2021 NDIA Ground Vehicle Systems Engineering and Technology Symposium
VEA/Cyber Technical Session
August 10-12, 2021 – Novi, Michigan

RANSOMWARE VEHICLE EMBEDDED SYSTEM ATTACKS

Charles Parker, II

ABSTRACT

Ransomware is not a new method of malware infection. This historically had been experienced in the enterprise in nearly every industry. This has been especially problematic in the medical and manufacturing fields. As the attackers saturate the specifically targeted industries, the attackers will expand their target industries. One of these which has not been significantly explored by the ransomware groups are the embedded systems and automobile environment. This set of targets is massive and provides for a vast attack potential. While this has not experienced this attack methodology at length, the research and efforts are creeping towards this as a natural extension of the business. The research focusses on the history of ransomware, uses in the enterprise, possible attack vectors with automobiles, and defenses to be explored and implemented to secure automobiles, fleets, and the industries.

Citation: Parker, C., "Ransomware Vehicle Embedded System Attacks", In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, August 10, 2021.

1. Introduction

Ransomware began with describing the attacker's actions of ransoming software [1]. The first occurrence was created and distributed by Dr. Joseph Popp in 1989. With the internet not being prevalent, the attack mode instead was the USPS. Dr. Popp mailed 20,000 infected floppy disks to the targets. At this point in time, the attacker required the ransomware fee to be paid via a money order to be sent to a post office box in Panama [2], instead of Bitcoin as notably used today.

In recent years, the use of ransomware has increased exponentially [3] as the attack became operationalized. This has become such an epidemic that 2016, by some, has been named "The Year of Ransomware" [4]. This has grown to the point where the term Ransomware of Things (RoT) is used to describe the abundance of attacks [4]. The attack method has become so profitable to the point third parties are contracting their services with others to perpetrate yet more ransomware in the environment. The person simply contacts the service, provides email addresses and other data if needed, and waits for the attack proceeds. The activity has morphed into ransomware-as-a-service (RaaS). The attacker's client does not have to code the program for the ransomware. The ransomware is already operationalized to the point the business side of the transaction has their commission standardized.

Ransomware has become a global issue. Performing the attack has become standardized and conducting this has the same level of ease for a target 10 miles and 1/3 of the globe away. One reason for this is the level of inter-connectedness in society [5]. As more devices and targets are connected, this will continue to be an increasingly significant problem. When this is effective with the breach, the victim tends to incur downtime costs, potential loss of data, and other consequences [6].

Ransomware historically has primarily been experienced in the enterprise. Two automotive industry examples of this are France's Renault and Japan's Nissan being forced to temporarily idle a portion of their manufacturing plants in 2017 due to the WannaCry malware [7]. While this is significant, IoT has a new level of sophistication. The ransomware potentially has a much greater impact for IoT, connected devices, embedded systems due to the integral connectivity. With a breach, the attacker has the ability to control the entirety of the data and system. At best, the user would have limited access and usability [2]. This directly impacts vehicles. Currently and looking forward, the vehicles consumers and commercial entities drive daily are being engineered with more connectedness [8], which is a significant function of the infotainment and other systems. For the vehicle's environment, this brings the risk of ransomware.

2. General Operations

There are many forms of attacks for ransomware to take with these [9]. The general mode for the enterprise is to breach the defenses via an email with malicious links or attachments, encrypt the data, files, or system, and demand a ransom for the decrypt key. The alternative noted with the attack has been for the data to be exfiltrated and the ransom is paid for the promise not to publish the data. The victim would be able to recover the data after the ransom is paid with the decrypt key [10].

A natural extension of the attack is to pivot the focus to ground vehicles. With the enterprise being flooded with these attacks and the success rate, at some point there will be a saturation and the attackers will need to adjust their focus to a new set of targets to maintain their revenue and productivity levels. Each ground vehicle system is different. This form of an attack may need to be adjusted for each model due to the unique architecture and model being targeted. The nuance with the form of attack is focusing on the vehicle

architecture and attack opportunities. While dozens have shown the ease of hacking into a vehicle [11] using the present various tools and exploiting cybersecurity weaknesses with the CANBus and the modules, the ransomware attack provides for new targets and opportunities. This also provides the opportunity for new attack methods.

