

# THE USA FROM A CYBERCRIMINAL'S PERSPECTIVE



## SEARCHLIGHT. CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.



Crown  
Commercial  
Service  
Supplier

# CONTENTS

<b>4</b>	<b>INTRODUCTION</b>
<b>5</b>	<b>METHODOLOGY</b>
<b>6</b>	<b>INITIAL ACCESS BROKERS</b>
<b>8</b>	<b>RANSOMWARE</b>
<b>10</b>	<b>HACKTIVISM</b>
<b>12</b>	<b>ELECTIONS</b>
<b>14</b>	<b>COMMON VULNERABILITIES AND EXPOSURES (CVE)</b>
<b>16</b>	<b>FRAUD AND STOLEN GOODS</b>
<b>18</b>	<b>CONCLUSION</b>
<b>19</b>	<b>GATHERING DARK WEB INTELLIGENCE</b>

# INTRODUCTION

The United States has always been a target of cyberattacks. Incidents in the USA range from nuisance caused by inexperienced hackers on school networks (often referred to as script kiddies or skids), to financially-motivated attacks against some of the largest corporations in the world, to state-sponsored cyberwarfare and the targeting of critical national infrastructure. The USA has seen it all and has more experience than most countries in successfully defending against or mitigating these threats as well.

You could even argue that the USA was home to the first major “cyberattack”, which is often cited as the **Morris Worm**<sup>1</sup> incident in 1988. Deployed by a computer science graduate named Robert Tappan Morris, this worm was not necessarily designed for malicious intent and not anticipated to propagate as far as it did. Nevertheless, the Morris Worm succeeded in impacting at least a tenth of the computers connected to the internet at the time, including slowing vital military and university functions, and Morris was the first person found guilty under the 1986 Computer Fraud and Abuse Act.

Times have changed. Thankfully, cybersecurity has progressed to the point that a single malware strain cannot cause the equivalent amount of damage. On the other hand, we now operate in an environment where those perpetrating cyberattacks certainly do have malicious intent, developing software and techniques to steal, destroy, or disrupt - fueled by a variety of motivations.

Most cybercriminals on the dark web are financially motivated, which naturally makes the United States a target due to its status as the largest economy in the world. This means it is home to some of the largest corporations, who are targeted for the customer data, financial information, or intellectual property. It also has a relatively high-earning population compared to other countries, who are targeted by cybercriminals and fraudsters for their social security numbers and credit card details.

Geopolitics is also a factor impacting the threat landscape in the USA. A leading member of NATO and multiple other western alliances, the United States is a target for threat actors operating in nations with competing ideologies. In this report we discuss hacktivist activity against organizations within the United States but it should be noted that even financially motivated attackers favor attacks against businesses and individuals in the USA based on either their own political leanings or because of the knowledge that law enforcement in Russia - for example - are very unlikely to persecute them as long as their targeting is limited to “unfriendly” nations. Explicitly or implicitly, cybercriminals are encouraged by the state to carry out attacks against the USA, which is something we have observed in the increase in incidents following the outbreak of the war in Ukraine.

<sup>1</sup> <https://www.fbi.gov/history/famous-cases/morris-worm>

<sup>2</sup> <https://www.slcyber.io/dark-web-security-products/cerberus/ai-powered-dark-web-translation/>

## METHODOLOGY

This report contains our observations of the targeting of the United States that we have seen on the dark web, the hidden part of the internet that cybercriminals use to plan, share tactics, and buy the resources they need to execute their attacks. Intelligence gathered from the dark web provides an insight into the “cybercriminal perspective” - their motivations, objectives, and methods. While this is a broad overview at the country level, it demonstrates how interrogating dark web data can provide security teams with a better understanding of their adversaries, which they can use to prepare their defenses.

The intelligence in this report was gathered between July 2023 and July 2024 using our dark web investigations platform. Text from the dark web has been reformatted for readability. In some cases, data has been redacted for security purposes. Unless otherwise stated, the text is verbatim for how it appears on the dark web. We use our own proprietary **translation technology**<sup>2</sup> to convert text into English.



**LUKE DONOVAN**

Head of Threat Intelligence  
Searchlight Cyber





# CYBERCRIMINALS TARGETING THE USA

## INITIAL ACCESS BROKERS

Initial access brokers are financially motivated cybercriminals that specialize in gaining a foothold in organizations' networks. This "initial access" can be obtained by leveraging several methods including social engineering, malware deployment, vulnerability exploitation, or even collaborating with insiders working for the victim entity. Initial Access Brokers use dark web forums to monetize this access - usually auctioning it to the highest bidder - and therefore play an important part in the cybercriminal "ecosystem", undertaking a lot of the legwork for the likes of ransomware gangs.

According to our dark web data, Brokers have advertised access to US-based victims at least 730 times on popular cybercrime forums since the beginning of 2024. Of course, this number should only be considered a baseline, as many sellers operate privately with established customers, or only publicly advertise a small portion of their inventory to avoid attracting unwanted attention from law enforcement. Forums such as Exploit, XSS, RAMP, BreachForums, and CryptBB remain a popular choice among Initial Access Brokers but some have even opened their own dark web marketplaces to advertise just their products.

**Figure 1** depicts an example of an Initial Access Broker - known as Ddarknotevil - advertising network access to the IT systems of an undisclosed US-based oil and gas company. The actor also offers a comma-separated values file, which allegedly contains employee data. The actor specifically highlights the fact that this entity is in the USA and suggests that it would be a good target for ransomware.

