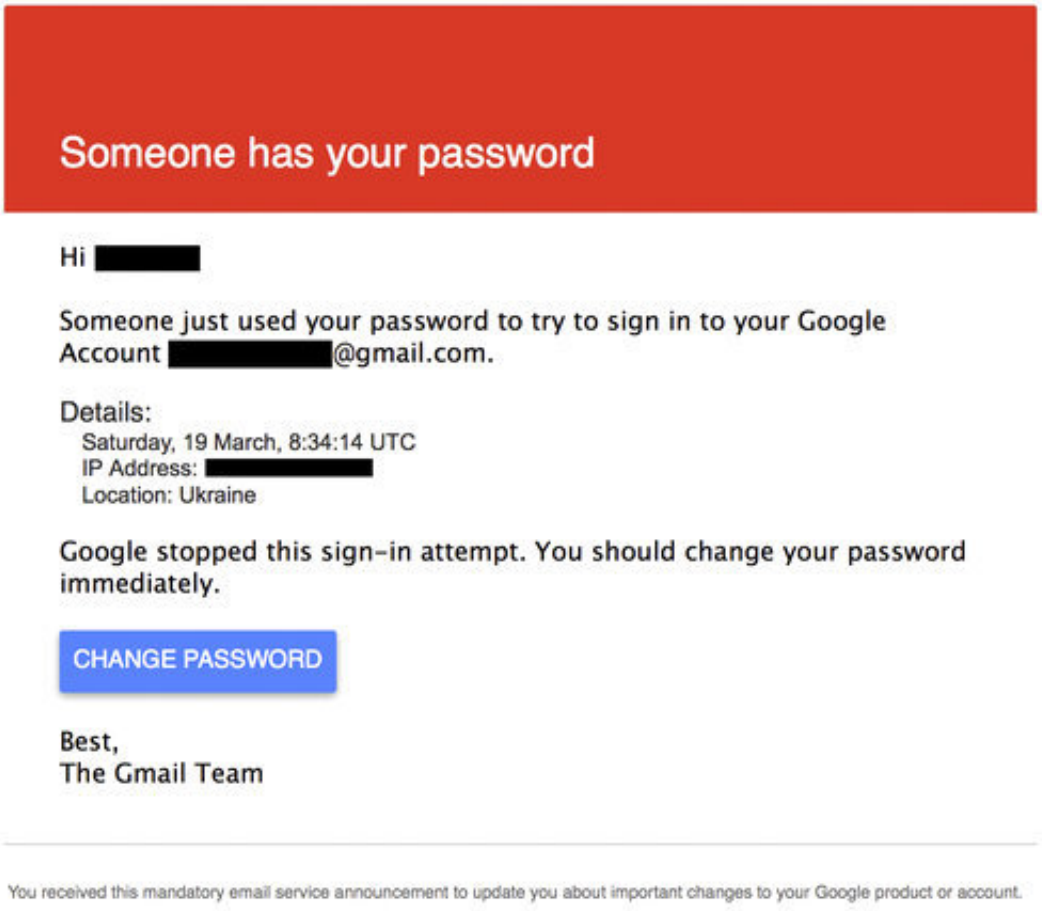
# Inside story: How Russians hacked the Democrats' emails

November 3 2017, by Raphael Satter, Jeff Donn And Chad Day




This image shows a portion of a phishing email sent to a Hillary Clinton campaign official on March 19, 2016. An Associated Press investigation into the hackers who disrupted the 2016 U.S. presidential contest has found that they tried to compromise a far wider group of people than has previously been reported using malicious messages like this one. The investigation leaves little doubt that whoever masterminded the intrusions worked in close alignment with

the Kremlin's interests. The email address of the recipient has been redacted to protect their privacy. (AP Photo)

It was just before noon in Moscow on March 10, 2016, when the first volley of malicious messages hit the Hillary Clinton campaign.

