INCIDENT RESPONSE CASE STUDY

Sangfor Solution: Cyber Command + Endpoint Secure + TIARA Service + Incident Response Service

Hong Kong

ISP

>50,000 employees

March 2021

Customer Background

Communications Industry

This customer is a well-respected ISP company in the world. It has been paying great attention to network security using leading technologies, products, and solutions. It has long been trusted by hundreds of millions of users, with thousands of employees specialized in cyber security. They also have their own unique insights into the global cyber threat situation. As an organization managing hundreds of millions of people's data, this client has been doing its utmost to reduce cyber threats. At the same time, it has real-time exchange of threat intelligence with the world's most well-known open cyber security information sharing platforms, and teamed up with the world's top cyber security vendors to provide comprehensive security protection before, during and after security events.

Incident Response Process

On 20th February 2021, a Saturday and thus a non-work day for employees, Staff member A's IP address was used to log into the firewall of an unrelated, different department. The user had made changes, which results in firewall disconnecting the port and generating an alarm.

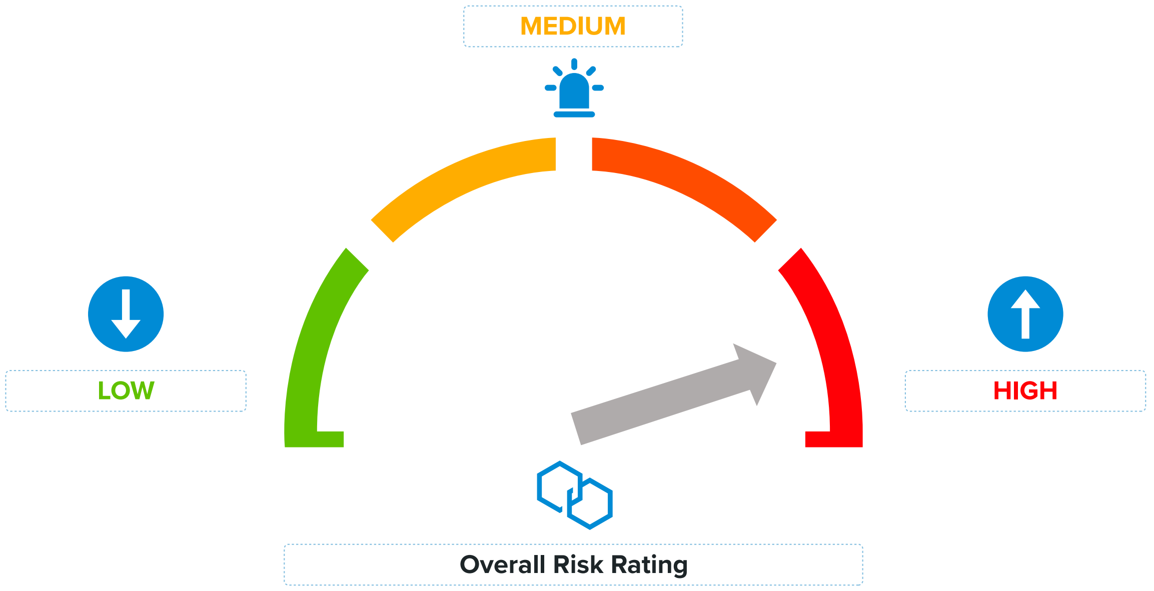
When Staff member A returned to the office, he noticed that the IP address of a different staff member, staff member B, had tried to log into his computer just 15 minutes before the incident. Staff member A approached Staff member B and asked that he or she change their passwords and log-in information, and unplug the network cable immediately. Still, the staff member didn't suspect cyber-attack. While the network cable had been unplugged on Monday at 6pm, it was discovered the next morning, that staff member B had logged in with the new login information and passwords on Monday evening, indicating that the account was hacked Monday evening, even with all the precautions taken.

