BlueVoyant®

STATE AND LOCAL GOVERNMENT SECURITY REPORT

2020 AUGUST

U.S. state, local, tribal, and territorial (SLTT) governments are at the front line of cybersecurity defense; and they are now under threat more than ever.

CONTENTS

In the last month of 2019 alone, municipalities in four states -

Rhode Island
California
Florida
Louisiana

- all suffered ransomware attacks

INTRODUCTION

U.S. state, local, tribal, and territorial (SLTT) governments are at the front line of cybersecurity defense;[1] and they are now under threat more than ever

Over the last few years, attacks against municipalities have risen in frequency and cost. These attacks are driven by pervasive ransomware strains, which hold governments to ransom for larger and larger sums and often exfiltrate sensitive data whether they are paid or not. In the last month of 2019 alone, municipalities in four states - Rhode Island, California, Florida, and Louisiana - all suffered ransomware attacks.

The rise in attacks is also often driven by ease of access. State and local governments are rapidly improving their cybersecurity posture to secure their systems and protect against persistent adversaries. However, they suffer from differences in funding and preparedness, a lack of standardized policies, and systems that are digitizing faster than their security and infrastructure can keep up.

Using proprietary tools and proprietary data, and commitment to a vision of collective defense, BlueVoyant's threat intelligence and cybersecurity risk teams examined local government's cybersecurity posture in an effort to support municipalities and help them prepare against future attacks.

SLTT governments have digitized rapidly in the last decade. The speed with which this enormous technological transformation has been accomplished is overlooked in favor of its many benefits: in municipalities across the US, citizens can pay taxes and fees, register for libraries, and register to vote online. In many ways, this transformation is still underway: some municipal bodies offer all of these services online, whereas others offer only some or none at all. This represents a revolution in citizen services and access; but at the cost of secure infrastructure and strategic planning.

[1] https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/chapter-1-introduction/

SLTT governments have digitized rapidly in the last decade.

The variety of services offered online from state to state and county to county reflects essential differences in revenue and legislative structure across the U.S. In some states, counties manage election services; in some few, towns do; in most, elections are managed at the state level. The same is true for paying fines and fees and other municipal transactions. Some counties are almost as large and complex as a small state; all of them have budgetary restrictions or shortages that are reflected in their ability to manage infrastructure. And of course as a result of these differences - and underlying the variety of different systems that are digitized or not-yet-digitized on a given government website - are differences in systems and networks that relate directly to risk.

This report examines cybersecurity across state and local governments using a variety of different tools and perspectives.

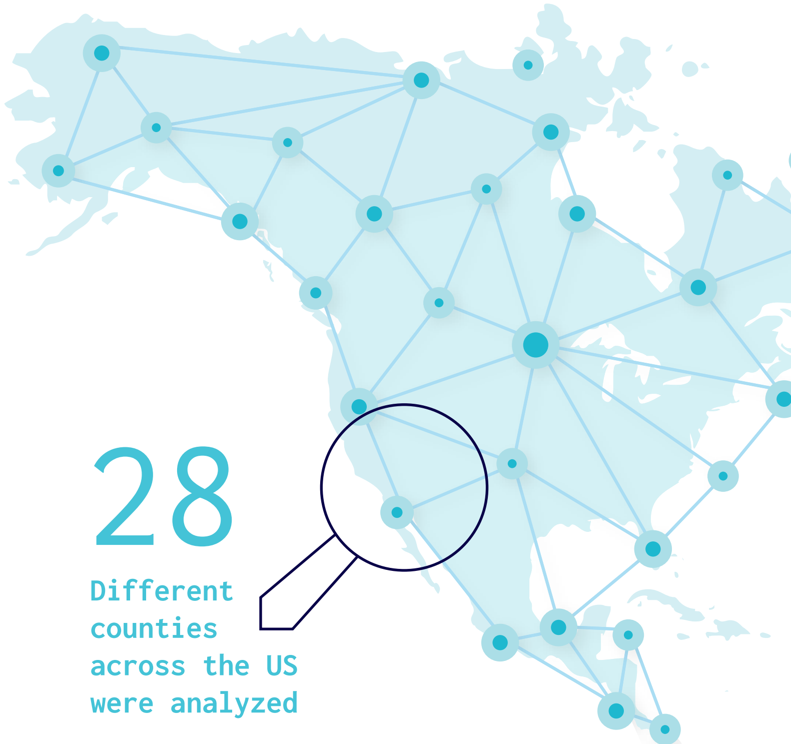
First, BlueVoyant prepared an overview of the digitization of local government over the last few decades until today. As government services have moved online, the attack surface presented to threat actors has grown substantially. This creates a complicated ecosystem of legislative change, evolving cybersecurity practices, and a timeline that shows increasing levels of risk.

Second, using Dark Web expertise and analysis, this report provides a case study of Wisconsin - showing how persistent deficiencies in cybersecurity hygiene combined with aggressive interest from threat actors can produce a hostile environment for local government.

Third, analysts looked at 28 different counties across the United States in an effort to discover the relative cybersecurity posture across the nation; how that might affect important systems and processes; and what steps can be taken to mitigate risks in the future. 28 isn't a magic number: these were counties notable for population distribution; geographic diversity; a wide range of socioeconomic averages and tax income; and, lastly, no clear party political leanings (many are considered 'swing' counties, or flipped in the last two elections).

Finally, using BlueVoyant proprietary tools and datasets, threat intelligence analysis identified and observed threat actors targeting these local government assets - and observed malicious traffic originating from these government assets, as well, indicating a significant amount of potentially compromised networks.

The federal government knows that state and local cybersecurity is a critical issue. They have created legislation to support improvements (State and Local Cybersecurity Act of 2019).[2] Many local governments have recruited and built some of the most advanced and forward-thinking cybersecurity teams in the nation.[3,4] And the recent Congressional Solarium Commission on Cybersecurity explicitly points out the need for improved coordination across federal government, state and local government, and the private sector. [5] Indeed, public-private partnerships can flourish in these conditions[6] - where circumstances are such that local and regional issues are deeply idiosyncratic, and where private sector expertise is agile and technical enough to support partners in the public sector.[7]



28

Different counties across the US were analyzed

[2] https://www.cbo.gov/publication/55474

[3] https://www.govtech.com/security/Iowa-Secretary-of-State-Puts-1M-Toward-Election-Cybersecurity.html

[4] https://azgovernor.gov/governor/news/2019/07/national-governors-association-selects-arizona-policy-academy-election

[5] https://drive.google.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view

[6] https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/chapter-1-introduction/

[7] https://www.govtech.com/workforce/The-Reality-of-the-Local-Government-Cybersecurity-Skill-Gap.html

KEY FINDINGS

108 attacks on state and local municipalities

Attacks on state and local governments are rising in frequency and cost

By analyzing open-source data on 108 attacks on state and local municipalities going back to 2017, BlueVoyant analysis found that attacks rose from an average almost 50% - almost certainly only a fraction of the true amount, since disclosure rules have changed over time. What's more concerning is that average ransom demands rose from a monthly average of $30,000 to nearly half a million - with total monetary value of ransom demands surging to millions of dollars.

Ransom demands rose from a monthly average of $30,000 to nearly half a million

State and local online infrastructure varies widely, with serious ramifications for security

By using a cross-section of the selected U.S. counties, BlueVoyant analysis showed wide variations in their organizational structure, security, and range of online services and datasets. 12 managed voting registration, whereas 14 referred visitors to state services. Domain TLDs varied between .gov, .org., .us, and one .me (for Maine). Whereas half provided only information services, the other half provided important online services including payment transactions for paying taxes and fees, voting registration, or requests for database records.

