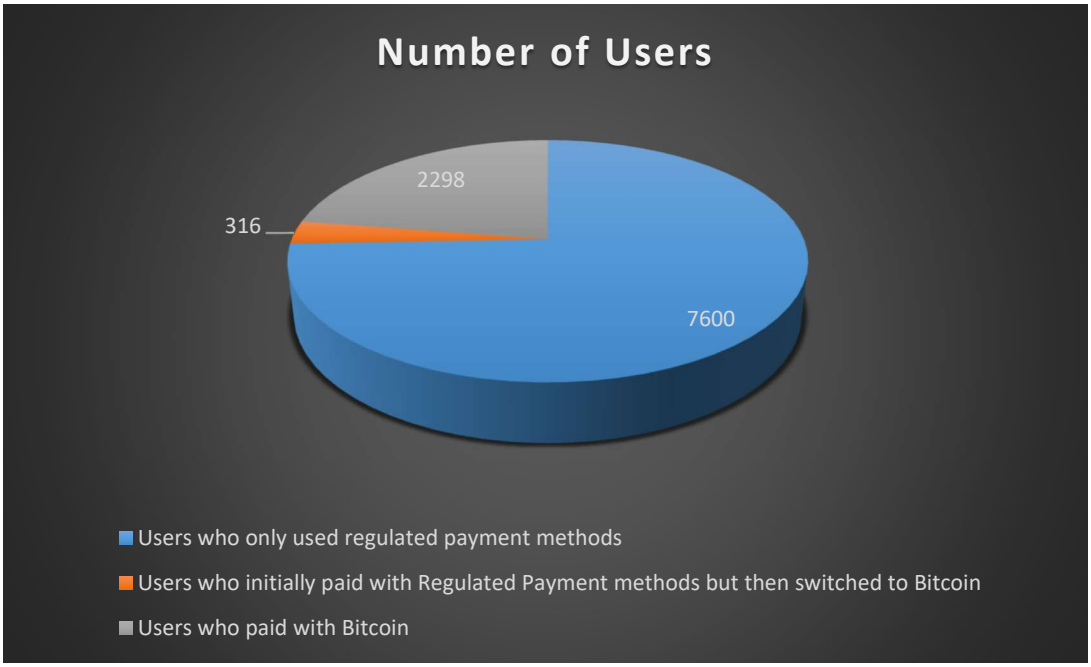
Undermining Cybercrime: A Case Study on User Response to Unregulated Payment Systems

Prakhar Pandey, Ryan Brunt, Damon McCoy
New York University

Abstract: In this case study, we use the leaked database of a DDoS for hire service, vdos-s.com (VDOS), to investigate how users responded to disruptions in their payment options. Earlier this year VDOS was hacked and authorities were able to arrest the people running the site [2]. Using their leaked database, we analyze user data from July 2014 through July 2016. During this time, interventions were launched by other researchers and law enforcement to disrupt access to PayPal, the primary method used to subscribe to these booter services. In response, many booters, including VDOS, scrapped regulated payment processors in favor of Bitcoin. We show that users who previously used regulated payments methods were unlikely to switch to Bitcoin. We also show that the disruptions to PayPal caused spikes in customer complaints. Our findings are limited to the VDOS users we analyzed so future work will need to be done to understand how users respond to payment disruptions.

In July 2015, VDOS announced it would no longer accept PayPal and would only take Bitcoin starting in January of 2016. After the announcement, we found that VDOS users who previously only used PayPal were unlikely to switch to Bitcoin. Of the 7916 users who began paying with PayPal or other regulated methods, only 316 transitioned to Bitcoin. The remaining 2298 users made payments using Bitcoin. Following graph depicts the same:



References

[1] Karami, M., Park, Y., McCoy, D.: Stress testing the booters: understanding and undermining the business of DDoS services. In: Proceedings of WWW (2016)

[2] Brian Krebs. Israeli Online Attack Service 'vDOS' Earned $600,000 in Two Years. https://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/

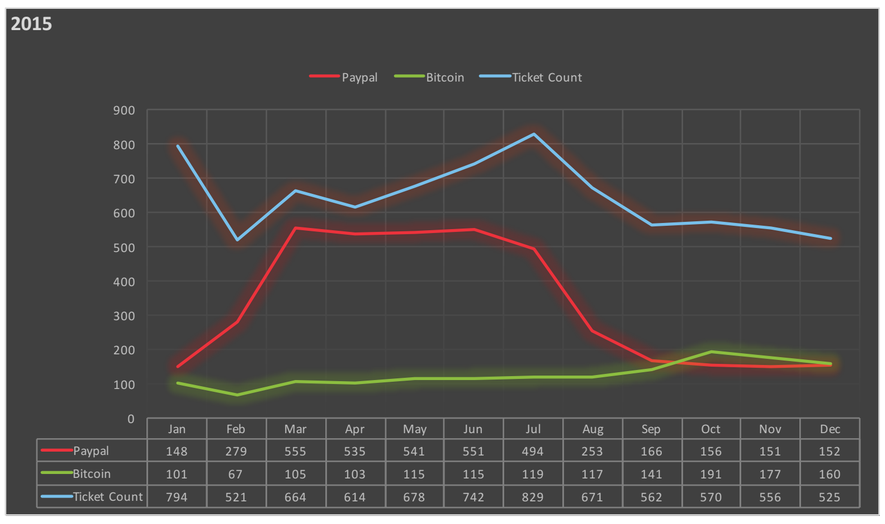
RSAConference Security Scholar

Undermining Cybercrime: A Case Study on User Response to Unregulated Payment Systems