It was also discovered that on Tuesday, a third staff member's (C) IP address was using SSH to log into the firewall of a separate department, after several failed login events. Staff member C then opened "Wire Shark" on his computers network port to find a package. On Wednesday, staff member C found that his IP address had logged into a completely different departments' firewall. He determined that the login had occurred on Tuesday evening, and he made a record of the configuration changes. Staff member C then searched for the package he had found when he opened "Wire Shark" the previous day, but failed to find a record of any actions or activity.

The customer came to SANGFOR for help.

Assessment Summary

Overall Risk Rating



Threat Categories

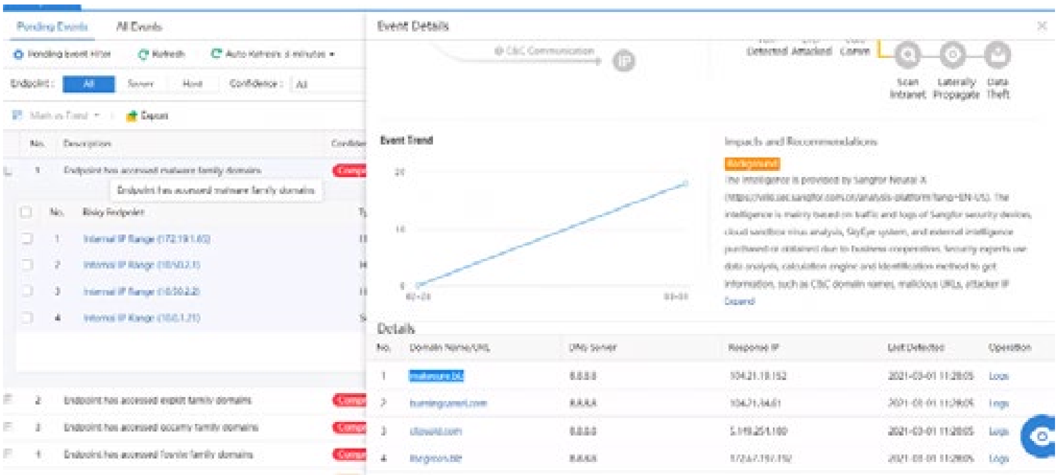
Total Threat Count: 10

Malware	Vulnerability	Attack	Intrusion Behavior	Potential Threat	Protocol
Count: 1	Count: 2	Count: 0	Count: 2	Count: 4	Count: 1

Forensic Investigation and Analysis--Security Events and Threats Analysis

1. Malware Event Analysis Malicious Domain Name Observed

A number of internal machines, servers, and PCs, were either accessed a malicious domain name or were infected by malware, ransomware, mining viruses, and trojan. A few malicious programs that were found were WannaMine, fosniw, expkit, occamy, and razy. There were a number of hosts that seemed to perform malicious domain name resolution and Command & Control communication as well.



No.	Description	Confidence
1	Endpoint has accessed malware family domains	Comp
2	Endpoint has accessed expkit family domains	Comp
3	Endpoint has accessed occamy family domains	Comp
4	Endpoint has accessed fosniw family domains	Comp

Endpoint has accessed malware family domains

No.	Risky Endpoint
1	Internal IP Range (172.19.1.60)
2	Internal IP Range (10.50.2.1)
3	Internal IP Range (10.50.2.2)
4	Internal IP Range (10.0.1.21)

