Uncovering the Anonymity Cloak

ke-la.com/uncovering-the-anonymity-cloak/

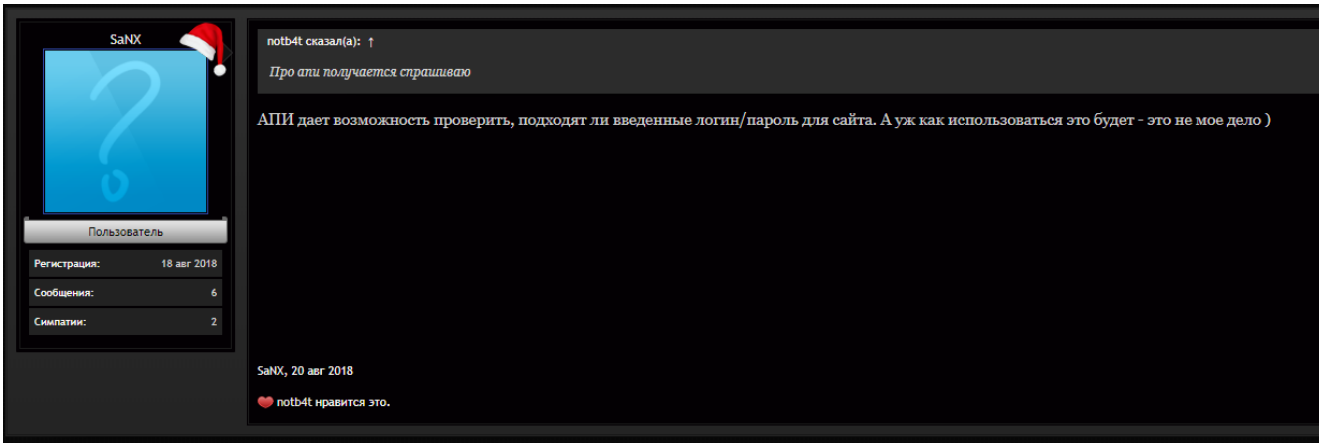
February 19, 2020

Due to its anonymity, the Darknet is flooded with threat actors working together to share information, services, and knowledge required to carry out successful cyber-attacks, particularly within the cybercrime financial ecosystem.

We've uncovered the real identity of a threat actor dubbed SaNX – a handle that has become an infamous one among many security departments of numerous leading corporations worldwide. Here, we'll also reveal his activities, other handles in the Darknet, and affiliations to other hacking groups.

A Creative Bypass for Account Validation

SaNX's line of services allows fraud actors to check whether a given set of stolen credentials are valid for popular banking, e-commerce and retail mobile apps.


SaNX

Пользователь

Регистрация: 18 авг 2018

Сообщения: 6

Симпатии: 2

notb4t сказал(а): ↑

Про апи получается спрашиваю

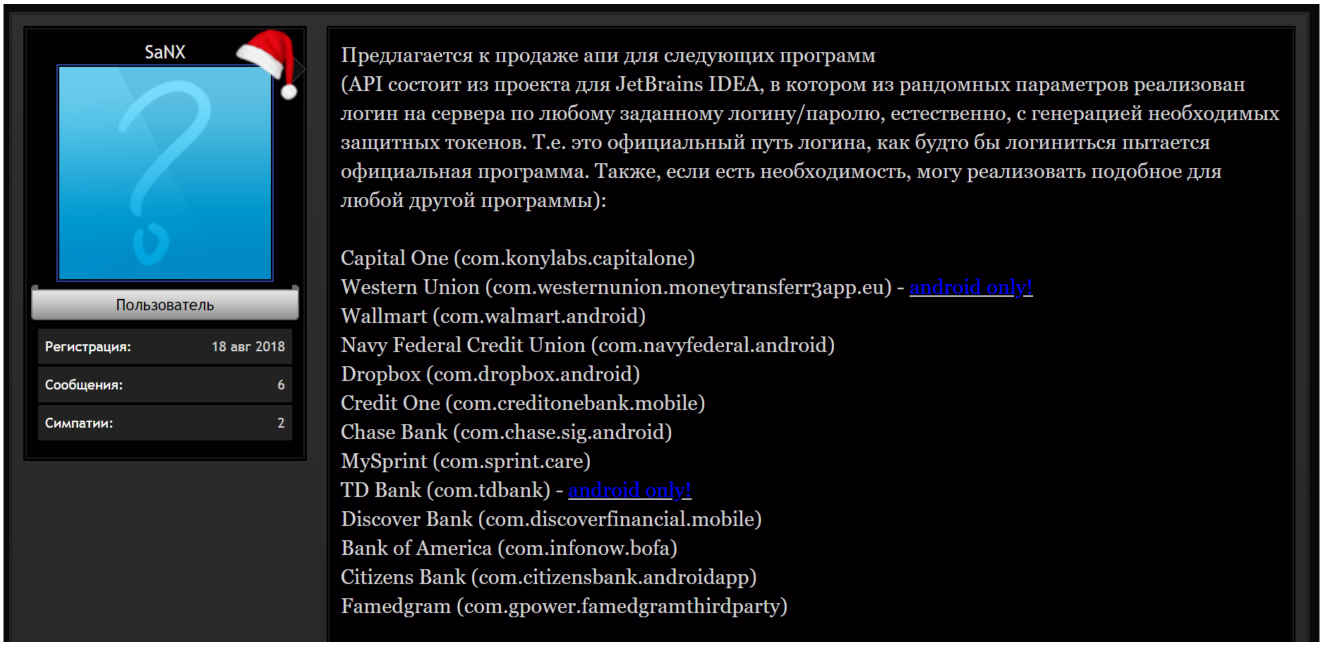
АПИ дает возможность проверить, подходят ли введенные логин/пароль для сайта. А уж как использоваться это будет - это не мое дело)

