Top prevalent malware with a thousand campaigns migrates to macOS

research.checkpoint.com/2021/top-prevalent-malware-with-a-thousand-campaigns-migrates-to-macos/

July 21, 2021

July 21, 2021

By: Alexey Bukhteyev and Raman Ladutska

From a simple keylogger to a top prevalent malware

Formbook is currently one of the most prevalent malware. It has been active for more than 5 years already. Check Point reported in December 2020 that Formbook affected 4% of organizations worldwide and made it to the top 3 list of the most prevalent malware.

According to AnyRun Malware Trends Tracker, Formbook occupies the 4th place in a list of the most prevalent malware families in 2020.

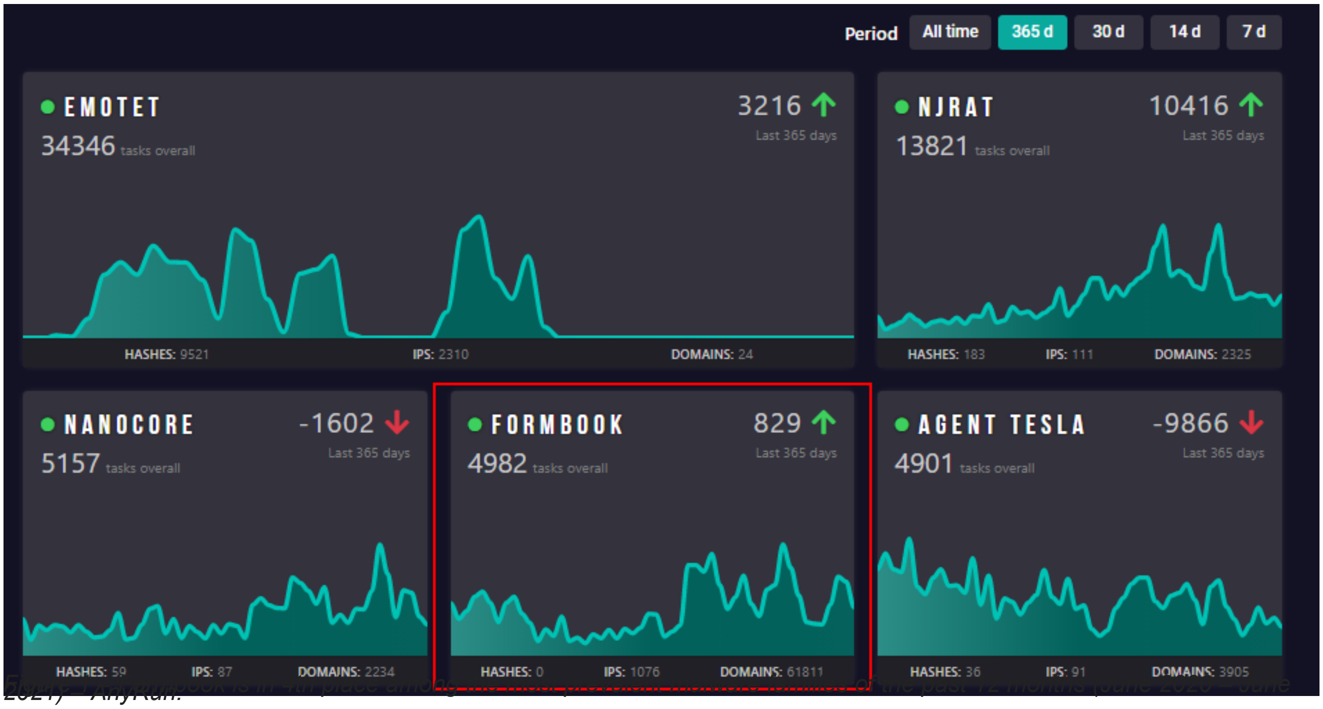


Figure 1: Formbook is in 4th place among the most prevalent malware families of the past 12 months (June 2020 – June 2021) – AnyRun.

Formbook is an Info Stealer that harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to the orders received from Command-and-Control (C&C) servers. The code is written in C with assembly inserts and contains a number of tricks to make it harder for researchers to analyze it.

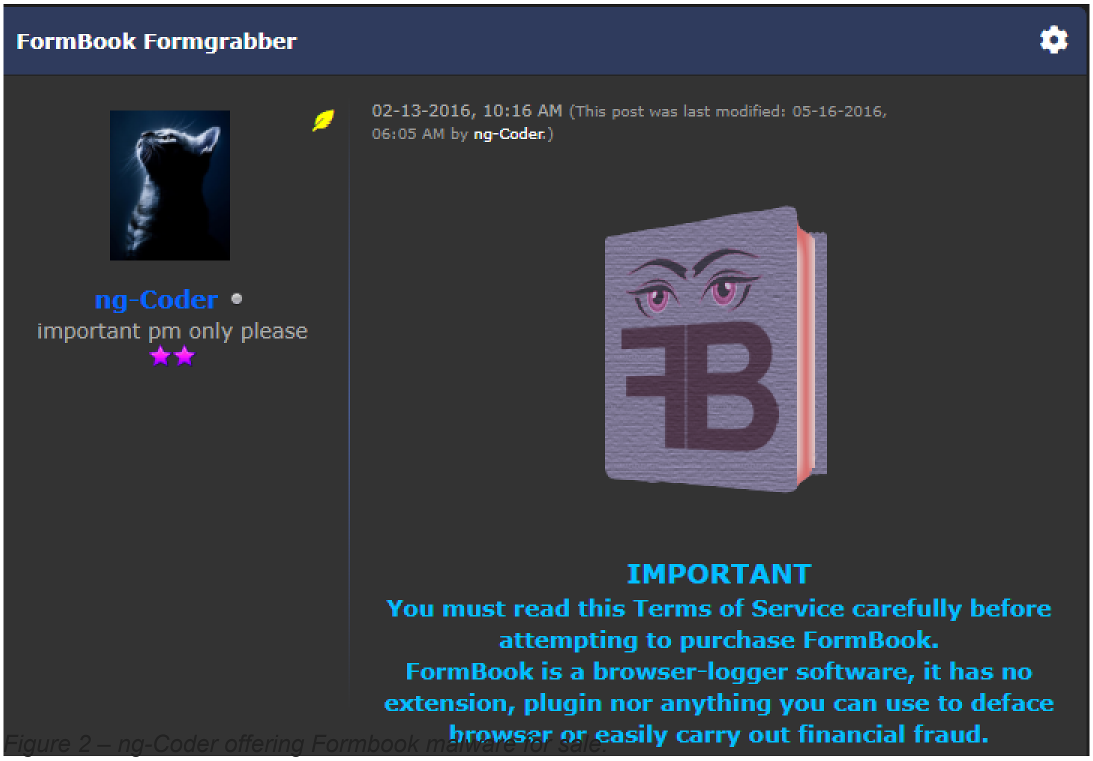
As stated by its author, Formbook was intended to be “a simple keylogger.” However, customers immediately saw its potential as a universal tool for use in broad spam campaigns that target organizations all over the world. As this potential became a reality, the author stopped sales of the product without giving detailed explanations about the motives behind this decision.

A short time later, Formbook was reborn as **XLoader**, and the malware is now available for sale in the underground forum by a different avatar. XLoader opened up several new opportunities, with the ability to operate in the macOS being one of the most exciting. XLoader’s story is on-going, and judging by the popularity of the malware, shows no signs of ending any time soon.

Let’s take a look at how it all began.

Formbook: unintended popularity

A post offering the earliest version of Formbook (what we could call a beta-version) for sale appeared on the underground forum on February 13, 2016.



FormBook Formgrabber

ng-Coder

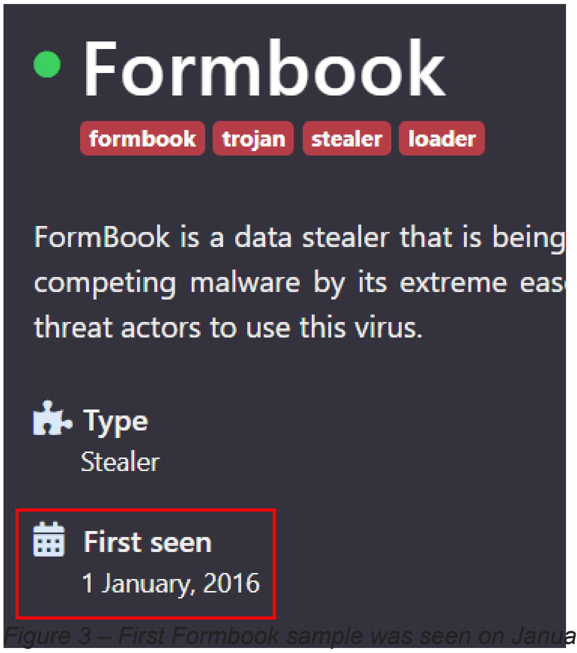
important pm only please

02-13-2016, 10:16 AM (This post was last modified: 05-16-2016, 06:05 AM by ng-Coder.)

