SANGFOR

Security Report

Period: 2019-03-19 to 2019-03-25

Generated At: 2019-03-26 22:42:00

Application Server Domain/IP: All

User: All

Security Summary

Summary

Period: 2019-03-19 to 2019-03-25

Before Protection: **Poor**

Overall Security Status

Turn On
NGAF Protection

After Protection: **Excellent**

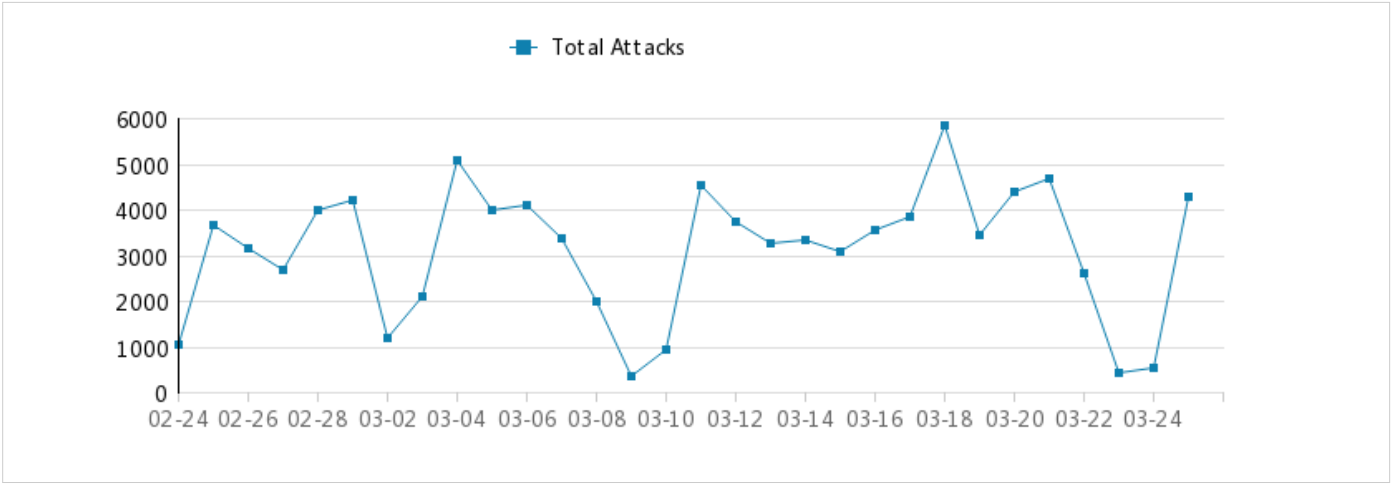
Overall Security Status After Protection

With Sangfor NGAF's protection, overall security rating is raised to **Excellent.**
Without protection, it may suffer the following attacks:

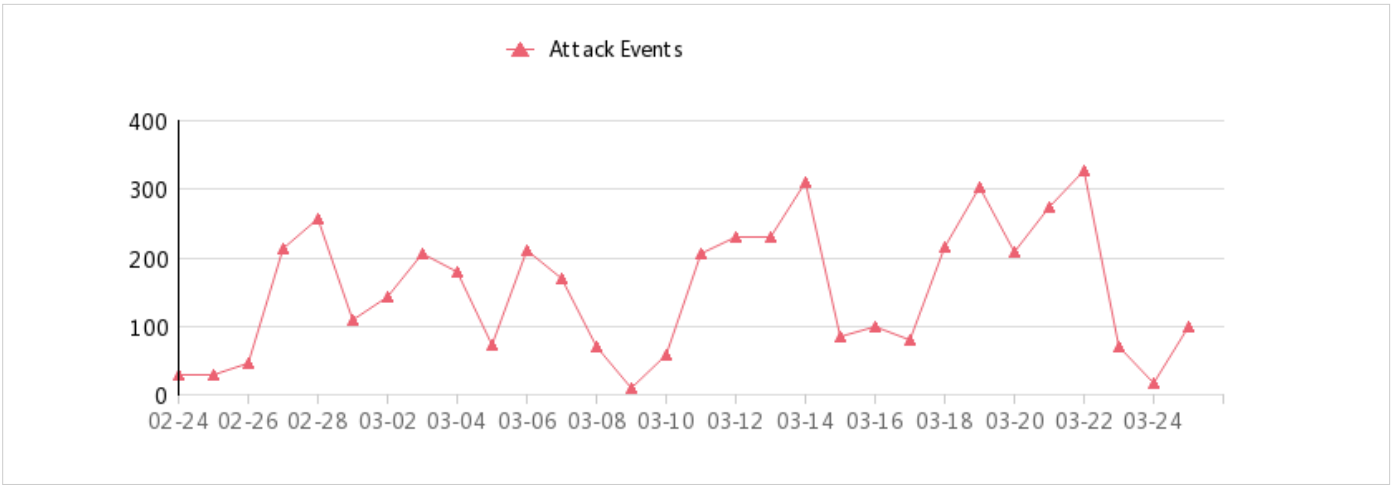
Risk	103.91.205.24,103.91.205.122,103.91.205.152 server(626) has been Ever been attacked 192.168.7.10,192.168.100.63,192.168.101.12 host(138) has been Infected	**Recommendations:** Follow the security enhancement recommendations in the corresponding server security or endpoint security sections to fix the issues as soon as possible for fear of business losses.
Attack	20430 attack(s) occurred	**Comments:** Overall security rating is Poor, though most of the attacks are blocked by Sangfor NGAF.
Vuln	No vulnerability has been detected.	**Comments:** None

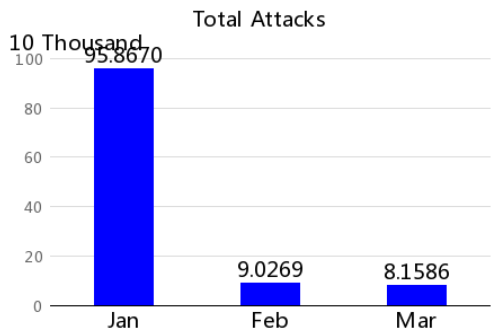
Trends

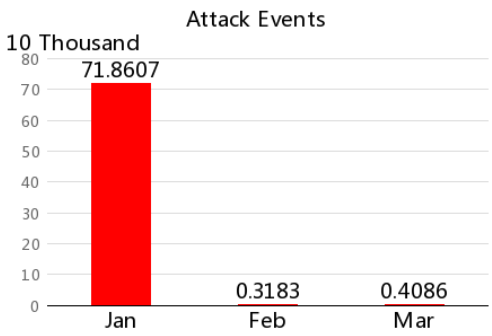
Total Attacks: Indicates the total number of attacks detected by the Sangfor NGAF that are against protected zones. The more the attacks, the worse the network security.