SaNX, 20 авг 2018

❤ notb4t нравится это.

Post by SaNX where he advertises his service, "API allows verification of the validity of the login details for a website. As to the possible exploits of the API, it's not my business"

While the service itself isn't new nor novel, the direction of SaNX's approach is interesting; he abuses possible flaws in the APIs used by mobile applications associated with the services, thus bypassing traditional security mechanisms used by companies. The capabilities supplied by these services are very useful to fraud actors and others who deal in account takeovers (ATO) for a variety of purposes.


SaNX

Пользователь

Регистрация: 18 авг 2018

Сообщения: 6

Симпатии: 2

Предлагается к продаже апи для следующих программ
(API состоит из проекта для JetBrains IDEA, в котором из рандомных параметров реализован логин на сервера по любому заданному логину/паролю, естественно, с генерацией необходимых защитных токенов. Т.е. это официальный путь логина, как будто бы логиниться пытается официальная программа. Также, если есть необходимость, могу реализовать подобное для любой другой программы):

Capital One (com.konylabs.capitalone)
Western Union (com.westernunion.moneytransferr3app.eu) - android only!
Wallmart (com.walmart.android)
Navy Federal Credit Union (com.navyfederal.android)
Dropbox (com.dropbox.android)
Credit One (com.creditonebank.mobile)
Chase Bank (com.chase.sig.android)
MySprint (com.sprint.care)
TD Bank (com.tdbank) - android only!
Discover Bank (com.discoverfinancial.mobile)
Bank of America (com.infonow.bofa)
Citizens Bank (com.citizensbank.androidapp)
Famedgram (com.gpower.famedgramthirdparty)

A list of the world's top financial organizations and mega-retailers, all targeted by SaNX. The list includes some of the major online retailers and banks across the United States, such as Walmart, Capital One, Bank of America, TD Bank, and more.

AI's Aid in Credential Stuffing

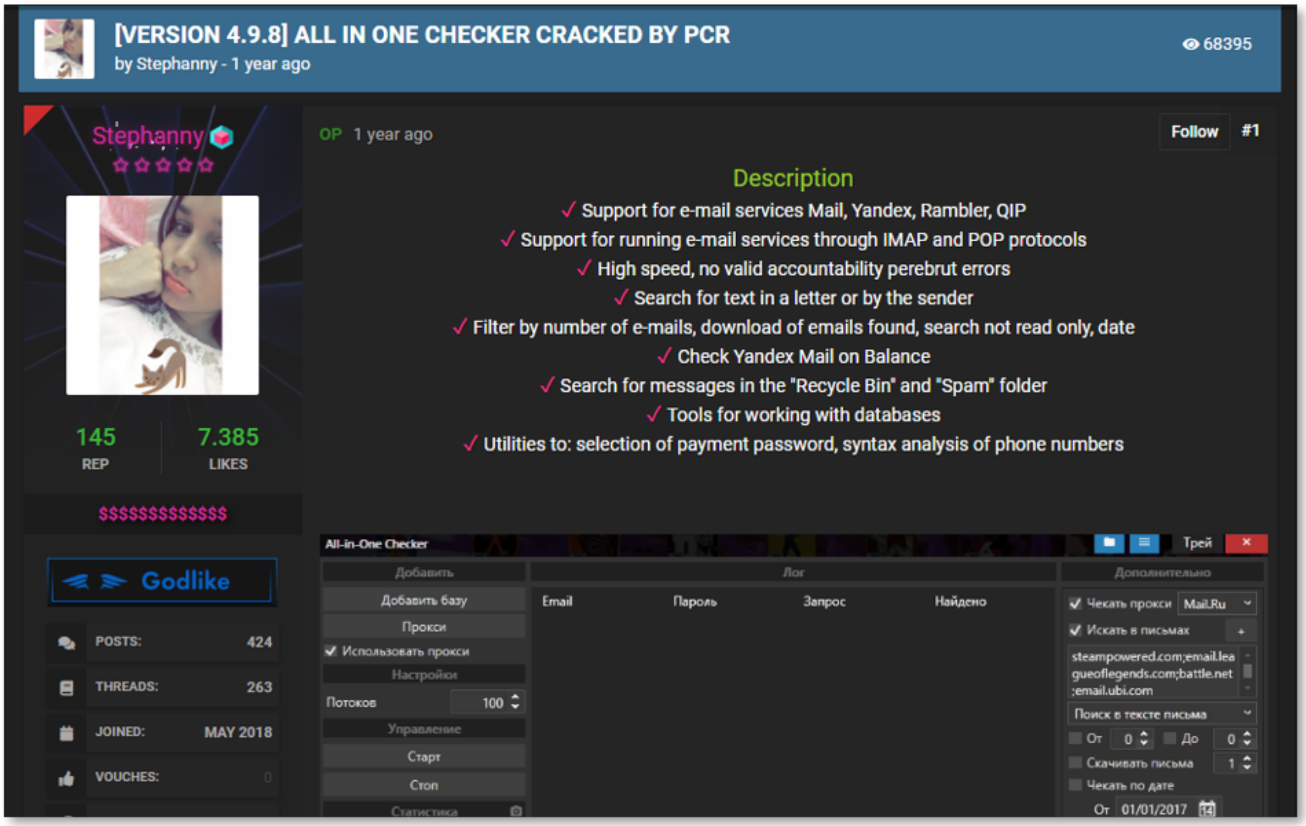
To best understand why SaNX’s products are so lucrative, let’s quickly review a generic scenario for how threat actors perform accounts takeovers by leveraging third-party data breaches.

