User Security Report

Period: 2016-06-01 to 2016-07-20

Generated At: 2016-07-21 17:19:54

User: Total

Purpose

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

Contents

Security Overview

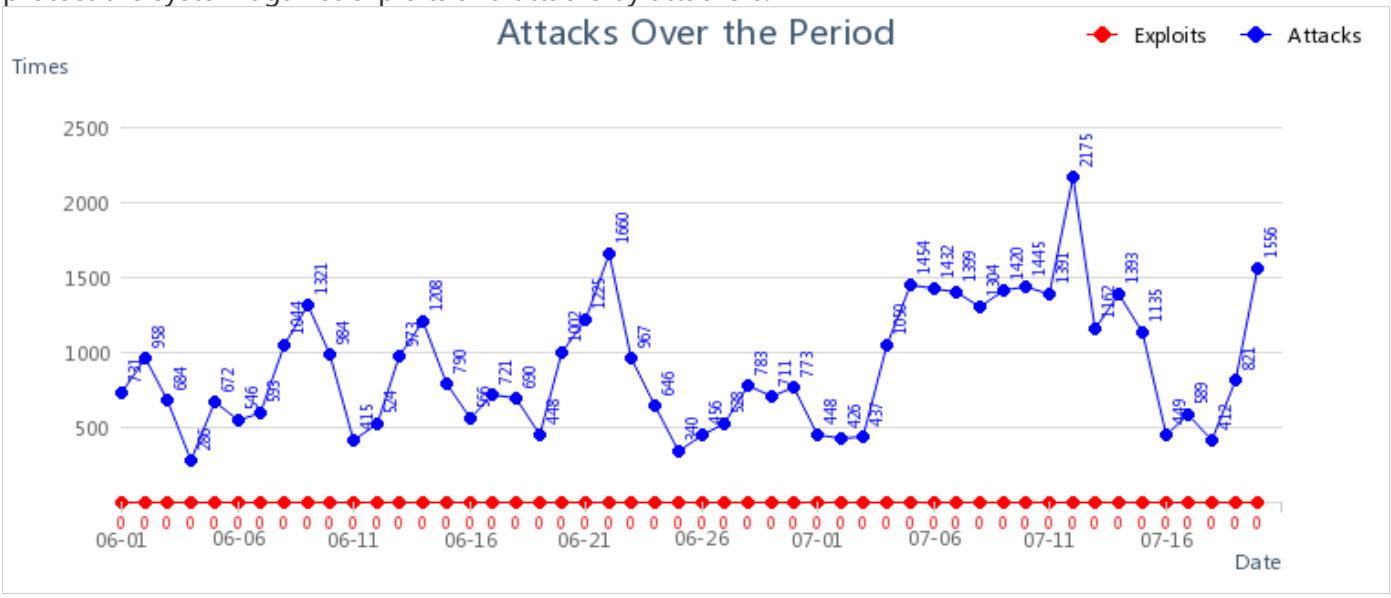
Summary

2016-06-01 to 2016-07-20, overall security rating is Poor, (see Security Rating Regulations).

After checking security of endpoint users, based on Layer 2 to Layer 7 analysis, License Detection, we found 1 Rule Database Expired, average number of attacks each day is between 100 and 1000. Users are undergoing some attacks, but the current protection policy can protect them.

Attack possibility over the past period is as follows:

The more threats, the more likely the network will be intruded by attacker.Using next-generation firewall can protect the system against exploits and attacks by attackers.



