Unit 9 Virus Proliferation

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**February 14, 2023**

**Part 1**

Viruses are an important concept to understand in today’s cybersecurity landscape. Although it is impossible to go over every virus in existence in their disciplines there are certain malicious attempts that stand out from the rest. Certain viruses live on through legacies and adaptations similar to their biological counterparts. As malicious intent is utilized, viruses will continue to grow more and more complex and require more and more complex disciplines to halt them in their tracks. One such complex virus would be that of the Stuxnet program. Stuxnet is a cyber virus that was targeted in potential, but was uncontained and caused spreading. The virus was initially reported to attack weapons facilities within Iran these weapons facilities were commissions to develop nuclear weapons (Alvarez, 2015). It would do this by causing physical damage to computer components that Iran utilized in order to enrich uranium for their nuclear weapons platform. As nuclear weapons pose a great threat to all of humanity, the Stuxnet virus was meant to be one of many points of contention to help ensure a diminished count of nuclear weapons in existence going forward (Alvarez, 2015). Particularly, this was meant to slow the development of Iran’s nuclear weapons by way of malware that would cause chaos and confusion within the development platform that Iran relied on in order to develop their nuclear weapons.

The original virus utilized a malware attack that targeted logic controllers within the automation processes of Iran’s nuclear weapons facilities. This crippled hardware, and caused physical damage within these systems. Because of this, the virus was reported to be the first cyber security threat to cause physical damage within targeted components. This caused a widespread media attention, as it was theorized to be created by the United States’ National Security Agency, the Central Intelligence Agency of the United States, and the Israeli Defense Forces and National Intelligence (Columbia University in New York, 2012). The virus with meant to halt the development of Iran’s nuclear weapons system by causing physical damage while engineers working on the systems would not be able to determine the root cause of this damage. Reportedly, it was successful in this endeavor. Arguably the success of this virus was a bit too far spread. Certain outages in attacks have been reported since the release of this virus that seemed to correlate with warning signs and attack vectors that were originally used against Iran systems. This is lead cybersecurity analysts to believe that the Stuxnet virus is indeed spread further than just simply Iran’s nuclear weapons facility. Although there are many different theories of how Stuxnet exactly was administered to the irons weapon facilities, common theories include physical USB sticks that were carried in to the facility compounds via Central Intelligence Agency operatives in the area. The malware would then be uploaded to the automation systems associated with irons nuclear weapons facilities and become infested. Later, Stuxnet would become known to the security community due to an office in Iran calling security analysts for technical support. Certain systems in their office were experiencing shutdowns of computer components and windows devices despite having a clean software portfolio installed onto them. Interestingly, these systems that were failing are not linked to any Iran weapons facilities.

From this point onward Stuxnet is thought to continue throughout unrelated technical systems even today. Is global container would be practically impossible for a device that scaled, Stuxnet may continue to be an issue going forward. This is also spawned a number of different child malware utilizing certain aspects within this Stuxnet virus to perpetrate malicious attacks (Langer, 2013). In this, Stuxnet has a legacy that will continue to persevere even should the initial virus be wiped from computer components across the globe. This makes the Stuxnet virus particularly important to cyber security analysts and researchers even today. The inciting event of nuclear weapons research was undeniably forefront in the development of the Stuxnet virus and programs associated with it. Due to this inciting event, physical damage has been done to computer components, and a methodology of cybersecurity has been perpetrated throughout its appearance. Many particulars remain a mystery concerning Stuxnet, in the state that it is in today. It is not currently known the exact methodology that it was used in order to perpetrate its attack on Iran’s nuclear weapons facilities, and it likely will not be discovered for the foreseeable future.