Fraud actors commonly attack financial institutions, retailers and other consumer-facing businesses by taking over accounts via credential stuffing. To perform such a strike, the attacker needs only three elements:

1. Targets – The cybercrime financial underground is chock-full of tutorials and walkthroughs on fraudulent cashing out of “cracked” e-commerce, retail and even gaming accounts.

2. Credentials – A known commodity in the criminal underground, as multiple vendors specialize in breaching internet-facing databases and selling their content to other criminals. This usually comprises usernames, emails and passwords that can later be re-used against popular targets.

3. Automation, however, is key in the credential stuffing process. Since attackers usually employ a spray-and-pray approach, more credentials equal a higher success rate. Tools that automate the checks of credentials against a target website are widespread in low-level carding and cracking communities. They come in a variety of flavors – from SaaS services operated by cybercriminals to simple “checkers” desktop clients – with a few tools, such as Sentry MBA, achieving well-earned notoriety and having dedicated communities in the criminal underground.


[VERSION 4.9.8] ALL IN ONE CHECKER CRACKED BY PCR

by Stephanny - 1 year ago

68395

Stephanny

145 REP

7.385 LIKES

$$$$$$$$$$$$$

Godlike

POSTS: 424

THREADS: 263

JOINED: MAY 2018

VOUCHES: 0

OP 1 year ago

Description

✓ Support for e-mail services Mail, Yandex, Rambler, QIP
✓ Support for running e-mail services through IMAP and POP protocols
✓ High speed, no valid accountability perebrut errors
✓ Search for text in a letter or by the sender
✓ Filter by number of e-mails, download of emails found, search not read only, date
✓ Check Yandex Mail on Balance
✓ Search for messages in the "Recycle Bin" and "Spam" folder
✓ Tools for working with databases
✓ Utilities to: selection of payment password, syntax analysis of phone numbers