Security Rating

Security Rating Based on Attack

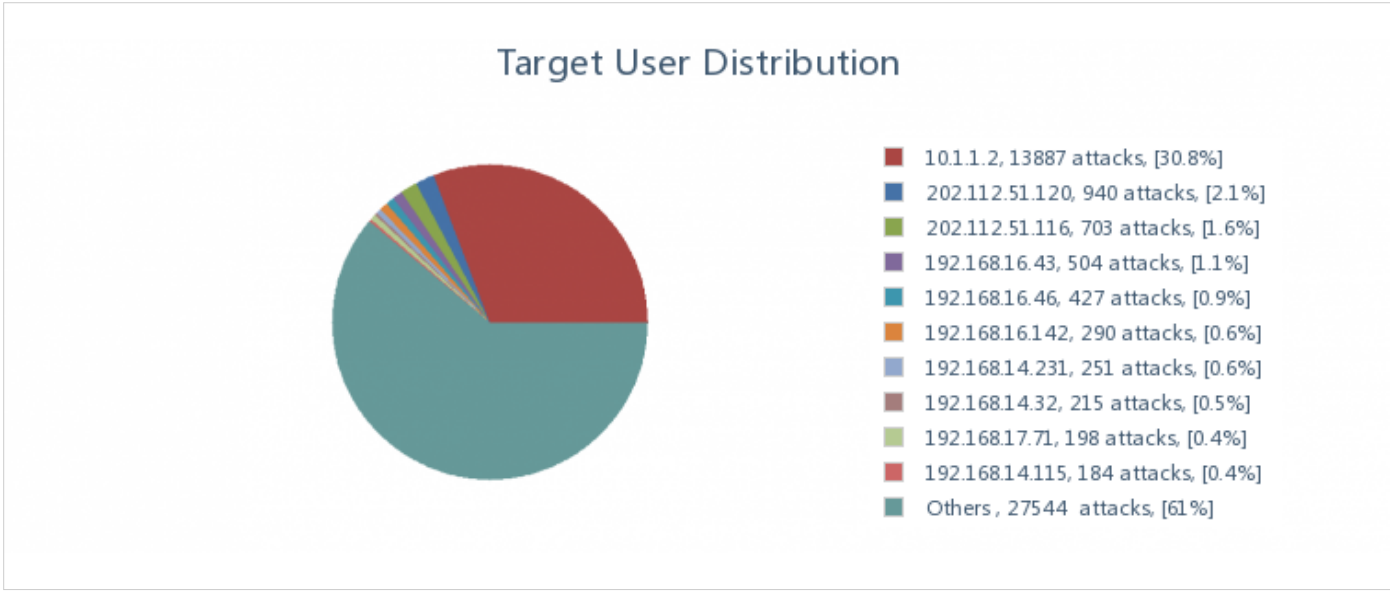
No.	Attack Type	Description	Attacks Per Day	Security Level
1	User Security	Attacked but protected now	902	Fair
2	Mobile Security	Mobile device is under attack, but prevented from attacks now.	0	Excellent

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

User Security

User 10.1.1.2, 202.112.51.120, 202.112.51.116 are facing the highest threat.



Top Targeted Users

No.	User	Attack Type	Attack Count	Percent	Threat Level
1	10.1.1.2	(Botnet) >Malware(13887)	13887	30.76%	High
2	202.112.51.120	(Botnet) >Malware(940)	940	2.08%	High
3	202.112.51.116	(Botnet) >Malware(682), -(21)	703	1.56%	High
4	192.168.16.43	(Botnet) >Malware(474), Malicious Connection(30)	504	1.12%	High
5	192.168.16.46	Malicious Connection(241), (Botnet) >Malware(186)	427	0.95%	High
6	192.168.16.142	(Botnet) >Malware(277), Malicious Connection(13)	290	0.64%	High
7	192.168.14.231	(Botnet) >Malware(232), Malicious Connection(19)	251	0.56%	High
8	192.168.14.32	(Botnet) >Malware(189), Malicious Connection(26)	215	0.48%	High
9	192.168.17.71	(Botnet) >Malware(169), Malicious Connection(29)	198	0.44%	High
10	192.168.14.115	(Botnet) >Malware(168), Malicious Connection(16)	184	0.41%	High
11	Others		27544	61%	