Case study revealed a vibrant and active online marketplace for selling access to state and local networks and systems

The case study 'Disabling Dairyland', an insight into Wisconsin state and county threat targeting, found hundreds of thousands of government employee credentials for sale in online dark web forums. Many of these were recently compromised, came from multiple distinct breaches, and altogether showed signs of worrying cybersecurity hygiene practices that could lead to network and database compromise.

Hundreds of thousands of government employee credentials for sale in online dark web forums

5 counties showed signs of potential compromise

Threat intelligence data gleaned from BlueVoyant proprietary datasets and tools showed widespread targeting of state and local governments - as well as signs of compromise

Data pulled from BlueVoyant's unique proprietary insight into relevant datasets showed active threat targeting across the board - for every selected county's online footprint, evidence showed some sign of intentional targeting. What's more, 5 counties - 17% - showed signs of potential compromise, indicating that traffic from government assets was reaching *out* to malicious networks.

OVERVIEW: DIGITIZATION OF LOCAL GOVERNMENT

$1tn

Digitized services can 'unlock' up to $1 trillion globally

Digitizing state and local government services is a global trend that has been occurring, in different counties and with varying levels of success, for decades. By moving citizen services online, municipalities create levels of access, efficiency, cost-savings, and transparency that are simply unavailable otherwise. The pressure is on: think tanks and consultancies insist that digitized services can 'unlock' up to $1 trillion globally.[8] This means providing online services for citizens in the form of websites or apps that enable central government-provided touchpoints for multiple services.[9] This means everything from simple services like up-to-date public transportation data, to payment services for fees, licenses, and taxes, to more sensitive provisions for online ID and voter registration.

In the wake of Covid-19, calls for increasing the provision of digital services are even stronger.[10] Processes that used to require in-person applications are increasingly being shifted online - affecting municipal responsibilities as varied as distributing permits, awarding licenses, collecting voter and ID data, and collecting fees, fines, and taxes.

In this digitized landscape, states and municipal governments are on the front lines of digital security.[11] They hold access to sensitive databases and PII, and they transact a larger and larger number of payment processes. However, the speed with which many state and local governments have digitized has ramifications: often, infrastructure and security are not tested sufficiently to provide adequate defense. This has led not only to attack after successful attack, but also to embarrassing failures in systems and tools. For example, the voting app designed for the 2020 Iowa caucus[12] failed first and foremost because of rushed adoption of new technologies. Further complicating matters, policy approaches between states differ considerably[13], which in turn has an impact on how counties and cities manage cybersecurity, incident response, and information security budgets. The government has identified cybersecurity funding and standardization as an issue (cf., State and Local Cybersecurity Act of 2019[14]), but practical challenges persist.

Elections are a case in point. While allegations of voter fraud have been roundly refuted by empirical studies, the mechanisms by which counties and states store and transfer voter information vary widely.[15][16][17] This lack of standardization affects digital electoral processes: as of March 2020, 39 states and DC offer online voter registration.[18] Critically, county-by-county integration into state systems differs widely: according to the Pew Center, "the use of real-time, electronic data transfer varied by county depending on the county's level of integration with the state system."[19] The National Association of Counties reports likewise.[20] While many states manage voting registration through Secretaries of State, many counties are still involved - either in storing voter registration data or transferring voting data. This can lead to concerns around the theft of PII, even where manipulation is less of a concern. In order to avoid public concerns around voter fraud and misinformation, securing data storage and transfer is a critical security issue.[21]

[8] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/public-sector-digitization-the-trillion-dollar-challenge
[9] https://www.civicplus.com/blog/ce/how-digital-transformation-is-impacting-local-government
[10] https://www.govtech.com/opinion/Digital-Government-More-Critical-Than-Ever-Contributed.html
[11] https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/chapter-1-introduction/
[12] https://www.nytimes.com/2020/02/03/us/politics/iowa-caucus-app.html
[13] https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/chapter-2-three-approaches
[14] https://www.cbo.gov/publication/55474
[15] https://www.brennancenter.org/issues/ensure-every-american-can-vote/vote-suppression/myth-voter-fraud
[16] https://www.brookings.edu/blog/fixgov/2020/06/02/low-rates-of-fraud-in-vote-by-mail-states-show-the-benefits-outweigh-the-risks/
[17] https://votingrights.news21.com/interactive/election-fraud-database/
[18] https://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx#table
[19] https://www.pewtrusts.org/~/media/Assets/2015/05/OVR_2015_brief.pdf?la=en
[20] https://www.naco.org/resources/featured/all-elections-are-local-county-role-elections-process
[21] https://www.nytimes.com/2020/06/07/us/politics/remote-voting-hacking-coronavirus.html

39 states and DC offer online voter registration

In these conditions - lack of standardization, varying security issues from county to county and state to state, varying levels of federal and state budgetary assistance - private-public partnerships can flourish.[22] A core principle of the recent Congressional Solarium Commission on Cybersecurity is the central importance of provisioning for greater public-private integration on matters of cybersecurity: private sector partners have the agility and specialized knowledge necessary to provide local governments with complex vulnerability assessment and threat monitoring solutions. [23]

THREAT LANDSCAPE

OVERVIEW

Cybersecurity landscapes change rapidly. For local governments, the one constant over time has been that attacks are becoming more sophisticated and the costs of recovery are skyrocketing. For example, in 2019, the city of Baltimore suffered a widespread attack that cost over $18 million in damages and remediation. Following the attack, the city's Board of Estimates approved the purchase of a $20 million cyber insurance policy.

Precise, complete records of attacks on municipal systems are hard to come by because so many never make it to the public record. With disclosure rules changing over time, and often tight IT security staff and budgets, many local governments turn to private cybersecurity companies for incident response and remediation. This means that any record is necessarily incomplete. But thanks to dozens of headline-grabbing incidents over the last several years, attacks on local governments are gaining greater notice.

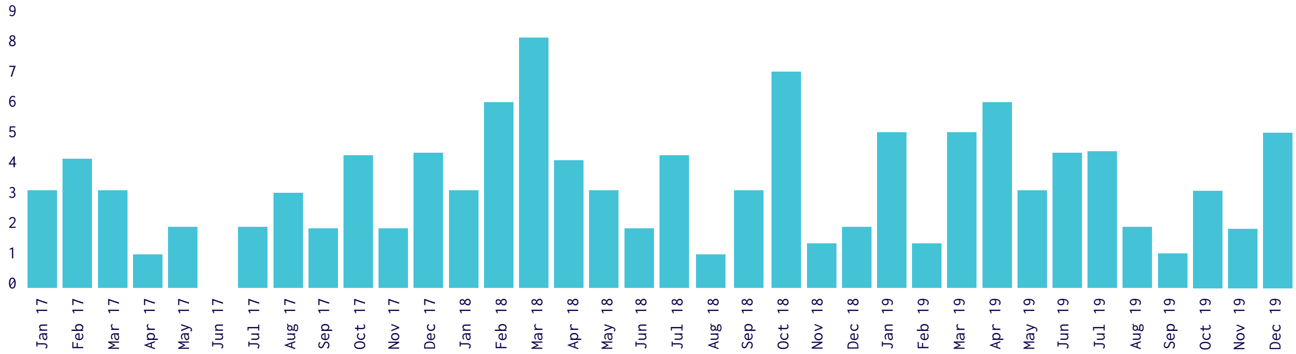
BlueVoyant analysts compiled a list of cyberattacks on state and local municipalities from 2017 to the end of 2019, using publicly available documentation and open-source records. Excluding attacks on school districts, the total number of attacks comes to 108--a large tally over two years and still only a shadow of the true figure. By analyzing these attacks and known information about them, analysts are able to demonstrate an unequivocal rise in the cost of attacks over time.

