D-Link DNS-320 NAS Cr1ptT0r Ransomware ARM Dynamic Analysis - QEMU and Raspberry PI VM

E resolverblog.blogspot.com/2019/02/d-link-dns-320-nas-cr1ptt0r-ransomware.html

NS-320L with full firmware compatibility), and I must confess that I had not updated the firmware so it should be a bay, and downloaded the latest firmware but too late. I found more FW versions ere : <u>https://support.dlink.com/ProductInt</u>

21 + range, with port forwarding.

files that we all found on the root directory, I have a new "Application" with a bright red icon that appeared in the user i

now a few victims but no previous reference on the whole internet before my creation of this topic.)

Hi Everybody,

a few days ago I saw a tweet from @Amigo_A_ asking for help about a new ransomware which was affecting a D-Link 320 NAS.

The first thought was directed to the historical disabling of dlink to make sufficiently secure firmware and their willingness not to support updates. Those facts made me to think about an attack conducted over the net targetting all the devices exposed on internet itself.

Jacobia de (19 leg 1999 - 452) Rej, casti	-
4	
4Kine .	
No.2009 (2019) (2019) for this water at water stagram 200 (20, which invest completely) and water state of a bird applicable borners or constant a signal (3) Constant control for each of a second to be dust, according to the former second to the two PP weeks or a line (according to the back of a second to the second to the back of the back of the back of the second to the back of the bac	
Noted was represented that and through and the field and the part of the composate performance of	
The file for length to some makes measure a solid or the solid measure of the solid measure of the solid measure of the solid measurement to some median of the solid measurement to improve solid and solid measurements. (In the solid measurement to be solid measurement to be solid measurements to be solid measurement to be solid measurements to be solid measurements to be solid measurements to be solid measurements.)	
Constructions further indexe operating prediments as we are used for which the pressure of the effect and other increases of the spectrum.	
may be enough to a set the section of	

Apparently was the right hypothesis.

All the users with D-Link 320XX are nowdays are at very high risk.

TURN OFF THE DEVICE AND DISCONNECT IT FROM WAN.On <u>BleepingComputer's</u> <u>forum</u> I asked to the affected users to check their own firmwares and trying to grab the malware. Someone did and shared the ELF on VirusTotal.

Thanks to Michael Gillespie @demonslay335 I was able to have a copy of that sample. Hash: 9a1de00dbc07271a27cb4806937802007ae5a59433ca858d52678930253f42c1 (very few) years ago I had experience on some router exploiting and reversing (Italian ISP company named Telecom Italia and their ADSL routers), they were based on MIPS with a very good OS (Jungo OpenRG) always trivial to exploit. But this is another story, I'lve spent a lot of time on those devices learning some useful stuffs which today apparently become a good knowlege.

Since the fact that this ransomware is stripped (with removed debugging informations!) and statically compiled, the static analysis is very hard to do since the fact that any calls appear to be just a sub_XXXXX because of the stripped ELF.

Because of this, we have few options to make our life less complicated:

- 1) do a dynamic analysis
- 2) create IDA pro FLIRT signatures

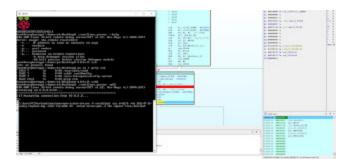
Starting from the first point we faced a new problem: where to run the ARM malware? 2 opportunities: the first on a QEMU VM, the second on a D-Link device (of course IoI). I do not buy D-Link stuffs, so I had only one opportunity: QEMU. Since I'm Iazy (and the executable is statically linked), I decided to try with my Kali x64 VM and qemu-static-arm with -g parameter which enable the gdb debugger. I really dont know why, but something go wrong bringing ida pro to crash. LOL 😔

It was a fail, so I've started to look at a new easy path and I thought about raspberry pi. On Sourceforge there is a nice prebuild, preconfigured QEMU Raspberry emulator: https://sourceforge.net/projects/rpiqemuwindows/

On the run.bat file I've added a parameter to be able in order to upload with FileZilla over sftp protocol the malware and the remote debug server, and then killing the sshd, I've used the same port to connect with IDA. Smart lazyness

qemu-system-arm.exe -M versatilepb -cpu arm1176 -hda 2012-07-15-wheezy-raspbian.img - redir tcp:2200::22 -kernel kernel-qemu -m 192 -append "root=/dev/sda2"

