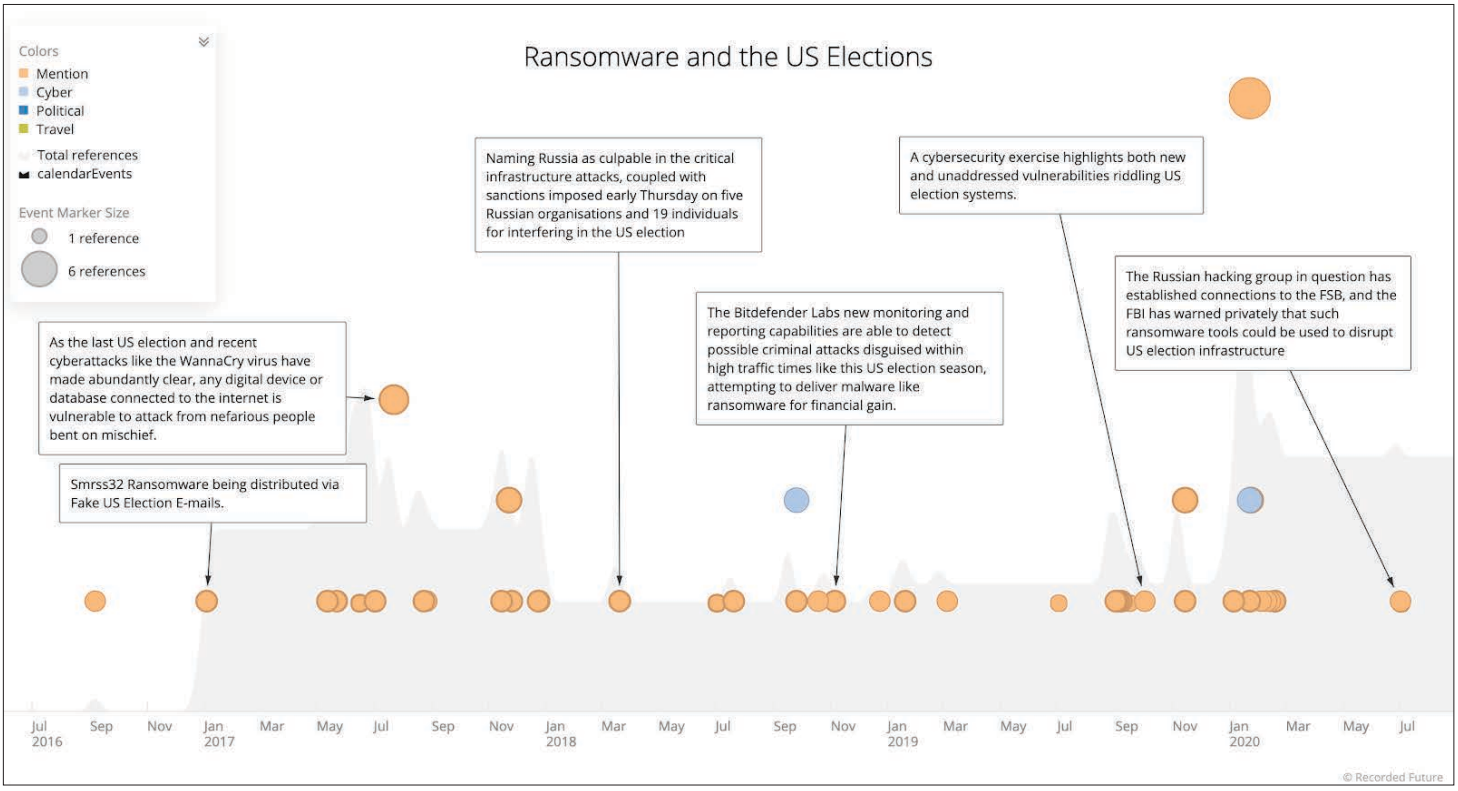
Pulse Report: Analyzing the Threat of Ransomware Attacks Against US Elections

Note: Prior to this report being publicly released, Recorded Future sent a copy of the report to all relevant state agencies, as well as CISA, for review. Many thanks go out to election experts at the local, state, and federal level who were willing to offer candid feedback on early drafts of this report, and a special thanks to Ryan Macias, SME — Election Technology & Security, for his comprehensive feedback.

The threat of a ransomware attack against elections in the United States has been a growing concern within the government and the private sector. We already know that threat actors managed to infiltrate the networks of election offices in multiple states, and according to a Senate Intelligence Report, those same adversaries were targeting all 50 states. In addition, it was reported earlier this year that the Palm Beach County Supervisor of Elections Office was hit with a ransomware attack in September of 2016, which was not reported to the FBI or Homeland Security. According to reports released under FOIA request by Recorded Future the Cybersecurity and Infrastructure Security Agency (CISA) has issued warnings that ransomware actors are planning to do the same again.

However, there is a big difference between gaining access to the networks of elections offices and actively disrupting the election. In either case, ransomware affords threat actors a low-cost, high-reward intrusion vector. The goal of this report is to take a realistic look at the different ransomware threats to the U.S. elections and offer suggestions to protect against those threats.



Source: Recorded Future

It is important to note from the start that it is extremely unlikely that a ransomware attack, even one coordinated across multiple states, would be enough to fully disrupt the 2020 election. But, depending on the state or states that were hit, and the timing of the attacks, a ransomware attack could still cause major disruption. And, of course, a single adversary does not necessarily need to coordinate an attack across multiple states. There may be dozens of threat actors targeting election infrastructure for the purpose of launching ransomware attacks. The timing of these attacks will undoubtedly be similar, designed to maximize damage by pursuing one of two goals: disrupting the election or generating income (it is possible that one actor could have both goals in mind).

In addition, there is concern among election officials who spoke to Recorded Future that a ransomware attack could be used as part of a disinformation campaign to cast doubt on an election. For instance, a county is hit with ransomware and several systems are locked and unavailable. This has an indirect impact on elections because the election team uses the mail server on the county domain. However, the critical assets (i.e., voter registration databases) are segmented and not affected. A disinformation campaign is then organized touting the "election system has been hit with ransomware."

Even if an attack is not used as part of a disinformation campaign, many election officials Recorded Future spoke to are concerned that a successful attack could lead to what they perceive as the biggest threat to this election: A breakdown in the perception of the validity of the election results. A successful attack, whether it is ransomware or otherwise, could further undermine confidence in an election that just 45 percent of Americans are confident will be counted accurately. Ransomware attacks are a low technical barrier of entry to this type of disruption.

Threat Scenarios

There are three ransomware attack scenarios that this report will investigate:

1. Ransomware attacks against voter registration databases
2. Ransomware attacks against voting results databases
3. Attacks against poll books

Current attack trends reveal that the threat of ransomware is very realistic. Although some of these scenarios are more likely than others, they all have the potential to disrupt the election or election infrastructure.

This report does not examine the differences between nation state attackers and cybercriminals. While each group's motivations may be different (though, that is not always the case), in terms of skill, there is little difference between nation state actors and the more advanced ransomware groups. The methods of gaining access and moving around the network before deploying ransomware tend to be similar.

One notable exception to these similarities is that nation state actors often use wipers, rather than ransomware - even when they do encrypt the files. Whether it is Russia deploying NotPetya, North Korea with the WannaCry attack and use of VHD ransomware, or Iran's use of Shamoon, nation state actors either delete critical files or they encrypt files without any hope of the victim receiving a decryption key.

In particular, the more advanced ransomware actors have become sophisticated at understanding targets in the United States (and the rest of the world) and time their attacks to be as disruptive as possible. For example, in July and August of 2019, Recorded Future noted 17 ransomware attacks against school districts across the United States. These attacks were timed to coincide with the start of the school year, forcing schools to delay opening or pay the ransomware to avoid delaying the start of the school year. Another example of ransomware threat actors having a sophisticated understanding of their targets is how rapidly threat actors, including ransomware groups, were able to capitalize on real-world COVID-19 concerns to launch a wide range of successful COVID-19 themed phishing attacks. Quickly jumping from themes like "sharing information," to "tracking cases," and to "helping victims get state relief funds and loans." In June, many of those actors switched to phishing campaigns using Black Lives Matter lures, continuing the trend of using latest news for lures. Many of these campaigns were very successful targeting both consumers and organizations.