Attack Events: Indicates the major attack events extracted and categorized based on a variety of security logs and attack chain analysis techniques. The more the attack events, the more the attacks. The servers in protected zone will be more likely attacked, and network security will become worse.







As number of attacks increases, network security level goes down accordingly. The more the attack events, the more the attacks. Likewise, the more the vulnerabilities, the more the intrusions.

Vulnerability Distribution

No data available

Application Server Security

The following are the top attacked servers:

No.	Fixed	Target Server	Application Server	Severity (Level)	Latest Threat	Threat Count
1	No	103.91.205.24	-	Ever been attacked(3)	2019-03-23 15:51:09	19
2	No	103.91.205.122	-	Ever been attacked(3)	2019-03-23 15:55:22	19
3	No	103.91.205.152	-	Ever been attacked(3)	2019-03-23 15:56:50	19
4	No	103.91.205.173	-	Ever been attacked(3)	2019-03-23 15:57:34	18
5	No	103.91.205.253	-	Ever been attacked(3)	2019-03-23 16:01:52	18
6	No	103.91.205.183	-	Ever been attacked(3)	2019-03-23 15:58:14	18
7	No	103.91.205.170	-	Ever been attacked(3)	2019-03-23 15:57:28	18
8	No	103.91.205.228	-	Ever been attacked(3)	2019-03-23 16:00:30	17
9	No	203.150.103.55	-	Ever been attacked(3)	2019-03-25 13:09:15	15
10	No	203.150.103.93	-	Ever been attacked(3)	2019-03-25 13:10:12	15

Server Risk Distribution

Attack Events

The following are the major attack events categorized and extracted according to analysis of security logs, in conjunction with attack chain analysis techniques.

- Hacked (server has been infected with Trojan or defaced)
- Bot Controlled (host or server has become "zombie")
- Ever been attacked (server has ever been attacked, but no data proves that any attack is successful)

No.	Event Category	Details
1	Hacked	No data available
2	Bot Controlled	No data available

3	Ever been attacked	1) 103.91.205.24 has suffered 19 attack(s), which fall into the following major types: system Vulnerability. Attack sources: 192.168.11.5(Internal IP) 5 occurrence(s), 192.168.7.3(Internal IP) 5 occurrence(s), 192.168.11.22(Internal IP) 4 occurrence(s) 2) 103.91.205.122 has suffered 19 attack(s), which fall into the following major types: system Vulnerability. Attack sources: 192.168.11.5(Internal IP) 5 occurrence(s), 192.168.7.3(Internal IP) 5 occurrence(s), 192.168.11.22(Internal IP) 4 occurrence(s) 3) 103.91.205.152 has suffered 19 attack(s), which fall into the following major types: system Vulnerability. Attack sources: 192.168.11.5(Internal IP) 5 occurrence(s), 192.168.7.3(Internal IP) 5 occurrence(s), 192.168.11.22(Internal IP) 4 occurrence(s)

All Attack Sources

The following are the attack sources that have launched the most attacks against the server. We are recommended to log in to the NGAF GUI and add those attack sources into the Global Blacklist in Policies > Blacklist/Whitelist.

No.	IP Address	Attack Type	Attack Count	Location
1	192.168.11.5	system Vulnerability (341)	341	Internal IP
2	192.168.11.7	system Vulnerability (179)	179	Internal IP
3	192.168.103.62	system Vulnerability (156)	156	Internal IP
4	192.168.11.12	system Vulnerability (123)	123	Internal IP
5	192.168.11.3	system Vulnerability (70)	70	Internal IP
6	192.168.3.41	system Vulnerability (67)	67	Internal IP
7	192.168.103.141	system Vulnerability (67)	67	Internal IP
8	192.168.103.25	system Vulnerability (62)	62	Internal IP
9	192.168.7.3	system Vulnerability (61)	61	Internal IP
10	192.168.11.2	system Vulnerability (58)	58	Internal IP

Endpoint Security

Top Bot-Infected Hosts

The following are the top bot-infected hosts:

No.	Fixed	Host	Zone	Severity (Level)	Latest Threat	Threat Count
1	No	192.168.7.10	LAN@SCPHC-B1	Infected(8)	2019-03-25 16:08:50	3376
2	No	192.168.100.63	WIFI@SCPHC	Infected(8)	2019-03-22 02:01:53	1272
3	No	192.168.101.12	WIFI@SCPHC	Infected(8)	2019-03-21 23:59:13	1242
4	No	192.168.11.13	LAN@SCPHC-B8	Infected(8)	2019-03-25 17:21:37	1220
5	No	192.168.102.137	WIFI@SCPHC	Infected(8)	2019-03-21 01:35:29	957
6	No	192.168.11.12	-	Infected(8)	2019-03-25 17:21:39	833
7	No	192.168.11.15	LAN@SCPHC-B8	Infected(8)	2019-03-20 17:09:09	660
8	No	192.168.3.21	WIFI@PERSON	Infected(8)	2019-03-21 02:09:33	574

9	No	192.168.103.141	WIFI@SCPHC	Infected(8)	2019-03-25 15:07:23	486
10	No	192.168.102.8	WIFI@SCPHC	Infected(8)	2019-03-21 22:56:45	484

Recommendations: Download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

Malicious Files

The following are the top malicious files detected based on sandbox technology that involved in 0-Day vulnerability exploit:

No.	File MD5	Virus Name	Threat Level	Host	Infected Hosts	Threat Count	Latest Threat

No data available

Malicious Websites

The following are the top malicious websites detected based on sandbox technology that have involved in 0-Day vulnerability exploit:

No.	Website	Category	Host	Hosts	Threat Count	Latest Threat
1	cobalten.com/apu.php	Malicious webpage	192.168.103.26 (1) 192.168.102.190 (1)	2	2	2019-03-24 22:49:20
2	www.ladyissue.com/wp-includes/js/wp-emoji-release.min.js	Malicious webpage	192.168.100.196 (2)	1	2	2019-03-22 09:33:26
3	www.ladyissue.com/wp-includes/js/jquery/jquery-migrate.min.js	Malicious webpage	192.168.100.196 (1)	1	1	2019-03-22 09:28:20

