Notes on Linux/BillGates

bartblaze.blogspot.com/2017/12/notes-on-linuxbillgates.html

In a previous blog post, I wrote some (extensive) notes on Linux/Xor.DDoS, also known as just Xor.DDoS, an interesting type of Linux malware.

You can find that particular blog below, in which I give some history, details, remediation and prevention in regards to the specific threat Xor.DDoS poses:
Notes on Linux/Xor.DDoS

This post will include some notes on Linux/BillGates, hereafter referred to as just 'BillGates', and rather than being very in-depth as the previous blog, I will mostly list high-level notes and remediation or disinfection steps. Additionally, after the conclusion, you will find other resources if necessary. In case of questions, comments or feedback, leave a comment or contact me on Twitter.

What is BillGates?

BillGates is malware designed primarily for Linux, and since it is a botnet, it is mostly used for DDoS purposes.

However, just as Xor.DDoS, it has limited rootkit and backdoor functionality and thus it's possible remote commands are executed as well as additional malware downloaded.

How can I identify BillGates artefacts?

Please find below a table with indicators.

Indicator	Notes
/etc/cmd.n	
/etc/conf.n	
/etc/init.d/DbSecuritySpt	
/etc/init.d/selinux	
/etc/rc**X**.d/97DbSecuritySpt	Where X is a number, usually symlinks to /etc/init.d/DbSecuritySpt
/home/ll2	Identify all files with random names in /home/
/tmp/.bash_root.tmp3	

/tmp/.bash_root.tmp3h	
/tmp/bill.lock	Identify all .lock files in /tmp/
/tmp/bill.lod	Contains Process ID (PID) of malware main module
/tmp/gates.lod (or gates.lock)	Contains PID of malware main module
/tmp/moni.lod (or moni.lock)	Contains PID of malware 'watchdog'
/tmp/notify.file	
/usr/bin/*.lock	Identify all .lock files in /tmp/
/usr/bin/bsd-port/.sshd	
/usr/bin/bsd-port/*.lock	
/usr/bin/bsd-port/getty	
/usr/bin/bsd-port/getty/*.lock	Identify all .lock files in /usr/bin/bsd-port/getty/
/usr/bin/pojie	Identify all files with random names in /usr/bin/
/usr/lib/libamplify.so	Configuration file

How can I identify BillGates DDoS modules?

These modules are usually stored in **/etc/**, and will have the following names:

- atddd
- cupsdd
- cupsddh
- ksapdd
- kysapdd
- sksapdd
- skysapdd

It may however be useful to use the find command in conjunction with these names, in case they are residing in a different location than /etc/.

How can I identify other modifications BillGates made?

BillGates does create aliases and/or modifies/replaces files which are typically used to monitor processes or the network. The following may be replaced:

- /bin/lsof
- /bin/netstat
- /bin/ps
- /bin/ss
- /usr/bin/lsof
- /usr/bin/netstat
- /usr/bin/ps
- /usr/bin/ss
- /usr/sbin/lsof
- /usr/sbin/netstat
- /usr/sbin/ps
- /usr/sbin/ss

A copy of the legitimate files is normally stored in:
/usr/bin/dpkgd/

Additionally, check for any potentially created *jobs* by looking in:
/etc/cron.X where X is a name or folder, for example /etc/cron.daily.

You may also wish to look in:
/var/spool/cron/

Removal instructions

While the **ps** command may be replaced, **top** is not. Run the **top** command and verify any illegitimate processes, usually they will be randomly named. Alternatively, identify the *.lod and *.lock files, and use **cat** for example to read them, and identify the PID of the malware.

Then, use **kill** to end the malicious process(es), and remove the files or artefacts as indicated in the table above.

Afterwards, use **mv** to move the legitimate files back to their original location. You can also use a file manager to easily move them, if you have one.

You may also use an anti-virus to identify and remove any malicious files, for example ClamAV does a great job - BillGates is a rather older botnet by now and thus most antiviruses should have coverage for it. Don't forget to update the anti-virus' signatures first, if needed.

This same explanation but step-by-step to make it easy:

- Identify malicious processes: use **top** or check the PID in BillGates' config files;
- Killmalicious processes: use **kill -9** to kill any of its processes;
- Remove malicious files and folders, see the sections above;

- Replace potentially hijacked files and restore them to their original location, see also above:
- Identify any malicious tasks and delete them as indicated above;
- Run **top** again to verify there are no malicious processes left;
- Run an anti-virus or anti-malware as a secondary opinion;
- Change your passwords, better be safe than sorry!

Conclusion

While Linux/BillGates may not be the biggest player on the market anymore, or even not as popular or common nowadays, the threat still exists, just like Xor.DDoS.

Practice proper security hygiene and take appropriate preventative measures.

In the resources section below, you may find additional useful links.

Resources

Blaze's Security Blog - Notes on Linux/Xor.DDoS
HabraHabr - Let's explore Linux Botnet "BillGates"
Linux.com - How to Move Files Using Linux Commands or File Managers
LiquidWeb - How to Display (List) All Jobs in Cron / Crontab
MakeUseOf - The 7 Best Free Linux Anti-Virus Programs
MalwareMustDie - ChinaZ made new malware: ELF Linux/BillGates.Lite
Netlab 360 - New Elknot/Billgates Variant with XOR like C2 Configuration Encryption Scheme
nixCraft - Kill Process in Linux or Terminate a Process in UNIX / Linux Systems
QueQuero - Inside a Kippo honeypot: how the billgates botnet spreads
ThisIsSecurity - When ELF.BillGates met Windows
ValdikSS (Github) - BillGates botnet tracker