3. Literature Review

Attacking vehicles is not a new venture. This began decades ago by mechanical means with the method involving a brick and screwdriver. The technology-based attacks are updated regularly with advances created by cybersecurity researchers. These attacks have proved to be a very successful and profitable business endeavor, leading more persons getting involved. As this attack has become more prevalent, there has been more variants introduced. In recent years, vehicle ransomware applications have gained more attention.

a. General Background

The computer equipment used by consumers and business continues to decrease in size [2]. With these miniaturizations, there are minimal differences between the devices and sensors. These, due to the resource constraints commonly used defensive measures may not be applicable. This has allowed for more attacks with greater devastating effects.

b. Processes

Ransomware is vacuous malware, in that the attack is flexible and allows for a variety of targets. Other attacks are much more clearly defined. An example of this is the DDoS attack. The attack method is relatively clear, as is the effect. Bae, Lee, and Im [12] researched ransomware's operations. Generally, the attack works rapidly to lock or encrypt the victim's files or systems. The researchers proposed a new method to distinguish ransomware from normal files and processes, in addition to other malware. This analyzed API sequences, focusing on only the file-related APIs with machine language (ML). The noted sequences were noted and flagged as ransomware when scored above a certain benchmark. With the potential to remove all uses for the data and system, at times with only one click, this pertinent topic garnered the attention of other researchers. Cabaj, Gregorczyk, and Mazurczyk [10] researched this, noting for nearly all cases ransomware has used the internet as the attack vector. The researchers pivoted from this and analyzed using hardware as the vector. From this, a nuance was created to detect ransomware in a system. This application applied a Software-Defined-Networking (SDN) detection method. The focus, for this method, was searching for the feature's ransomware uses while communicating. To test this, the researchers used two ransomware variants (CryptoWall and Locky). The research indicted the HTTP sequence for messages and content size was sufficient for detection. While the industry predominantly has begun using HTTPS, this still has attributes to learn from and apply.

Other researchers have also analyzed the traffic to detect ransomware. This works by infecting documents and shared volumes the victim has access to. The intent is to cease the malicious activity. The researchers' new method monitors in a passive mode the network traffic [13]. To test this, the researchers used 19 variants from the different forms of ransomware. The research indicated the ransomware activity may be detected within 20 seconds. This equates to less than 10 files being encrypted. The algorithm provided for a low false positive ratio. To analyze the ransomware behavior to create detection methods, the logs are examined [3].

Monitoring the traffic appears to be the prominent ransomware detection method. Ng, Rajasegarar, Pan, Jiang, and Zhang [1] moved this in a partially different direction and used a honeypot for their research. The proposed new method involved intercepting the traffic and analyzing these for executable payloads. While simplistic, the new method incorporated machine learning (ML).

c. Vehicle Ransomware

A majority of the research previously published has been centered on the enterprise. This is natural as the ransomware attacks began years ago with the enterprise. Talib, Abbas, Nasir, and Mowakey [14] pivoted from this and researched applied security to the internet of vehicles. As most consumers have experienced the popularity and use of connected vehicles, and the level for the technology required for this has been increasing quickly. The focus for the development teams has been implementing this and improving the tech in the vehicles as vehicles become more autonomous. The research was based on 127 articles published between 2010 and 2018. The articles were divided into groups for different attack forms, solutions for these attacks, and performance results. In particular, the researchers noted the attackers may use ransomware to create revenue streams, with ransomware having the opportunity to create wealth for the attackers based on the target market.

