Joshua Shilts

Mobile Apps II

The Fallout of Foreign and Domestic Cyber-Security Threats

Abstract

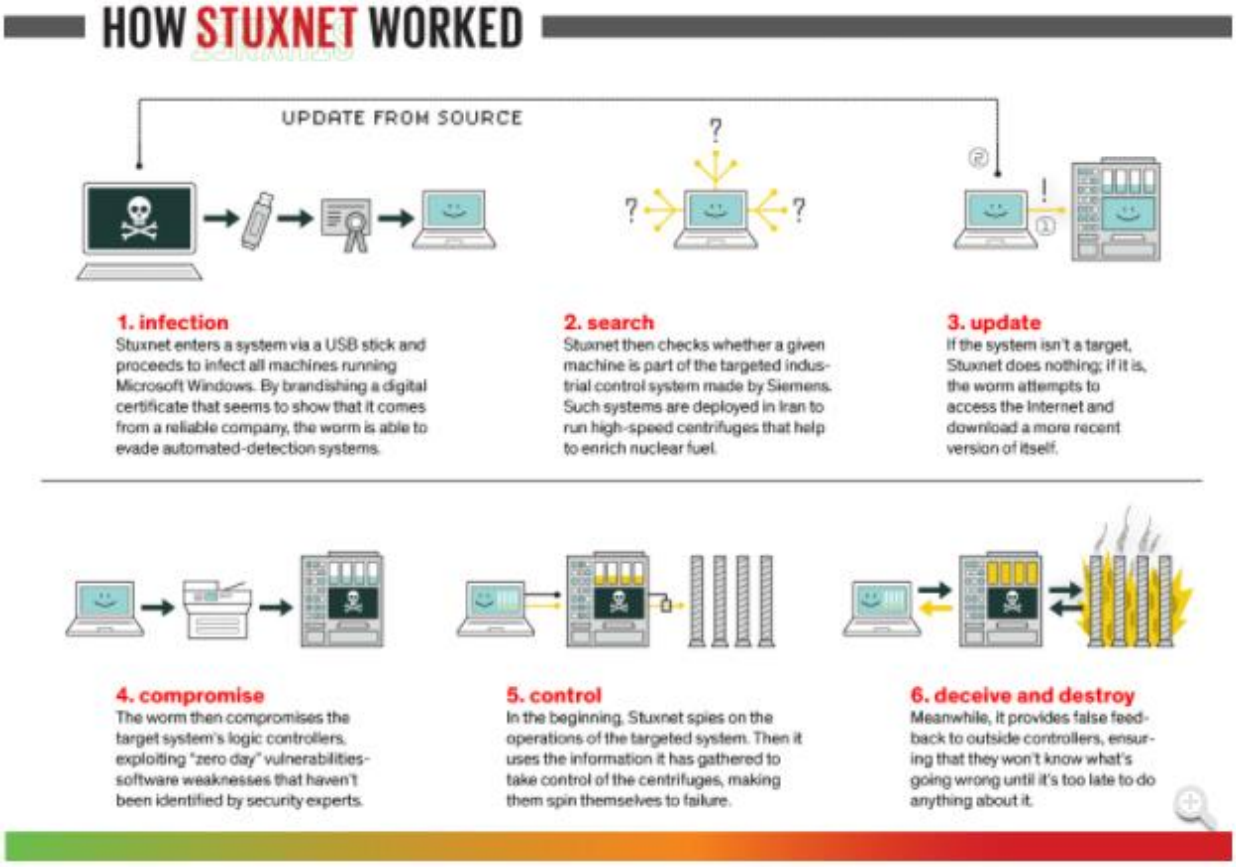
Cybersecurity currently is becoming paramount to any defense system, and both foreign government and nefarious individuals are using cyberattacks to hinder both government and business systems. What are the tactics these individuals or nations use, and why are they doing this? In this paper, we look at how foreign powers have in the past and are currently utilizing offensive cybersecurity tactics to achieve their goals. We will also examine the fallout from the US government's trust in untested cybersecurity software and look at just how undefended our own public infrastructure is at the state and federal level.

Introduction

The advent of the internet and digital technology changed the world, and it is hard to think of something today that does not have some form of a computer in it. Because of technology's omnipresence, it seems only a matter of time before someone weaponized this environment or utilized it to achieve their means dangerously. We will look at how cyberattacks were first accomplished, and how the United States has failed to prepare for this new type of warfare.

Section 1: The First State Sponsored Cyber Attack.

