



ZEROFOX[®]

Your Intelligence Digest

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

War In Ukraine: Takeaways From The Underground

The ongoing war in Ukraine is making it increasingly more difficult for threat actors to remain politically neutral in the criminal underground. This has led to an increase in cyber attacks against entities that are either perceived to be pro-Russian or pro-Ukrainian.

In early March 2022, ZeroFox observed the hacktivist group “Against the West” publish new leaks of sensitive data related to several Chinese targets, on the English language Deep Web forum [raidforums2\[.\]com](#). These targets were likely selected due to China’s muted response to Russia’s invasion of Ukraine. The impacted companies include:

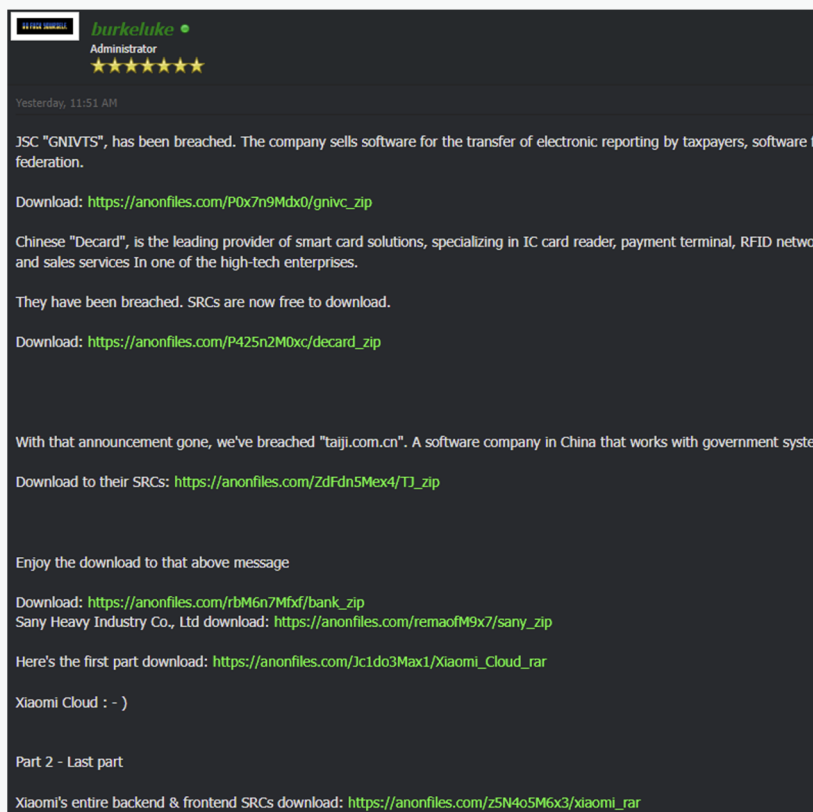
- Decard, a smart card solutions provider
- Xiaomi, a software contractor with the Chinese government
- SANY, a heavy equipment manufacturing company

ZeroFox researchers have not observed any public deals involving network access to U.S. companies featured on Russian speaking underground forums like [exploit\[.\]in](#), [xss\[.\]is](#), or [RAMP](#) since late February 2022. This could indicate that initial access brokers are now communicating directly with ransomware teams or through over other covert channels. Ransomware teams have shown more aggression in their attacks since the start of the war, as there is currently little fear of prosecution in Russian for these acts. ZeroFox researchers warn that an increase in access deals could lead to a surge in ransomware attacks in 2022, especially against U.S. companies.

Finally, ZeroFox researchers have observed malware being disguised as leaks of Russia-based entities on Telegram. The heightened interest among threat actors to acquire data related to Russia likely increases the chances of threat actors successfully compromising more systems.

Screenshots highlighting recent "Against the West" leaks on "RaidForums2" (left) and lack of public network access deals involving U.S. companies on Russian underground (right)

War In Ukraine Takeaways Cont.