Furthermore, it is not currently known how Stuxnet was able to spread throughout unrelated technical devices. Two further confiscate the situation, the Stuxnet virus was meant to attack specific systems within Iran’s nuclear weapons facilities. The infested devices that were reported following these Stuxnet inciting event were unrelated to nuclear weapons development, and serve to only add confusion into the atmosphere as to how exactly Stuxnet was able to affect these devices similarly to how it would need to for the nuclear weapons automation services (Baskin Engineering of UC Santa Cruz, 2018). All of this information, and lack thereof, provides an atmosphere of unease surrounding cybersecurity disciplines. Should an attack like this be perpetrated towards essential life services such as sustainability efforts and essential planetary maintenance, the event could be devastating. There are no shortage of individuals that would perpetrate malicious attacks to any degree. Because of that fact, vigilance is needed to be kept in order to maintain a safe atmosphere for all individuals living in harmony.

Although the disposal and slowing of nuclear weapons development life cycle may be seem as a positive outlook to some, the same disciplines may be used to unjustly strike grief and devastation into innocent citizens globally. As the Stuxnet virus was a major innovation in the way wars were fought further innovations are given to humanity. Stuxnet may be just simply the first event that a cyber security compromise was able to read devastation upon a certain industry, and most certainly not the last. It is paramount to understand the cause and effect one may have when regarding the development of these incredibly lethal devices, particularly in the modern age when technology is so prevalent in the daily lives of citizens around the globe.

**Part 2**

**Construct a security policy for the physical domain.**

The following is a policy for a cloud storage facility specifically with regards to physical security.

1. Employee training
   1. Employees will undergo a series of informational lectures regarding security policies that focus on physical security and behavioral mechanisms to maintain physical security.
   2. Employees will have a direct route to training personnel that they may use to ask questions, or gather further information relating to physical security policies being implemented in the organization.
2. Access Cards
   1. Physical cards are to be kept on all related security personnel at all times during their daily job functions.
   2. Physical Cards will not be switched between personnel under any circumstances.
   3. Compromised cards that have been lost, or are suspected to be cloned will be reported no later than one day after it comes to the attention of staff.
      1. These cards will be replaced using a new set of identity metrics at the discretion of the Chief Security Officer.
      2. The Employee responsible for the maintenance of their card will be recorded.
         1. If there have been no other security concerns related to this employee, they will be instructed to attend a mandatory security meeting to enforce compliance through understanding.
         2. If there have been one or two security breach events regarding this employee, they will receive written notice and be scheduled a meeting with supervisors to discuss behavioral adaptations.
         3. If there have been three or more security events regarding this employee, their employment with the organization will be terminated.
3. Physical Locks and Critical Entry Points
   1. Locks will be placed on all entry points to critical systems and data centers.
      1. These locks will respond and open upon presentation of a valid access card by organization staff.
      2. These locks will allow for automatic shutdown in cases of emergency to refuse entry to any personnel regardless of access card clearance.
      3. These entry points will have an automatic opening located within the data center to allow for personnel to escape in the event of a disaster such as a fire within the critical system.
         1. These automatic opening switches are not to be accessible by any means from the outside areas.
   2. Locks will utilize asymmetric encryption platforms with PGP integration with checking privilege information to ensure relevant and accurate entry information to prevent recently terminated employees or compromised cards from entry.

# **References**

Alvarez, J. (2015, February 3). *Stuxnet: The World's First Cyber Weapon*. Retrieved from Stanford University: https://cisac.fsi.stanford.edu/news/stuxnet

Baskin Engineering of UC Santa Cruz. (2018, March 12). *Stuxnet*. Retrieved from Dangerous World: https://dangerousworld.soe.ucsc.edu/2018/03/12/stuxnet/

Columbia University in New York. (2012, August 19). *Stuxnet: Tool of Nonproliferation or Pandora’s Box*. Retrieved from columbia.edu: https://k1project.columbia.edu/news/stuxnet

Langer, R. (2013, November 19). *Stuxnet's Secret Twin*. Retrieved from Brookings.edu: https://www.brookings.edu/articles/stuxnets-secret-twin/