International Journal of Research in Engineering, Science and Management
Volume-2, Issue-4, April-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Call to Deal with Technical Support Scams

Musadiq Bin Javid[1], Sudeshna Chakraborty[2]
[1]*M.Tech. Student, Department of Computer Sciences Cyber security, Sharda University, Greater Noida, India*
[2]*Assistant Professor, Department of Computer Sciences Cyber security, Sharda University, Greater Noida, India*

***Abstract*: With the advancement in E Commerce, Threats that came along as an excepted side effect have been professionally handled by machine learning techniques and data mining-based systems. Most important implemented techniques are under training all the time which has provided ease in further development. Yet, unfortunately Technical Support Scams and Frauds are hidden in plain sight for a decade now. The scam starts with a deception by landing fake but well-crafted webpage that freezes the users screen. User is then manipulated to believe that a malware with ability to steal information has got downloaded on his computer, and for assistance a Toll-Free number is also mentioned on the web page. The next and most crucial step is to gain trust and make user believe the infected computer must be remotely connected to diagnose the issue and for fixation a sales pitch is made. Users who fall end up paying hefty amount by his credit card or they use other modes of payment as well. The amount of money being charged by these fake support centers is enormous and this is just a beginning of very large process. Once contact is made and user has been charged for nothing, all the information involved during the transaction like credit card numbers with both Expiry Date and CVV, personal information of the user and in some case even the data on the computer, is then sold to highest bidder.**

Based on the experience during research, I felt the call of millions of innocent people to identify such charges made on remotely monitored computer as fraudulent and machine learning techniques will then effectively flag such fraudulent charges and further blocked and hence it may put an end to lot of others scams as well. This paper can also help researchers to design and implement more machine learning rules and advanced data mining systems, to fill in the void and provide more advance security to the users over the globe.

***Keywords*: Secure Future of E Commerce, Cyber Security, Tech Support Scam, Fake Web pages.**

1. Introduction

Technical Support Scams exist and there is huge amount of evidence available over internet to support this claim. Microsoft itself is well aware about this fact but yet so far none of the actions have proved effective to counter these scams. Fortunately, a first systematic study was published last year by a team from stony brook university New York that has proven effective to put light on these scams and made it easy for law enforcing agencies to take suitable actions against the people involved in it. Tech support scams, how people pay for fake computer help and end up not only getting scammed, the personal information of the victim is also vulnerable to the scammers who are remotely connected to victims' computer. And once the remote desktop connection is established the fraudulent transaction made by the scammers is processed successfully and the victims have generally no clue what is going on with their computer. Hence, it becomes the responsibility of Cyber Security Professionals to first understand the nature of this scam and then present solutions to counter these scams. A scam that has been operating in shadows from a decade now claims loss of billions of dollars every year. It does not require any advance skills to be a part of this scam. All the tools required are easily available. It just takes a bit extra convincing power just to manipulate the user to think he is speaking with genuine personnel who is there to help him.

In a recent case, Arzella Sally Moser, a retired banker in Hayward California said, since she had worked in the fraud division of what is now Chase bank. Yet she and many others most which are elderly are among a large number of people targeted by companies running such scams. One of the major among these scams is Technical Support Scam. Microsoft claims they received 153,000 reports last year from customers who were victim to tech support scams, and this is about 24% rise from the year before. Also these reports came from 183 countries, therefore a global problem.

Approximately 15% of these customers lost their money in the scam, on average between $200 and $400. In some cases, victims pay a lot more. In December 2017, Microsoft received a report of a scammer by taking an amount of €89,000 during a tech support scam in the Netherlands [17].

However, it's tricky to put an absolute number to the problem. The figures above represent reports from Microsoft only. So we can have an idea of how big this problem is, given that tech support scams have now upgraded because the more advance system we develop becomes an ease to them, they also target customers of various other devices, platforms, or software. Even though we know that this kind of scam exists, and scammers are getting away with billions of dollars every year, still there is no solid response from security community.