The first 29 phishing emails were almost all misfires. Addressed to people who worked for Clinton during her first presidential run, the messages bounced back untouched.

Except one.

Within nine days, some of the campaign's most consequential secrets would be in the hackers' hands, part of a massive operation aimed at vacuuming up millions of messages from thousands of inboxes across the world.

An Associated Press investigation into the digital break-ins that disrupted the U.S. presidential contest has sketched out an anatomy of the hack that led to months of damaging disclosures about the Democratic Party's nominee. It wasn't just a few aides that the hackers went after; it was an all-out blitz across the Democratic Party. They tried to compromise Clinton's inner circle and more than 130 party employees, supporters and contractors.

While U.S. intelligence agencies have concluded that Russia was behind the email thefts, the AP drew on forensic data to report Thursday that the hackers known as Fancy Bear were closely aligned with the interests of the Russian government.

The AP's reconstruction— based on a database of 19,000 malicious links

recently shared by cybersecurity firm Secureworks—shows how the hackers worked their way around the Clinton campaign's top-of-the-line digital security to steal chairman John Podesta's emails in March 2016.

It also helps explain how a Russian-linked intermediary could boast to a Trump policy adviser, a month later, that the Kremlin had "thousands of emails" worth of dirt on Clinton.

In this Wednesday, Nov. 9, 2016 file photo, John Podesta, Hillary Clinton campaign chairman, walks off the stage after announcing that Clinton will not be making an appearance at Jacob Javits Center in New York as the votes were still being counted. Data from the threat intelligence firm Secureworks shows a malicious link being generated by the hacking group Fancy Bear for Podesta on March 19, 2016 at 11:28 a.m. Moscow time; Documents subsequently published by WikiLeaks show that the rogue email arrived in his inbox six minutes later. The link was clicked twice. Podesta's messages—at least 50,000 of them—were in the hackers' hands. (AP Photo/Matt Rourke)

———

PHISHING FOR VICTIMS

The rogue messages that first flew across the internet March 10 were dressed up to look like they came from Google, the company that provided the Clinton campaign's email infrastructure. The messages urged users to boost their security or change their passwords while in fact steering them toward decoy websites designed to collect their credentials.

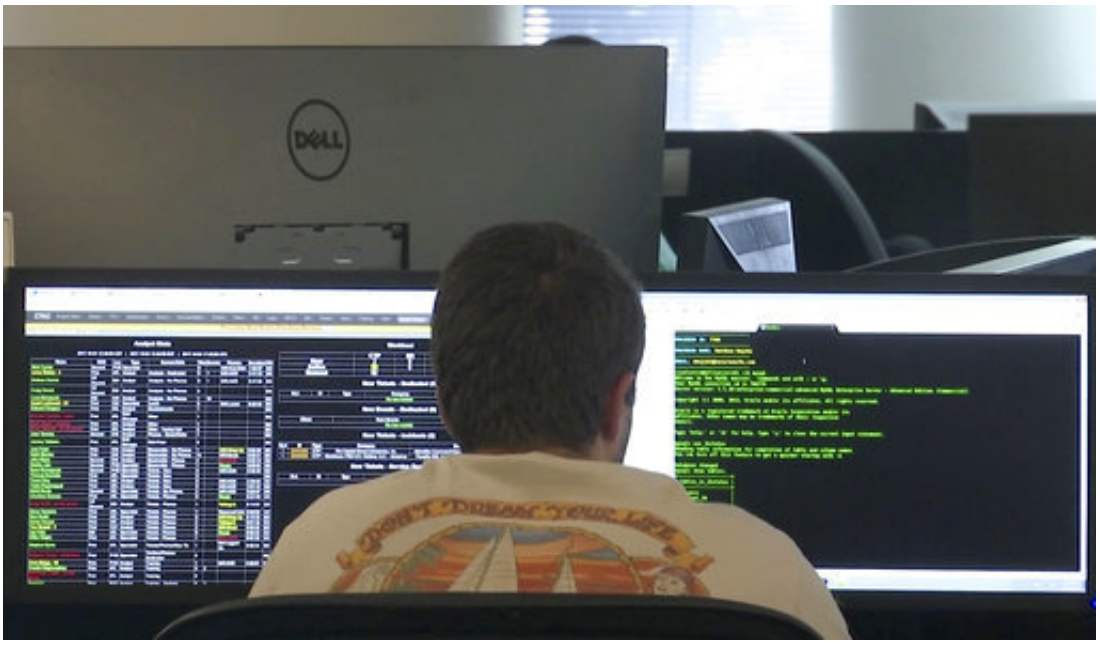
One of the first people targeted was Rahul Sreenivasan, who had worked as a Clinton organizer in Texas in 2008—his first paid job in politics. Sreenivasan, now a legislative staffer in Austin, was dumbfounded when told by the AP that hackers had tried to break into his 2008 email—an address he said had been dead for nearly a decade.