● **Продажа Шеллов с DA / Шопы magento**
By DezMond, January 6, 2021

● **I BUY Bulk CPANELsss**
By TCVInvestments, August 17, 2021

● **Сотрудничество!**
By SergeyMavrodi, August 15, 2021

● **Продажа качественных брут дедиков [hacked rdps]**
By Neizvestnost74, February 23

● **[ПРОДАЮ] Cpanels**
By SoulCollector001, Wednesday at 08:25 AM

● **Продам шелы**
By Amigo_01, February 22

● **Продажа cPannels** 1 2
By valeanz, July 24, 2021

▲ **Selling SS7 Gateway Access**
By CryptBB, Sunday at 05:04 PM

● **куплю доступы**
By farnetwork, October 24, 2020

● **Материал для 1/0-Day Exploits / Spear Phishing / Brute-Force - Scan Service**
By marmalade_knight, October 1, 2021

● **Выкуплю доступы**
By JohnDetmer, April 7, 2021

● **Продажа cPannels, WordPress**
By Saiwer, January 14

Zero-day Advertised For RCE Vulnerability In SS7 Gateway Devices

On 15 March 2022, well-regarded threat actor, administrator, and known signaling system no. 7 (SS7) access dealer “LongPig” advertised a zero-day exploit for a remote code execution (RCE) vulnerability in Sangoma Netborder SS7 gateway devices, on the English language Dark Web forum “CryptBB”. This is significant since multiple telecommunications companies around the world use these gateways to decode the SS7 signaling protocols responsible for establishing wired/wireless phone calls, SMS messages, number translation, and prepaid billing services.

The actor claims that their exploit would allow an unauthenticated threat actor to remotely execute code on the impacted SS7 gateway devices. This would potentially facilitate various types of attacks, including:

- SIM-swapping
- Bypassing multi-factor authentication (MFA) codes for services sent via SMS

The actor charged \$80,000 for the exploit.

“LongPig” advertised the same zero-day exploit on the Russian language Deep Web forum exploit[.]in. However, the deal was shut down based on the actor’s failure to meet forum escrow requirements.

ZeroFox researchers note that legitimate access to SS7 gateways and exploits in SS7 gateways are difficult to obtain, and when publicly advertised, these kinds of deals are typically purchased immediately through off-forum communications.

Original post from threat actor "LongPig" announcing a zero-day exploit for a remote code execution (RCE) vulnerability in Sangoma Netborder SS7 gateway devices

Zero-day For RCE Vulnerability In SS7 Gateway Devices Cont.

[New Reply](#)

[Official] Netborder SS7 0day RCE as root



LongPig •
CryptBB Admin
Administrator
●●●●●●●●

Posts: 420
Joined: May 2017

11 hours ago

#1

I am selling a 0day RCE as root for Netborder SS7 gateway web panel, it doesnt require login and you can exec almost any bash command, also i will provide small bash obfuscated script to spawn a reverse shell for netcat from the RCE.

Price: 80k\$ both BTC and XMR are accepted.

Contact me on XMPP or via PM to buy please avoid contact me if you do not have the required money or just to waste my time asking info, price can be negotiated.

XMPP: longpig@jabber.calyxinstitute.org

Contacts:

XMPP: longpig@jabber.calyxinstitute.org
XMPP: longpig@cryptbbsfmzv6dq4ec2iv6ravrw5ohgmikfagqhtvkgiaknvt5fylqd.onion

Compromised SCADA Systems In U.S. & Other Countries

New but positively trending threat actor “boxi” advertised compromised supervisory control and data acquisition (SCADA) systems located in the U.S. and other countries, on the Russian language Dark Web forum “RAMP”. These systems are used to control and monitor physical industrial processes, like the flow of water through a pipeline. The actor claimed that attackers could access these devices remotely via virtual network computing (VNC).

