

REvil

Steal, Encrypt & Auction

Ransomware Team Recent Activities
and Developments

CONTENTS

| | |
|----------------------------|----|
| Introduction | 3 |
| Press Coverage | 4 |
| Auction Feature | 6 |
| Auction Registration | 7 |
| Summary | 9 |
| Contact Information | 10 |

INTRODUCTION

Following ongoing monitoring of targeted ransomware threats, this advisory summarizes the recent activities and developments of REvil Ransomware Team, the threat actors also known as Sodinokibi.

Infamously responsible for the Travelex incident at beginning of 2020¹, REvil have remained active throughout the first half of 2020 and continue to post details of new victims, along with stolen data samples, on their 'Happy Blog', a hidden service website hosted on the Tor anonymity network.

Based on regular weekly, if not daily, posts to their site, new small and large organizations continue to fall victim to REvil's targeted attacks and come from a variety of sectors including consulting, financials, industrials, legal, retail and technology.

New small and large organizations continue to fall victim to REvil's targeted attacks and come from a variety of sectors

REvil have often claimed that stolen data would be sold, or published for free, in the event of ransoms not being paid

Previously using the 'steal, encrypt and leak' tactic, REvil have often claimed that stolen data would be sold, or published for free, in the event of ransoms not being paid. Seemingly rather than attempting to sell any stolen data via third-party underground forums or marketplaces, June 2020 saw the release of a new 'auction' feature on REvil's dark website and this allows anonymous participants to bid directly on stolen data.

¹ Cyberint Research - Travelex Hit by an Alleged Ransomware Attack (January 2020)

A case with **Universal Food & Marine Distributors** was agreed for \$7,500,000

- Link: <http://dnpsnbaix.blogspot.in/2014/05/2014-05-27-01.html>, onion/posts/52

Next. The hottest news, which we associate with GRUBMAN SHIRE MEISELAS & SACKS. Our demand was only 21.000.000\$. The work was also done with the above mentioned [REDACTED]. After 10 days, we asked how much money had been collected from the amount. The answer was 365k. Of course, we realized that people are not determined to solve the problem. Correspondingly, our tactics the same:

- Link: <http://dnpsnbaix.blogspot.in/2016/07/dnssec.html>

So, the ransom is now \$42,000,000. They have that's the kind of money. And even more. But let's about nice one.

The next person we'll be publishing is Donald Trump. There's an election race going on, and we found a ton of dirty laundry on time. Mr. Trump, if you want to stay president, poke a sharp stick at the guys, otherwise you may forget this ambition forever. And to you voters, we can let you know that after such a publication, you certainly don't want to see him as president. Well, let's leave out the details. The deadline is one week. Grubman, we will destroy your company to the ground if we don't see the money. Read the story of Traveler, it's very instructive. You repeating their scenario one to one.

War to victory, only this way.

² Cyberint Research - REvil Ransomware Keeps Claiming Victims (March 2020)

Subsequently, a 19th May 2020 post suggested that the data related to President Trump has been purchased by an 'interested' party whilst preparations to auction data stolen from GSMS related to Madonna are underway (Figure 2).

Interested people contacted us and agreed to buy all the data about the US president, which we have accumulated over the entire time of our activity. We are pleased with the deal and keep our word.

05/25/2020 we are preparing to auction Madonna data. The rules are the same:

1. One-handed information
2. Confidentiality of the transaction
3. We delete our copy of the data
4. The buyer has the right to do whatever he sees fit with the data received.

Starting price - 1 million dollars.

Figure 2 - Madonna auction preparations (19 May 2020)

Notably, REvil seeks to reassure would-be purchasers that only one copy of the data will be sold and that they will delete their own copy upon completion of a confidential transaction. Whilst some might question the honesty and integrity of a cybercriminal gang that has extorted countless victims, it is likely that the group would adhere to their own 'rules', maintaining their reputation and ensuring further future transactions.