First, a timeline of attacks month-by-month shows a gradual but steady increase from 2017 to December 2019. Attacks per month rose 50% from 2017 to 2018, from 2.5 in 2017 to 3.5 in 2018, and then stayed more or less steady through 2019. For the purpose of clarity, in this case cyber attacks refer to targeted instances of intrusion, fraud, or damage by malicious cyber actors - not discovery of insecure databases or accidental online leaks.

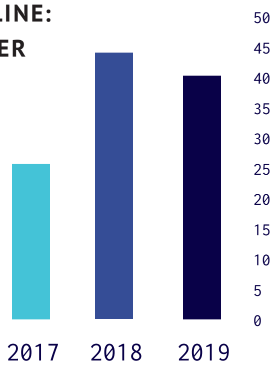
Attacks per month rose 50% from 2017 to 2018, from 2.5 in 2017 to 3.5 in 2018, and then stayed more or less steady through 2019.

[22] https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/chapter-1-introduction/
[23] https://drive.google.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view
[24] https://www.wsj.com/articles/baltimore-to-buy-20-million-in-insurance-in-case-of-another-cyber-attack-11571246605
[25] https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-cyber-attack-insurance-20191016-4owu233bmfgnjmqu3yf2rzjxt4-story.html
[26] https://www.nytimes.com/2019/08/20/us/texas-ransomware.html
[27] https://securityboulevard.com/2020/01/cyber-attacks-against-state-and-local-governments-surge/

ATTACK TIMELINE:
FREQUENCY PER MONTH



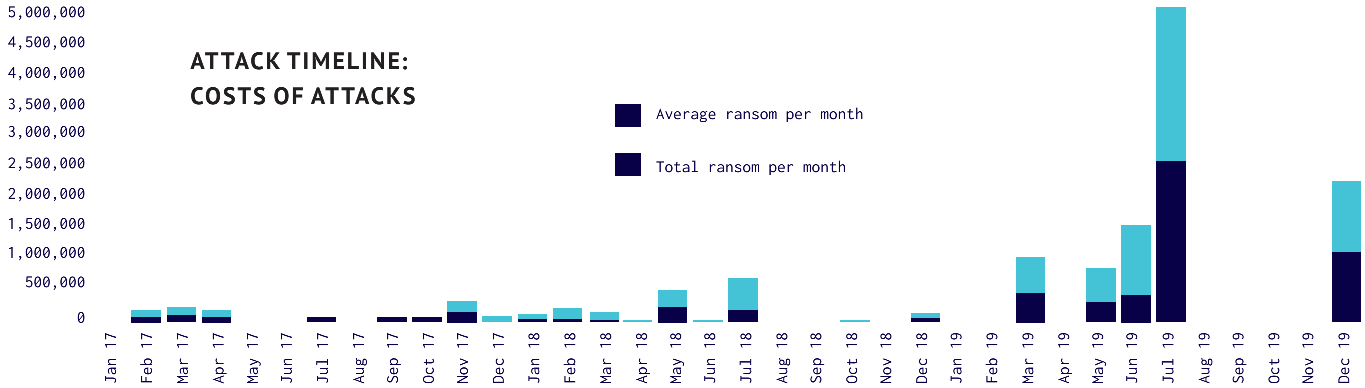
ATTACK TIMELINE:
FREQUENCY PER
YEAR



More concerning, the demanded ransom for cyber attacks rose dramatically in the same period - from an average of $30,000 per attack in 2017 to averages of $380,000, with some even reaching over $1,000,000 in 2019. This reflects a trend the cybersecurity research community terms 'big game hunting:' the shift in 2018 from opportunistic ransomware attacks to targeted ransomware intrusions focused on larger organizations, with critical digital services, that could be ransomed for high amounts.

Ransom rose from an average of $30,000 per attack in 2017 to averages of $380,000, with some reaching over $1,000,000 in 2019

ATTACK TIMELINE:
COSTS OF ATTACKS



RANSOMWARE

Ransomware, as a tool for threat actors, underwent a major evolution over the course of 2018. Before 2018 ransomware was a pervasive, but largely non-targeted, threat to computer systems all over the world. Targets would fall victim to a malspam campaign, their system was infected, and they paid a modest fee in the hundreds of dollars to regain access to all their encrypted files.

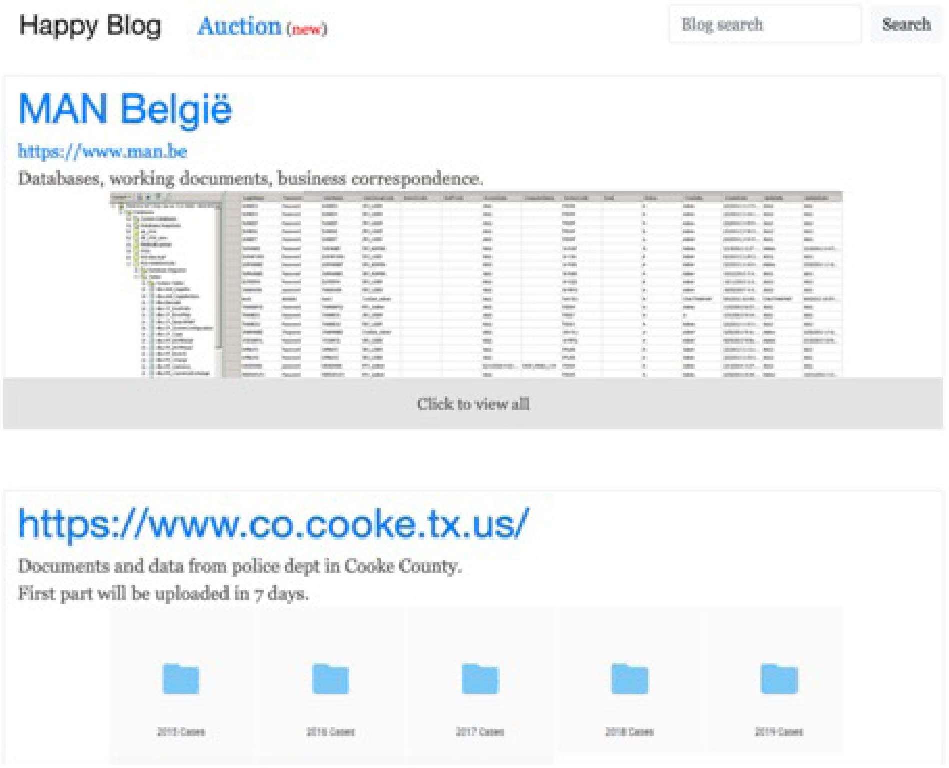
During 2018, that changed. First, as ransomware began to be more and more successful, threats became more targeted in nature. Ransomware attached to spear-phishing became more common. Targets were selected for size, and for having critical digital services and databases. Ransomware rates began to surge.

