Malware Must Die!

Semper legerent "Salve Regina" ante venatione malware

Sunday, November 22, 2015

MMD-0044-2015 - Source code disclosure (part1) of bunch of ELF malware

MalwareMustDie,NPO is a white-hat non-profit security research workgroup launched in August 2012 for/by security professionals and malware researchers gathered to form a work-flow to reduce malware infection in internet. In this opportunity I, hereby, on behalf of the active projects and field operational ELF malware researches, am sharing first series of ELF malware source code collected in action and secured in 2015, wrapped in a form of RAR(version 5) password-archive, with its further additional.

As per internally decided, we are now having new scheme of sharing malcodes, to reduce the unwanted access to the archive, the file was uploaded to the virus total with the hash of:

```
SHA256 (ELF-malware-in-C-leaks.rar)
43a383bb8b2fa799a0a06a585c52e91f6ea1c877bba12c21e691e32a99f9adf4
```

The password has a high character count and the archive was built in a way to avoid brute. You can receive the password by commenting this post with informing your current active email address and the detail of which **known** security entity you are actually working with (or anti-viruses entities, or law enforcement research agencies, or government related interet security incident response & research teams, i.e: SOC/CERT/CSIRT, as entities allowed t receive these code) and the comment will not be published to the public (feel free to test it first).

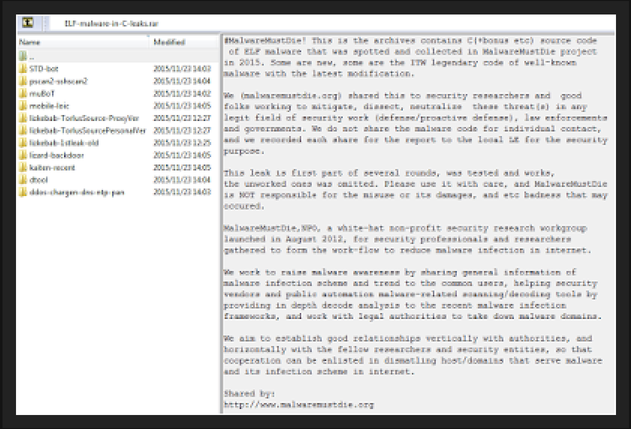
We will check each request and not sharing the password to unknown individual/independent contacts without clear confirmed information/identification of who they are. These are malware source codes and not malware samples nor toys to play with, it is a very dangerous material to be passed to wrong hands. Please bear with the slowness in response due to the check process and due the fact that we are a non-profit organization, with limited resources and only active in our spare time.

The archive will stay online for two months, after that period we won't share it anymore and will delete our files. Don't request the code after this time has passed. We are not responsible to any of damage that will occur due to the misuse of the shared material, please read our Legal Disclaimer and Sharing Guide for more information-->[here]

What can be achieved by these source code are:

```
- better mitigation of the leaked ELF botnet specific type/variants
- several hard coded leads for prevention of DDOS attack methodology used t
o research
- several exploitation research that can be produced and implemented by eac
h ELF botnet
- you may publish research of these code(s), on a condition: mention us, #M
alwareMustDie.
  (we did the hard part in achieving, collecting, selecting, testing and sh
aring -
   these codes, for free)
```

Below is the snapshot of the original archive, that you will see after you open it correctly.
The total codes shared in this part is 21 (twenty one) source code, all in C except one bonus in html.



ELF-malware-in-C-leaks.rar

Name	Modified
..	
STD-bot	2015/11/23 14:03
pscan2-sshscan2	2015/11/23 14:04
muBoT	2015/11/23 14:02
mobile-leic	2015/11/23 14:05
lizkebab-TorlusSource-ProxyVer	2015/11/23 12:27
lizkebab-TorlusSourcePersonalVer	2015/11/23 12:27
lizkebab-1stleak-old	2015/11/23 12:25
lizard-backdoor	2015/11/23 14:05
kaiten-recent	2015/11/23 14:05
dtool	2015/11/23 14:04
ddos-chargen-dns-ntp-pan	2015/11/23 14:03

```
#MalwareMustDie! This is the archives contains C(+bonus etc) source code
 of ELF malware that was spotted and collected in MalwareMustDie project
in 2015. Some are new, some are the ITW legendary code of well-known
malware with the latest modification.

We (malwaremustdie.org) shared this to security researchers and  good
folks working to mitigate, dissect, neutralize  these threat(s) in any
legit field of security work (defense/proactive defense), law enforcements
and governments. We do not share the malware code for individual contact,
and we recorded each share for the report to the local LE for the security
purpose.

This leak is first part of several rounds, was tested and works,
the unworked ones was omitted. Please use it with care, and MalwareMustDie
is NOT responsible for the misuse or its damages, and etc badness that may
occured.

MalwareMustDie,NPO, a white-hat non-profit security research workgroup
launched in August 2012, for security professionals and researchers
gathered to form the work-flow to reduce malware infection in internet.

We work to raise malware awareness by sharing general information of
malware infection scheme and trend to the common users, helping security
vendors and public automation malware-related scanning/decoding tools by
providing in depth decode analysis to the recent malware infection
frameworks, and work with legal authorities to take down malware domains.

We aim to establish good relationships vertically with authorities, and
horizontally with the fellow researchers and security entities, so that
cooperation can be enlisted in dismetling host/domains that serve malware
and its infection scheme in internet.

Shared by:
http://www.malwaremustdie.org
```

