

HOW RUSSIA PULLED OFF THE BIGGEST ELECTION HACK IN U.S. HISTORY

PUTIN, WIKILEAKS, THE NSA AND THE DNC EMAIL FIASCO THAT GAVE TRUMP AND CLINTON ANOTHER REASON TO BE AT ODDS.

BY THOMAS RID OCT 20, 2016

f

135.8k

n an April afternoon earlier this year, Russian president Vladimir Putin headlined a gathering of some four hundred journalists, bloggers, and media executives in St. Petersburg. Dressed in a sleek navy suit, Putin looked relaxed, even comfortable, as he took questions. About an hour into the forum, a young blogger in a navy zip sweater took the microphone and asked Putin what he thought of the "so-called Panama Papers."

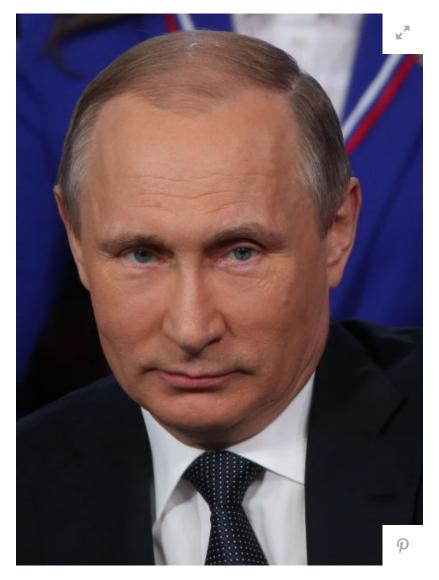
 (\mathbf{C})

ADVERTISEMENT - CONTINUE READING BELOW

 \bowtie

—

The blogger was referring to a cache of more than eleven million computer files that had been stolen from Mossack Fonseca, a Panamanian law firm. The leak was the largest in history, involving 2.6 terabytes of data, enough to fill more than five hundred DVDs. On April 3, four days before the St. Petersburg forum, a group of international news outlets published the first in a series of stories based on the leak, which had taken them more than a year to investigate. The series revealed corruption on a massive scale: Mossack Fonseca's legal maneuverings had been used to hide billions of dollars. A central theme of the group's reporting was the matryoshka doll of secret shell companies and proxies, worth a reported \$2 billion, that belonged to Putin's inner circle and were presumed to shelter some of the Russian president's vast personal wealth.



Vladimir Putin in St. Petersburg at a media forum in April 2016

When Putin heard the blogger's question, his face lit up with a familiar smirk. He nodded slowly and confidently before reciting a litany of humiliations that the United States had inflicted on Russia. Putin reminded his audience about the sidelining of Russia during the 1998 war in Kosovo and what he saw as American meddling in Ukraine more recently. Returning to the Panama Papers, Putin cited WikiLeaks to insist that "officials and state agencies in the United States are behind all this." The Americans' aim, he said, was to weaken Russia from within: "to spread distrust for the ruling authorities and the bodies of power within society."

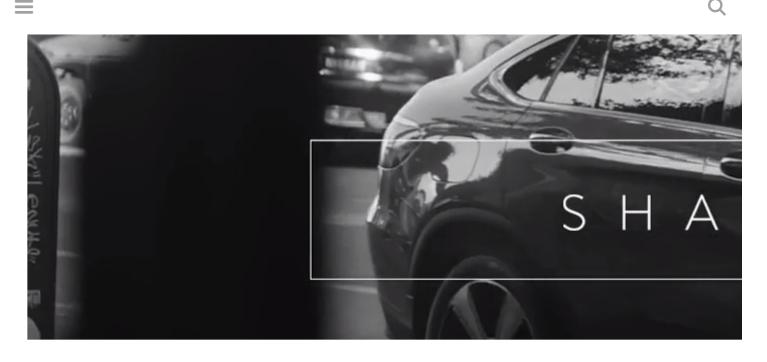
Though a narrow interpretation of Putin's accusation was defensible—as WikiLeaks had pointed out, one of the members of the Panama Papers consortium had received financial support from USAID, a federal agency—his swaggering assurance about America's activities has a more plausible explanation: Putin's own government had been preparing a vast, covert, and unprecedented campaign of political sabotage against the United States and its allies for more than a year.