### USA \$4B GAS MANUFACTURERS IT ACCESS

🕒 9th Jul 2024, 01:11:05 pm // Posted on [BreachForums](#)

🕒 9th Jul 2024, 01:11:05 pm      🌐 English  
- Posted by [Ddarknotevil](#)

Hello BreachForums Community,  
I offer you an IT system Access,  
Includes: extracted employees' data.csv file.

Revenue: \$4B

The company is listed as the largest in its industry in the US region, which makes it a valuable target for ransomware and other attacks

XMR, BTC \$4.5K - BF MM\XSS Escrow

\*Sample & Details:interested only

Contact Telegram, PM XXXXXXXX

Thanks for readin.

**Figure 1:** An Initial Access Broker advertises access to an oil and gas company in the USA with a revenue of \$4bn.

This thread was posted on BreachForums, where the actor has obtained a significant number of positive reputation points (more than 1,000) but it should be noted that Ddarknotevil has an established presence on other forums as well, including XSS. On this occasion, the Initial Access Broker did not provide any proof of claims but - based on the actor's reputation across multiple forums - this threat should be taken seriously.

In another example (**Figure 2**) the actor hehehek is observed offering access to an undisclosed US-based healthcare company. In this case, the Broker has chosen to start an auction on the Exploit forum, as indicated by the “start”, “step”, and “blitz” prices, which respectively refers to the opening price for the auction, the increments at which bidding can be increased, and the price that the actor will sell the access outright.

The post contains further clues to the identity of the victim organization (a \$6m revenue healthcare company), how the actor gained access (potentially by leveraging an AnyDesk remote desktop application), and how severe of a threat this may be (with the actor claiming domain admin privileges). This is critical information that a security team could use to firstly identify if they are the victim and secondly to identify the compromise within their system before this access has been sold and exploited.

Attackers are increasingly targeting patient protected health information (PHI) and there have been observed incidents of cybercriminal gangs using this data to blackmail and extort patients. Healthcare organizations therefore need to be on high-alert to Initial Access Broker posts related to their infrastructure being advertised on the dark web as - beyond brand damage and security considerations - they can also be fined for failing to comply with the **HIPAA Security Rule**.<sup>3</sup>

<sup>3</sup> <https://www.hhs.gov/hipaa/for-professionals/security/index.html>



## BROKERS HAVE ADVERTISED ACCESS TO US-BASED VICTIMS AT LEAST 730 TIMES ON POPULAR CYBERCRIME FORUMS SINCE THE BEGINNING OF 2024

### US \$6M HEALTHCARE DA

🕒 14th Mar 2024, 08:07:00 am // Posted on **Exploit**

🕒 14th Mar 2024, 08:07:00 am 🌐 English  
- Posted by **hehehek**

Type access: AnyDesk

Domain admin

Finance revenue: \$6M

Industry: Hospitals & Clinics, Healthcare

// Windows Server 2016 / AV: Windows Defender /  
Domain admin / 98 users, 61 computers in domain

🕒 15th Mar 2024, 01:25:00 pm 🌐 German  
- Posted by **hehehek** [Translate to English](#)