One of the first examples of a foreign government weaponizing the digital world is the Stuxnet virus that inhibited Iran's ability to enrich uranium. Previously malicious cyber-attacks had been low in complexity and damage resulting in minor and aesthetic effects.[1] This all changed in 2010 when centrifuges in Iran's nuclear facilities started breaking at a suspicious rate, causing them to halt operations. According to sources, Stuxnet was an unprecedently masterful and malicious piece of code that attacked in three phases which target machines running the Windows OS, then sought Siemen's Step7 software, and then compromised logical controllers.[1] This virus caused the machines to operate well outside of their designed parameters, causing them to break. This virus was built and designed by foreign governments with the clear intention of destroying Iran's centrifuges and delaying their ability to enrich its uranium. It has long been believed that this virus was designed and built by the United States and Israeli governments to impede Iran's nuclear weapons program. [1] By carrying out this attack, the governments that created this virus introduced the world to a new kind of warfare that eventually set the stage for the modern-day cybersecurity threats being conducted by all major countries.



Section 1.2 North Korea utilizing Cyber Attack to fund ICBM Research.

Today foreign governments such as North Korea are following in the footstep of the Stuxnet virus and are utilizing cyber theft to achieve their goal of acquiring nuclear weapons. The United States government as well as the United Nations have attempted to thwart the North Korean nuclear weapons program with harsh sanctions. In 2019 the United Nations stated that North Korea had generated an estimated 2 billion for its weapons of mass destruction program using widespread and increasingly sophisticated cyberattacks to steal from banks and cryptocurrency exchanges. [2] This immense amount of money that was acquired through state-sponsored cyber-attacks was used to nullify the effects of the sanctions imposed on the country and to achieve their goals of developing weapons of mass destruction. These attacks have proven incredibly ineffective since it is apparent that North Korea has successfully continued its nuclear weapons program despite the sanctions imposed by the United Nations. The extent of these cyber-attacks grew beyond private institutions to include foreign governments. It is said that between 2019 and 2020 that North Korean hackers had stolen virtual assets worth 316.4 million dollars to pay for the nuclear weapons program from an unspecified country. [3] This is important to note because the regime is using cyber-attacks to mitigate the effects of these sanctions as well as expand its target list to include countries that are inadequately defended for such sophisticated cyber warfare tactics. These kinds of actions change the balance of power in some respects because if the sanctions do not affect North Korea's ability to procure and produce nuclear

weapons then what chance do the sanctions have at stopping them at all. This is the unmitigated power that the new front of cyber warfare has brought to the Geopolitical power scale.

Sections 2.1 Shortcomings of Contemporary Cyber Defense Technology

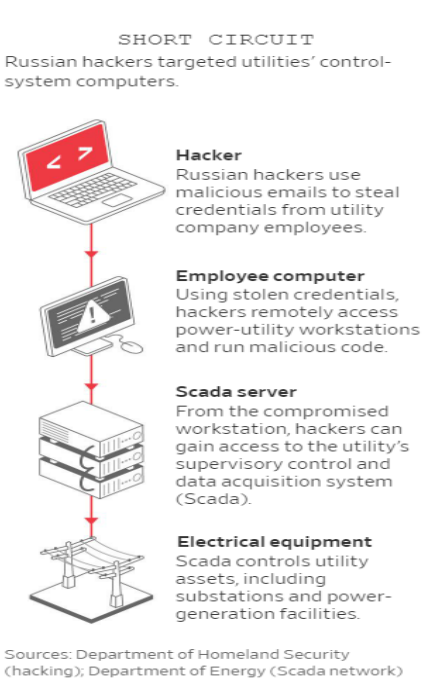
Many cybersecurity companies that sell software to defend against cyber threats have instead themselves become a trojan horse into company and government systems. The most recent example of this is the SolarWinds hack, in which it is believed that Russian hackers breached SolarWinds systems and compromised up to 18,000 companies' systems that went undetected for close to a year. [4] This kind of breach is the very thing software like SolarWinds is meant to protect against but instead it categorically failed to defend many of its clients. This is significant because vendors like SolarWinds are usually entrusted to setup their client's software, giving them broad access to their clients' networks. [4] When the servers of SolarWinds were compromised it gave the Russian hackers unprecedented access into private and government systems. This allowed them to avoid tripping alarms of the detection tools used by government agencies to catch known malware and other suspicious activity. [4]. It is hard to hear that since just one line of defense was compromised malicious activity went undetected, which points to a lack of defensive redundancy in this cyber defense technology. Another shortcoming of the software is that once the Hackers are in the system it is almost impossible to get them out. The fact that a foreign intelligence agency was able to do this kind of damage, even with implemented cyber defense technology, shows that we often rely heavily on cybersecurity software that has many shortcomings. The need for a cybersecurity software solution that can be relied on to contain enough redundancy to defend itself is vital, and until such a solution is achieved many companies and countries will be at the mercy of cyber attackers.