The most sophisticated ransomware actors, such as Ryuk, Maze, Sodinikibi, and WastedLocker, have spent weeks and even months inside an organization, learning the network, waiting to get the accesses they need to effectively move around and steal large amounts of data before deploying the ransomware. The combination of sophisticated attacks and staff layoffs at many state and local governments due to budgetary shortfalls creates the very real possibility of a successful ransomware attack on election infrastructure in November.

Ransomware Attacks Against Voter Registration Databases

An attack on voter registration databases (VRDBs) is most likely to generate the most attention and cast public doubt on the integrity of the election. A well-timed encryption of a VRDB (and the system software) could prevent voters from voting, or cast doubt on voting results and throw the entire election into chaos. These attacks likely won't occur on the day of the election, as the VRDB is not widely used that day. Instead there are certain dates that are critical to the election where a well-timed ransomware attack could cause maximum damage (some of these dates vary by state):

- National Voter Registration Day (September 22nd, in 2020)
- The first day of early voting
- A day or two prior to pollbooks being pushed out
- With the expected rise of mail-in voting this election, a ransomware attack on the VRDB 45-60 days before the election could disrupt the ability of a state to disseminate mail-in ballots
- An attack the day after the election could prevent polling officials from verifying mail-in ballots

In addition, because many ransomware actors have added extortion to their toolkit, ransomware attacks against voter registration databases now pose a dual threat: election disruption and the potential publication of millions of sensitive voting records on an extortion site or sold on the dark web.

There are a number of challenges involved in securing voter registration databases. First, the United States does not have a single voter registration database. Each of the 50 states is responsible for maintaining its own voter registration, as is the District of Columbia, American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands, for a total of 56 separate voter registration databases. Adding to the complexity, there are three types of VRDBs: top-down, bottom-up, and hybrid. The Election Assistance Commission (EAC) maintains a list of the states and the type of VRDB each uses.

A top-down VRDB is a centralized VRDB that distributes information to local counties or precincts as needed. This means the authoritative VRDB is maintained by the state and when you register to vote all of your information resides in the database. According to the 2018 Election Administration and Voting Survey, 72.7% of states use a top-down VRDB system. One concern with a top-down voter registration system is that each registry point is a potential vector for a ransomware attack.

On the other hand, 14.5% of states use a bottom-up voter registration system, in which local jurisdictions maintain their own voter registration databases, which sync with the state voter registration database. This means there are hundreds of potential VRDBs that could be targeted by ransomware attackers (there are 3,141 counties, or county-like areas in the United States, but not all counties maintain their own VRDB). Despite many counties being responsible for the security of their VRDBs, there is a lot of disparity in security funding, with many counties relying on IT staff to also manage the security of the voting infrastructure. Even when there is help, it can be inadequate. In 2018, Arizona (which maintains a hybrid system) received a $7.4 million grant from the Help America Vote Act (HAVA) for election security. Of that $7.4 million $2.4 million was distributed to the counties. The two largest counties, Maricopa and Pima, which account for 75% of registered voters in Arizona only received $352,000 and $251,000 respectively, despite each county having to maintain and manage its own voting infrastructure.

On top of logistical and financial challenges, there are also political challenges to securing VRDBs. Many of the election officials Recorded Future talked to for this report complained of jurisdictional challenges. There is often confusion about who is responsible for securing different parts of the VRDB and competing teams at the local and state level vying for control.

Securing Voter Registration Databases

States do not like to reveal the specifics around the technology used to store their VRDBs or the systems used to connect into those databases. Fortunately, thanks to the Help America Vote Act (HAVA) Recorded Future was able to gain some insight into what VRDBs, and their surrounding infrastructure look like.

After the passage of HAVA, there was a rush to update VRDBs from 2003 to 2005, and security was not a primary concern for this first generation of post-HAVA EMS. Many states have since replaced those systems, but there are a number of states still making updates to VRDBs built in the 2003-2005 timeframe, while acknowledging that the security of these systems is severely lacking.

In an effort to improve security, the EAC, under HAVA, created the Election Security Fund. This fund provided $380 million in grants specifically for election security in 2018, and additional $425 million in grants were provided in 2020. Every state, plus the District of Columbia and the territories, took advantage of the available security funding, to different levels. Given procurement and implementation cycles, funding available in 2018 and 2020 is not enough time to build a whole new system.

But, even with the Election Security Fund, consistent baseline security standards were not established. Instead, only vague guidance was given that the funds were to "...improve the administration of elections for Federal office, including to enhance election technology and make election security improvements."

This leads to the current state of election security, which varies greatly from state to state. A review of grant requests and RFPs show that most VRDBs are running on standard commercial off the shelf (COTS) software and often mirror the infrastructure in place in the rest of the state's network. It makes sense that states are trying to maintain a holistic administrative and security view of their network and do not want to have radically different software in place.

It appears the majority of VRDBs are running on Oracle or Microsoft SQL databases and are often administered by traditional remote administration tools such as Remote Desktop Protocol (which Recorded Future found indications that at least seven EMS are using) and Citrix (which appears to be used by at least six VRDB). Microsoft's .NET and Sharepoint were also mentioned as being in use across multiple states' voting infrastructure. In addition, as recently as July of 2019 there were as many as 10,000 Windows 7 systems, currently unsupported by Microsoft, being used to administer voting systems, all of which are systems potentially vulnerable to ransomware attacks.

Some states have opted to build their own infrastructure from scratch, others have decided to use companies that have developed out-of-the-box VRDB, such as BPro TotalVote and Election Systems & Software (ES&S) PowerProfile. While a lot of attention has been given to the security of electronic voting systems, VRDB systems have been given very little scrutiny. Neither BPro nor ES&S have any vulnerabilities reported in the NIST National Vulnerability Database, which on the surface may seem like a good thing, but given the complexity of these systems it is doubtful that there have been no vulnerabilities directly in their systems or on the components that make up their VRDB. The lack of transparency in vulnerability reporting makes it difficult to evaluate their security posture. At Black Hat this year, ES&S announced a policy that would allow it to work with security researchers who find vulnerabilities in the company's network infrastructure and website. Obviously, this is not the same as having a policy that allows security researchers to inspect your VRDB, but it is a start.

In 2017, DHS designated election infrastructure as a critical infrastructure sub sector but, unlike other critical infrastructure, there are no security requirements for voting infrastructure hardware or software that states and local governments can use.

In fact, the Brennan Center for Justice at the New York University Law School has advocated that election software vendors should be required to report any vulnerabilities discovered. In testimony before the House of Representatives Lawrence Norden, Deputy Director of the Democracy Program stated that:

Note: One important step would be to mandate that vendors report any cybersecurity incident they discover to both the federal authorities as well as state and local customers. Reporting of cybersecurity incidents for election vendors may seem like a small step, but it will have a large impact on the overall security position of election officials around the country. Election vendors have stated that such requirements are unnecessary and burdensome and that they are somehow different from the vendors in other critical infrastructure sectors. This is simply not true. We know that the lack of transparency in vendor security is a significant vulnerability to election security.

Given that ransomware threat actors have become increasingly sophisticated, the relative lack of transparency in election systems may mean there are vulnerabilities exploitable by these actors and those responsible for securing VRDBs may not even know they exist.

Ransomware is a top concern for election officials in 2020. Both the Election Infrastructure ISAC (EI-ISAC) and CISA have released reports detailing the threat of ransomware to VRDBs and the EI-ISAC Weekly News Alert (labeled TLP:WHITE), which Recorded Future has viewed through FOIA requests, regularly discusses ransomware incidents and how they could impact election infrastructure. DHS' Election Infrastructure Sector-Specific Agency (SSA) has also warned about vulnerabilities specific to VRDB. One bulletin from the Election Infrastructure SSA dated June 19th and received through FOIA request (labeled TLP:WHITE) specifically called out CVE-2019-0604 (Microsoft SharePoint), CVE 2019-18935 (Telerik UI for ASP.NET), and CVE 2019-1978 (Citrix) as vulnerabilities that needed to be patched immediately.