☑ Использовать прокси

Потоков 100

☑ Чекать прокси Mail.Ru

☑ Искать в письмах

steampowered.com;email.leagueoflegends.com;battle.net;email.ubi.com

Поиск в тексте письма

□ От 0 □ До 0

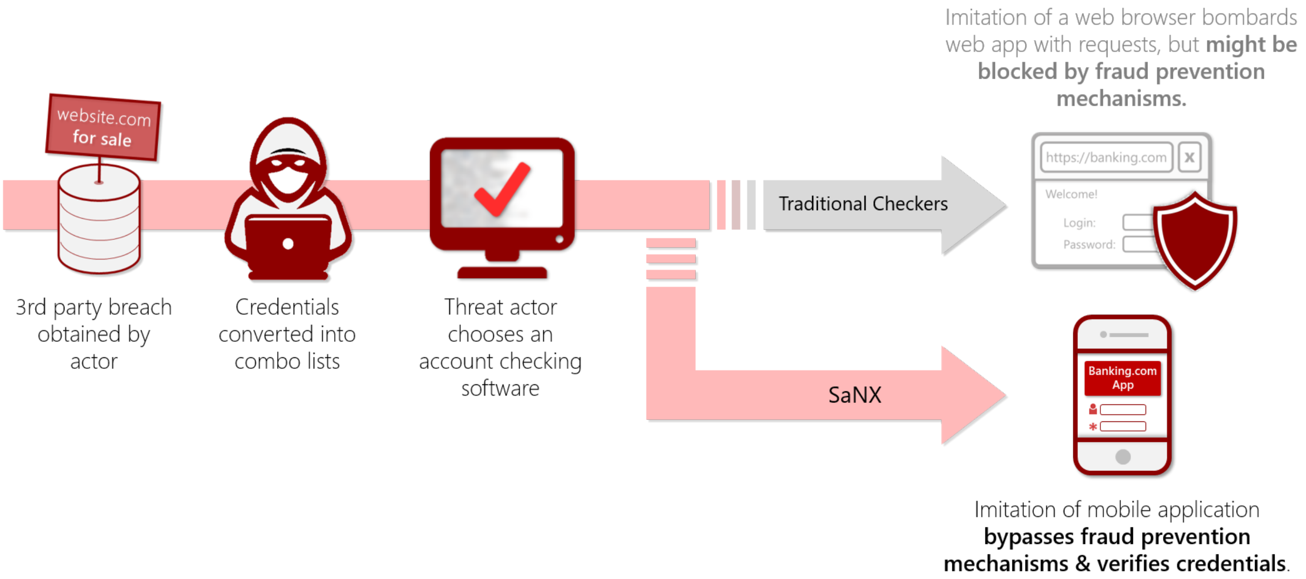
□ Скачивать письма 1

□ Чекать по дате

От 01/01/2017

A generic, "all in one" checker offered on a cracking forum

As credential stuffing tools grew ubiquitous in the criminal underground, most organizations implemented anti-fraud mechanisms to thwart "checking" attempts from low-level tools. This is where SaNX enters the equation. Most checkers target web applications via imitating browsers, and as such are susceptible to being intercepted by fraud prevention. SaNX's approach tackles the mobile API – thus allegedly bypassing the standard.

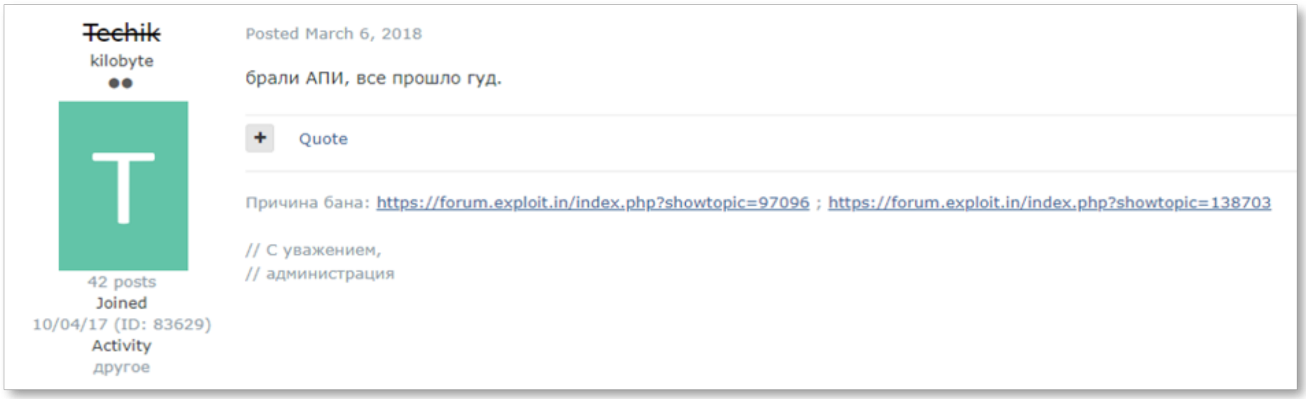

Imitation of a web browser bombards web app with requests, but **might be blocked by fraud prevention mechanisms.**
website.com for sale
3rd party breach obtained by actor
Credentials converted into combo lists
Threat actor chooses an account checking software
Traditional Checkers
https://banking.com
Welcome!
Login:
Password:
SaNX
Banking.com App
Imitation of mobile application **bypasses fraud prevention mechanisms & verifies credentials**.

The general process of account takeovers. Threat actors can choose a traditional checker for credential stuffing, or alternatively go through SaNX's services that imitate a mobile application's API, and likely bypasses fraud prevention mechanisms.

SaNX's services pose fraud threats to organizations' security as they expose them to brute force or credential stuffing attacks by leveraging what appears to be a security blind spot. Even though offering relatively sophisticated services, it's important to note that SaNX is simply another link to the chain of services offered in the cybercrime financial ecosystem; acquiring the "private APIs" isn't a magic bullet that attackers can use against an organization. Unlike simple checkers, SaNX puts most of his effort into the API itself and not necessarily on mass scale and automation, requiring his clients to integrate the tools into a wider credential stuffing framework.