Start: 750\$

Step: 50\$

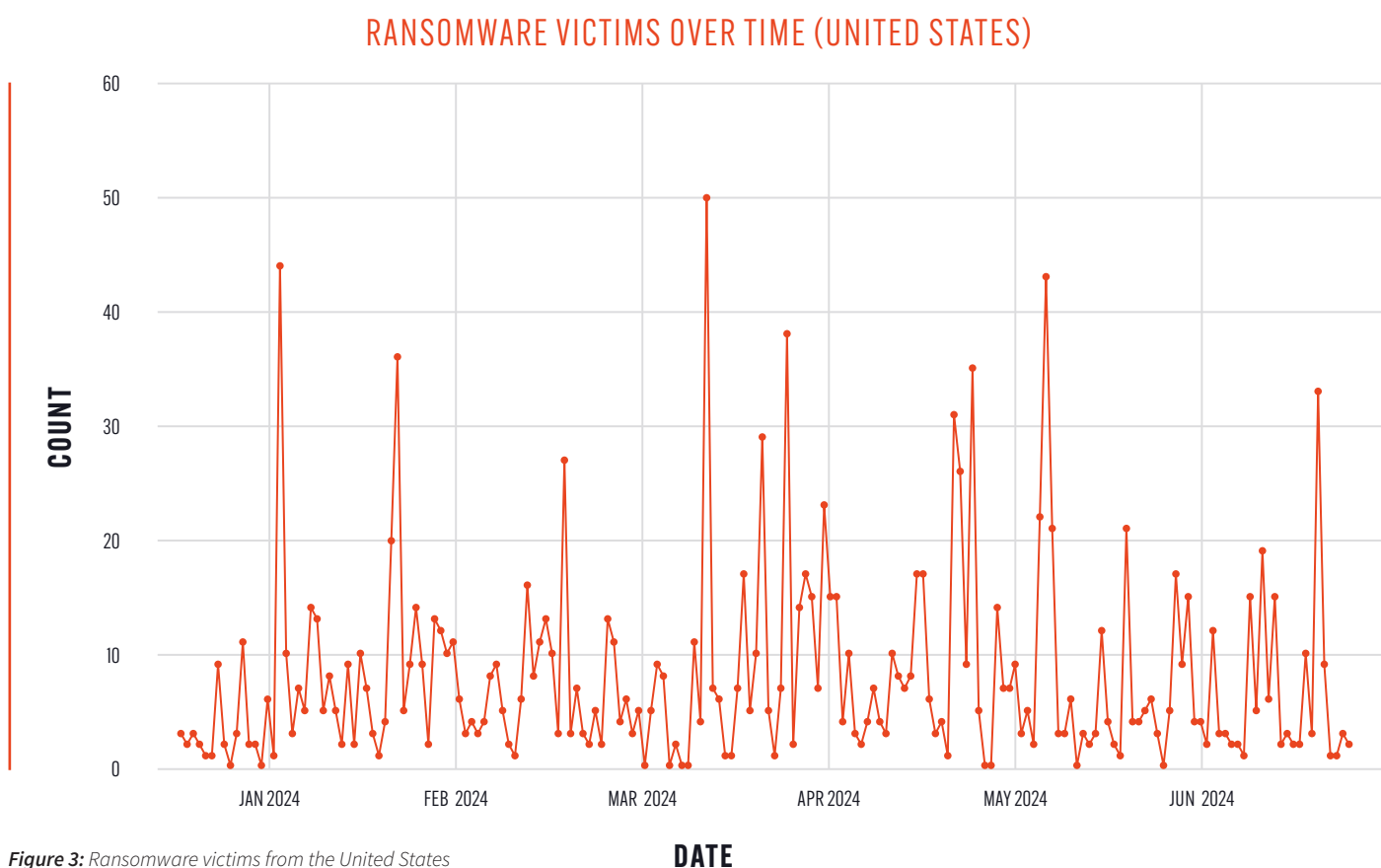
Blitz: 1800\$

**Figure 2:** An Initial Access Broker auctions access to a US-based healthcare organization on the Exploit hacking forum.

# RANSOMWARE

The United States is targeted by ransomware operations more than any other nation. According to our data, more than 1,400 entities in the USA have been listed as a victim of ransomware gangs since the beginning of 2024.

The war against ransomware is relentless. As seen in **Figure 3**, US-based victims have been targeted constantly over the course of the year, with only rare exceptions where no victims were announced over a 24 hour period. Through our constant monitoring of ransomware leak sites we have also observed noticeable spikes, with more than 15 instances when 20 or more ransomware victims in the USA were announced in a single day.



**Figure 3:** Ransomware victims from the United States listed over the course of 2024.

Once again, we have to note that these figures are actually a conservative estimate of the total number of victims, as they only account for those that have been publicly listed on ransomware groups' dark web leak sites. Many smaller ransomware groups do not use leak sites and even those that do have leak sites won't name every victim, often only listing organizations to apply pressure if the business refuses to pay the ransom.

