Security Report

Period: 2016-07-14 to 2016-07-20

Generated At: 2016-07-21 17:08:23

Application Server Domain/IP: Total

User: Total

Purpose

1. Help to find risk quickly and provide information such as attack source, target, impact and solutions.

Contents

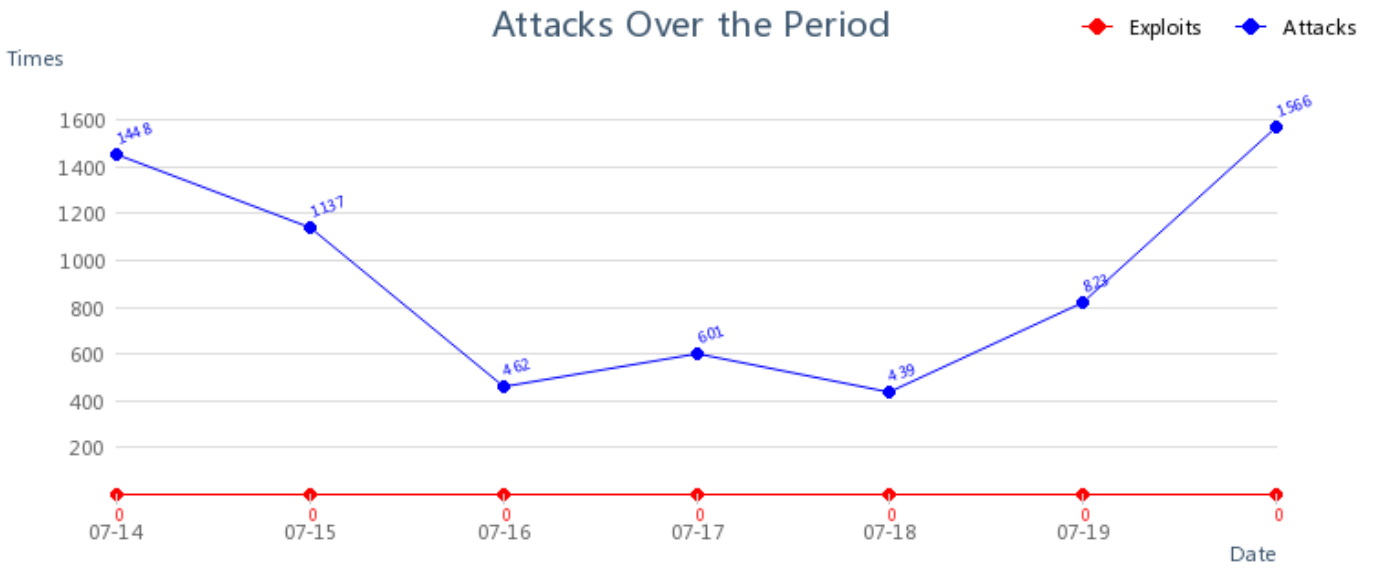
Security Overview

Summary

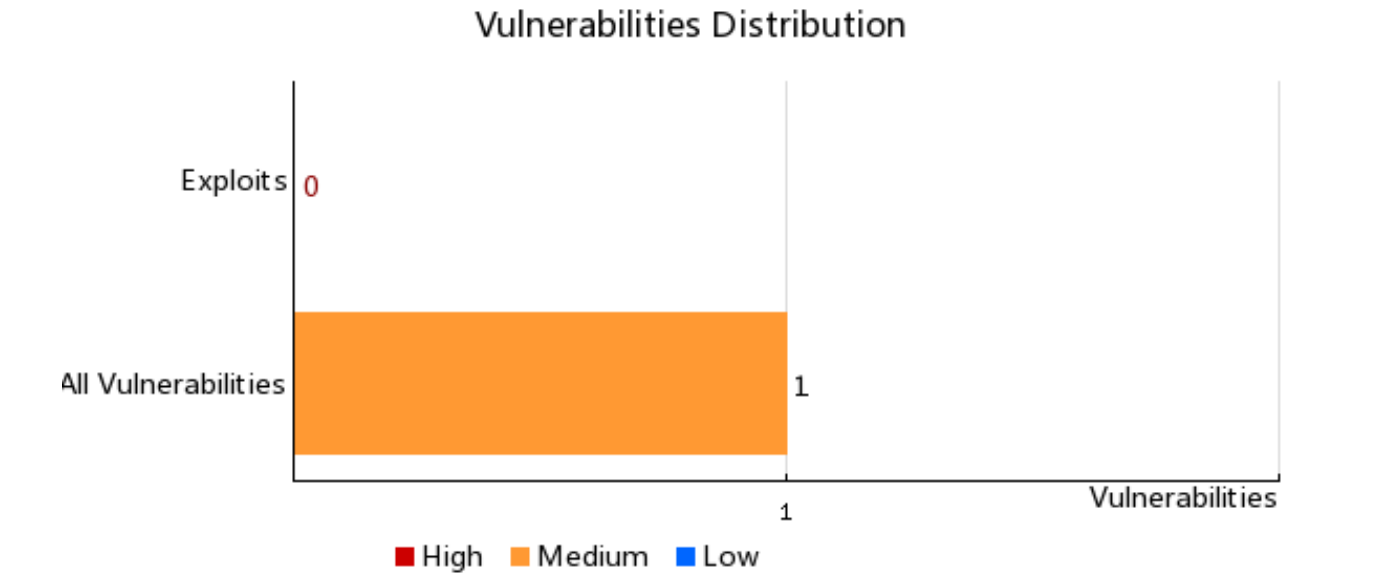
2016-07-14 to 2016-07-20, overall security rating is Poor, (see Security Rating Regulations).

After checking security of application servers and endpoint users, based on Layer 2 to Layer 7 analysis, vulnerability analysis, License Detection, we found 1 Rule Database Expired, 0 high-risk vulnerabilities, average number of attacks each day is between 100 and 1000. Vulnerable targets are 192.168.20.100, 172.217.24.225 Application Server Domain/IP,Application server and user are undergoing few attacks, and the current protection policy can shield them away from eventual attack.

Attack possibility over the past period is as follows:
The more attacks, the worse the network security. The more exploits, the more likely the network will be intruded by attacker. Using next-generation firewall can protect the system against exploits and attacks by attackers. An exploit may be a piece of software that takes advantage of a bug or vulnerability in order to cause unintended behavior to computer software. And it's the attack that can be exploited by attackers, such as denial-of-service attack.



Vulnerability Distribution:
2016-07-14 to 2016-07-20, 1; for medium-risk vulnerability, there are 1.



Security Rating

Security Rating Based on Attack

No.	Attack Type	Description	Attacks Per Day	Security Level
1	Application Server Security	Exploited but protected now	17	Good
2	User Security	Attacked but protected now	907	Fair
3	Mobile Security	Mobile device is under attack, but prevented from attacks now.	0	Excellent

