KillDisk now targeting Linux: Demands $250K ransom, but can't decrypt

welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

January 5, 2017

ESET has discovered a Linux variant of the KillDisk component that renders Linux machines unbootable, while encrypting files and requesting a large ransom at the same time.

ESET has discovered a Linux variant of the KillDisk component that renders Linux machines unbootable, while encrypting files and requesting a large ransom at the same time.

ESET researchers have discovered a Linux variant of the KillDisk malware that was used in Ukraine in attacks against the country's critical infrastructure in late 2015 and against a number of targets within its financial sector in December 2016. This new variant renders Linux machines unbootable, after encrypting files and requesting a large ransom. But even if victims do reach deep into their pockets, the probability that the attackers will decrypt the files is small.

KillDisk – from wiping to encrypting

KillDisk is a destructive malware that gained notoriety as a component of successful attacks performed by the BlackEnergy group against the Ukrainian power grid in December 2015 and attacks against one of the country's main news agencies in November 2015. More recently, we detected cyber-sabotage attacks utilizing KillDisk against a number of different targets within the financial sector in Ukraine planned for December 6, 2016. At that time, a group, which we dubbed as TeleBots, had utilized a different set of tools, abusing the popular Telegram messenger service.

KillDisk attack campaigns continued throughout December, aimed at several targets in the sea transportation sector in Ukraine. The attack toolset has evolved as well – attackers now make use of Meterpreter backdoors and C&C communication no longer travels through Telegram API.

While the December 6th KillDisk variants were quite artistic and displayed a screen referring to the popular Mr. Robot show on television, recent variants add a more sinister feature – file-encrypting ransomware. The ransom message begins with a provocative "we are so sorry…" and demands that the victim pay an exceptionally high ransom in return for the encrypted files – 222 Bitcoin, which is approximately USD 250,000 at the time of writing.

