Unveiling the Locker Bomba (aka Lucky Locker v0.6 aka Lyposit/Adneukine)

malware.dontneedcoffee.com/2013/05/unveiling-locker-bomba-aka-lucky-locker.html

2013-05-21 - Affiliate

On the 10th of may was advertised on underground forum by bomba_service a new Ransomware in Affiliate mode.

LOCKER BomBa best service - максимальный заработок

Bomba Locker advert

Original Text

LOCKER BomBa best service - максимальный заработок
В связи с унылой ситуацией на рынке локеров, мы предлагаем вам уникальное решение - BomBa локер, наш проект направлен на совместный заработок в течении длительного времени, мы предлагаем активную помощь адвертам и решение всяческих ситуаций, всегда открыты к диалогу - и новым направлениям!В партнерку будут набраны 10-20 активных адвертов, после чего она перейдет в приватный режим.

========== ==========
Некоторые технические данные:

+++ методы обхода UAC от висты до W7, 0-day
+++ метод загрузки локера из памяти(минуя диск), 0-day
+++ динамическая подмена минипорт-драйвера жесткого диска
+++ сокрытие/подмена данных на диске на уровне подмены секторов
+++ инжект в процессы, также локер использует всевозможные методы закрепления в системе - от самых простых до извращений, практически не удалим(даже в AB отчетах - рекомендация - формат диска и переустановка системы - понятно что не всех такое устроит, чем мы и воспользуемся)
+++ защищенный проверенными алгоритмами протокол обмена бот-сервер (казалось бы локер - но ип после прогруза более 50к тестовых
ботов - остался 0/34)+ коды в панель отправляются не по стандартной схеме(комерческая тайна), идут до 7 дней активно, бывали случаи даже после 20 суток бот вводил валидный код(после долгих попыток ввода невалида)
+++ используется хитрая система установки локера - не тупой запуск сразу(таким образом ваши порно ресурсы остануться чистыми бесконечно долго

- Полезная штуки: Крутые лендинги многократно протестированные на трафике различных направлений, и постоянное их измения - под новые тренды в этом направлении для максимальной прибыли.
- Размер exe(не сжатый): 70 Кб
- Написан на: C++/ASM
- Работает на след. OS: Вся линейка Windows начиная от Windows 98 и до Windows 7(локер был протестирован на всевозможных вариациях ОС, от ограниченной до pro, включая x32 и x64 версии)
- Отстук с трафа - 80%
========== ==========
Поддерживаемые локером Страны:
US|DE|IR|CH|ES|AT|BE|FR|PL|DK|PT|CA|IT|NL|RO|SE|UK |TR|RO|LV (20 стран)
========== ==========

Антивирусы
Были установлены максмимальные версии(самые дорогие) антивирусов, скачаны и обовлены актуальные базы, и выставлен самый высокий уровень безопаности, после чего был осуществлен запуск локера, была проверена отправка кодов (ничего не блокируется)
Обходы АВ:
AVAST - OK
Microsoft - OK
Avira - OK
ESET - ok
Symantec - ok
AVG - ok
Kaspersky - ok
McAfee - ok
Trend Micro - ok
Panda - ok

Обходы Фаерволов
комодо - ок
битдеф - ок
оутпост - ок
нортон - ок
== =========
Это более 90% от всех тачек, как правило у большинства юзеров стоит какой либо АВ, и пробить его это еще полдела - необходимо чтобы локер нормально установился и смог отправить коды.BomBa локер справляется с этим максимально эффективно. Учитывая все вышесказанное, без преувелечения могу сказать что BomBa локер лучшее решение доступное сейчас на рынке, кто не верит - можно устроить показательные тесты.
== =========
Рейтинги:
до 1к лоадов в сутки - ваши 60% от полученных чеков
до 3к лоадов в сутки - ваши 70% от полученных чеков
до 10к лоадов в сутки - ваши 80% от полученных чеков
от 10к лоадов в сутки - ваши 90% от полученных чеков
== =========
Супер возможности:
1)В наличие множество старых аков бирж (от 1 до 5 лет реги с историей покупок и продаж - все аки переданы адалт мастерами либо были регнуты в те годы) это позволяет избежать ограничений наложенные на новые акаунты + техники слива и методы работы по каждой из бирж(как что палит где и тп) - эту возможность надо

спрашивать у сапорта - он передаст запрос админу(имеет смысл подавать заявку если у вас есть большой опыт работы и не надо особо ничему обучать - только грамотно направить) все условия обговриваются при личном общении.

2) Возможно выдача системы по скрытию трафика от любой адалт биржи(все через наш сервер), можно сливать даже с трафикхолдера хоть и коверт оттуда никакой.все сугубо индивидуально - обговаривается через админа сервиса - контакт брать у сапорта.

3) Выдаем связку - не всем, а только трудолюбивым адвертам.(кол-во трафа и ваше адекватность - главные факторы)

Контакты сапорта -
http://bomba .asia

Translated by @Malwageddon (Thanks !!) :

LOCKER BomBa: Best service - maximum earnings

Due to Lockers market being dull at the moment, we are glad to present you - Bomba Locker. Our goal is to have long term relationship partners to share the earnings with. We offer active help to adverts and flexible support. We are always open to a dialog on new ideas. We're looking to partner with 10-20 adverts at the moment and after that any further partnership discussions will only be done privately.

=== =========
Some of the key features:

+++ UAC bypass - works on Vista through to Windows 7, 0-day
+++ loading the locker from the memory(not using the disk), 0-day
+++ dynamic HDD miniport driver replacement
+++ HDD sector level data hiding/replacent
+++ process injection, the locker is using variety of method to attach itself to the system - from simple to most sofisticated ones. Almost impossible to delete (even AV vendors recommend reformating the disk and reinstalling OS if infected with our locker - of course it's not a desirable solution for many people, so we use it in our advantage)
+++ bot-server communications are protected/encrypted(test IP hasn't been blacklisted even after testing with 50K+ bots). Not using any standard schemes to send codes to the panel(our own 'Know How'). Normally, it takes upto 7 days for bots to send in a valid code, but we've seen cases where 20 days later bots were sending valid codes after many invalid entering attempts.
+++ using tricky locker deployment method - not just simply starting it up immediately(in this way your servers will stay 'clean' longer)

- Useful features: Amazing lendings stress tested with different type of traffic. Constant upgrades to faclitate any new trends to maximize the earnings.
- EXE file size (not compressed): 70 Kb
- Written in: C++/ASM
- Works on the following OS': All Windows starting from 98 to Windows 7(the locker was tested on all possible versions - 'core' and upto 'pro' editions including x32 and x64 versions)
- Callback - 80%
=== =========
Countries supported by the locker:
US|DE|IR|CH|ES|AT|BE|FR|PL|DK|PT|CA|IT|NL|RO|SE|UK |TR|RO|LV (20 in total)
=== =========
AntiVirus products
Tested with the latest versions of AntiVirus software - all patched and updated. The locker was launched with AV software set to the maximum security level. Tested sending the codes to the panel - nothing is being blocked.
AV evasion:
AVAST - OK
Microsoft - OK
Avira - OK
ESET - ok
Symantec - ok
AVG - ok
Kaspersky - ok
McAfee - ok
Trend Micro - ok
Panda - ok

Firewall evasion:
Comodo - ok
BitDefender - ok
Outpost - ok
Norton - ok
== =========
In more than 90% of the cases, users have some AV software installed and to evade it is only half of the work - the locker has to be properly installed and verified to be able to send the codes. Bomba Locker handles it quite effectivelly. Taking all of the above into concideration and without any exaggeration I can assure you that Bomba Locker is the best product currently available on the market. Product demonstration can be arranged if any further prove is required.
== =========
Rates:
upto 1K loads in a day - you get 60% from the earnings
upto 3K loads in a day - you get 70% from the earnings
upto 10K loads in a day - you get 80% from the earnings
from 10K loads in a day - you get 90% from the earnings
== =========
Super features:

1)We have many old stock accounts (from 1 to 5 years registration and trade history - all accounts have either been handed over to us by 'veterans' or registered back than) - it allows us to avoid any limits applied on the newly opened accounts. Also, we have timeprooved methods of fund withdrawal specific to each stock - this feature can be requested from the admin through our support(only submit the requests if you have previously worked in this area and do not require any training). All details and conditions are discussed individually in private.

2)We can provide adult traffic hiding systems(through our server only). We can pull traffic from traffic holders even though the convert rate is quite low there. Any specific individual requests can be addressed to service administrator - contact details can be requested from support.

3) We can supply EK - available for most productive adverts only(traffic volumes and being adequate - are deciding factors here).