Prakhar Pandey, Ryan Brunt, Damon McCoy
New York University

Problem Statement and Goals

Criminal sites like VDOS have been using credible payment processors for a long time. Once these methods are no longer available how do users respond



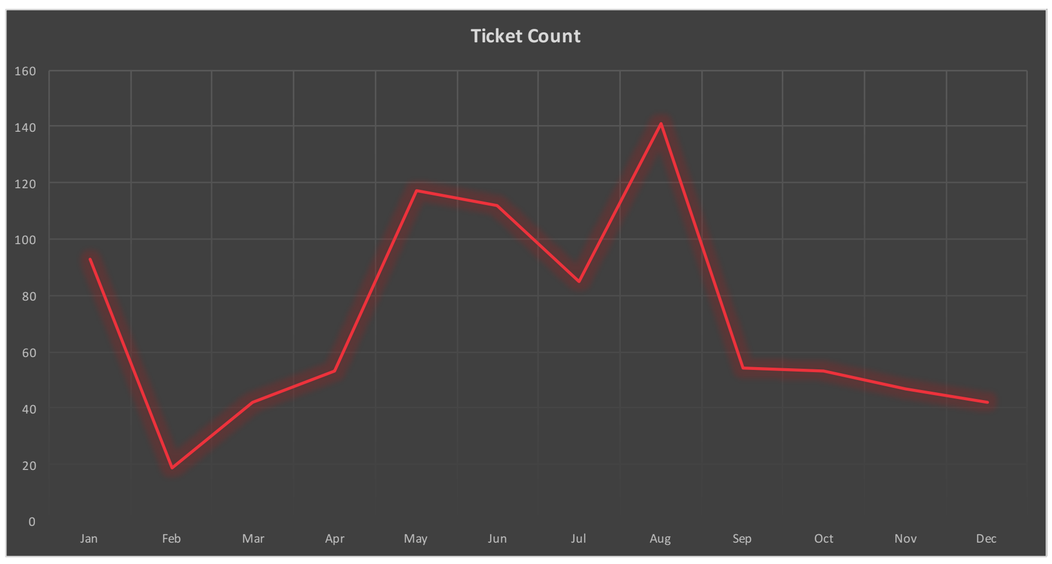
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Paypal	148	279	555	535	541	551	494	253	166	156	151	152
Bitcoin	101	67	105	103	115	115	119	117	141	191	177	160
Ticket Count	794	521	664	614	678	742	829	671	562	570	556	525

Our work is a case study of a DDoS as a service platform called VDOS-s.com (VDOS). Other work [1] has demonstrated how to undermine these DDoS as a service platforms. Earlier this year VDOS was hacked and authorities were able to arrest the people running the site [2]. Using their leaked database, we investigate how payment interventions affected the users.

Approach

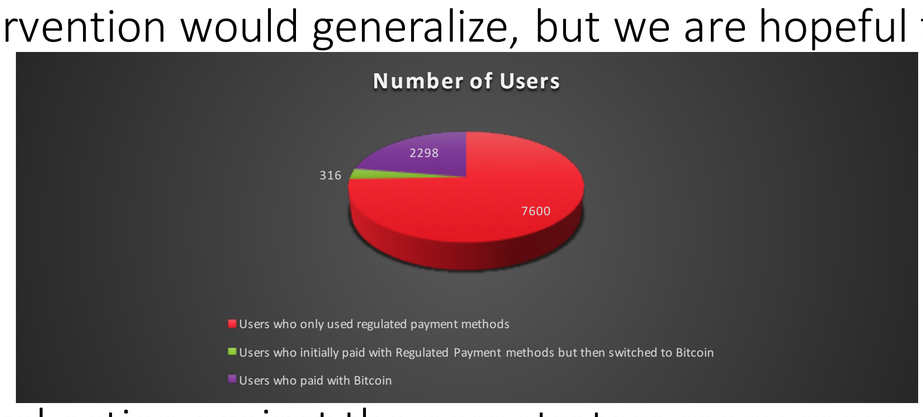
To analyze the user response we use the tickets, users, and payments tables in the database. We used regular expressions and manually examined the tickets to identify tickets related to problems with payments. In particular, we looked for problems with PayPal since it was the most used payment method although other regulated payment systems were used such as VISA and PaySafe Cards.

We found large surges in ticket in particular related to PayPal volume during the interventions mentioned above.



Results

In conclusion, this case study demonstrates how forcing users to turn to unregulated payment methods was effective at reducing the user base for VDOS. It also illustrates how payment interventions increase the burden put on these services in the form of user complaints. As the data for other DDoS platforms is unavailable we cannot make any claims about how this type of intervention would generalize, but we are hopeful their users would respond in kind.



Though the VDOS story ends in legal action against the perpetrators many more services exist and more work needs to be done to understand how to effectively undermine these commoditized crime services.

- References

[1] Karami, M., Park, Y., McCoy, D.: Stress testing the booters: understanding and undermining the business of DDoS services. In: Proceedings of WWW (2016)

[2] Brian Krebs. Israeli Online Attack Service 'vDOS' Earned $600,000 in Two Years. https://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/