I think I will see how this first part of the new scheme of sharing goes with studying the negative

About #MalwareMustDie!

Since malware and its evolution is becoming the serious threat in our internet and computer industry. We are now coming to the stage to admit the fact that malware is actually "winning" this longest 15+ years historical "battle" by keep on its existence, infecting and lurking us....[Read More]

Links

- Home Page
- RSS Feeds
- News Search
- Video Demonstration
- MMD Google Code (Tools, Wiki)
- Analysis DropBox & Samples
- Our Full Disclosure Pastebin
- Disclaimer & Sharing Guide
- Malware Dismantling Ops
- Follow & Contact us in Twitter

Search This Blog

Search

Blog Archive

Blog Archive

DropBox: Send your sample!

OPEN

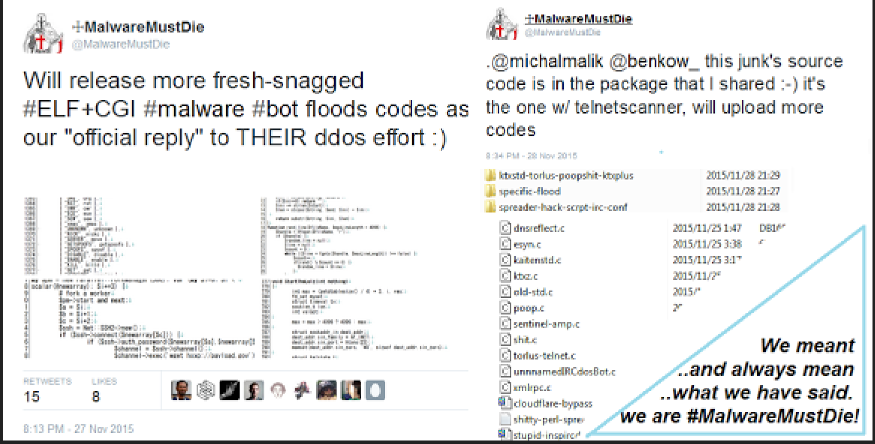
Recent Posts

- MMD-0044-2015 - Source code disclosure (part1) of bunch of ELF malware
- MMD-0043-2015 - Polymorphic in ELF malware: Linux/Xor.DDOS
- MMD-0042-2015 - Hunting Mr. Black IDs via Zegost cracking
- MMD-0041-2015 - Reversing PE Mail-Grabber Spambot & its C99 WebShell Gate
- MMD-0040-2015 - Dissecting & learning about VBE Obfuscation & AutoIt Banco Trojan

aspects for it, if things go well, for the next part (part 2 of sharing) will be focusing on the share on source codes for the ELF threats codes that is collected from some "specific" regions :-)

Additional ELF malware source code..

As per mentioned below:



✝MalwareMustDie
@MalwareMustDie

Will release more fresh-snagged #ELF+CGI #malware #bot floods codes as our "official reply" to THEIR ddos effort :)

RETWEETS 15 LIKES 8

8:13 PM - 27 Nov 2015

✝MalwareMustDie
@MalwareMustDie

.@michalmalik @benkow_ this junk's source code is in the package that I shared :-) it's the one w/ telnetscanner, will upload more codes

8:34 PM - 28 Nov 2015

```
ktxstd-torlus-poopshit-ktxplus   2015/11/28 21:29
specific-flood                   2015/11/28 21:27
spreader-hack-scrpt-irc-conf     2015/11/28 21:28
dnsreflect.c                     2015/11/25 1:47
esyn.c                           2015/11/25 3:38
kaitenstd.c                      2015/11/25 3:1
ktxz.c                           2015/11/2
old-std.c                        2015/
poop.c                           2
sentinel-amp.c
shit.c
torlus-telnet.c
unnnamedIRCdosBot.c
xmlrpc.c
cloudflare-bypass
shitty-perl-spre
stupid-inspirc
```

This is the additional's share with the same method & the arvhive was uploaded to virus total with hash:

```
SHA256 (mmd-extra.7z)
9464b4443d4ce19977d774bddf4b1987c4e090f1ac4ccb80d534e0e593a2b41c
```

it's using a different long-password, you can ask for it by the same scheme.