Overall Security Enhancement Recommendations

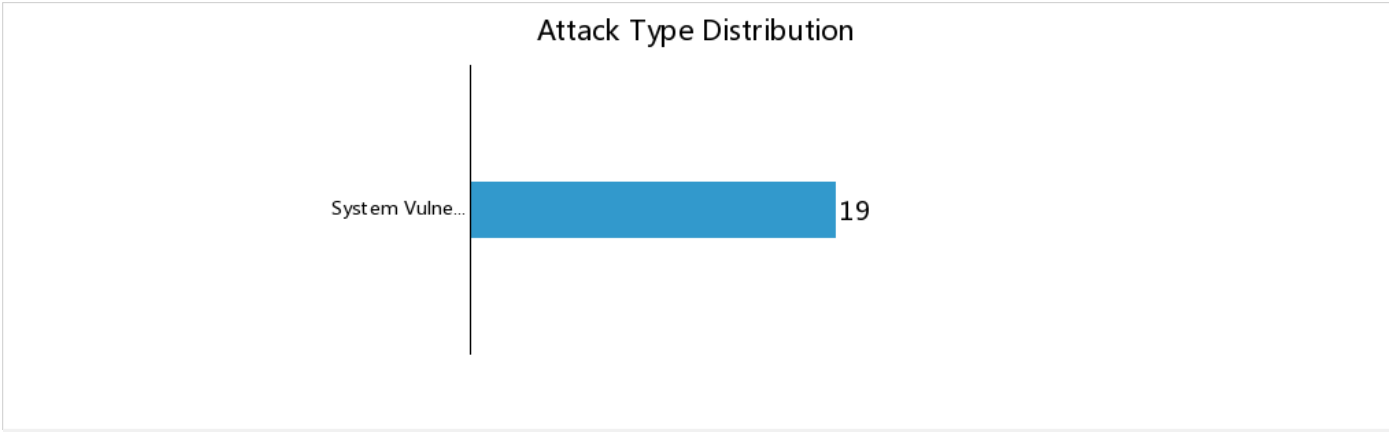
1. Log in to the NGAF GUI and follow the recommendations in Security Operations tab to fix the vulnerabilities.
2. Log in to the NGAF GUI and go to Status > Business System Security > Realtime Vulnerability Analytics to generate the report and follow the recommendations to fix the existing vulnerabilities.
3. Add the attack sources to Global Blacklist in Policies > Blacklist/Whitelist.
4. Carefully read all the Security Enhancement Recommendations in every Security Detail section in this report.

Server Security

103.91.205.24 Security Details (To be Fixed)

103.91.205.24 overall security rating is **High** (Ever been attacked)

103.91.205.24 suffered 19 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.24 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 09:56:35 End Time: 2019-03-22 11:08:04 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.24 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 13:52:30 End Time: 2019-03-22 15:01:24 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.24 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 13:55:50 End Time: 2019-03-20 14:35:10 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.24, 19 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (3)	Internal IP	3
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

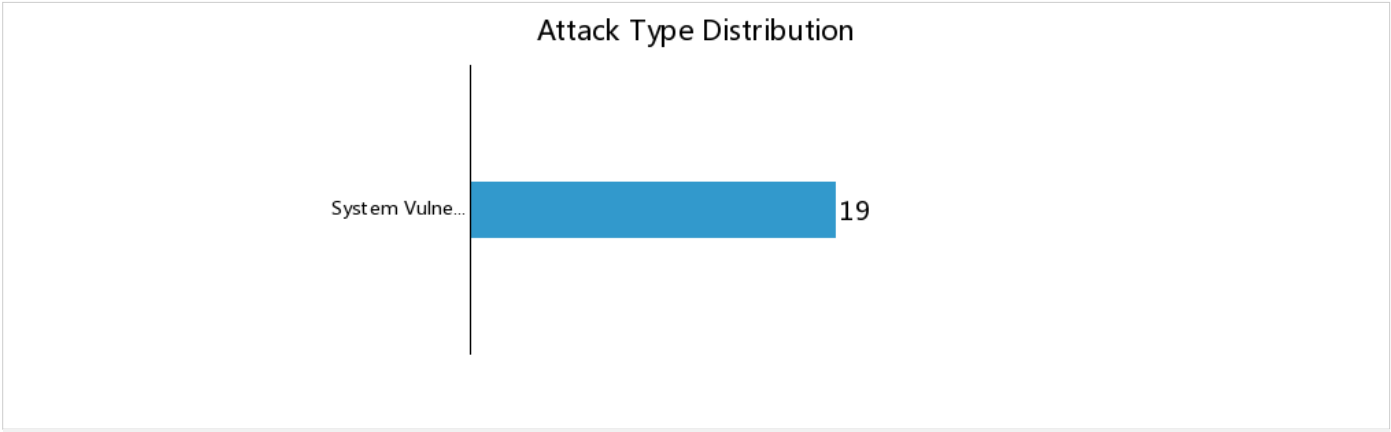
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.122 Security Details (To be Fixed)

103.91.205.122 overall security rating is High (Ever been attacked)

103.91.205.122 suffered 19 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.122 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:00:28 End Time: 2019-03-22 11:11:58 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.122 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 13:56:22 End Time: 2019-03-22 15:05:19 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.122 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 13:59:36 End Time: 2019-03-20 14:38:55 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.122, 19 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (3)	Internal IP	3
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

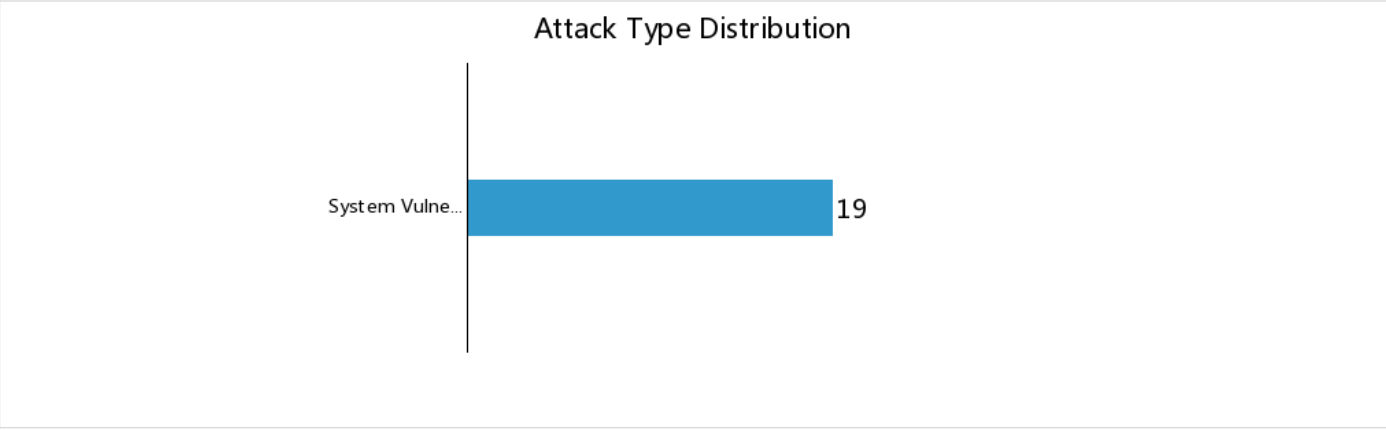
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.152 Security Details (To be Fixed)

103.91.205.152 overall security rating is High (Ever been attacked)