The Russian campaign burst into public view only this past June, when *The Washington Post* reported that "Russian government hackers" had penetrated the servers of the Democratic National Committee. The hackers, hiding behind ominous aliases like Guccifer 2.0 and DC Leaks, claimed their first victim in July, in the person of Debbie Wasserman Schultz, the DNC chair, whose private emails were published by WikiLeaks in the days leading up to the Democratic convention. By August, the hackers had learned to use the language of Americans frustrated with Washington to create doubt about the integrity of the electoral system: "As you see the U. S. presidential elections are becoming a farce," they wrote from Russia.

The attacks against political organizations and individuals absorbed much of the media's attention this year. But in many ways, the DNC hack was merely a prelude to what many security researchers see as a still more audacious feat: the hacking of America's most secretive intelligence agency, the NSA.

ADVERTISEMENT - CONTINUE READING BELOW

—



ussian spies did not, of course, wait until the summer of 2015 to start hacking the United States. This past fall, in fact, marked the twentieth anniversary of the world's first major campaign of state-on-state digital espionage. In 1996, five years after the end of the USSR, the Pentagon began to detect high-volume network breaches from Russia. The campaign was an intelligence-gathering operation: Whenever the intruders from Moscow found their way into a U.S. government computer, they binged, stealing copies of every file they could.

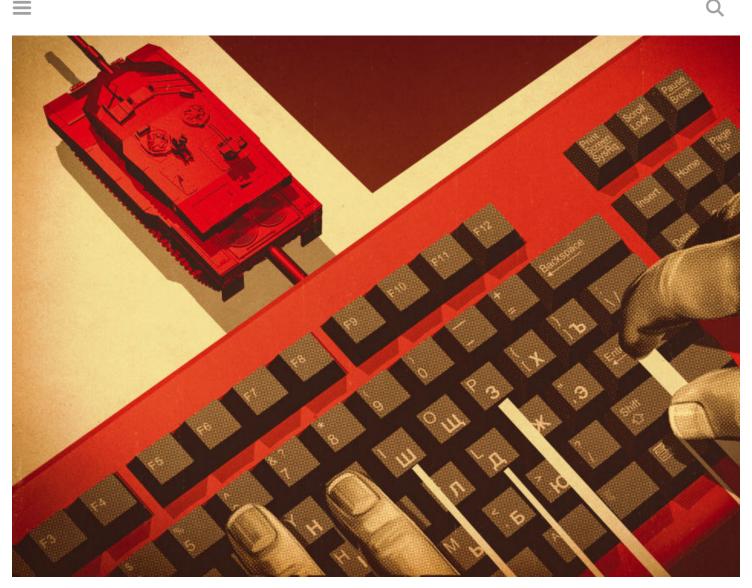
By 1998, when the FBI code-named the hacking campaign Moonlight Maze, the Russians were commandeering foreign computers and using them as staging hubs. At a time when a 56 kbps dial-up connection was more than sufficient to get the best of Pets.com and AltaVista, Russian operators extracted several gigabytes of data from a U.S. Navy computer in a single session. With the unwitting help of proxy machines—including a Navy supercomputer in Virginia Beach, a server at a London nonprofit, and a computer lab at a public library in Colorado-that accomplishment was repeated hundreds of times over. Eventually, the Russians stole the equivalent, as an Air Intelligence Agency estimate later had it, of "a stack of printed copier paper three times the height of the Washington Monument."

Q

copier paper three times the height of the Washington Monument."

