Ingalls Threat Intelligence Report

How the 2020 Presidential Election Could be Hacked

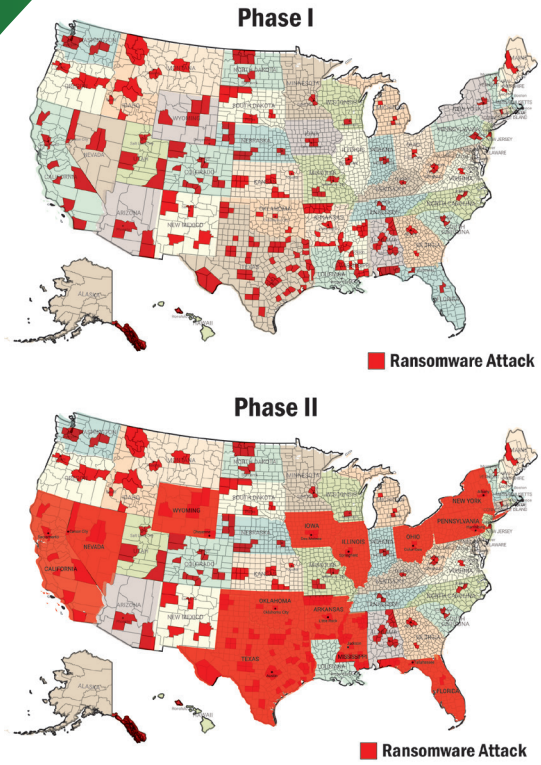

Figure 1: A two-phased attack scenario that disrupts local election authorities in the week prior to elections and state-level agencies on Election Day. Affected areas are for illustrative purposes only.

Introduction

Our Republic's representative democracy can be thought of as the consolidated will of the people, a form of civilization that peacefully transfers political power based on a popular vote.

This has led to what is arguably the greatest platform in human history for upward mobility, business activity, scientific progress, and quality of human life. There are issues with our election system that have yet to be solved, but it does work. The entire process is managed by decentralized armies of citizens, who assist anyone willing and eligible to vote. Local government agencies report state and Federal results up through a hierarchy that certifies the lower tier results and contributes to the national tally, eventually producing a consensus about who gets to run the Republic. It is a spectacle that is deserving of awe.

Technology has added some efficiency to the age-old processes of democracy; however, this increased efficiency has not come without risk. Much has been said about the need to improve cybersecurity for election equipment, and more funds are needed to provide modern infrastructure to local precincts. Now, there is a new specter looming

INGALLS INFORMATION SECURITY

over our next Presidential Election, one that threatens to create a situation that hasn't been seen in this country since Bush v. Gore: contested election results. There is evidence that the election could be disrupted by a coordinated attack on both local and state-level election authorities. This whitepaper explores the attack threat model, the mechanism of attacks, and how an attack could be mitigated.

A Two-Phased Cyber Attack Threat Model

The basic premise of this attack model is that a coordinated set of ransomware attacks could be staged: the first at the local level in the week preceding the election, followed by attacks on state-level election certification and publishing agencies on or immediately after election day. Both attacks would leverage pre-existing access by nation-state adversaries in targeted state and local government networks. Both attacks would use readily available, advanced malware that is undetected by the consumer-grade endpoint protection used in most local- and state-level agencies. In this model, local government agencies would likely be attacked through their IT support providers, known as Managed Service Providers (MSPs). State-level agencies would be attacked directly through phishing emails, which drop stealthy and persistent backdoors and ransomware to be deployed on command.

When attackers strike, ransomware would be used to effectively shut down local agencies in the critical run-up period to the election. Local agencies need their computers during this critical time to print out voter lists for polling places, coordinate volunteer and paid labor activity (which is usually done via email) and perform other essential job functions. In the immediate aftermath of the election, hackers would then execute a ransomware strike on state-level agencies, such as Secretaries of State or other Chief Election Officials, attacking their infrastructures and disrupting the ability of these agencies to publish the local election results and report them to Federal election officials. All of this would serve to impede, and possibly cripple, the usually smooth process that gives legitimacy to our election results. But how vulnerable are local and state election authorities, really?

IT Managed Service Providers (MSPs) & Remote Monitoring & Management (RMM)

Most local election officials and boards are not capable of staffing sufficient IT experts for in-house maintenance and system administration, and so the vast majority outsource their IT maintenance to small businesses called Managed Service Providers, or MSPs. These MSPs employ about 15 employees on average[1], and primarily support user help requests and maintenance efforts such as data backups, anti-virus updates, system patching, and firewall deployment. Unfortunately for MSPs, criminal groups targeted them heavily with ransomware in 2019, exacting a heavy toll[2].