<sup>4</sup> <https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/>

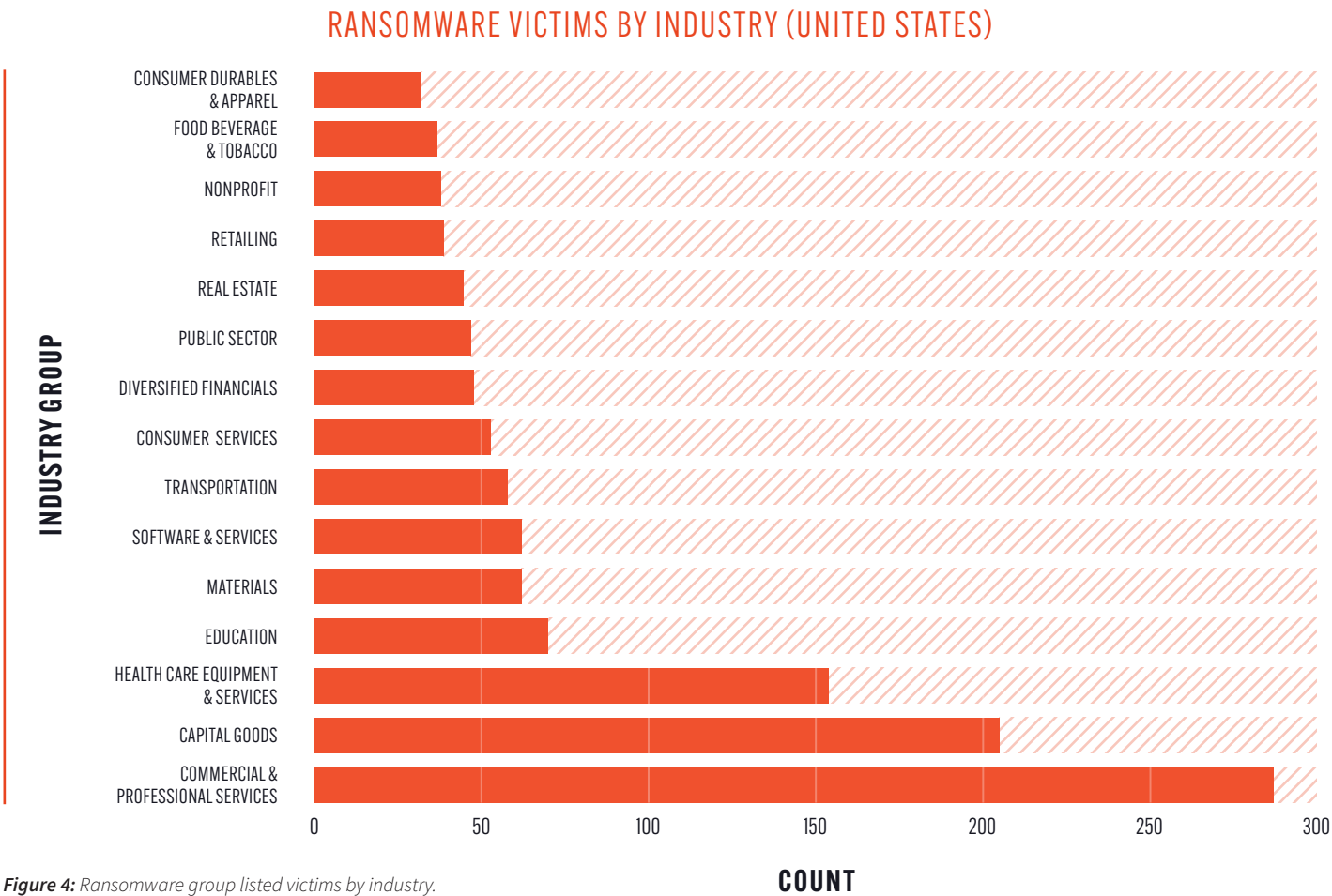


According to reports,<sup>4</sup> more than 50 percent of ransomware victims choose to pay the demanded ransom after negotiation, with an average payout of US \$2 million, making ransomware attacks against organizations in the USA a very lucrative business for cybercriminals.

Based on our data, the ransomware gang with the most claimed US-based victims in 2024 so far is **LockBit**, with 255 entities posted on their leak site, followed by **Play** with 142 victims, **IncRansom** with 113, **BianLian** with 76, and **Cactus** with 65 claimed victims.



**Figure 4** shows the most commonly targeted industries in the United States in 2024. Approximately 285 victims from the Commercial & Professional Services industry were targeted, followed by 204 entities active in the Capital Goods industry, and 154 victims from the Health Care Equipment & Services industry.



**Figure 4:** Ransomware group listed victims by industry.

# HACKTIVISM



We decided to visit the Los Angeles Police Department again. We have disabled the official website of the Los Angeles Police Department.

✗ <https://www.lapdonline.org/>

★ <https://check-host.net/check-report/1b2231a4k279>

#DARKSTORM

#Opusa

#Opisrael



<https://www.airport-la.com> | Los Angeles Airport

<https://check-host.net/check-report/11d0d361k610>

Attack time: 1 hour

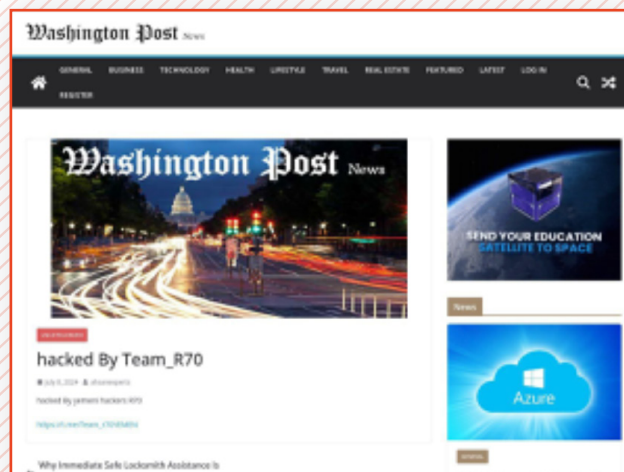
#DARKSTORM

#Opusa

**Figure 5:** Posts from the hacktivist group Team Dark Storm claiming attacks on the Los Angeles police department and airport.

Hacktivists are a different category of threat actors to financially motivated cybercriminals like ransomware gangs and Initial Access Brokers. They are generally not looking to obtain financial benefit from their attacks but instead are looking to make a point by disrupting entities who have opposing views - typically related to religion, geopolitics, historical or present events, or have affiliation to specific international alliances.

Hacktivists typically use the messaging app Telegram to recruit or attract supporters, as well as to advertise their operations and boast about their selection of victims and the disruption they have caused (see examples in **Figures 5 - 9**). This desire for notoriety and publicity also differentiates them from financially motivated cybercriminals, who typically do not want to draw any more attention to themselves than is strictly necessary for conducting their attacks.



Washington Post news hacked by Team\_R70

<https://wpostnews.com/>

#Yemeni\_hackers

#Team\_R70

#USA

**Figure 6:** The hacktivist group Team\_R70 claims an attack on the Washington Post.

The damage from hackers groups is often minimal and short term, as they favor tactics including Distributed Denial-of-Service (DDoS) attacks and website defacement that usually only have a temporary impact. Occasionally hackers do undertake data exfiltration operations, which are more damaging in the long term.

The USA has been targeted by hackers in several contexts, with entities often selected due to the country's association with NATO. More recently, hackers launched attacks against the United States due to its military and financial backing of Ukraine and Israel. At the time of writing this report, hacker attention was centered on the 2024 NATO summit taking place in Washington, D.C (**Figures 8 & 9**).