As a corollary, ransomware campaigns became more complex. More and more they were bundled with other malware: spear phishing attempts came equipped with Emotet, a modular trojan, as a loader, with the secondary injection of an infostealer (often Trickbot) finally followed by ransomware (often enough variants of Ryuk, Sodinokibi, or Maze) as the coup de grace. In these earlier stages, ransomed data was rarely exposed; if it was exfiltrated at all, it was sold or distributed by non-public methods.

Ransomware campaigns have become more **complex**

Second, following the enormous success and media attention gained by some of these more targeted attacks, ransoms began to soar. Ransomware groups were able to threaten the exposure of compromised data as leverage for their payoff demands. Ransomware gangs even began to create public websites for naming and shaming victims who didn't pay ransoms.

More recently, threat actors distributing Maze have escalated extortion on a grand scale. Having gained notoriety for their willingness to steal and publish data as a means to coercing payment, Maze's success has resulted in a wave of ransomware gangs following suit. There are even examples of public auction sites selling victim data to a field of bidders, as evidence indicates that multiple ransomware operators have come together to form cartel-like organizations focused on extortion.



MAN België

https://www.man.be

Databases, working documents, business correspondence.

https://www.co.cooke.tx.us/

Documents and data from police dept in Cooke County.

First part will be uploaded in 7 days.

Screenshot from Happy Blog, an auction website for data exfiltrated by ransomware - in this case featuring data stolen from Cooke County, TX.

OTHER THREAT VECTORS

Ransomware necessarily takes most of the attention, but online municipal assets are targeted in multiple other ways. Typosquatting has lately been on the rise; where threat actors impersonate trusted government domains with near-identical website URLs.[28] Such sites are often created as a means of advanced threat infrastructure: pre-positioning for many phishing, spear-phishing, and SM influence campaigns. These have been especially prominent in the lead-up to the 2020 election. Similarly, VPN solutions have increasingly come under scrutiny during the pandemic for providing potential points of vulnerability - particularly as government employees are forced to work from home. Both Citrix and Pulse VPN, a remote desktop application and a prominent proxy service, have had major vulnerabilities of late: vulnerabilities that allow remote execution, and do not require

[28] https://www.darkreading.com/vulnerabilities---threats/typosquatting-websites-proliferate-in-run-up-to-us-elections/d/d-id/1336110

an unwary insider to click a link. BlueVoyant's Incident Response team has been inundated with clients who have been compromised due to these same vulnerabilities.

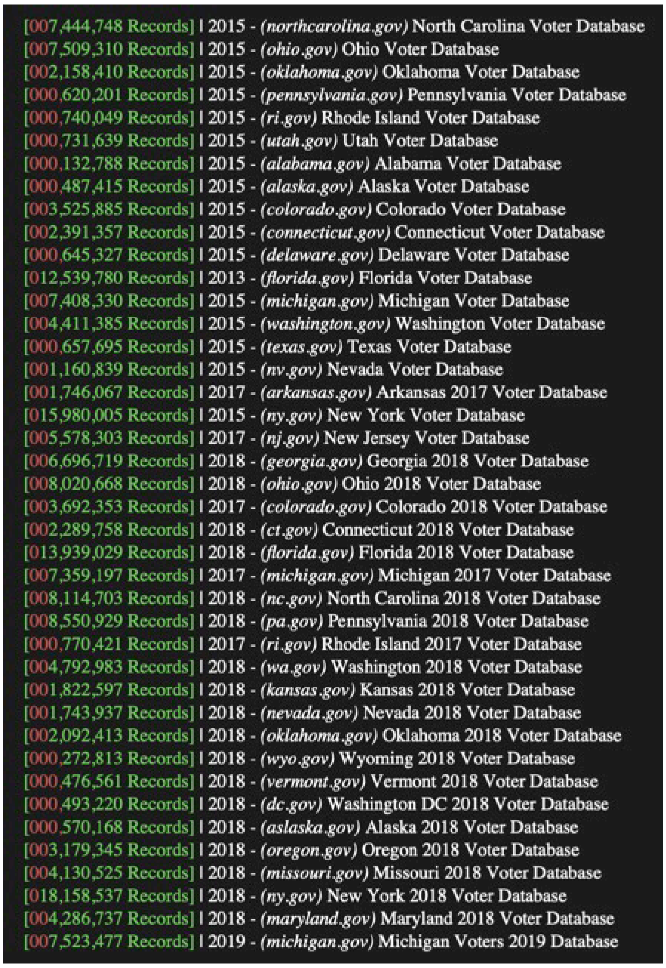
DATA BREACHES

While much election security news focuses on misinformation and the false threat of massive voter fraud, data breaches are a real threat that can undermine public confidence in voter registration systems and voting itself. In 2016, for example, the DNC was not the only election body hacked--two Florida counties were hacked, breaching voter registration rolls.[29] While there is not any evidence that the stolen information was put to use, the hackers - suspected to be Russian - were successful in publicizing the breach and thereby undermining public faith in electoral processes. This is a duty of trust that local government is obliged to uphold.

Similarly, in 2017 a breach occurred in Chicago giving access to a backend voter registration database.[30] The database was accessed through a SQL injection attack. More than 70,000 voter roll accounts were accessed before the breach was discovered.

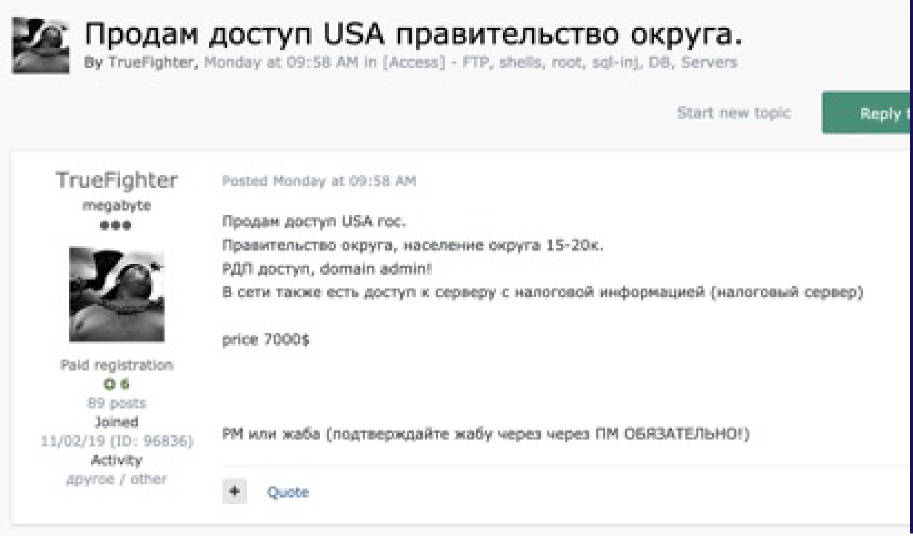
Lastly, breaches do not necessarily target PII stored in electoral databases. States and counties are increasingly offering transactional services that allow payment of taxes, fees, and fines online. The payment data is one source of concern, but so too is voluminous and detailed tax information. BlueVoyant analysts have identified posts in fraud and cybercriminal forums advertising network access to local government networks, specifically touting the value of tax and payment information.