AUCTION FEATURE

Seemingly added to REvil's site on or around 2 June 2020, a 'new' auction feature allows anonymous users to register and bid on stolen data obtained from their targeted ransomware campaigns. The announcement of this feature includes details of the first lot, data stolen from a Canadian agriculture organization including accounting information along with document files and databases (Figure 3).

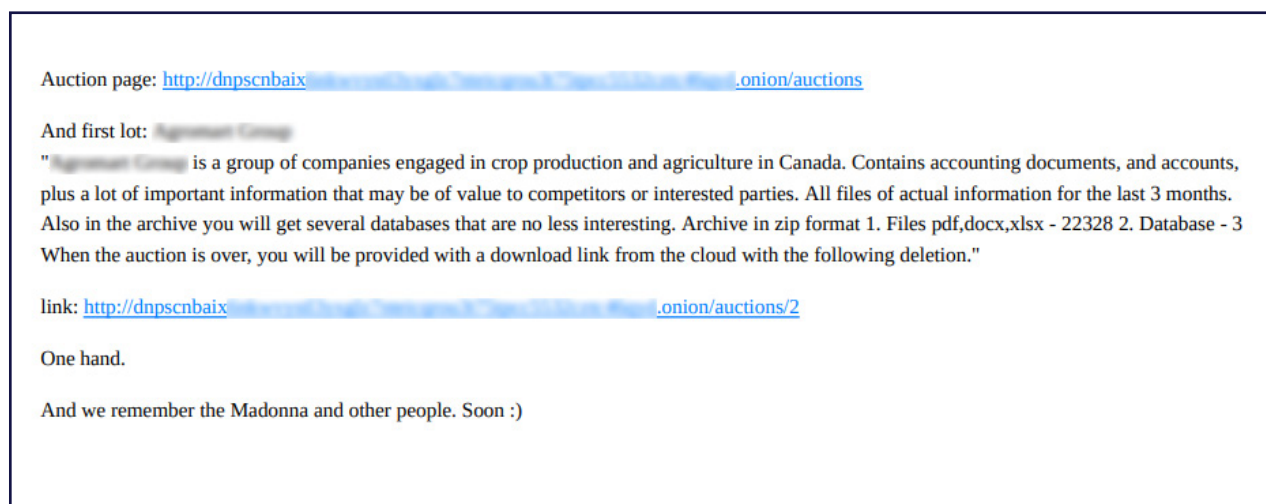


Figure 3 - Auction feature announcement

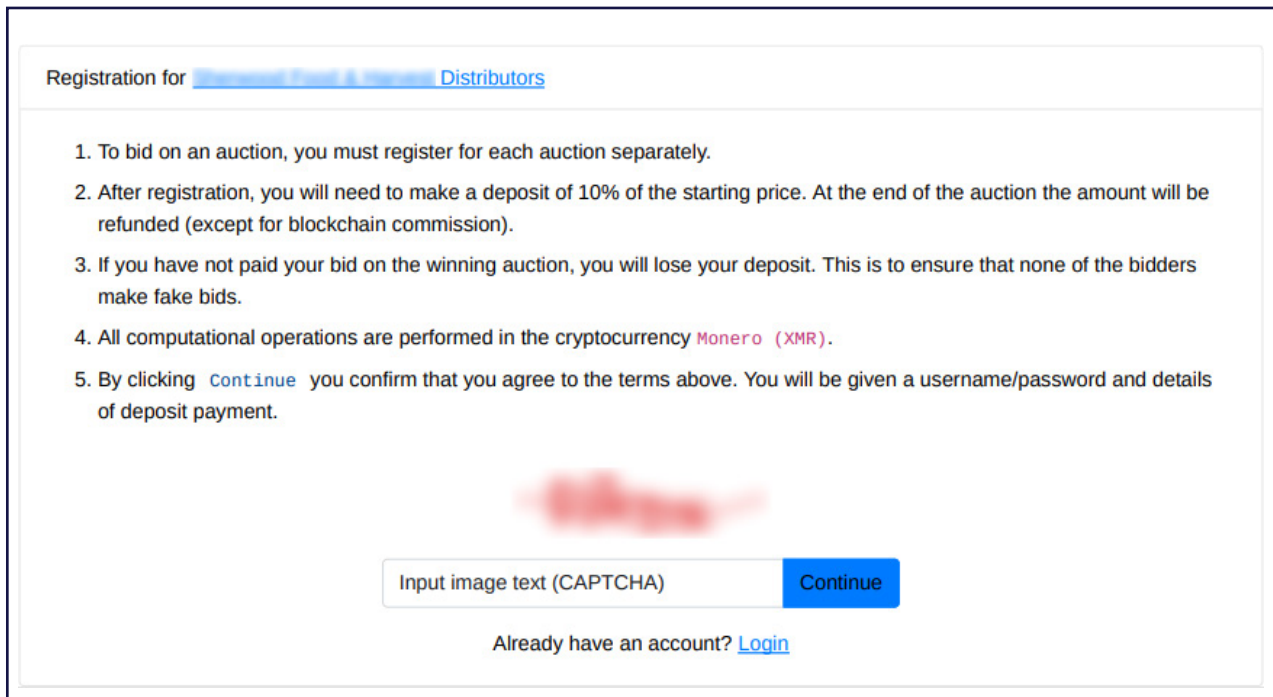
As of 8 June 2020, stolen data obtained from four victims is available to bid on, or buy-now using the 'blitz' price:

- Canadian agriculture group - Includes accounts and documents with a starting of USD 50,000 and a blitz price of USD 100,000;
- US food distributor - Includes accounts and documents with a starting price of USD 100,000 and a blitz price of USD 200,000;
- US law firm - 50GB of data including client confidential and personal information with a starting price of USD 30,000 and a blitz price of USD 50,000;
- US intellectual property law firm - 1.2TB of data including 'all' internal documentation, correspondence, patent agreements and client confidential information with a starting price of USD 1,000,000 and a blitz price of USD 10,000,000.

Data stolen from the intellectual property law firm reportedly includes information related to new technologies and unfiled patents that, given the high-profile client list, likely explains the high starting and blitz prices. Whilst this data would possibly be of interest to competitors or even a nation-state seeking to gain economic advantages, any would-be purchaser would likely find it difficult to develop any stolen technology or product without arousing suspicion as to its origin and inviting legal repercussions.

AUCTION REGISTRATION

Unlike traditional auction websites, each individual auction requires registration and, other than completing a 'CAPTCHA' challenge-response test, the bidder does not need to submit any personal information (Figure 4).



Registration for [redacted] [Distributors](#)

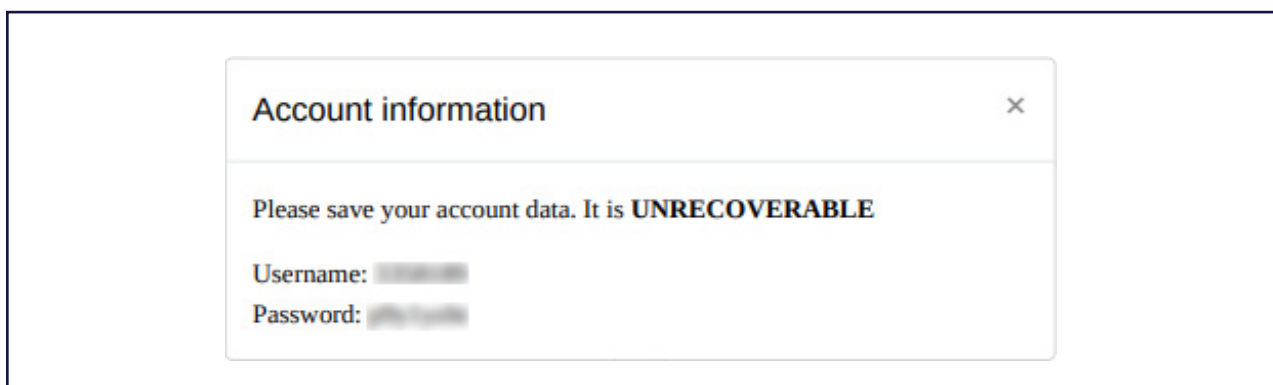
1. To bid on an auction, you must register for each auction separately.
2. After registration, you will need to make a deposit of 10% of the starting price. At the end of the auction the amount will be refunded (except for blockchain commission).
3. If you have not paid your bid on the winning auction, you will lose your deposit. This is to ensure that none of the bidders make fake bids.
4. All computational operations are performed in the cryptocurrency **Monero (XMR)**.
5. By clicking [Continue](#) you confirm that you agree to the terms above. You will be given a username/password and details of deposit payment.

