REvil ransomware creates eBay-like auction site for stolen data

By Lawrence Abrams

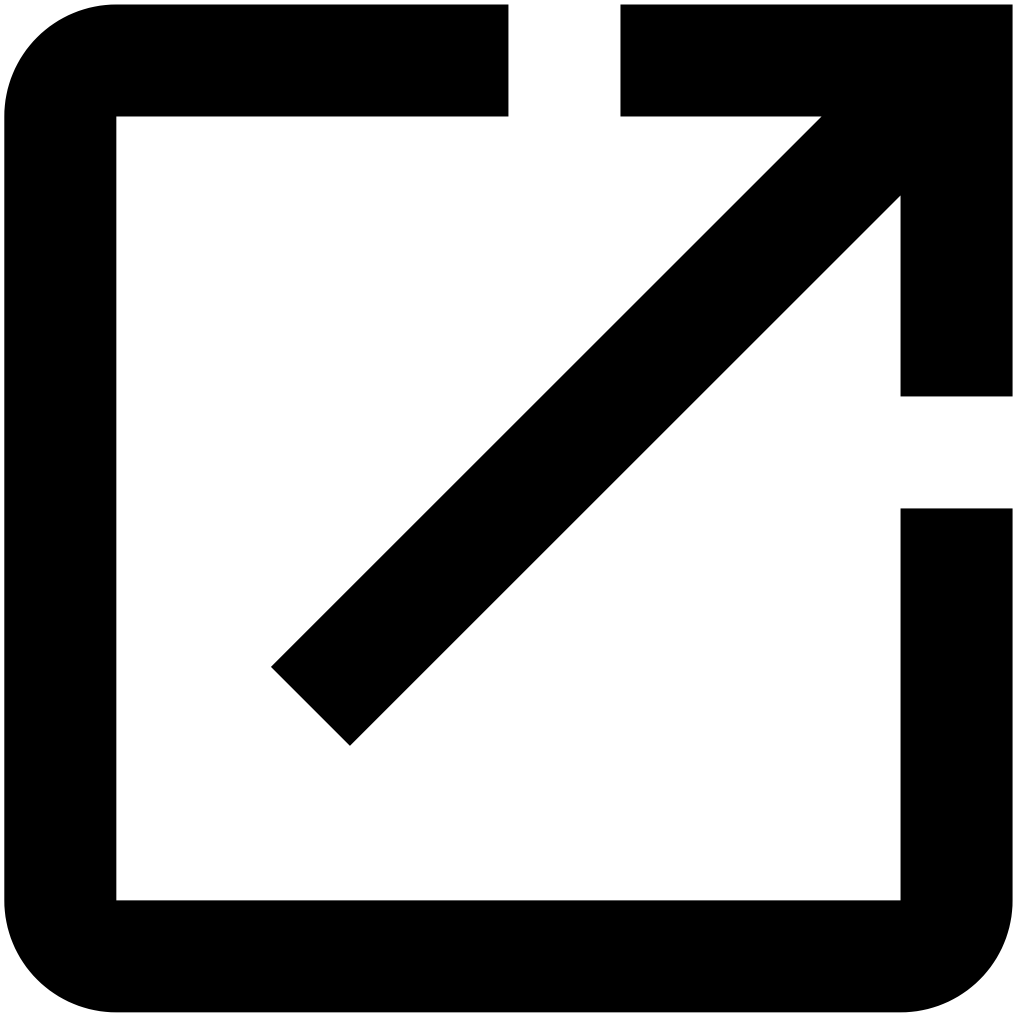
Published: 2020-06-02 · Archived: 2026-04-05 14:49:18 UTC

The operators of the REvil ransomware have launched a new auction site used to sell victim's stolen data to the highest bidder.

REvil, otherwise known as Sodinokibi, is a ransomware operation that breaches corporate networks using exposed remote desktop services, spam, exploits, and hacked Managed Service Providers.

Once established on a network, they quietly spread laterally through the company while stealing unencrypted data from workstations and exposed servers.