Two Florida counties were **hacked** breaching voter registration rolls



```
[007,444,748 Records] | 2015 - (northcarolina.gov) North Carolina Voter Database
[007,509,310 Records] | 2015 - (ohio.gov) Ohio Voter Database
[002,158,410 Records] | 2015 - (oklahoma.gov) Oklahoma Voter Database
[000,620,201 Records] | 2015 - (pennsylvania.gov) Pennsylvania Voter Database
[000,740,049 Records] | 2015 - (ri.gov) Rhode Island Voter Database
[000,731,639 Records] | 2015 - (utah.gov) Utah Voter Database
[000,132,788 Records] | 2015 - (alabama.gov) Alabama Voter Database
[000,487,415 Records] | 2015 - (alaska.gov) Alaska Voter Database
[003,525,885 Records] | 2015 - (colorado.gov) Colorado Voter Database
[002,391,357 Records] | 2015 - (connecticut.gov) Connecticut Voter Database
[000,645,327 Records] | 2015 - (delaware.gov) Delaware Voter Database
[012,539,780 Records] | 2013 - (florida.gov) Florida Voter Database
[007,408,330 Records] | 2015 - (michigan.gov) Michigan Voter Database
[004,411,385 Records] | 2015 - (washington.gov) Washington Voter Database
[000,657,695 Records] | 2015 - (texas.gov) Texas Voter Database
[001,160,839 Records] | 2015 - (nv.gov) Nevada Voter Database
[001,746,067 Records] | 2017 - (arkansas.gov) Arkansas 2017 Voter Database
[015,980,005 Records] | 2015 - (ny.gov) New York Voter Database
[005,578,303 Records] | 2017 - (nj.gov) New Jersey Voter Database
[006,696,719 Records] | 2018 - (georgia.gov) Georgia 2018 Voter Database
[008,020,668 Records] | 2018 - (ohio.gov) Ohio 2018 Voter Database
[003,692,353 Records] | 2017 - (colorado.gov) Colorado 2018 Voter Database
[002,289,758 Records] | 2018 - (ct.gov) Connecticut 2018 Voter Database
[013,939,029 Records] | 2018 - (florida.gov) Florida 2018 Voter Database
[007,359,197 Records] | 2017 - (michigan.gov) Michigan 2017 Voter Database
[008,114,703 Records] | 2018 - (nc.gov) North Carolina 2018 Voter Database
[008,550,929 Records] | 2018 - (pa.gov) Pennsylvania 2018 Voter Database
[000,770,421 Records] | 2017 - (ri.gov) Rhode Island 2017 Voter Database
[004,792,983 Records] | 2018 - (wa.gov) Washington 2018 Voter Database
[001,822,597 Records] | 2018 - (kansas.gov) Kansas 2018 Voter Database
[001,743,937 Records] | 2018 - (nevada.gov) Nevada 2018 Voter Database
[002,092,413 Records] | 2018 - (oklahoma.gov) Oklahoma 2018 Voter Database
[000,272,813 Records] | 2018 - (wyo.gov) Wyoming 2018 Voter Database
[000,476,561 Records] | 2018 - (vermont.gov) Vermont 2018 Voter Database
[000,493,220 Records] | 2018 - (dc.gov) Washington DC 2018 Voter Database
[000,570,168 Records] | 2018 - (aslaska.gov) Alaska 2018 Voter Database
[003,179,345 Records] | 2018 - (oregon.gov) Oregon 2018 Voter Database
[004,130,525 Records] | 2018 - (missouri.gov) Missouri 2018 Voter Database
[018,158,537 Records] | 2018 - (ny.gov) New York 2018 Voter Database
[004,286,737 Records] | 2018 - (maryland.gov) Maryland 2018 Voter Database
[007,523,477 Records] | 2019 - (michigan.gov) Michigan Voters 2019 Database
```

US voter databases available for purchase on Raid Forums, a cybercriminal venue that specializes in data breaches.



Продам доступ USA правительство округа.

By TrueFighter, Monday at 09:58 AM in [Access] - FTP, shells, root, sql-inj, DB, Servers

TrueFighter
megabyte
Paid registration
6
89 posts
Joined
11/02/19 (ID: 96836)
Activity
другое / other

Posted Monday at 09:58 AM

Продам доступ USA гос.
Правительство округа, население округа 15-20к.
РДП доступ, domain admin!
В сети также есть доступ к серверу с налоговой информацией (налоговый сервер)

price 7000$

PM или жаба (подтверждайте жабу через через ПМ ОБЯЗАТЕЛЬНО!)

BV TRANSLATION:

[I'm selling access to USA gov.
District(regional) gov, population 15-20K
RDP access, domain admin!
The network also has access to a server with tax info (tax server)

Price $7000

PM or Jabber
(must confirm Jabber via PM)]

Screenshot in Russian of a threat actor offering network access to a local government.

[29] https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016
[30] https://www.upguard.com/breaches/cloud-leak-chicago-voters

CASE STUDY:
DISABLING DAIRYLAND

Consider Wisconsin. A pivotal state for achieving victory in the electoral college, Wisconsin is also home to some of the "swingingest" counties in the US. According to Ballotpedia, a non-profit, non-partisan reference for electoral data and information, "There were 23 counties in Wisconsin that voted for Donald Trump in 2016, and Barack Obama in 2008 and 2012."[31] What is more, the average results of these Wisconsin swing counties predicts the next US president at much greater than even odds: "Since 1960, Pivot Counties in Wisconsin have matched the national election result in 77.39% of presidential elections."[32]

77.39%

Since 1960, Pivot Counties in

Wisconsin

have matched the national election result in 77.39% of presidential elections

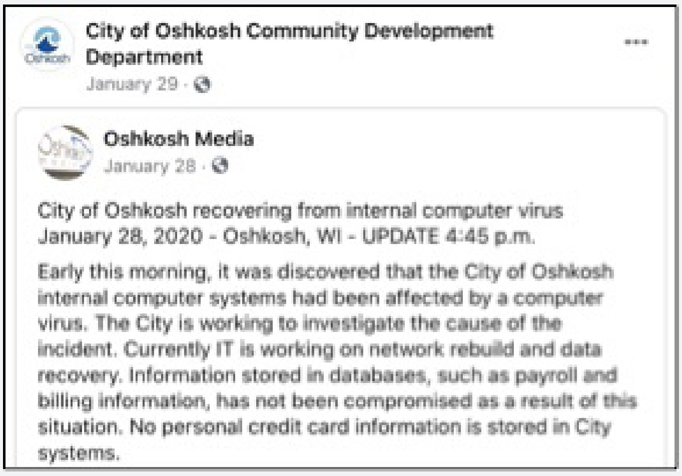
Oshkosh is the largest city and county seat of Winnebago County, WI. In 2016, the city counted 39,757 registered voters - 146% more voters than the statewide margin of victory for the presidential election that year.[33] Racine is another critical Wisconsin swing county. In 2016, the Republican Party carried the vote there by 4.6%. However, in 2012 and 2008, the Democratic Party won by 3.54% and 7.41%, respectively.[34] Oshkosh and Racine serve to show how a cyber event can adversely affect two critical counties.

WHERE'S THE CHEESE?

In January of 2020 the cities of Oshkosh and Racine were disabled by ransomware attacks. To the credit of both municipalities, data backups were in place and secured against the infection. This is an essential precaution for any organization to take for business continuity, however it does not serve to protect against election interference.

Oshkosh was rendered supine by the attack. In the words of their City Manager: "Our ability to access anything on our computer files right now is non-existent."[35] In Racine, the havoc was more limited, but the city's website, email, voicemail, and payments systems were rendered inoperable. Disruption and confusion were manifest.