103.91.205.152 suffered 19 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.152 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:01:59 End Time: 2019-03-22 11:13:27 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.152 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 13:57:51 End Time: 2019-03-22 15:06:47 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.152 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 14:00:59 End Time: 2019-03-20 14:40:19 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.152, 19 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (3)	Internal IP	3
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

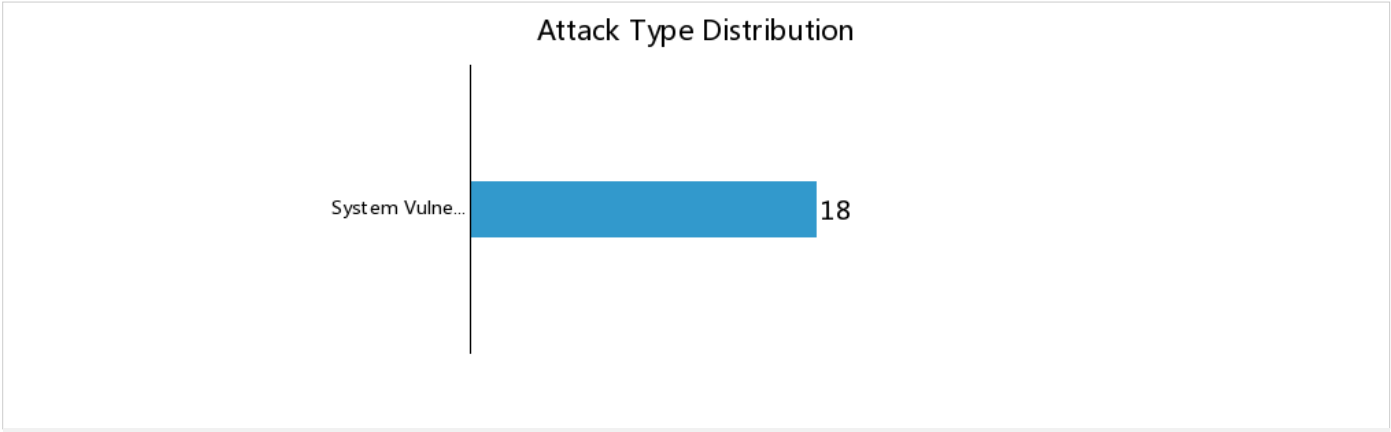
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.173 Security Details (To be Fixed)

103.91.205.173 overall security rating is High (Ever been attacked)

103.91.205.173 suffered 18 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.173 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:02:42 End Time: 2019-03-22 11:14:11 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.173 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)

Details	Start Time: 2019-03-22 13:58:33 End Time: 2019-03-22 15:07:30 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.173 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 14:01:40 End Time: 2019-03-20 14:40:59 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.173, 18 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (2)	Internal IP	2
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

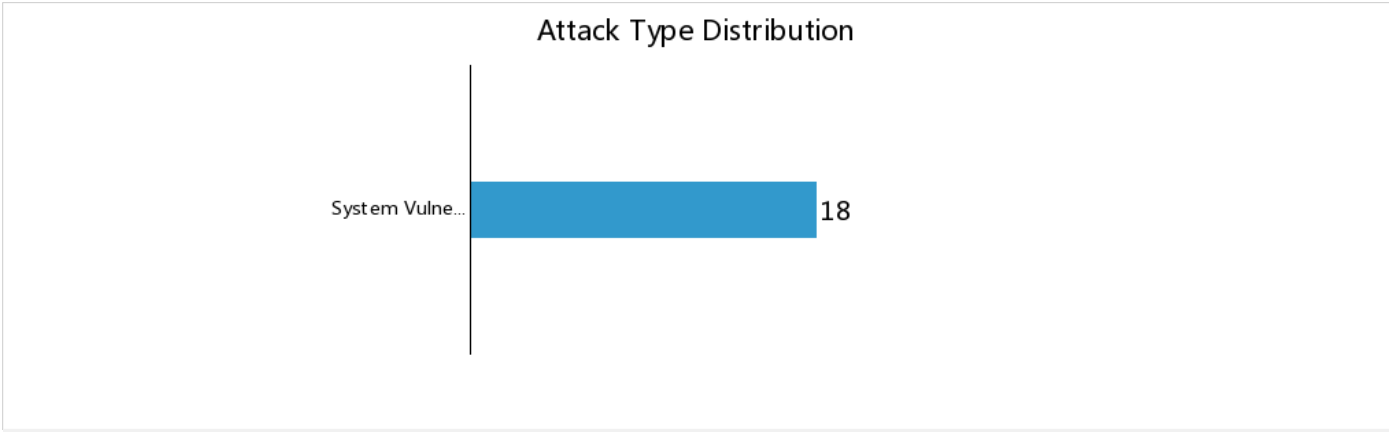
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.253 Security Details (To be Fixed)

103.91.205.253 overall security rating is High (Ever been attacked)

103.91.205.253 suffered 18 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.253 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:07:05 End Time: 2019-03-22 11:18:32 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.253 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 14:02:51 End Time: 2019-03-22 15:11:48 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.253 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 14:05:50 End Time: 2019-03-20 14:45:13 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.253, 18 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (2)	Internal IP	2
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

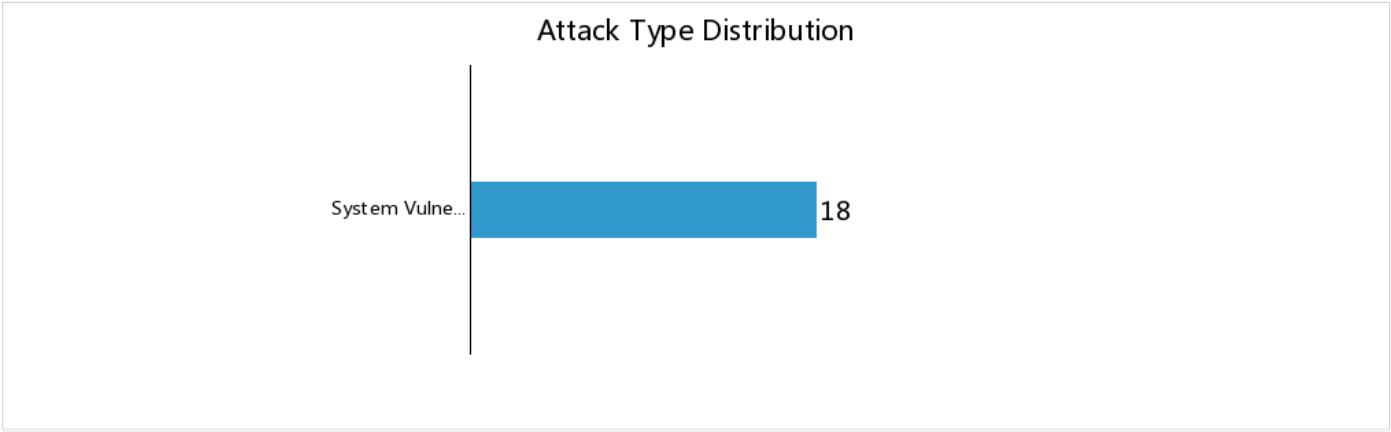
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.183 Security Details (To be Fixed)