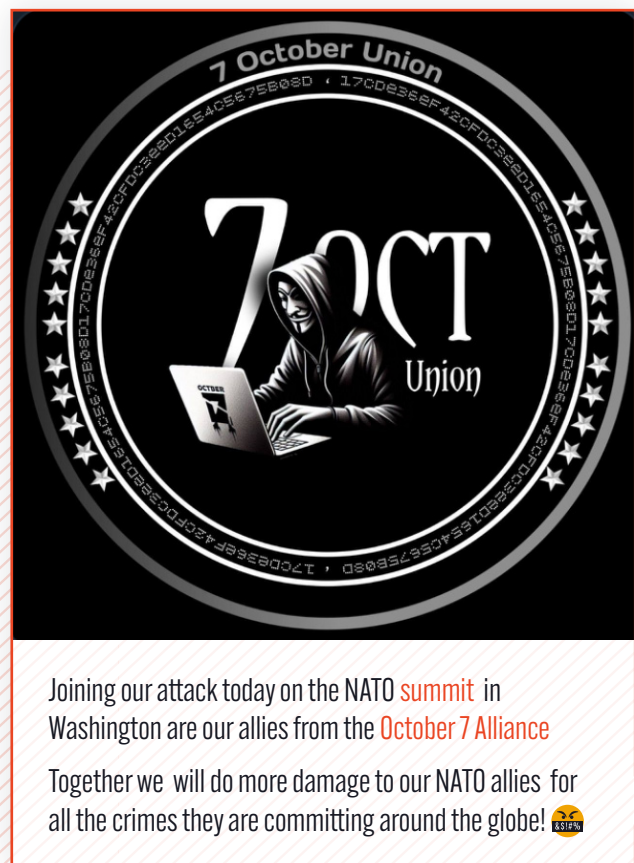


**Figure 7:** The hacker group Gloriamist India threatens the USA.



Today in Washington begins another summit of war criminals from NATO. We, with our friends from People's Cyber Army and UserSec stopped by this coven of Russophobes and "cleaned up" 🐼

**Figure 8:** The hacker group NoName057(16) claims to have collaborated with other hacker groups to DDoS several NATO related websites: NATO Centers of Excellence (COEs), NATO Science and Technology Organization, Authorization on the NATO NEC CCIS Support Center Portal, NATO Forum Partner, NATO's Special Operations Forces Command (SOFCOM), NATO Munitions Safety Information and Analysis Center (MSIAC) portal.



**Figure 9:** The 7 October Union, a collaboration between several different hacker groups, threatens attacks against the NATO summit.



## ELECTIONS

The motivation behind targeting entities involved in elections in a foreign country is also geopolitical. However, the capabilities required to execute a successful campaign require more resources than the typical hacktivist group possesses - and typically involve government backing - which means that this activity falls into the realm of state-backed cyberwarfare.

The US has historically been targeted both before and during elections, with demonstrated interference of the [Russian government in the 2016 Election](#)<sup>5</sup> and of [Iran in the 2020 Election](#)<sup>6</sup>. As the 2024 presidential election gets closer, there is the possibility of new campaigns that aim to influence, disrupt, or discredit the election.

Even since 2020 technology has developed significantly, opening up the possibility of new attacks by hackers. For example, due to the greater prevalence of capability of generative artificial intelligence it has been [assessed as likely](#)<sup>7</sup> that state-backed actors attempt to use deepfakes and other computer generated materials to spread misinformation in order to influence voters. Video deepfakes have already been observed in the US, for example in videos [featuring altered footage](#)<sup>8</sup> of Nancy Pelosi, Alexandria Ocasio-Cortez, and Joe Biden in 2023.

Threat actors will also try to monetize data with information related to elections. In May 2024 we observed a member of BreachForums trying to sell a database allegedly exfiltrated from the Virginia Department of Elections with about 6,500 rows of data (**Figure 10**). Subsequently, a forum moderator, the notorious actor IntelBroker, offered the data for free. Our analysis indicated the data was likely downloaded from a publicly available resource.

### ELECTIONS.VIRGINIA.GOV - VIRGINIA DEPT. OF ELECTIONS

🕒 8th May 2024, 04:02:46 pm // Posted on [BreachForums](#)

🕒 9th Jul 2024, 01:11:05 pm

🌐 English

- Posted by [pwms3c](#)

Virginia Dept. of Elections: Home  
Contains data on election results.

Timestamp, Username, Election, Source, Locality, Precinct, Contest, Choice, VotingMethod, FieldName, PreviousValue, ChangeReason, Comments, PrecinctID, PrecinctName, DistrictID, DistrictType, DistrictName, OfficeID, OfficeTitle, ElectionID, ElectionType, ElectionDate, ElectionName, NumberOfSeats

The "/" represents different files.

Records: 6.5K

Sample 1:

**Figure 10:** A threat actor claims to be selling a database related to election results on BreachForums.

In a similar incident in October 2023, a ransomware group known as RansomedVC claimed to have compromised and exfiltrated data from District of Columbia Board of Elections (DCBOE). The gang announced that they were looking to sell the data containing voter information, while releasing sample data via their dark web leak site. Although the gang is no longer active, the text of the sales advertisement captured in our dark web intelligence platform is shown in **Figure 11**.

### **(SALE) DISTRICT OF COLUMBIA ELECTIONS 600K LINES VOTERS DATA**

**Last Updated:** 2023-10-13T09:19:07.244377

We have successfully breached the District of Columbia Board Of Elections and have gotten more than 600k lines of USA Voters: see a small sample here: <https://paste.ec/raw/UhDgH818#ub86MOR2-yKYUVcuZRbXXW5hQzBXYIHWtmvntzHSEE1>

Contact us at <https://t.me/RansomedSupport>

**Figure 11:** RansomedVC posts a sample of DCBOE data on their dark web leak site.



<sup>5</sup> <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>

<sup>6</sup> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a>

<sup>7</sup> <https://apnews.com/article/election-interference-facebook-tiktok-russia-putin-china-1b5e5ce56d64dc356c2ad332068e2f8c>

<sup>8</sup> <https://www.reuters.com/article/fact-check/video-features-deepfakes-of-nancy-pelosi-alexandria-ocasio-cortez-and-joe-biden-idUSL1N36V2E0/>



## COMMON VULNERABILITIES AND EXPOSURES (CVE)

Improper setup or the use of outdated software can allow threat actors to exploit vulnerable systems to conduct their attacks. For example, some of the Initial Access Brokers already discussed in this report actively scan for vulnerabilities to exploit as their main attack vector.


