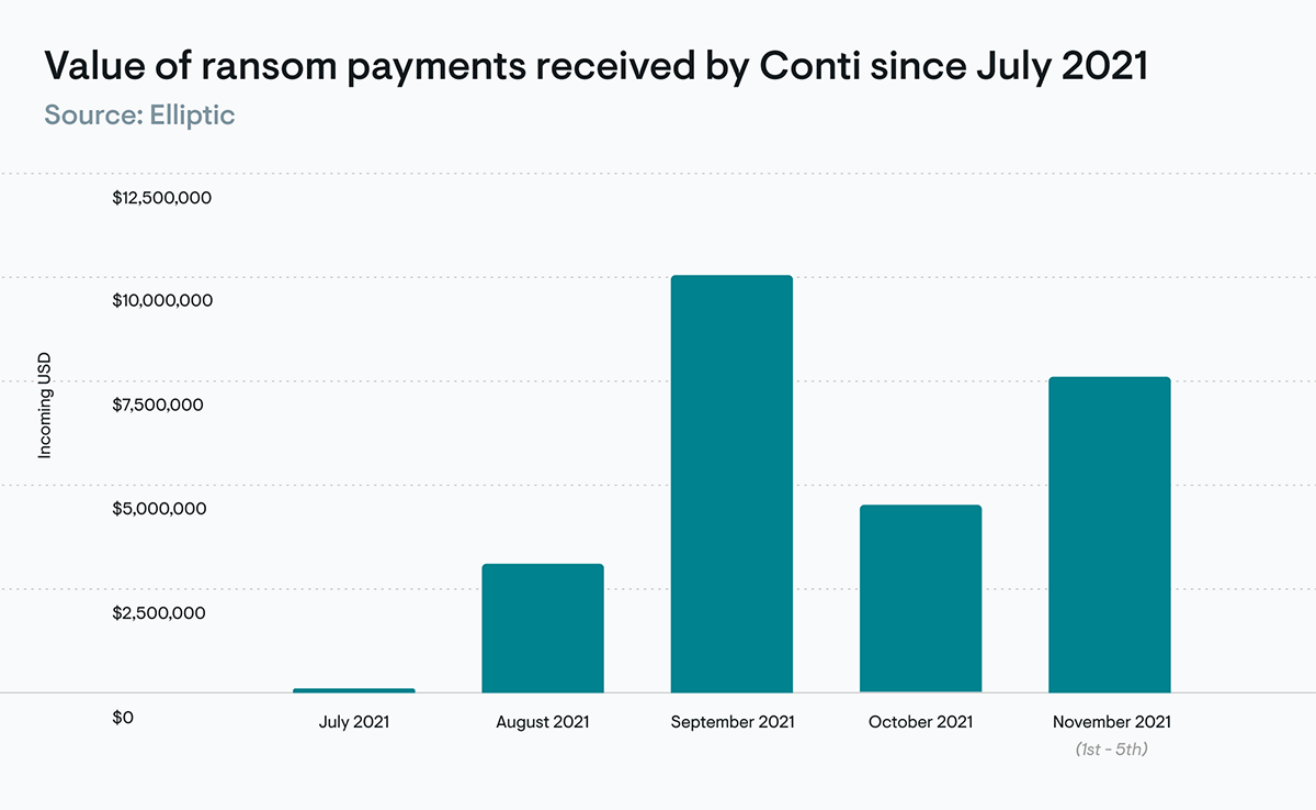
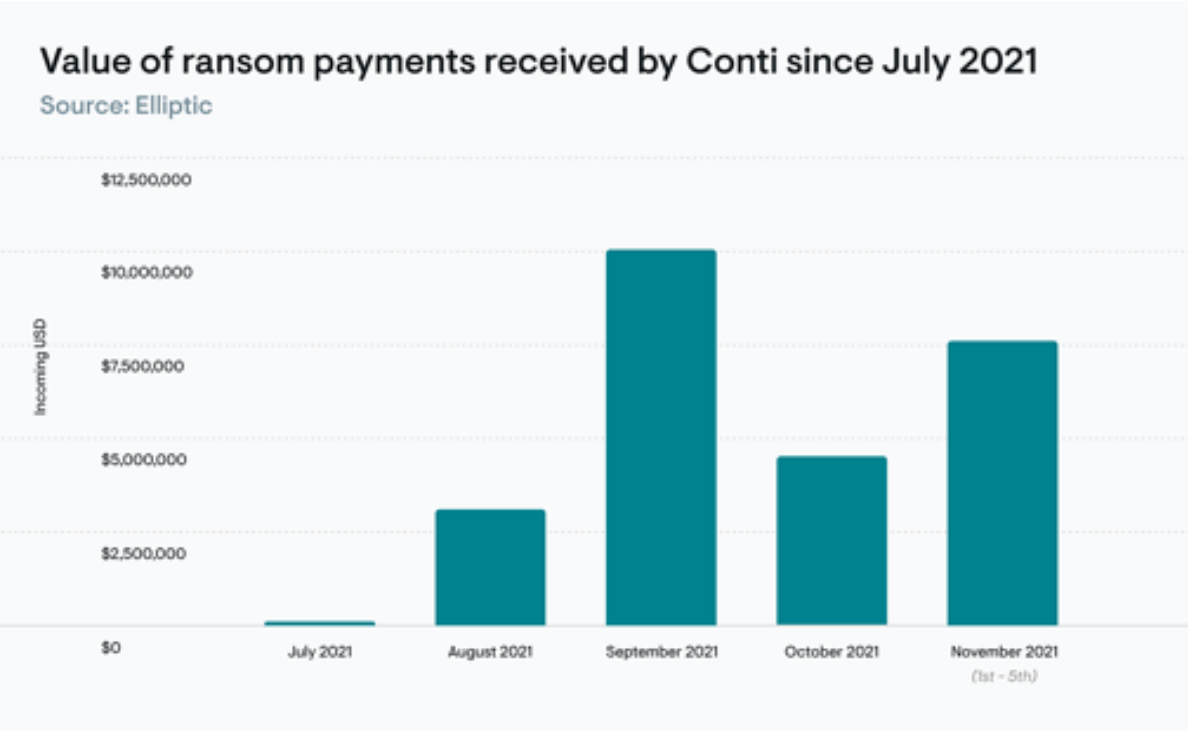
Conti Ransomware Nets at Least $25.5 Million in Four Months