Users with Most Suspicious Connections

Among which10.1.1.2, 192.168.13.174, 202.112.51.120 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	-	-	14059
2	192.168.13.174	http://p.rfihub.com/cm?in=1&pub=345&userid=-6898256394825235126	203.131.243.181	China,Hong Kong	1277
3	202.112.51.120	http://smtp.py.kopolar.com	204.11.56.48	United States	940
4	192.168.17.200	http://p.rfihub.com/cm?pub=24472&in=1	203.131.243.181	China,Hong Kong	928
5	192.168.13.185	http://p.rfihub.com/cm?in=1&pub=19591	203.131.243.181	China,Hong Kong	845
6	192.168.15.77	http://sync.ad-stir.com/?symbol=TURN&uid=2636676506-907640227	52.68.210.14	Japan	828
7	192.168.13.5	http://clickadu.com/afu.php?zoneid=624005	203.76.173.22	Singapore	821
8	192.168.16.46	http://amnsreiuojy.ru	-	-	813
9	192.168.13.138	http://p.rfihub.com/cm?in=1&pub=64	203.131.243.181	China,Hong Kong	731
10	202.112.51.116	http://smtp.py.kopolar.com	204.11.56.48	United States	703
11	Others	-			54451

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 3 categories of applications are in security threat. For those at high threat level, there are 2. For those at medium threat level, there are 1, which are as follows:

User Security Details Attack Type

No.	Attack Type	Attack Count	Percent	Threat Level
1	(Botnet) >Malware	24931	55.23%	High
2	Malicious Connection	20191	44.73%	High
3	-	21	0.05%	Medium

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: 24931 attacks, which are as follows:

No.	Target IP	Details	Attack Count
1	10.1.1.2	**Dst Name:** http://ecpmrocks.com	13887
2	202.112.51.120	**Dst Name:** http://www.oxitr.net	940
3	202.112.51.116	**Dst Name:** http://www.mobtimizer.com	682
4	192.168.16.43	**Dst Name:** http://amnsreiuojy.ru	474
5	192.168.14.231	**Dst Name:** http://amnsreiuojy.ru	232
6	192.168.14.32	**Dst Name:** http://amnsreiuojy.ru	189
7	192.168.16.46	**Dst Name:** http://go.mobtrks.com	186
8	192.168.14.115	**Dst Name:** http://amnsreiuojy.ru	168
9	192.168.14.152	**Dst Name:** http://amnsreiuojy.ru	165
10	192.168.14.95	**Dst Name:** http://amnsreiuojy.ru	126
11	Others	-	2963

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: 20191 attacks, which are as follows:

No.	Target IP	Details	Attack Count
1	192.168.16.46	**Dst Name:** wct.link/click?c=eyJhIjoyNiwibyI6MTM2LCJwIjozfSAg&ptrack=MTE5NzA2MnxyZXBvcm8uY29tfFRIQXx8MTI3OTYyMDJ8fHwxOTgzMjM4fDIwMi4yOS4xMD...	241
2	192.168.13.142	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=19591	147
3	192.168.14.14	**Dst Name:** http://sync.ad-stir.com/?symbol=TURN&uid=2927917717142167110	138
4	192.168.16.84	**Dst Name:** http://prmobiles.com/hotnewsindo.info/jczl/direct/t:intlib	131
5	192.168.17.231	**Dst Name:** http://euphimie.info/wp-content/uploads/2015/04/euphimie.png	120
6	192.168.15.164	**Dst Name:** http://p.rfihub.com/cm?in=1&pub=7115&rid=84ef7017eb0b43dc9127dab4cbea9010	115
7	192.168.17.186	**Dst Name:** http://sync.ad-stir.com/?symbol=TURN&uid=2675529611068374469	93
8	192.168.16.64	**Dst Name:** http://p.rfihub.com/cm?pub=24472&in=1	91
9	192.168.17.34	**Dst Name:** p.rfihub.com/cm?in=1&pub=24273&userid=Cqp3S1cpur8xWAXgIDptAg%3D%3D&url=http%3A%2F%2Fseg.sharethis.com%2FgetSegment.php%3Fpurl%3...	87
10	192.168.13.189	**Dst Name:** http://p.rfihub.com/cm?pub=24472&in=1	81
11	Others	-	18947

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.

-

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

-: 21 attacks, which are as follows:

No.	Target IP	Details	Attack Count
1	202.112.51.116	**Dst Name:** http://www.bekendnaakt.net	21

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.

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