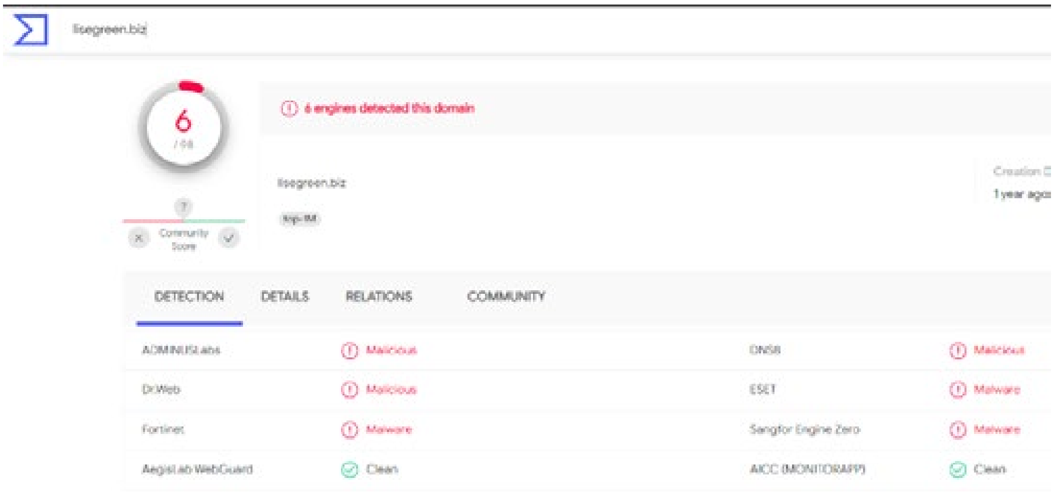
Impacts and Recommendations

Background

The intelligence is provided by Sangfor Neural-X (https://wiki.sec.sangfor.com.cn/analysis-platform?lang=EN-US). The intelligence is mainly based on traffic and logs of Sangfor security devices, cloud sandbox virus analysis, SkyEye system, and external intelligence purchased or obtained due to business cooperation. Security experts use data analysis, calculation engine and identification method to get information, such as C&C domain names, malicious URLs, attacker IP

Details

No.	Domain Name/URL	DNS Server	Response IP	Last Detected	Operation
1	malwaure.biz	8.8.8.8	104.21.18.152	2021-03-01 11:28:05	Logs
2	burningcamel.com	8.8.4.4	104.21.44.61	2021-03-01 11:28:05	Logs
3	ulbswid.com	8.8.8.8	5.119.251.100	2021-03-01 11:28:05	Logs
4	lisegreen.biz	8.8.4.4	172.67.197.192	2021-03-01 11:28:05	Logs



6 engines detected this domain

ADMINUSLabs	Malicious	DNS8	Malicious
Dr.Web	Malicious	ESET	Malware
Fortinet	Malware	Sangfor Engine Zero	Malware
AegisLab WebGuard	Clean	AICC (MONITORAPP)	Clean

Risk

Pre-Attack Phase

Internet Filtering:

There was insufficient Internet Access Management/proxy with the latest threat intelligence to block a users access to malicious websites.

Endpoint Protection:

There was insufficient endpoint protection, including antivirus software, to quarantine and block the executable malware files. Slow detection of such events often helps attackers create backdoor access or spread malware from machine to machine.

Monitoring System:

Implement security mechanisms or devices to monitor, detect, and block attacks before they take place.

Mid-Attack Phase

Command & Control:

The attacker may already have basic control over victim hosts with the help of a Trojan. Attackers instruct victim hosts to download malicious files, webshell hosted on the attacker's machine via vulnerabilities.

Once the Trojan or Webshell is downloaded and executed, the attacker has remote code execution on the victim host for further attacks including privilege escalation, and fully compromise the server.

Network Monitoring:

Ths customer needed security mechanisms or devices to monitor the web server traffic, ensuring the web server does not have any suspicious outgoing traffic to an unknown destination.

Monitoring Mechanism:

The customer lacked monitoring mechanisms with machine learning features, to detect abnormal traffic.

Data Exfiltration:

Compromised hosts continuously transmit sensitive information to attacker machines, leading to data leakage.

Recommendations

I. Run a full scan using Sangfor AntiBot and Sangfor Endpoint Secure, with the latest signatures, to identify and quarantine all malicious executable files.

II. Implement Sangfor IAG or proxy to block users from accessing non-work related or potentially malicious websites.

III. Implement a Next-Generation Application Firewall (NGAF), with WAF functions, IPS signatures, threat intelligence, and Command and Control (C&C) detection engines, to detect suspicious traffic early, and to block it before the next attack phase.

IV. Implement security mechanisms or devices to monitor, detect, and block attacks before any further attacks take place.

V. Implementation of exploit execution mechanisms is recommended. In the case of an attacker successfully installing malware, there should be a restriction that prevents the execution of unknown malware.

