:  None
Level:             Information                  Keywords:
User:              SYSTEM                       Computer:       AXDBPLATO.[redacted]com
OpCode:            Info
More Information:  Event Log Online Help
```

• 88.88.XX.XXX

According to the modified encrypted file time, the ransomware encryption was around 5:28 pm on July 23, 2020:



88.88.88.109

Operational Number of events: 7

inetpub

Computer ▸ Local Disk (C:) ▸ inetpub ▸

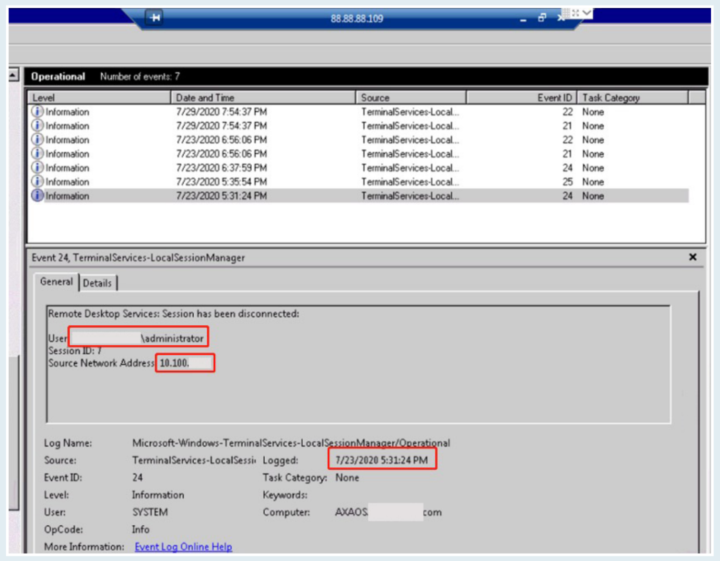
Search inetpub

Organize ▾ Include in library ▾ New folder

Name	Date modified	Type	Size
EVER	7/23/2020 5:30 PM	File folder	
history	3/21/2018 11:55 PM	File folder	
logs	3/21/2018 9:16 PM	File folder	
temp	3/21/2018 9:16 PM	File folder	
wwwroot	7/23/2020 5:28 PM	File folder	
NC	9/6/2018 12:53 PM	Application	125 KB
PCHunter64.zip.id-700D9E71.[decrypt@files....	7/23/2020 5:28 PM	ROGER File	4,997 KB

The investigation log found an RDP logout record at 5:31:24 PM on July 23, 2020.

The login IP was 10.100.X.XXX, and the login account was XXXXXXX\administrator. They believed that the hacker was logged in and executed his ransomware file through 10.100.X.XXX and cleared the login system log:



88.88.88.109

Operational Number of events: 7

Level	Date and Time	Source	Event ID	Task Category
Information	7/29/2020 7:54:37 PM	TerminalServices-Local...	22	None
Information	7/29/2020 7:54:37 PM	TerminalServices-Local...	21	None
Information	7/23/2020 6:56:06 PM	TerminalServices-Local...	22	None
Information	7/23/2020 6:56:06 PM	TerminalServices-Local...	21	None
Information	7/23/2020 6:37:59 PM	TerminalServices-Local...	24	None
Information	7/23/2020 5:35:54 PM	TerminalServices-Local...	25	None
Information	7/23/2020 5:31:24 PM	TerminalServices-Local...	24	None

Event 24, TerminalServices-LocalSessionManager

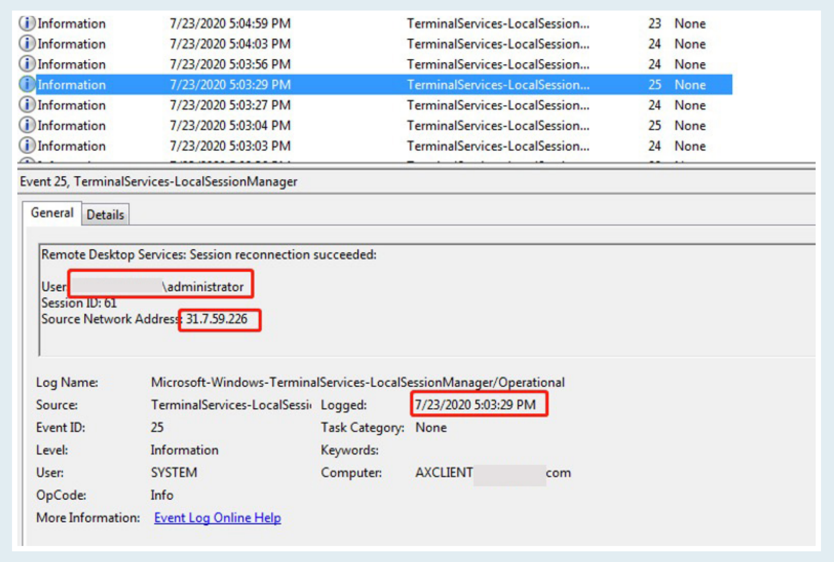
General | Details