2. Dial one for scam

A first systematic study of Technical support scams and the operators was presented last year by a team from department of computer science of stony brook university. They have identified Malwartising as a major cause of how people get in contact with the technical support scammers.

The team designed a web crawler tool which they named as

"ROBOVIC" capable of discovering hundreds of phone numbers and domains operated by scammers on weekly bases and the results they retrieved helped them to analyse the whole infrastructure of basic Technical Support Scam.

They continued to run their automated web crawler tool for 8 months and collected a huge amount of data exposing domains and Toll Free numbers used by the scammers'. Further, they interacted with 60 scammers posing as one of their customers to get the insight of the whole process. The work done by the team was very effective and taken seriously by the law enforcing agencies who were able to nab few culprits from the information provided from their tool "ROBOVIC" [2].

A. Robovic

For finding of every possible scam, there was a development of a tool known as the "ROBOVIC" (or robotic victim that visits millions of websites itself in search of scams. their crawler was targeted to the best known websites in which the scammers create "typosquatting" i.e pages that impersonate as legitimate web sites and there are certain URL shorteners showing the spammy ads to the visitors. ROBOVIC visited about 5 million pages and discovered that about 22,000 tech support scam pages were hosted at a rough estimate of 8,700 domains. There was luck and, they found that an Apache module used in 142 of those pages was exposing the traffic counting codes, which allowed the research people to know how many people were visiting those sites. The prior fake antivirus scams research indicate about two percent of the people fall for these similar traps, then the team estimated, that $2,000 a day were charged by these domains. By periodically visiting of these scam sites, they got an idea of how much time these pages stay online before disappearing likely as the hosting companies of these domains removed the fraud. About 70 percent survived for between one and three days, though about 7 percent lasted well over a month. Based on all of that data taken together, the researchers roughly estimated that the scam domains they discovered made about $75 million a year. But the researchers only found a fraction of these frauds and not the companies which create them, moreover they don't have the claim of the total no of fraud in the industries.

3. Interaction with scammers

Once the team understood how people get in contact with the scammers, they further dialed 60 scam numbers which they were certain of the numbers do not belong to any legitimate organization. Creating a fake pop up of this kind is easily done in JavaScript and it is easier to deploy these fake pop ups along with a fake advertisement website. Once a customer selects any such website, within no time, the pop-up lands on victim's screen and freezes the computer. Generating calls is itself a whole new industry, who only deals with generating such calls using Ad Campaigns available easy nowadays. During my research one call is sold at an average $10.The amount of such campaigns have risen to such value that even Google has undergo regular updates, to suspend such fake Ad Campaigns. I have given a sample of commonly used fake pop up.

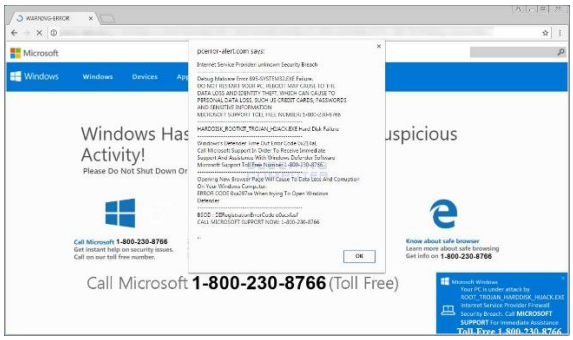

Fig. 1. Fake Microsoft alert warning

A. An organised technical support scam business model

Tech support scams come in several forms, but they share a common plan and basic plan of attack:

Fig. 2. Organized Tech Support

The scammers claim to be certified technicians and they create an environment where a user ends up believing that all the information on the computer is under threat as there has been a network breach.

To achieve this level of trust, scammer uses few basic scare tactics and runs them on victim's computer and while scammer is faking the diagnosis of the computer, he keeps the victim involved in conversations to make the problem sound huge and to create necessity for the victim to take care of the issue.