In January 2020 the cities of Oshkosh and Racine were disabled by ransomware attacks



City of Oshkosh Community Development Department

January 29 ·

Oshkosh Media

January 28 ·

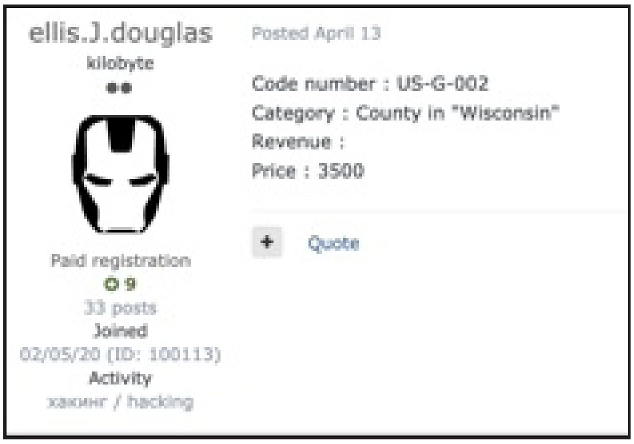
City of Oshkosh recovering from internal computer virus

January 28, 2020 - Oshkosh, WI - UPDATE 4:45 p.m.

Early this morning, it was discovered that the City of Oshkosh internal computer systems had been affected by a computer virus. The City is working to investigate the cause of the incident. Currently IT is working on network rebuild and data recovery. Information stored in databases, such as payroll and billing information, has not been compromised as a result of this situation. No personal credit card information is stored in City systems.

The City of Oshkosh, WI announces the ransomware event on Facebook.[36]

[31] https://ballotpedia.org/Pivot_Counties_in_Wisconsin
[32] https://ballotpedia.org/Pivot_Counties_in_Wisconsin
[33] hxxps://www2[.]ci.oshkosh[.]wi[.]us/WebLink/DocView[.]aspx?id=967622&dbid=0&repo=Laserfiche
[34] hxxps://ballotpedia[.]org/Pivot_Counties_in_Wisconsin#2016_election_results
[35] hxxps://wtaq[.]com/news/articles/2020/jan/31/oshkosh-city-computers-hit-by-ransomware/980495/
[36] hxxps://www[.]facebook[.]com/OshkoshDevelop/?ref=nf&hc_ref=ARSZL_PO1D4k616QCmQVlpanJBQMK4qWliFcdjFwEaH5Hc0qdUXm33iFWvoDkhSey_I



ellis.J.douglas
kilobyte
●●

Paid registration
9
33 posts
Joined
02/05/20 (ID: 100113)
Activity
хакинг / hacking

Posted April 13

Code number : US-G-002
Category : County in "Wisconsin"
Revenue :
Price : 3500

Threat actor "ellis.J.douglas" advertises unauthorized access to a Wisconsin county network on the top-tier, Russian language hacker forum Exploit.

Reportedly, attackers lay dormant in Oshkosh's system since September 2018 - more than one year - before conducting the attack.[37] This extraordinary dwell time is not typical of ransomware attacks motivated by financial gain. What is more, there was no actual ransom demand made in either case. Neither the cities nor the FBI has informed the public of who the attackers were, beyond describing them as "Russian hackers." Ransomware is an extraordinarily lucrative criminal endeavor. The absence of a ransom demand could indicate a non-financial motivation for disrupting these city infrastructures.

> "It just takes one weak spot in your entire system for this problem to rush in."
>
> Oshkosh City Manager[38]

MORE HOLES THAN SWISS CHEESE

For ransomware events, there are two dominant avenues of infection. As was the case with Racine and Oshkosh (and the majority of ransomware attacks), the malware was introduced via a malicious phishing email. The next-most common avenue of infection is by gaining direct access to the victim network, typically achieved by using exploits of remote access protocols such as RDP or SSH. BlueVoyant cyber threat analysts have observed instances of malicious actors selling network access to US counties and states in top-tier dark web forums. The threat actor "ellis.J.douglas" has been active under their current alias on the top-tier dark web forum Exploit since February 2020. They have credibly purported to sell network accesses to a variety of global enterprises both public and private.

@4,518

Instances of a County email address implicated in 64 distinct data breach events

Several of the major ransomware variants are introduced to the environment by phishing emails. Recall that both of the ransomware events in Oshkosh and Racine were perpetrated using phishing emails. As part of our investigation, BlueVoyant analyzed the email credential breach history of the Oshkosh County and Racine County email domains. Phishing emails are more convincing and malicious if they are sent by a trusted user. So what is the likelihood that a bad actor could compromise a County email inbox and introduce malware to the system by impersonating a government worker?

For Oshkosh, BlueVoyant detected 555 unique instances of compromised email accounts throughout 38 different data breach events. For Racine County's email domain, BlueVoyant observed 266 instances of email credential compromise from February 2017 to as recently as May, 2020 in 18 distinct breach events.

Oshkosh City Manager's paraphrasing of the precipitating event demonstrates the low-level of understanding of cyber intrusions such as that which crippled Oshkosh: "Essentially, what happens is somebody opens an email that looks rather innocuous, but it's very bad for your system, so somebody opened it and that's what happened."[39]

BlueVoyant expanded this analysis and investigated the email password breach history for all 23 of the Obama-Trump swing counties in Wisconsin. Taken as a whole, we observed 4,518 instances of a County email address implicated in 64 distinct data breach events.

We noted three instances in which County email addresses were used to register for AdultFriendFinder, a social platform for those seeking casual or discreet sexual encounters. One of these three emails was the administrator account for the County. Breach information such as this could provide the basis for blackmailing County employees.

555
Detected

BlueVoyant detected 555 unique instances of compromised email accounts throughout 38 different data breach events

[39] hxxps://fox11online[.]com/news/local/oshkosh-becomes-one-of-ransomewares-latest-victims

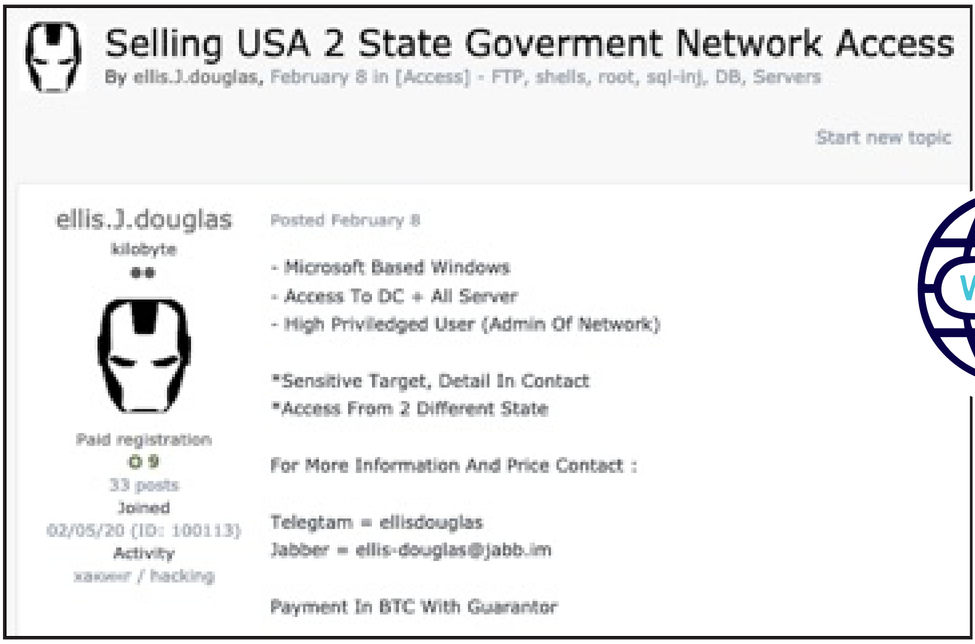
BlueVoyant analysts also noticed several publicly, anonymously posted Pastebin dumps that are suggestive of vulnerability targeting. Pastebin and other paste sites are online services where one can anonymously store and share text information such as draft code, lists, or copywriting. These repositories are often used by cybercriminals in their schemes; they can be hosted on the clear web or the dark web.