Alleged U.S. compromised entities include:

- Oil refineries
- Energy companies
- Biosparging and skimmer systems
- Water pressure boosters

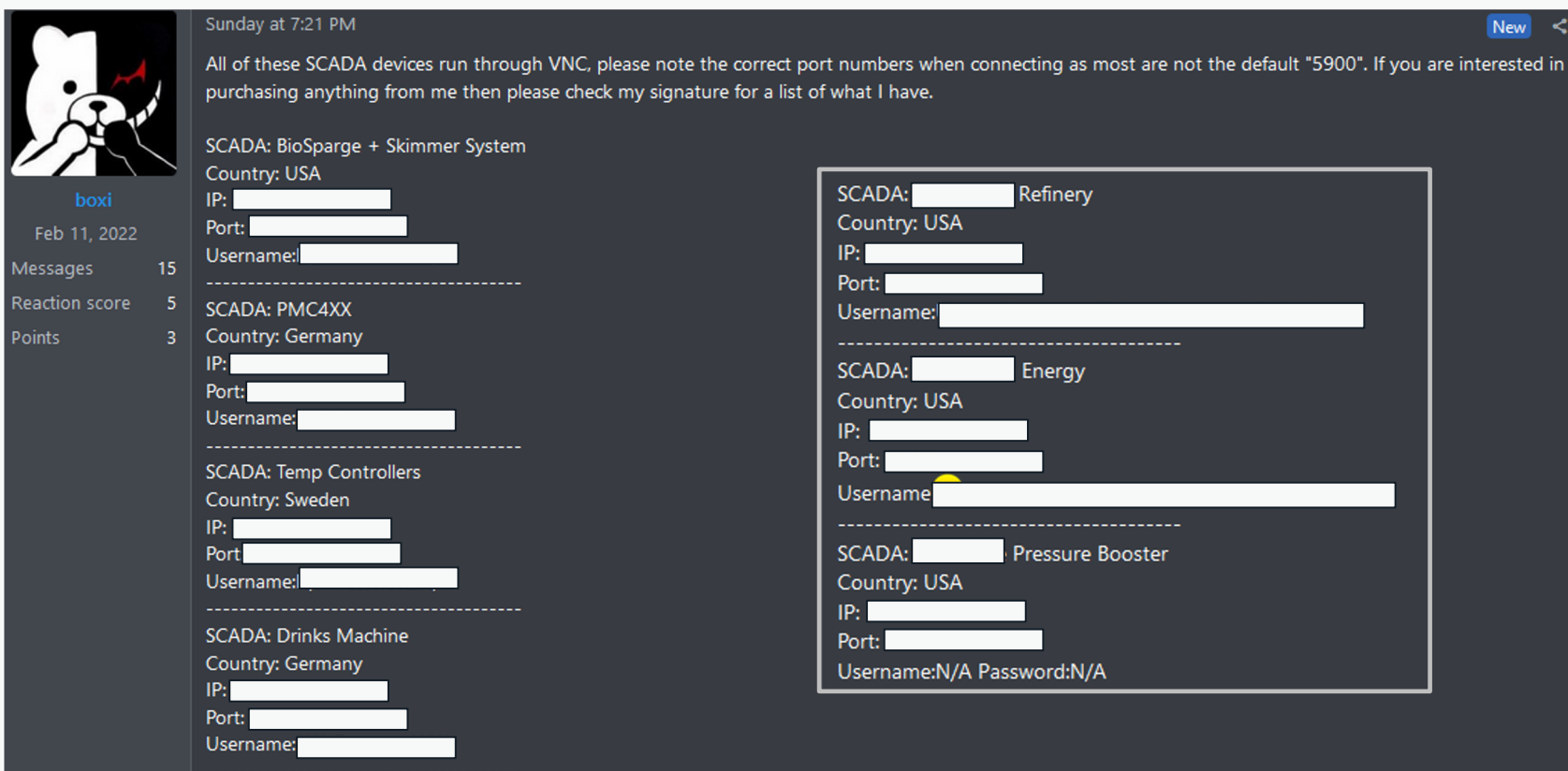
In addition to location, the actor specified the following for each device:

- IP address
- Port number
- Login credentials

ZeroFox researchers note that while some of these systems appear to use weak passwords, like “1111” or “1234”, others did not appear to require a password at all. Additionally, many of these devices use default ports to connect. This is likely due to a misconfigured VNC server.

Original post from the
threat actor "boxi"
advertising
compromised SCADA
systems

Compromised SCADA Systems In U.S. & Other Countries Cont.