The Proof is in the Pudding

The key to a business's growth and success is to execute it in a way that will attract and satisfy customers. As Darknet businesses evolve towards more "professional" business models and practices, attracting new customers is dependent on the level of innovation and novelty of the idea. Long-term success, however, is particularly dependent on customer satisfaction. To determine SaNX's credibility as a seller in the Darknet, we decided to assess his buyers' reviews. Numerous posts indicated that SaNX maintains a high level of credibility and is considered to be a particularly professional threat actor (see below).



~~Techik~~
kilobyte
●●
42 posts
Joined
10/04/17 (ID: 83629)
Activity
другое

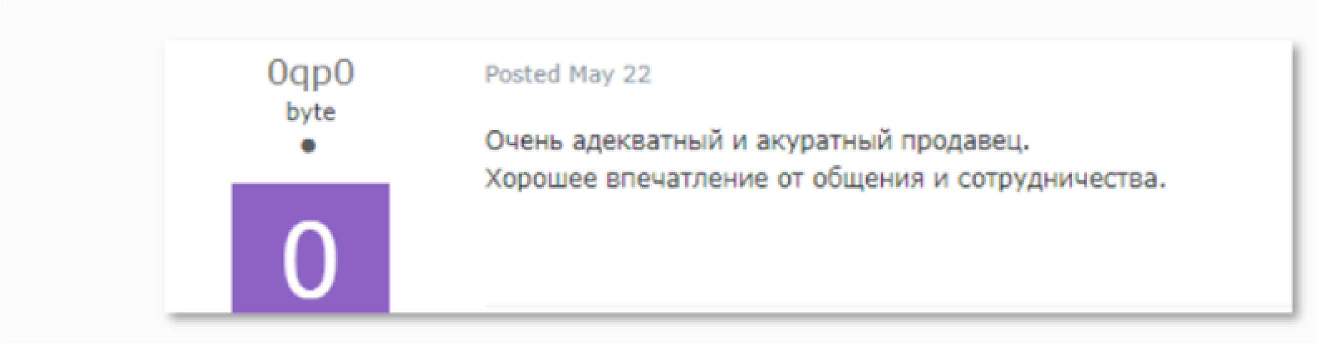
Posted March 6, 2018

брали АПИ, все прошло гуд.

Причина бана: https://forum.exploit.in/index.php?showtopic=97096 ; https://forum.exploit.in/index.php?showtopic=138703

// С уважением,
// администрация

User in a Russian-speaking underground forum says about SaNX's services: "We bought API; everything went well" (March 5, 2018)



0qp0
byte
●

Posted May 22

Очень адекватный и акуратный продавец.
Хорошее впечатление от общения и сотрудничества.

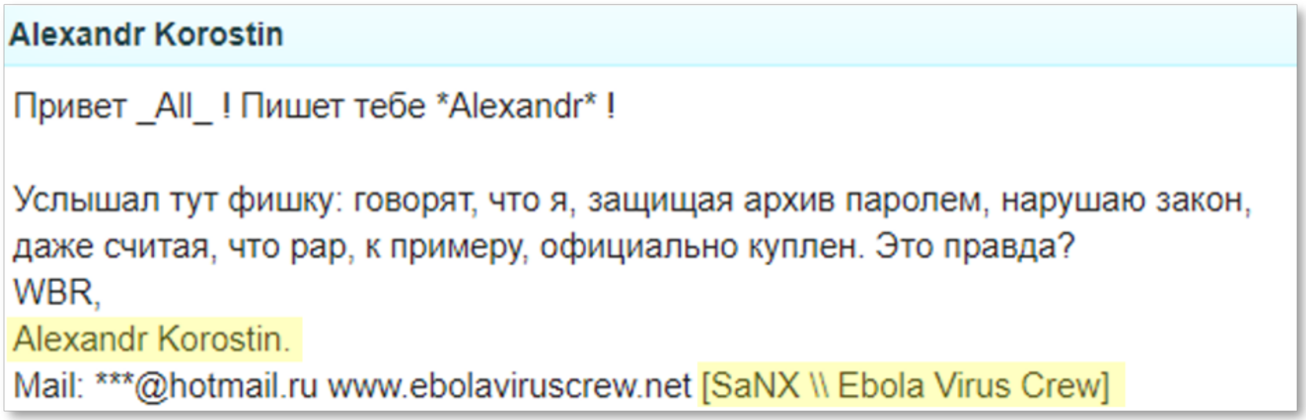
From Russian: "Very professional and accurate seller. I've gotten a good impression of working with him" (May 22, 2019)

These relatively recent reviews confirm SaNX's ongoing efforts and successes, which only motivated our researchers to dig further and identify this harmful threat actor by name and any other PII that could help track him down.

Lifting the (Limited) Anonymity Cloak of the Darknet

Maintaining anonymity has become a difficult challenge in the Darknet with the growth of digitalization. Hackers will almost inevitably leave traces of their activities, enabling threat researchers to perform research to identify them.

We began by finding a post signed by SaNX in a FidoNet thread where we were already able to assert his connection to the hacking group, Russian Ebola Virus Crew ("EVC"), along with his full name and email address.