Input image text (CAPTCHA) [Continue](#)

Already have an account? [Login](#)

Figure 4 - Auction registration

Having anonymously registered, a set of bidder credentials are generated and displayed along with a warning that they are unrecoverable, unsurprisingly given that no email address or other contact information has been submitted (Figure 5).



Account information ×

Please save your account data. It is **UNRECOVERABLE**

Username: [redacted]

Password: [redacted]

Figure 5 - Auction credentials

Additionally, a Monero (XMR) cryptocurrency wallet address is uniquely generated for the bidder and this would be used to both pay a deposit, equal to ten percent of the starting bid, and any final sum upon winning the auction (Figure 6).

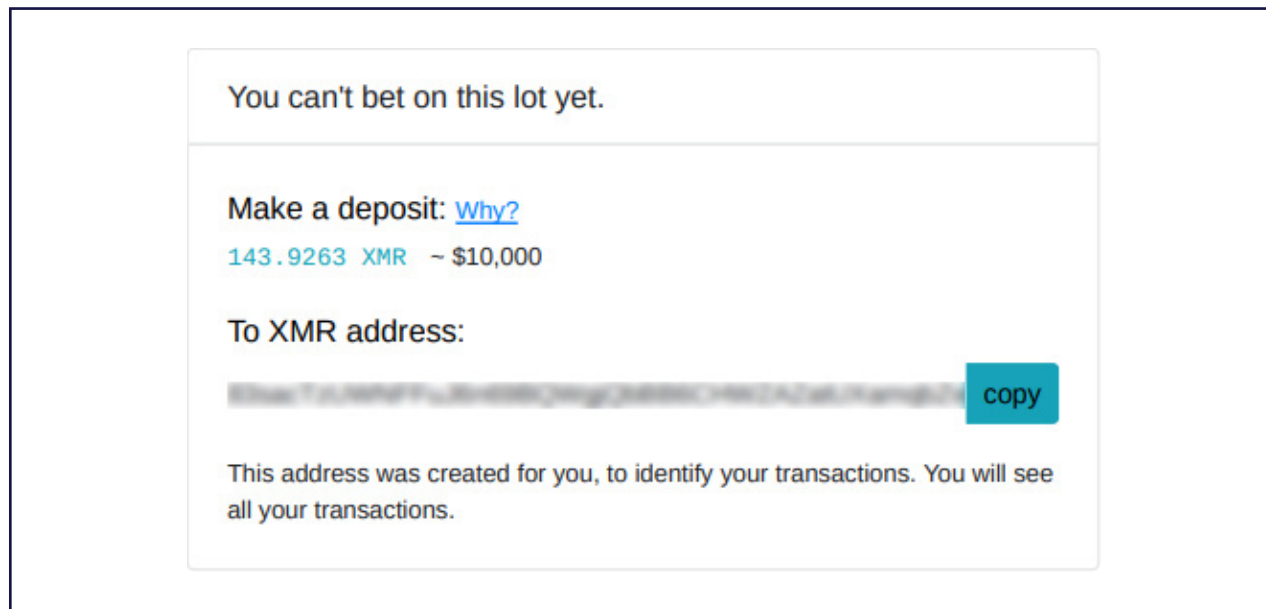


Figure 6 - Monero cryptocurrency wallet address

The deposit system is used to discourage fake bids and to encourage final payment in the event of winning an auction, unsuccessful bidders will see their deposits returned.