103.91.205.183 overall security rating is High (Ever been attacked)

103.91.205.183 suffered 18 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.183 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:03:23 End Time: 2019-03-22 11:14:51 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.183 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 13:59:13 End Time: 2019-03-22 15:08:10 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.183 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 14:02:20 End Time: 2019-03-20 14:41:41 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.183, 18 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (2)	Internal IP	2
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

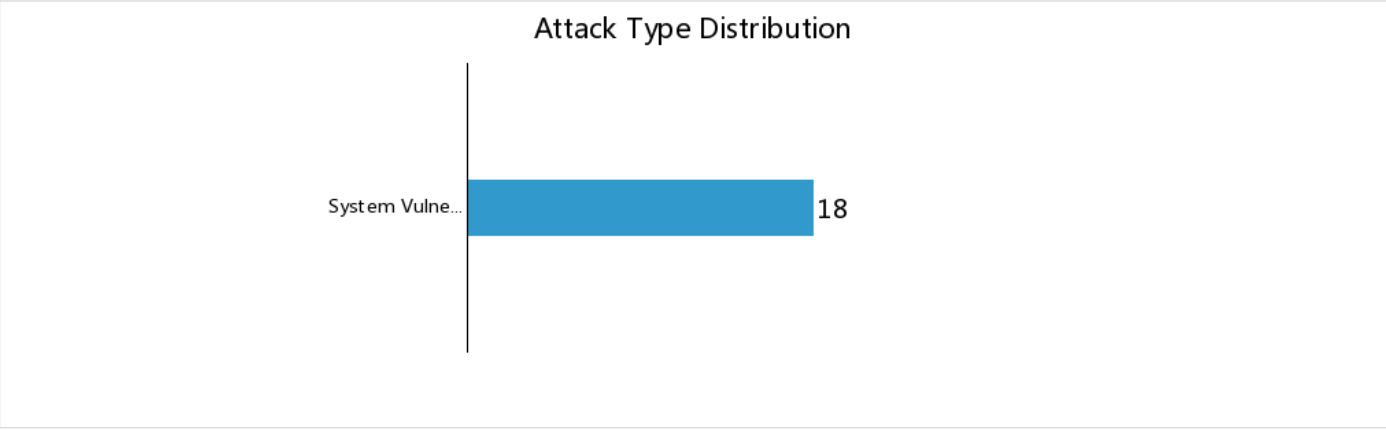
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.170 Security Details (To be Fixed)

103.91.205.170 overall security rating is High (Ever been attacked)

103.91.205.170 suffered 18 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.170 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:02:37 End Time: 2019-03-22 11:14:06 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.170 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 13:58:28 End Time: 2019-03-22 15:07:25 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.170 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 14:01:34 End Time: 2019-03-20 14:40:54 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.170, 18 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (2)	Internal IP	2
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

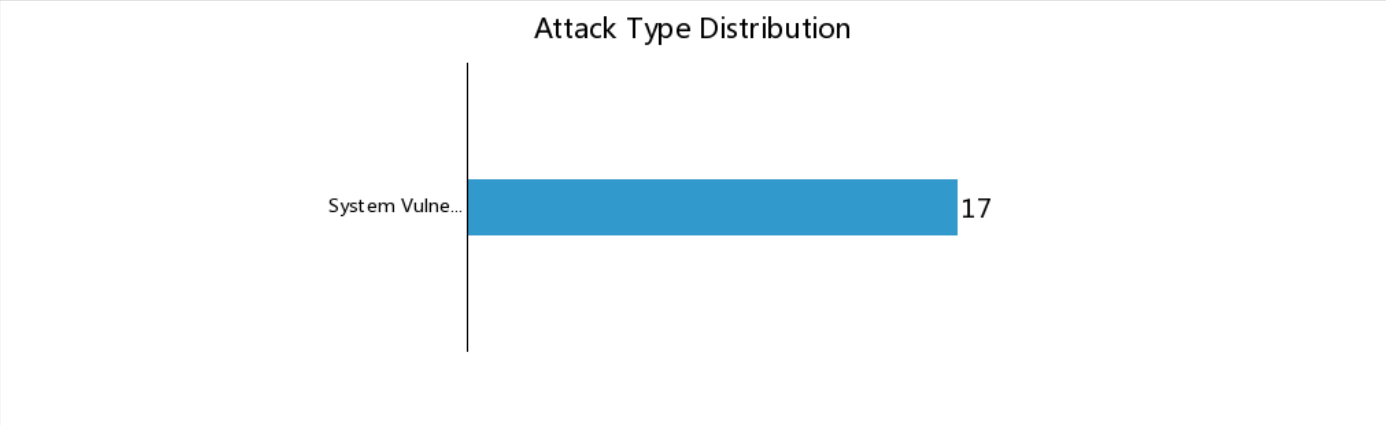
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

103.91.205.228 Security Details (To be Fixed)

103.91.205.228 overall security rating is High (Ever been attacked)

103.91.205.228 suffered 17 attack(s)



Attack Events

Category	Ever been attacked
Summary	103.91.205.228 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-22 10:05:43 End Time: 2019-03-22 11:17:10 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.228 has been attacked by 192.168.7.3(Internal IP, 5 occurrences), system Vulnerability(5)

Details	Start Time: 2019-03-22 14:01:30 End Time: 2019-03-22 15:10:27 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	103.91.205.228 has been attacked by 192.168.11.22(Internal IP, 4 occurrences), system Vulnerability(4)
Details	Start Time: 2019-03-20 14:04:35 End Time: 2019-03-20 14:43:58 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 103.91.205.228, 17 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.7.3	system Vulnerability (5)	Internal IP	5
3	192.168.11.22	system Vulnerability (4)	Internal IP	4
4	192.168.100.38	system Vulnerability (2)	Internal IP	2
5	192.168.11.2	system Vulnerability (1)	Internal IP	1