Weiss, Schroette, and Hackberg [8] created an algorithm to estimate the risk of each vehicle ransomware attacks. The researchers took their experience from real-world ransomware and applied this to vehicles. The research did not delve into attack methods. Their method with generalized nodes allowed for risk estimation. This also provided for detecting potential weaknesses to ransomware in the vehicle design. Bajpai, Enbody, and Cheng [15] likewise noted the natural extension from the enterprise to automobiles as ransomware evolved. These researchers likewise did not explore ransomware attack methods. As the vehicles continue to be connected and at a greater pace, the attack surface grows. Knowing the enterprise is not the same for attacks as vehicles, the researchers noted possible constraints with ransomware attacks in the vehicles.

4. Vehicle Ransomware Attack Methods

The automobile manufacturers have been more focused on updating the technology in vehicles than other areas, (i.e., cybersecurity) [16]. This is understandable, as the technology is one of the primary factors consumers review when purchasing a vehicle. When confronted with two options, the automobile with more and better features and technology include will garner more attention and subsequent sales. As a bi-product of the increase in technology in the automobiles, more cybersecurity attacks have been performed.

One of the biggest threats to vehicles in the near future will be ransomware [11]. The application of ransomware may take the same form it has with the enterprise and consumers. This may take one of many forms. This may lock the users out of their vehicle or inside of these, cease the ignition operations, or other critical operations, and/or demand the Bitcoin payment for the key. One notable issue with this is its structure. The initial difficulty with ransomware is the speed of infection, dependent on the malware's functionality. The indicators of compromise have a time lag that tends to be too long to be very useful, dependent on the architecture.

a. Market

The enterprise market has been targeted and successfully attacked for years. The attackers have gained financially from each successful attack's victim for a few hundred dollars to over a million. As the detection and mitigation improve, reducing the return on the attacker's efforts, the focus will need to change to a new target market for it to be lucrative for the attackers. The automobile market is a natural target for the next generation of ransomware attacks. In 2018, there were 275.3M vehicles registered in the U.S. This increased to 279.6M in 2019 [17]. Most of these vehicles are viable targets. The attackers would exclude the vehicles which are not connected and do not have the required technology to be susceptible to these attacks. Fleets are also a significant target [11].

On an architecture level, the lack of segmentation to the infotainment system, ECG, body controller, power train, and ADAS controllers have added to the ransomware's opportunity. There is also the usage factor. People do need to use their vehicles for work, errands, and other needs. When the ransom is reasonable, the victim may be more inclined to simply pay the fee to regain the use of their vehicle, in comparison to attempting to have the vehicle towed to a dealership and firmware and memory flashed.

b. Attack Vectors

The vehicle architecture holds many areas in the attack surface to test and breach. This is increasing as more distinct modules are added to the vehicle and technology improves. There are likewise sufficient areas within the automobile to apply the ransomware threat.

The automobile has ample modules, and communication points to attack. Dependent on the architecture for the individual model, these may be access points for the ransomware attack. This issue is amplified due to the safety systems of a car are managed by computers in the vehicle. Historically these have included USB port(s), OBD-II port, BLE, Wi-Fi, and aftermarket equipment [19] for the standard attacks already experienced. These historic attack points have been targeted for years, as these have been part of the vehicle architecture and have had various levels of security applied. With the OBD-II part, the OEMs have started to lock these for se only with specific equipment or trusted sources. This step adds a layer to the defense in depth for the OBD-II port. While this is a general list, this is a fair representation for the hardware attack points to start with looking forward. There are many more within the vehicle modules. The attackers may also work through applications on smart phones as an alternative (e.g., Apple CarPlay and Android Auto). Any of these and any interface is susceptible to an attack, dependent on its architecture. This has been as a result of design vulnerabilities, vulnerabilities with software (SW), and hardware (HW) implementation, data and files being uploaded to the vehicle, and others [20].

The OBD-II port is well-known as an issue due to the ease of connection and attack. This has been addressed in earnest. This gateway to the vehicle's network also allows the attacks to introduce malicious messages and potential other issues, including installing malware onto the ECUs [20].