Election Infrastructure GCC and SCC,

You may have seen reports of a cyber incident in Australia. While CISA has not confirmed any information, the publicly available information references several Common Vulnerabilities and Exposures (CVEs). These CVEs are related to Microsoft SharePoint, Citrix Application Delivery Controller, Citrix Gateway, and the Telerik UI. The Citrix vulnerability In particular has been prominent across several critical infrastructure sectors this year. Please take particular note of your organization's susceptibility to this vulnerability. CISA's guidance on these CVEs is available at the following links/attachments:

- CVE-2019-0604:
  - https://www.us-cert.gov/ncas/alerts/aa20-133a : A remote code execution vulnerability exists in Microsoft SharePoint
- CVE 2019-18935:
  - MS-ISAC Cybersecurity Advisory attached : A Vulnerability in Telerik UI for ASP.NET Could Allow for Arbitrary Code Execution
- CVE 2019-19781:
  - https://www.us-cert.gov/ncas/alerts/aa20-020a : Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP
  - https://www.us-cert.gov/ncas/alerts/aa20-031a : Detecting Citrix CVE-2019-19781

If you have questions about these CVEs please contact EISSA@cisa.dhs.gov.

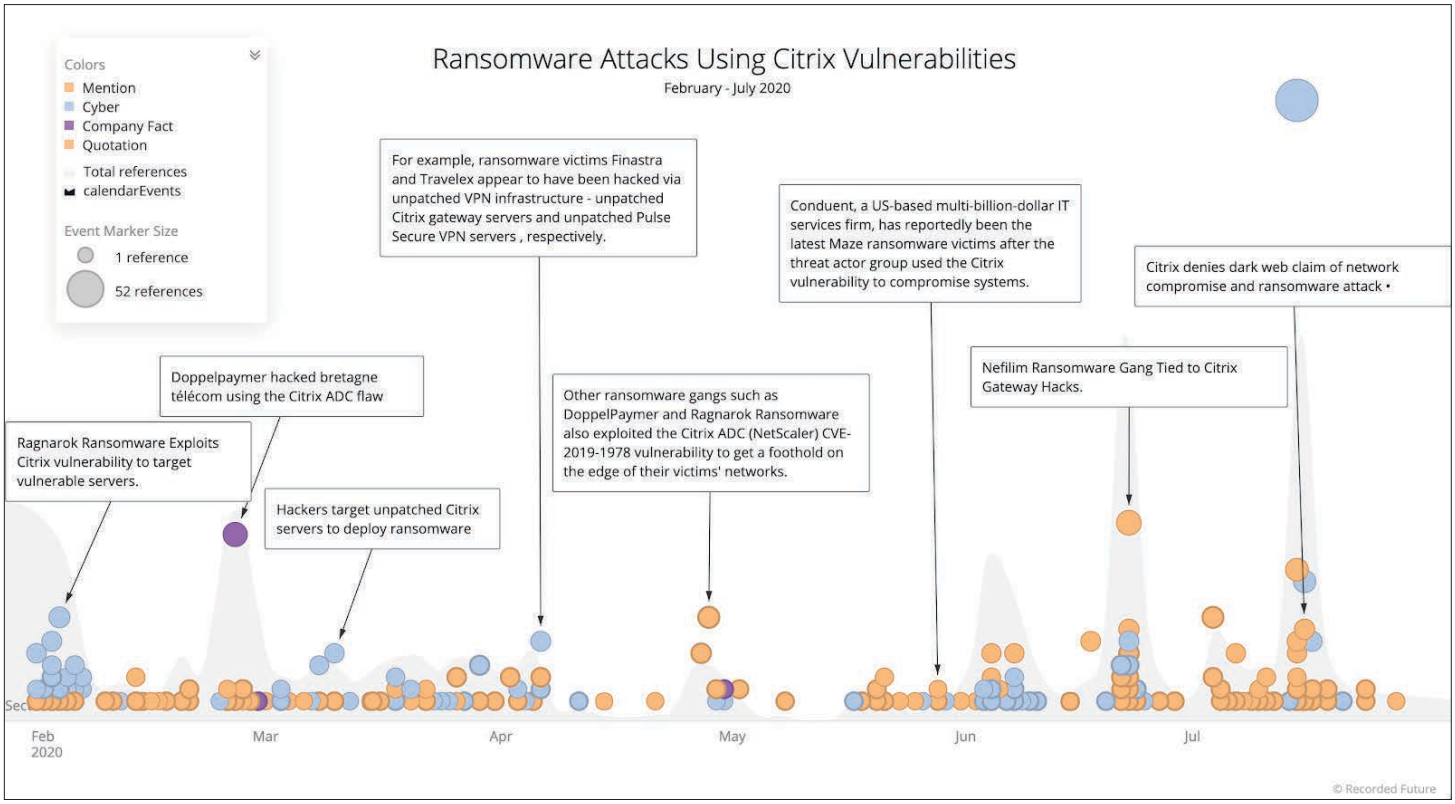
Respectfully,

EI SSA
EI SSA/ESI, National Risk Management Center
Cybersecurity and Infrastructure Security Agency
Email: EISSA@CISA.DHS.GOV

(Source: June 19, 2020 letter from The Election Infrastructure Sector Specific Agency (SSA) to Members (Retrieved via FOIA Request)

The incident referred to in this bulletin is the announcement from the Australian Prime Minister about a wide ranging, state-sponsored cyber attack targeting Australian government and infrastructure.

The worry is understandable: in the last six months ransomware attacks have repeatedly exploited Citrix systems. Citrix has become one of the most common exploit vectors for ransomware actors, and, as previously noted, many VRDB rely on Citrix to manage their infrastructure.