In addition to displaying details of the lot including current bids and the time remaining, each auction page also provides a series of links to websites where XMR can either be purchased or exchanged (Figure 7).

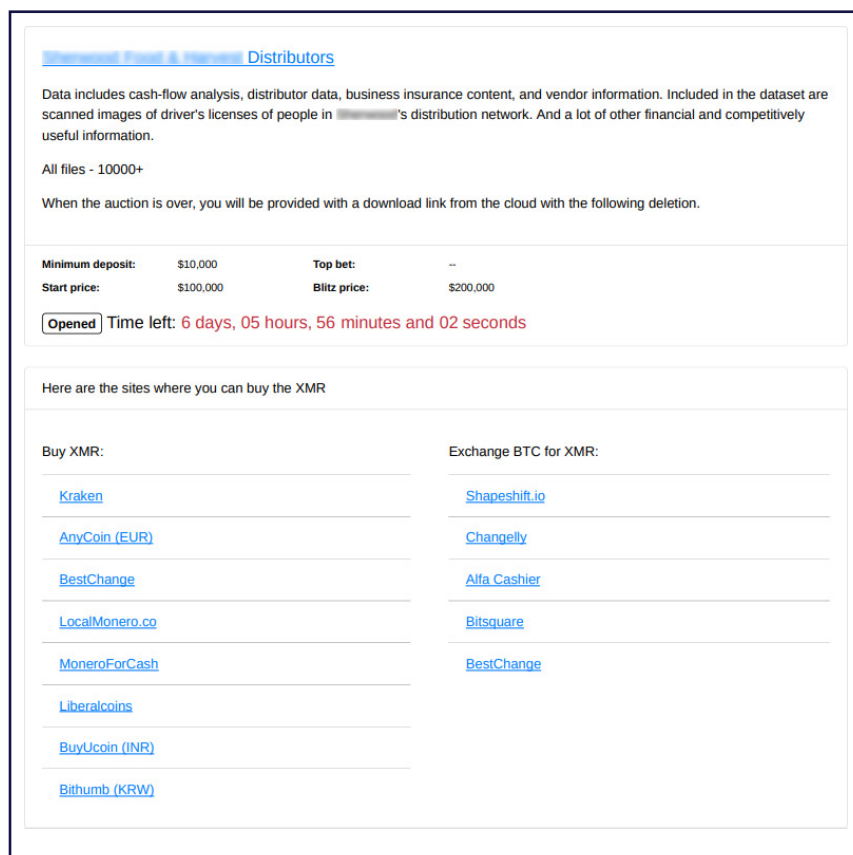


Figure 7 - Auction listing

The use of a cryptocurrency such as XMR provides a further element of anonymity albeit there is a need for trust between the two parties as it would not be possible to request a charge-back in the event of non-delivery.

SUMMARY

Whilst the creation of their own auction facility allows REvil to directly monetize their stolen data, without the need to pay commission to third-party forums or marketplaces, it remains to be seen what will happen to any stolen data if the auctions fail to attract any bidders. Aside from reducing the auction starting price, it is possible that REvil make seek to offload seemingly valuable data via other sources if these auctions prove unsuccessful.

Regardless of REvil's monetization practices, the threat of organized cybercriminal gangs conducting targeted ransomware attacks against organizations of all sizes worldwide remains high.

CONTACT INFORMATION

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

214 W 29th St
New York, 10001
Tel: +1-646-568-7813

Israel

17 Ha-Mefalsim St
4951447 Petah Tikva
Tel: +972-37-286-777

United Kingdom

WeWork Fox Court
14 Grays Inn Rd, Holborn
WC1X 8HN, London
Tel: +44-203-514-1515

Singapore

135 Cecil St. #10-01 MYP
PLAZA 069536
Tel: +65-3163-5760

Latin America

Panama City
Tel: +507-6255-8074