Security Rating Based on Vulnerability

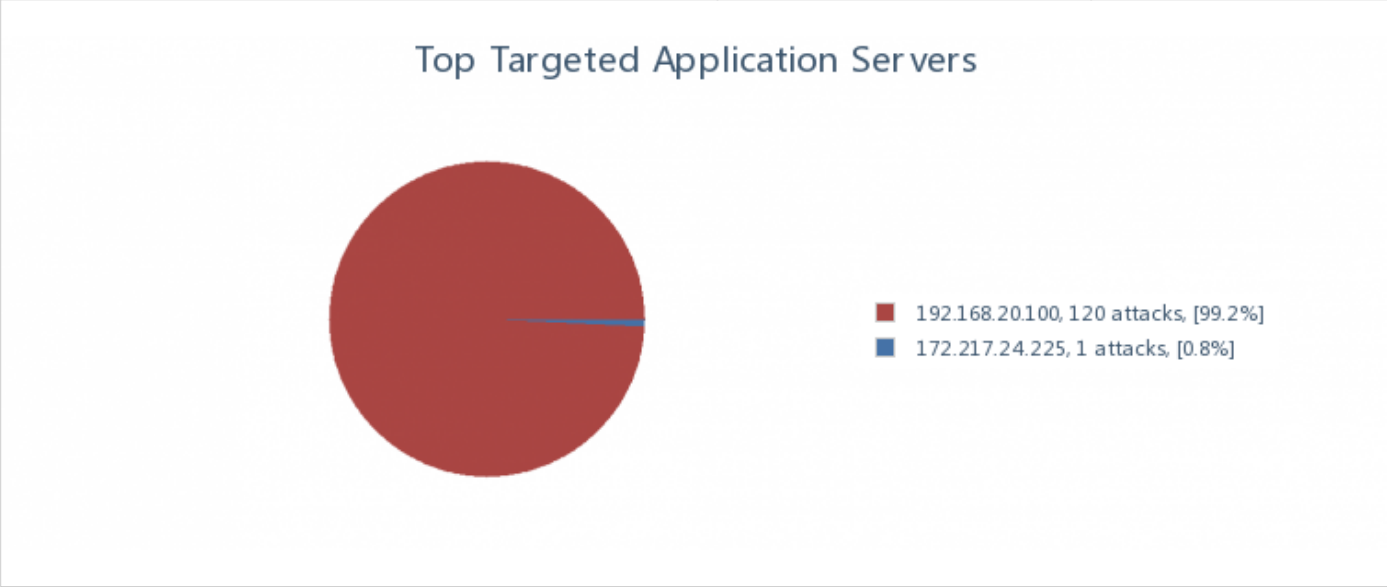
No.	Vulnerability Type	Description	High-Risk Vulnerabilities	Security Level
1	All Vulnerabilities	Potential risk	0	Excellent

Security rating is based on rule event:

No.	Type	Description	Count	Security Level
1	Rule Database Detection	Anti-Virus Database Rule Database Expired	1	Poor

Application Server Security

Application server 192.168.20.100 accounts for 99.17%, 172.217.24.225 accounts for 0.83%, The higher the t-hreat level, the more vulnerable the server is, and the higher threat the server is facing.