One notable area, which continues not to have an adequate level of research involves the supply chain and aftermarket equipment for the vehicles and OEMs. While both the supply chain and aftermarket equipment industries are different from each other, these hold a commonality with bringing the third party's products into the vehicle. As the parts are manufactured and assembled from the various suppliers, there is an opportunity at every step to add malware, including the code to apply ransomware, infecting the electronic parts [9] or to not mitigate vulnerabilities, allowing for attacks. The effect is the same for aftermarket parts. When these are not properly or fully tested for their cybersecurity stance, this allows for an issue and an attack point. The potential for the vehicle to be infected by malware, i.e. ransomware, is viable and will be an increasing issue.

The prior research has primarily been with the traditional ransomware forms. Related to vehicles, the prior research analyzed the potential for this to be applied to the vehicle architecture. There are a number of specific attacks and vectors not addressed with the prior research. One area not sufficiently addressed is the smartphone as the attack vector. As the consumer plugs the smart phone (e.g. iPhone or Android) into the vehicle's infotainment system, the consumer intends to interact with the vehicle's infotainment system as the host or tenant for the consumer with iPhone CarPlay or Android Auto. The connection with the smart phone provides for another

avenue for attack. The applications provide many functions demanded by the consumers to use while in their vehicle. The weak point in the attack surface is the consumer's phone may have vulnerabilities arising from updates not being applied or malicious applications being installed onto the phone. In this use case, the ransomware may use the phone as a pass-through to the infotainment system, and pivot to other areas within the vehicle's network.

Other attack paths have been researched for individual vehicles and fleets [18] [19]. The attackers would begin with acquiring a vehicle or module to work on their attack. After becoming well-acquainted with the system, the attackers would create the malware and decide on the delivery system. The delivery would depend on the individual OEM and model. The attackers could use physical means with the USB or OBD-II ports, or over the air (OTA). This would include the USB access to the infotainment system, OBD-II port to the vehicle's CANBus, CD/DVD access to the infotainment system, Bluetooth buffer overflow, cellular access to the vehicle's communication, WIFI vulnerabilities, aftermarket modules, and others [19]. These would be active measures to infect the vehicle. A passive measure may include having the user visit a website through the infotainment system. Just as with the enterprise, the attack path would be through the website. The nuance with this option would be the website would download the malware coded specifically for the vehicle's system. The system architecture will drive which method is preferable. At this point, it is important to note this may be a direct or indirect (i.e., through another source) attack. The vehicle targeted module would be infected with the ransomware. To increase the effectiveness of the attack, a module central to the vehicle's operations or communication would be selected.

The malware may be coded to communicate to the attacker's command-and-control (C&C) servers, encrypt or lock down certain systems. The malware may also comment with the C&C center to request further instructions, if not coded for this already. Once the malware infection is complete, the ransomware may use the CANBus to communicate with other modules to infect these also, or issue commands to lock down the module or vehicle, and also demand the ransom, which may appear on the infotainment system and screen for the user to react to.

5. Post-Infection

Once there is a successful attack against a module or the entire vehicle, the resulting encryption or locking out may be immediate or time-delayed. The user would not be able to use all or part of the vehicle's applications or operations. The malware may be coded to set a critical ECU to update the firmware or to be placed into maintenance mode until the key is provided by the attacker. While not encrypting, this would effectually act the same to the user in that the vehicle would not be usable. This attack is not complex, but very effective. The attackers could also lock down important cryptographic credentials the vehicle would use for communication or updates. These would not be recovered without significant effort on the user's part. Dependent on the configuration, this may present ECU authentication, V2X communication, vehicle platooning, and other critical functions. The ransomware could simply encrypt personal data, media, communications, logs, and other data [19].

6. Mitigations & Defenses

Ransomware has been a known issue for the enterprise for years. There has been ample time to create and implement sufficient defenses to combat this. These always have not worked to the preferred extent. While this is the case, these are still a vital step forward to a holistic cybersecurity application.

As more defenses are utilized and the revenue potential begins to decrease for the attackers, the attackers will migrate their ransomware attacks to other targets (i.e., vehicles). While this will not be as widespread

as the enterprise-oriented attacks initially there are still defenses available which may be adjusted for the vehicle cybersecurity architecture.

