



CASE STUDY


Sangfor Incident Response (IR)

Integrated Solar Cell And Module Manufacturer

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: Vietnam	Company Size: 800 employees
Industry: Manufacturing	Date & Time: 2021.2.22 10:24
Customer Old Solution	Sangfor Solution
Fortigate + Symantec Norton	 NGAF + Endpoint Secure

Customer Background

Solar Cell And Solar Panel Manufacturing

This customer is a famous integrated solar cell and module manufacturer in Vietnam equipped with highly automatic production lines generating 1GW annual capacity. Their products are available globally through local regional offices and resell partners.

Incident Response Process

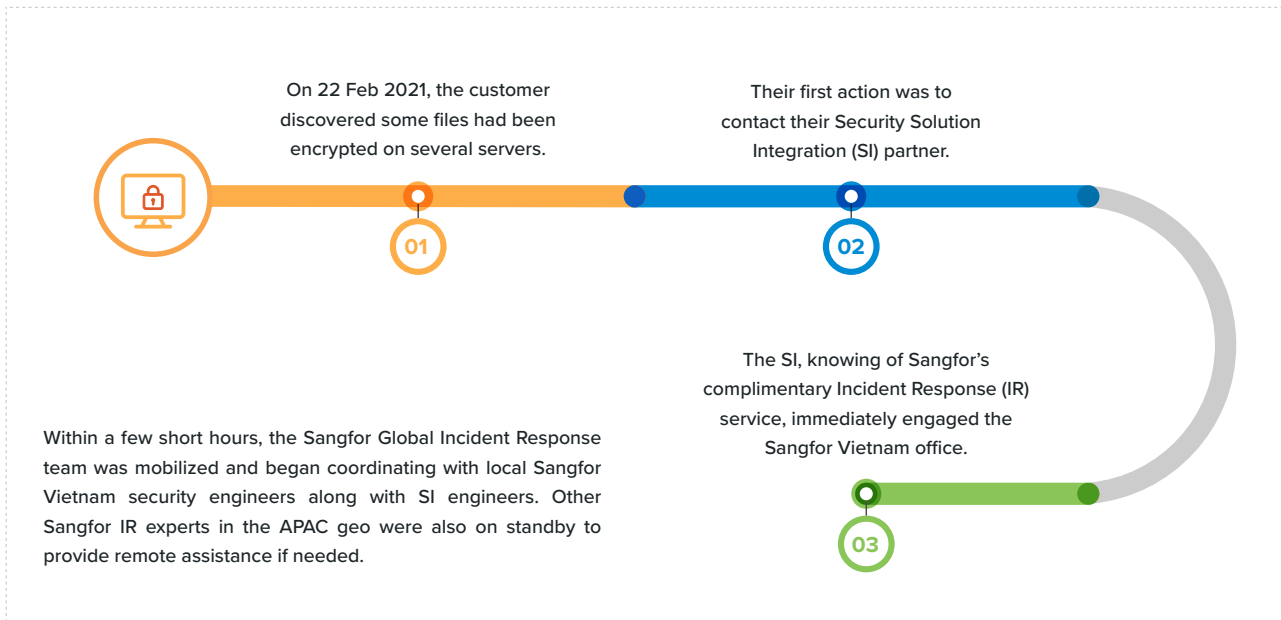
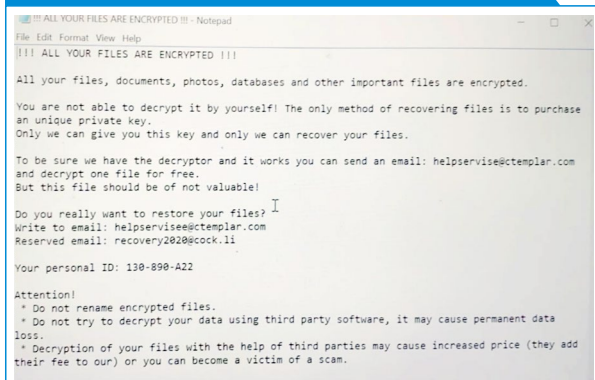
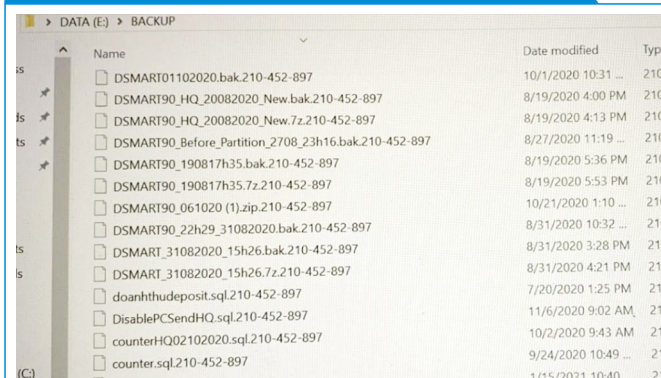