"They probably crawled the internet for this stuff," he said.

Almost everyone else targeted in the initial wave was, like Sreenivasan, a 2008 staffer whose defunct email address had somehow lingered online.

But one email made its way to the account of another staffer who'd worked for Clinton in 2008 and joined again in 2016, the AP found. It's possible the hackers broke in and stole her contacts; the data shows the phishing links sent to her were clicked several times.

Secureworks' data reveals when phishing links were created and indicates whether they were clicked. But it doesn't show whether people entered their passwords.



Seen though an interior window, an employee looks at computer screens in the offices of Secureworks in Atlanta on Oct. 4, 2017. Nineteen thousand lines of targeting data obtained from threat intelligence firm Secureworks lays out in unprecedented detail who the hackers tried to compromise, providing a minute-by-minute look at how the group often dubbed "Fancy Bear" penetrated the Democratic National Committee, tried to break into the Clinton campaign and eventually stole chairman John Podesta's emails. (AP Photo/Marina Hutchinson)

Within hours of a second volley emailed March 11, the hackers hit pay dirt. All of a sudden, they were sending links aimed at senior Clinton officials' nonpublic 2016 addresses, including those belonging to longtime Clinton aide Robert Russo and campaign chairman John Podesta.

The Clinton campaign was no easy target; several former employees said the organization put particular stress on digital safety.

Work emails were protected by two-factor authentication, a technique

that uses a second passcode to keep accounts secure. Most messages were deleted after 30 days and staff went through phishing drills. Security awareness even followed the campaigners into the bathroom, where someone put a picture of a toothbrush under the words: "You shouldn't share your passwords either."