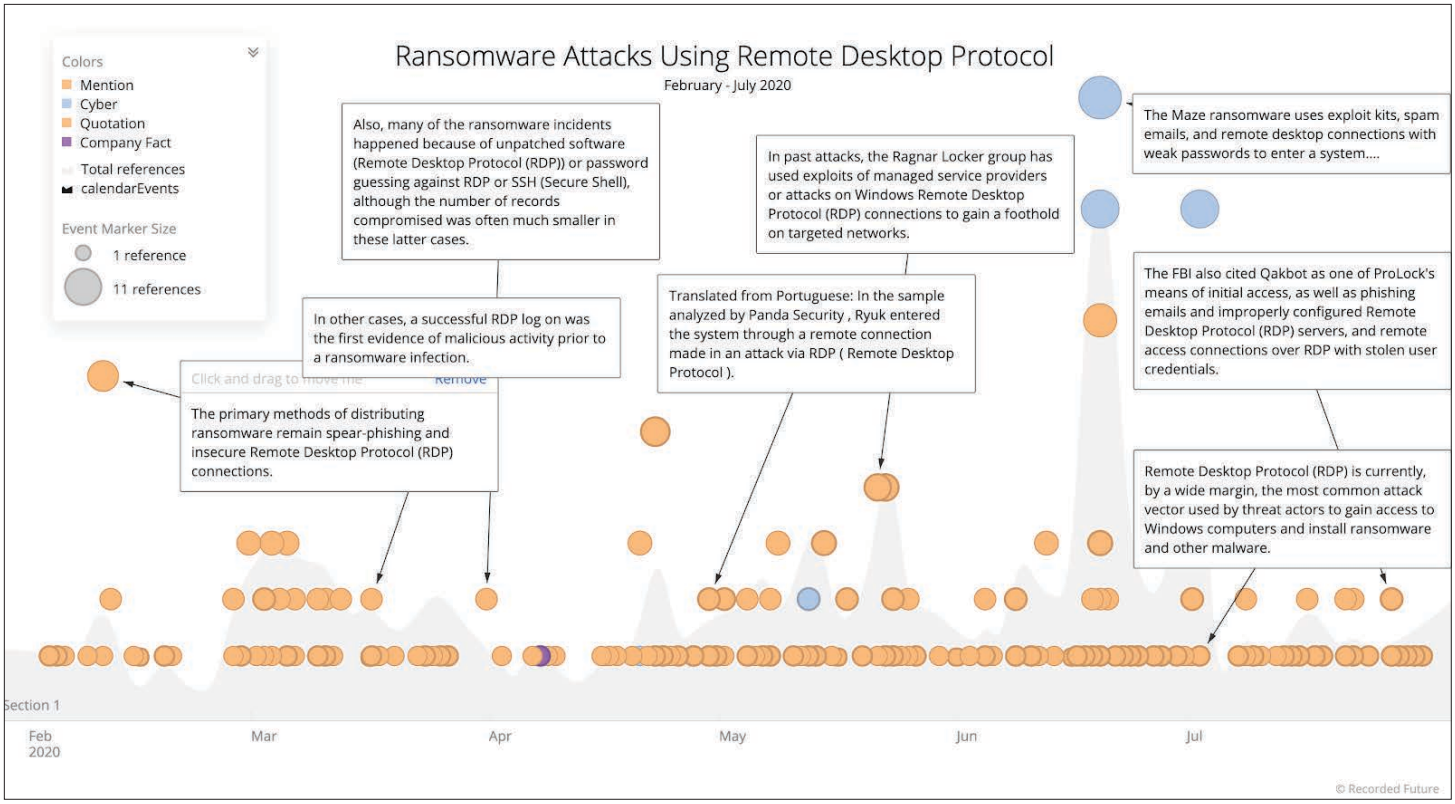


Source: Recorded Future

In addition to Citrix, Remote Desktop Protocol (RDP), which is commonly deployed in state networks, is often used to facilitate ransomware attacks. In fact, RDP often rivals phishing as an entry point for ransomware attacks.

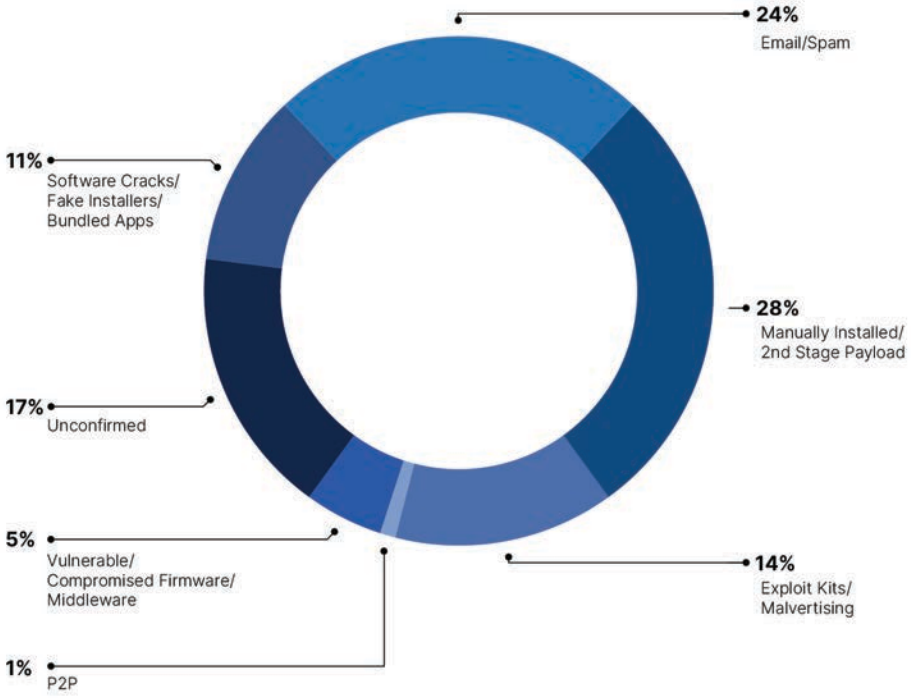
Both Citrix and RDP appear to be widely used to manage VRDB, which means that election infrastructure is potentially vulnerable to ransomware actors' preferred method of attacks. Recorded Future did not make any attempt to scan infrastructure for vulnerable systems.

Aside from normal management of VRDB using Citrix and RDP, many states, like all organizations, have expanded their remote workforce during the COVID-19 pandemic. This remote workforce is often using tools like RDP and Citrix to connect into state government systems. Initially, these remote workforces were intended to be a short-term fix, but many states have extended their remote workforce timelines indefinitely. This means that these short-term fixes have now become more or less permanent, and it is unknown whether reduced staff has had the opportunity to review the security protections in place for these "temporary" work from home solutions.



Source: Recorded Future

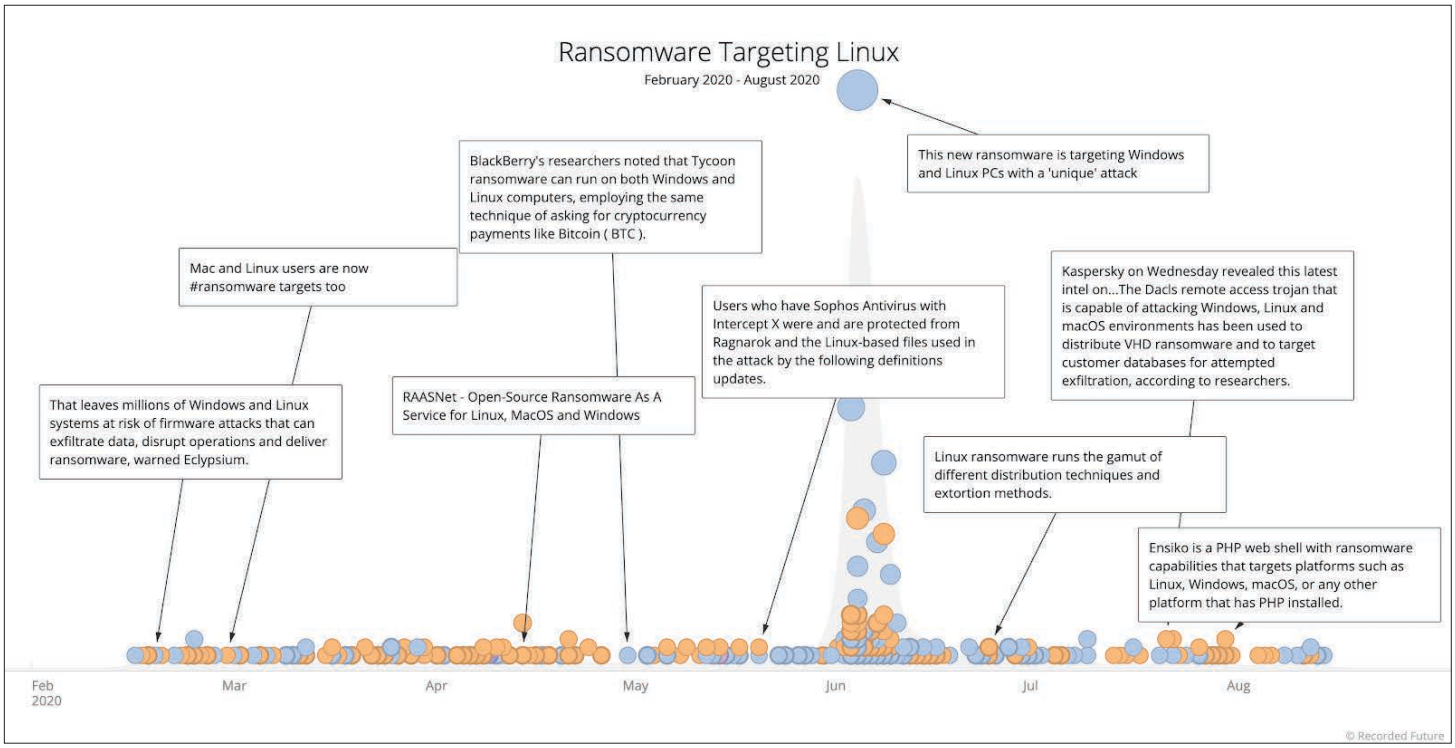
The concern around RDP and Citrix protections is that, according to reporting from F-Secure, Citrix, RDP, and other remote attack vectors accounted for more ransomware attacks than phishing campaigns in the second half of 2019. While phishing attacks accounted for 24% of ransomware attacks, remote exploitation and manual deployment of ransomware accounted for 28% of all attacks.