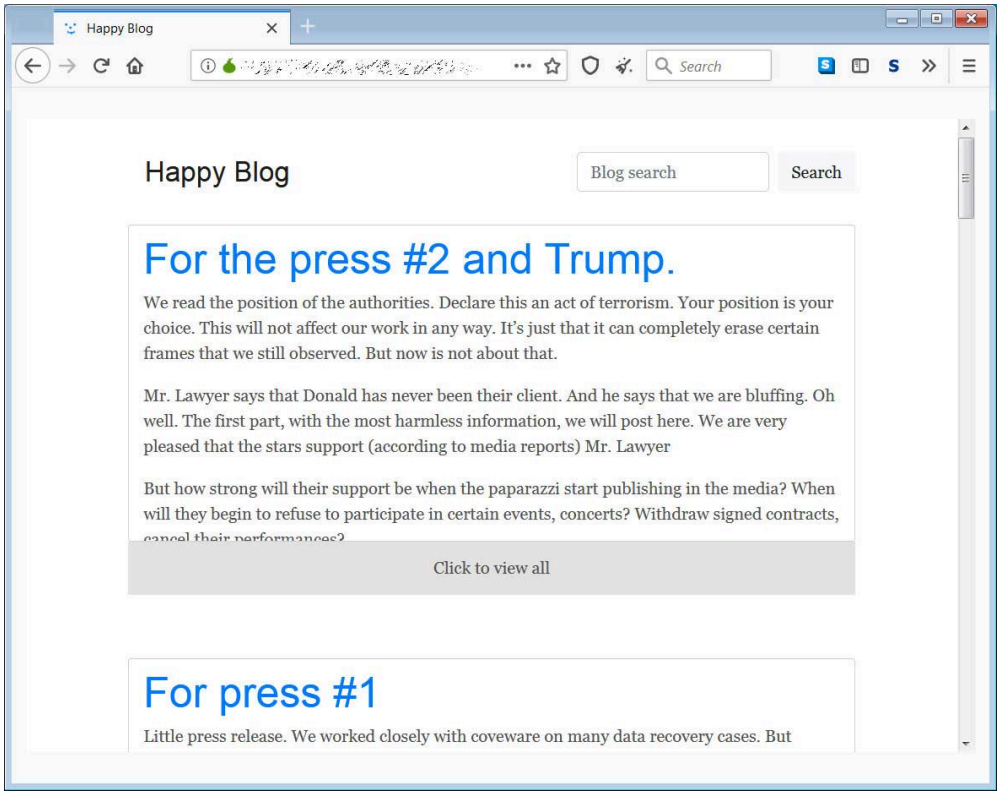

DIE LINKE.
0:00



When they gain administrative access to a domain controller, they proceed to deploy the ransomware to encrypt all of the computers on the network.

Earlier this year, the REvil operators released a data leak site that is used to publish a victim's data if a ransom is not paid.

Named the 'Happy Blog,' the ransomware gang uses the site to post samples of the stolen data and then threaten to release the actual files.



REvil data leak site

Historically, after a few days, the ransomware operators post a link to the stolen data so that other threat actors can use it for free.

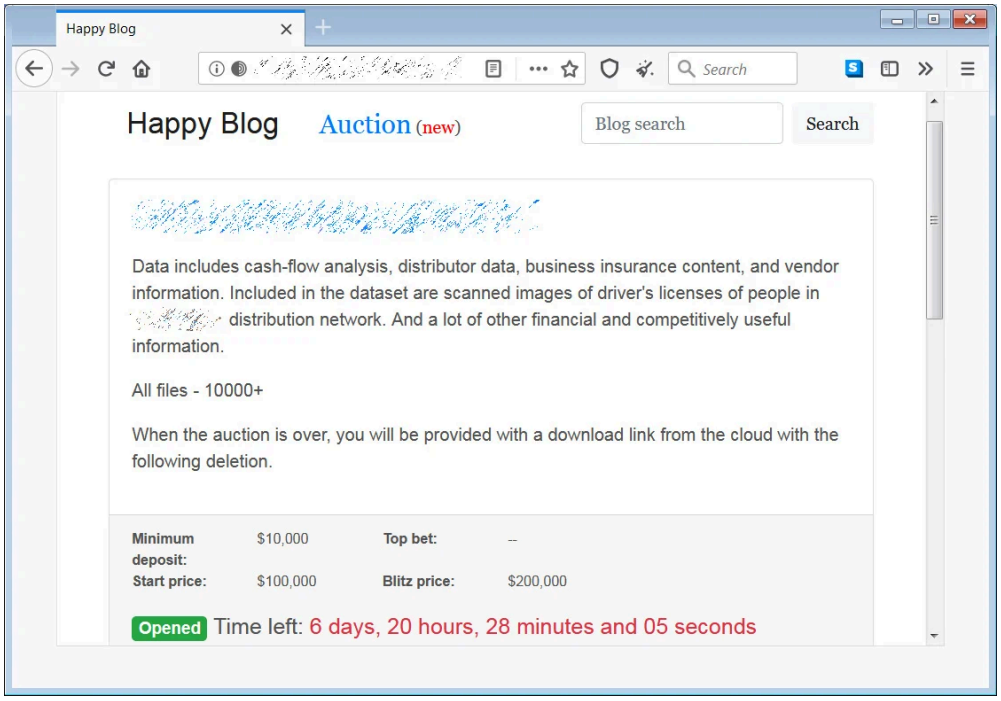
Stolen data auctioned to the highest bidder