4. Results

A. Use of computer's inbuilt utilities

- CMD
- NETSTAT
- Action Center
- Event viewer
- Defining a certain virus to the user
- Stopped services and drivers

- *Command prompt:* CMD is used in the beginning to run a directory scan by command 'dir/s or tree' and this explained as Scan of the computer and network for problems. While the files are flashed in CMD, scammer has already pasted a prewritten Text and presents it as warning alert.
- NETSTAT: Once this command is executed, we get active connection list IN CMD. The Foreign address column is explained as those devices who have tried to establish a connection with victims' computer. The entries that come up with different name apart from system host name are described as connections that are unauthorized.

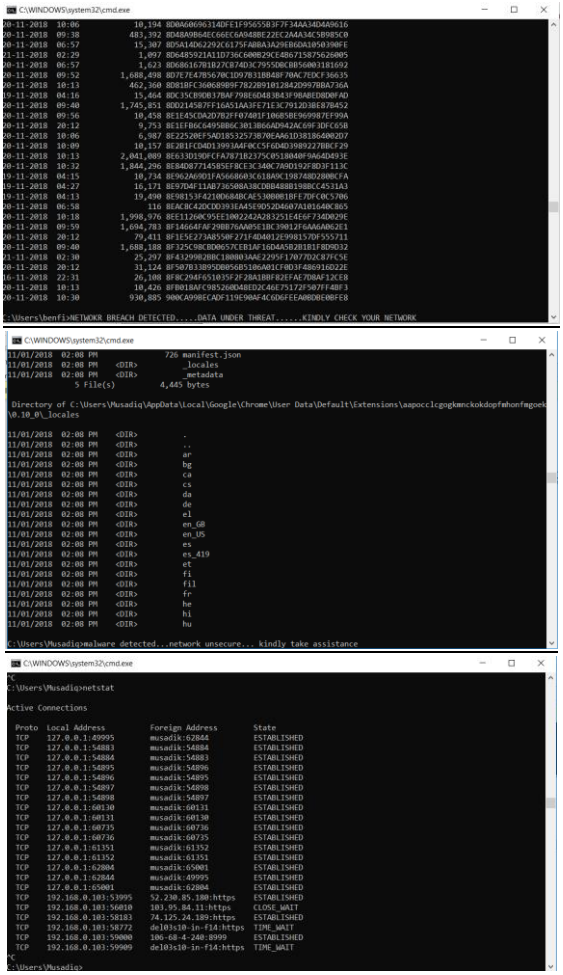

Fig. 3. Use of CMD commands

- The scammer also shows few operating system utilities like stopped Services and Drivers, to keep the victim under impression that a problem exists within the system The tools for remote desktop connection are easily available and does not even cost anything sign up for such a tool. The commonly used tool is GoToAissist by LogMeIn. Around 80% of total scammers use this tool for establish a connection.

Table 1
Basic computer utility

Technique	% Calls
Stopped Services/Drivers	67
Event Viewer	52
Specific Virus Explained	50
System Information	47
Action Center	40
Fake CMD Scan	40
Netstat Scan	40
Installed/Running Programs	35
Browsing History/Settings	27
Downloaded Scanner	17
Reliability/Performance	15
Other (Temp, Registry)	13

B. *Price of the service and Duration of the calls*

The money asked for fixation depends on how much victim can pay, which is never less than $99.99, and the amount is processed using a gateway by a credit card or other mode of payment. Most scammers offer two to three different options with support packages ranging from a one-time fix, to multi-year support, ranging anywhere from $69.99 to $999.99. Figure 1.5.2 shows the ECDF of the amount requested, split in its minimum, average, and maximum [1].