Figure 1 Sample ransom demand

Figure 2 Backup directory with files untouched by ransomware


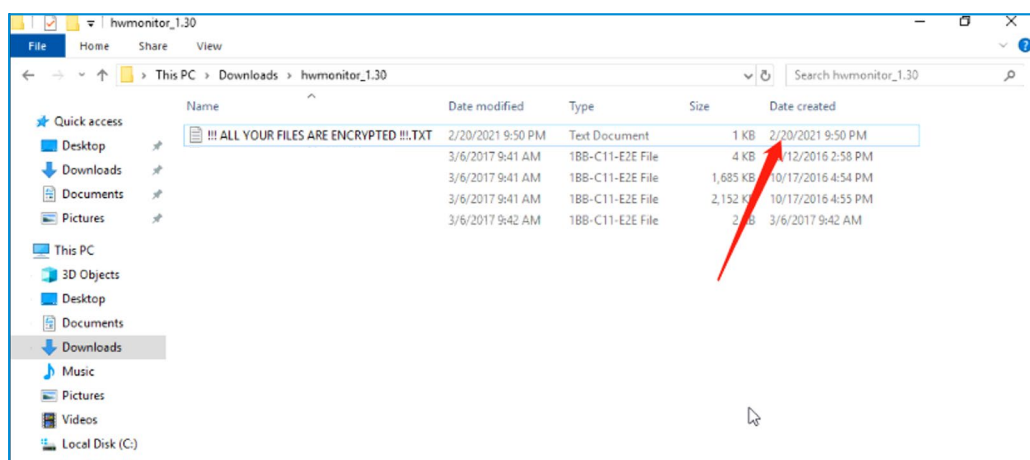
Name	Date modified	Type
DSMART01102020.bak.210-452-897	10/1/2020 10:31 ...	210
DSMART90_HQ_20082020_New.bak.210-452-897	8/19/2020 4:00 PM	210
DSMART90_HQ_20082020_New.7z.210-452-897	8/19/2020 4:13 PM	210
DSMART90_Before_Partition_2708_23h16.bak.210-452-897	8/27/2020 11:19 ...	210
DSMART90_190817h35.bak.210-452-897	8/19/2020 5:36 PM	210
DSMART90_190817h35.7z.210-452-897	8/19/2020 5:53 PM	210
DSMART90_061020 (1).zip.210-452-897	10/21/2020 1:10 ...	210
DSMART90_22h29_31082020.bak.210-452-897	8/31/2020 10:32 ...	210
DSMART_31082020_15h26.bak.210-452-897	8/31/2020 3:28 PM	210
DSMART_31082020_15h26.7z.210-452-897	8/31/2020 4:21 PM	210
doanhthudeposit.sql.210-452-897	7/20/2020 1:25 PM	210
DisablePCSendHQ.sql.210-452-897	11/6/2020 9:02 AM	210
counterHQ02102020.sql.210-452-897	10/2/2020 9:43 AM	210
counter.sql.210-452-897	9/24/2020 10:49 ...	210

According to the encrypted content and file suffixes, it was confirmed that multiple servers were infected by Buran family ransomware. Figure 1 is a sample of the ransom demand text file left on the infected systems.

Currently, there is no public decryption tool available for this ransomware strain. Interestingly, there was no sign that the ransomware was trying to spread further throughout the organization such as infecting backups.

Forensic Investigation and Analysis

According to the timestamp of the ransom note, the ransomware encryption process ended at 9:50 PM on Feb 20th, 2021.