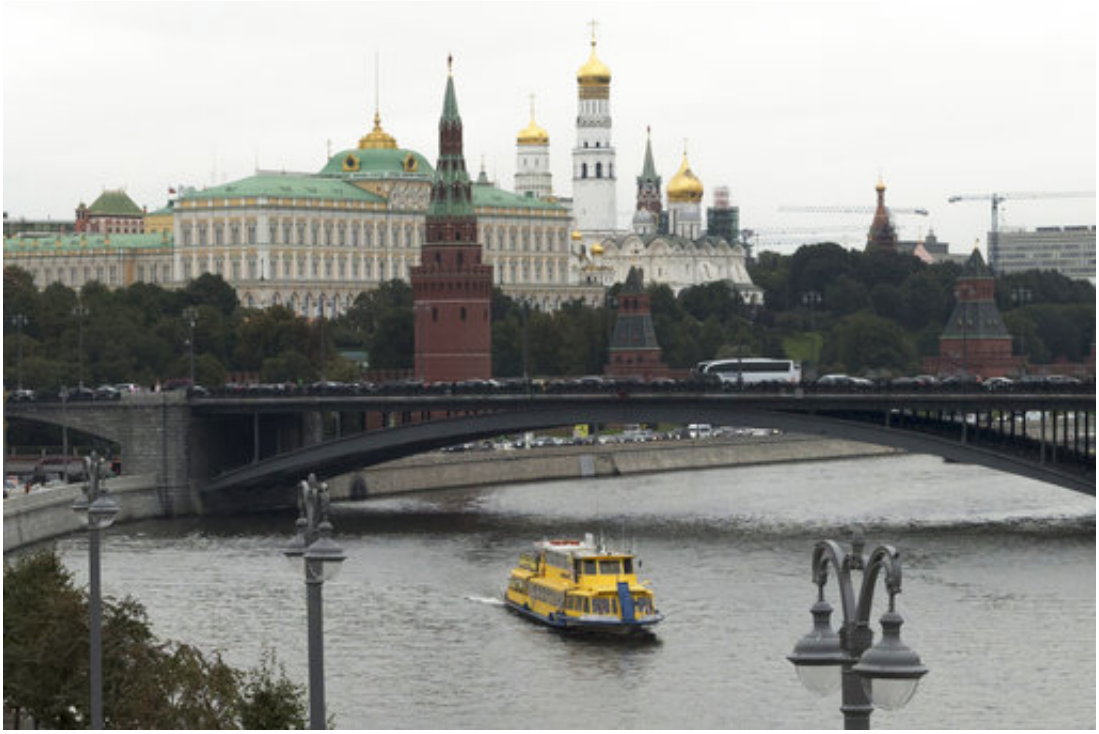
Two-factor authentication may have slowed the hackers, but it didn't stop them. After repeated attempts to break into various staffers' hillaryclinton.com accounts, the hackers turned to the personal Gmail addresses. It was there on March 19 that they targeted top Clinton lieutenants—including campaign manager Robby Mook, senior adviser Jake Sullivan and political fixer Philippe Reines.

A malicious link was generated for Podesta at 11:28 a.m. Moscow time, the AP found. Documents subsequently published by WikiLeaks show that the rogue email arrived in his inbox six minutes later. The link was clicked twice.

Podesta's messages—at least 50,000 of them—were in the hackers' hands.

___

A SERIOUS BREACH



This Friday, Sept. 29, 2017 photo shows the Kremlin in Moscow. The hackers who intervened in America's 2016 presidential contest cast their net far wider than has previously been reported, The Associated Press has found. Data obtained from threat intelligence firm Secureworks provides the most explicit evidence yet that the hacking group known as Fancy Bear operates in close alignment with the Russian government's interests. (AP Photo/Ivan Sekretarev)

Though the heart of the campaign was now compromised, the hacking efforts continued. Three new volleys of malicious messages were generated on the 22nd, 23rd and 25th of March, targeting communications director Jennifer Palmieri and Clinton confidante Huma Abedin, among others.

The torrent of phishing emails caught the attention of the FBI, which had spent the previous six months urging the Democratic National Committee in Washington to raise its shield against suspected Russian hacking. In late March, FBI agents paid a visit to Clinton's Brooklyn

headquarters, where they were received warily, given the agency's investigation into the candidate's use of a private email server while secretary of state.

The phishing messages also caught the attention of Secureworks, a subsidiary of Dell Technologies, which had been following Fancy Bear, whom Secureworks codenamed Iron Twilight.

Fancy Bear had made a critical mistake.

It fumbled a setting in the Bitly link-shortening service that it was using to sneak its emails past Google's spam filter. The blunder exposed whom they were targeting.

It was late March when Secureworks discovered the hackers were going after Democrats.

"As soon as we started seeing some of those hillaryclinton.com email addresses coming through, the DNC email addresses, we realized it's going to be an interesting twist to this," said Rafe Pilling, a senior security researcher with Secureworks.

By early April Fancy Bear was getting increasingly aggressive, the AP found. More than 60 bogus emails were prepared for Clinton campaign and DNC staffers on April 6 alone, and the hackers began hunting for Democrats beyond New York and Washington, targeting the digital communications director for Pennsylvania Gov. Tom Wolf and a deputy director in the office of Chicago Mayor Rahm Emanuel.