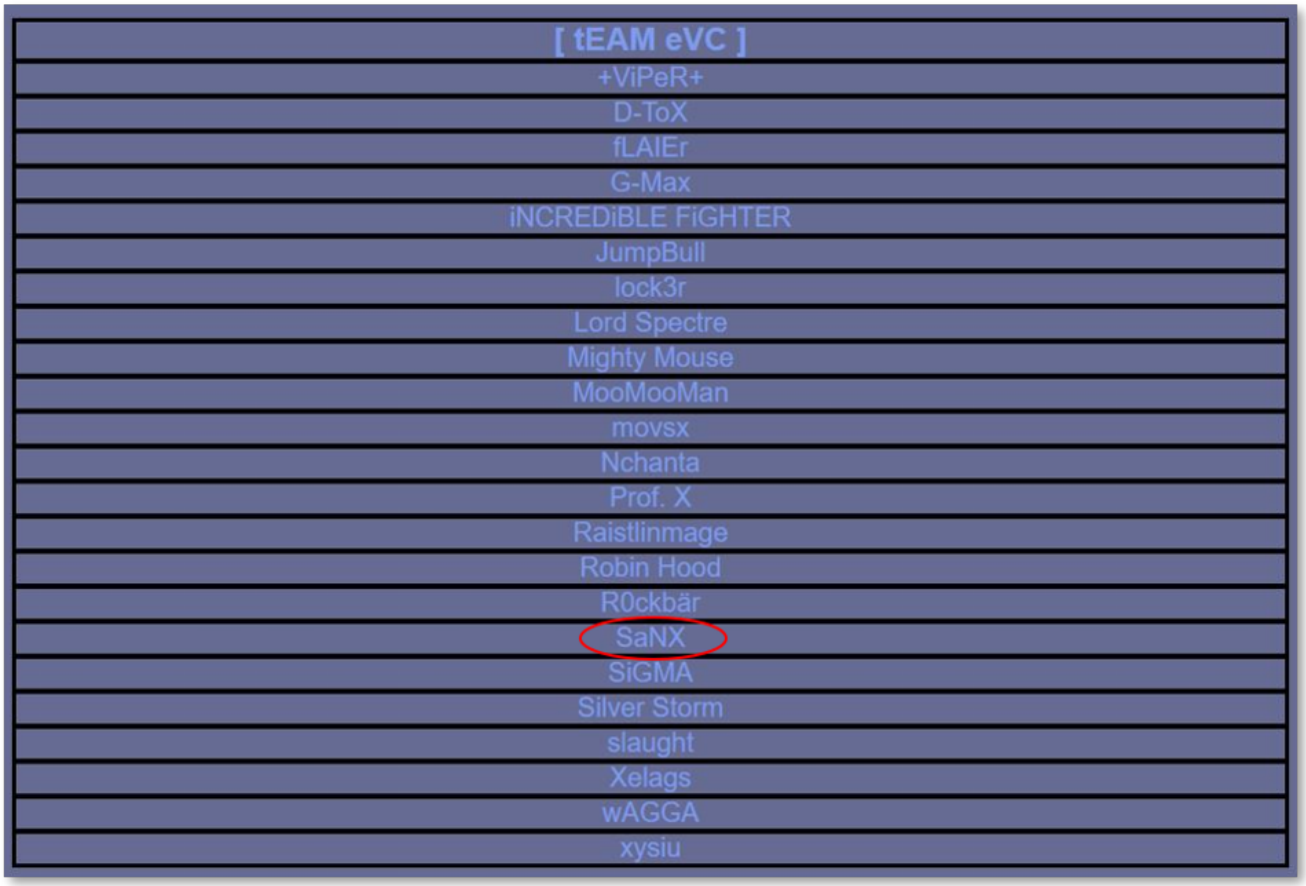
Alexandr Korostin

Привет _All_ ! Пишет тебе *Alexandr* !