IMPORTANT
You must read this Terms of Service carefully before attempting to purchase FormBook.
FormBook is a browser-logger software, it has no extension, plugin nor anything you can use to deface browser or easily carry out financial fraud.

Figure 2 – ng-Coder offering Formbook malware for sale.

Although the first sales thread appeared on February 13, 2016, Formbook samples were seen earlier as evidenced by AnyRun:



Formbook

formbook trojan stealer loader

FormBook is a data stealer that is being
competing malware by its extreme eas
threat actors to use this virus.

Type
Stealer

First seen
1 January, 2016

Figure 3 – First Formbook sample was seen on January 1, 2016, according to AnyRun.

The Formbook’s seller was hidden under “**ng-Coder**” avatar.

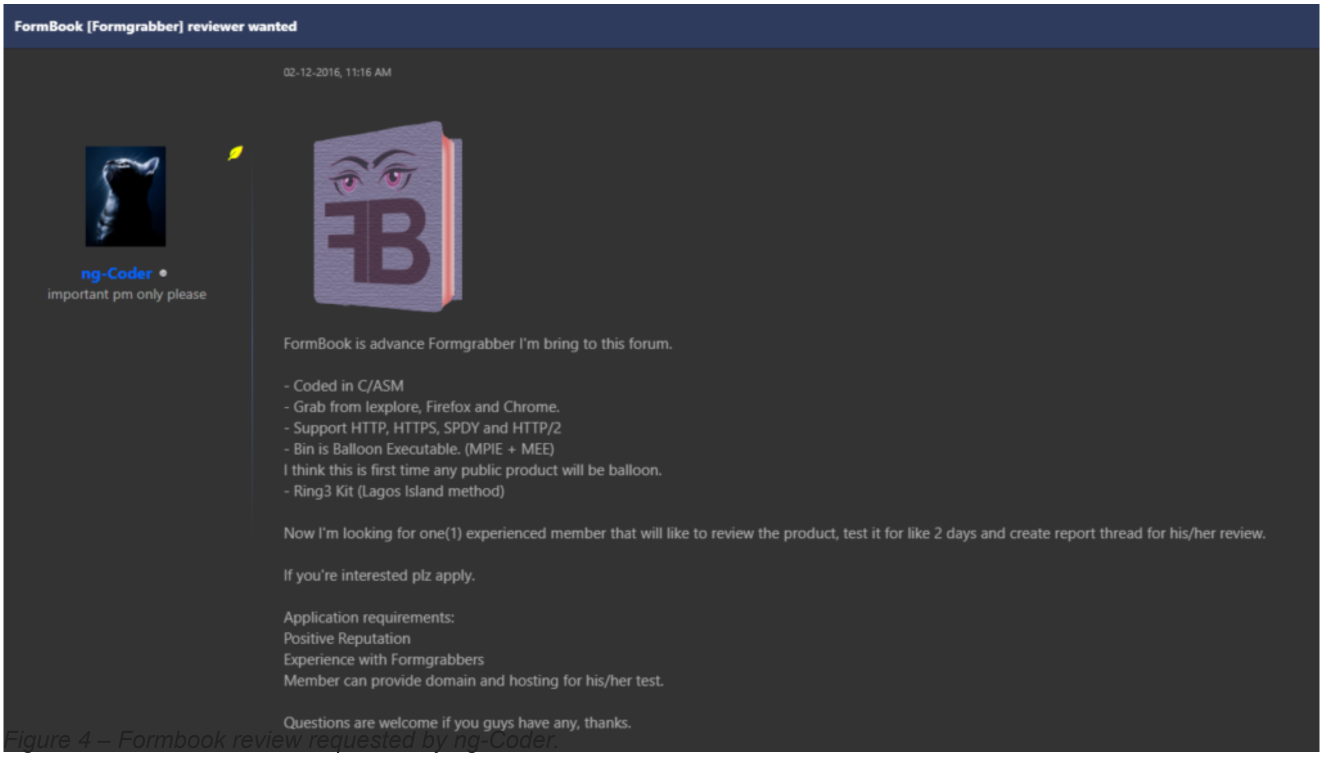
Note: we assume ng-Coder is a male, though we have no direct evidence, and will refer to the avatar as “he” throughout this article.

Profile

```
e-mail: [email protected]
Skype: Ng.Coder
skills:
* strong c\c++ knowledge
* strong assembly x86\x64 knowledge
```

ng-Coder joined the underground hack forum on October 27, 2015. According to his own statement on the forum, he was selling exploits at that time. We cannot point to ng-Coder's exact country of origin, but judging by his phrasing, English is likely not his native language.

A day before creating the sales thread we saw above, ng-Coder requested a review of his product from an experienced member of the community.



FormBook [Formgrabber] reviewer wanted

02-12-2016, 11:16 AM

ng-Coder
important pm only please

FormBook is advance Formgrabber I'm bring to this forum.

- Coded in C/ASM
- Grab from Iexplore, Firefox and Chrome.
- Support HTTP, HTTPS, SPDY and HTTP/2
- Bin is Balloon Executable. (MPIE + MEE)
I think this is first time any public product will be balloon.
- Ring3 Kit (Lagos Island method)

Now I'm looking for one(1) experienced member that will like to review the product, test it for like 2 days and create report thread for his/her review.

If you're interested plz apply.

Application requirements:
Positive Reputation
Experience with Formgrabbers
Member can provide domain and hosting for his/her test.

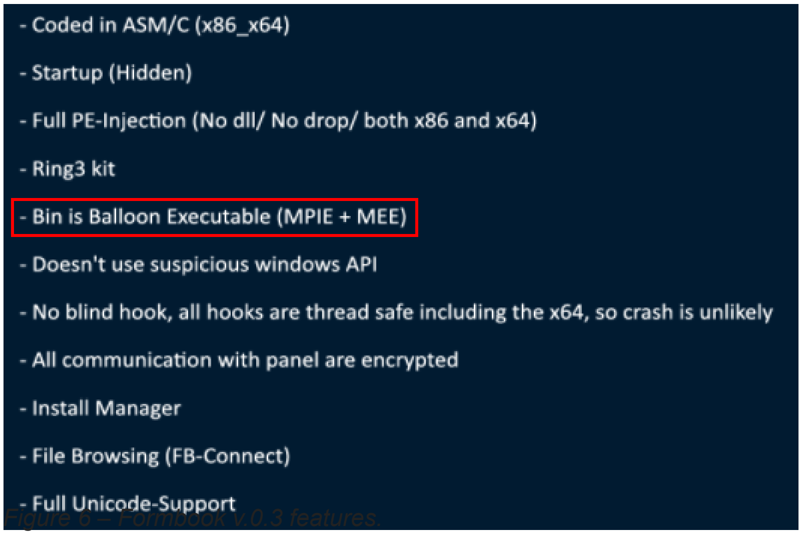
Questions are welcome if you guys have any, thanks.

Figure 4 – Formbook review requested by ng-Coder.

On May 9, 2016, three months later after publishing the first sales thread, Formbook v.0.3 was offered for sale.

Figure 5 – Formbook v.0.3 icon.