The Russians' tactics became more sophisticated over time; they even hacked satellites to cover their tracks. But while the American code names used to track the Russian effort changed from Moonlight Maze to Storm Cloud to Makers Mark—the operation itself never really stopped. Over the next two decades, the FSB (successor to the KGB) and the GRU (Russia's premier military intelligence organization) went after political and military targets, while the NSA and the UK's GCHQ returned the favor.

This sort of espionage was business as usual, a continuation of long-standing practice. And during the cold war, both the USSR and the United States subtly, and sometimes covertly, interfered with foreign elections. What changed over the past year, however—what made the DNC hack feel new and terrifying—was Russia's seeming determination to combine the two. For the first time, Russia used a hacking operation, one that collected and released massive quantities of stolen information, to meddle in an American presidential election. The inspiration and template for this new attack was a poisonous cocktail of fact and fabrication that the Russians call *kompromat*, for "compromising material." _



Tavis Coburn

Kompromat had been deployed by the Soviet Union since at least the 1950s, but in 1999 the Kremlin gave the tactic a high-tech update. With parliamentary elections fast approaching, and with post-USSR corruption at a peak, the government of president Boris Yeltsin used anonymous websites to sling mud at opposition candidates. One notorious kompromat repository was run specifically to slander the mayor of Moscow, a rising star in the opposition with his eyes on the presidency. In 2009, a senior British diplomat working in Russia was forced to resign after the appearance online of a four-minute video that showed him having sex with two blond women in a brothel.

ADVERTISEMENT - CONTINUE READING BELOW

One of the first American targets of *kompromat* was Victoria Nuland, who served as the top U. S. diplomat for Europe during Obama's second term. In February 2014, at the peak of the crisis in Ukraine, Nuland was surreptitiously recorded while speaking on the phone with the U. S. ambassador to Kiev. Frustrated with Europe's lackluster response to the Ukrainian crisis, Nuland said, "Fuck the EU." Shortly after, an aide to the Russian deputy prime minister tweeted a link to a recording of the intercepted phone call. The State Department called the leak "a new low in Russian tradecraft."



Victoria Nuland Getty

The Nuland leak prompted a minor diplomatic hiccup between the European Union and the United States. But the *kompromat* campaign of the past year appears to be aimed at much

until May, however, that the DNC asked for help from a cybersecurity company called CrowdStrike, which had experience identifying digital espionage operations by nation-states. CrowdStrike immediately discovered two sophisticated groups of spies that were stealing documents from the Democrats by the thousands.

CrowdStrike was soon able to reconstruct the hacks and identify the hackers. One of the groups, known to the firm as Cozy Bear, had been rummaging around the DNC since the previous summer. The other, known as Fancy Bear, had broken in not long before Putin's appearance at the St. Petersburg forum. Surprisingly, given that security researchers had long suspected that both groups were directed by the Russian government, each of the attackers seemed unaware of what the other was doing.

Meanwhile a mysterious website named DC Leaks was registered on April 19. In early June, a Twitter account associated with the site started linking to the private conversations of Philip Breedlove, who had been, until a few weeks earlier, NATO's Supreme Allied Commander in Europe. DC Leaks was well designed, but nobody seems to have noticed it until early July.

DC Leaks was well designed, but nobody seems to have noticed it until early July.

On June 14, less than an hour after *The Washington Post* reported the breach at the DNC, CrowdStrike posted a report that detailed the methods used by the intruders. The firm also did something unusual: It named the Russian spy agencies it believed responsible for the hack. Fancy Bear, the firm said, worked in a way that suggested affiliation with the GRU. Cozy Bear was linked to the FSB.

The day after the *Post* story broke, a website appeared that claimed to belong to a hacker who identified himself as Guccifer 2.0. (Guccifer was the nickname of a Romanian hacker who, among other things, broke into the email account of George W. Bush's sister.) The operators, posing as Guccifer 2.0, dismissed CrowdStrike's attribution, insisting instead that the DNC had been "hacked by a lone hacker." As proof, Guccifer published eleven documents from the DNC, including an opposition-research file on Donald Trump and a list of major Democratic donors.

to WikiLeaks."