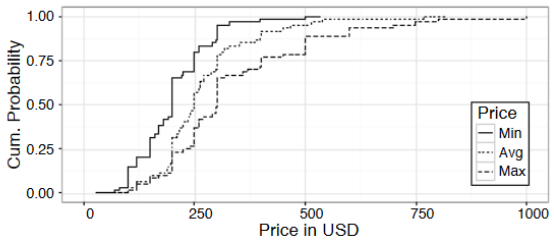

Fig. 4. Amount claimed by scammers

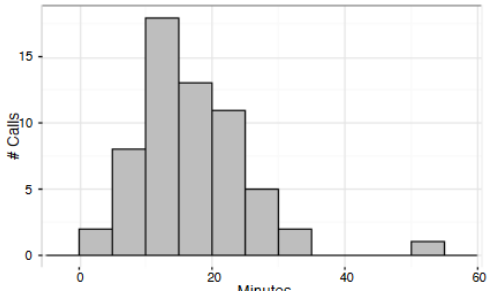

Fig. 5. Distribution of the time duration

As per the survey of 100 days, a Technical Support Scam with 20 agents for sale takes 150 such calls a day. Sale made in Total is half million dollars, once we pay attention to these numbers, it is hard to believe such a basic deception can lead to loss of billions of dollars every year. With loss of money the next important thing which is lost is information of the victim, that can be further used to for other fraudulent activities.

C. *Other ways to scam and important points*

- QUICKBOOKS SCAM
- REFUND SCAM
- TAX COLLECTION
- BIT COIN SCAM

The above-mentioned processes are much worse than Technical Support Scam because money that is involved is much large is number. There have been cases where all the money was taken from victims account and it never raises an alarm as money is being processed on victim's own computer. The sales data is also then further sold and the same customers are asked for money again in the same manner. And due to lack to awareness in the related subject around 50% of customers pay again. The chargeback filed are in very high ratio, but in most of the cases until then scammers flees away with money, leaving customer, Bank and merchant to bear the loss.

5. Interaction with scammers

The main question that arises is "How can such a basic fraud escape recent advancement in machine learning techniques and data mining-based systems".

Based on the research answer to this question is very simple, once the remote connection of a user's computer is taken and user is already playing on the hands of the scammers, the transaction that would be made will have users consent and hence it bypasses most of tools used in monitoring electronic fraud. And most of times scammer gets away with money. The need is to identify payments made by the scammers by remotely connecting with victim's computer as fraudulent transactions. And, also technical support scams are still basic scams compared to other scams that have evolved from the same idea of taking remote control and later on deceive the user. This approach may put an end to other scams that have use the same attack plan.

6. Objective

The objective of the research is to identify all the transactions made on any remotely monitored computer as fraudulent transactions. The scam has now spread to various other platforms but still gaining access of victim's computer remain a key point of all these scams. So, I believe once our payment gateways will be able to decline payments made on remotely monitored computers, it will put an end to most of such scams. There are cases where victims end up paying these scammers by send physical checks, gift cards like ITunes, Wal-Mart coupons, amazon gift cards. But the most transaction are made via credit cards and we will lay our focus on the objective stated above.

7. Research methodology

The research method will be purely based on survey results that will be conducted by first hand interaction with call vendors and scammers themselves, to join all the dots to prove how such scams are advancing to different platforms and why payment transitions made on a remotely monitored computer should be considered as fraudulent.

8. Sources of resource

Primary source: Surveys conducted while direct interactions with different kind of scam establishments present in the area of research.

Secondary source: purchasing calls from the call vendors. The leads as we know and even has been explained by the team of stony brooks university in their paper, are provided by these call vendors whole use domain parking and other techniques to generate the calls. So, our attempt will be get hold of this data and analyze it summarize and provide proof to our objective.

9. Expected outcome of the study

As increase in usage of credit cards has become more and more common in every field of the daily life, credit card fraud has become much more evident. To improve security of the financial transaction systems in an effective way, building an efficient credit card fraud detection system is one of the major tasks for the financial institutions.