elliptic.co/blog/conti-ransomware-nets-at-least-25.5-million-in-four-months





Elliptic Intel

Elliptic's analysis of newly-uncovered ransomware transactions has revealed that Conti's illicit activities have netted the group at least $25.5 million since July 2021, which includes one ransom payment of over $7 million in November 2021.

In a collaboration with threat intelligence company Prodaft, Elliptic has analysed Bitcoin addresses connected to 14 ransomware attacks conducted by Conti between July 1st and November 5th 2021. These addresses were identified by Prodaft after they were able to access Conti's management admin portal.

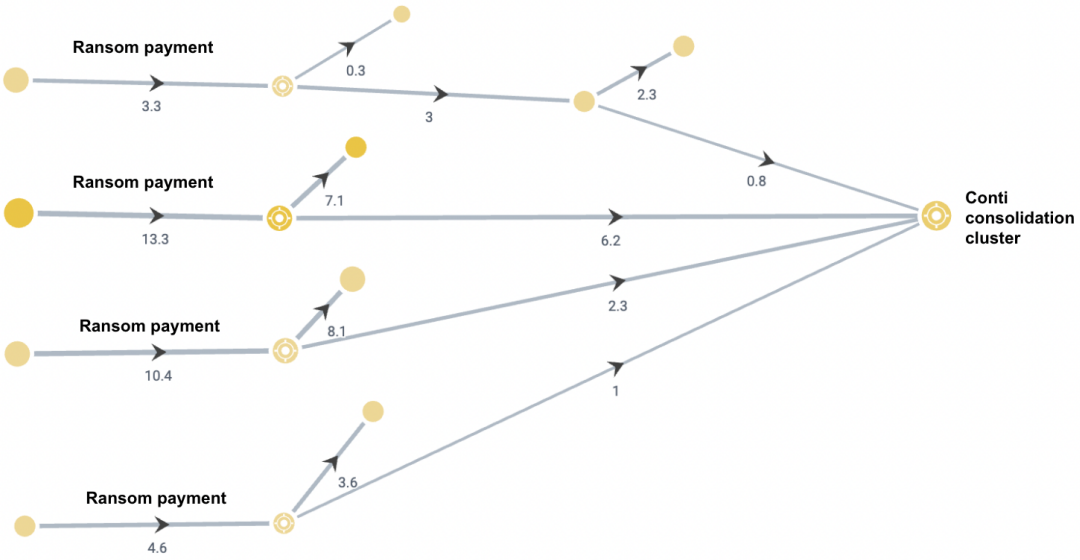
Conti ransomware was first observed in 2020 and is believed to be the successor to Ryuk, which has been active since 2018. Both Conti and Ryuk are operated by the Russian cybercrime group, Wizard Spider.

Conti has attacked numerous high profile victims, including the Japanese electronics supplier JVCKenwood, and London-based high society jeweller Graff. In September 2021, Prodaft's threat intelligence team observed a surge of ransomware attacks attributable to Conti, which is currently one of the most active ransomware strains.