Typically, most vulnerabilities are found by the software developers before they are weaponised in the wild - with “zero day” vulnerability attacks being relatively rare. However, applying patches to vulnerable software is a time consuming and resource-intensive process, which means that organizations are often caught out by known vulnerabilities that simply have not been addressed in time.

In mid-2023, the notorious ransomware group Cl0p leveraged the [CVE-2023-34362](#)<sup>9</sup> SQL injection vulnerability found in the MOVEit Transfer file transfer solution. A patch was released a couple of days after the vulnerability was discovered, however attacks continued. **In total**,<sup>10</sup> more than 2,600 victims were impacted, with almost 2,300 of those being US-based.

More recently, a vulnerability that allowed remote code execution in OpenSSH’s server and tracked as [CVE-2024-6387](#)<sup>11</sup> was discovered. A patch was released on July 1st 2024, however, two weeks later, we observed that approximately 288,000 US-based systems were still vulnerable. Of course, this quickly became a topic of interest for threat actors, who we have observed sharing proof-of-concept exploits and engaging in discussions on cybercrime forums, as seen in **Figure 12**.

### CVE-2024-6837 REGRESSHION

🕒 12th Jul 2024, 03:52:27 am // Posted on [BreachForums](#)

🕒 12th Jul 2024, 03:52:27 am  English  
- Posted by [itspizzatime](#)

----BEGIN PGP SIGNED MESSAGE---

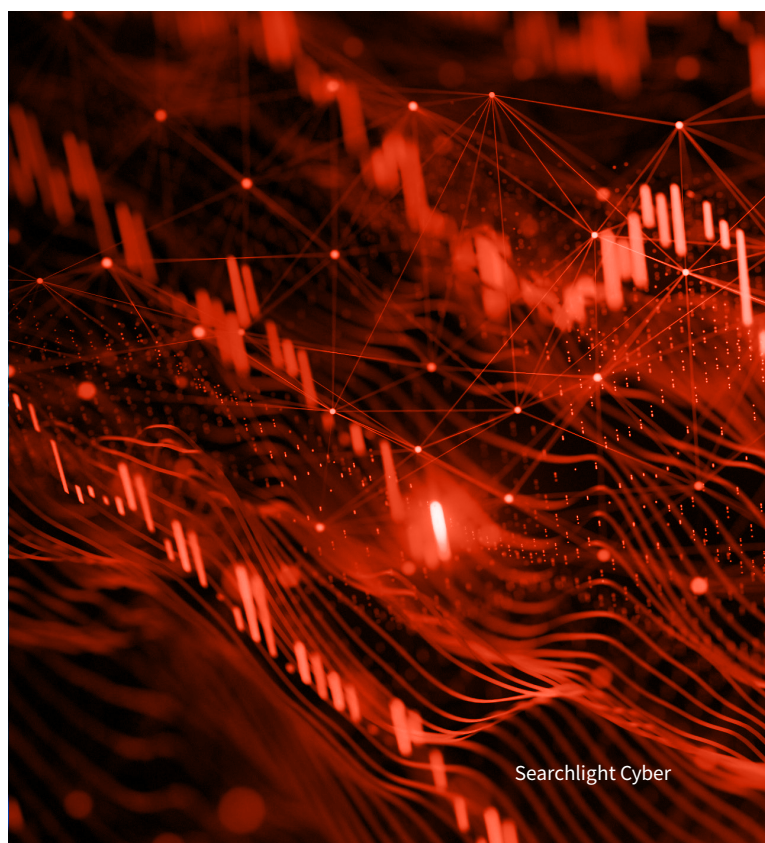
Hasg: SHA512

Hello BreachForum Users!

I'm sure you all might have heard of a recent vulnerability by the user of RegreaSSHion. RegreSSHion, CVE-2024-6387, is an unauthenticated remote code execution in OpenSSH's sever (sshd) that grants full root access. It affects the default configuration and does not require user interaction. This exploit is also on the CISA known culns list.

Today I'm posting a POC, I'm not the original creator; source: xonoxitron

**Figure 12:** A threat actor on BreachForums shares a proof of concept (POC) exploit for CVE-2024-6387.



Another vulnerability that could allow an attacker to execute arbitrary code was recently found in the GlobalProtect feature of Palo Alto Networks PAN-OS software ([CVE-2024-3400](#))<sup>12</sup>. The vendor quickly released patches in April 2024, however, in July we found over 31,000 vulnerable systems located in the USA alone. Moreover, we have observed a notorious threat actor offering to sell a private exploit for this vulnerability on a cybercrime forum (**Figure 13**).

## [SELL] EXPLOITS

🕒 26th Jul 2022, 03:31:00 am // Posted on [Exploit](#)

🕒 26th May 2024, 03:39:00 pm 🌐 English  
- Posted by [LORD1](#)

- \*+ GlobalProtect RCE\* (CVE-2024-3400)
- \*+ Fortinet FortiOS RCE\* (CVE-2024-21762)
- \*+ CrushFTB RCE\* (CVE-2024-4040)
- \*+ ScreenConnect RCE\* (CVE-2024-1709)
- \*+ Jenkins Exploit\* (CVE-2024-23897)

**Figure 13:** A threat actor offers to sell exploits for a number of vulnerabilities on the dark web forum Exploit, including CVE-2024-3400 in Palo Alto Networks' PAN-OS software.