A motorcycle is parked outside the THCServers.com company headquarters, outside Craiova, southern Romania, Wednesday, Oct. 4, 2017. This company based in a remote part of the eastern European country was used to register the website DCLeaks, which U.S. intelligence has accused of being a front for Russian spies. (AP Photo/Vadim Ghirda)

The group's hackers seemed particularly interested in Democratic officials working on voter registration issues: Pratt Wiley, the DNC's then-director of voter protection, had been targeted as far back as October 2015 and the hackers tried to pry open his inbox as many as 15 times over six months.

Employees at several organizations connected to the Democrats were targeted, including the Clinton Foundation, the Center for American Progress, technology provider NGP VAN, campaign strategy firm 270 Strategies, and partisan news outlet Shareblue Media.

As the hacking intensified, other elements swung into place. On April 12, 2016, someone paid $37 worth of bitcoin to the Romanian web hosting company THCServers.com , to reserve a website called Electionleaks.com, according to transaction records obtained by AP. A botched registration meant the site never got off the ground, but the records show THC received a nearly identical payment a week later to create DCLeaks.com.

By the second half of April, the DNC's senior leadership was beginning to realize something was amiss. One DNC consultant, Alexandra Chalupa, received an April 20 warning from Yahoo saying her account was under threat from state-sponsored hackers, according to a screengrab she circulated among colleagues.

The Trump campaign had gotten a whiff of Clinton email hacking, too. According to recently unsealed court documents, former Trump foreign policy adviser George Papadopoulos said that it was at an April 26 meeting at a London hotel that he was told by a professor closely connected to the Russian government that the Kremlin had obtained compromising information about Clinton.

"They have dirt on her," Papadopoulos said he was told. "They have thousands of emails."

A few days later, Amy Dacey, then the DNC chief executive, got an urgent call.

There'd been a serious breach at the DNC.


In this June 14, 2016 file photo, people stand outside the Democratic National Committee headquarters in Washington. Hackers tried to break into DNC inboxes in March 2016 and intensified their efforts in early April. (AP Photo/Paul Holston, File)

___

## 'DON'T EVEN TALK TO YOUR DOG ABOUT IT'

It was 4 p.m. on Friday June 10 when some 100 staffers filed into the Democratic National Committee's main conference room for a mandatory, all-hands meeting.

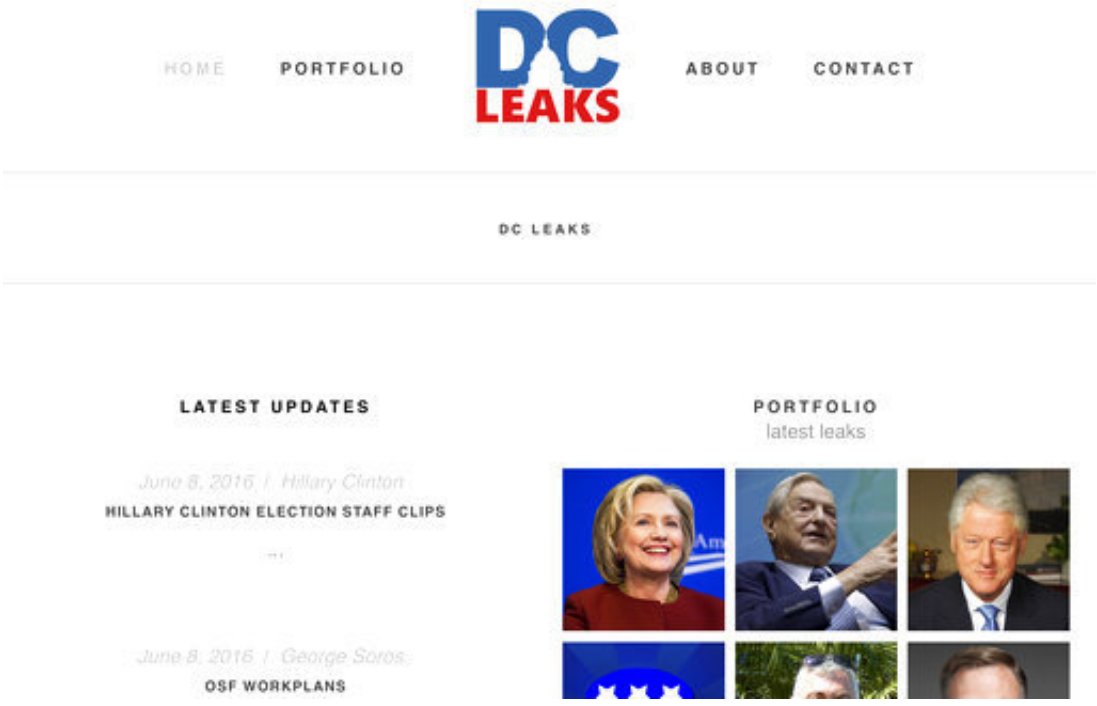
"What I am about to tell you cannot leave this room," DNC chief operating officer Lindsey Reynolds told the assembled crowd, according to two people there at the time.

