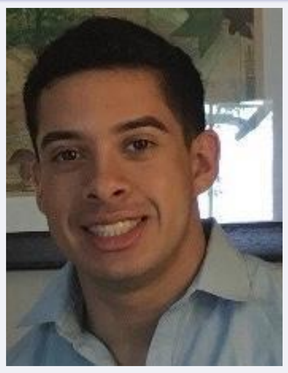
Analysis of Malware and Ransomware Generation through 5G

Austin Ramos

The University of Texas at San Antonio, San Antonio TX, 78249



Name: *Austin Ramos*
Status: *Junior*
Department: *COE/COS*
Area of Study: *Computer Science*
USDA/UTSA Mentor(s): *Guenevere Qian Chen*

WeARE Research Area

The main area of research will focus on the security infrastructure of 5G, and what holds truth to malware/ransomware propagation throughout the security landscape of the new generation cellular network.

Motivation or Background

With the latest implementation of fifth generation (5G) cellular network by IEEE (Institute of Electrical and Electronics Engineers), 5G is being sought as to improve cellular frequency, bandwidth and latency thresholds. IEEE comprises 5G of five necessary technologies that bring the full spectrum to life. Millimeter Waves, Small Cells, Massive Multiple-Input-Multiple-Output (MIMO), Beamforming and Full Duplex are the underlying foundations that 5G requires before implementation. Due to the increase of malware/ransomware attacks on local municipalities, hospitals and federal agencies [4; there is a better need to understand how these types of attacks propagate throughout systems. However, these aren't the only domains that malicious adversaries have thwarted upon. 5G has become increasingly deployed to replace previous cellular generations without secondhand thought to the security faults that lie within technologies that 5G will be conducted upon. For millimeter waves to be actuated, 5G requires Small Cell networks (base stations), which is further comprised of FemtoCells, MicroCells, PicoCells and MeadowCells. Each of the types of cells are made by a different manufacture and serve the same purpose, while having a different view on security implementation. This fact jeopardizes 5G to be used as a medium to distribute possible cyber threats, as shown by Fang [1]. The purpose of this research is to gain a better understanding of the security pitfalls of 5G and what threat malware/ransomware poses to the cellular landscape.

Objectives

1. To better understand propagation of malware/ransomware throughout testing of F.O.G computing.
2. Analyzing behaviors and effects of malware/ransomware to what threats they pose to the domain of 5G.
3. Defining a classification metric for future research into machine learning models that can be used to predict future malware/ransomware threats can be easily defeated.
4. Enhance 5G small cell manufacturer knowledge in regards to malware/ransomware threats and what can be done to mitigate the issue.

Methodology

For use of the malware/ransomware testing, F.O.G computing was used since it was best suited for this specific type of testing. Most malware/ransomware will recognize if it has been deployed on a hypervisor, rendering security analysis useless as it will not deploy. F.O.G computing uses the predefined operating system (i.e. Windows 10) and copies it and saves it (preimage) to a central server, from which the user can deploy the image to a set host [2].

The samples were a collection from the VirusTotal academic repository of malware [5], the samples are then saved to the preimage of the operating system along with W.L.S (Windows Logging Service) which contributes enhanced operating system details in the Linux syslog format [3]. The preimage is then uploaded to the F.O.G server in which then is saved for deployment as the post image. Malware/Ransomware is then executed for the allotted time of ten minutes to give static means of collecting across all samples.

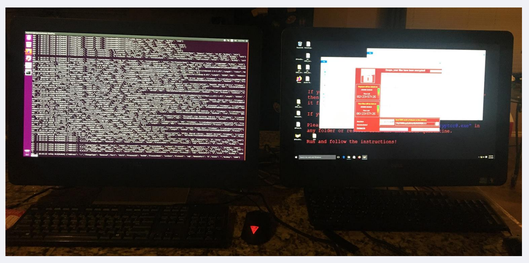


Fig. 1
The left monitor hosts the FOG server and WLS server, while the right monitor is where the malware/ransomware conducted on.

Results

Fig. 2 shows the result of sample testing, with services.exe having the higher precedence of all occurrences at fourteen, with Microsoft.Photos.exe following right after with eleven occurrences. Each of these first instances were first pre recorded by WLS to see how executables would traverse throughout the Windows 10 operating system.

As Fang [1] shows that a fault in 5G is Denial of Service and Distributed Denial of Service (DoS and DDoS) are still a possibility through different layers, including base stations. H. Wang notes that even though Google has a vetting process for the Google Play Store, malicious applications still seep through into vulnerable android users [6].