Server operational logs recorded an RDP login at 7:51:34 PM on Feb 20th, 2021, and the source IP was from an external source with 192.168.XX.XX.

Figure 3 Server operational log showing RDP login

The screenshot shows the Windows Event Viewer interface. The top pane displays a list of operational events. The bottom pane shows the details for Event 21, TerminalServices-LocalSessionManager.

Level	Date and Time	Source	Event ID	Task Category
Information	2/21/2021 10:37:02 AM	TerminalServ...	40	None
Information	2/21/2021 10:31:11 AM	TerminalServ...	25	None
Information	2/21/2021 10:31:06 AM	TerminalServ...	40	None
Information	2/20/2021 7:51:35 PM	TerminalServ...	22	None
Information	2/20/2021 7:51:34 PM	TerminalServ...	21	None
Information	2/20/2021 7:51:30 PM	TerminalServ...	42	None
Information	2/20/2021 7:51:30 PM	TerminalServ...	41	None
Information	2/20/2021 7:36:19 PM	TerminalServ...	40	None
Information	1/4/2021 11:20:14 AM	TerminalServ...	24	None
Information	1/4/2021 11:20:14 AM	TerminalServ...	40	None

Event 21, TerminalServices-LocalSessionManager

General Details

Remote Desktop Services: Session logon succeeded:

User: FAMIMA\test1
 Session ID: 4
 Source Network Address: 192.168.

Log Name: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
 Source: TerminalServices-LocalSessionManager
 Logged: 2/20/2021 7:51:34 PM

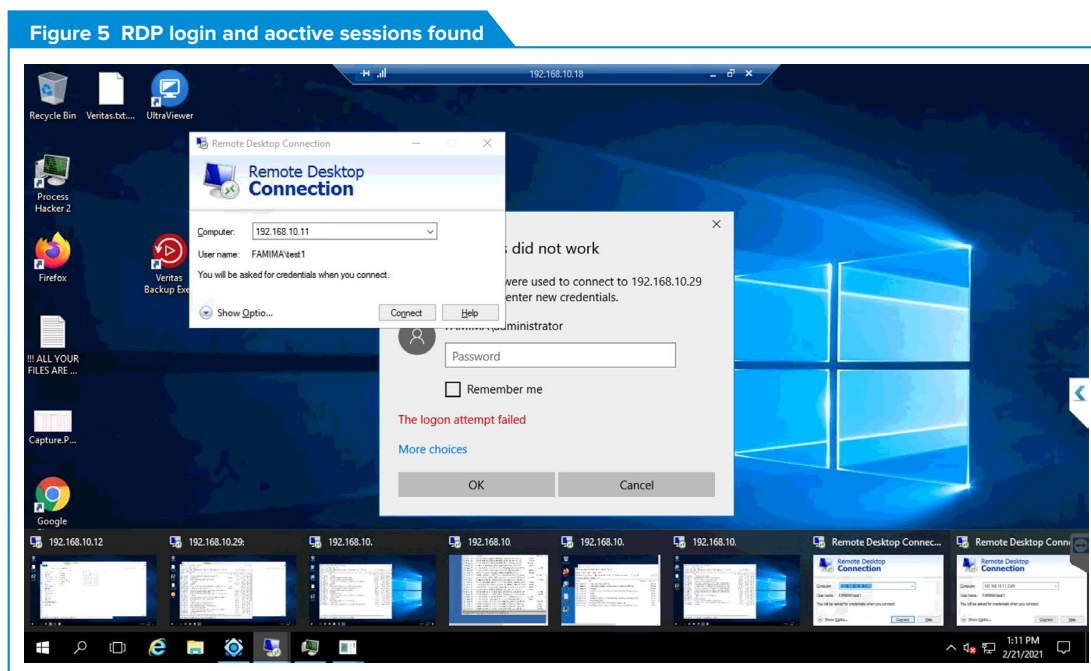
Several hacking tools, such as PCHunter, HRSword, and minikatz were found on the server. These tools were likely used by the attackers to kill any security software that was running and to grab host passwords.