One aspect to address is segmenting the vehicle networks to isolate these. This would work to minimize the effect of any successful attack. With this in place only a portion of the vehicle network would be affected with the successful ransomware attack. To affect the majority of the network, the attacker would need to have several successful infections on the vehicle's network, all the while not being noticed. The systemic attack not being detected would be problematic for the attacker.

While segmenting is a valid defense, there are other active measures which could be implemented within the vehicle architecture. With this system, the development and security architecture teams need to leverage the indicators of behavior (IoB) to analyze the actions and tasks executed within teach system. This would take many forms, dependent on the system. Two of the possibilities would be monitoring the activities for any files, folders, or systems being encrypted or locked down, and heuristic analysis. These deployed in the system would be able to detect the anomalous behavior, as the teams have the baseline activity for the comparison. Dependent on the system there may also be present an ML program coded to recognize malicious code. This would have access to the code for the modules already present and there is a large sample pool for the ML program to learn from. The larger the pool, the better the ML program will be able to detect the issue. While these will work and prove themselves to be beneficial, there are resource requirements. These applications and others are not free. These will require memory, processing, and development to implement correctly. As time passes, technology improves, and ransomware shifts to ground vehicles, this will become accepted and implemented at a greater rate. As an analogy, there was a time when power brakes and windows were options. The point at which the vehicles are actively targeted may occur when the number of vehicles susceptible to this, from the architecture or online presence are available to attack. The same malware cycle has occurred with PCs. The PCs were predominantly targeted for attack above other platforms, until the others gained popularity and more consumers were using these. At this junction, this has not been a significant issue. This will grow to be a much more prominent issue, especially with electric vehicles (EV). To limit the potential issues, the system should control the applications, including the update process, and authentication [20]. There is also the opportunity to segment the automobile network architecture and utilize a form of the hypervisor to protect the automobile, and the occupants [21]. The ground vehicle architecture should also include some form of IDS or IPS.

7. Discussion

Vehicles have been targeted for attack for years. As the technology has increased in the vehicles, so have the actual and PoC attacks. There are more ECUs and computers in the vehicle which provide more points to probe and attack. The modules, along with their attack points, provide an even greater attack surface with their OTA updates, and dependencies in the cloud and servers. With all of these testable points, the attack surface has become more enticing. Once the attacker becomes more familiar with the individual vehicle architecture, the others of the same model are available for the same forms of attacks.

Artificial intelligence (AI) continues to be a growing field. While this started in the 1950's, there have been incredible strides forward in the last decade. One area which has began to incorporate AI has been ground vehicle systems. The ransomware malware may be adjusted to attack these systems. Looking forward, instead of the standard encryption or locking down a system, ransomware could be coded and implemented to hijack the vehicle and occupants. Certain systems, e.g., GPS, could be shut down or spoofed until the ransom

would be paid. As much as this appears to be a moot tangent for ransomware, there have been like alternative routes taken from other technology and mechanical devices.

For ransomware, the attack methodology provides a nuance, pivoting from the standard methods. The attack is not merely a thought experiment. The proof-of-concept (PoC) for this attack has been completed successfully [19]. This used a Raspberry Pi, Arduino, and a tachometer from a vehicle. Using these lessons learned in the testing phase, the attackers are able to ramp up the attack methods quicker for a more widespread attack not only against one vehicle model but many. This would when successful increase the return on investment (ROI) for the attacker. If we don't fully embrace this and prepare in a proactive manner, the industry will again be paying for this financially and operationally. The choice is ours.