Attack Analysis

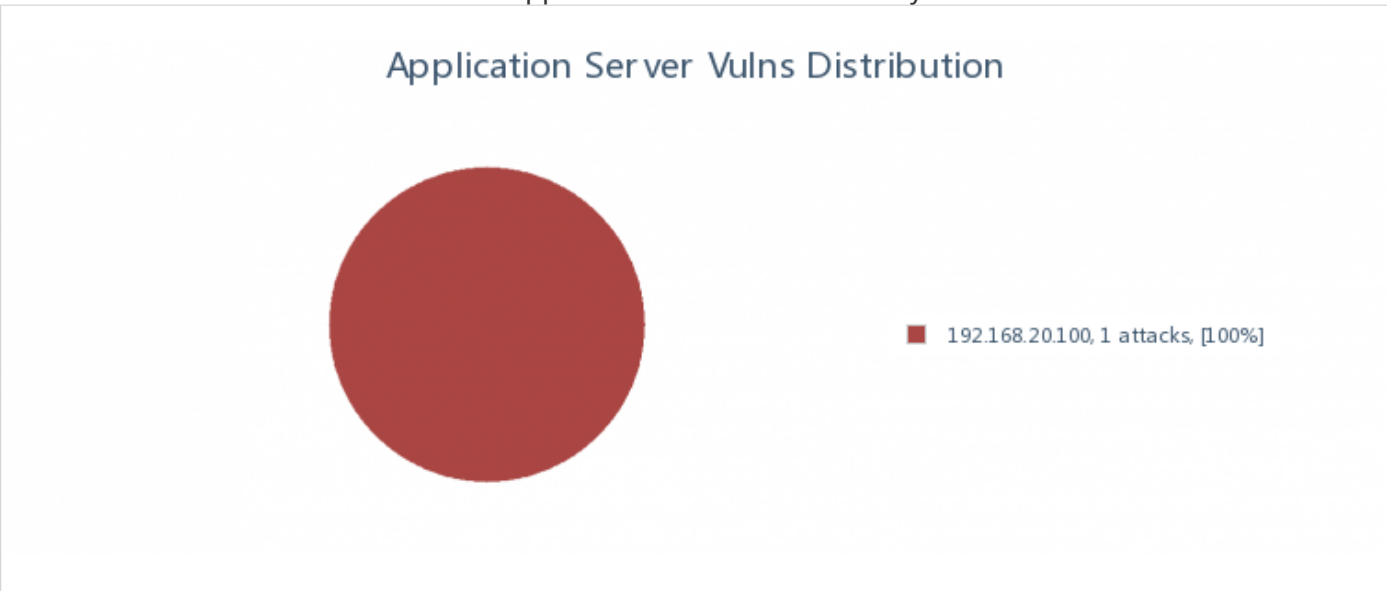
Top Targeted Application Servers

No.	Application Server	Attack Type	Attack Count	Percent	Exploits	Threat Level
1	192.168.20.100	Brute-force attack(6-7), Request method filter(52), Port scan(1)	120	99.17%	0	High

2	172.217.24.225	UDP flooding attack(1)	1	0.83%	0	High

Vulnerability Assessment

192.168.20.100 are the most vulnerable application servers. Vulnerability distribution is as follows:

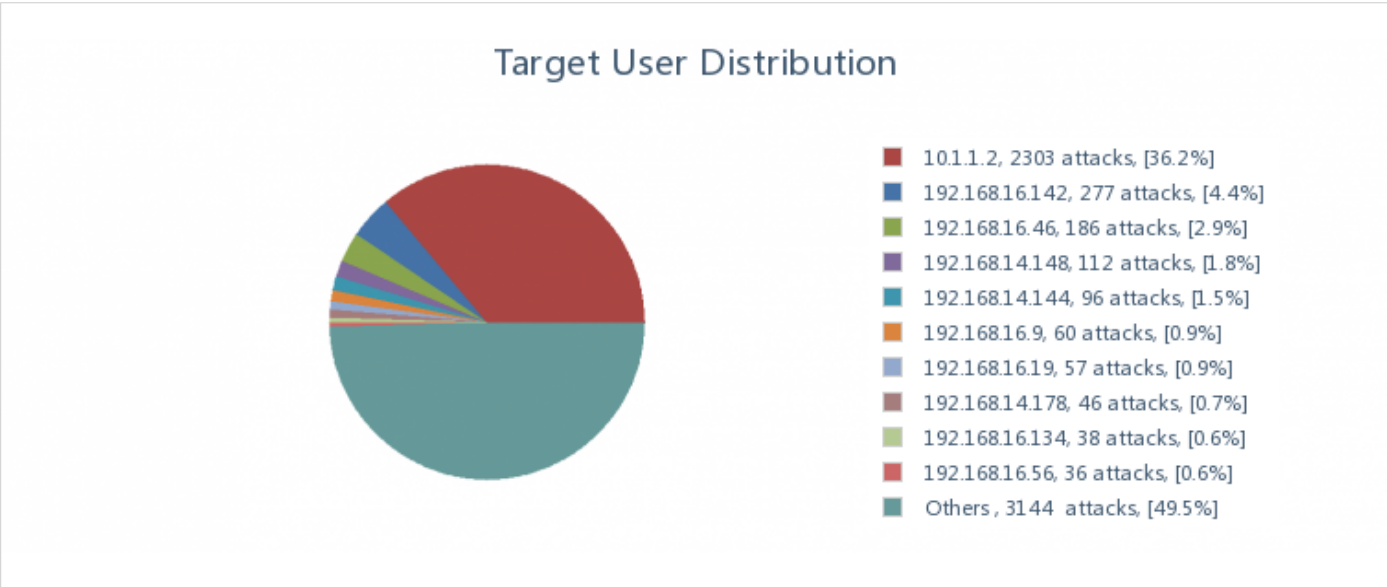


Most Vulnerable Application Servers

No.	Application Server	Vulnerability Type	Vulnerability Count	Exploits	Threat Level
1	192.168.20.100	Wrong Configuration(1)	1	0	Medium

User Security

User 10.1.1.2, 192.168.16.142, 192.168.16.46 are facing the highest threat.



Top Targeted Users

No.	User	Attack Type	Attack Count	Percent	Threat Level
1	10.1.1.2	(Botnet) >Malware(2303)	2303	36.24%	High
2	192.168.16.142	(Botnet) >Malware(277)	277	4.36%	High
3	192.168.16.46	(Botnet) >Malware(186)	186	2.93%	High

4	192.168.14.148	(Botnet) >Malware(111), Malicious Connection(1)	112	1.76%	High
5	192.168.14.144	(Botnet) >Malware(75), Malicious Connection(21)	96	1.51%	High
6	192.168.16.9	(Botnet) >Malware(60)	60	0.94%	High
7	192.168.16.19	(Botnet) >Malware(57)	57	0.9%	High
8	192.168.14.178	(Botnet) >Malware(46)	46	0.72%	High
9	192.168.16.134	(Botnet) >Malware(35), Malicious Connection(3)	38	0.6%	High
10	192.168.16.56	(Botnet) >Malware(36)	36	0.57%	High
11	Others		3144	49.5%	

Users with Most Suspicious Connections

Among which10.1.1.2, 192.168.14.178, 192.168.16.142 are involved in suspicious connections and may be taken advantaged by hacker to become part of botnet. Action needs to be taken to prevent hacker from performing springboard attack or APT attack.

No.	User	Accessed URL	Dst IP	Dst Location	Suspicious Connections
1	10.1.1.2	http://npkxghmoru.biz	-	-	2328
2	192.168.14.178	http://xjpakmdcfuqe.ru	195.22.28.198	Portugal	345
3	192.168.16.142	http://servicemap.conduit-services.com/Toolbar/?ownerId=CT3220468	23.10.23.188	Singapore	277
4	192.168.13.127	http://loaris.com/check_ver.php?ver=1338	192.237.188.201	United States	246
5	192.168.16.46	http://amnsreiuojy.ru	-	-	186
6	192.168.15.164	http://p.rfihub.com/cm?in=1&pub=7115&rid=84-ef7017eb0b43dc9127dab-4cbea9010	203.131.243.181	China,Hong Kong	120
7	192.168.14.148	http://amnsreiuojy.ru	-	-	112
8	192.168.10.146	ads.whoarethisstrangeguy.com/cgi-bin/advert/settags?x_mode=args&x_format=javascript&x_dp_id=1203-&x_pub_id=238143&tag=EN_RECOVER...	149.202.198.20	France	107
9	192.168.14.144	http://amnsreiuojy.ru	-	-	96

10	192.168.12.204	http://loaris.com/check_ver.php?ver=1348	192.237.188.201	United States	96
11	Others	-			3177

Mobile Security

Mobile Botnet

No data available

Mobile Virus

No data available

Analysis Based on Risk Type

Based on analysis on traffic from several aspects, we found 7 categories of applications are in security threat. For those at high threat level, there are 4. For those at medium threat level, there are 3, which are as follows:

