SANGFOR

CASE STUDY

Sangfor Incident Response (IR)

Integrated Solar Cell And Module Manufacturer

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

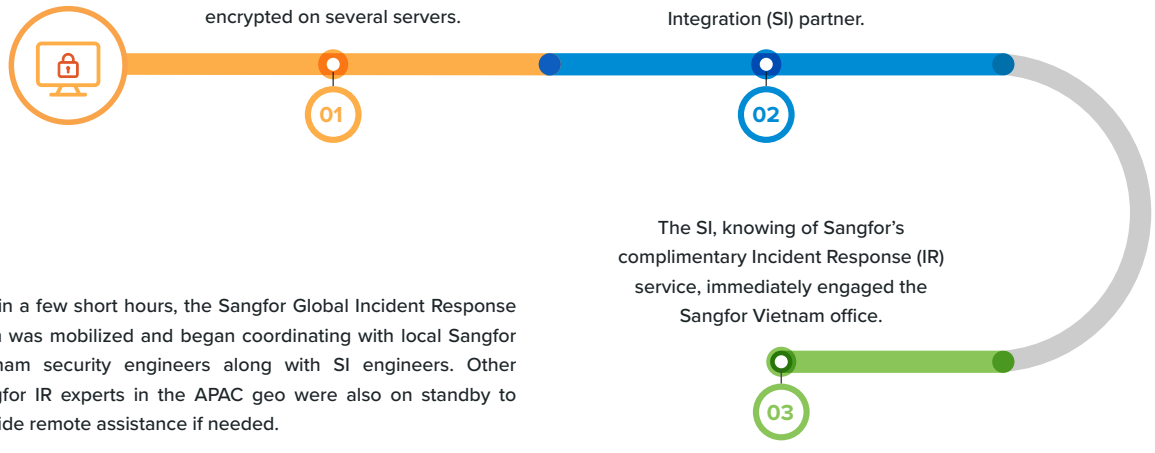


Figure 1 Sample ransom demand

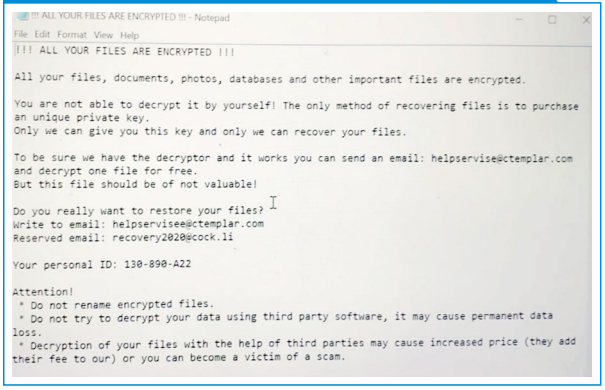
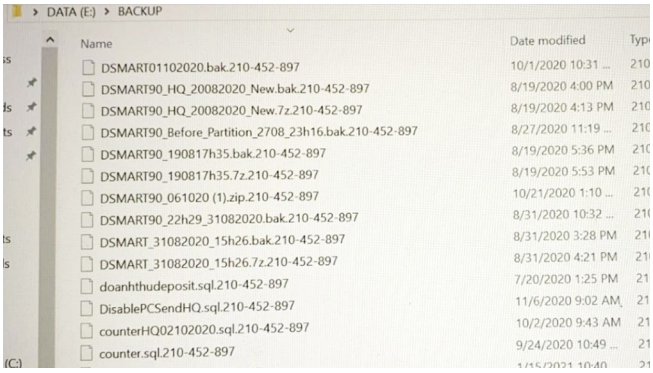


Figure 2 Backup directory with files untouched by ransomware

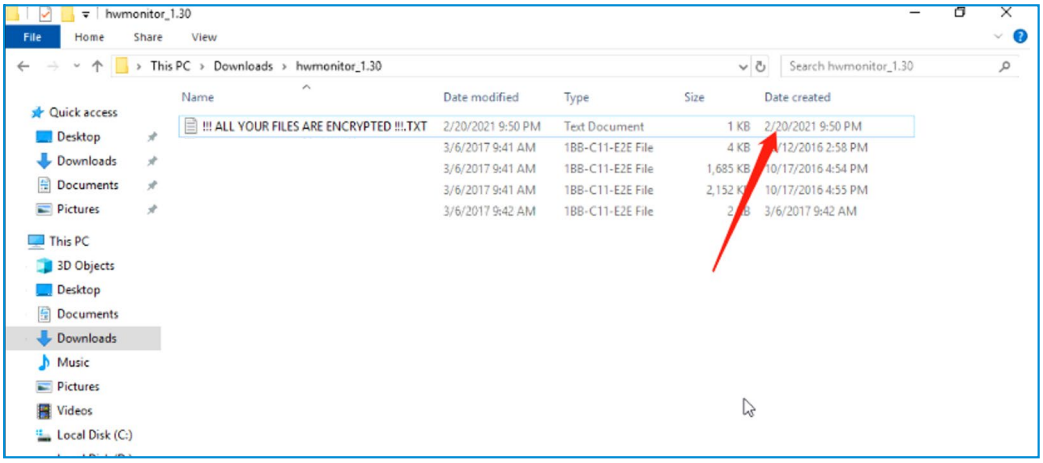


According to the encrypted content and file suffixes, it was confirmed that multiple servers were infected by Buran family ransomware. Figure 1 is a sample of the ransom demand text file left on the infected systems.