VI. Implementation of a gateway protection mechanism is recommended. A firewall should have the ability to identify and block malicious domains with either latest Threat Intelligence, or engines, to detect domains that utilize Domain Generation Algorithm (DGA).

2. Potential Threat Event Analysis

Inbound Port Scanning Behavior Observed:
The source IP addresses were performing scanning on the internal host, via TCP ports between 3252 and 3293.

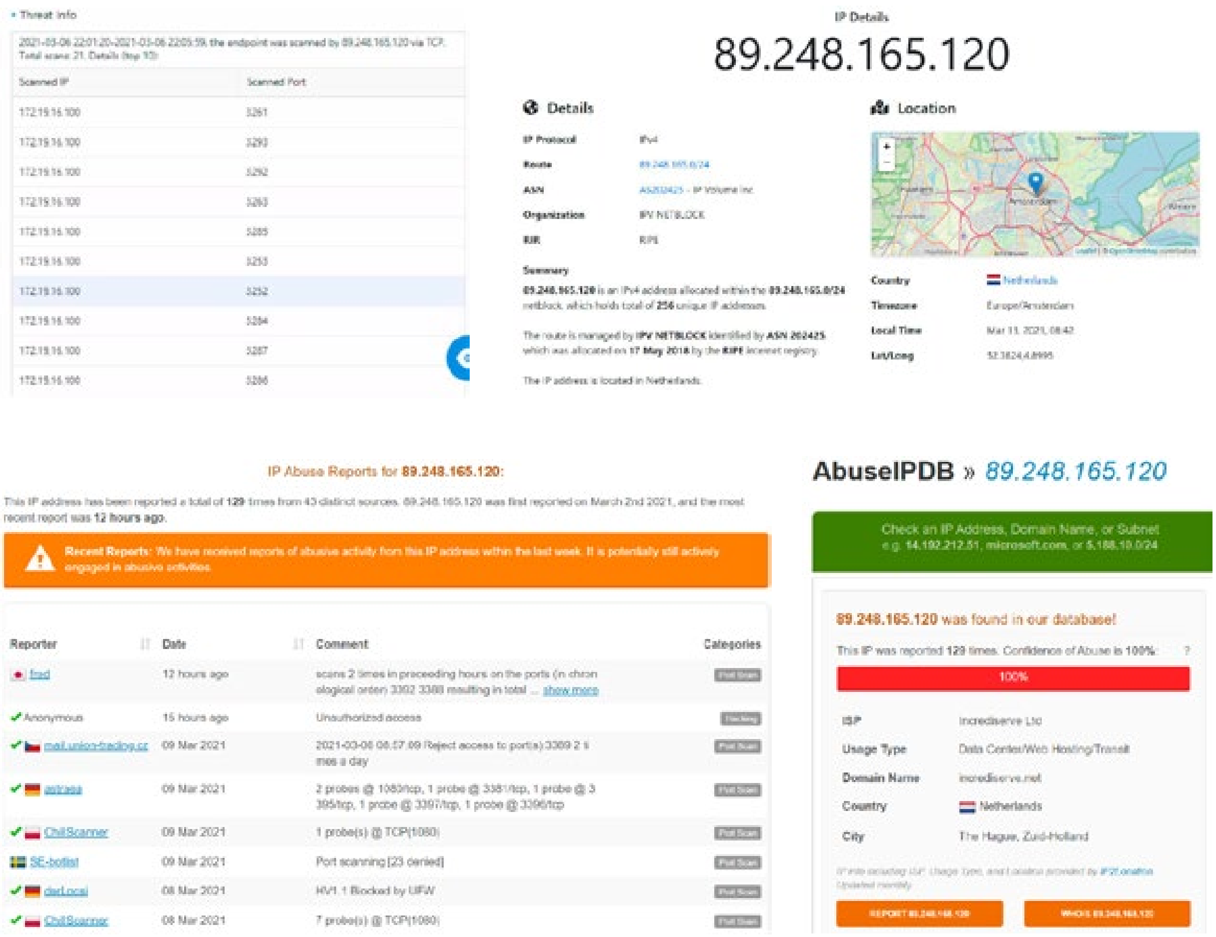
Description:
Scanning is a common pre-activity for an attacker. Hosts perform IP scanning on other hosts to locate live hosts, and then perform port scanning on these live hosts to find weaknesses. Should a vulnerability be discovered, the attackers exploit the vulnerability to gain access, compromise the host, and then continue to scan, exploit and compromise other hosts, in other segments.