Figure 4 Discovered hacking tools

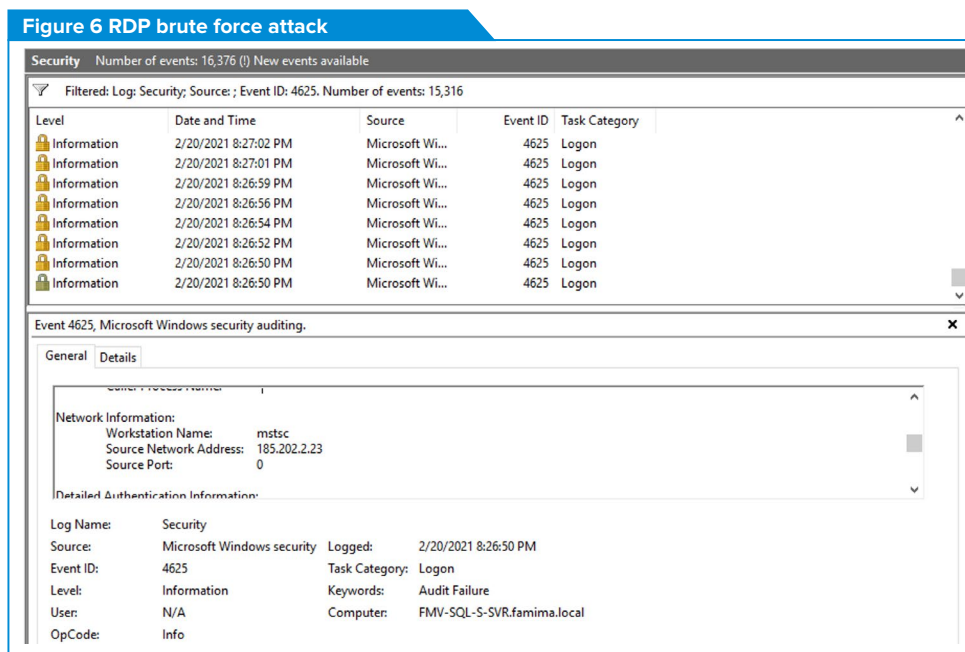
The screenshot shows a Windows File Explorer window displaying the contents of the C:\Users\test1\Pictures directory. The files and folders listed are:

Name	Date modified	Type	Size
Mimik	2/20/2021 9:05 PM	File folder	
!!! ALL YOUR FILES ARE ENCRYPTED !!!	2/20/2021 9:18 PM	Text Document	1 KB
DefenderControl.exe.1BB-C11-E2E	12/17/2019 12:49 PM	1BB-C11-E2E File	828 KB
DefenderControl.ini.1BB-C11-E2E	2/20/2021 9:01 PM	1BB-C11-E2E File	4 KB
desktop.ini	2/20/2021 7:51 PM	Configuration sett...	1 KB
HRSword.exe.1BB-C11-E2E	8/14/2020 8:14 AM	1BB-C11-E2E File	1,921 KB
Mimiknewtest.exe.1BB-C11-E2E	10/21/2020 2:03 AM	1BB-C11-E2E File	1,920 KB
mmmmmm.exe	12/11/2020 7:20 AM	Application	212 KB
pchunter.ek.1BB-C11-E2E	8/7/2020 10:45 AM	1BB-C11-E2E File	2 KB
Pchunter64.exe	1/31/2019 4:20 PM	Application	10,661 KB
Process Hacker.exe.1BB-C11-E2E	11/11/2020 6:59 PM	1BB-C11-E2E File	2,217 KB