In May, REvil started leaking the data for the celebrity law firm Grubman Shire Meiselas & Sacks (GSMLaw) after a ransom was not paid.

As part of these leaks, the ransomware gang claimed to have data about President Trump and auctioned it with a starting price of $1,000,000.

They later claimed to have sold the President's data and warned that they would auction data belonging to Madonna in the future.

To continue generating revenue when a victim does not pay, the REvil operators have launched a new section on their data leak site used to conduct auctions.



New REvil auction site

Currently, the ransomware operators are auctioning off the stolen data for two companies.

The first is a U.S. food distributor whose auctioned data has a starting price of $100,000 but can be bought immediately at a "Blitz price" of $200,000.

The second victim is a Canadian agricultural company whose auction starts at $50,000 and has a buy now of $100,000.

To bid on an auction, bidders must agree to the following rules.

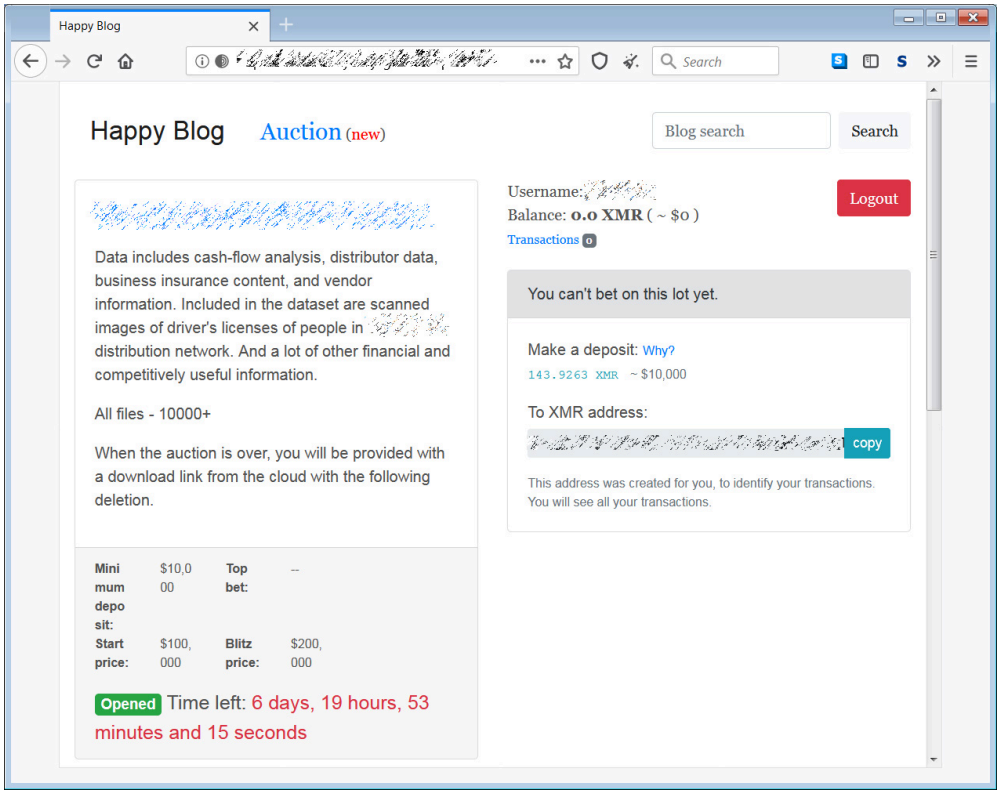
To bid on an auction, you must register for each auction separately.

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).

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.

All computational operations are performed in the cryptocurrency Monero (XMR).

By clicking Continue you confirm that you agree to the terms above. You will be given a username/password and details of deposit payment.



Bidding interface

In their auction site announcement, the operators hinted that other auctions are coming soon with the statement, "And we remember the Madonna and other people. Soon."

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