Source: F-Secure

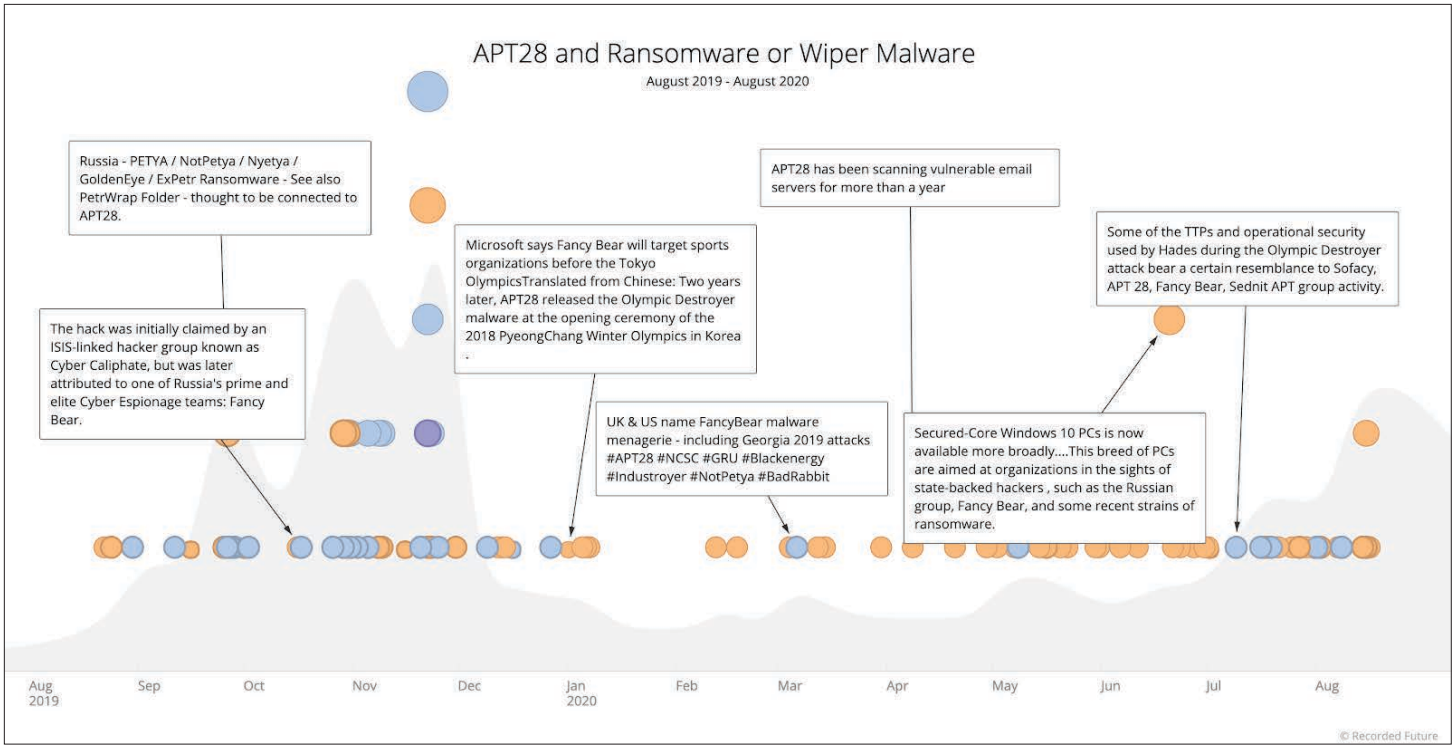
One concern specific to VRDBs is that many ransomware variants have trouble decrypting large file sizes. Given the size of VRDBs, even some of the tables stored as backup may be larger than a ransomware's decryptor can support. If a state is forced to pay the ransom, there is a real possibility that the decryptor will not work on the VRDB.

Things are not much better for states running their VRDBs on Linux. Ransomware attacks against Linux systems are on the rise with several high-profile attacks and a proliferation of ransomware variants targeting Linux over the last six months. Ransomware actors are increasingly interested in Linux systems and Linux vulnerabilities.



Source: Recorded Future

Unfortunately, it is not just cybercriminals. The NSA and FBI recently released a comprehensive report on the Drovorub malware [PDF] operated by APT28 (aka Fancy Bear), a nation-state group that targeted election infrastructure in 2016. APT28 has been linked to both ransomware and wiper capabilities in the past. There is no indication from the NSA and FBI report that APT28 has been targeting election infrastructure ahead of the 2020 election, but there is speculation that the release of the report was timed because of concerns around 2020 election interference.



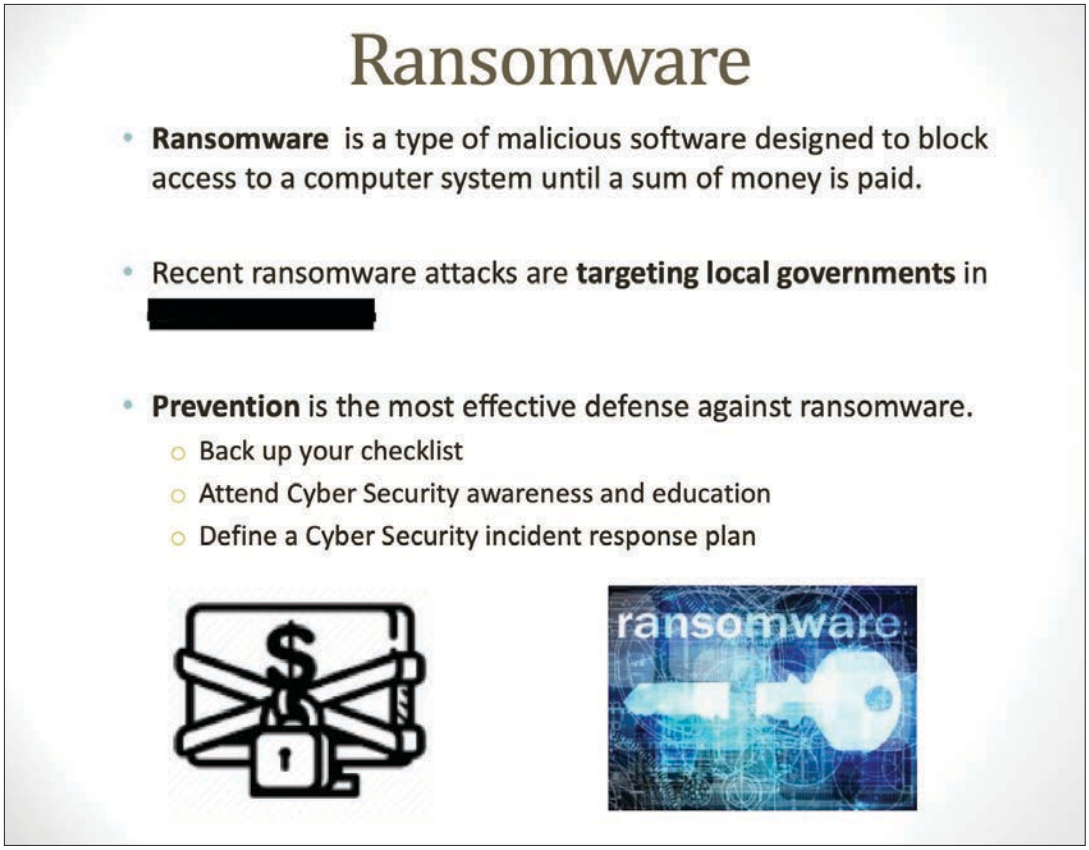
Source: Recorded Future

Training

While the threat of remote access ransomware attacks continues to grow, states remain focused on phishing attacks when it comes to ransomware campaigns. A review of several states' current internal ransomware training showed no mention of RDP or Citrix as an avenue of entry, instead the focus was entirely on phishing attacks. Sometimes offering potentially bad advice, such as using the Preview Pane in Microsoft Outlook to determine if an email is legitimate. There are several exploits that take advantage of the Preview Pane to deliver their payload, especially when that payload is embedded in a Microsoft Office document. Alternatively, the advice seemed to be geared toward protecting against ransomware attacks from four to five years ago.