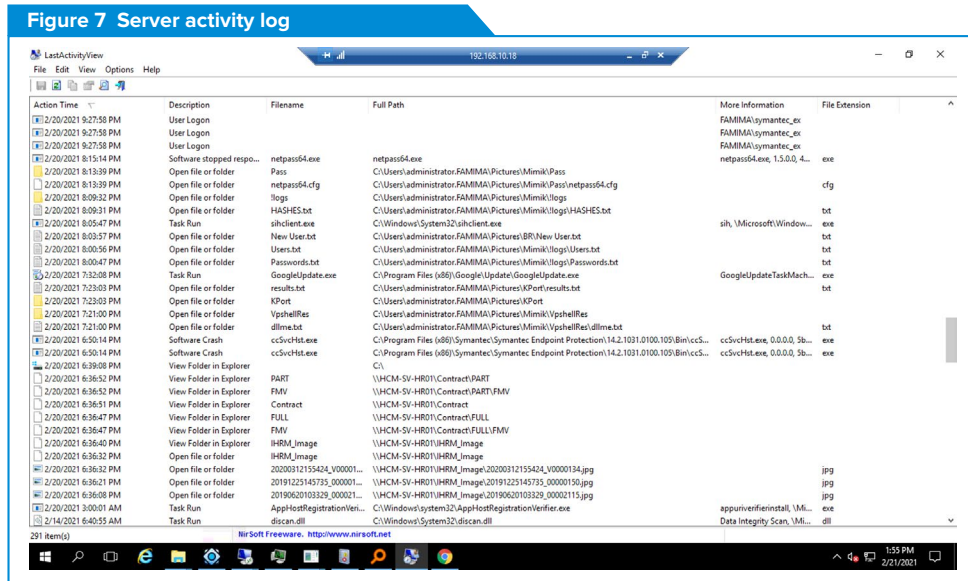
One host had multiple RDP login and active session windows open.



Server security logs showed evidence of an RDP brute force attack from that host, many of which were successful.



It can be inferred from the host activity log that the attacker remotely logged into the server and killed all **Symantec Norton** processes. Then, the attacker scanned the internal network, grabbed passwords, and invaded other hosts through RDP brute force.



The ransomware connected back to command & control (C&C) servers for instructions and to exfiltrate data. However, the Fortigate firewall did not see nor stop those communications. The onsite team installed the Sangfor NGAF at the perimeter which quickly blocked all C&C communications.

Conclusion

The IR forensic investigation concluded the following:

1. The ransomware family is Buran, and there is currently no public decryption tool, no active spread activity.
2. The attacker logged into 10.100.2.103 through an RDP brute force attack from an external source with IP address 192.168.10.18.
3. The attacker used hacking tools to kill all Symantec processes while scanning other hosts in the internal network.
4. The attacker successfully logged into several other servers because all the compromised servers shared the same password. The attacker then initiated the ransomware process after killing the security software.

5. The ransomware attack did not propagate and attack other drives or more servers.

6. Fortigate did not stop C&C communication between victim hosts and attacker servers; Sangfor NGAF stopped it immediately.

Sangfor IR Remediation Recommendations

01

Close the RDP service if not needed and do not directly map RDP port 3389 to the external network. If there is a business need, it is recommended to use the micro-isolation capability of Sangfor Endpoint Secure to control and block the targeted ports from unauthorized hosts or use VPN for access.

02

Use the Endpoint Secure security policy baseline assessment function to find weak passwords on hosts and notify system administrators to change them immediately.

03

Turn on the Endpoint Secure RDP brute force attack and automatic blocking function. When a brute force attack is detected, a password strength check should be run on all hosts and system administrators should be alerted to change passwords immediately.

04

Security personnel should conduct log reviews and analysis regularly to look for potential high-risk attack surfaces and abnormal behavior; you can also contact the Sangfor Incident Response team to conduct assessments of the company's network security.

05

Change all server passwords. Do not to use the same password for different hosts.

Customer Feedback

“

“We greatly appreciate Sangfor’s help and ability to quickly respond. We chose industry leading brands before, Fortinet & Symantec, but we were still breached, and files encrypted. And they refused to support us when their products got hacked. We paid lots of money to them, but they threw us away like trash. It is really sad.”

”

“

“When our SI called Sangfor after we were hacked, Sangfor helped us stop the ransomware encryption process, cleaned up our systems, discovered our weaknesses and traced back the attacking source, etc. Sangfor even provided a professional IR report in the end for us to use. All this service for free!”

”

“

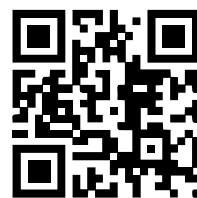
“Now we trust Sangfor more than any other vendor. We believe Sangfor can protect our cybersecurity 24*7. I hope more and more people will know this company.”

”



SANGFOR

Make IT Simpler, More Secure and Valuable!



www.sangfor.com