Consider this list BV analysts noted titled "All US Government Sites."[40] This paste included 11,775 URLs that appear to be US government websites ranging from municipalities to federal agencies. BV analysts observed an abundance of Wisconsin towns, cities, county, and state websites enumerated here. All told, BV observed 105 .wi subdomains in this list, an underrepresentation of the targeted Wisconsin websites since some fall under different top-level domains (ie .com or .org).

Or consider the Wisconsin government Citrix portal links posted to a January 11, 2020 anonymous Pastebin post:

hxxps://citrix[.]co[.]washington[.]wi[.]us
hxxps://citrix[.]co[.]winnebago[.]wi[.]us
hxxps://apps[.]co[.]door[.]wi[.]us
hxxps://apps[.]co[.]rock[.]wi[.]us
hxxps://apps[.]co[.]wood[.]wi[.]us
hxxps://bb9[.]waukesha[.]k12[.]wi[.]us
hxxps://portal[.]co[.]portage[.]wi[.]us
hxxps://storefront[.]co[.]walworth[.]wi[.]us
hxxps://calcitrix[.]co[.]calumet[.]wi[.]us
hxxps://mediasite[.]co[.]walworth[.]wi[.]us
hxxps://remote[.]co[.]saint-croix[.]wi[.]us
hxxps://remote[.]swib[.]state[.]wi[.]us
hxxps://remotebr[.]swib[.]state[.]wi[.]us
hxxps://remotemfa[.]swib[.]state[.]wi[.]us[41]

Exploit code for CVE-2019-19781, which exploits Citrix, was released January 10, 2020 - one day before these Citrix portal URLs were proliferated online. What likely happened was attackers were scanning the internet for sites susceptible to this attack and dumped a targeting list on Pastebin. This vulnerability enabled attackers to perform directory traversal, which then in turn enabled an attacker to remotely execute arbitrary code -- plainspeak: it is a devastating exploit.



Selling USA 2 State Goverment Network Access

By ellis.J.douglas, February 8 in [Access] - FTP, shells, root, sql-inj, DB, Servers

ellis.J.douglas
kilobyte
Paid registration
0 9
33 posts
Joined
02/05/20 (ID: 100113)
Activity
xaxoer / hacking

Posted February 8

- Microsoft Based Windows
- Access To DC + All Server
- High Priviledged User (Admin Of Network)

*Sensitive Target, Detail In Contact
*Access From 2 Different State

For More Information And Price Contact :

Telegtam = ellisdouglas
Jabber = ellis-douglas@jabb.im

Payment In BTC With Guarantor

Notorious network penetrator "ellis.J.douglas" offers access to two US states on the top-tier dark web forum Exploit. Later they updated the thread to include a third. The asking price was $80,000 for all three illicit accesses.

WWW

11,775 URLs

appear to be US government websites ranging from municipalities to federal agencies

[40] hxxp://pastebin[.]com/cG4uiSn5
[41] hxxps://pastebin[.]com/Fw8jm5Xq

THREAT INTELLIGENCE DATA

In order to examine state and local cybersecurity in more detail, BlueVoyant analysis selected 28 counties to analyze in detail. The counties selected vary socioeconomically, geographically, and by population; they are notable for their differences and for one common characteristic, their political unpredictability (all counties either switched party allegiance in 2016 or demonstrate indicators for likely switching in 2020).

Using both open-source analysis and proprietary datasets and tools, including BlueVoyant's specialized visibility into global internet traffic and access to known malicious networks, BlueVoyant analysts uncovered radical differences in the way county and state governments organized their online infrastructure. In addition, analysts observed threat traffic targeting local government websites, from the county level to state. And finally, analysts observed evidence of compromise - indicating that threat actors had compromised devices or networks belonging to local governments.

COUNTY INFRASTRUCTURE OVERVIEW

The 28 counties selected range widely over the U.S. They cover 27 states and vary in population from just under 3,000 in Lincoln, Maine to almost 4.5 million in Maricopa, Arizona.

COUNTY	STATE	POPULATION	WEBSITE
Delaware	IN	114,315	co.delaware.in.us
Koochiching	MN	12,440	co.koochiching.mn.us
Douglas	NE	7,303	douglascounty-ne.gov
Anne Arundel	MD	579,234	aacounty.org
Conejus	CO	8,200	conejuscounty.org
Hillsborough	NH	417,025	hcnh.org
Montgomery	OH	531,687	mcohio.org
Sawyer	WI	16,489	sawyercountygov.org
Watauga	NC	56,177	wataugacounty.org
Gallatin	MT	114,434	gallatincomt.virtualtownhall.net/
Buckingham	VA	16,999	buckinghamcountyva.org
Cedar	IA	18,627	cedarcounty.org
Chester	PA	524,989	chesco.org
Hidalgo	NM	4,240	hidalgocounty.org
St Lawrence	NY	107,740	stlawco.org
Lincoln	ME	2,884	lincolncountymaine.me
Dewey	SD	5,904	sd.gov
Maricopa	AZ	4,485,000	maricopa-az.gov
Windham	CT	116,782	Portal.ct.gov
Woodruff	AR	6,490	woodruffcounty.arkansas.gov
Fort Bend	TX	811,688	fortbendcountytx.gov
Franklin	KY	50,991	franklincounty.ky.gov
Suffolk	NY	1,477,000	suffolkcountyny.gov
Chickasaw	MS	17,171	chickasawcoms.com
Nevada	CA	99,775	mynevadacounty.com
Steele	ND	1,903	steelend.com
Dooley	GA	13,706	doolycountyga.com

Counties varied widely by top-level domain (TLD)- whether .gov, .org, or, in one case, .me. The lack of standardization here - which often enough prohibits county governments from leveraging the benefits of a .gov - is reflected in other ways.[42]

In addition, state and county infrastructure varied in terms of the size and sophistication of their architecture. The majority of counties relied on hosting providers for IP space, although 10 registered netranges of their own.

The difference is significant: registering IP space indicates sufficient IT policy and expertise to create and maintain a county's own online infrastructure. Not surprisingly, the counties that did so are either larger and better-funded (Fort Bend) or known for their advanced cybersecurity teams (Maricopa).

FOR EXAMPLE: available digital services varied widely county to county. Many offered no services at all - simply bulletin boards for further information, or links to state services (usually, voter registration). However, 14 counties allowed citizens to make payments online - either for taxes, fines, or fees. In such cases, county networks processed transactions and stored payment data. Usually, when a county supplied any digital services at all, they provided many: in Douglas, Nebraska; Cedar, Iowa; Chester, Pennsylvania; and Fort Bend, Texas, citizens can make payments, request information, register to vote (or view registration information), and apply for licenses, all online.

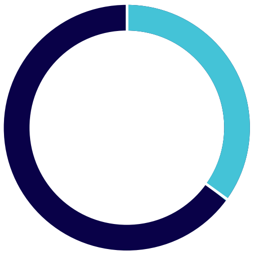
It's worth noting that these services are not provided only in larger governments or in wealthier ones. The counties that provide the most services range in size from 7,000 people to 811,000. They are two .govs and two .orgs. Three of those states allow online voter registration, and one doesn't.

