Ransomware & auctions

Threat Memo - Date: 04/06/2020 - Version: 1.1
TLP:WHITE

FOR INFORMATION	Category	Type	Domain	Sector	Confidence
	Cybercrime	Ransomware, auction	World	Any	A1

Key Points

- Cybercriminals behind the REvil ransomware are auctioning off sensitive data stolen from their victims.
- The current auction prices range from $50 000 to $200 000.
- The new tactic adopted by REvil operators marks an escalation in methods aimed at coercing victims to pay up.
- Like for other recently introduced ransomware extortion schemes, it is likely to be adopted by other cybercriminal groups.

Summary

The criminal entity dubbed Pinchy Spider operating the REvil (aka Sodinokibi) ransomware has reportedly[1] begun auctioning off sensitive data stolen from their victims. The criminal entity used their dark web "Happy Blog" to announce their first ever stolen data auction. As of writing, the ransomware operators are auctioning off the stolen data of two companies.

Date	Sector	Country	Auctioning	Start price	Blitz price
June 1	Telecom	South Africa	No		
June 1	Agriculture	Canada	Yes	$50 000	$100 000
May 31	Utilities	UK	No		
May 30	Legal	US	No		
May 14	Food distributor	US	Yes	$100 000	$200 000

Table 1 – Recent REvil breaches

In both cases auctioned data has a starting price, currently ranging from $50 000 to $100 000, but buyers can obtain the data immediately at a "Blitz price", currently ranging from $100 000 to $200 000. To bid on an auction, bidders must agree to certain rules.

- Register for each auction separately.
- After registration, make a deposit of 10% of the starting price, refunded at the end of the auction.
- If you have not paid your bid on the winning auction, you will lose your deposit to avoid fake bids.
- All "computational operations" (sic) are performed in the cryptocurrency Monero (XMR).

The new tactic adopted by REvil operators marks an escalation in methods aimed at coercing victims to pay up. Recently introduced tactics (threatening to leak sensitive exfiltrated data and public shaming) has been adopted by a growing number of ransomware operators.

Figure 1 – Recent evolution of ransomware coercion tactics

[1] https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/

Comments

The REvil criminal group is behind the development of the ransomware known as GandCrab, which was active between January 2018 and the end of May 2019. REvil (aka Sodinokibi) was brought into operation at the beginning of April 2019. The developer of REvil is selling access to their ransomware under a partnership program with a limited number of accounts, often referred to as Ransomware-as-a-Service (RaaS).

New extortion methods such as publicly naming victims or threatening to leak sensitive data have been recently adopted by most major ransomware operators, including Maze, Netwalker, Nefilim, Clop, DoppelPaymer, Nemty, Pysa, Ragnar locker, Sekhmet, CryLock, ProLock, and Snake.

In is therefore likely that if the auction tactic proves to be efficient, it will be adopted by other ransomware operators.