ADVERTISEMENT - CONTINUE READING BELOW

Ultimately, more than two thousand confidential files from the DNC found their way to the public. Throughout the campaign, Guccifer maintained that he was the only person behind the hacking and leaking. "This is my personal project and I'm proud of it," he—or they—wrote in late June. But several sloppy mistakes soon revealed who was really behind the operation. The unraveling happened more quickly than anybody could have anticipated.

s soon as Guccifer's files hit the open Internet, an army of investigators including old-school hackers, former spooks, security consultants, and journalists —descended on the hastily leaked data. Informal, self-organized groups of sleuths discussed their discoveries over encrypted messaging apps such as Signal. Many of the selfappointed analysts had never met in person, and sometimes they didn't know one another's real names, but they were united in their curiosity and outrage. The result was an unprecedented open-source counterintelligence operation: Never in history was intelligence analysis done so fast, so publicly, and by so many. _

Q



Tavis Coburn

Matt Tait, a former GCHQ operator who tweets from the handle @pwnallthethings, was particularly prolific. Hours after the first Guccifer 2.0 dump, on the evening of June 15, Tait found something curious. One of the first leaked files had been modified on a computer using Russian-language settings by a user named "Feliks Dzerzhinsky." Dzerzhinsky was the founder of the Cheka, the Soviet secret police—a figure whose mythic renown was signaled by a fifteenton bronze statue that once stood in front of KGB headquarters. Tait tweeted an image of the document's metadata settings, which, he suggested, revealed a failure of operational security.

A second mistake had to do with the computer that had been used to control the hacking operation. Researchers found that the malicious software, or malware, used to break into the DNC was controlled by a machine that had been involved in a 2015 hack of the German parliament. German intelligence later traced the Bundestag breach to the Russian GRU, aka Fancy Bear.

Ξ

pointed out. But the hackers' gravest mistake involved the emails they'd used to initiate their attack. As part of a so-called spear-phishing campaign, Fancy Bear had emailed thousands of targets around the world. The emails were designed to trick their victims into clicking a link that would install malware or send them to a fake but familiar-looking login site to harvest their passwords. The malicious links were hidden behind short URLs of the sort often used on Twitter.

RELATED STORY

The Head of CrowdStrike Is Putin's Worst Nightmare

To manage so many short URLs, Fancy Bear had created an automated system that used a popular link-shortening service called Bitly. The spear-phishing emails worked well—one in seven victims revealed their passwords—but the hackers forgot to set two of their Bitly accounts to "private." As a result, a cybersecurity company called SecureWorks was able to glean information about Fancy Bear's targets. Between October 2015 and May 2016, the hacking group used nine thousand links to attack about four thousand Gmail accounts, including targets in Ukraine, the Baltics, the United States, China, and Iran. Fancy Bear tried to gain access to defense ministries, embassies, and military attachés. The largest group of targets, some 40 percent, were current and former military personnel. Among the group's recent breaches were the German parliament, the Italian military, the Saudi foreign ministry, the email accounts of Philip Breedlove, Colin Powell, and John Podesta—Hillary Clinton's campaign chairman—and, of course, the DNC.

ADVERTISEMENT - CONTINUE READING BELOW

Q

be identified so quickly, a theory that would explain, among other things, the peculiar animus Guccifer seemed to have for CrowdStrike. According to this hypothesis, the tradecraft blunders that Tait and others had identified were the result of a hasty effort by the GRU to cover its tracks.

As if to regroup after the initial rush of activity, Guccifer and DC Leaks went quiet at the end of June. But the 2016 presidential campaign, already the most bizarre in living memory, had a further surprise in store, one that worked in favor of the Russians. At a time when only 32 percent of Americans say that they trust the media to report the news fairly and accurately, the hackers were about to learn that getting called out publicly didn't really matter: Their *kompromat* operations would still work just fine.