Source: Example from a state (intentionally withheld) training

In addition to the lack of discussion around remote ransomware attacks there was no discussion on internal training about ransomware and the exfiltration of data combined with subsequent extortion demands to avoid making that data public. Extortion (sometimes referred to as double extortion in the case of ransomware) is a widely adopted tactic by ransomware actors and should be of great concern to those responsible for maintaining VRDBs, as voter registration data is incredibly sensitive and would command a high price on underground markets. In 2018, 35 million voter records from 19 states were found for sale for $42,200 in an underground forum.

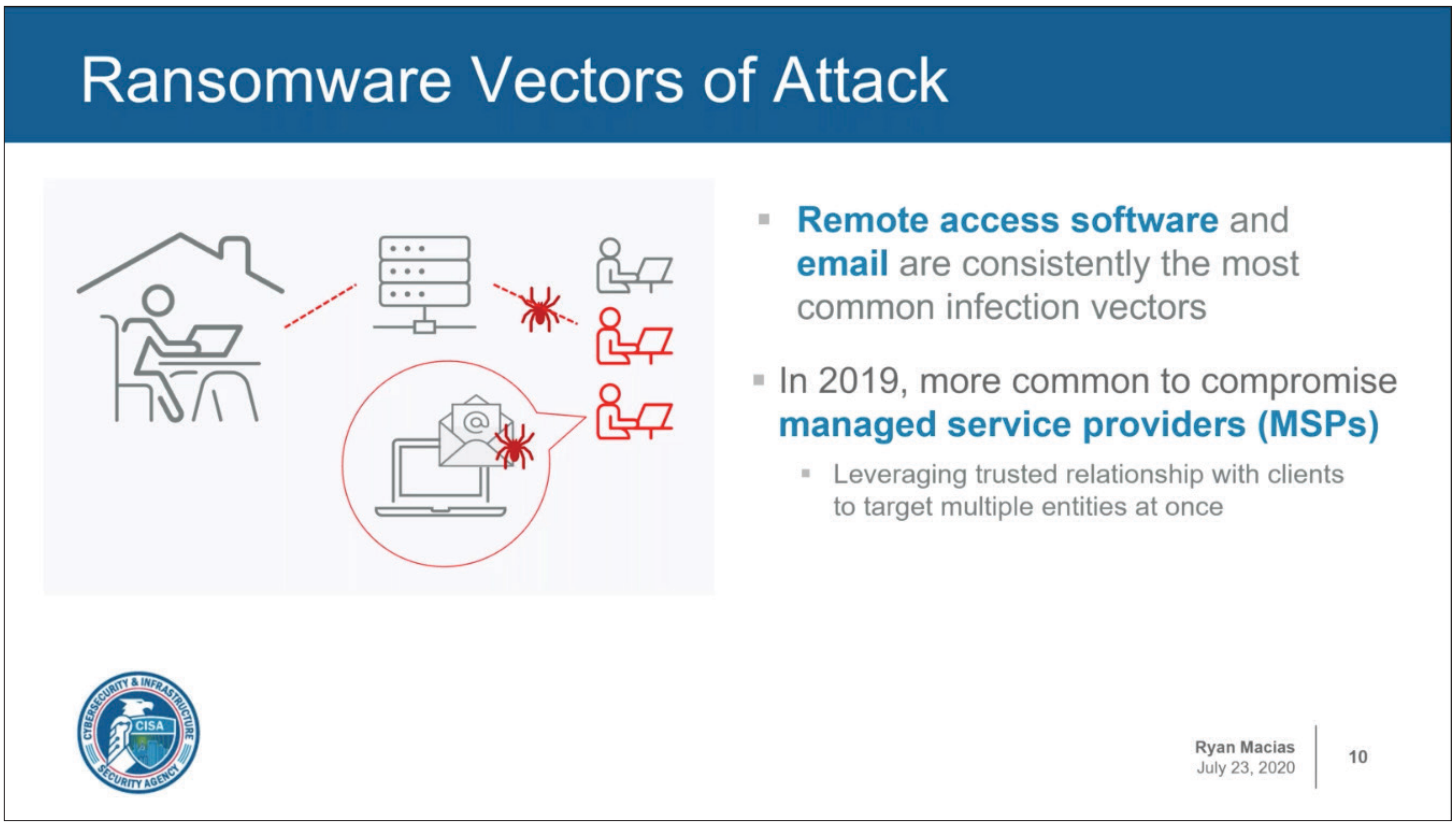


Source: Example from a state (intentionally withheld) training

If a ransomware actor were to exfiltrate a VRDB as part of a ransomware attack, even if the state or municipality did not pay the ransom, the threat of a multimillion dollar extortion would still loom over the state, or worse, having all voter records posted for sale. It is also conceivable that, given that the extortion tactic is still relatively new, a ransomware actor will promise to delete files after an extortion is paid but will opt to sell that sensitive data instead. Interestingly, none of the EI-ISAC Weekly News Alert bulletins reviewed under FOIA request mention extortion as a concern when it comes to ransomware.

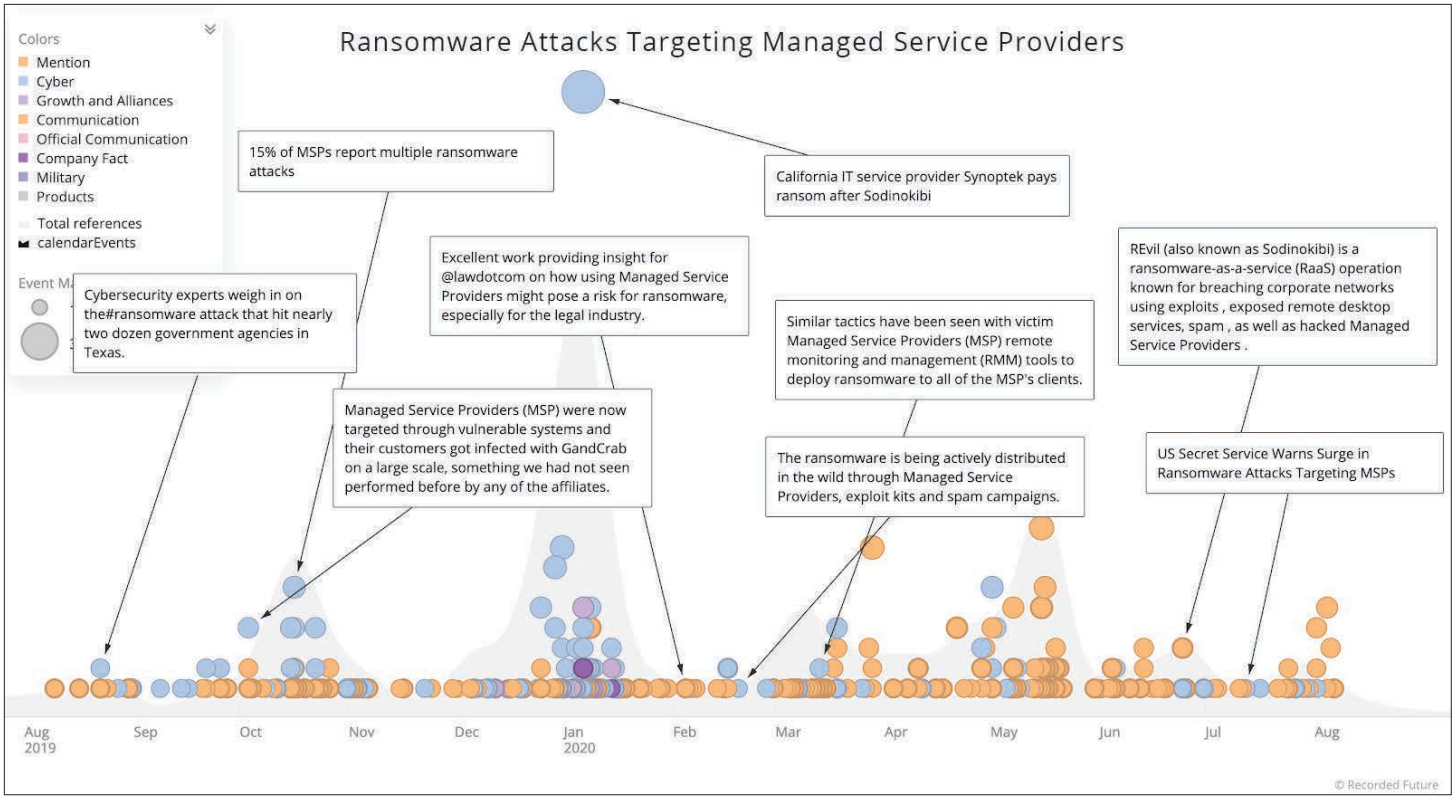
However, a training webinar sponsored by the National Association of Counties (NACo) Tech Xchange with speakers from CISA and EI-ISAC did mention extortion. It also highlighted the significance of remote attacks, as well as phishing campaigns for ransomware.