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

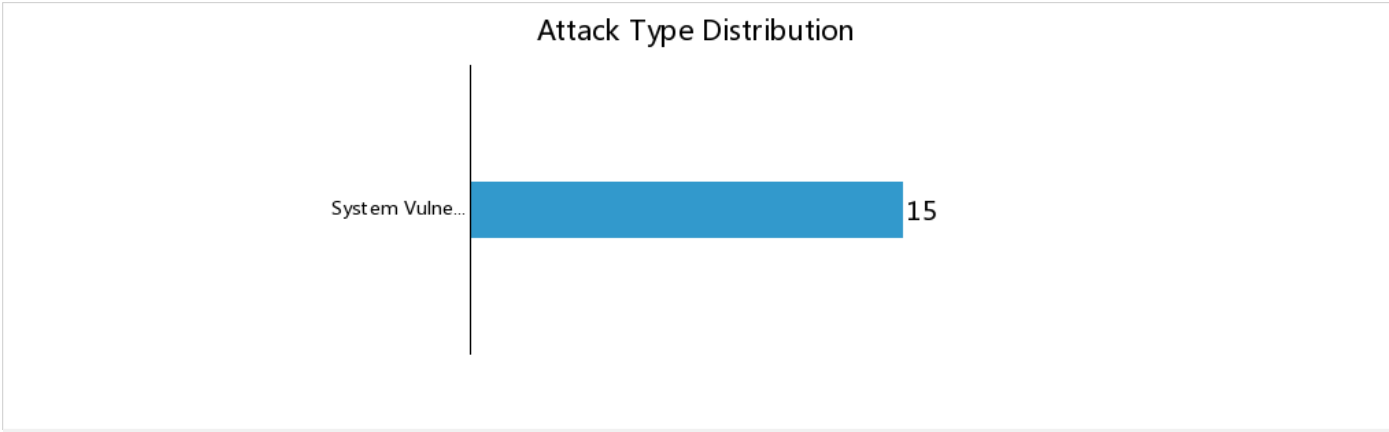
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

203.150.103.55 Security Details (To be Fixed)

203.150.103.55 overall security rating is High (Ever been attacked)

203.150.103.55 suffered 15 attack(s)



Attack Events

Category	Ever been attacked
Summary	203.150.103.55 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-19 12:29:08 End Time: 2019-03-19 16:19:22 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	203.150.103.55 has been attacked by 192.168.103.95(Internal IP, 2 occurrences), system Vulnerability(2)
Details	Start Time: 2019-03-25 12:49:07 End Time: 2019-03-25 13:09:15 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	203.150.103.55 has been attacked by 192.168.103.62(Internal IP, 2 occurrences), system Vulnerability(2)
Details	Start Time: 2019-03-22 10:59:18 End Time: 2019-03-22 14:18:57 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 203.150.103.55, 15 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.103.62	system Vulnerability (2)	Internal IP	2
3	192.168.11.7	system Vulnerability (2)	Internal IP	2
4	192.168.103.95	system Vulnerability (2)	Internal IP	2
5	192.168.11.12	system Vulnerability (2)	Internal IP	2

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

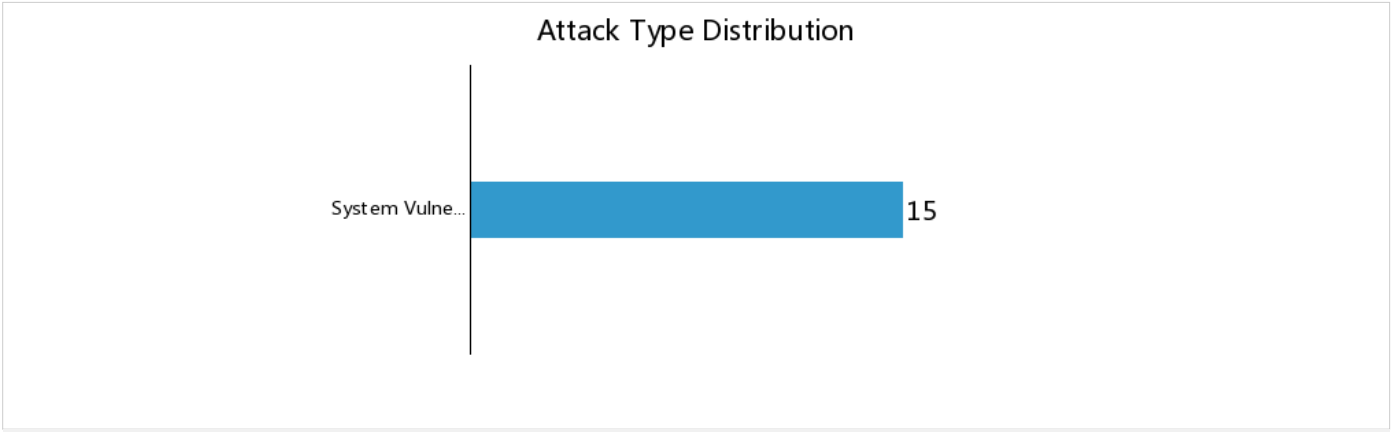
3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

203.150.103.93 Security Details (To be Fixed)

203.150.103.93 overall security rating is High (Ever been attacked)

203.150.103.93 suffered 15 attack(s)



Attack Events

Category	Ever been attacked
Summary	203.150.103.93 has been attacked by 192.168.11.5(Internal IP, 5 occurrences), system Vulnerability(5)
Details	Start Time: 2019-03-19 12:30:04 End Time: 2019-03-19 16:20:18 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	203.150.103.93 has been attacked by 192.168.103.95(Internal IP, 2 occurrences), system Vulnerability(2)
Details	Start Time: 2019-03-25 12:50:03 End Time: 2019-03-25 13:10:12 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Category	Ever been attacked
Summary	203.150.103.93 has been attacked by 192.168.103.62(Internal IP, 2 occurrences), system Vulnerability(2)
Details	Start Time: 2019-03-22 11:00:15 End Time: 2019-03-22 14:19:55 More logs are available in Internal Report Center, in Logs > WAF and Intrusion Prevention.

Vulnerabilities

No data available

Attack Sources

The following are the major sources launched attacks against 203.150.103.93, 15 attack(s) in total. We are recommended to add them into the Global Blacklist in Policies > Global Whitelist/Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.168.11.5	system Vulnerability (5)	Internal IP	5
2	192.168.103.62	system Vulnerability (2)	Internal IP	2
3	192.168.11.7	system Vulnerability (2)	Internal IP	2
4	192.168.103.95	system Vulnerability (2)	Internal IP	2
5	192.168.11.12	system Vulnerability (2)	Internal IP	2

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Fixed) in Status > Business System Security > Summary.

2. Ever been attacked

- All the attacks against the server have been blocked by Sangfor NGAF and the existing vulnerabilities have been fixed. No more action is required.

3. Blacklist Attack Sources

- To prevent subsequent attacks from the above sources, log in to the NGAF GUI and add the above IP addresses into global blacklist in Policies > Global Whitelist/Blacklist.