Everyone needed to turn in their laptops immediately; there would be no last-minute emails; no downloading documents and no exceptions. Reynolds insisted on total secrecy.

"Don't even talk to your dog about it," she was quoted as saying.

Reynolds didn't return messages seeking comment.

Two days later, as the cybersecurity firm that was brought in to clean out the DNC's computers finished its work, WikiLeaks founder Julian Assange told a British Sunday television show that emails related to Clinton were "pending publication."




This image shows part of an archive capture from the Internet Archive's "Wayback Machine" of the website DCLeaks.com on June 13, 2016. The Associated Press found powerful evidence of a direct link between Fancy Bear hackers and the interlocking leakers DCLeaks, WikiLeaks and Guccifer 2.0. All

the Democrats whose private correspondence was published in the run-up to the 2016 U.S. election were targeted by Fancy Bear. (Wayback Machine/Internet Archive via AP)

"WikiLeaks has a very good year ahead," he said.

On Tuesday, June 14, the Democrats went public with the allegation that their computers had been compromised by Russian state-backed hackers, including Fancy Bear.

Shortly after noon the next day, William Bastone, the editor-in-chief of investigative news site The Smoking Gun, got an email bearing a small cache of documents marked "CONFIDENTIAL."

"Hi," the message said. "This is Guccifer 2.0 and this is me who hacked Democratic National Committee."

___

'CAN IT INFLUENCE THE ELECTION?'

Guccifer 2.0 acted as a kind of master of ceremonies during the summer of leaks, proclaiming that the DNC's stolen documents were in WikiLeaks' hands, publishing a selection of the material himself and constantly chatting up journalists over Twitter in a bid to keep the story in the press.

He appeared particularly excited to hear on June 24 that his leaks had sparked a lawsuit against the DNC by disgruntled supporters of Clinton rival Bernie Sanders.


This June 29, 2016 photo shows signs posted in a bathroom at Hillary Clinton's campaign headquarters in the Brooklyn borough of New York, reminding campaign workers to keep their computers and passwords secure. After repeated attempts to break into various staffers' hillaryclinton.com accounts, the hackers turned to their personal Gmail addresses. (AP Photo/Julie Pace)

"Can it influence the election in any how?" he asked a journalist with Russia's Sputnik News, in uneven English.

Later that month Guccifer 2.0 began directing reporters to the newly launched DCLeaks site, which was also dribbling out stolen material on Democrats. When WikiLeaks joined the fray on July 22 with its own disclosures the leaks metastasized into a crisis, triggering intraparty feuding that forced the resignation of the DNC's chairwoman and drew angry protests at the Democratic National Convention.

Guccifer 2.0, WikiLeaks and DCLeaks ultimately published more than 150,000 emails stolen from more than a dozen Democrats, according to an AP count.