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.

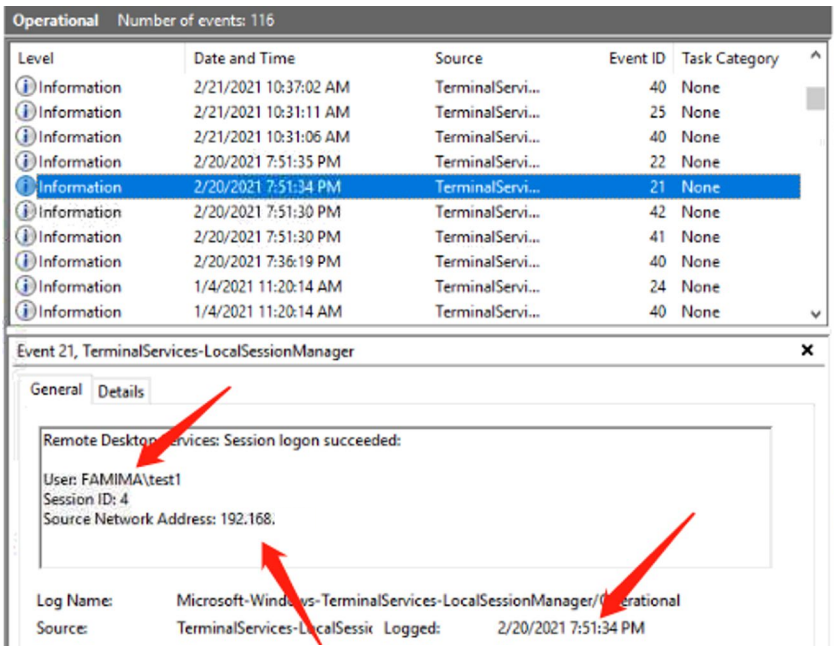
Forensic Investigation and Analysis

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



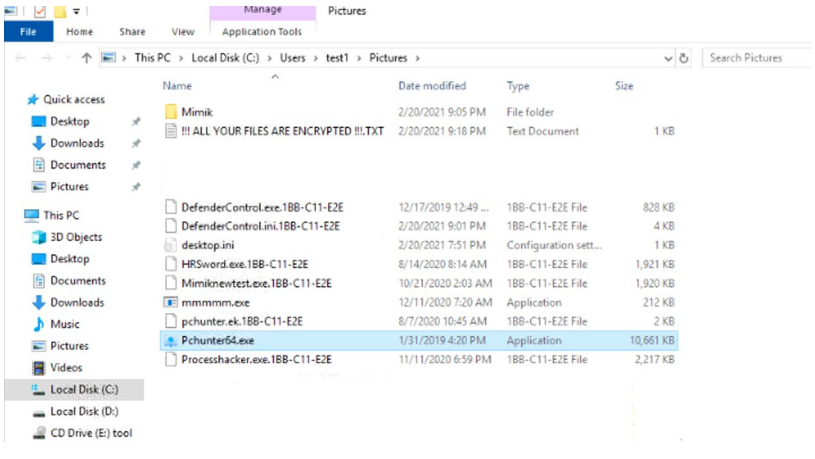
Server operational logs recorded an RDP login at 7:51:34 PM on Feb 20th, 2021, and the source IP was from an external source with 192.168.XX.XX.

Figure 3 Server operational log showing RDP login



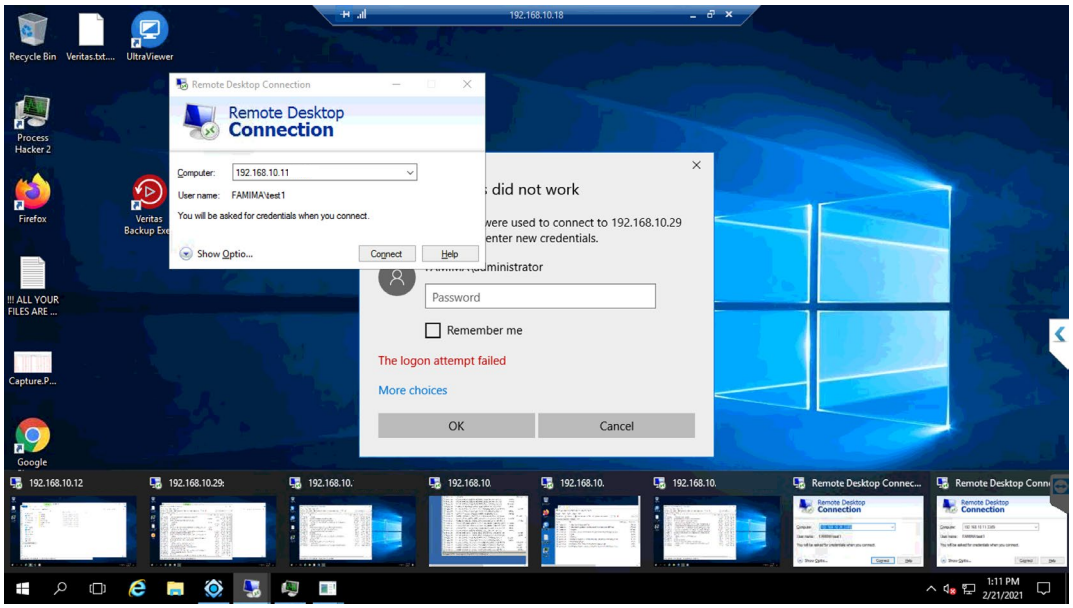
Several hacking tools, such as PCHunter, HRSword, and minikatz were found on the server. These tools were likely used by the attackers to kill any security software that was running and to grab host passwords.