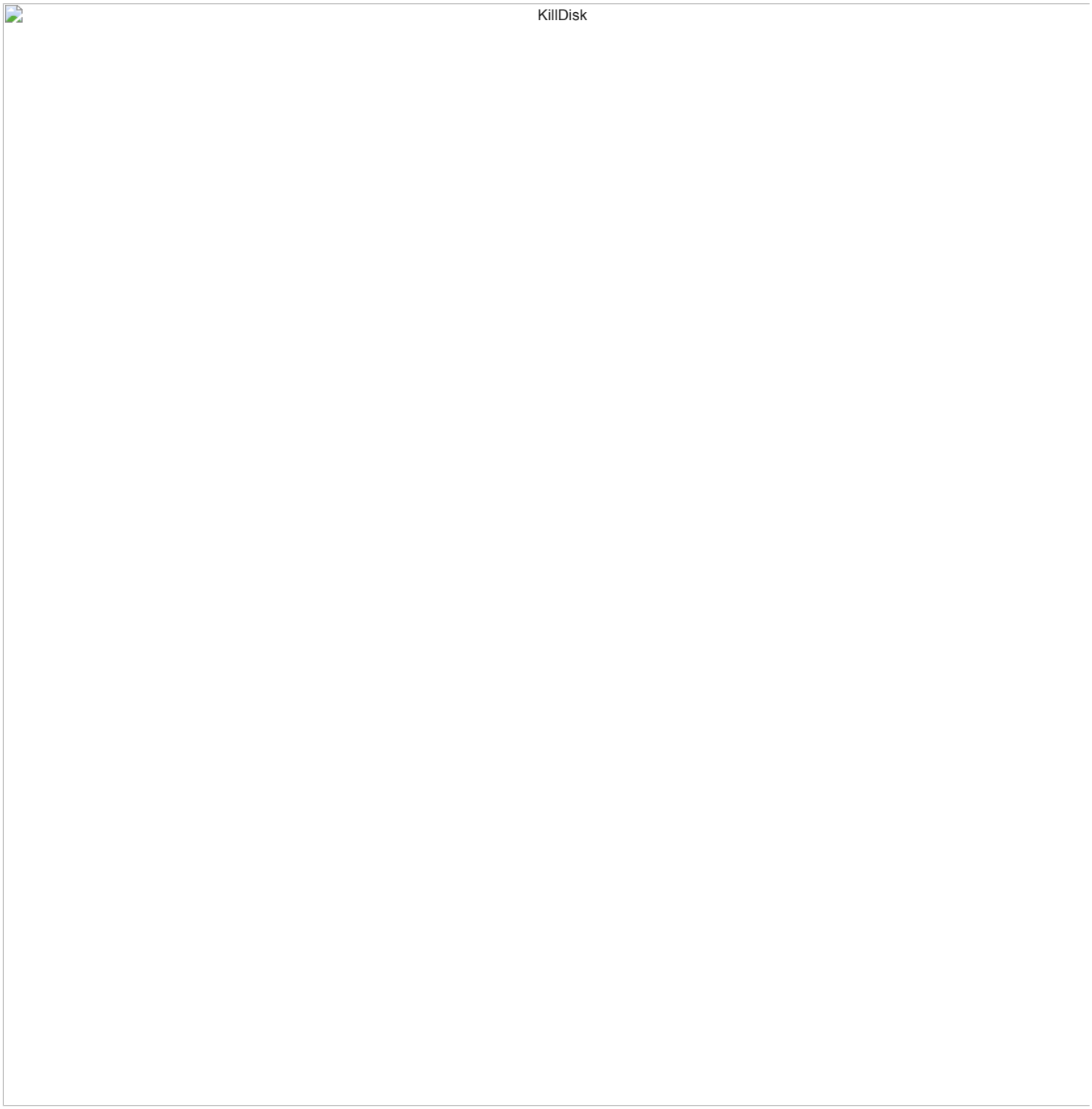

Figure 1 – Windows KillDisk ransom message

These recent ransomware KillDisk variants are not only able to target Windows systems, but also Linux machines, which is certainly something we don't see every day. This may include not only Linux workstations but also servers, amplifying the damage potential.

The Windows variants, detected by ESET as Win32/KillDisk.NBK and Win32/KillDisk.NBL, encrypt files with AES (256-bit encryption key generated using CryptGenRandom) and the symmetric AES key is then encrypted using 1024-bit RSA. In order not to encrypt files twice, the malware adds the following marker to the end of each encrypted file: DoN0t0uch7h!$CrYpteDfilE.

Figure 2 – Linux KillDisk ransom message

In both Windows and Linux variants, the ransom message is exactly the same, including the ransom amount – BTC 222, Bitcoin address, and contact email.

Linux/KillDisk.A technical analysis

While the ransom details for both platforms are identical, the technical implementation is, obviously, different. The ransom message is displayed in an unusual manner – within the GRUB bootloader. When the malware executes, the bootloader entries are overwritten in order to display the ransom text.

The main encryption routine recursively traverses the following folders within the root directory up to 17 subdirectories in depth:

/boot
/bin
/sbin
/lib/security
/lib64/security
/usr/local/etc
/etc
/mnt
/share
/media
/home
/usr
/tmp
/opt
/var
/root

Files are encrypted using Triple-DES applied to 4096-byte file blocks. Each file is encrypted using a different set of 64-bit encryption keys.