THREAT TARGETING AND COMPROMISE

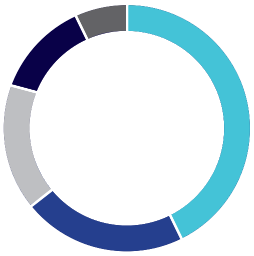
Using BlueVoyant's proprietary datasets and insight, analysts were able to identify and observe both inbound activity targeting county and state online infrastructure - as well as outbound communications suggesting compromised devices and networks. As a result of this analysis, all 28 counties - and, where applicable, their supporting state infrastructure - showed signs of being targeted. In addition, five counties showed signs of compromise.

14

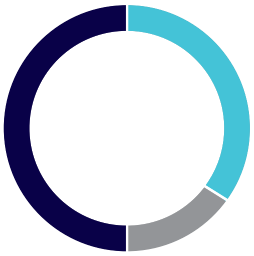
counties allowed citizens to make payments online either for taxes, fines or fees



Counties with owned IP space vs. counties relying on hosting providers for IP netranges



Distribution of top-level domains



Available online services by county

[42] https://www.cisa.gov/publication/election-security-fact-sheets

BlueVoyant uses proprietary and third-party feeds to identify traffic between county online infrastructure and domains and blacklisted IP ranges, seeking evidence of malicious probing or scanning from potential malicious actors. In addition, BlueVoyant digs deeper to identify any interactions between these counties and possible malicious actors: where traffic may reveal not only initial probing, but fraudulent or malicious communication with government domains and IP addresses.

95,000

BlueVoyant observed over 95,000 incidents of inbound targeting

Over a period of six months, BlueVoyant observed over 95,000 incidents of inbound targeting focused on the 28 counties and their online infrastructure - domains and IPs. In most cases, this activity indicated targeting of a lower order of risk: spam and low-level scanning. However, at least five states were recipients of much more targeted probing: probing that sought login webpages, wordpress sites, and other vulnerable assets. What's worth noting is that no county was wholly free from targeting - every single footprint BlueVoyant identified had some probing that was either targeted, malicious, or at the least suspicious.

17%

of observed counties showed signs of potential compromise

More concerning, 17% of observed counties showed signs of potential compromise. There are two different ways to examine compromise. One is to monitor evidence of local government IPs and domains reaching out to blacklisted assets. This can sometimes be evidence of a security appliance – many security companies offer services that reach out to known blacklisted assets in a continual process of updating their index of malicious infrastructure. However, no security appliances were detected by our analytics on the networks in question. That means this traffic is more likely evidence of compromise: malware is installed on a device or network and is now reaching out to a malicious command and control server. This was seen in one county.

The second way to examine compromise is to monitor evidence of traffic originating from government assets contacting malicious domains. This is suspicious: there is little reason for local government devices to be reaching out to external IPs or domains known for frequent malicious activity. Occasionally this browsing may be innocent. However, while this is not evidence of a definitive breach in security, many of the contacted sites - such as zeusmafia[.]xyz and xyz[.]n1272serv - are known for hosting malware or use in DDoS attacks as stressors. This indicates likely, if not certain, network or device compromise.

4

of the compromised counties provide numerous digital services

While BlueVoyant is not publicizing the names of counties that are targeted or compromised, it is worth noting that four of the compromised counties provide numerous digital services - including payment systems and voter registration or other sensitive databases.

These observations show that municipal governments operate under extreme and persistent scrutiny, and often targeting, from known threat actors; that those threat actors target vulnerable login portals and other vulnerable webpages; and that sometimes, they succeed.

INSURANCE ISSUES

The data gathered by the BlueVoyant team reflects threats that are often contemplated for coverage under today's cyber insurance policies. These policies not only function as financial risk transfer tools, but provide access to experts to assist in the investigations. Some also provide for the implementation of proactive security tools and training. Almost half of state governments had cyber insurance in 2019, and the number is expected to rise.

Almost half of state governments had cyber insurance in 2019, and the number is expected to rise

Specifically, cyber insurance is designed to cover the phishing attacks, ransomware attacks and other incidents arising out of indicators of compromise. Carriers typically provide funds for investigations, ransom payments and legal fees. Additionally, carriers will provide funds for litigation arising out of an incident, and should there be a finding of the exfiltration of PII or PHI, for example, cyber insurance will cover those associated costs.

Cyber insurance metrics and cyber modeling for underwriting purposes can also provide important data needed to support the private-public partnerships for which the legislators are advocating.

CONCLUSION AND RECOMMENDATIONS

As stated in the introduction to this report, SLTT governments operate on the very front lines of cybersecurity defense. Rapid digitization, the development of online citizen services, digitally-enabled voter registration and electoral systems - all of these benefits have and will continue to have a net positive impact on national democracy and government efficiency.

That same digitization comes with attendant issues. This report shows that counties and states operate with widely differing approaches to online infrastructure: sometimes offering many core citizen services, and sometimes none; often under different TLDs; and with different online architecture, their hosted or leased infrastructure, and different relationship to their states. Through the case study of Wisconsin, the report also shows worrying cybersecurity hygiene failures and an active threat actor ecosystem interested in purchasing and selling local government credentials. Lastly, the report shows active targeting - and more worryingly, active compromise.

As the Solarium Commission notes, these conditions are excellent for public-private partnerships. Private sector organizations have the technical expertise and organizational agility to support state and local governments, especially on cybersecurity issues where different regions face deeply idiosyncratic and varied obstacles.

Regardless, local governments can mitigate their risks - especially with respect to ransomware - by following these

RECOMMENDATIONS:

Cybersecurity Risk Assessment

Local government entities can benefit from cybersecurity risk assessments that provide technical and detailed insights into how to improve cybersecurity posture. These vulnerabilities are often multiplied in periods of rapid change, such as the rapid rollout of digital services currently occurring in states and counties nationwide.

Managed Security Service

Similarly, dedicated managed risk services can provide enormous cost savings and security against attacks and compromises. These fully-integrated services monitor, mitigate, and alert clients to vulnerabilities, as well as possible attacks and compromises, in real time: severely reducing the chance of critical and costly cyber incidents.

Cyber Insurance

Cyber insurance is an integral part of risk management as well as cost savings. The completion of an underwriting application is a good first step to understand vulnerabilities and identify areas of improvement. Further, once a policy is bound, not only is funding a response to an event provided, but typically policies include approved cyber experts at reduced rates. The possession of cyber insurance also shows preparedness and is a useful tool in the defense strategy in any emerging litigation or regulatory proceeding.

Professional Services - incident response, remediation and mitigation

Municipal governments are unfortunately all too familiar with incident response and remediation processes. Experienced investigators, when called in immediately (and when coupled with appropriate disclosure protocols), are the best possible means of avoiding mistakes and implementing proper response and remediation steps.

Resiliency

Above all, any third-party cybersecurity service or internal review will be insufficient unless resiliency is built into systems. Not only do local governments need to build defense in depth, they also need to prepare for resiliency and recovery in the event of an attack. This means backing up data, having plans in place should systems or datasets be offline, and preparing for recovery scenarios.

BlueVoyant

CONTACT THE TEAM

Contact Us
BlueVoyant Headquarters
335 Madison Ave, Suite 5G
New York, NY 10017

Tel: 646-558-0052 (8-5 EST)
Email: contact@bluevoyant.com
www.bluevoyant.com