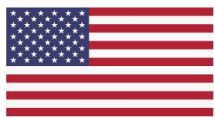


This computer contains pirated software and has been blocked by ICE-Homeland Security Investigations.



Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a \$250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)

As a first-time offender you are required by law to pay a fine of 500 USD

If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities. You will be charged, fined, convicted for up to 5 years.

How to pay a fine? There are two ways to pay a fine:

1.You can pay the fine online through BitCoin. BitCoin is available nationwide.

Click the tabs below to find the nearest vendor. Your computer will be unlocked after the payment is made.

2.(Offline Option) You can come to your local courthouse and pay the fine at the 'Cashiers' window.

A special restoration software will be sent to you by mail within a week after the payment is made.

To regain access now transfer BitCoins to the following address (click to copy):

1NdR8tEKRB0QioiyAPhpuks9Uct6XtEdW

After the payment is finalized enter Transfer ID below.

Amount: Transfer ID:

BTC 1.773

PAY FINE

Note: All files on this computer have been encrypted with a strong symmetric algorithm and a 4096-bit key. Files will be inaccessible until the fine is paid.

Attempt to remove this message will result in irreversible damage to your files, hardware and Windows installation.

[View encrypted files](#)

[Payment](#)

[BitCoin Information](#)

[BitCoin Exchanges](#)

[BitCoin ATMs](#)

[Internet Browser](#)

[Notepad](#)

Project Global 3 is a coordinated effort by U.S., Canadian, European, Australian, New Zealand and other law enforcement agencies across the globe targeting computers with pirated content and their operators.