Of the 14 attacks analysed by Elliptic, 50% resulted in a payment to Conti, though the group's overall success rate is likely to be considerably lower. Over the same time period, Conti's public leak site listed more than 130 victims.

Conti uses the Ransomware-as-a-Service (RaaS) model. RaaS Bitcoin transactions characteristically split — as the proceeds of each ransom payment is distributed between the ransomware operator and the affiliate that infected the victim — with the exact percentage split differing between RaaS groups. In most instances, the affiliates are awarded the majority of the ransom payment, with the ransomware operators taking a smaller percentage.

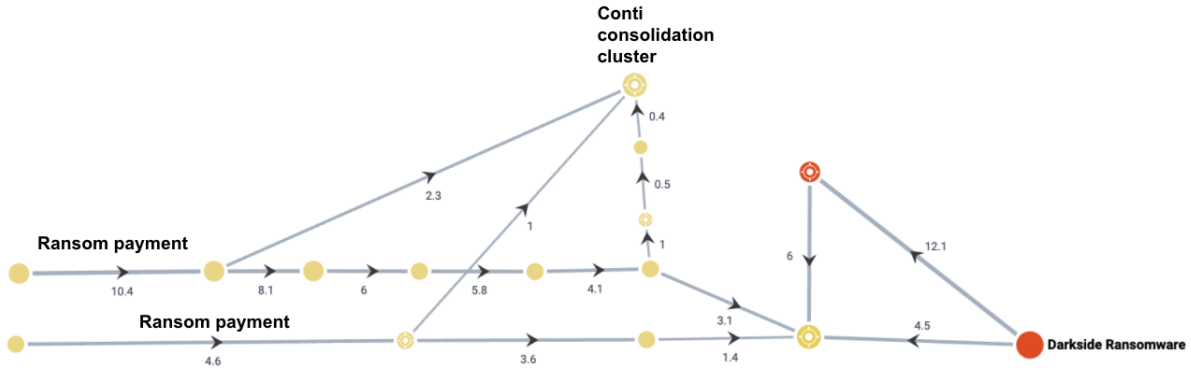
Analysing the ransom payment addresses identified by Prodaft resulted in the identification of a consolidation cluster, which has received a 22.5% split of several of the ransom payments, believed to represent the operator's share. In total, Conti received at least $25.5 million (more than 500 BTC) in ransom payments since July 2021, $6.2 million of which was kept by the Conti operator.



IMG 1: Screenshot from Elliptic's cryptocurrency investigations software, *Forensics — showing the destination of the Conti operator's share of the ransom payments*

Apart from one outgoing payment of 0.07 Bitcoin which was sent from the consolidation cluster to a prominent exchange in August 2021, the Conti operator has not sent any of the Bitcoins in this wallet to services such as exchanges where they could cash-out their proceeds. Blockchain records indicate that the remaining 123.06 Bitcoin is currently held in an unhosted wallet.

Elliptic also tracked the ransomware proceeds received by Conti affiliates. One identified wallet has received payments from both Conti and DarkSide, which may indicate that an individual has worked as an affiliate for both of these groups.



IMG 2: Screenshot from Elliptic's cryptocurrency investigations software, *Forensics — showing the destination of the affiliates' share of the Conti ransom payments*

Conti affiliates appear to conduct a sophisticated money laundering operation, avoiding obvious consolidation of funds. Despite this, Elliptic has identified affiliate funds being sent to exchanges, coin swaps, privacy enhancing wallets including Wasabi, and the Russian-language darknet market Hydra.

The Importance of Countering Ransomware Groups and How Elliptic Can Help

Countering ransomware has become a top priority for the world's largest financial jurisdictions, with the United States' OFAC recently imposing sanctions on two cryptocurrency exchanges believed to be laundering ransomware proceeds. The latest, against Latvia-based Chatex, coincided with an international law enforcement operation against REvil, another ransomware group.

Virtual asset service providers and financial institutions have a legal and financial responsibility to ensure that they have effective transaction screening tools in place to prevent the facilitation of ransomware-related money laundering. Any attempt by Conti operators or affiliates to cash out presents a risk to VASPs.

At Elliptic, we provide blockchain analytics solutions to assist regulated cryptoasset businesses and financial institutions in preventing exposure to illicit actors such as ransomware groups.

Elliptic's clients can visualise and investigate wallets and transactions, including ransomware payments, using Elliptic Forensics, in order to 'follow the money' to its ultimate source or destination. Elliptic Lens and Navigator allow you to screen wallets and transactions to ensure you remain compliant with a regulatory landscape that is becoming increasingly concerned with ransomware.

Contact us for a demo and to learn more about how Elliptic's industry-leading blockchain analytics solutions can enable you to address the dual challenges of sanctions and ransomware.

Disclaimer