MSPs use automation tools to scale their service delivery to as many customers as possible. These automation tools are referred to as Remote Monitoring and Management (RMM), and there are lots of Web-based versions for MSPs to choose from. Because they are Web-based, anyone with an internet connection can log into them using a username and password. This presents a serious security problem, because attackers who steal the login credentials for RMM tools can leverage those tools to deploy malware and ransomware to MSP clients and the MSP itself. At the time of this writing, none of the RMM tools we have reviewed require Multi-Factor Authentication (MFA) to be enabled. Multi-Factor Authentication

[1] "2019 Trends in North American Managed Services," Solarwinds, retrieved from https://www.solarwindsmsp.com/sites/solarwindsmsp/files/resources/2018_Trends_In_NAmerican_Managed_Services_Report.pdf

[2] "Managed service providers are ransomware hackers' new gold mine," Houston Chronicle, retrieved from https://www.houstonchronicle.com/techburger/article/Managed-service-providers-are-ransomware-hackers-14441149.php

requires users to provide more than just a username and password to log in (the most common form is a one-time code delivered via text message or a smartphone app), and makes account credentials much more difficult to use if stolen. MSPs using RMM without MFA are creating an existential threat to both themselves and their clients from attackers who are targeting them. Nation-state level attackers, who are well-funded and employ highly trained offensive cyber operators, have little difficulty stealing credentials and using RMM to execute cyberattacks.

Because election agency information about purchases and vendors is a matter of public record, it is easy for nation-state adversaries like Russia, China, or Iran to identify the MSP vendors for local election authorities. Threat actors could generate a list of all MSPs serving local election agencies, target them through phishing and other means, and gain access to any RMM tool consoles that don't have MFA. Once inside, they could lie in wait and deploy ransomware to all MSP customer computers using the RMM tool. If they planned this for the critical week prior to the national election, their attacks could easily result in a disruption of local-level agencies' ability to perform election duties.

State-Level Election Authorities

There are ample resources available on the web for adversaries to research and develop a target list of state-level election authorities. Targeted "spear phishing" attacks are almost guaranteed to succeed, given enough time. This is especially risky for state agencies operating workstations with legacy anti-virus programs that rely on signature-based detection of malware.

Once attackers have access to workstations on the State election authority network, they can harvest credentials, pivot to higher-privileged access accounts, and "live off the land," becoming invisible to most detection systems. After a latent period, and during or immediately following Election Day, these attackers could deploy ransomware across the State election agency networks, debilitating computers that will require days or weeks to recover.

Leveraging Attacks to Create Lack of Confidence in Election Results

By coordinating attacks on local and state election authorities and disrupting the IT infrastructure to a significant degree, we believe that attackers could create a crisis that leads to the general public, news media, and potentially the candidates themselves questioning the election results. No election machines would need to be tampered with, and no ballot boxes would need to be stuffed. All an attacker has to do to cast doubt on the legitimacy of the Presidential election is create a situation where local and state-level authorities were unable to do their sworn duties in a timely manner.

Irregularities Leading to Disputed Election Results

Sometimes election results contain data anomalies and voting irregularities that at first glance look suspicious but turn out to be statistical flukes. Sometimes these anomalies rise to a level of suspicion that draws the attention of press coverage[3]. In the scenario we have presented, where both local and state level election authorities are impacted by cyberattacks leveraging ransomware, any irregularity such as an undervote might be viewed in an even more suspicious light, making it easier for candidates, parties, and the public to reject the legitimacy of the results. They will almost certainly be used as political fodder for our highly polarized national news media and political parties.

[3]"Georgia voting irregularities raise more troubling questions about the state's elections," Politico.com, retrieved from https://www.politico.com/story/2019/02/12/georgia-voting-states-elections-1162134

Conclusion

It is undeniable that hackers seek to disrupt our elections. With the 2020 Elections right around the corner, officials must be proactive in guarding the systems used in elections. In order to ensure the voting public's confidence in the 2020 national election, these cyber defense tools and techniques must be in place long before Election Day:

- Advanced Endpoint Protection
- Threat Detection (Network and Endpoint)
- Multi-Factor Authentication for remote login credentials
- Incident Response Planning
- Log aggregation, analysis and review

Resources on election security can be found on the Department of Homeland Security, Election Resource Library. Protecting the democratic process and infrastructure is the most important responsibility we have as a Republic. Prevention is possible and absolutely essential, lest we find ourselves confronted with an existential crisis stemming from a contested election result. For more information about Ingalls Information Security, please visit our website at iinfosec.com.

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452