Formbook was advertised as a product supporting multiple features:



- Coded in ASM/C (x86_x64)
- Startup (Hidden)
- Full PE-Injection (No dll/ No drop/ both x86 and x64)
- Ring3 kit
- Bin is Balloon Executable (MPIE + MEE)
- Doesn't use suspicious windows API
- No blind hook, all hooks are thread safe including the x64, so crash is unlikely
- All communication with panel are encrypted
- Install Manager
- File Browsing (FB-Connect)
- Full Unicode-Support

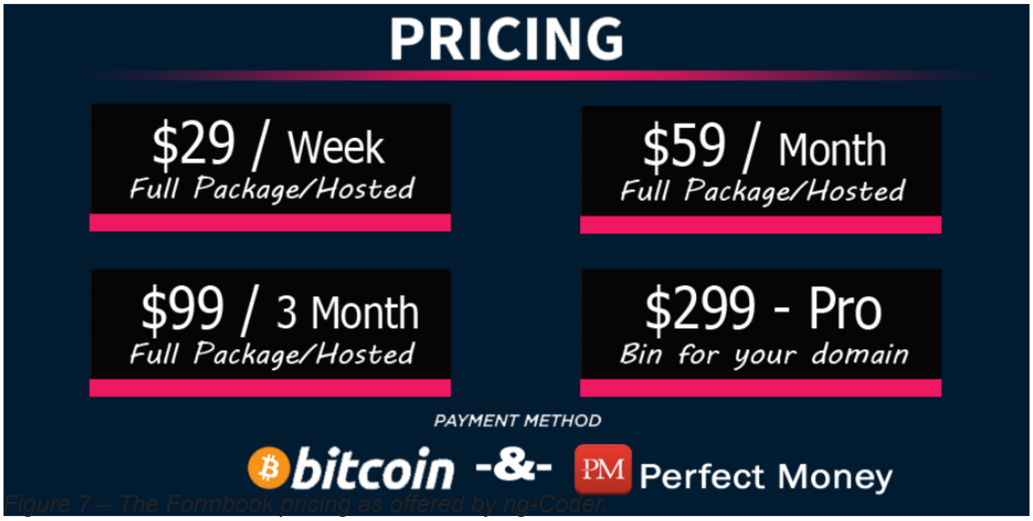
Figure 6 – Formbook v.0.3 features.

What attracted our attention here is a strange description including the phrase “Balloon Executable” and the acronyms MPIE and MEE. These terms, which do not exist in the cyber community, were used by ng-Coder to describe how Formbook operates, i.e., uses position-independent code (shellcode) to inject the malware into a legitimate system process and initiate the shellcode execution.

Other features listed include network traffic sniffing, keylogging, clipboard monitoring, and password extraction for almost one hundred applications including browsers, messengers, FTP and email clients.

The sales pitch was a combined model, in which a customer could choose where to host the panel: on the host provided by the seller (thus using a “Malware-as-a-Service” scheme) or the customer’s own machine (direct acquiring). If the latter was selected, the author also provided the panel source code along with a pre-built binary.

Different types of Formbook subscriptions had different prices:



PRICING

$29 / Week
Full Package/Hosted

$59 / Month
Full Package/Hosted

$99 / 3 Month
Full Package/Hosted

$299 - Pro
Bin for your domain

PAYMENT METHOD

bitcoin -&- PM Perfect Money

Figure 7 – The Formbook pricing as offered by ng-Coder.

ng-Coder offered a number different source code protectors to support Formbook. For example, **Net-Protector** is a cross-platform crypting service with the price of $100 for a Windows executable and $200 for a macOS one:

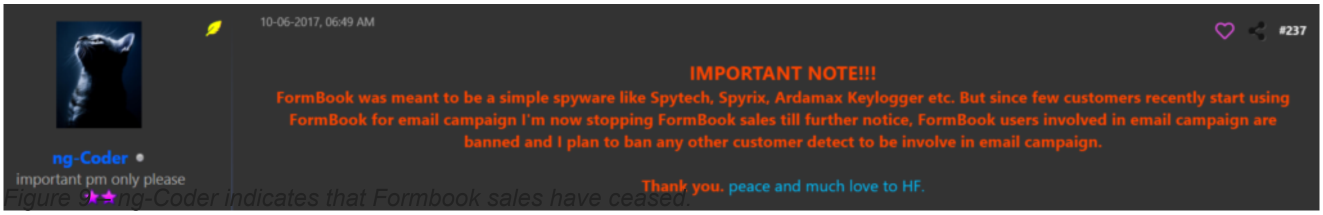
Figure 8 – Net-Protector logo.

ng-Coder was so confident in his creation that he offered to re-crypt an executable for free if it was detected by any AV in the first 30 days after the encryption:

> *If the crypted PE file gets flagged by AV in less than 30 days after the first crypt, we will recrypt the same crypted SHA1 for free.*

Other examples of protectors included shared source codes of crypting solutions on .NET and Delphi.

On October 6, 2017, Formbook sales abruptly stopped. The reason given was its use in spam campaigns:



ng-Coder
important pm only please

10-06-2017, 06:49 AM

#237

IMPORTANT NOTE!!!

FormBook was meant to be a simple spyware like Spytech, Spyrix, Ardamax Keylogger etc. But since few customers recently start using FormBook for email campaign I'm now stopping FormBook sales till further notice, FormBook users involved in email campaign are banned and I plan to ban any other customer detect to be involve in email campaign.

Thank you. peace and much love to HF.

Figure 9 – ng-Coder indicates that Formbook sales have ceased.

As we stated at the beginning of this article, the Formbook author didn't want his creation to be used in email campaigns and banned all customers who did so.

On May 27, 2018, ng-Coder made his last public post on the forum where he provided a technical answer to one of the questions not related to Formbook. No further activity from him has been observed since.

As we will see, although Formbook sales were stopped, its activity was continuing. Not only could users who bought the malware to be hosted on their own servers continue to use it, but ng-Coder could make use of Formbook as well.

Used for the author's own purposes?

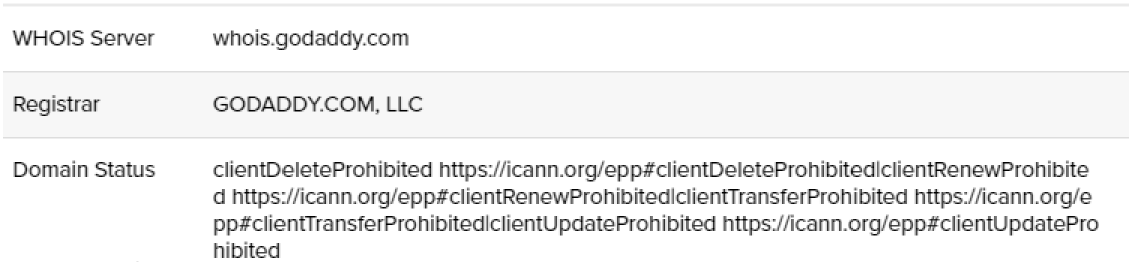
We found evidence that ng-Coder might have his own plans for his creation. We analyzed the domains linked to the ng-Coder email address “[email protected]][.com” and discovered that these were used in Formbook configurations for particular campaigns labeled “private”, “list” and “zog”. We found 16 unique C&C URLs inside the Formbook malware that pointed to 13 different sub-campaigns.

```
http[://www.unlimitedgiveaways.net/zog/hx/
http[://www.unlimitedgiveaways.net/zog/hx69/
http[://www.unlimitedgiveaways.net/zog/ab/
http[://www.socialbumps.net/zog/ct2/

http[://www.alienzouks.com/private/
http[://www.adomax1.com/private/
http[://www.ryandeby.com/private/
http[://www.gfather.net/private/

http[://www.surfpay.website/list/ch/
http[://www.bingo-clicker.site/list/jo/
http[://www.click-bingo.site/list/le/
http[://www.click-bingo.site/list/kv/
http[://www.click-bingo.site/list/mo/
http[://www.jesse-list.info/list/kw/
http[://www.wowtracking.info/list/hx47/
http[://www.wowtracking.info/list/oz/
```

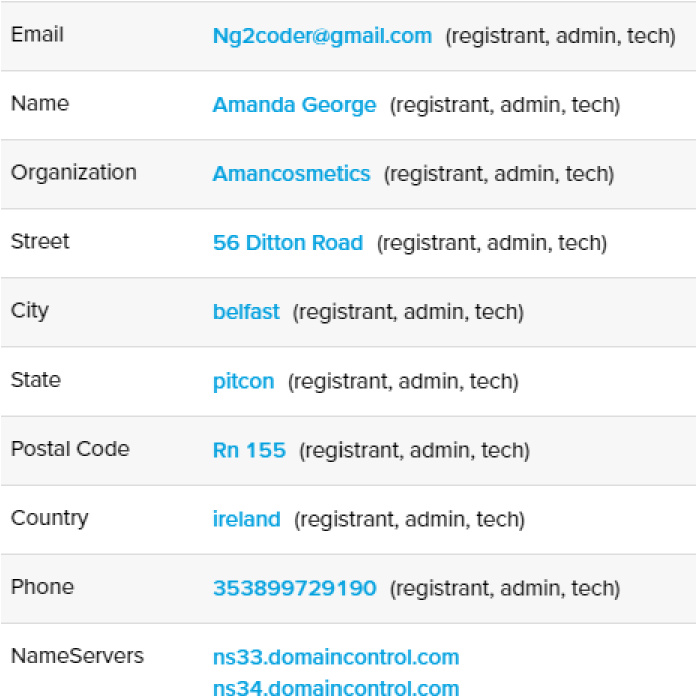
All the listed domains share common features. They all were registered by the GoDaddy registrar:



WHOIS Server	whois.godaddy.com
Registrar	GODADDY.COM, LLC
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited|clientRenewProhibited https://icann.org/epp#clientRenewProhibited|clientTransferProhibited https://icann.org/epp#clientTransferProhibited|clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Figure 10 – GoDaddy registrar appears in domains’ details.

And they all shared the same details about the person who registered them:

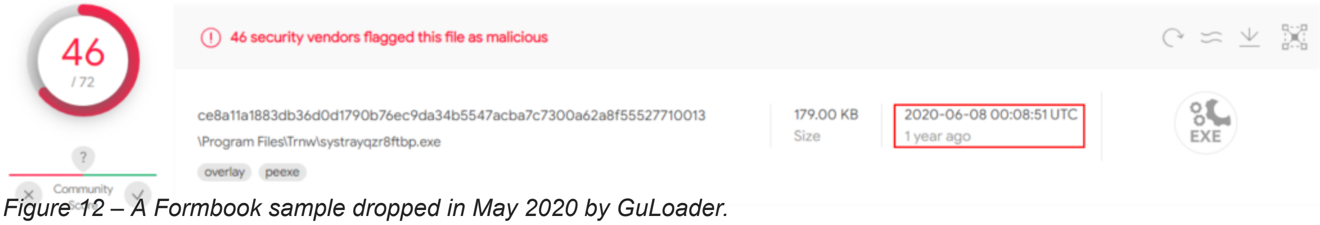


Email	Ng2coder@gmail.com (registrant, admin, tech)
Name	Amanda George (registrant, admin, tech)
Organization	Amancosmetics (registrant, admin, tech)
Street	56 Ditton Road (registrant, admin, tech)
City	belfast (registrant, admin, tech)
State	pitcon (registrant, admin, tech)
Postal Code	Rn 155 (registrant, admin, tech)
Country	ireland (registrant, admin, tech)
Phone	353899729190 (registrant, admin, tech)
NameServers	ns33.domaincontrol.com ns34.domaincontrol.com

Figure 11 – Details for registering domains as provided by ng-Coder.

According to the LocateFamily site, “Amanda George” was living at the address provided at the time of registering the domains. However, we cannot link this person with ng-Coder avatar.

The Formbook activity didn’t just stop there. For example, in May 2020 we discovered a Formbook sample dropped by GuLoader. It was submitted to VirusTotal in June 2020:



46 / 72

46 security vendors flagged this file as malicious

ce8a11a1883db36d0d1790b76ec9da34b5547acba7c7300a62a8f55527710013
\Program Files\Trnw\systrayqzr8ftbp.exe

overlay peexe

179.00 KB
Size

2020-06-08 00:08:51 UTC
1 year ago

EXE

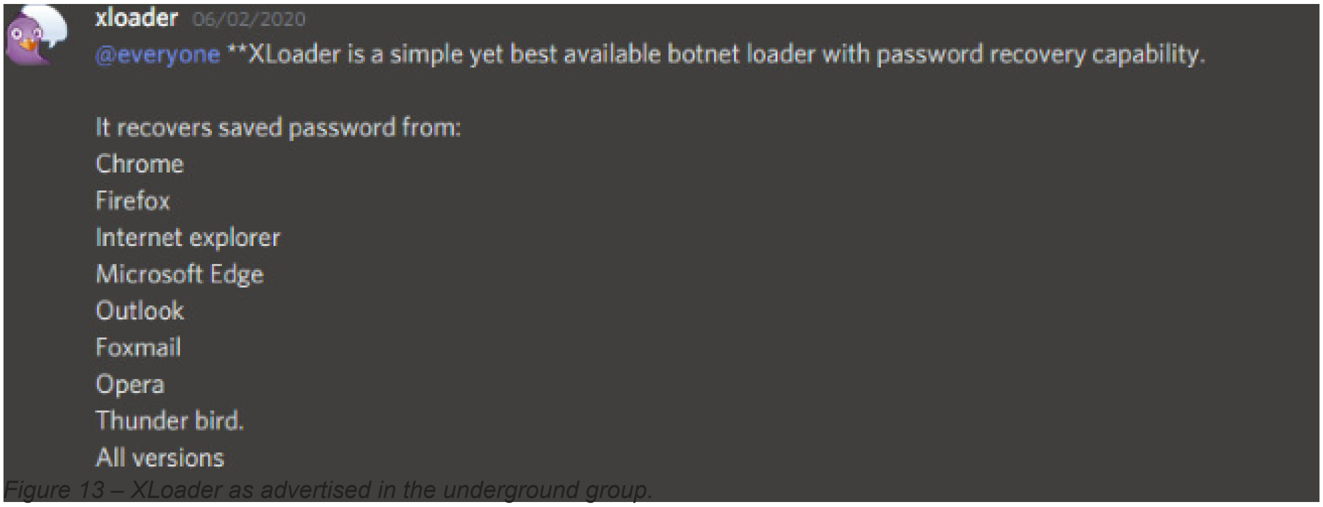
Community Score

Figure 12 – A Formbook sample dropped in May 2020 by GuLoader.

The campaign name in this sample was “private” and the main domain was registered by ng-Coder (ryandeby[.com).

XLoader: the time-proved tricks re-applied in a new environment

On February 6, 2020 a new era began: the era of the Formbook successor called XLoader. On this day, XLoader was advertised for sale in one of the underground groups.



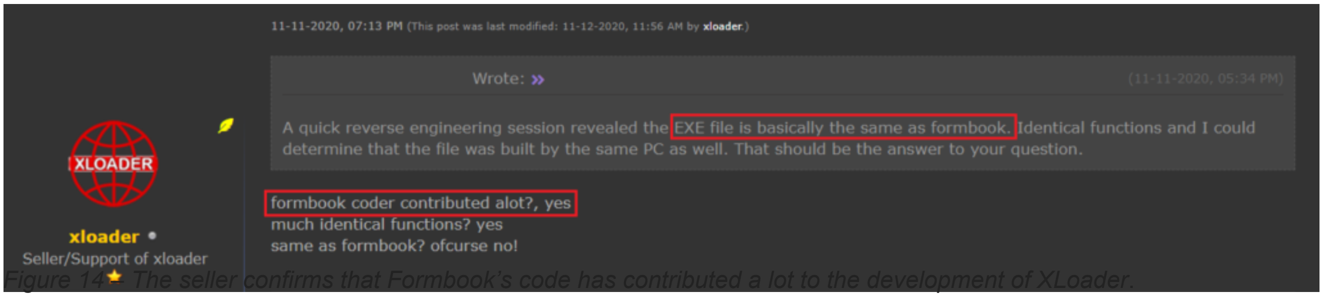
xloader 06/02/2020

@everyone **XLoader is a simple yet best available botnet loader with password recovery capability.

It recovers saved password from:
Chrome
Firefox
Internet explorer
Microsoft Edge
Outlook
Foxmail
Opera
Thunder bird.
All versions

Figure 13 – XLoader as advertised in the underground group.

Formbook and XLoader share the same code base, and there are other connections between them as well, as we will see later.



11-11-2020, 07:13 PM (This post was last modified: 11-12-2020, 11:56 AM by xloader.)

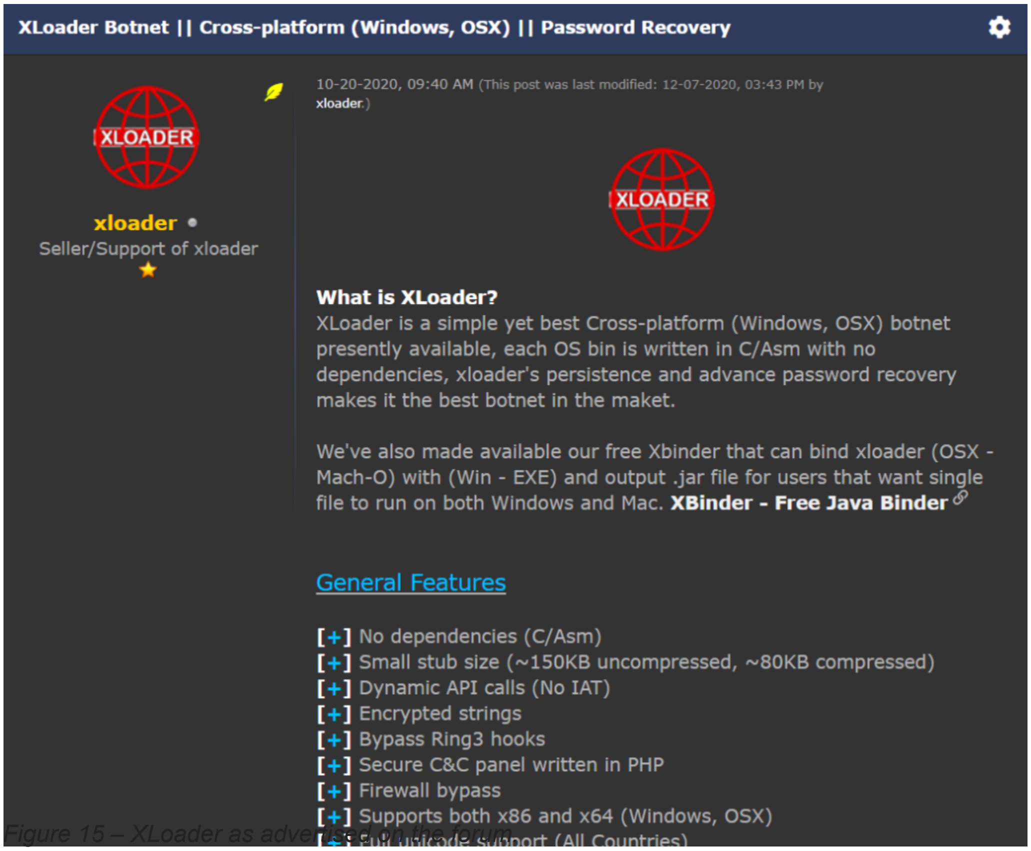
Wrote: » (11-11-2020, 05:34 PM)

A quick reverse engineering session revealed the EXE file is basically the same as formbook. Identical functions and I could determine that the file was built by the same PC as well. That should be the answer to your question.

formbook coder contributed alot?, yes
much identical functions? yes
same as formbook? ofcurse no!

Figure 14 – The seller confirms that Formbook's code has contributed a lot to the development of XLoader.

On October 20, 2020, XLoader was offered for sale on the same forum which was used for selling Formbook.



XLoader Botnet || Cross-platform (Windows, OSX) || Password Recovery

xloader
Seller/Support of xloader

10-20-2020, 09:40 AM (This post was last modified: 12-07-2020, 03:43 PM by xloader.)

What is XLoader?
XLoader is a simple yet best Cross-platform (Windows, OSX) botnet presently available, each OS bin is written in C/Asm with no dependencies, xloader's persistence and advance password recovery makes it the best botnet in the maket.

We've also made available our free Xbinder that can bind xloader (OSX - Mach-O) with (Win - EXE) and output .jar file for users that want single file to run on both Windows and Mac. **XBinder - Free Java Binder**

General Features

[+] No dependencies (C/Asm)
[+] Small stub size (~150KB uncompressed, ~80KB compressed)
[+] Dynamic API calls (No IAT)
[+] Encrypted strings
[+] Bypass Ring3 hooks
[+] Secure C&C panel written in PHP
[+] Firewall bypass
[+] Supports both x86 and x64 (Windows, OSX)
[+] Full unicode support (All Countries)

Figure 15 – XLoader as advertised on the forum

Note: XLoader malware for PC and Mac should not be confused with XLoader malware for Android, first discovered in 2019.

One of the most exciting things about the new malware was its ability to operate in the macOS. With approximately 200 million users operating macOS in 2018 (as reported by Apple), this is definitely a promising new market for the malware to enter.

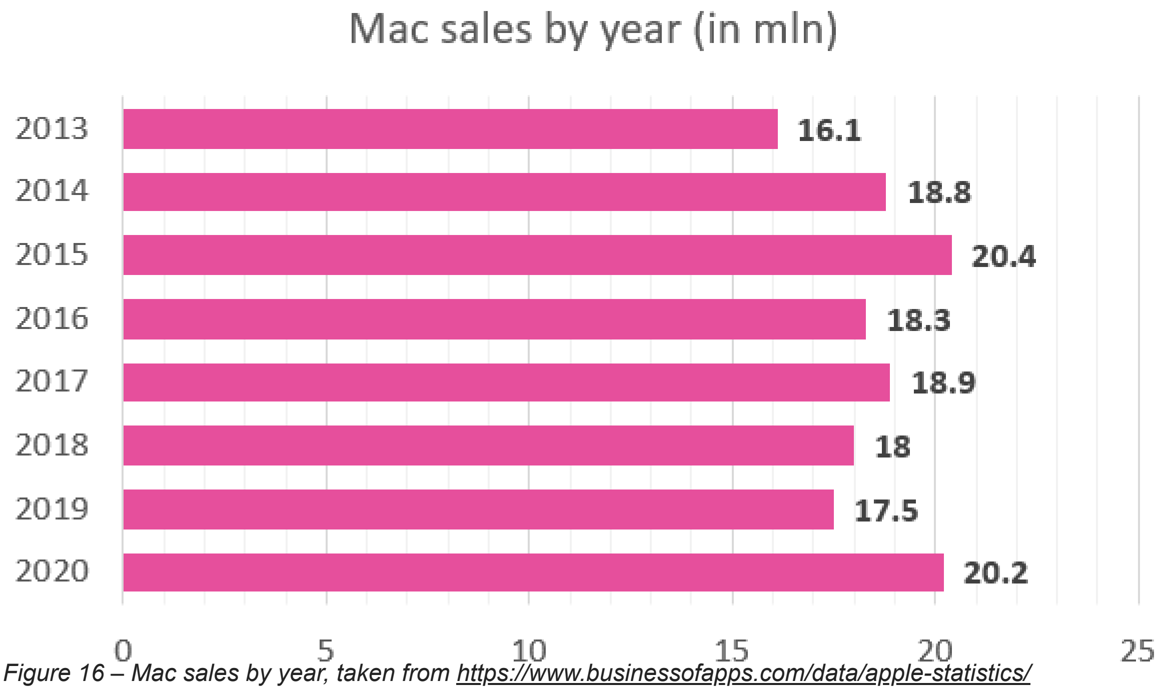
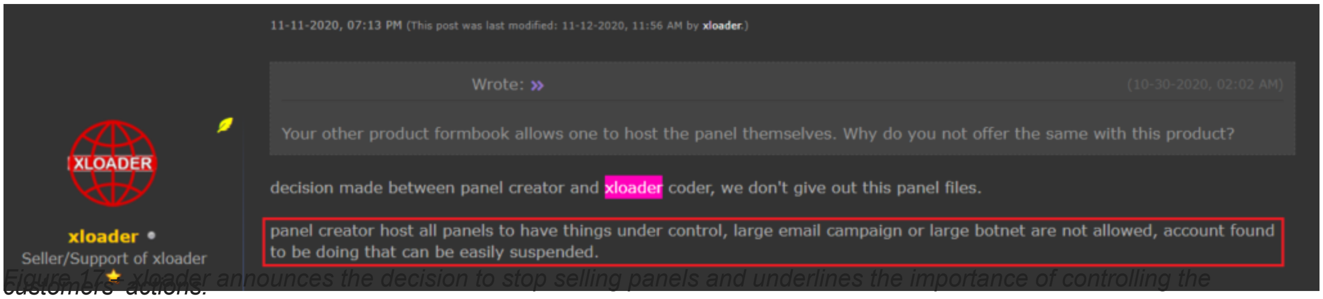


Figure 16 – Mac sales by year, taken from https://www.businessofapps.com/data/apple-statistics/

Note: Apple stopped reporting Mac sales in Q4 2018. All subsequent values are estimates.

The malware now features a more lucrative economic model for the authors as compared to Formbook. Customers may only buy the malware for a limited time and are only able to use a server provided by the seller; no panel sources codes are sold anymore. Thus, a "Malware-as-a-Service" scheme is used. Centralized C&C infrastructure allows the authors to control how the malware is used by the customers.



11-11-2020, 07:13 PM (This post was last modified: 11-12-2020, 11:56 AM by xloader.)

Wrote: » (10-30-2020, 02:02 AM)

Your other product formbook allows one to host the panel themselves. Why do you not offer the same with this product?

decision made between panel creator and xloader coder, we don't give out this panel files.

panel creator host all panels to have things under control, large email campaign or large botnet are not allowed, account found to be doing that can be easily suspended.

Figure 17: xloader announces the decision to stop selling panels and underlines the importance of controlling the customers' actions.

The pricing for different options is listed in the table below:

Package	Price
Windows, executable, 1 month	$59
Windows, executable, 3 months	$129
macOS, Mach-O, 1 month	$49
macOS, Mach-O, 3 months	$99

XLoader's seller also released a free Java binder which is intended to create a standalone JAR file uniting Mach-O and exe binaries:

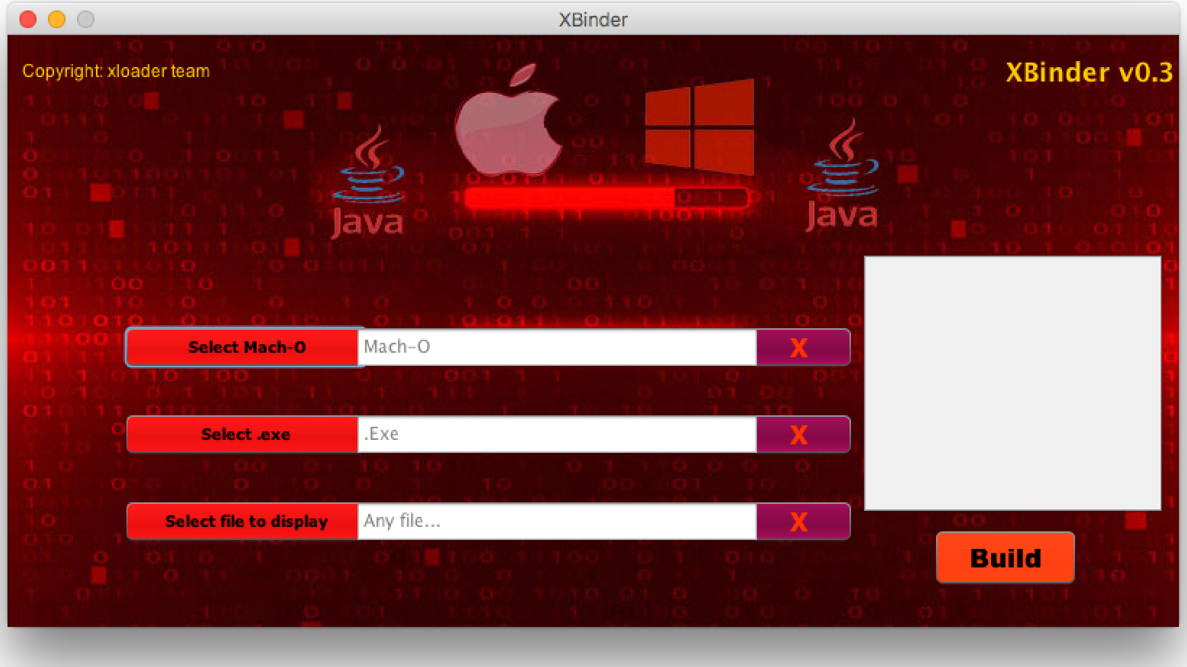
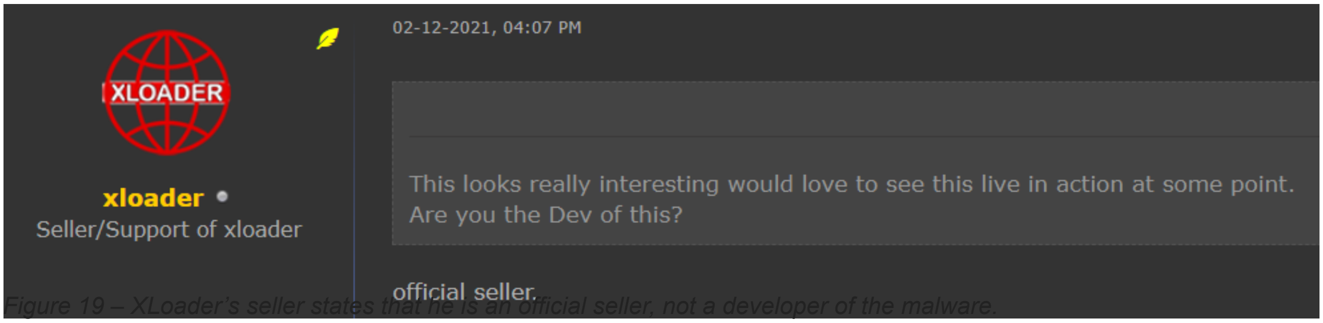


Figure 18 – Interface of the XBinder tool.

A new developer?

Did the new seller also take on duties as the developer and maintainer of this version of the original Formbook malware? We believe this is not the case. A new seller is just a seller, not a developer. There must be someone else behind the curtain to handle the technical part.



xloader
Seller/Support of xloader

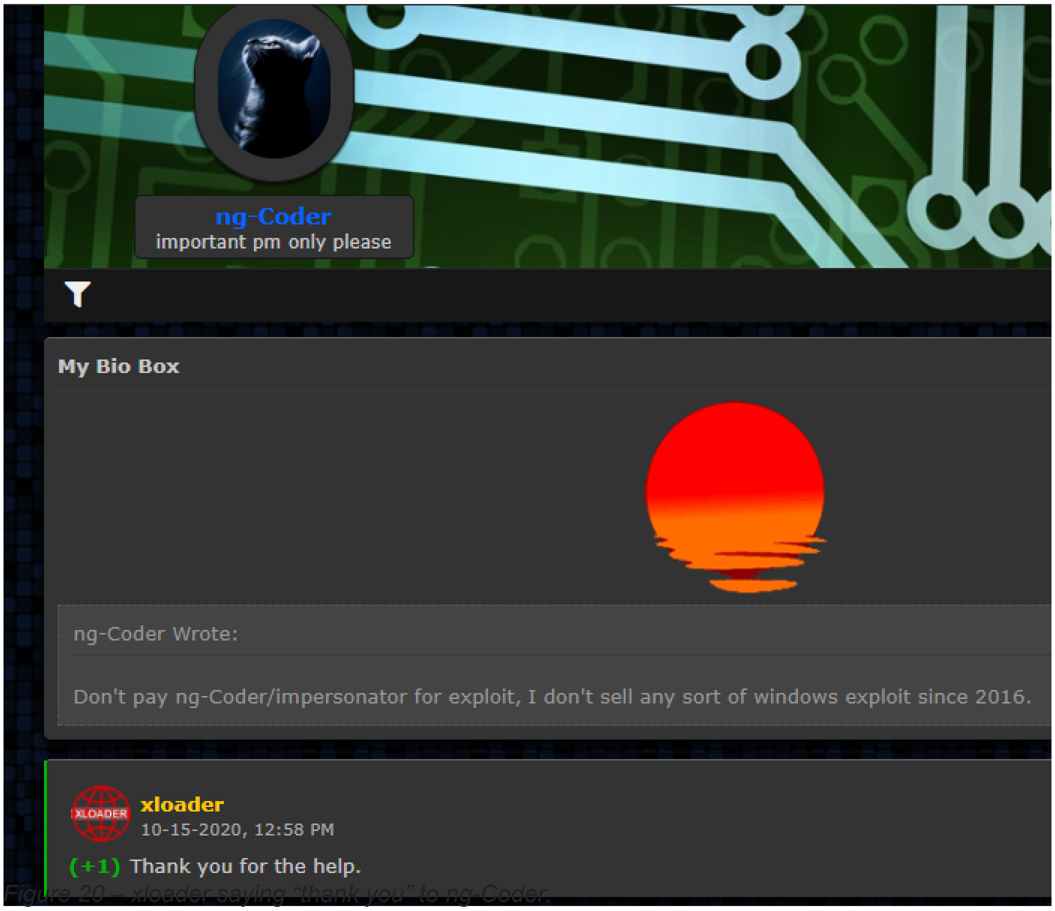
02-12-2021, 04:07 PM

This looks really interesting would love to see this live in action at some point. Are you the Dev of this?

official seller.

Figure 19 – XLoader's seller states that he is an official seller, not a developer of the malware.

We already saw that ng-Coder wasn't completely out of the picture, even though he no longer operated publicly. Could he be the one continuing to develop the new malware? Apart from technical similarities, we found evidence of a connection between XLoader's seller and ng-Coder, namely a message from xloader to ng-Coder saying, "Thank you for the help":



ng-Coder
important pm only please

My Bio Box

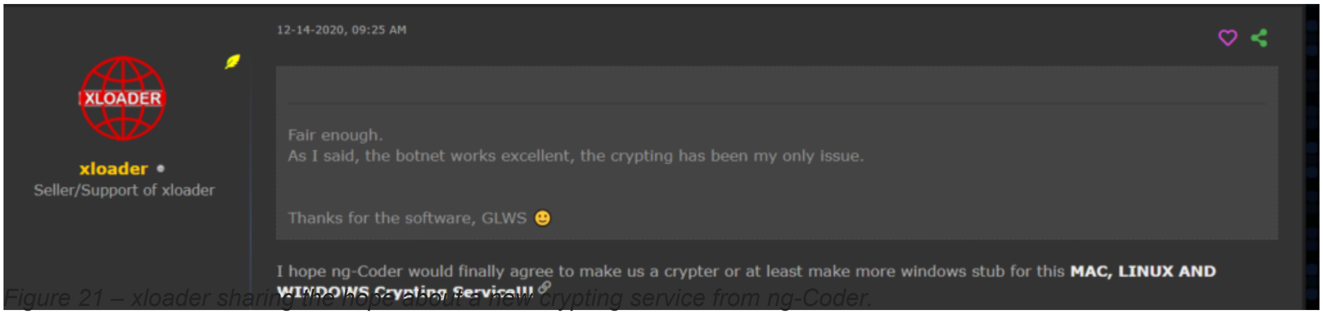
> ng-Coder Wrote:
>
> Don't pay ng-Coder/impersonator for exploit, I don't sell any sort of windows exploit since 2016.

xloader
10-15-2020, 12:58 PM
(+1) Thank you for the help.

Figure 20 – xloader saying “thank you” to ng-Coder.

We cannot say for sure if the thanks were for a one-time helping hand or if it was for continuous support.

Another piece of evidence that points at ng-Coder’s continued participation is the statement by XLoader’s seller (posted on December 14, 2020) where he shared his hope that ng-Coder could create a newer cross-platform crypting service:



xloader ●
Seller/Support of xloader

12-14-2020, 09:25 AM

> Fair enough.
> As I said, the botnet works excellent, the crypting has been my only issue.
>
> Thanks for the software, GLWS 😃

I hope ng-Coder would finally agree to make us a crypter or at least make more windows stub for this **MAC, LINUX AND WINDOWS Crypting Service!!!**

Figure 21 – xloader sharing the hope about a new crypting service from ng-Coder.

Recap

We recap the malware activity timeline and its milestones in the diagram below.

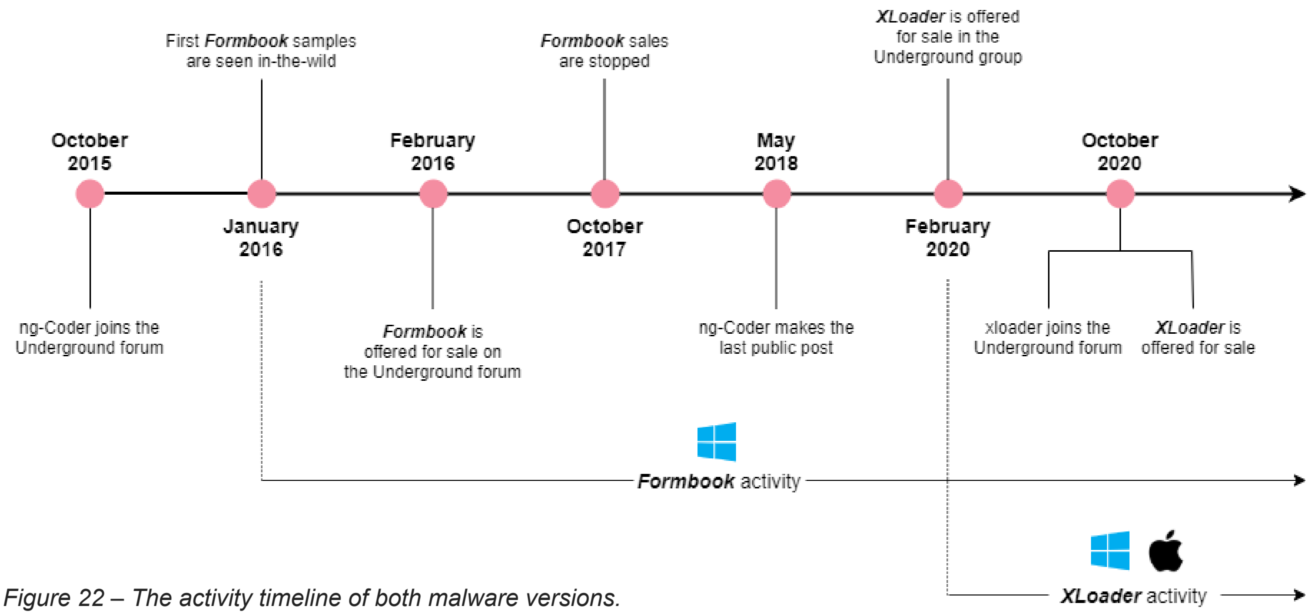

First Formbook samples are seen in-the-wild
Formbook sales are stopped
XLoader is offered for sale in the Underground group
October 2015
February 2016
May 2018
October 2020
January 2016
October 2017
February 2020
ng-Coder joins the Underground forum
Formbook is offered for sale on the Underground forum
ng-Coder makes the last public post
xloader joins the Underground forum
XLoader is offered for sale
Formbook activity
XLoader activity

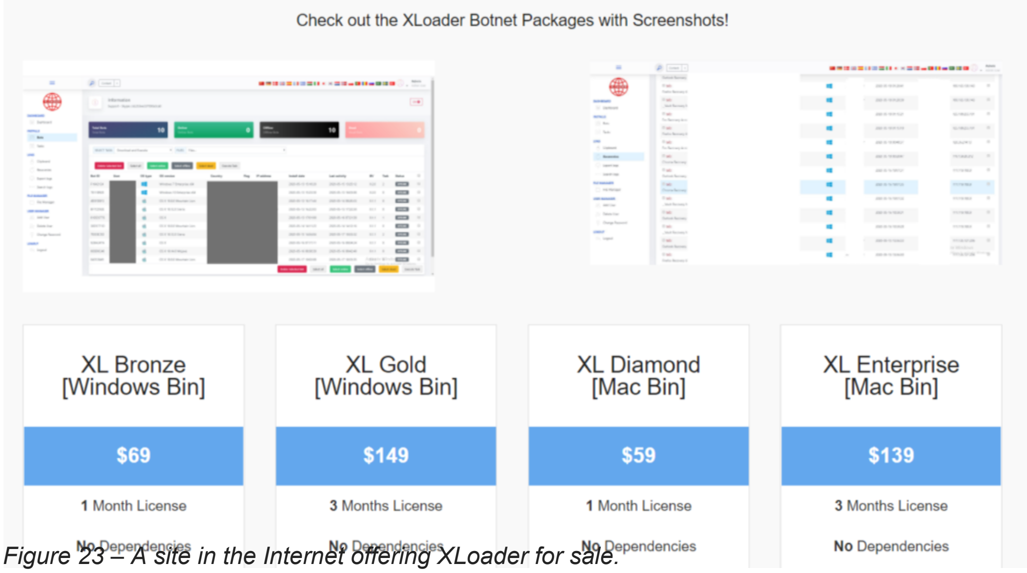
Figure 22 – The activity timeline of both malware versions.

Re-sellers

During the lifecycle of Formbook/XLoader malware, a number of impersonators and re-sellers claimed they were the official contacts.

It began 5 years ago when ng-Coder raised a warning not to send a payment to him or anyone impersonating him for the exploit, as he stopped selling exploits in 2016. Note that there were impersonators even before Formbook was first available for sale.

In 2021, the situation hasn't changed much. For example, there is a site freely accessible from the Internet which offers XLoader for sale, but for a higher price than the malware is sold for in the Darknet:



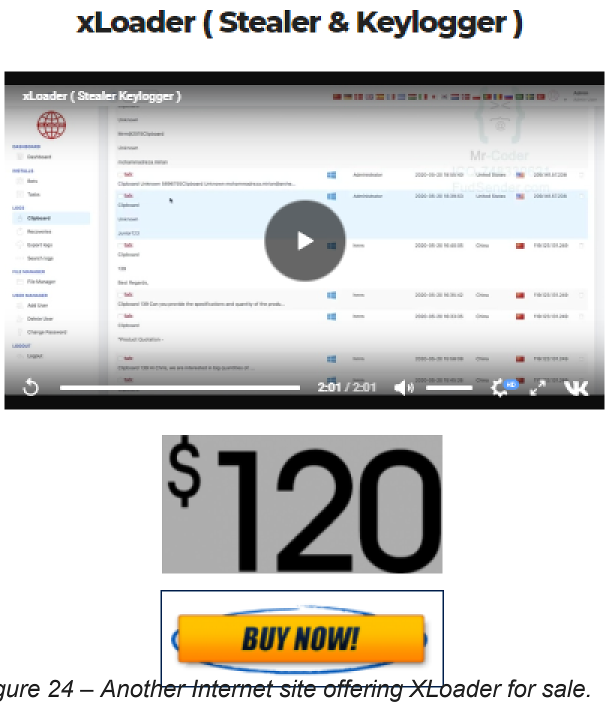
Check out the XLoader Botnet Packages with Screenshots!

XL Bronze [Windows Bin]	XL Gold [Windows Bin]	XL Diamond [Mac Bin]	XL Enterprise [Mac Bin]
$69	$149	$59	$139
1 Month License	**3** Months License	**1** Month License	**3** Months License
No Dependencies	**No** Dependencies	**No** Dependencies	**No** Dependencies

Figure 23 – A site in the Internet offering XLoader for sale.

The biggest difference is in the 3 months package for macOS, which is $40 higher than the Darknet price.

Another site offers XLoader for $120:


xLoader (Stealer & Keylogger)

$120

Figure 24 – Another Internet site offering XLoader for sale.

Prevalence: countries and campaigns

During the 6 months between December 1, 2020 and June 1, 2021, we saw Formbook/XLoader requests from as many as 69 countries, which is more than a third of the total 195 countries recognized in the world today.

The breakdown of victims by country is presented in the diagram below:

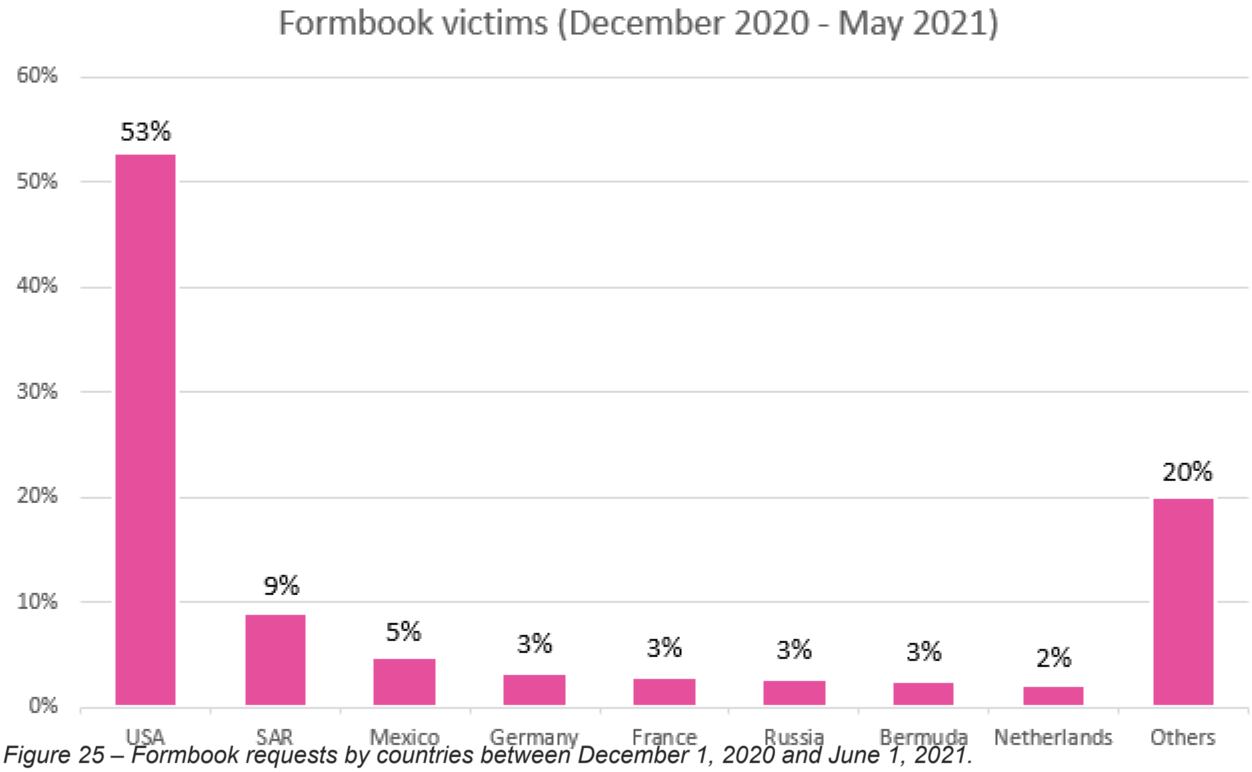


Figure 25 – Formbook requests by countries between December 1, 2020 and June 1, 2021.

Victims from the United States constitute more than the half of the victims worldwide.

As we stated previously, according to AnyRun, Formbook is in 4th place among the most prevalent malware families of the last year and in 6th place for all time. This fact implies that there should be quite a lot of Formbook\XLoader campaigns in-the-wild. Indeed, we observed more than 1400 different campaigns of the malware during several years of monitoring its activity.

In the upcoming articles we share the technical details of the malware's macOS version which reveal how XLoader operates under the hood and help us to understand how the Formbook\XLoader family secured its place in malware top prevalence lists.

We also describe a distinctive feature of the XLoader malware which helps it to fool sandboxes and researchers and keep its real C&C servers hidden. Out of almost 90,000 domains used in network communication by the malware, only 1,300 are the real C&C servers – which constitutes just 1.5% of the total. The other 88,000 domains belong to legitimate sites; however, the malware sends malicious traffic to them as well. This presents security vendors with the dilemma of how to determine which are the real C&C servers and not false-positively identify legitimate sites as malicious.

We also share our methods to correctly analyze the XLoader's communication with the servers and to identify the real C&C – only one out of all the 64 domains present in any chosen sample.

Stay tuned!

Check Point Protections

Check Point Provides Zero-Day Protection Across Its Network, Cloud, Users and Access Security Solutions, SandBlast provides the best zero-day protection while reducing security overhead

SandBlast Network Protections:

```
Trojan.WIN32.Formbook.A
Trojan.WIN32.Formbook.B
Trojan.WIN32.Formbook.C
Trojan.WIN32.Formbook.D
Trojan.WIN32.Formbook.E
Trojan.WIN32.Formbook.F
Trojan.WIN32.Formbook.G
Trojan.WIN32.Formbook.H
Trojan.WIN32.Formbook.I
Trojan.WIN32.Formbook.J
Trojan.WIN32.Formbook.K
Trojan.WIN32.Formbook.L
Trojan.WIN32.Formbook.M
Trojan.WIN32.Formbook.N
Trojan.WIN32.Formbook.O
Trojan.WIN32.Formbook.P
Trojan.WIN32.Formbook.Q
Trojan.WIN32.Formbook.R
```

Threat Emulation protections:

```
Infostealer.Win32.Formbook.C
Infostealer.Win32.Formbook.D
Infostealer.Win32.Formbook.E
Infostealer.Win32.Formbook.gl.F
Infostealer.Win32.Formbook.TC
Formbook.TC
Infostealer.Win32.XLoader.TC
XLoader.TC
Trojan.Mac.XLoader.B
```

Sources

1. Check Point Press Release December 2020 // https://www.checkpoint.com/press/2021/december-2020s-most-wanted-malware-emotet-returns-as-top-malware-threat/#
2. Malware Trends Tracker // https://any.run/malware-trends/
3. Malware Analysis Spotlight: Formbook (September 2020) // https://www.vmray.com/cyber-security-blog/formbook-september-2020-malware-analysis-spotlight/

4. Significant FormBook Distribution Campaigns Impacting the U.S. and South Korea // https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
5. Formbook Research Hints Large Data Theft Attack Brewing // https://www.cyberbit.com/blog/endpoint-security/formbook-research-hints-large-data-theft-attack-brewing/
6. Selling FormBook // https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/selling-formbook/
7. Cybercrime, new Formbook malspam campaign against hotels // https://www.difesaesicurezza.com/en/defence-and-security/cybercrime-new-formbook-malspam-campaign-against-hotels/
8. VB 2018: Inside Formbook Infostealer // https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-inside-formbook-infostealer/
9. GuLoader? No, CloudEyE // https://research.checkpoint.com/2020/guloader-cloudeye/
10. Yes, Cyber Adversaries are still using Formbook in 2021 // https://yoroi.company/research/yes-cyber-adversaries-are-still-using-formbook-in-2021/