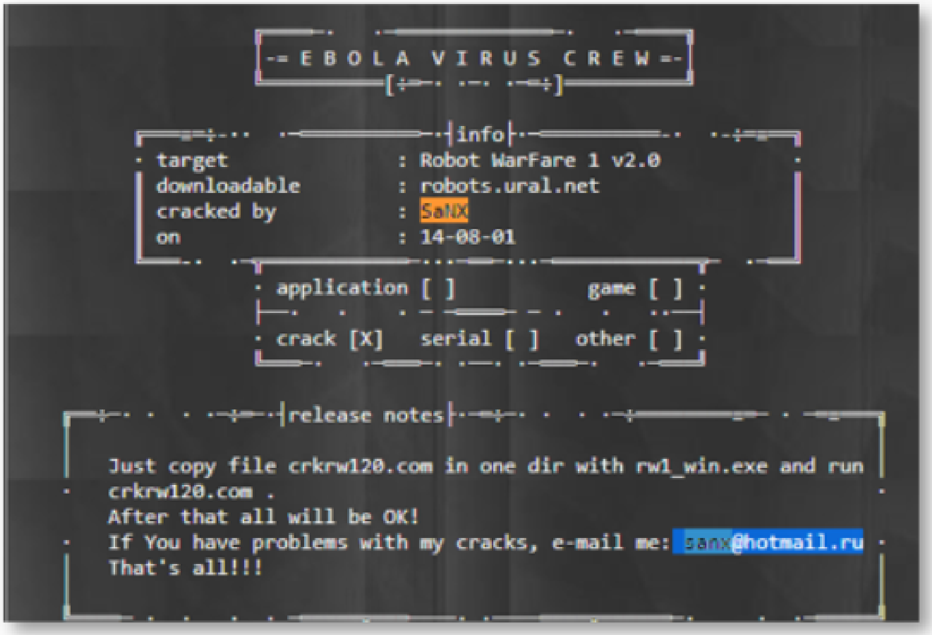
Услышал тут фишку: говорят, что я, защищая архив паролем, нарушаю закон, даже считая, что рар, к примеру, официально куплен. Это правда?
WBR,
Alexandr Korostin.
Mail: ***@hotmail.ru www.ebolaviruscrew.net [SaNX \\ Ebola Virus Crew]

This was a post found as a part of an in-depth research performed when looking for posts by SaNX. Here, SaNX was seen signing his name (Alexander Korostin) and EVC connection on a post from 2003 within a FidoNet thread. This research was done using KELA's proprietary tool, DARKBEAST, which enables users to search through years of historical Darknet data stored in KELA's data lake.

We then found further affirmations of the connection between EVC and SaNX, when various statements by EVC were found declaring SaNX as one of its members.



[tEAM eVC]
+ViPeR+
D-ToX
fLAIEr
G-Max
iNCREDiBLE FiGHTER
JumpBull
lock3r
Lord Spectre
Mighty Mouse
MooMooMan
movsx
Nchanta
Prof. X
Raistlinmage
Robin Hood
R0ckbär
SaNX
SiGMA
Silver Storm
slaught
Xelags
wAGGA
xysiu



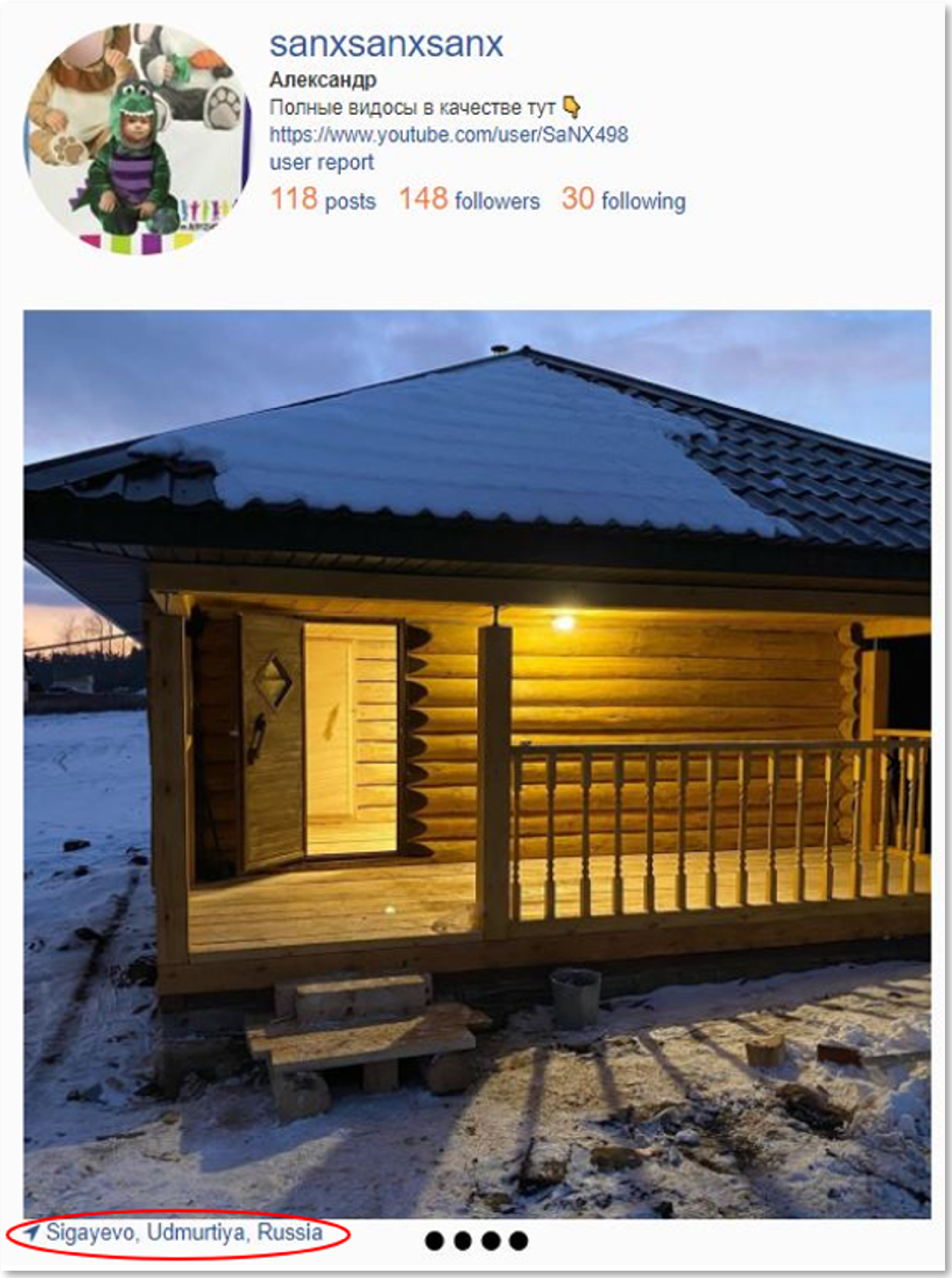
```
                 -= E B O L A   V I R U S   C R E W =-

        ┌─────────────────────┤info├─────────────────────┐
        · target              : Robot WarFare 1 v2.0     ·
        │ downloadable        : robots.ural.net          │
        │ cracked by          : SaNX                     │
        │ on                  : 14-08-01                 │
        └────────────────────────────────────────────────┘
                 · application [ ]          game [ ] ·
                 · crack [X]   serial [ ]   other [ ] ·

    ┌──────────────┤release notes├────────────────────────────────┐
    │                                                             │
    │  Just copy file crkrw120.com in one dir with rw1_win.exe and run │
    ·  crkrw120.com .                                             ·
    │  After that all will be OK!                                 │
    ·  If You have problems with my cracks, e-mail me: sanx@hotmail.ru ·
    │  That's all!!!                                              │
    └─────────────────────────────────────────────────────────────┘
```