<sup>9</sup> <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34362>

<sup>10</sup> <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html>

<sup>11</sup> <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6387>

<sup>12</sup> <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-3400>

## FRAUD AND STOLEN GOODS

The dark web also fosters a community of scammers and fraudsters looking to make money out of individuals, rather than enterprises. These fraudsters target personally identifiable information, bank account data, credit card information, and social security numbers that could be leveraged to steal money. When direct monetization is not feasible, fraudsters choose to sell the data to more capable actors. Fraudsters typically obtain this information using the following methods:

### ➤ SOCIAL ENGINEERING

Specially crafted phishing websites, often sent to victims via SMS or email to trick them into believing they are communicating with a legitimate service. Fraudsters also call victims (a technique known as voice-phishing or vishing) as a direct conversation is often a successful route to convincing an individual into handing over their personal details.

### ➤ INFORMATION-STEALER MALWARE

Also known as Infostealers, this is a specific type of software that is designed to infect a victim's device and extract data including credentials, cookies, and keylogs.

### ➤ INSIDER THREATS

Rogue employees within an organization who exploit their access to customer data, selling it on to criminals for financial gain.

**Figure 14** is an advertisement on Telegram for data that was likely obtained using one of the methods described above. Based on the type of services provided, denominations, and the acronyms of the exploited governmental entities and services (DEA - Drug Enforcement Administration, EIN - Employer Identification Number, MVR - Motor Vehicle Records, etc.), it is clear that the seller has specifically targeted US-based individuals.

**Figure 15** is more explicit: this vendor is selling credit cards (CCS) from the USA, obtained through a phishing website.

I can provide

- 🚀 **FAKE IDS and DRIVING LICENSE**
- 🚀 **SSN LOOKUP + DOB**
- 🚀 **DL LOOK UP + DOB**
- 🚀 **TLO LOOK UP**
- 🚀 **MMN LOOK UP**
- 🚀 **MVR LOOK UP**
- 🚀 **DEA LOOK UP**
- 🚀 **EIN / Tax ID Look up**
- 🚀 **TLOxp Account**
- 🚀 **VIN Lookup**
- 🚀 **Background Check + SSN**
- 🚀 **Business FULLZ**
- 🚀 **Passports**
- 🚀 **SIM SWAP**
- 🚀 **pros available all states**

And many more.....

**Figure 14:** A criminal advertises data related to organizations in the United States in a Telegram channel dedicated to fraud.