Application Server Security - Attack Types

No.	Attack Type	Attack Count	Percent	Exploited?	Threat Level
1	Brute-force attack	67	55.4%	No	High
2	UDP flooding attack	1	0.8%	No	High
3	Request method filter	52	43%	No	Medium
4	Port scan	1	0.8%	No	Medium

Application Server Security - Top Vulnerability Types

No.	Name	Vulnerability Count	Target IP	Threat Level
1	Wrong Configuration	1	-	Medium

User Security Details Attack Type

No.	Attack Type	Attack Count	Percent	Threat Level
1	(Botnet) >Malware	3765	59.25%	High
2	Malicious Connection	2590	40.76%	High

Analysis Based on Specific Attack

Brute-force Attack

Description

Open password authentication service server, an attacker can use brute force tool for servers. once a successful brute force, the attacker can do anything through the server.

Target Server

Brute-force attack: 67 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	192.168.20.100	-	67

Solution

1.Try to limit the server only allows network users to access.
2.Change the password for the special characters plus numbers plus characters at least 8 characters mixing.
3.Open IPS turned brute tactics and select block.

UDP Flooding Attack

Description

DDoS, Distributed Deny of Service in short, is an attack that attacker sends immense error data packets or partially connected packets to target server, with the purpose of consuming all the bandwidth and allowed connections, CPU and memory resources of the server, so that the server cannot provide services to legitimate users properly.

Target Server

UDP flooding attack: 1 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	172.217.24.225	-	1

Solution

1.Enable anti-DDoS attacks, both inside and outside DDoS attack, and configure the corresponding policy.

Request Method Filter

Description

Attacker takes advantage of the vulnerability to download files from Web server, upload malicious file or remove any file without logging in to the Web server.

Target Server

Request method filter: 52 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	192.168.20.100	**Dst Name:** http://rtsp://202.29.105.31:3454/Media/Live/Normal?camera=C_1&streamindex=2	52

Solution

1.Disable unnecessary HTTP methods, including the method for defining WEBDAV.

Port Scan

Description

DDoS, Distributed Deny of Service in short, is an attack that attacker sends immense error data packets or partially connected packets to target server, with the purpose of consuming all the bandwidth and allowed connections, CPU and memory resources of the server, so that the server cannot provide services to legitimate users properly.

Target Server

Port scan: 1 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	192.168.20.100	-	1

Solution

1.Enable anti-DDoS attacks, both inside and outside DDoS attack, and configure the corresponding policy.

Analysis Based on Specific Vulnerability

Wrong Configuration

Description

Wrong configuration or security vulnerability of Web server often makes information disclosed to the Internet. System files or configuration files are vulnerable to leakage, making sensitive information available to Internet users, such as username, password, source code, server information, configuration, internal IP address, email address, etc.

Target Server

Wrong Configuration: 1, which are as follows:

No.	Target Domain/IP	Count
1	192.168.20.100	1

Solution

1.Webmaster changes the settings to not show user the returned error information.
2.Use Web Application Firewall(WAF).

Analysis Based on Specific Threat

(Botnet) >Malware

Description

Attacker can make infected hosts to initiate DDoS attacks, or make hosts in botnet to attack other internal hosts, with the purpose of stealing user account, password, sensitive information, crucial files and so on.

Target Server

(Botnet) >Malware: 3765 attacks, which are as follows:

No.	Target IP	Details	Attack Count
1	10.1.1.2	**Dst Name:** http://ecpmrocks.com	2303
2	192.168.16.46	**Dst Name:** http://go.mobtrks.com	186
3	192.168.14.148	**Dst Name:** http://amnsreiuojy.ru	111
4	192.168.14.144	**Dst Name:** http://amnsreiuojy.ru	75
5	192.168.16.9	**Dst Name:** http://amnsreiuojy.ru	60
6	192.168.16.19	**Dst Name:** http://amnsreiuojy.ru	57
7	192.168.14.178	**Dst Name:** http://xjpakmdcfuqe.ru	46
8	192.168.16.56	**Dst Name:** http://amnsreiuojy.ru	36
9	192.168.16.134	**Dst Name:** http://amnsreiuojy.ru	35
10	192.168.16.191	**Dst Name:** http://amnsreiuojy.ru	18
11	Others	-	84

Solution

1.Scan and remove virus and Trojan on endpoint.