ECryptolocker

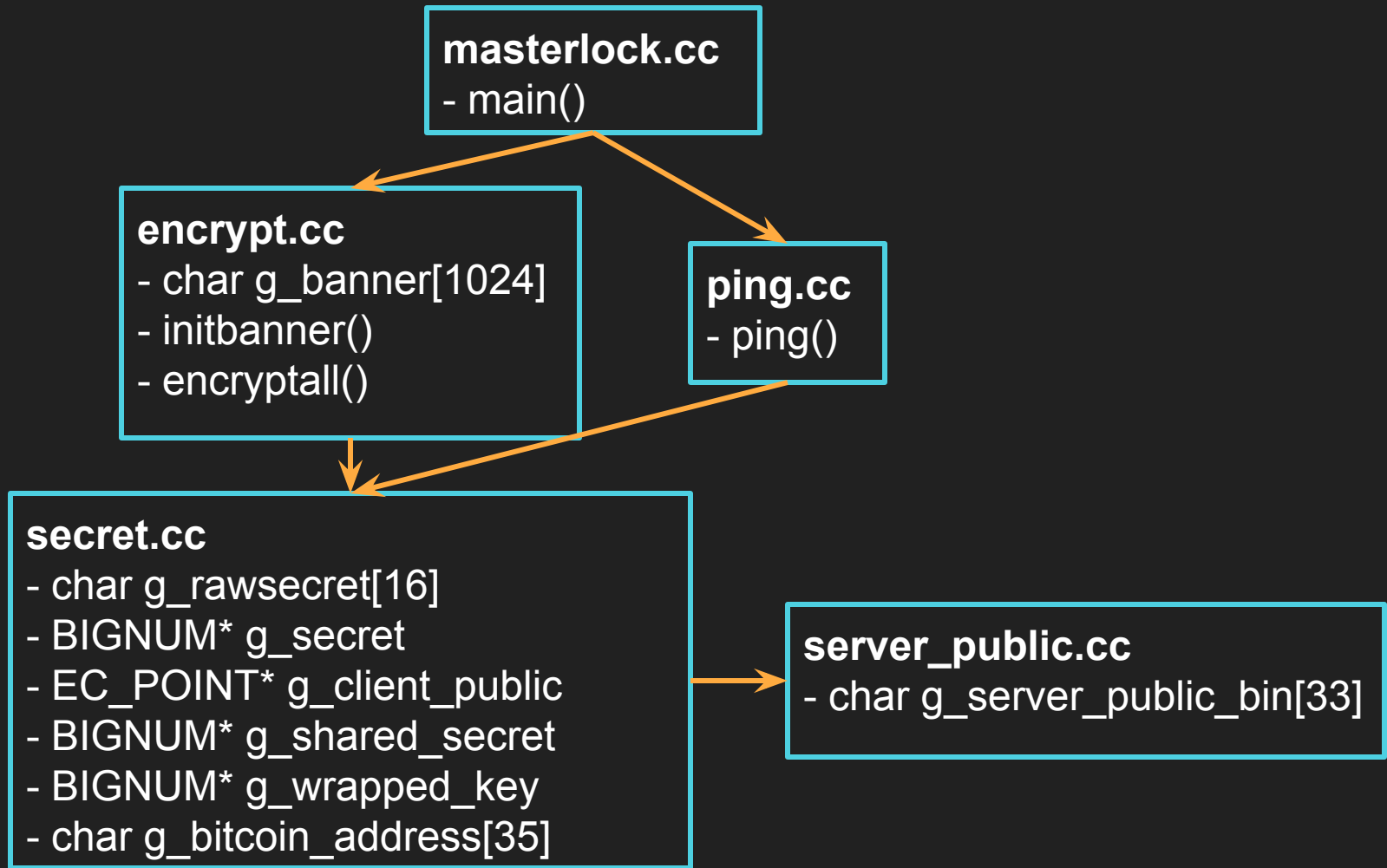
Montréhack 2015/10/19

Catalin Patulea

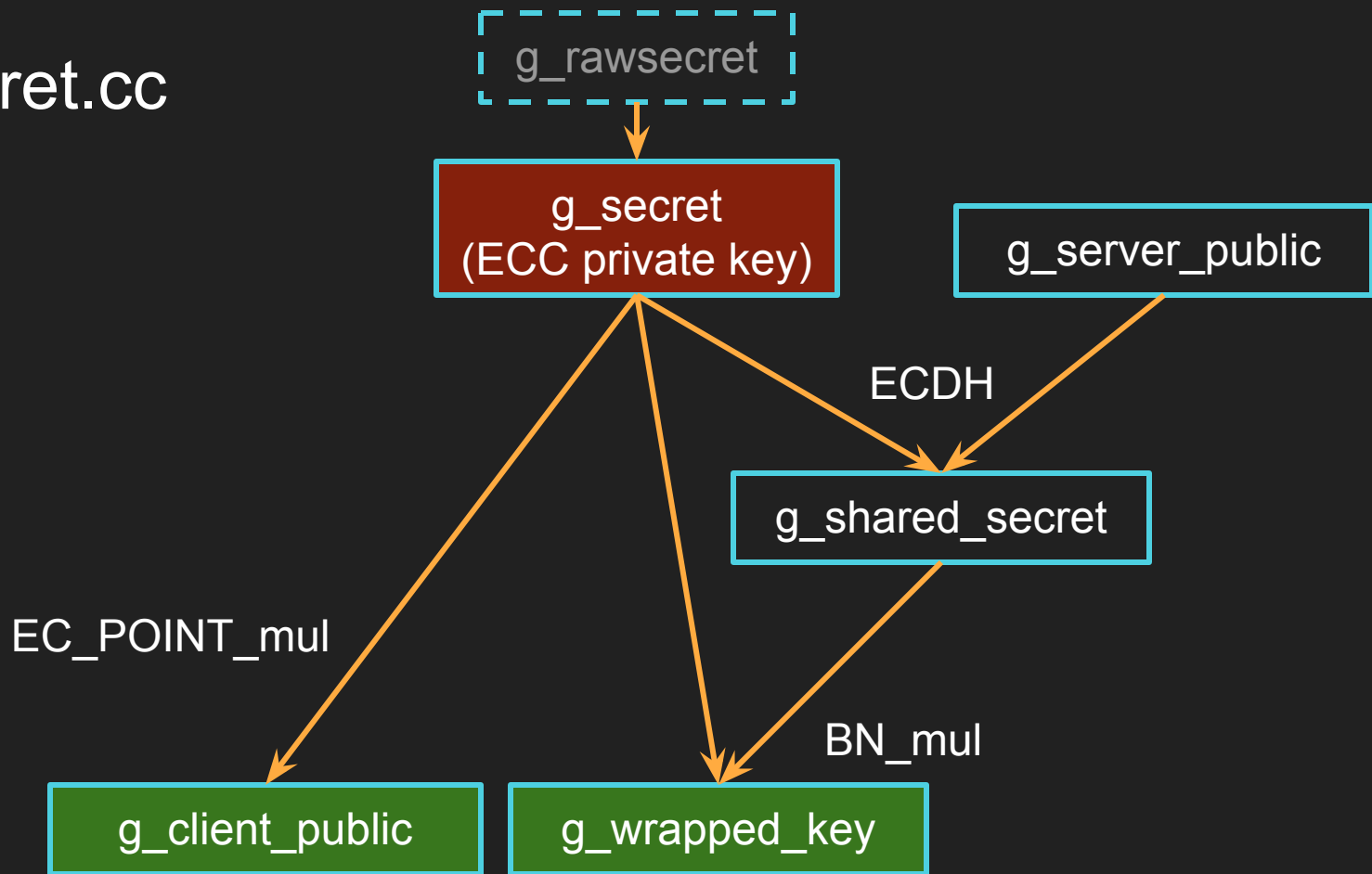
<http://github.com/cpatulea>

<http://tinyurl.com/montrehack-20151019>

< 5 minutes de calcul



secret.cc



g_wrapped_key

g_secret * g_shared_secret = **g_wrapped_key**

128 bits * 256 bits = 384 bits

a * b = 0x0636...61BC

$p_0 p_1 p_2 p_3 \dots$ = n

ex. $a = p_0 p_2 p_3$ $b = p_1 p_4 p_5 p_6$

Factorisation

Techniques

Pollard's rho (ρ): $< 2^{64}$ (38 chiffres)

Lenstra elliptic curve factorization
(ECM): < 80 chiffres

Quadratic sieve (MPQS): < 100 chiffres

General number field sieve (GNFS):
 > 100 chiffres

Outils

GNU factor (ρ)

Python primefac (ρ , ECM, MPQS)

pyecm (ECM)

msieve (MPQS, GNFS)

ggnfs (GNFS)