Impact:

From the screenshot above, we can see source 89.248.165.120 is trying to perform port scanning on one of the internal hosts, to determine if the port or service is listening. It was also observed that most of the request packet is SYN packet only.

The host was found in the global blacklisted database, where it has a bad reputation for hacking and port scanning activities. The host was verified to have abnormal behavior in multiple regions.

Analysis:



• Threat info

2021-03-06 22:01:20-2021-03-06 22:05:59, the endpoint was scanned by 89.248.165.120 via TCP. Total scans: 21. Details (top 10):

Scanned IP	Scanned Port
172.19.16.100	3261
172.19.16.100	3293
172.19.16.100	3292
172.19.16.100	3263
172.19.16.100	3285
172.19.16.100	3253
172.19.16.100	3252
172.19.16.100	3284
172.19.16.100	3287
172.19.16.100	3286

IP Details

89.248.165.120

Details

IP Protocol	IPv4
Route	89.248.165.0/24
ASN	AS202425 - IP Volume inc
Organization	IPV NETBLOCK
RIR	RIPE

Summary

89.248.165.120 is an IPv4 address allocated within the **89.248.165.0/24** netblock, which holds total of **256** unique IP addresses.

The route is managed by **IPV NETBLOCK** identified by **ASN 202425**, which was allocated on **17 May 2018** by the **RIPE** internet registry.

The IP address is located in Netherlands.

Location

Country	Netherlands
Timezone	Europe/Amsterdam
Local Time	Mar 11, 2021, 08:42
Lat/Long	52.3824,4.8995

IP Abuse Reports for **89.248.165.120**:

This IP address has been reported a total of **129** times from 43 distinct sources. 89.248.165.120 was first reported on March 2nd 2021, and the most recent report was **12 hours ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
fnd	12 hours ago	scans 2 times in preceeding hours on the ports (in chron ological order) 3302 3388 resulting in total ... show more	Port Scan
✓ Anonymous	15 hours ago	Unauthorized access	Hacking
✓ mail.union-trading.cz	09 Mar 2021	2021-03-06 08:57:09 Reject access to port(s):3389 2 times a day	Port Scan
✓ antcasa	09 Mar 2021	2 probes @ 1080/tcp, 1 probe @ 3381/tcp, 1 probe @ 3395/tcp, 1 probe @ 3397/tcp, 1 probe @ 3396/tcp	Port Scan
✓ ChillScanner	09 Mar 2021	1 probe(s) @ TCP(1080)	Port Scan
SE-botlist	09 Mar 2021	Port scanning [23 denied]	Port Scan
✓ darLocal	08 Mar 2021	HV1.1 Blocked by UFW	Port Scan
✓ ChillScanner	08 Mar 2021	7 probe(s) @ TCP(1080)	Port Scan

AbuseIPDB » *89.248.165.120*

Check an IP Address, Domain Name, or Subnet
e.g. **14.192.212.51**, **microsoft.com**, or **5.188.10.0/24**

89.248.165.120 was found in our database!

This IP was reported **129** times. Confidence of Abuse is **100%**: ?

ISP	Incrediserve Ltd
Usage Type	Data Center/Web Hosting/Transit
Domain Name	incrediserve.net
Country	Netherlands
City	The Hague, Zuid-Holland

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly

Recommendation:

The customer perform an internal investigation and review. It is good to check the associated process from the command prompt and task manager. They further investigated to determine if the process was originating from internal software or potentially unwanted application (PUA), and its value. If the source machines belonged to the IT department, and the purpose of scanning was for business needs, such as vulnerability scanning activity, then the source machines needed to be properly controlled, audited, and limited to authorized personnel only. If the machines were infected by malicious software, and there were malicious processes and malicious scheduled tasks, Sangfor recommended installing an antivirus with the latest virus definitions, and to run a full scan on all the machines in the network.

