



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

War In Ukraine Shifts Landscape Of The Criminal Underground

The ongoing war in Ukraine is challenging longstanding codes of conduct that have governed behaviour in the criminal underground, which is likely to lead to an escalation in information warfare and cyber attacks against competing ideological camps. Like-minded groups are forming camps around those who support Russia, those who support Ukraine, and those who are striving to maintain the code of remaining politically neutral and not attacking a fellow CIS country.

In late February 2022, untested threat actor “devulz” shared a statement from the Conti ransomware team on the Russian language Deep Web forum “RAMP”. In the statement, the Conti gang came out strongly for Russia, threatening to retaliate against any U.S. cyber-attacks aimed at critical infrastructure in Russia or any other Russian-speaking country. In retaliation, an undisclosed actor leaked private chats and Bitcoin addresses related to Conti.

Conti’s stance has caused a schism amongst Russian-speaking threat actors; well-regarded threat actor “Rehub” argued on the Russian language Deep Web forum xss[.]is that because of the heightened tensions between the U.S. and Russia, that ransomware teams were no longer being pursued by the Russian government. In other extreme cases, researchers observed threat actors make the argument that because of the U.S. sanctions on Russia, ransomware attacks should be legalized and taxed by Russia.

Conversely, threat actors on the new English language Deep Web forum raidforums2[.]com have made it their mission to battle back against Russia. The original “RaidForums” domain was hijacked by undisclosed actors in late February 2022 with rumors abounding the site was turned into a phishing page to harvest user credentials. The newly launched “RaidForums2” domain includes an entire forum section dedicated to fresh leaks of Russian-based targets, successfully compromised by the “Against the West” hacktivist group, which is publishing dozens of leaks daily.

A post from threat actor “devulz” sharing a statement from the Conti ransomware team; a screenshot of the new raidforums2[.]com domain.

War In Ukraine Shifts Landscape Of Underground Cont.

Conti & USA?
devulz · Friday at 8:50 PM

Forums > Other \ 其他讨论 > Offtopic \ 其他社区讲座

Jump to new Watch

Friday at 8:50 PM

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression."

devulz
Nov 2, 2021
Messages 25
Reaction score 16
Points 3

RAIDFORUMS2

Portal Forum Member List Calendar Help *****WARNING Raidforums.com has been SIEZED*****

transaction id, and proof of payment. Also which package did you purchase?', 1421089994), 124812, 'Please provide transaction id, and proof of payment. Also

RaidForums2

Breaking News

ATW Updates ATW has begun another round of raids against Russia	18 18	RUSSIAN PromEngineering L... Yesterday, 11:55 PM by burkeluke
Ukraine Invasion Mega-Thread Post any insight into the ongoing conflict	6 6	NEW TARGETS from IT Army ... Yesterday, 01:30 PM by burkeluke
Raidforums.com Tracking the current status of Raidforums.com	2 9	Status update 02-27-2022, 06:25 PM by theklob

New Tool Facilitates Negotiations Between Ransomware Operators, Victims

Well-regarded threat actor “darksoftware” advertised their new tool to facilitate negotiations between ransomware operators and their victims on the Russian language Deep Web forum exploit[.]in. The appearance of this tool, dubbed “BusinessCallback”, indicates that new ransomware attacks are likely imminent because it is focused on the anonymity of ransomware operators, allowing them to host the application on their own servers.

The tool provides these threat actors with access to an administrative panel where they can easily add or delete new users and manage contact lists. Victims are given access to a separate web interface where they can securely chat with ransomware operators via Tor if they are willing to negotiate. Additional features of the tool include:

- Sends text messages
- Uploads files
- Displays status of victim (online, typing message)
- Logs victim activity
- Works with systems running Windows and Debian
- Backend written in C++ using Qt5 framework
- Frontend does not contain software dependencies

The actor charged \$500 USD to own the tool; they also offered the source code for \$1,500.

Original post from the threat actor "darksoftware" announcing the "BusinessCallback" tool.

New Tool Facilitates Ransomware Negotiations Cont.