**N** Update 06/07



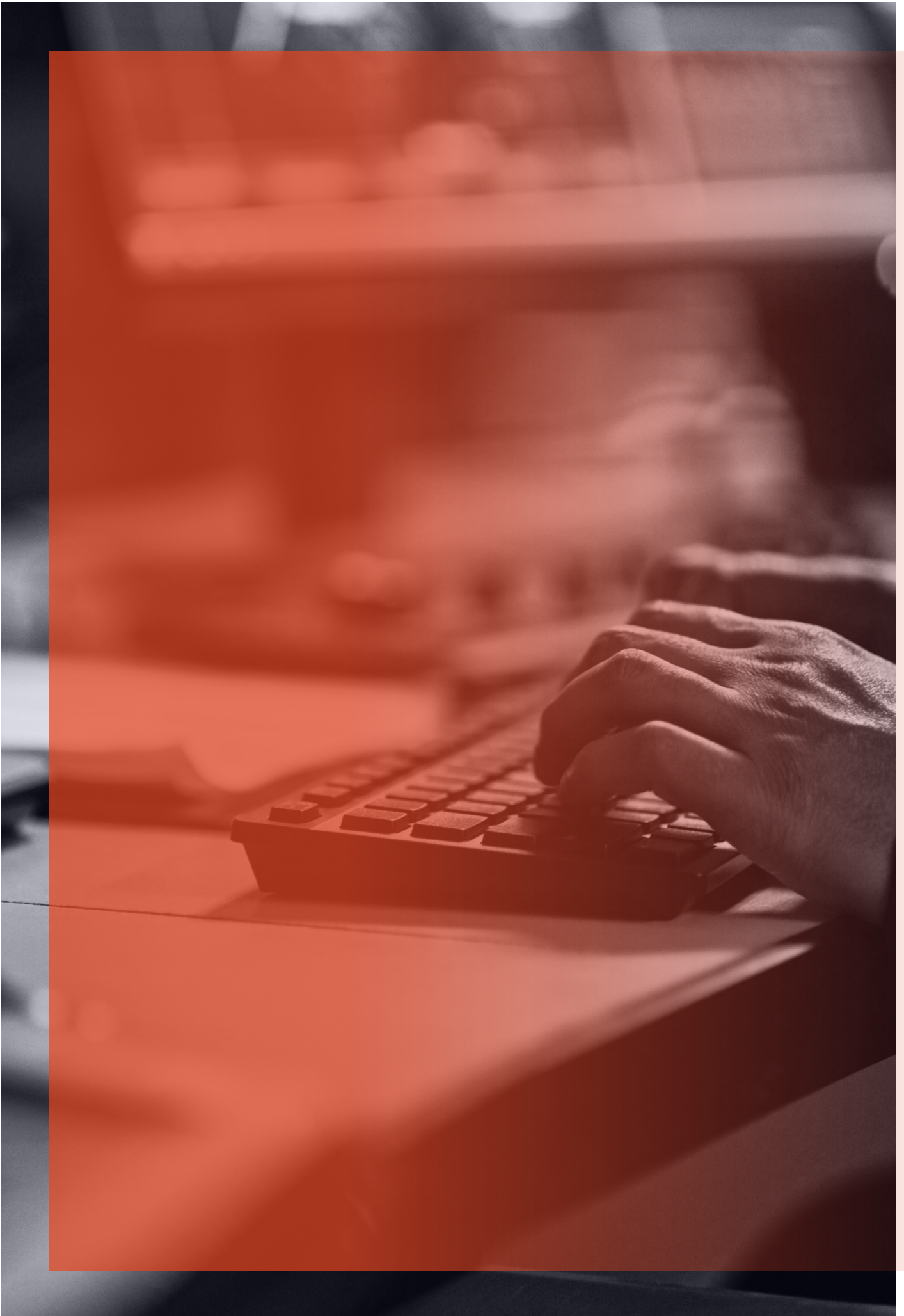
Fresh USA CCS 2520 updates



All our CCS are obtained through phishing website in the picture ensures that every CC sold is live and fresh

**Figure 15:** A criminal offers credit card data from customers in the United States, obtained through a phishing website.





# THE USA FROM THE CYBERCRIMINAL'S PERSPECTIVE

## CONCLUSION

Having visibility into the dark web plays a crucial role in successfully defending your organization against cyber threats. It is significantly easier to keep up with adversaries' techniques, tactics and procedures (TTPs) when you have access to their “safe-space”, such as underground forums and instant messaging platforms. Cybercrime is a continuously evolving landscape and threat actors will always look to find new ways to conduct attacks, either for obtaining monetary benefits or just for feeding their ego.

Historic data suggests the United States will remain a target for threat actors looking to conduct lucrative cyberattacks that are, at the same time, devastating for the victims. The examples in this report demonstrate the flexibility and adaptability of threat actors in developing the next scheme to exploit or disrupt their target. Gathering dark web intelligence is key to understanding the attack landscape and choosing the defenses that need to be put in place to keep organizations secure.

### Other tips to help protect your assets:

#### ➤ **EDUCATE CUSTOMERS AND EMPLOYEES**

Awareness about common threats is vital, employees are often viewed as a weak link even in a mature cybersecurity program, while customers should be able to detect a fraudulent call during a vishing attempt.

#### ➤ **CONSIDER A PROACTIVE APPROACH TO VULNERABILITY MANAGEMENT**

Those responsible with network and infrastructure security should stay up to date with the latest CVEs and continuously update and monitor their systems.

#### ➤ **MONITOR THE DARK WEB FOR PRE-ATTACK INTELLIGENCE**

A solution like Searchlight Cyber can help cyber security teams keep a close eye on the newest methods discussed by threat actors on the dark web, allowing them to secure systems before hackers get a chance to put their endeavors into practice.



**IT IS SIGNIFICANTLY EASIER TO KEEP UP WITH ADVERSARIES' TECHNIQUES, TACTICS AND PROCEDURES (TTPS) WHEN YOU HAVE ACCESS TO THEIR “SAFE-SPACE”**



## GATHERING DARK WEB INTELLIGENCE

Criminals use the dark web to plan their attacks, share tactics, and buy the resources they need because they believe its anonymity will stop them from being identified. However, this makes the dark web an invaluable source of intelligence on the criminal ecosystem - and provides security teams with a unique insight into the cybercriminal perspective on their business.

Gathering intelligence from the dark web can help organizations to identify the cybercriminals that are targeting their geography, industry, or even their specific company - understand their tactics - and adjust their security strategy accordingly. This visibility into cybercriminal activity outside of the network gives organizations a rare opportunity to act before the threat actor has launched their attack, meaning that breaches can be completely avoided.

Governments, law enforcement agencies, and enterprises around the world use Searchlight Cyber's dark web investigation and monitoring tools in their fight against criminal activity on the dark web:

### DARK WEB INVESTIGATION



#### DARK WEB SEARCH

Query more than 15 years of dark web data gathered from forums, marketplaces, hidden sites, cybercriminal communication channels, and more.



#### STEALTH BROWSER

Safely access dark web sites through a secure virtual browser to gather threat intelligence on cybercriminals directly from the source.



#### RANSOMWARE SEARCH AND INSIGHTS

Track and investigate the dark web activity of the most active ransomware groups through a continuously updated dashboard.

### DARK WEB MONITORING



#### ATTRIBUTE-BASED MONITORING

Continuously scan the dark web for attributes related to your organization - including domains, ports, IP addresses, and employee credentials.



#### DARK WEB TRAFFIC MONITORING

Monitor traffic to and from an organization's network and Tor, a reliable signal of malicious activity.



#### EXTERNAL ATTACK SURFACE MONITORING

Identify IP address and port vulnerabilities by using dark web exposure analysis to assess your footprint beyond your perimeter.



VISIT [WWW.SLCYBER.IO](http://WWW.SLCYBER.IO) TO FIND  
OUT MORE OR BOOK A DEMO NOW.

**UK HEADQUARTERS**

Suite 63, Pure Offices,  
1 Port Way, Port Solent,  
Portsmouth PO6 4TY  
United Kingdom

**US HEADQUARTERS**

200 Massachusetts  
Avenue Northwest,  
Washington, DC 20001  
United States