This event exposed risks within the customer environment, including:

· Most machines in the network did not have antivirus installed
· Most machines in the network did not have the latest antivirus virus definition update s
· Potentially no or Improper firewall configuration on ingress and egress access, based on necessary ports

Long-Term Improvement Plan

As the cybersecurity world is a fast and dynamic environment, ensuring continuous protection means the customer ust consider their practices and methods of improvement to increase the overall security posture of the organization:

a) The Principle of Least Privilege encourages network segmentation and zero-trust networks, before performing any administrative tasks like addition, modification, or deletion of activities.

b) A defense in depth architecture approach should be implemented, as a single point of protection can no longer protect organizations from attack. Enforce stricter security protection on systems supporting critical business operations.

c) Improve the overall security baseline and security status of networks by comprehensively implementing security strengthening and hardening on every single asset in the organization.

d) Further strengthen APT attack detection, threat monitoring capabilities, daily security inspections, improving grade protection and risk assessment mechanisms, and regularly check and evaluate security reinforcements and protection to identify and eliminate risks in a timely manner.

e) Always introduce security into the Software Development Life Cycle (SDLC) and System Life Cycle (SLC) for all systems, both in-house or by a third-party providers, and document the results of each phase for later review and audit.

f) Perform security assessments like vulnerability scanning, penetration testing, and baseline configuration review, prior migration of new hosts, servers, systems, or applications into the production environment, and repeat on a regular basis.

g) Continuously strengthen the overall information security management system in the technical, management, and operational sectors of the organization. Of vital importance is education and development of security and risk awareness for all personnel, made easier by implementing internal policies, stricter rules, and tighter regulations.

h) Perform a risk assessment on both the internal and external organizational network, to evaluate and maintain proper security reinforcement and protection effects and to mitigate risks and threats in a timely manner.

i) Review and audit the operation of each host and application with the help of security event correlation products on a regular basis to maintain effective security controls.

j) Establish a patch monitoring and distribution mechanisms to ensure that server patches, hosts, firmware, and software are continuously updated, to avoid attacks designed to exploit vulnerabilities and bugs.

k) Always be aware of, and follow vendor and third-party best practices or hardening guidelines for applications, servers, and network security hardware appliances.

l) Implement a change management system and enforce a strict approval process for any administrative tasks done on production systems, and document all the changes for future audits.

m) The CIA triad of Confidentiality, Integrity, and Availability, together with other security controls like non-repudiation and authentication, are essential to understand, practice, and consider when tasked with protecting all organizational information.

Conclusions:

In order to prevent data loss due to human or technological error, please ensure all important data is backed-up prior to implementing any changes, like vulnerability patching or security hardening. It is recommended that the host be restarted after applying any fixes.

Sangfor provides other security analysis functions beyond those above, including:

- Security Gap Analysis
- Security Events and Threats Analysis
- Malicious Domain Name Observed
- Intrusion Behavior Event Analysis
- Web Application Brute Force Attack
- SMB Brute Force Attack
- Potential Threat Event Analysis
- Internal Port Scanning Behavior Observed
- Inbound Port Scanning Behavior Observed
- Outbound Port Scanning Behavior Observed
- Suspicious Email Delivery Observed
- Vulnerability Event Analysis
- Outdated Software Version in Use & Misconfigurations
- Weak Password Observed
- Protocol and Services Auditing
- Plain Text Protocol in Use Observed

Customer feedback

"Many thanks to Sangfor's help. During this incident, we know more about Sangfor's security ability and also Sangfor products and solutions. We trust this vendor and hope cooperate deeper in the future."

"When our engineers called Sangfor Hong Kong office on this issue, they responded immediately and carried their security products which stopped the threat quickly. Very happy to get help from Sangfor!"

SANGFOR

Make IT Simpler, More Secure and Valuable!

www.sangfor.com