2.Enable APT detection and cut off the communication between botnet infected host and controller.

Malicious Connection

Description

Attacker often launches APT attack by utilizing malicious connection, such as webpage mounted with trojan, trojan virus, to decieve user to access it so as to steal user crucial information, such as sensitive information, account and important file.

Target Server

Malicious Connection: 2590 attacks, which are as follows:

No.	Target IP	Details	Attack Count
1	192.168.15.164	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=7115&rid=84ef7017eb0b43dc9127dab4cbea9010	114
2	192.168.12.8	**Dst Name:** http://clickadu.com/apu.php?zoneid=462853	51
3	192.168.17.186	**Dst Name:** http://sync.ad-stir.com/?symbol=TURN&uid=2675529611068374469	40
4	192.168.12.120	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=19591	38
5	192.168.17.15	**Dst Name:** eclkspbn.com/adServe/sa?cid=112690_188961_1&pid=&q=fas.li&ap=cmp%3DPOPUNDER%26evp%3DutUnKj-C1yDHPqxTyYWVjlY37AsT2AewJtnSmCu_CUw...	37
6	192.168.17.4	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=10861	30
7	192.168.17.147	**Dst Name:** rotator.trafficstars.com/iframes2/088e288d72b1404ea62653e5192fec73.html?categories=porn&keywords=%20Watch%20Mobile%20Porn%20Vid...	30
8	192.168.16.138	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=7115&rid=05ce165931b84c199a751c1af495e151	28
9	192.168.10.168	**Dst Name:** http://upornia.com/videos/544097/kendra-lust-bruce-venture-in-my-friends-hot-mom2/?promo=11914	28
10	192.168.12.249	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=19591	24
11	Others	-	2170

Solution

1.Enable Malicious connection option on Access Control > APT Detection page, and configure policy accordingly to make affected or important host protected.

2.Install anti-virus software on client PC, keep it to latest version and scan virus regularly.

Security Rating

Excellent

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, no high-risk vulnerability is found. Threat does not affect application server security and user access right assignment. Critical security issue will not occur at present.

Good

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, less than 10 high-risk vulnerabilities are found. Average number of attacks each day is less than 100. Application server and user are undergoing few attacks, and the current protection policy can shield them away from eventual attack.

Fair

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, 10 - 50 high-risk vulnerabilities are found. Average number of attacks each day is between 100 and 1000. Application server and user are undergoing some attacks, and the current protection policy can shield them away from eventual attack.

Poor

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, more than 50 high-risk vulnerabilities are found. Average number of attacks each day is more than 1000. Application server and user are undergoing a lot attacks, or even APT(Advanced Persistent Threat) attack. Urgent protection is needed and vulnerability must be fixed.

Remarks

When the device detects that license gets invalid, expired or the rule database license gets expired, the security rating will de degraded one rank; while APT or WebShell attack is detected, the security rating becomes critical.

Description

Current Software Version: AF6.8.232 EN Build20160328

Current Database Version:

No.	Name	Current Version Released
1	Anti-Virus Database	20160627 18:00:00
2	URL Database	20160711 09:00:00
3	Vulnerability Database	20160714 17:00:00
4	Software Update	20160517 17:16:29
5	Application Ident Database	20160530 12:34:56
6	WAF Signature Database	20160630 17:00:00
7	Data Leak Protection	20160627 09:39:55
8	Malware Signature Database	20160715 09:22:22
9	Vulnerability Analysis Rule	20160706 17:00:00
10	Malicious Connection Database	20160715 10:50:12
11	Threat Intelligence Database	20160718 16:30:01