Starting again the IDA Pro remote debugging, the following stuffs comes up!!!!! YEAH IT WORKS!!!! ******



So far we know few things about such ransomware which are:



in addition, the strings shows up that he also use crypto routines from Libsodium library https://libsodium.gitbook.io/doc/

Usage	Append for
<pre>Hetalationation(b) Hetalation(b) If (parket, bit()) = -0 () If (parke</pre>	$ \begin{array}{l} \inf_{i=1}^{n} \inf_{i \in I} \phi_{i} \phi_{i}^{(i)} \\ \inf_{i=1}^{n} \bigoplus_{i=1}^{n} \phi_{i}^{(i)} \phi_{i}^{(i)} \\ \inf_{i=1}^{n} \bigoplus_{i=1}^{n} \phi_{i}^{(i)} \phi_{i}^{(i)} \\ \inf_{i=1}^{n} \bigoplus_{i=1}^{n} \phi_{i}^{(i)} \phi_{i}^{(i)} \\ \inf_{i=1}^{n} \phi_{i}^{(i)} \\ \inf_{i=1$
suction. In the only header that has in to included. The Maray In called isotrow (see -Loottow to link 4), or obtained using large-carity on systems where it is reals	
 cmutet-lipig-coeffgcflags-limastras) utilitati-lipig-coeffgClin-limastras) 	1
For static linking, Waxel Studie usem should define : soon required an other platforms.	(a) (00000000000000000000000000000000000
Projects using DMale can include the Tindaudium cmale	1

kddress.	Length	Type	2 ring
	000000000	С	systemlie
	00000005	c	ntu
	00000012	C	file is encrypted
.odata/000	00000016	C	file is not encrypted
official and a second second	00000017	e	sodur
.rodete:000	00000008	C	protey
	00000007	C	publicy
.rodatarono.	000000122	C	encrypting using public keys healty's
opportation 2	00000023	C	decrypting using private keyr. Yurk to
.000x4sbor. 2	00000007	C	donely'm
	00000009	С	Nes_Prog
	00000009	C	وبغرصك
	00000018	c	_or totals_support.txt
000vatabon.	00000010	С	FILELENCI/PTED_REACHE.IM
	00000016	C .	ur tottotut
	00000013	C	pringel, other states
oportation a	00000004	C	prot_hex
	00000008	C	wy.bectlin
nedata-000	00000008	с	. Julie .c.
	00000004	c	hex
vodete:000	000000112	C	errors his 2hes maloc could not alocate memoryly ly-
.odata:000	00000011	C	error berzhewig to
	000000000	C	(Na) (Na)/vie
nodeta:000	00000018	c	brien_senty == binten
.rodete:000	00000018	c	involutions values Nuclean
rodete:000	00000019	C	invalid seed size: Navily's
.codata:000	00000005	C	seed
rodetar000_	00000023	C	error opening the for reading, it in
	00000022	C	error opening 'No for writing, Is'm
vodete:000.	00000014	C	error opening file:
vodeta:000	00000005	C	Settin
	00000008	c	0.640
odete:000	00000007	C	Ne.http
rodete:000_	00000010	C	encrypted: Nehrin
rodete:000.	00000008	C	do demot
vodetac000	00000038	C	message conjupted or not intended for this redpants %w/y/m
x rodata:000_	00000004	C	%e.outino
vodete:000_	00000014	C	incomplicite header's in
rodete:000_	00000012	C	completi drunkirim
vodete:000.	00000044	С	prenature and (and of file reached before the and of the stream)/r/n
vodeta:000_	00000010	C	dectypated: %ely/in
rodetac000	00000000	C	
odets:000	00000009	c	ret == 0
	00000018	C	prve2553/heaths20ady1385

Like I said before, the - hardest - next step is to create a IDA FLIRT signature, by cross compiling some example from Libsodium repo (hoping that it will use the same functions as the malware), extract the signatures by using FireEye idb2pat tool https://www.fireeye.com/blog/threat-research/2015/01/flare_ida_pro_script.html to have an understandable static analysis to MAYBE retrive the private key and decrypt the files, or at least have a reduced keyspace to make possible a brute force attack.

Follow me on Twitter and I'll keep you updated. Cheers RE Solver