BusinessCallback A one-stop solution for anonymous customer feedback

By darksoftware, 22 hours ago in [Other] - everything else

Follow 1

Start new topic

Reply to this topic

darksoftware

gigabyte

•••••



Paid registration

8

107 posts

Joined

06/05/21 (ID: 117090)

Activitycoding

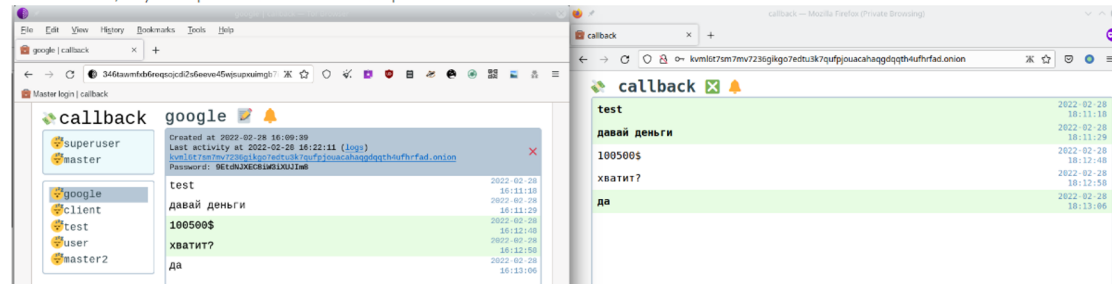
/ coder

Posted 22 hours ago (edited)

BusinessCallback

A universal solution for organizing anonymous feedback from customers.

BusinessCallback or simply "bc" is a lightweight cross-platform messenger server with a web interface. It is focused on the anonymity of the administrative staff, the simplicity of creating new users, as well as the complete portability of the existing database to the new server, that is, portable. Provides self-hosting on your server without any calls to the outside world from your side. The architecture is based on the complete isolation of users from each other, only direct parent-child connections are quoted.



Cooperation More Likely Between Chinese, Russian Ransomware Actors

Untested threat actor “RTM” advertised their team’s new ransomware-as-a-service (RaaS) project in multiple languages, including Chinese, on the predominantly Russian-speaking Deep Web forum “RAMP”. This suggests that Chinese-speaking threat actors are likely becoming more willing to cooperate with Russian threat actors on matters involving ransomware.

The actor also shared their post in Russian and English; however, they specified that they were only willing to work with Russian-speaking threat actors. This is significant because it could mark the first time that a state-sponsored, Chinese speaking threat actor has offered their services to the Russian public.

According to the actor, the project is written in C++ and does not contain software dependencies. The ransomware is designed to target:

- VMware EXSi servers
- Systems running Windows
- Network-attached storage (NAS) devices

The untested threat actor “Charodej” replied to the actor’s thread, asking if they translated the English and Russian versions of their post because they both contained grammatical errors. This further adds legitimacy to the assertion that this is a RaaS project coded by Chinese-speaking threat actors.

Original post from
threat actor "RTM" in
Chinese

Cooperation More Likely Between Chinese, Russian Actors Cont.

RTM
team

RTM

Nov 30, 2021

Messages 6

Reaction score 1

Points 3

Thursday at 4:19 AM

介绍 RTM Team Locker 联盟计划

柔软的:

- C++
- 该软件是在没有任何依赖关系的情况下编写的
- ESXI/WIN/NAS
- 强大的全加密

=====

禁止:

- 在独联体工作
- 排出构建和面板/博客地址

=====

- 任何通讯只 TOX
- 我们将有趣的目标纳入工作中
- 提交申请时, 准备好回答一些问题
- 我们不与讲英语的人合作 (除非有讲俄语的合作伙伴)
- 工作从您的方向的 70% 开始, 从声誉、目标数量修改条件
- 我们不把每个人都当成合作伙伴, 我们对质量和经验感兴趣
- 与具有潜在共振的目标一起工作
- 可以为您的 TOH 创建构建 (仅适用于有声誉的人)

=====

只能通过论坛的 PM 联系 (仅限 TOX)

我提前请求那些乱码乱写的人不要写, 不要浪费我们的时间。

New Service Creates NFT Projects To Be Used In Fraudulent Operations

Well-regarded threat actor “gustavdore” advertised their service to create non-fungible token (NFT) projects they claim can be used in fraudulent operations on the Russian language Deep Web forum “RAMP”. ZeroFox researchers assess this growing trend could mirror the initial coin offering (ICO) scams that lure victims into investing in fake cryptocurrencies, due to the rise in popularity of NFTs.

The actor claims their service includes advertising for the fraudulent NFT project, which ZeroFox notes is one of the underlying conditions that would need to be met for the operation to be successful. The actor also claimed they were willing to customize the project based on customer input. There is no indication the actor is creating malicious NFTs; it is more likely their service employs social engineering to steal money from victims.

Prices for the service started at \$2,500.