Endpoint Security

192.168.7.10 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.7.10 has undergone 3376 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-22 16:40:12 Host 192.168.7.10 accessed C&C address: devicesta.ru/gate02.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (5 occurrence(s))

Event Category	Bots Propagation
Details	Host is suspicious of scanning IP addresses.
Description	2019-03-21 16:31:03 Host 192.168.7.10 is initiating IP scanning (5 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.100.63 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.100.63 has undergone 1272 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-22 02:00:43 Host 192.168.100.63 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-22 02:00:42 Host 192.168.100.63 accessed C&C address: disorderstatus.ru/order.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.101.12 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.101.12 has undergone 1242 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-21 23:59:13 Host 192.168.101.12 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-21 23:59:12 Host 192.168.101.12 accessed C&C address: disorderstatus.ru/order.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2019-03-21 13:59:08 Try to communicate with C&C server disorderstatus.ru/order.php on botnet. (24 occurrence(s)) 2019-03-21 13:56:07 Sangfor security engine detected that gvaq70s7he.ru accessed by host is probably a C&C address of malware. The host may have been attacked by virus. (10 occurrence(s)) 2019-03-21 13:55:05 Try to communicate with C&C server differentia.ru/diff.php on botnet. (14 occurrence(s)) 2019-03-21 13:08:28 Sangfor security engine detected that disorderstatus.ru accessed by host is probably a C&C address of malware. The host may have been attacked by virus. (1 occurrence(s)) 2019-03-21 13:08:28 Sangfor security engine detected that differentia.ru accessed by host is probably a C&C address of malware. The host may have been attacked by virus. (1 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.11.13 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.11.13 has undergone 1220 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-25 17:16:32 Host 192.168.11.13 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s)) 2019-03-25 17:16:31 Host 192.168.11.13 accessed C&C address: atomictrivia.ru/atomic.p-hp, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s))

Event Category	Bots Propagation
Details	Host is suspicious of scanning IP addresses.
Description	2019-03-20 14:16:07 Host 192.168.11.13 is initiating IP scanning (5 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.102.137 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.102.137 has undergone 957 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-21 01:35:29 Host 192.168.102.137 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-21 01:35:28 Host 192.168.102.137 accessed C&C address: disorderstatus.ru/order.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.11.12 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.11.12 has undergone 833 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.

Description	2019-03-25 17:21:39 Host 192.168.11.12 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-25 17:21:35 Host 192.168.11.12 accessed C&C address: disorderstatus.ru/order.-php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Event Category	Bots Propagation
Details	Host is suspicious of scanning IP addresses.
Description	2019-03-25 14:45:27 Host 192.168.11.12 is initiating IP scanning (3 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.11.15 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.11.15 has undergone 660 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-20 17:04:04 Host 192.168.11.15 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-20 17:04:04 Host 192.168.11.15 accessed C&C address: atomictrivia.ru/atomic.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.3.21 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.3.21 has undergone 574 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-21 02:09:33 Host 192.168.3.21 accessed C&C address: atomictrivia.ru/atomic.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-21 02:09:33 Host 192.168.3.21 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Event Category	C&C Communication
Details	Host visited Conficker worm C&C domain.
Description	2019-03-20 21:55:07 Having ever attempted to parse address of the C&C server(1:idepg-zezctmpiv.com, 2:cbcrmnejanclkron.com, 3:nqvehstadkpij.com, 4:zenqxmrqdyfaxah.com, 5:dilo-fwfgxivcd.com, 6:apaferixezatsfej.com, 7:enmrglsjsxub.com, 8:kbofalurmzwp.com, 9:tknqvubcp-idcfsl.co... (2 occurrence(s)) 2019-03-20 21:50:53 Having ever attempted to parse address of the C&C server(1:mhqt-kjslsluhynwzqj.com, 2:cpwfgxqrifqr.com, 3:insxahofiviz.com, 4:jgpozyfkfolodyh.com, 5:qjohkfw-zsdwxsfmj.com, 6:pazexinergbubkfgf.com, 7:upcfsvshibsj.com, 8:uhehwrkzybqnmvkp.com, 9:tc-topedklev... (1 occurrence(s)) 2019-03-20 21:49:10 Having ever attempted to parse address of the C&C server(1:tybqv-cjopadm.com, 2:xgbcfgnmdipux.com, 3:dulkvmxmfsjct.com, 4:nkpgfknmtujqt.com, 5:oxufidkvk-zetkhqfev.com, 6:wtermrszavsbuj.com, 7:jqxyfulkbylaz.com, 8:nknyxsnifuxoh.com, 9:rurqjqtapg-tyfafoz.co... (1 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.103.141 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.103.141 has undergone 486 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Event Category	Bots Propagation
Details	Host is suspicious of scanning IP addresses.
Description	2019-03-21 15:22:07 Host 192.168.103.141 is initiating IP scanning (1 occurrence(s))

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

192.168.102.8 Security Details (To be Fixed)

Overall security rating: **Critical** (Infected)

192.168.102.8 has undergone 484 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-03-21 22:56:45 Host 192.168.102.8 accessed C&C address: differentia.ru/diff.php, which is proved by virustotal. Host may be infected with virus botnet.malware. (3 occurrence(s)) 2019-03-21 22:56:44 Host 192.168.102.8 accessed C&C address: disorderstatus.ru/order.-php, which is proved by virustotal. Host may be infected with virus botnet.malware. (2 occurrence(s))

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

Security Enhancement Recommendations

1. To be Fixed

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Fixed) in Status > User Security > Summary.

2. Infected

- The host is infected with malware. We are recommended to download anti-malware software to scan for and remove malware on the infected hosts. (Download Anti-malware Software: http://sec.sangfor.com/apt)

Risk Assessment & Impacts

Risk Assessment

Server security is based on comprehensive analysis of all the security logs related to the internal servers in protected zones. Server security rating falls into four types, namely, Hacked, Ever been attacked, Data ever been harvested and Vulnerable. Endpoint security is based on comprehensive analysis of all network security logs related to all the hosts in protected zones, and rating also falls into four types, namely, Infected, High, Medium and Low.Overall security is assessed according to server security and endpoint security, and the rating falls into the following:

Overall security rating **Poor**:

- This indicates that severity of at least one server is rated **Critical**(hacked), or severity of at least one host is rated **Critical**(infected with malware).

Overall security rating **Fair**:

- This indicates that severity of at least one server is rated **High**(ever been attacked), or severity of at least one host is rated **High**(most likely infected with malware).
- This indicates that severity of at least one server is rated **Medium**(data ever been harvested), or severity of at least one host is rated **Medium**(likely infected with malware).

Overall security rating **Good**:

- This indicates that severity of at least one server is rated **Low**(vulnerable), or severity of at least one host is rated **Low**(less likely infected with malware).

Overall security rating **Excellent**:

- This indicates that no server is vulnerable or has been attacked, or no host is likely infected with malware.

Impacts

WebShell Backdoor

By exploiting vulnerabilities on a Web server, the hacker has uploaded WebShell file into the Web system, which may be accessed by the hacker to perform unauthorized operations and manipulate the Web system in the long run.