Support -
http://bomba .asia

As you can see there is also a web site associated

Website promoting Locker Bomba

It took few hours to spot something new and that could be related.
Pushed in a rented blackhole :
199.180.114.213 namesrootslist .net - Landing : /building/aim-circuit-proposing.php
I fond that sample : 31efd51e5c31ea38a30ebd9d005575beThe User-Agent and C&C call were familliar :

User-Agent and C&C Call Lyposit-ish

Like Lucky Locker (which is Lyposit v0.1 and Adneukine - v0.2) ...but no lock screen (!?).
So I wait...wait (> 10 min) till i got :

German Design for Bomba Locker / Lyposit
(which is the same as Nymaim based on Urausy...itself inspired by Reveton June 2012)

Here are all other available looks like the German design except the US one.

All known Bomba Locker/Lyposit Design as of may 2013

TR = US Design

IR (read IE :D) like BE, CH, PL and DK show Blank screen like that :

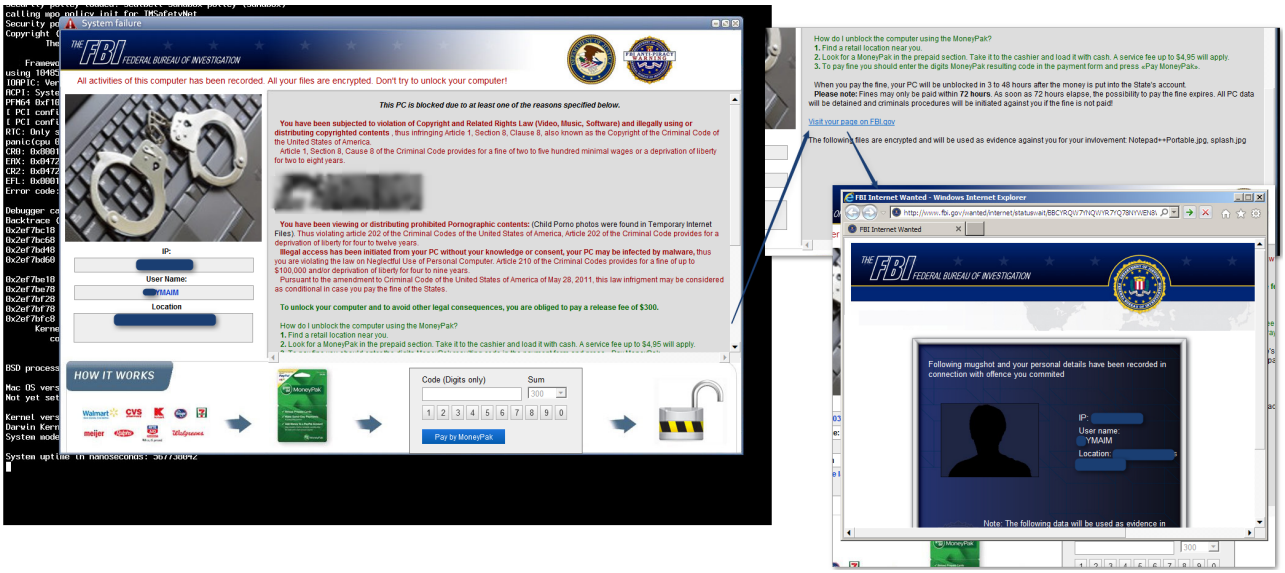
IE (!=IR) CH, BE, PL DK design... sic

The US Design is like :

Bomba Locker/Lyposit US Design

This design has already been seen in Uremtoo (Urausy variant) in February

and in Nymaim (but is a little more evolved there)



Nymaim US design

Out of topic:

I did not wrote about Nymaim for now but it's related to the /Home/ BHEK (which evolved to q.php BH EK which was behind the LA Times infection and is getting traffic via Darkleech apache Module)

That C&C is pushing junk instead of 404 the same way Lucky Locker C&C was...

Trash Data instead of 404

And here is the piece of code behind that on previous version of Lyposit :

C&C Side code used to push trash

As the Advert for Lucky Locker is not available anymore it seems we had here a good candidate for this "new" locker.

And..tada! I've find a way to get a screenshot of the Admin Panel for Bomba Locker :

Bomba Locker Panel
(same as Lucky Locker but v0.6)
IP is not blurred -> QED

And as a conclusion for those wondering what is the 0day UAC bypass on Windows 7

0day UAC Bypass :)

File :

Here (Owncloud via goo.gl) contains : 31efd51e5c31ea38a30ebd9d005575be
https://malwr.com/analysis/ZjE5NmVlNjgxOTFlNGM5ZGIzZDAzYWFiYzVjNDE2YjE/

Read More :

Lockscreen Win32:Lyposit displayed as a fake MacOs app - 2013-05-20 - Avast - Peter Kálnai
Inside view of Lyposit aka (for its friends) Lucky LOCKER - 2012-11-29