This is excellent training, indicating that CISA and the EI-ISAC are providing detailed and up-to-date training around the latest ransomware threats, but based on documents received through FOIA requests, it does not seem that information from the training is being widely distributed within the states.



Source: NACo Tech Xchange Webinar

Also mentioned in the training are ransomware attacks that originate through a managed service provider (MSP). In August 2019, 22 cities in Texas were hit with a ransomware attack that originated through a shared MSP. MSPs are increasingly being used as a launching ground for ransomware attacks, and MSPs are a growing target for ransomware actors. With state budgets cut and staff furloughed, many states are increasingly relying on MSPs to manage critical state infrastructure, including the voting infrastructure.

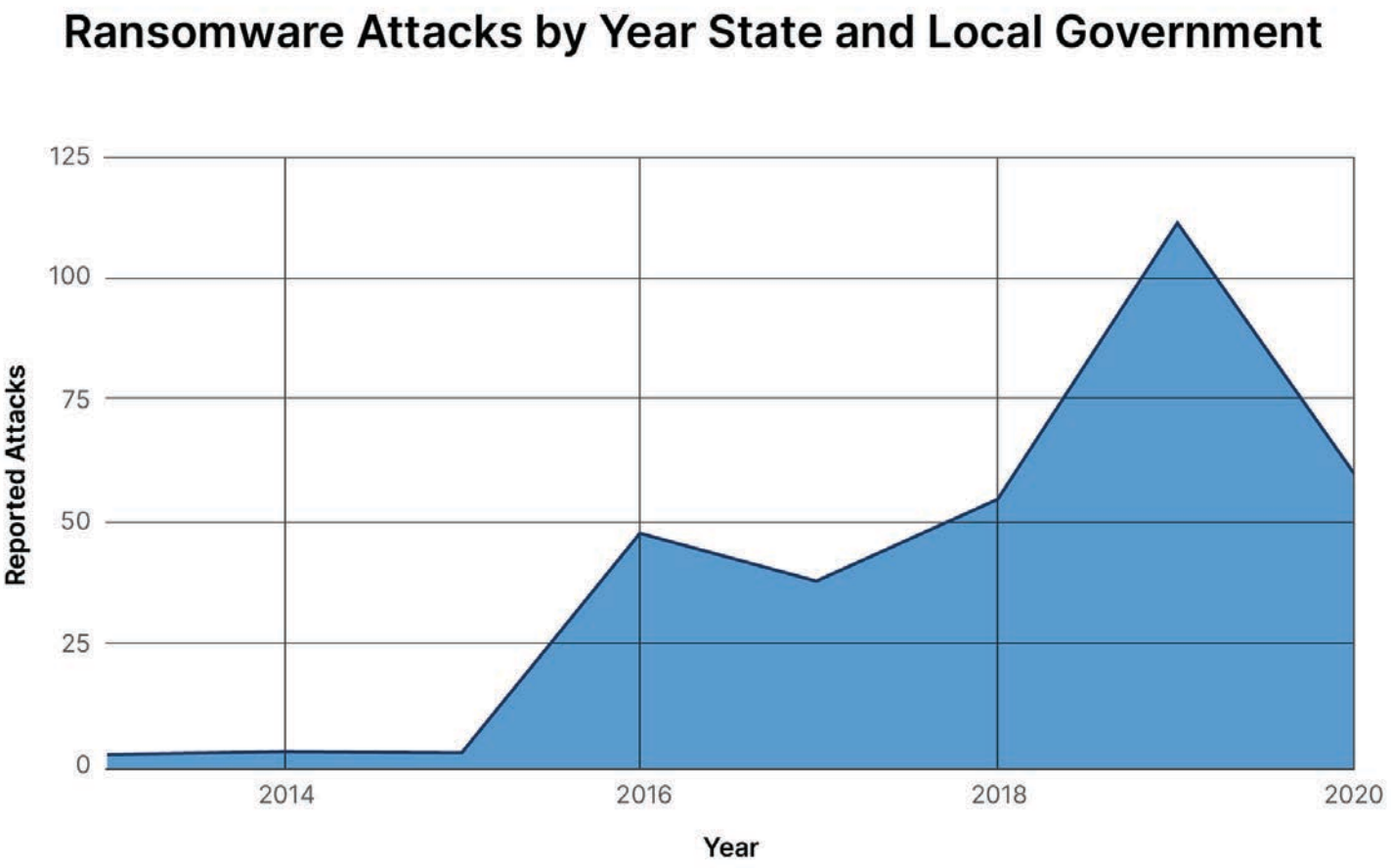


Source: Recorded Future

Ransomware Attack Scenarios

Based on what is publicly available, we know that ransomware actors are using attack techniques that state VRDB are potentially vulnerable to, and that states continue to be targeted by nation state actors who may deploy ransomware as well as cybercriminals who focus on ransomware attacks.

Recorded Future noted over 110 publicly reported ransomware attacks on state and local governments in 2019, and there were undoubtedly even more that were not publicly reported.