Sunday at 7:21 PM

All of these SCADA devices run through VNC, please note the correct port numbers when connecting as most are not the default "5900". If you are interested in purchasing anything from me then please check my signature for a list of what I have.

boxi
Feb 11, 2022
Messages 15
Reaction score 5
Points 3

SCADA: BioSparge + Skimmer System
Country: USA
IP: [REDACTED]
Port: [REDACTED]
Username: [REDACTED]

SCADA: PMC4XX
Country: Germany
IP: [REDACTED]
Port: [REDACTED]
Username: [REDACTED]

SCADA: Temp Controllers
Country: Sweden
IP: [REDACTED]
Port: [REDACTED]
Username: [REDACTED]

SCADA: Drinks Machine
Country: Germany
IP: [REDACTED]
Port: [REDACTED]
Username: [REDACTED]

SCADA: [REDACTED] Refinery
Country: USA
IP: [REDACTED]
Port: [REDACTED]
Username: [REDACTED]

SCADA: [REDACTED] Energy
Country: USA
IP: [REDACTED]
Port: [REDACTED]
Username: [REDACTED]

SCADA: [REDACTED] Pressure Booster
Country: USA
IP: [REDACTED]
Port: [REDACTED]
Username: N/A Password: N/A

Free SIM Swapping Method Enables Threat Actors To Target U.S. Phone Carriers

ZeroFox identified a free and widely distributed SIM swapping method that is almost certainly enabling threat actors to target AT&T and other U.S. phone carriers on different fraud-focused Telegram channels. This method likely explains why ZeroFox researchers have observed a growing number of SIM swapping services zeroing in on U.S. phone carriers since mid-2021.

The method requires a threat actor to collect the full PII of a victim, including:

- Full name
- Date of birth
- Phone number
- Phone carrier
- Email address
- Physical address

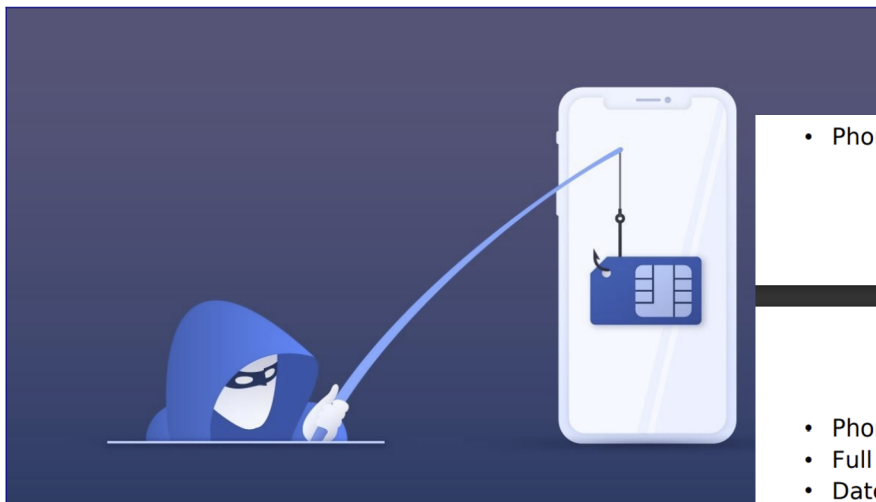
After a threat actor has acquired the PII, the method requires social engineering to convince the phone carrier to transfer the victim's phone number over to a threat actor-owned SIM card.

ZeroFox researchers note that threat actors reselling this method likely have large datasets containing the PII of victims with phone numbers registered to AT&T, or other U.S. phone carriers, making them more vulnerable to this method.

Screenshot of the free SIM-swapping method that is being widely distributed among threat actors on the underground

Free SIM-Swapping Method Enables Threat Actors Cont.

WHAT IS SIMSWAPPING AND HOW TO SIMSWAP?



- Phone Number (obvious)

- Phone Carrier
- Full Name
- Date of Birth
- Primary Email
- Primary Address

You have to have the above info, the best way to go about it is to get the sim with the same mobile carrier as your victim, lets say your victim is with AT&T get a sim with AT&T and then do a sim swap on yourself so this will tell you all the information you will need to do this job successfully.