The project has the goal of identifying Payment Transactions made on Remote Accessed computers as fraudulent charges. This paper can also help researchers for designing, developing and implementing a risk scoring system (using data mining techniques), that can put an end to most proportion of the online scams.

10. Conclusion

This paper presents an overview on Technical Support Scams.

References

[1] Nuno Carneiro, Gonadal Figueroa, Miguel Costa (3 Jan 2017), "A data mining based system for credit-card fraud detection in e-tail", Decision Support Systems.
[2] Najmeh Miramirkhani, Oleksii Starov, Nick Nikiforakis (19 Mar 2017)," Dial One for Scam: A Large-Scale Analysis of Technical Support Scams".
[3] Evandro Caldeira, Gabriel Brand˜ao, Adriano C. M. Pereira, (2014)," Fraud Analysis and Prevention in e-Commerce Transactions", 9th Latin American Web Congress.
[4] Parvinder Singh, Mandeep Singh, (February 2015)," Fraud Detection by Monitoring Customer Behavior and Activities", International Journal of Computer Applications, Volume 111, No. 11.
[5] Agten, P., Joosen, W., Piessens, F., and Nikiforakis, N. Seven months' worth of mistakes: A longitudinal study of typo squatting abuse. In Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS) (2015).
[6] Alrwais, S., Yuan, K., Alowaisheq, E., Li, Z., and Wang, X. Understanding the Dark Side of Domain Parking. In Proceedings of the USENIX Security Symposium (2014).
[7] C. Phua, V. Lee, Smith, R. Gayler, A comprehensive survey of data mining-based accounting-fraud detection research, International Conference on Intelligent Computation Technology and Automation 1 (2010) 50–53. doi:10.1109/ICICTA.2010.831.
[8] Costin, A., Isacenkova, J., Balduzzi, M., Francillon, A., and Balzarotti, D. The role of phone numbers in understanding cyber-crime schemes.
[9] Google. How we fought bad ads in 2015. https://googleblog. blogspot.com/2016/01/better-ads-report.html.
[10] Google's Anti-Malvertising Team. Anti-malvertising.com. http://www.anti-malvertising.com/.
[11] Gupta, P., Srinivasan, B., Balasubramaniyan, V., and Ahamad, M. Phoneypot: Data-driven understanding of telephony threats. In Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS) (2015).
[12] Harley, D., Grooten, M., Burn, S., and Johnston, C. My PC has 32,539 errors: how telephone support scams really work. In Virus Bulletin (2012).
[13] Invernizzi, L., Comparetti, P. M., Benvenuti, S., Kruegel, C., Cova, M., and Vigna, G. Evilseed: A guided approach to finding malicious web pages. In IEEE Symposium on Security and Privacy (2012).
[14] Khan, M. T., Huo, X., Li, Z., and Kanich, C. Every second counts: Quantifying the negative externalities of cybercrime via typo squatting. In Proceedings of the 36th IEEE Symposium on Security and Privacy (2015).
[15] Kharraz, A., and Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E. Cutting the Gordian knot: A look under the hood of ransom ware attacks. In Proceedings of the 12th Conference on Detection of Intrusions and Malware &Vulnerability Assessment (DIMVA) (2015).
[16] https://www.chargebee.com/blog/credit-card-fraud-detection-tools/

[17] https://www.thestar.com.my/tech/tech-news/2018/08/06/tech-support-scams-are-on-the-rise-heres-how-to-avoid-them/
[18] https://arstechnica.com/information-technology/2014/11/ftc-windows-tech-support-scams-took-another-120-million-from-pc-users/
[19] AWS |Amazon Elastic Compute Cloud (EC2) – Scalable Cloud Hosting. https://aws.amazon.com/ec2/.
[20] Bing Ads. Low quality ad submission & escalation. http://advertise.bingads.microsoft.com/en-us/report-spam-form.
[21] Internet Crime Complaint Center (IC3), New Twist to the Telephone Tech Support Scam.
[22] http://www.ic3.gov/media/2014/141113.aspx, 2014.