

# 20160614A: Russia-based Groups Compromise Democratic National Committee



**Type**  
Incident

**Owner**  
Common Community

**Event Date**  
06/14/2016

**Date Added**  
06/19/2016

## Description

As of 14 June 2016, two sophisticated, advanced persistent threat (APT) groups compromised the computer systems of the U.S. Democratic National Committee (DNC). The groups - referred to as Cozy Bear and Fancy Bear by CrowdStrike - are both believed to have a nexus to Russia and conduct cyber espionage operations likely pursuant to the intelligence collection requirements of the Government of the Russian Federation.

According to the CrowdStrike publication describing their investigation of the compromise, evidence indicates the two groups had access to the same systems at the same time, but were not working together. Cozy Bear compromise of the DNC dates back to at least the summer of 2015. The Fancy Bear compromise likely occurred in April 2016. Analysis has not revealed any indication of collaboration between the two threat actors, "or even an awareness of one by the other."

The Cozy Bear compromise primarily leveraged an implant called SeaDaddy that was developed in Python. This malware was compiled with py2exe and a Powershell backdoor which enabled the threat actors to establish persistence on the compromised computer systems and easily make changes to the malware's functionality and command and control infrastructure. The Powershell backdoor is made up of only one line of code, but that one line contains a command that establishes an encrypted communication channel to Cozy Bear c2 infrastructure and downloads additional Powershell modules. The malware was designed to evade detection and analysis efforts, and used different encryption keys for communications from each infected system. To facilitate lateral movement, Cozy Bear used a variant of the MimiKatz tool to steal credentials.

The Fancy Bear compromise of the DNC involved different tradecraft. The group leveraged X-Agent malware which can be used to execute commands on infected systems from a remote location. The malware can also send files and keystroke logs to the threat actor's c2 infrastructure.

# 20160614A: Russia-based Groups Compromise

## Democratic National Committee

Incident Report

It is not uncommon for sophisticated cyber threat actors to target presidential candidates and political parties ahead of an election. Given the world attention garnered by the current U.S. presidential campaign, it is likely threat actors, such as Cozy Bear and Fancy Bear, have been directed to collect information on the candidates in order to better understand each candidate's position on a variety of issues. Such targeting will likely continue until the U.S. election in November.

### Tags

Advanced Persistent Threat | Cozy Bear | DNC | Powershell | SeaDaddy Implant | U.S. Presidential Election | X-Agent | X-Tunnel | apt

### Attributes

#### Attribution Assessment

Cozy Bear and Fancy Bear have been active for several years. These two groups are considered some of the most advanced, sophisticated adversaries globally. Both groups regularly conduct political and economic espionage to benefit the Government of the Russian Federation. Additionally, Cozy Bear and Fancy Bear are believed to have close ties to the Russian Government's intelligence services which are highly advanced, powerful, capable, and well resourced.

These groups are persistent in their

#### Adversary Origin & Source

Russia

#### Source

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

# 20160614A: Russia-based Groups Compromise

## Democratic National Committee

Incident Report

### Associated Indicators



MD5:CC9E6578A47182A941A478B276320E06

SHA1:CB872EDD1F532C10D0167C99530A65C4D4532A1E

SHA256:40AE43B7D6C413BECC92B07076FA128B875C8DBB4DA7C036639ECCF5A9FC784F

**Type**  
File

**Date Added**

06/19/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Confirmed

(100/100)



MD5:004B55A66B3A86A1CE0A0B9B69B95976

SHA1:F09780BA9EB7F7426F93126BC198292F5106424B

SHA256:4845761C9BED0563D0AA83613311191E075A9B58861E80392914D61A21BAD976

**Type**  
File

**Date Added**

06/19/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Confirmed

(100/100)

# 20160614A: Russia-based Groups Compromise

## Democratic National Committee

Incident Report

MD5:19172B9210295518CA52E93A29CFE8F4

SHA1:0B3852AE641DF8ADA629E245747062F889B26659

SHA256:FD39D2837B30E7233BC54598FF51BDC2F8C418FA5B94DEA2CADB24CF40F395E5



**Type**  
File

**Date Added**

06/19/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Confirmed

(100/100)

MD5:9E7053A4B6C9081220A694EC93211B4E

SHA1:E2B98C594961AAE731B0CCEE5F9607080EC57197

SHA256:B101CD29E18A515753409AE86CE68A4CEDBE0D640D385EB24B9BBB69CF8186AE



**Type**  
File

**Date Added**

06/19/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Confirmed

(100/100)

# 20160614A: Russia-based Groups Compromise Democratic National Committee

Incident Report

MD5:CE227AE503E166B77BF46B6C8F5EE4DA

SHA1:74C190CD0C42304720C686D50F8184AC3FADDBE9

SHA256:6C1BCE76F4D2358656132B6B1D471571820688CCDBACA0D86D0CA082B9390536



**Type**  
File

**Date Added**

06/19/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Confirmed

(100/100)



**23.227.196.217**

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Unknown

# 20160614A: Russia-based Groups Compromise Democratic National Committee

Incident Report



45.32.129.185

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Unknown



185.86.148.227

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Unknown

# 20160614A: Russia-based Groups Compromise Democratic National Committee

Incident Report



187.33.33.8

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Unknown



218.1.98.203

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Unknown

# 20160614A: Russia-based Groups Compromise Democratic National Committee

Incident Report



58.49.58.58

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

Critical

(5/5)

**Confidence**

Unknown



185.100.84.134

**Type**  
Address

**Date Added**

06/15/2016

**Description**

Bears in the Midst

**Source**

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

**Rating**

High

(4/5)

**Confidence**

Unknown