1. References

[1] Ng, C.K., Rajasegarar, s., Pan, L., Jiana, F., & Zhang, L.Y. (2019). VoterChoice: A ransomware detection honeypot with multiple voting framework. *Concurrency and Computation, 32*(14), 1-29. http://dx.doi.org/10.1002/cpe.5726

[2] Yaqoob, I., Ahmed, E., Rehman, M., Ahmed, A., Al-garadi, M., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the internet of things. *Computer Networks, 129*(2), 444-458. http://dx.doi.org/10.1016/j.comnet.2017.09.003

[3] Hampton, N., Baig, Z., & Zeadally, S. (2018). Ransomware behavioral analysis on windows platforms. *Journal of Information Security and Applications, 40*, 44-51. http://dx.doi.org/10.1016/j.jisa.2018.02.008

[4] Cobb, S. (2017). RoT: Ransomware of things. https://www.eset.com/fileadmin/ESET/US/Newsroom/2017/03/ESET_Trends-and-Prediction_2017_Ransomware.pdf

[5] Thomas, M. (2017). Insurance: Challenges to the business model. *JASSA, 2*, 14-21.

[6] Al-rimy, B., Maarof, M.A., & Shaid, S.Z. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 44-168. http://dx.doi.org/10.1016/j.cose.2018.01.001

[7] Slaby, J.R. (n.d.). Ransomware still threatens the automotive industry. https://www.acronis.com/en-us/articles/ransomware-automotive/

[8] Weiss, N., Schroetter, M., & Hackenberg, R. (2019). On threat analysis and risk estimation of automotive ransomware. In *ACM Computer Science in Cars Symposium*, 1-9. http://dx.doi.org/10.1145/3359999:3360492

[9] Sectigo. (2019, July 7). Bad cars: Anatomy of a ransomware attack. https://sectigo.com/resource-library/bad-cars-anatomy-of-a-ransomware-attack

[10] Cabaj, K., Gregorczyk, M., & Maaurczyk, W. (2019). Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Computers and Electrical Engineering, 66*, 353-368. http://dx.doi.org/10.1016/j.compeleceng.2017.10.012

[11] Suciu, P. (2016, October 26). Ransomware: The next big automotive cybersecurity threat. https://www.caranddriver.com/news/a15443355/

[12] Bae, S., Lee, G.B., & Im, E.G. (2019). Ransomware detection using machine learning algorithms. *Concurrency and Computation, 32*(18), 1-11. http://dx.doi.org/10.1102/cpe.5422

[13] Morato, D., Berrueta, E., Magana, E., & Izal, M. (2018). Ransomware early detection by the analysis of file sharing traffic. *Journal of*

Network and Computer Application, 124(15), 14-32. http://dx.doi.org/10.1016/j.jnca.2018.09.013

[14] Talib, M.A., Abbas, S., Nasir, Q., & Mowakeh, M.F. (2018). Systemic literature review on internet-of-vehicles communication security. *International Journal of Distributed Sensor Networks, 14*(2). http://dx.doi.org/10.1177/1550147718815054

[15] Bajpai, P., Enbody, R., & Cheng, B.H.C. (2020). Ransomware targeting automobiles. In *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, 23-29. http://dx.doi.org/10.1145/3375706.3380558

[16] Goud, N. (n.d.). Connected cars are vulnerable to ransomware attacks. https://www.cybersecurity-insiders.com/connected-cars-are-culnerable-toransomware-attacks/

[17] Statistica. (2020, May 14). Number of vehicles in operation in the United States between 1st quarter 2016 and 4th quarter 2019. https://www.statistca.com/statistics/859950/vehciles-in-operation-by-quarter-united-states/

[18] Goldberg, J. (2018, April 29). When an automotive ransomware attack strikes a fleet. https://blog.guardknox.com/automitve-ransomware-attack-on-car-and-vehicle-fleet

[19] Wolf, M., Lambert, R., Schmidt, A., & Ederle, T. (n.d.). WannaDrive? Feasible attack paths and effective protection against ransomware in modern vehicles. https://www.escrypt.com/sites/default/files/documents/Ransomware-against-cars.pdf

[20] Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things Journal, 1*(1), 10-21. http://dx.doi.org/10.1109/JIOT.2014.2302386

[21] Parker, II, C., & Wasen, J. (2020). Hypervisor implementation in vehicle networks. WCX SAE World Congress Experience, Detroit, MI. https://www.sae.org/publications/technical-papers/content/2020-01-1334/