```
Remote Desktop Services: Session has been disconnected:

User [redacted]\administrator
Session ID: 7
Source Network Address 10.100.[redacted]
```

```
Log Name:          Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source:            TerminalServices-LocalSessi   Logged:          7/23/2020 5:31:24 PM
Event ID:          24                            Task Category:   None
Level:             Information                   Keywords:
User:              SYSTEM                        Computer:        AXAOS[redacted]com
OpCode:            Info
More Information:  Event Log Online Help
```

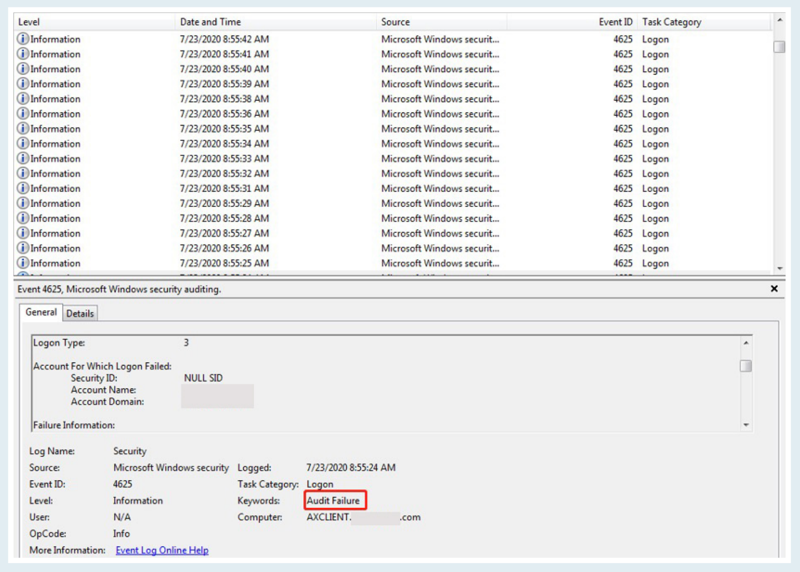
• 10.100.X.XXX

This host was not encrypted, but suspicious logs were found. The host was logged in using IP 31.7.XX.XXX (Zurich, Switzerland) at 5:03:29 PM on July 23, 2020. The login account was XXXXXXX\administrator:



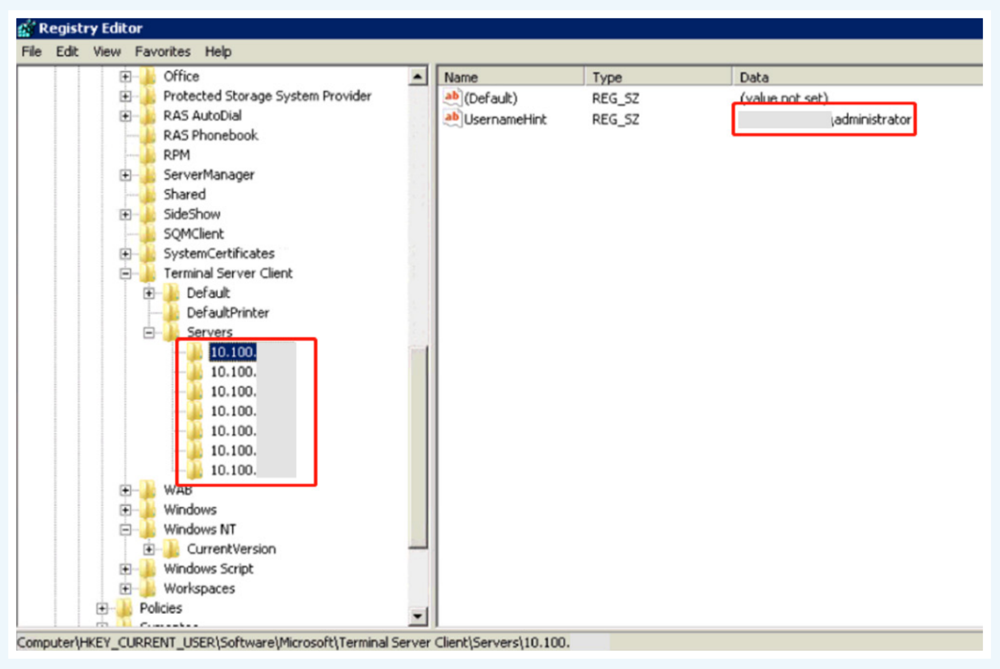
```
Information    7/23/2020 5:04:59 PM    TerminalServices-LocalSession...    23  None
Information    7/23/2020 5:04:03 PM    TerminalServices-LocalSession...    24  None
Information    7/23/2020 5:03:56 PM    TerminalServices-LocalSession...    24  None
Information    7/23/2020 5:03:29 PM    TerminalServices-LocalSession...    25  None
Information    7/23/2020 5:03:27 PM    TerminalServices-LocalSession...    24  None
Information    7/23/2020 5:03:04 PM    TerminalServices-LocalSession...    25  None
Information    7/23/2020 5:03:03 PM    TerminalServices-LocalSession...    24  None