Read more: https://en.wikipedia.org/wiki/Backdoor_Shell

Solution:

- Download anti-malware software, scan for and remove the potential WebShell or viruses on the server (-Download Anti-Malware software: http://sec.sangfor.com/apt)
- Configure a corresponding web application protection rule and set Action to Deny.

WebShell File Access

By exploiting vulnerabilities on a Web server, the hacker has uploaded WebShell file into the Web system and has successfully accessed the WebShell file to perform unauthorized operations and manipulate the Web system.

Solution:

- Download, install and launch anti-malware software to scan websites for and remove the WebShell file. (Download Anti-malware Software: http://sec.sangfor.com/apt)
- Configure and enable Web application protection rule and set Action to Deny.

Bot Controlled

Once a host is infected with worm, virus or Trojan, the host could be remotely controlled by the attacker who may launch a variety of attacks(DoS, APT, etc.), aiming to destroy customer's network or crucial application system and steal confidential data.

Read more: https://en.wikipedia.org/wiki/Botnet

Solution:

- Download anti-malware software to scan for and remove malware on the infected host. (Download Anti-malware Software: http://sec.sangfor.com/apt)

Ever been attacked

The attacker employs advanced techniques to initiate intrusions and attacks against a specific enterprise network, with the purpose of stealing cooperate data. This type of attack is often more hidden, organized and persistent, after long-term planning and operating. Since the attacker is very good at hiding, data theft may turn to cyber spying eventually.

- SQL Injection: The attacker makes use of the vulnerability on database and steal data from it, causing data and account leaks.
- Brute-force Attack: The attacker uses tools to perform brute-force attacks against the servers that are with password-based authentication enabled. After attack success, the attacker can execute arbitrary command through that server.
- XSS Attack: The attacker makes use of the vulnerability to execute command, obtain system running information, create new system user account and enable remote control to control the web server.

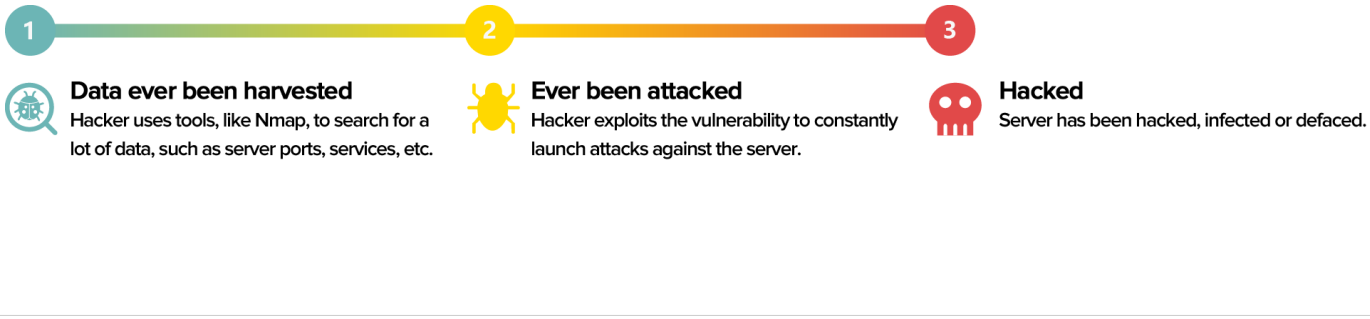
Read more: https://en.wikipedia.org/wiki/SQL_injection

Solution:

- Configure a corresponding web application protection rule and set Action to Deny.
- Configure a corresponding Intrusion Prevention rule and set action to Deny.

Server Security Ratings

- Stages of Attack

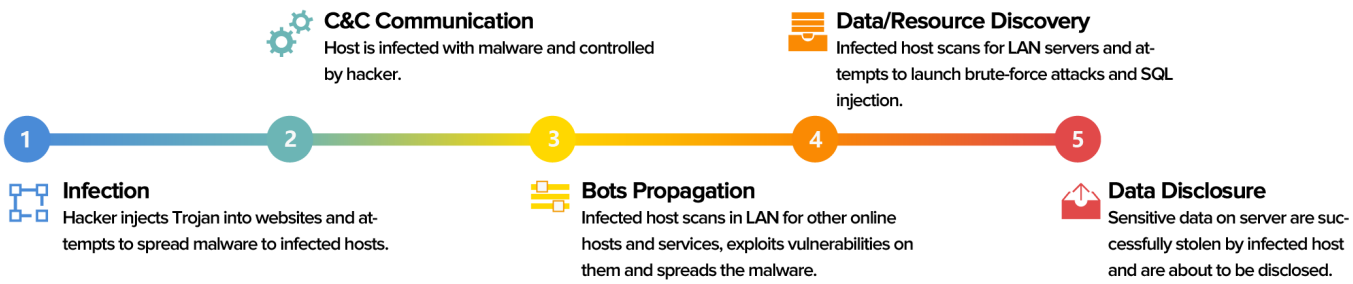


- Severity Ratings

No.	Severity	Description	Level
1	**Hacked**	Server has been hacked with WebShell or backlink, etc.	5
2	**Ever been attacked**	No data proves that server has been hacked, but some logs show that intrusions have ever occurred, such as SQL injection, brute-force login, WebShell Upload, etc.	3-4
3	**Data ever been harvested**	No data proves that server has been hacked, but there is proof that data have been harvested.	2
4	**Vulnerable**	No data or log proves that server has been hacked, but server contains security vulnerabilities.	1

Bot Threat

- Stages of Attack



- Severity Ratings

No.	Severity	Threat Level	Description
1	**Infected** Host is acting like a host infected with malware.	10	Host visits malicious URL, domain name and IP address related to known malware, sends data out and may have infected database server.
		9	Host visits malicious URL, domain name and IP address related to known malware, attempts to spread malicious file to other hosts.
		8	Host visits URL, domain name or IP address related to known malware.
2	**High** Host is most likely infected with malware	7	Host launches outgoing DDoS attacks or visits suspicious Conficker domain names.
		6	Host sends or receives suspicious packets related to malware, or spreads malicious shellcode.
		5	Host visits DGA-generated domain names, or initiates reverse connection.
3	**Medium** Host is not acting like an infected host but malware intrusion has ever occurred	4	Host downloads malicious executable files, PDF files or Trojan virus-infected webpage, but has not been infected yet.
		3	Host downloads suspicious files with unmatching extension or name, but has not been infected yet.

4	**Low** Host is less likely infected with malware	**2** **1**	Host uses protocols related to malware(such as IRC, HFS, etc) and accesses suspicious domain names or IP addresses related to malware. Abnormal traffic is detected, such as SSL protocol uses other ports rather than the standard port 443, but threat level is low. Host may visit phishing/fake websites/emails that steal accounts.