The AP has since found that each of one of those Democrats had previously been targeted by Fancy Bear, either at their personal Gmail addresses or via the DNC, a finding established by running targets' emails against the Secureworks' list.

All three leak-branded sites have distanced themselves from Moscow. DCLeaks claimed to be run by American hacktivists. WikiLeaks said Russia wasn't its source. Guccifer 2.0 claimed to be Romanian.

But there were signs of dishonesty from the start. The first document Guccifer 2.0 published on June 15 came not from the DNC as advertised but from Podesta's inbox, according to a former DNC official who spoke on condition of anonymity because he was not authorized to speak to the press.

The official said the word "CONFIDENTIAL" was not in the original document.

Guccifer 2.0 had airbrushed it to catch reporters' attention.

In this Friday May 19, 2017 file photo, WikiLeaks founder Julian Assange leaves after greeting supporters outside the Ecuadorian embassy in London. The Associated Press found powerful evidence of a direct link between Fancy Bear hackers and the interlocking leakers WikiLeaks, Guccifer 2.0 and DCLeaks. All the Democrats whose private correspondence was published in the run-up to the 2016 U.S. election were targeted by Fancy Bear. (AP Photo/Frank Augstein)

—

'PLEASE GOD, DON'T LET IT BE ME'

To hear the defeated candidate tell it, there's no doubt the leaks helped swing the election.

"Even if Russian interference made only a marginal difference," Clinton told an audience at a recent speech at Stanford University, "this election

was won at the margins, in the Electoral College."

It's clear Clinton's campaign was profoundly destabilized by the sudden exposures that regularly radiated from every hacked inbox. It wasn't just her arch-sounding speeches to Wall Street executives or the exposure of political machinations but also the brutal stripping of so many staffers' privacy.

"It felt like your friend had just been robbed, but it wasn't just one friend, it was all your friends at the same time by the same criminal," said Jesse Ferguson, a former Clinton spokesman.

An atmosphere of dread settled over the Democrats as the disclosures continued.

One staffer described walking through the DNC's office in Washington to find employees scrolling through articles about Putin and Russia. Another said she began looking over her shoulder when returning from Clinton headquarters in Brooklyn after sundown. Some feared they were being watched; a car break-in, a strange woman found lurking in a backyard late at night and even a snake spotted on the grounds of the DNC all fed an undercurrent of fear.

In this Thursday, Sept. 15, 2016 file photo, senior aide Huma Abedin, center, and Director of Communications Jennifer Palmieri, right, stand nearby as Democratic presidential candidate Hillary Clinton answers a question after a rally in Greensboro, N.C. On the 22nd, 23rd and 25th of March 2016, three volleys of malicious messages were generated targeting Abedin and Palmieri, among many others. (AP Photo/Andrew Harnik)

Even those who hadn't worked at Democratic organizations for years were anxious. Brent Kimmel, a former technologist at the DNC, remembers watching the leaks stream out and thinking: "Please God, don't let it be me."

___

'MAKE AMERICA GREAT AGAIN'

On Oct. 7, it was Podesta.

The day began badly, with Hillary Clinton's phone buzzing with crank messages after its number was exposed in a leak from the day before. The number had to be changed immediately; a former campaign official said that Abedin, Clinton's confidante, had to call staffers one at a time with Clinton's new contact information because no one dared put it in an email.

The same afternoon, just as the American electorate was digesting a lewd audio tape of Trump boasting about sexually assaulting women, WikiLeaks began publishing the emails stolen from Podesta.

The publications sparked a media stampede as they were doled out one batch at a time, with many news organizations tasking reporters with scrolling through the thousands of emails being released in tranches. At the AP alone, as many as 30 journalists were assigned, at various times, to go through the material.

Guccifer 2.0 told one reporter he was thrilled that WikiLeaks had finally followed through.

"Together with Assange we'll make america great again," he wrote.