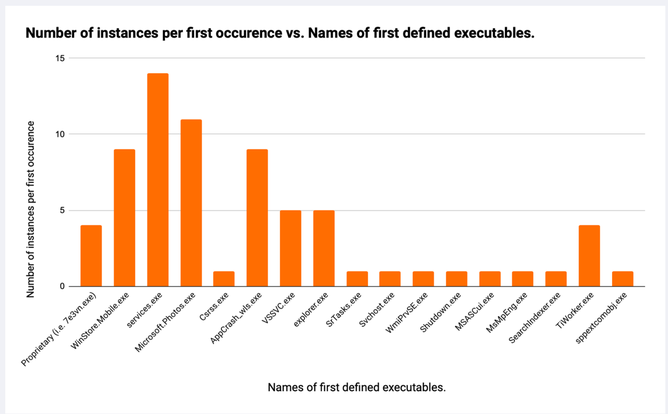


Fig. 2
Graph representing the total amount of instances a executable was noticed according to WLS.

However, it is with great magnitude that the samples that could be passed are also magnified at the larger scale when it comes to 5G networks. Logic bombs (part of the samples tested) are malicious pieces of code that activate once a certain condition is met. Having a pseudo-safe application downloaded from the Google Play Store and having this piece of code (Logic Bomb) on multiple devices could be detrimental to 5G networks, as little research has been done into DoS and DDoS for base stations.

In conclusion, even though malware still arises, there is a need to better understand the executables at work. Creating a supervised machine learning algorithm and distributing multitudes of datasets for types of ransomware/malware executables will deter adversaries from having compromised mobile devices, as better understanding can be made for these types of threats cascading down to 5G networks with rendering DoS and DDoS attacks trivial.

Skills and Experience

The U-GREAT experience has granted me the opportunity to work with real world threats by contributing to my undergraduate Spring 2020 semester. Not only did I get to learn how to use use ransomware/malware analysis techniques, but also put forth work for UTSA that reinforces its prominence in Cybersecurity and academic research. The ability to use F.O.G computing has made threat analysis non trivial compared to deploying within a virtual machine. Having had already used WLS for a previous project and knowing what significant impact it had on contributing to host based detection for malicious activities, it was helpful already having a background in the application and applying it to this project.

What I Learned

Being able to take what testing I conducted and apply it to real world scenarios, has allowed me to enhance my scope of view for what threats adversaries pose on from academic institutions, local municipalities, federal workplaces and medical facilities. The continuous threat with the constant evolvement of threats enchnaches the cyber landscape for further understanding which can be reinforced with machine learning models.

Future Plans

I will collect more specific 5G and cellular related malware/ransomware that traverse through cellular networks. In expansion of this collection, processing the data with machine learning models will yield extensive classification. The use of this classified data by machine learning models will help us better understand the cyber threat realm of cellular networks and what can be done to mitigate these issues for 5G. Constructing these machine learning models with the guidance of my mentor, Dr. Chen, we can help contribute to real world applications being the security of base stations and 5G.

Acknowledgments

This work is supported by the USDA National Institute of Food and Agriculture, Interdisciplinary Hands-on Research Traineeship and Extension Experiential Learning in Bioenergy/Natural Resources/Economics/Rural project, U-GREAT (UnderGraduate Research, Education And Training) program (2016-67032-24984).

References

[1]D. Fang, Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks," in IEEE Access, vol. 6, pp. 4850-4874, 2018, doi: 10.1109/ACCESS.2017.2779146.
[2]"Introduction - FOG Project", *Wiki.fogproject.org*, 2016. [Online]. Available: https://wiki.fogproject.org/wiki/index.php?title=Introduction#What_is_FOG.
[3]A. Myers, "Windows Logging Service", *Kcnsc.doe.gov*, 2017. [Online]. Available: https://kcnsc.doe.gov/docs/default-source/kcnsc-software/windows-logging-service-summary_073117.pdf.
[4]S. Cook, "Ransomware Statistics 2018-2020 : 50+ Ransomware Stats & Facts", *Comparitech*, 2020. [Online]. Available: https://www.comparitech.com/antivirus/ransomware-statistics/.
[5]"VirusTotal", *Virustotal.com*, 2020. [Online]. Available: https://www.virustotal.com/gui/home.
[6] H. Wang, H. Li, L. Li, Y. Guo and G. Xu, "Why are android apps removed from google play?: A large-scale empirical study", *Proceedings of the 15th International Conference on Mining Software Repositories (MSR '18)*, pp. 235, 2018.