Event 25, TerminalServices-LocalSessionManager

General | Details

Remote Desktop Services: Session reconnection succeeded:

User: [redacted]\administrator
Session ID: 61
Source Network Address: 31.7.59.226

Log Name:          Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source:            TerminalServices-LocalSessi  Logged:         7/23/2020 5:03:29 PM
Event ID:          25                           Task Category:  None
Level:             Information                  Keywords:
User:              SYSTEM                       Computer:       AXCLIENT[redacted]com
OpCode:            Info
More Information:  Event Log Online Help
```

Looking at the security log, you can see a large number of login failure records. It can be inferred that the hacker invaded 10.100.X.XXX from the external network through brute force attack:



```
Level          Date and Time          Source                       Event ID  Task Category
Information    7/23/2020 8:55:42 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:41 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:40 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:39 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:38 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:36 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:35 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:34 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:33 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:32 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:31 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:29 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:28 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:27 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:26 AM   Microsoft Windows securit...     4625  Logon
Information    7/23/2020 8:55:25 AM   Microsoft Windows securit...     4625  Logon

Event 4625, Microsoft Windows security auditing.

General | Details

Logon Type:                 3

Account For Which Logon Failed:
        Security ID:        NULL SID
        Account Name:       [redacted]
        Account Domain:

Failure Information:

Log Name:          Security
Source:            Microsoft Windows security  Logged:         7/23/2020 8:55:24 AM
Event ID:          4625                        Task Category:  Logon
Level:             Information                 Keywords:       Audit Failure
User:              N/A                         Computer:       AXCLIENT.[redacted].com
OpCode:            Info
More Information:  Event Log Online Help
```

You can see that 10.100.X.XXX has remotely logged into several hosts. Except for 10.100.X.XXX and 10.100.X.XXX, all data has been encrypted. Therefore, it can be inferred that hackers logged into 10.100.X.XXX from the external network using RDP. They used it as a jumping off point to encrypt other hosts on the intranet:



```
Office
Protected Storage System Provider
RAS AutoDial
RAS Phonebook
RPM
ServerManager
Shared
SideShow
SQMClient
SystemCertificates
Terminal Server Client
    Default
    DefaultPrinter
    Servers
        10.100.[redacted]
        10.100.
        10.100.
        10.100.
        10.100.
        10.100.
        10.100.
WAB
Windows
Windows NT
    CurrentVersion
Windows Script
Workspaces
Policies
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
UsernameHint	REG_SZ	[redacted]\administrator

Computer\HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\10.100.[redacted]

Conclusions

• According to Investigation Results

01 The ransomware family is CrySis, and there is currently no public decryption tool.

02 Hackers logged into 10.100.X.XXX through brute force cracking from the external network, then used it as a platform to log onto other hosts on the internal network and manually run the ransomware.

Overall Improvement Recommendations

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

Perform server hardening before migrating to the production environment

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

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

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

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

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

Ensure no unnecessary ports are listening externally and exposed to Internet

Sangfor Solution

Ensure that network security devices are properly installed and deployed 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 - Anti-virus

Protect endpoints from both known and unknown malware and viruses *(Endpoint Secure)*

1.4. URL and Application Filtering

Ensure only authorized URL and applications are accessible by authorized employees *(NGAF)*

Ensure Continuous Monitoring of Any Possible Attacks and Threats, Early Detection and Proactive Response

1.1. Real-Time Monitoring

To continuously monitor for attack attempts, security incidents and events *(Platform X, Cyber Command)*

1.2. Security Assessment

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

1.3. Product Integration

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

1.4. Incident Management

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

Customer Feedback

★★★★★

> Sangfor Indonesia office left us with an indelible impression. When we were attacked by ransomware encryption, we first asked our SI for help. They helped us contact Sangfor.

> In the beginning, we did not trust this Chinese vendor very much, because we have never heard of its name. But their enthusiasm, professionalism and efficiency have won our trust. In the end, with everyone’s cooperation, the viruses in our network have been cleaned up, the protection has also been strengthened, and the business is recovered within one day.

> We have never paid much attention to the investment in network security. After this incident, we decided to purchase a batch of Sangfor firewalls and other equipment, hoping to stop being hacked again.

SANGFOR

Make IT Simpler, More Secure and Valuable !

www.sangfor.com