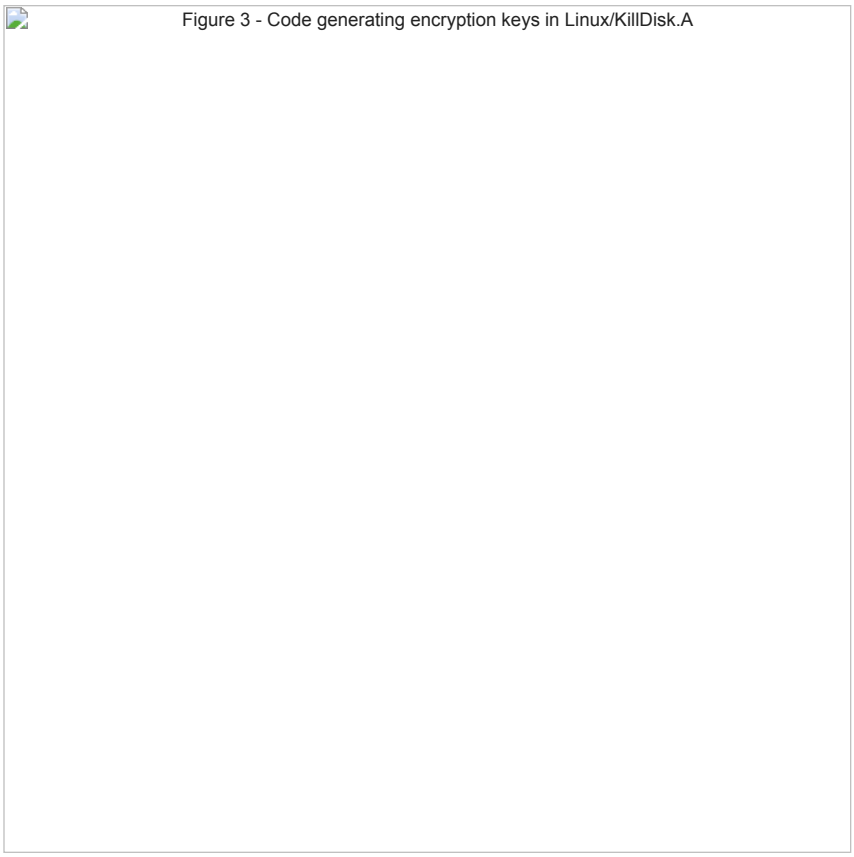

Figure 3 – Code generating encryption keys in Linux/KillDisk.A

After a reboot, the affected system will be unbootable.

It is important to note – that paying the ransom demanded for the recovery of encrypted files is a waste of time and money. The encryption keys generated on the affected host are neither saved locally nor sent to a C&C server.

Let us emphasize that – the cyber criminals behind this KillDisk variant *cannot* supply their victims with the decryption keys to recover their files, despite those victims paying the extremely large sum demanded by this ransomware.

Moreover, ESET researchers have noted a weakness in the encryption employed in the Linux version of ransomware, which makes recovery possible, albeit difficult. (Note that this does not apply to the Windows version.)

Conclusion – why ransomware?

While monitoring the BlackEnergy and TeleBots cyberattacks, we have observed an interesting evolution of the simple but destructive KillDisk component. Over the years we've detected attack campaigns against many different targets across various segments, including state institutions and critical infrastructure, many of them unrelated. The group (or groups) of attackers behind these operations has had an interest in various platforms – whether it was Windows PCs controlling SCADA/ICS systems, or workstations in a media agency. With this latest expansion, attackers can use KillDisk to destroy files on Linux systems. Nonetheless, any ties between orchestrators of these attacks remain unclear and purely circumstantial.

The recent addition of ransomware functionality seems a bit unusual, as previous attacks were cyber-espionage and cyber-sabotage operations. Considering the high ransom of around USD 250,000 – resulting in a low probability that victims would pay up, in addition to the fact that the attackers have not implemented an efficient way of decrypting the files, this seems more like a nail in the coffin, rather than a true ransomware campaign.

Whatever the true explanation, our advice still holds – if you've become a victim of ransomware, don't pay up, since there's no guarantee of getting your data back. The only safe way of dealing with ransomware is prevention – education, keeping systems updated and fully patched, using a reputable security solution, keeping backups and testing the ability to restore.

Indicators of Compromise (IoCs)

SHA1 file hashes

Win32/KillDisk.NBK trojan and **Win32/KillDisk.NBL trojan:**

2379A29B4C137AFB7C0FD80A58020F5E09716437
25074A17F5544B6F70BA3E66AB9B08ADF2702D41
95FC35948E0CE9171DFB0E972ADD2B5D03DC6938
B2E566C3CE8DA3C6D9B4DC2811D5D08729DC2900
84A2959B0AB36E1F4E3ABD61F378DC554684C9FC
92FE49F6A758492363215A58D62DF701AFB63F66
26633A02C56EA0DF49D35AA98F0FB538335F071C

Linux/KillDisk.A trojan:

8F43BDF6C2F926C160A65CBCDD4C4738A3745C0C

Ransom message

We are so sorry, but the encryption
of your data has been successfully completed,
so you can lose your data or
pay 222 btc to 1Q94RXqr5WzyNh9Jn3YLDGeBoJhxJBigcF
with blockchain.info
contact e-mail:vuyrk568gou@lelantos.org

5 Jan 2017 - 03:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion