Bablosoft; Lowering the Barrier of Entry for Malicious Actors

team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/

S2 Research Team View all posts by S2 Research Team May 25, 2022

Summary

Evidence suggests an increasing number of threat actor groups are making use of a free-to-use browser automation framework. The framework contains numerous features which we assess may be utilized in the enablement of malicious activities.

The technical entry bar for the framework is purposefully kept low, which has served to create an active community of content developers and contributors, with actors in the underground economy advertising their time for the creation of bespoke tooling.

The framework warranted further research due to the high number of distinct threat groups who include it in their toolkits.

Introduction

During three recent (and separate) investigations into command and control (C2) infrastructure for Bumblebee loader, and BlackGuard and RedLine stealers, our analysts observed connections from the C2s to a tool repository / marketplace called Bablosoft.

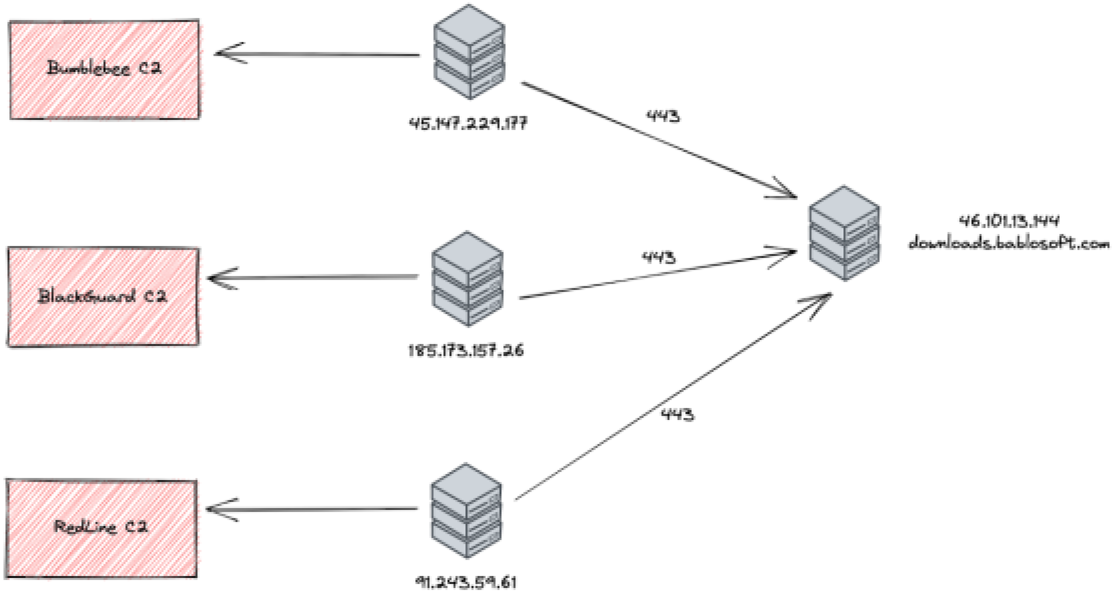


Figure 1:

Overview of Observed Relationships

Looking into open-source reporting, we found that other vendors had previously come across Bablosoft in their investigations:

- General research by F5 Labs into credential stuffing attacks
- Research by NTT into the toolkit utilized by GRIM SPIDER

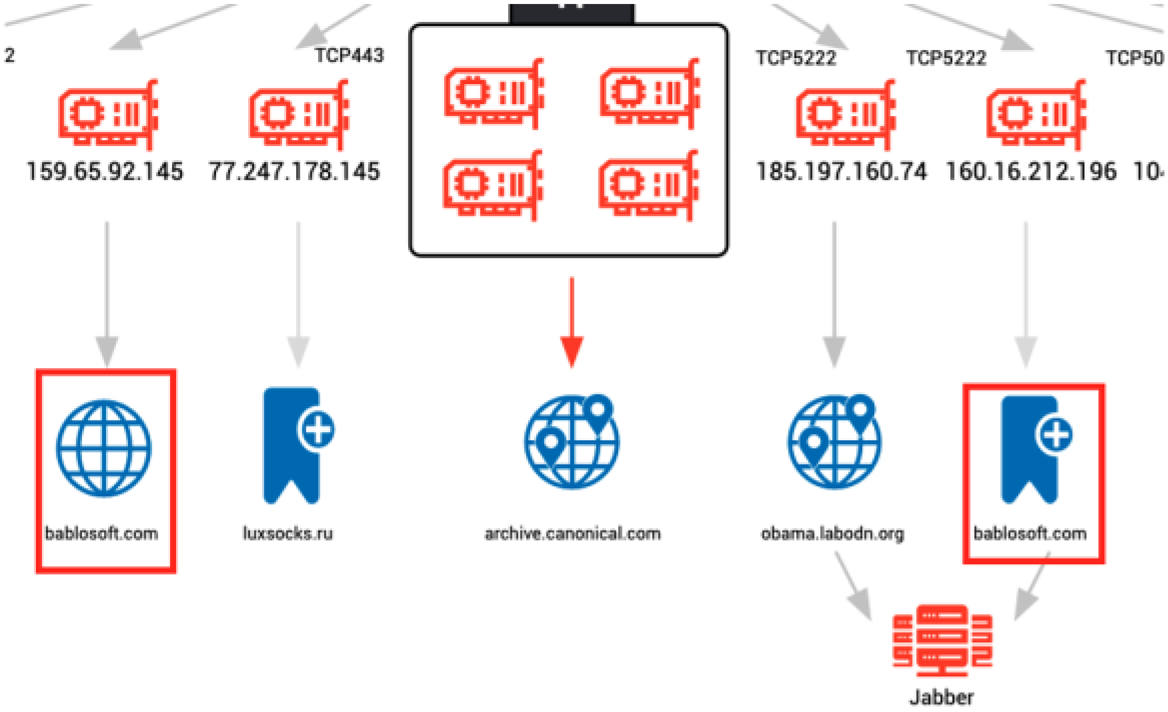


Figure 2:

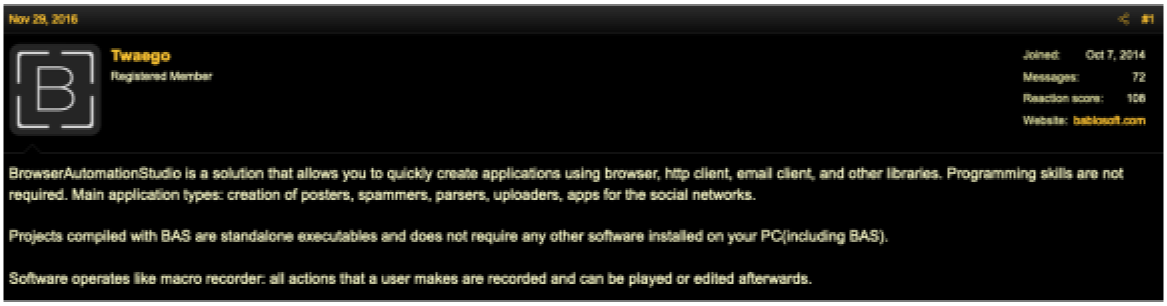
Screenshot from the NTT Analysis of GRIM SPIDER Infrastructure

In this blog post, we will examine Bablosoft in further detail, providing our hypotheses on the threat actor use cases for the tools on offer, and highlighting links to other threat activity.

Bablosoft

Insight from Open Source

References to Bablosoft first appeared within public forums during late 2016, when the 'main' developer – who goes by the moniker ***Twaego*** – posted about the release of a tool entitled ***BrowserAutomationStudio*** (***BAS***).



Nov 29, 2016 #1

Twaego
Registered Member

Joined: Oct 7, 2014
Messages: 72
Reaction score: 106
Website: bablosoft.com

BrowserAutomationStudio is a solution that allows you to quickly create applications using browser, http client, email client, and other libraries. Programming skills are not required. Main application types: creation of posters, spammers, parsers, uploaders, apps for the social networks.

Projects compiled with BAS are standalone executables and does not require any other software installed on your PC(including BAS).

Software operates like macro recorder: all actions that a user makes are recorded and can be played or edited afterwards.

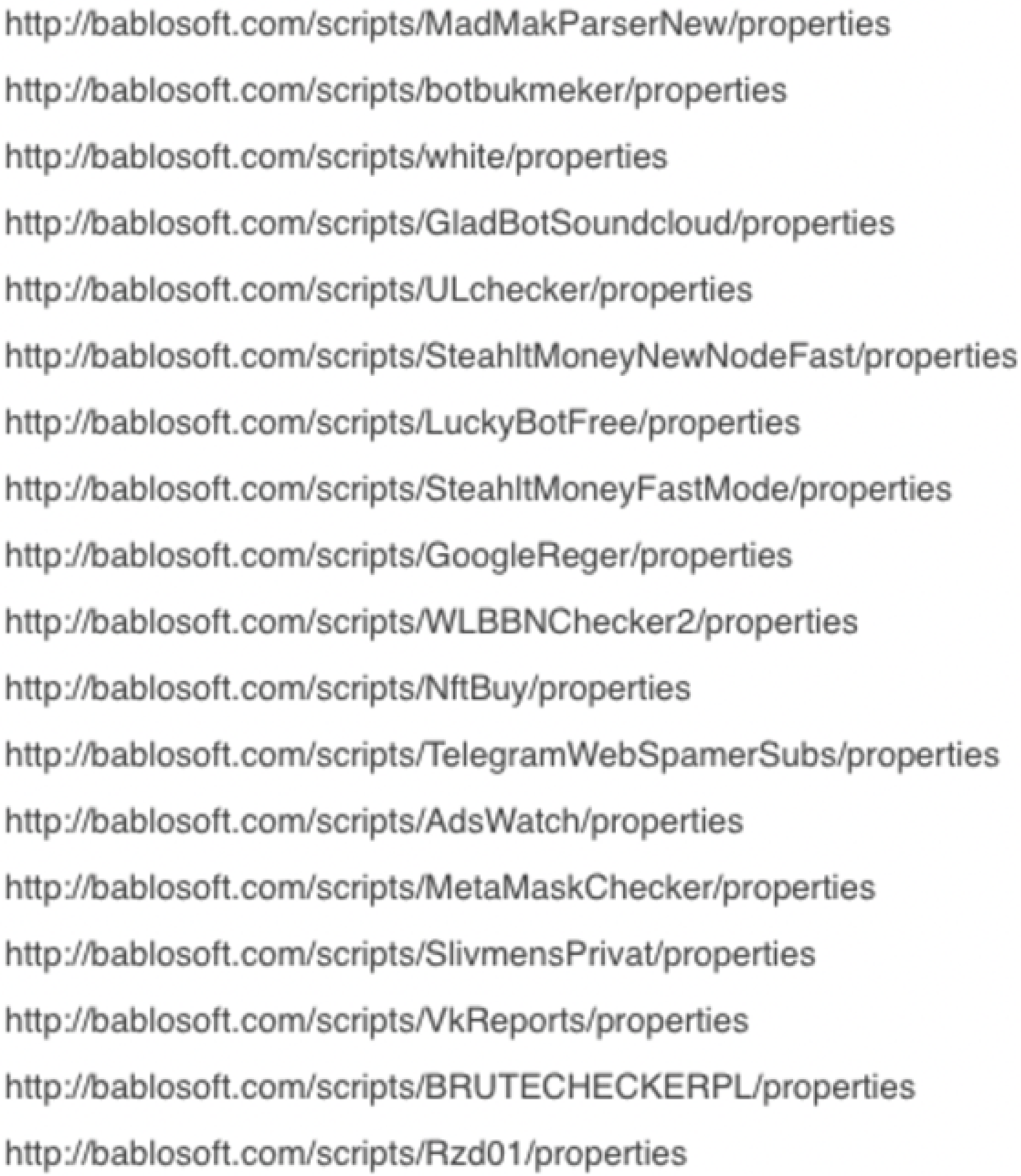
Figure 3:

Twaego's First Post About Bablosoft and BrowserAutomationStudio

As can be discerned from the advert, the purpose of ***BAS*** is to provide users with an easy-to-use framework for the creation of bots, including "spammers" and a "credentials checker".

Reviewing this and other public threads on ***BAS*** / Bablosoft, it is clear the tool was well received by the community, for several reasons:

- The tool is free – although a premium version with additional features is available
- The developer (***Twaego***) actively works on community feedback/requests to improve the tool
- Users can share applications/scripts through the Bablosoft community page



http://bablosoft.com/scripts/MadMakParserNew/properties

http://bablosoft.com/scripts/botbukmeker/properties

http://bablosoft.com/scripts/white/properties

http://bablosoft.com/scripts/GladBotSoundcloud/properties

http://bablosoft.com/scripts/ULchecker/properties

http://bablosoft.com/scripts/SteahltMoneyNewNodeFast/properties

http://bablosoft.com/scripts/LuckyBotFree/properties

http://bablosoft.com/scripts/SteahltMoneyFastMode/properties

http://bablosoft.com/scripts/GoogleReger/properties

http://bablosoft.com/scripts/WLBBNChecker2/properties

http://bablosoft.com/scripts/NftBuy/properties

http://bablosoft.com/scripts/TelegramWebSpamerSubs/properties

http://bablosoft.com/scripts/AdsWatch/properties

http://bablosoft.com/scripts/MetaMaskChecker/properties

http://bablosoft.com/scripts/SlivmensPrivat/properties

http://bablosoft.com/scripts/VkReports/properties

http://bablosoft.com/scripts/BRUTECHECKERPL/properties

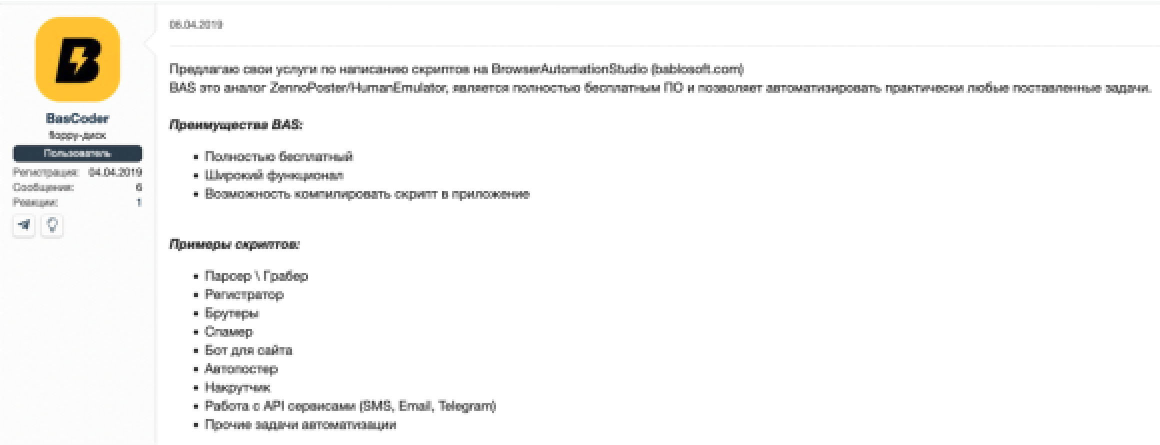
http://bablosoft.com/scripts/Rzd01/properties

Figure 4:

An Example of the Bablosoft Script Repositories

The postings also provided further insight into some of the tool’s capabilities; browser emulation, mimicking of human behavior (keyboard and mouse), proxy support, a mailbox search feature, and the ability to load data from file/URL/string. Features which have caught the eye of several distinct threat actor operations.

In underground forums we have identified users ‘offering their services’ for the creation of bespoke scripts for ***BAS***, for example to interact with the Telegram API, or the development of “bruters” and “recruiters”.



BasCoder
floppy-диск
Пользователь
Регистрация: 04.04.2019
Сообщения: 6
Реакции: 1

06.04.2019

Предлагаю свои услуги по написанию скриптов на BrowserAutomationStudio (bablosoft.com)
BAS это аналог ZennoPoster/HumanEmulator, является полностью бесплатным ПО и позволяет автоматизировать практически любые поставленные задачи.

Преимущества BAS:

- Полностью бесплатный
- Широкий функционал
- Возможность компилировать скрипт в приложение

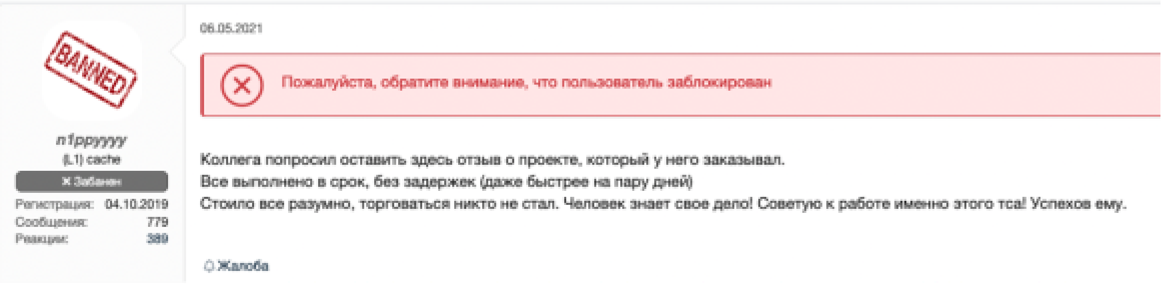
Примеры скриптов:

- Парсер \ Грабер
- Регистратор
- Брутеры
- Спамер
- Бот для сайта
- Автопостер
- Накрутчик
- Работа с API сервисами (SMS, Email, Telegram)
- Прочие задачи автоматизации

Figure 5:

Posting by ‘BasCoder’ on the XSS Forum

In the post above, the user ***BasCoder*** provides an overview of a business-like service, inclusive of a ‘free consultation’, with projects priced from $20 depending on scale. We identified a ‘thank you’ post from another user who appeared to have used ***BasCoder***’s services for a ***BAS****-related project.*



n1ppyyyy
(L1) cache
✖ Забанен
Регистрация: 04.10.2019
Сообщения: 779
Реакции: 389

06.05.2021

Пожалуйста, обратите внимание, что пользователь заблокирован

Коллега попросил оставить здесь отзыв о проекте, который у него заказывал.
Все выполнено в срок, без задержек (даже быстрее на пару дней)
Стоило все разумно, торговаться никто не стал. Человек знает свое дело! Советую к работе именно этого тса! Успехов ему.

Жалоба

A colleague asked me to leave a review here about a project I ordered from him. Everything was done on time, without any delays (even faster by a couple of days). The price was reasonable, not one to haggle. The man knows his stuff! I recommend this guy for work! Good luck to him.

Figure 6:

‘Customer’ Feedback Post on the XSS Forum

The customer in this case, a user called ***n1ppyyy***, is a now-banned but formerly active member of the XSS forum who engaged in numerous topics indicative of an interest or involvement in malicious activity.

Insight from Threat Telemetry

In the cases of the Bumblebee, BlackGuard and RedLine C2s, we observed connections to ***downloads.bablosoft[.]com*** (resolving to 46.101.13.144). Threat telemetry for this IP address provides an insight into the general user base for Bablosoft, with the majority of activity coming from locations in Russia and Ukraine (based on WHOIS information).

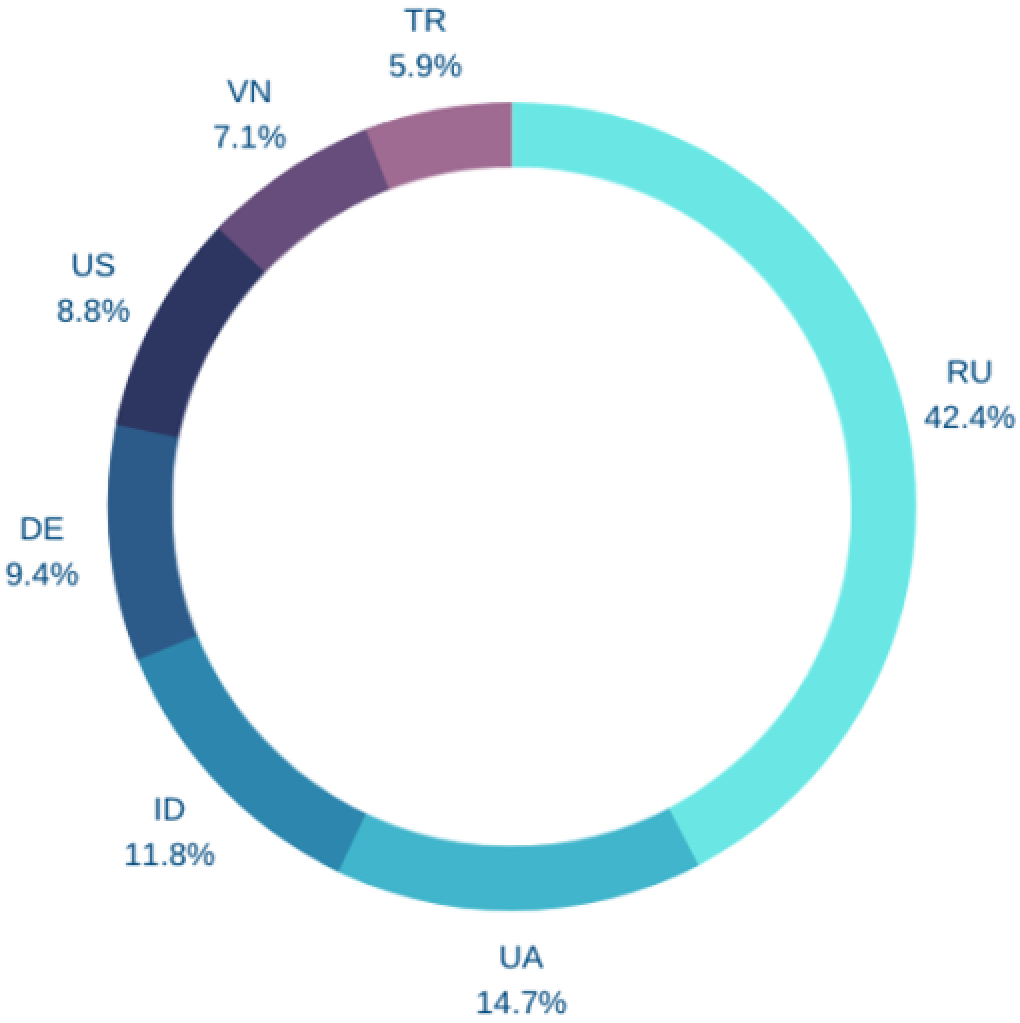
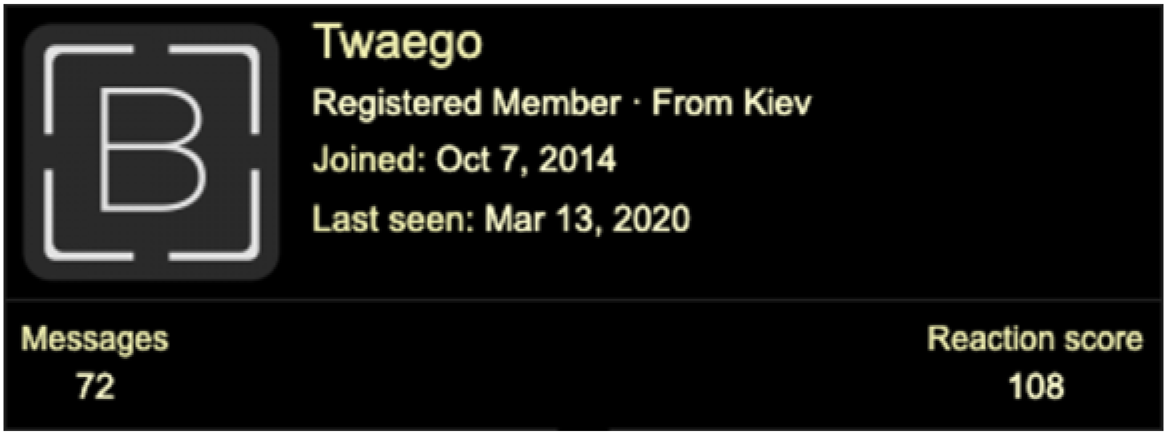


Figure 7:

Most Frequently Observed Country Codes

As for ***Twaego*** (the ‘owner’ of Bablosoft), their profile summary indicates they are from Kiev, Ukraine.



Twaego

Registered Member · From Kiev

Joined: Oct 7, 2014

Last seen: Mar 13, 2020

Messages
72

Reaction score
108

Figure 8:

Twaego User Profile Summary

We were able to corroborate this information based on management activity to several elements of the Bablosoft infrastructure, sourced from a single Ukrainian-assigned IP address. In addition, the IP was also involved with management connections to a number of hosts on TCP/27017 – commonly associated with MongoDB.

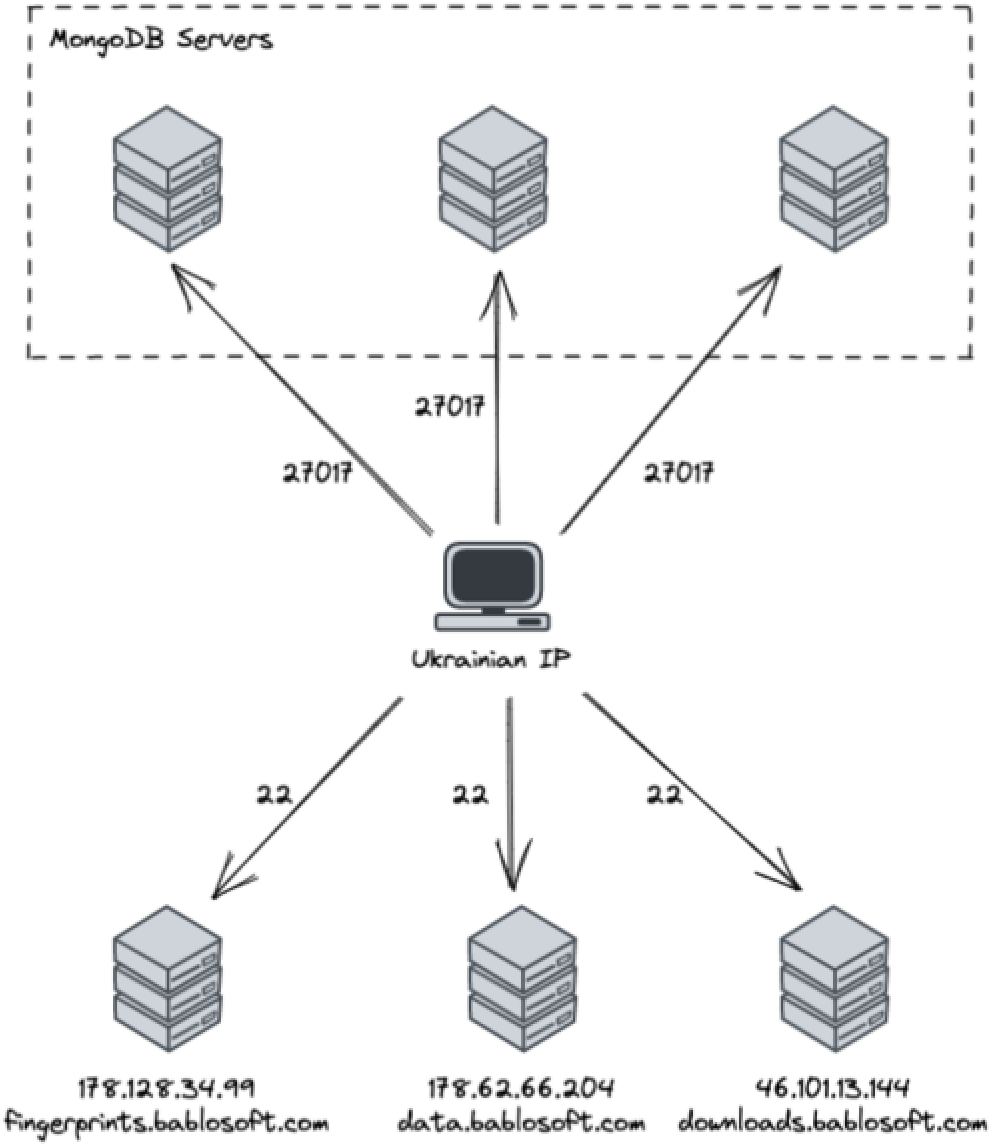


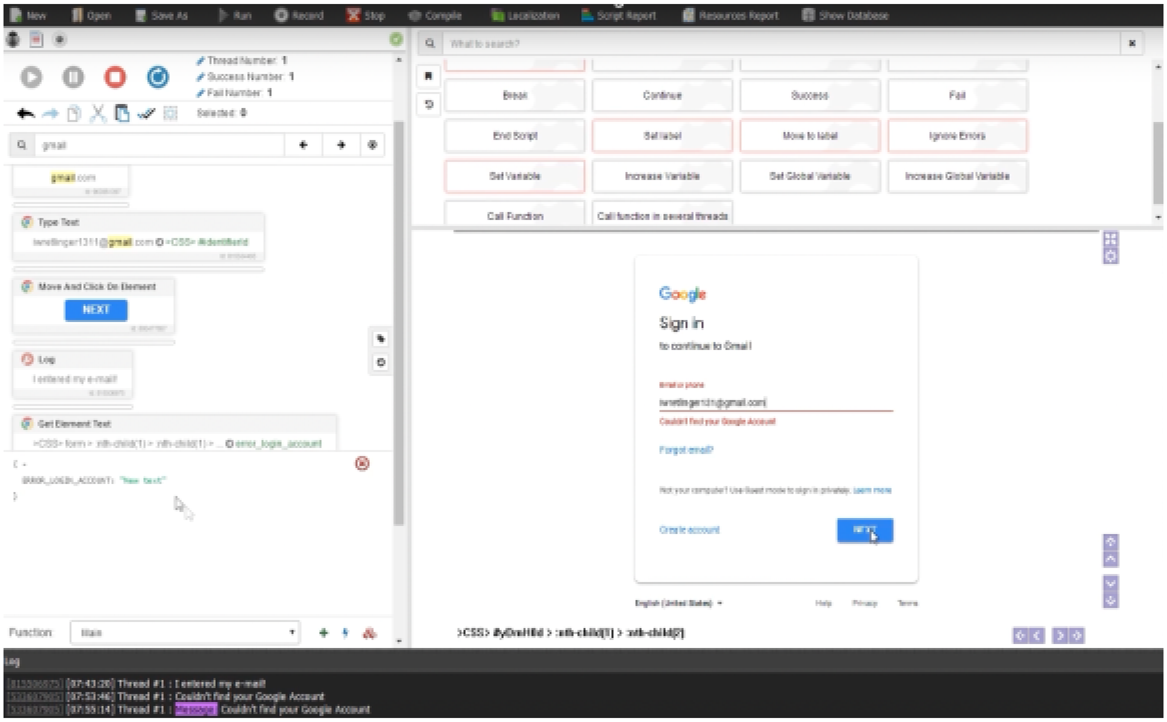
Figure 9:

Overview of Bablosoft Backend Infrastructure

Malicious Use Cases

As previously highlighted, we observed the Bumblebee, BlackGuard and RedLine C2 IPs connecting to the ‘downloads’ subdomain of ***bablosoft[.]com***, with the assumption that the operators were downloading tools for use in threat activities.

For the BlackGuard and RedLine C2s there are several use cases for ***BAS*** which may be applicable. For example, we identified a ‘gmail accounts checker’ which the threat actors might utilize for assessing the validity of stolen credentials.



```
[815306575] [07:43:20] Thread #1 : I entered my e-mail
[532607985] [07:53:46] Thread #1 : Couldn't find your Google Account
[532607985] [07:55:14] Thread #1 : Message Couldn't find your Google Account
```

Figure 10:

BAS Gmail Checker Tool

Whilst examining threat telemetry for other elements of the Bablosoft infrastructure, we identified several hosts associated with cryptojacking malware making connections to ***fingerprints.bablosoft[.]com***. The ***Fingerprint*** element of the ***BAS*** service allows users to alter their browser fingerprint, a function likely used by these particular actors as a means of anonymizing or normalizing their activity.

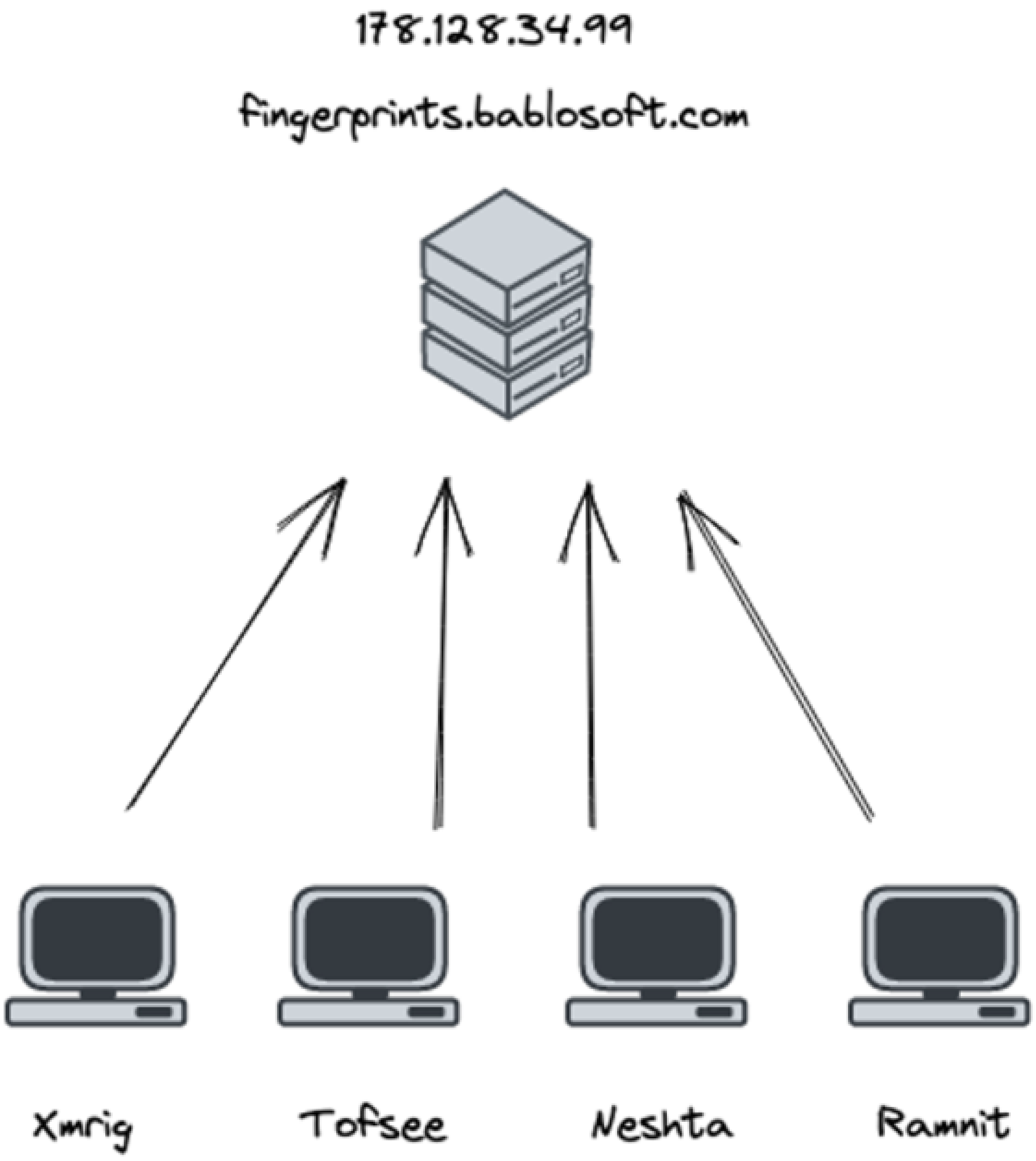


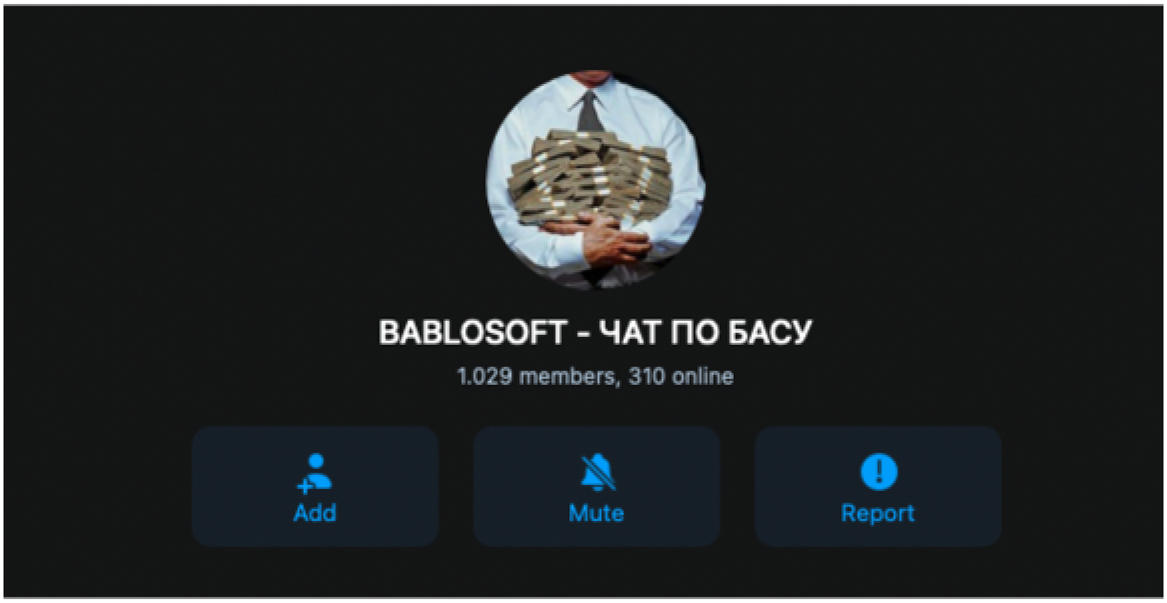
Figure 11:

Attribution of Cryptojacking Infrastructure

Conclusion

Based on the number of actors already utilizing tools offered on the Bablosoft website, we can only expect to see ***BAS*** becoming a more common element of the threat actor’s toolkit. As referenced by F5 Labs in their report on credential stuffing – “*One of the reasons we expect to see more of BAS is because of the Bablosoft community and how easy the software makes it to redistribute and sell work.*”.

An “unofficial” Telegram group, entitled ***Bablosoft – BAS chat*** (BABLOSOFT – ЧАТ ПО БАСУ), retains a membership of over 1,000 users, further highlighting the level of community activity around the tool. This group appears to be used predominantly by Russian speakers, to share updates on new features, scripts and tips.



BABLOSOFT - ЧАТ ПО БАСУ

1.029 members, 310 online

Figure 12:

Unofficial Bablosoft Telegram Group

IOCs

Bumblebee C2:

45.147.229.177

BlackGuard Panel C2:

185.173.157.26

RedLine Controller C2:

91.243.59.61