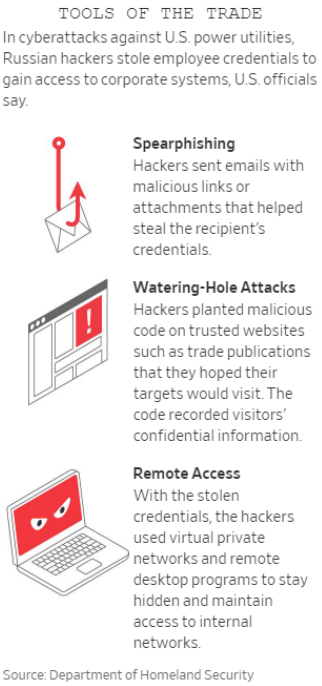
Section 2.2 The Fallout for the United States Government

The United States Federal government used untested cybersecurity software to thwart incursions into its systems which categorically failed to defend its companies and institutions. Despite the United States spending billions of dollars to defend and against these attacks while using platforms like SolarWinds they failed catastrophically to prevent and defend from this attack.[4] The inability to mitigate the damage from these attacks also shows how unprepared the United States is when it comes to cyber defense. Since it will take years until we can determine the extent of these attacks [4], it is rather difficult to tell how unprepared the government is to deal with incursions such as these. It is already clear by how long it is taking to even learn the extent of the damage and by how long foreign agencies had access to the systems it seems that we are insufficiently prepared to defend against such attacks. Although it is important to know that we cannot stop every attack but knowing that means we must be prepared to mitigate the damage of these attacks which is another deficiency in the US cyber defense. Some security experts state that ridding government computers of S.V.R., which is the Russian foreign intelligence agency, may be futile and the only way forward may be to shut systems down and start anew.[4] If we must rebuild our systems to guarantee they are clean after every attack then we will always be playing catch up with our adversaries. This reactionist strategy does not play out well for the US government or any government when it comes to offsetting the damage from cyber-attacks. In order to avoid such attacks in the future the United States government will need to change its strategy to defend itself as well as come up with a new way to mitigate the damage after the fact if we want to stand any chance of securing our digital environment.

Section 2.3 The Fallout for US state governments

As unprepared as the federal government is some states are at a much more significant risk of a cyber incursion. It has become increasingly apparent that public utilities such as water and power have become the target of hackers. Recently in Florida, a hacker gained access to a water treatment plant and tried to change the chlorine levels to toxic levels that put thousands at risk. Federal investigators revealed that an outdated version of Windows and a weak cybersecurity network allowed hackers to access the Florida water treatment plant's computer system and momentarily tamper with the water supply. [5] This situation was preventable because they were running an older unsupported version of Windows, it is directly because the state chose not to update their software that they left themselves open to attack. If this went unnoticed potentially thousands of people could have become sick or at the very least a large amount of water, a precious resource, could have been squandered. This shows how unprepared and unequipped some states are to deal with these kinds of high-level threats. Another public utility that is vulnerable and has been exploited by hackers is the US power grid. Russian hackers in 2018 used malicious emails to steal employee credentials, hack remotely access power utility workstations, and gained access to utility controls. [6] One place where this attack occurred was in Washington state where commercial contractors were subcontracted to maintain the power grid. It took the FBI two years to realize that the grid was being infiltrated by Russian state-sponsored hackers and learn what they were doing. Still to this day industry experts say Russian government hackers likely remain inside some systems undetected and waiting for further orders.[6] Since the FBI had to get involved this demonstrates that states are unprepared and incapable to deal with these kinds of attacks. Until they can, many public utilities will remain vulnerable and open to cyber-attacks that leave the population who relies on these utilities at great risk.





Conclusion

In this paper we looked at how foreign powers have and are currently utilizing offensive cyber security tactics to achieve their goals. While also examining the fallout from the US government trust in untested cyber security software and provided examples of how undefended our own public infrastructure is at the state and federal level. Since the first state sponsored act of cyber warfare with Stuxnet the cyber battle space has drastically changed. North Korea used cyber-attacks to steal billions of dollars through to circumvent sanctions and fund its ICBM program leaving opponents powerless to stop them. Today the tables have turned on the United States who is still unprepared to counter offensive cyber security tactics and has left both federal and state institutions vulnerable.

References:

[1] D. Kusher, "The Real Story of Stuxnet," Spectrum IEEE, 23 Feb 2013. [Online]. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[2] M. Nichols, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report," Reuters, August 2019. [Online]. Available: https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

[3] R. R. &. J. Berlinger, "CNN.com," Feb 2021. [Online]. Available: https://www.cnn.com/2021/02/08/asia/north-korea-united-nations-report-intl-hnk/index.html.

[4] N. P. a. J. E. B. David E. Sanger, "As Understanding of Russian Hacking Grows, So Does Alarm," The New York Times, 2 1 2021. [Online]. Available: https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

[5] J. M. a. Pereira, "Outdated computer system exploited in Florida water treatment plant hack," abc news, 11 2 2021. [Online]. Available: https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550.

[6] R. S. a. R. Barry, "America’s Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," The Wall Street Journal, 10 Jan 2019. [Online]. Available: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112.