PS: This (below) action will be executed as response of a further attacks from the shared source codes malware bad actors :-)

✝MalwareMustDie
@MalwareMustDie
Follow

Go ahead #DDOS us more & we put EACH #ELF BOTNET #EXPLOIT to be uploaded in #METASPLOIT soon :) #WeMeantWhatWeSaid twitter.com/MalwareMustDie…

9:32 PM - 28 Nov 2015

15 12

Cheers from #MalwareMustDie

Posted by unixfreaxjp at 10:43 PM

G+1 Recommend this on Google

No comments:

Post a Comment

Enter your comment...

Comment as: ggyy (Google) Sign out

Publish Preview □ Notify me

Home Older Post

MMD-0039-2015 - ChinaZ made new malware: ELF Linux/BillGates.Lite

MMD-0038-2015 - ChinaZ and ddos123.xyz

MMD-0037-2015 - A bad Shellshock & Linux/XOR.DDoS CNC "under the hood"

MMD-0036-2015 - KINS (or ZeusVM) v2.0.0.0 tookit (builder & panel source code) leaked.

MMD-0035-2015 - .IptabLex or .IptabLes on shellshock.. sponsored by ChinaZ actor

MMD-0034-2015 - New ELF Linux/DES.Downloader on Elasticsearch CVE-2015-1427 exploit

MMD-0033-2015 - Linux/XorDDoS infection incident report (CNC: HOSTASA.ORG)

MMD-0032-2015 - The ELF ChinaZ "reloaded"

MMD-0031-2015 - What is NetWire (multi platform) RAT?

MMD-0030-2015 - New ELF malware on Shellshock: the ChinaZ

China ELF botnet malware infection & distribution scheme unleashed

MMD-0029-2014 - Warning of Mayhem shellshock attack

MMD-0028-2014 - Fuzzy reversing a new China ELF "Linux/XOR.DDoS"

MMD-0027-2014 - Linux ELF bash 0day (shellshock): The fun has only just begun...

Tango down report of OP China ELF DDoS'er

MMD-0026-2014 - Router Malware Warning | Reversing an ARM arch ELF AES.DDoS (China malware)

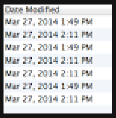
Another country-sponsored #malware: Vietnam APT Campaign

A protest! What's bad stays bad. Legalized any badness then you'll ruin the faith..

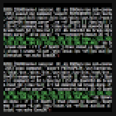
MMD-0025-2014 - ITW Infection of ELF .IptabLex & .IptabLes China #DDoS bots malware

MMD-0024-2014 - Recent Incident Report of Linux ELF (LD_PRELOAD) libworker.so malware attack in Joomla! VPS

Most read analysis



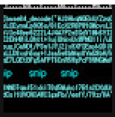
MMD-0020-2014 - Analysis of infection ELF malware: libworker.so - A shared (DYN) malicious library by LD_PRELOAD



MMD-0028-2014 - Fuzzy reversing a new China ELF "Linux/XOR.DDoS"

How EVIL the PHP/C99Shell can be? From SQL Dumper, Hacktools, to Trojan Distributor Future?

Subscribe to: Post Comments (Atom)

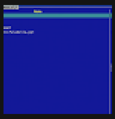


The Evil Came Back: Darkleech's Apache Malware Module: Recent Infection, Reversing, Prevention & Source Details

Threat Intelligence - New Locker: Prison Locker (aka: Power Locker ..or whatever those bad actor call it)

MMD-0036-2015 - KINS (or ZeusVM) v2.0.0.0 tookit (builder & panel source code) leaked.

China ELF botnet malware infection & distribution scheme unleashed



A journey to abused FTP sites (story of: Shells, Malware, Bots, DDoS & Spam) - Part 1

MMD-0027-2014 - Linux ELF bash 0day (shellshock): The fun has only just begun...

What Serenity Exploit Kit dropped? A Spambot Full Analysis & Samples

Subscribe To

Posts

Comments