Figure 4 Discovered hacking tools



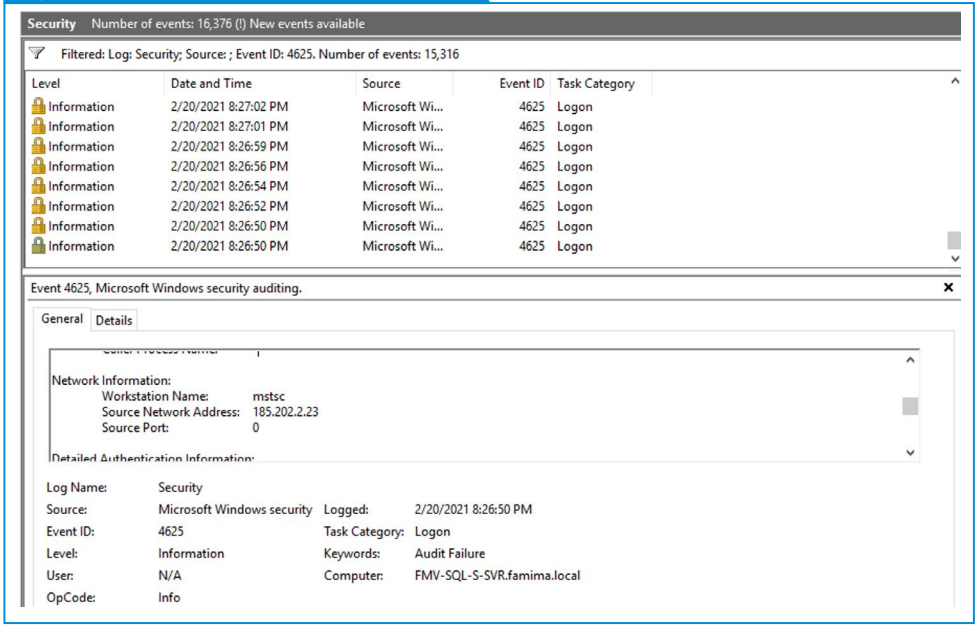
One host had multiple RDP login and active session windows open.

Figure 5 RDP login and aoctive sessions found



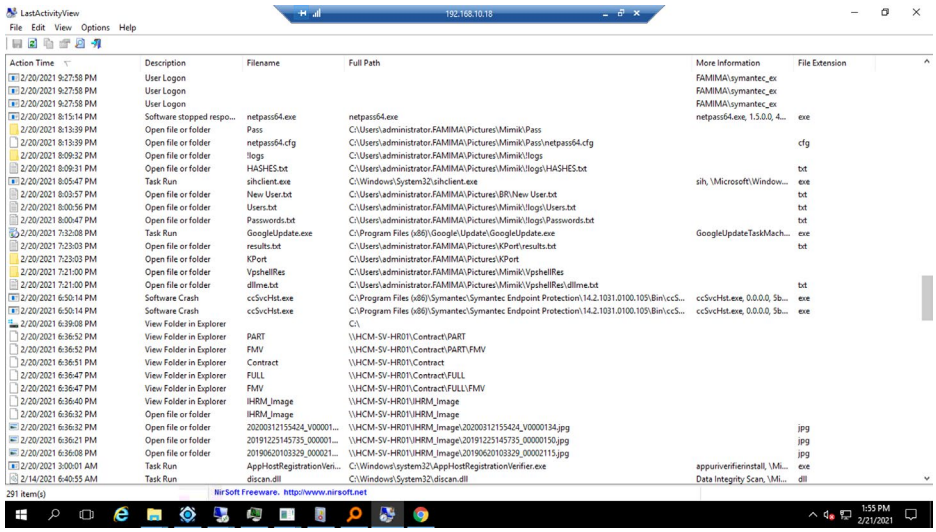
Server security logs showed evidence of an RDP brute force attack from that host, many of which were successful.

Figure 6 RDP brute force attack



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.

Figure 7 Server activity log



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