SaNX being listed as a member of the Russian Ebola Virus Crew (EVC) hacking team.

By using his name and affiliation to EVC as a basis to search other handles used by SaNX, we were led to more of his PII. We later noticed that SaNX began using a new name, which was simply a combination of his full name and affiliation to EVC, "Alkorevc": Al(exandr)kor(ostin)evc.

Enough proof was pointing to the fact that SaNX was indeed Alexander Korostin and that he was affiliated to EVC, but there was more information out there related to SaNX. We started browsing through various websites and we were eventually directed towards a local community website, Izhevsk.ru, where "SaNXeVC" was seen responding to one of the posts on a transportation-related thread in Sokolovka, a locality in the Sarapul District of the Udmurtiya Republic in Russia. Taking note of this location, we continued our search to see if it could be confirmed.

Looking at SaNX's social media pages, we found a YouTube channel registered as "SaNX498" by the name "Aleksandr Alekseyevich" with video uploads from the Udmurtiya Republic, but it didn't stop there. Just like your everyday internet user would link their social media accounts for convenience, SaNX's linked his YouTube page to an Instagram profile bearing the name "sanxevc", which he recently changed to "sanxsanxsanx". His Instagram showed photos of Aleksandr from Sigayevo, Sarapul District, Udmurtiya Republic, reconnecting us to the original location that we detected earlier.



sanxsanxsanx

Александр

Полные видосы в качестве тут 👇

https://www.youtube.com/user/SaNX498

user report

118 posts 148 followers 30 following

Sigayevo, Udmurtiya, Russia

●●●●

Pictures taken from SaNX’s Instagram profile, showing his location

One final search helped us confirm our findings. By searching the name “Aleksandr Korostin” in Russian (Александр Коростин) we were exposed to his profile in a local job-hunting board. We were given access to view his resume uncovering more information on his educational and occupational background, his date of birth (December 10, 1982), and a headshot.

All of these dots allowed us to finalize and close the priorly ambiguous case. So here we had it, SaNX or rather, 36-year-old, Aleksandr Alekseyevich Korostin (Александр Алексеевич Коростин) from Sigayevo, Sarapul District, Udmurtiya Republic, Russia, is no longer anonymous.

Takeaways and Lessons Learned

APIs are an imperative part of digitized organizations today, allowing mobile apps or websites to communicate more effectively, and ultimately make clients’ lives easier and more convenient. More flexibility for users, however, can exponentially increase the attack surface for bad actors. Organizations must continue to monitor for newer and more sophisticated threats that will continue to emerge with technological advancements. While we can’t take down every threat actor operating in the Darknet, we can certainly deter attacks and mitigate threats that are targeting large organizations.

Ask our team what your organization can do today to detect sophisticated threats against your organization before a potential cyberattack happens.