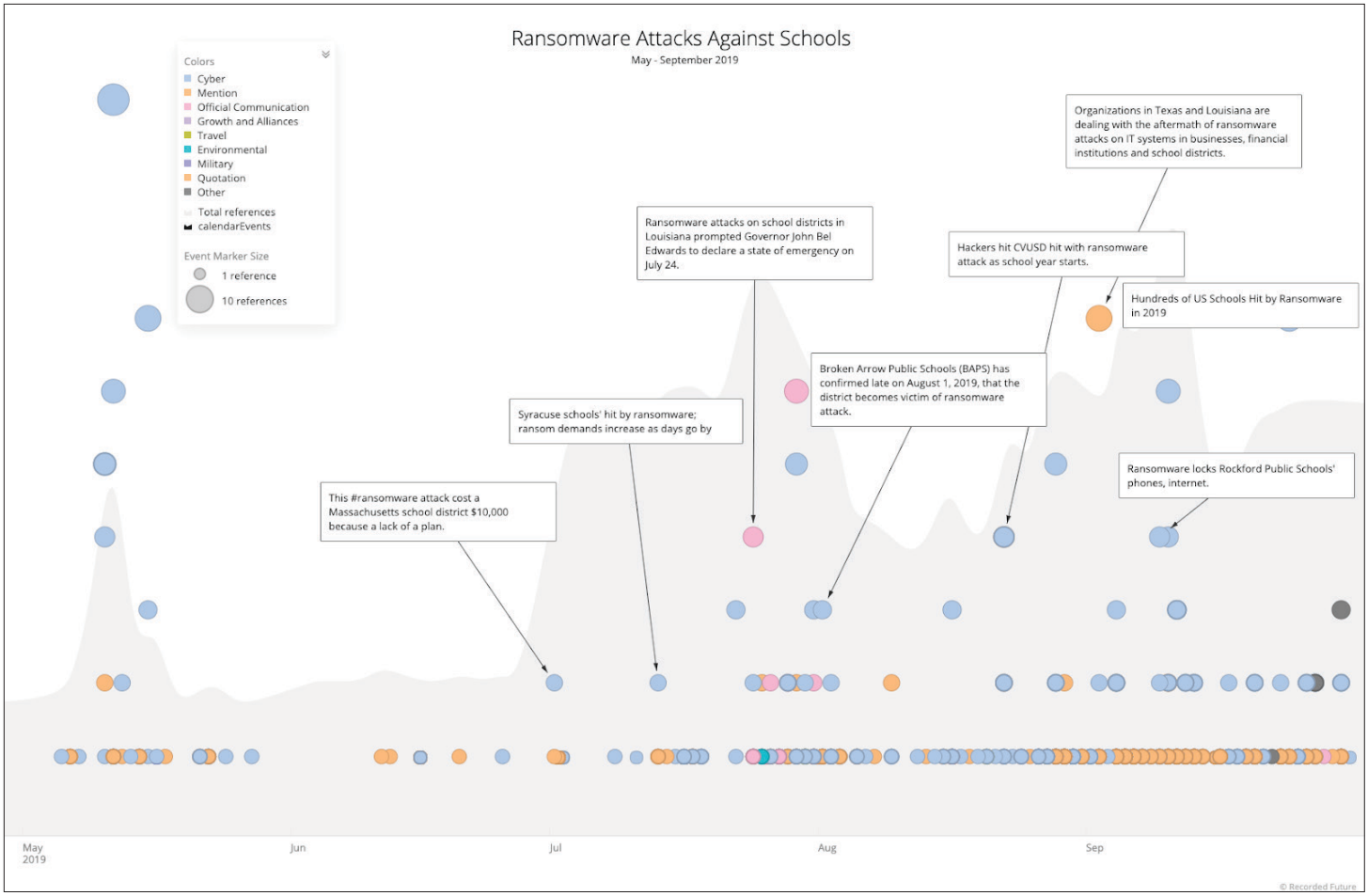


Source: Recorded Future

In 2020 there have already been 60 publicly reported ransomware attacks against state and local governments, and that includes a significant slowdown in reported attacks during the months of April and May because many local governments ceased operations due to the COVID-19 pandemic.

We know that ransomware actors are focused on state and local governments for a variety of reasons, but they are also getting more sophisticated in their attacks. Not just the scope of the attacks, but the timing of those attacks.

For example, in July through September of 2019, Recorded Future noted a significant uptick in ransomware attacks targeting schools. These attacks were timed to disrupt the start of school and force school systems to pay the ransom or delay the start of school, which happened in several cases.



Source: Recorded Future

Given the knowledge that ransomware actors acquire about their targets, it is possible that these actors are aware of critical election dates and are preparing to time their attacks to coincide with those dates.

In addition to state and local governments' network weaknesses that match the preferred method of attack for ransomware actors, a significant number of state and local government employees have leaked credentials available for sale on underground forums (colloquially known as the dark web).

Between May and July of 2020 Recorded Future noted 45,484 email addresses and passwords of state and local government employees were available for sale on underground forums. These included employees from all 50 states, and the District of Columbia. 28,818 of those credentials were leaked in July alone.

Given the prevalence of password reuse in organizations, this means that even fully patched RDP and Citrix servers being used to administer VRDB may be used by ransomware actors to gain access. Even if those credentials aren't used to gain initial access, they may be used to gain administrative privileges once the attackers are inside the network.

This leads to another point of concern: it may already be too late. Ransomware attacks on state and local governments are part of a new type of ransomware attack known as Big Game Hunting. From 2013 to 2017, most ransomware attacks were of the "smash and grab" variety. Similar to "knocking over a liquor store," the ransomware attacker gains access to the network and quickly infects whatever system is accessed, irrespective of the value of that system to the organization.

Big Game Hunting ransomware attacks are much slower and more methodical. Once the ransomware group has access they spend time learning the network, understanding which systems are important, where the backups are stored and which data to steal. This type of attack can take weeks or months. In the recent ransomware attack against Blackbaud, the attacker gained initial access February 7th and did not try to deploy the ransomware until May 20th - that is 3 1/2 months. In other words, by the time this report is released, ransomware actors may already have gained access to voter registration infrastructure and are plotting when to deploy the ransomware.

Both the EI-ISAC and CISA have unique sets of indicators that could be used by election security staff for threat hunting missions that could detect an attacker who slipped by the initial defenses. Because Big Game Hunting ransomware attacks are time consuming and manually intensive for the attacker, there are opportunities to hunt for indicators, such as command and control IP addresses, use of tools that allow attackers to move around the network and elevate privilege, and, of course, exfiltrating large amounts of data. This does present an opportunity for network defenders who work for state and local governments to detect and remove ransomware attackers before data is encrypted.

Because it is possible that ransomware attackers are already residing in election infrastructure networks, CISA and the EI-ISAC should encourage members to either engage directly in threat hunting activities or instruct their Managed Service Security Provider (MSSP) to do so, using indicators provided by EI-ISAC or CISA. In this year's Black Hat keynote Chris Krebs, the CISA Director, stated that CISA is rolling out a pilot Endpoint Detection and Response (EDR) program with 29 states already involved in the pilot program. The program is expected to begin this summer, which gives the opportunity for the MS-ISAC to conduct threat hunting missions.

One last point on ransomware attack scenarios. From July 28 to July 30 CISA conducted an exercise across multiple states and jurisdictions called Tabletop the Vote. The idea is to get relevant stakeholders together to run through scenarios that could impact the election. The focus of the July exercise was, rightfully, on COVID-19 pandemic response, and how that will impact the election.

One of the outcomes of these tabletop exercises has been the release of the Elections Cyber Tabletop Exercise Package, commonly referred to as "tabletop in a box." The tabletop in a box provides a number of different scenarios that local election officials can run through to see how they would respond and ensure that the correct systems and processes are in place to deal with the emergencies. Two of the three scenarios included in the tabletop in a box involve ransomware attacks. Unfortunately, both scenarios focus on phishing attacks as the means of delivering the ransomware. While it is good that ransomware is included as part of these exercises, the tabletop in a box provides a very limited view of ransomware attack vectors.

That being said, these tabletop exercises are incredibly valuable and should be used by state and local governments to understand the real threats posed by ransomware attacks and plan accordingly. As a number of election administrators mentioned in discussions with Recorded Future, the important thing is to capture your decisions before there is an attack, this way there is a record of security precautions taken which helps to reassure constituents that the vote is verified and non-corrupted.

Conclusion

Ransomware attacks against VRDBs are a real threat and it is likely that there will be both nation state and cybercriminals targeting election infrastructure this election season. In fact, the targeting has most likely started. There was already a shortfall in election security funding that has been exacerbated by the COVID-19 pandemic and staff furloughs.

In addition to budget shortfalls, the training that election officials receive appears to be inadequate and missing a number of important ransomware attack scenarios that should be considered in allocating defenses against ransomware attacks.

And, ransomware is just one of many threats faced by election officials during the 2020 election. The combination of the pandemic, challenges with the Post Office, and nation state and cybercriminal groups targeting election infrastructure is an overwhelming security challenge. The ransomware threat is only a small piece of the threat landscape, but it is an important one.

Public perception is an important part of validating the results of the election and a well-timed ransomware attack, even if it is not fully successful, could bring the outcome of the election into question. Ransomware is not the only way to create this doubt, Recorded Future will be looking at other threats that could undermine the threat of the election in future research.

Both CISA and the EI-ISAC offer a number of freely available services to state and local governments to help them prepare for and stop ransomware attacks. The question is, how well are states taking advantage of those services?

The possible bit of good news is that many of these same fears existed around the 2018 election, but no ransomware attacks against election infrastructure occurred, at least none that were publicly reported. However, being lucky in one election does not mean that we will be lucky in this election.

Editor's Note: This is the first of a three-part series covering parts of the election infrastructure that could be vulnerable to ransomware attacks. Parts 2 and 3 will be available in the coming weeks.