The hackers were about to learn that getting called out publicly didn't really matter.

On July 22, three days before the Democratic National Convention in Philadelphia, WikiLeaks published the largest trove of files to date, which included nearly twenty thousand hacked emails. Press coverage of the release quickly centered on emails that suggested a bias among some DNC staffers in favor of Hillary Clinton. The leaked emails lent credence to a suspicion held by some Democrats that the party establishment had never intended to give Bernie Sanders, Clinton's opponent in the primaries, a fair shake. Protesters in Philadelphia held up signs that read election fraud and dnc leaks shame. One day before the convention, the Russian *kompromat* campaign took its first trophy: Debbie Wasserman Schultz, the DNC chair, resigned from the organization.

—

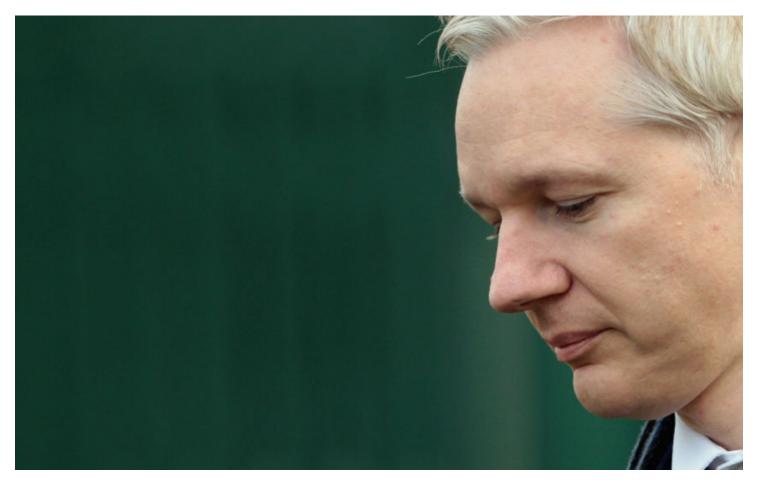


The episode shocked the Democratic establishment, not least because of what it augured for the future. As Clinton's lead in the polls widened after the convention, commentators began to speculate that a damaging leak late in the campaign might be the only chance for Donald Trump to win the election. Fears of a Russia-sponsored October surprise grew as it became clearer that the subversion effort was improving. When files appeared, they were now scrubbed of the sort of distinguishing metadata that had allowed analysts to trace the leak back to Russian intelligence.

ADVERTISEMENT - CONTINUE READING BELOW

The operators behind Guccifer and DC Leaks also appear to have recognized that American journalists were desperate for scoops, no matter their source. The Russians began to act like a PR agency, providing access to reporters at Politico, The Intercept, and BuzzFeed. Journalists were eager to help. On August 27, when part of the DC Leaks website was down for some reason, Twitter suspended the @DCLeaks account. The Daily Caller, a conservative news website, posted a story about the events, drawing an outcry from Trump supporters. Lou Dobbs, the Fox Business anchor, sneered that "leftist fascism" was throttling the last best hope for a Trump victory. Twitter soon reinstated @DCLeaks.

breaching Saudi Arabia's foreign ministry. A group called WikiSaudiLeaks, probably a Guccifer-like front for Fancy Bear, claimed that "WikiLeaks have been given access to some part of these documents." The so-called Saudi Cables showed princes buying influence and monitoring dissidents. They became a major news story, proving that the old methods worked even better in the twenty-first century.



Julian Assange Getty

A leak released at the end of this past summer showed how frictionlessly the *kompromat* campaign was able to operate in the fact-free atmosphere of the 2016 American presidential campaign. In late September, DC Leaks published hundreds of emails from the account of a twenty-two-year-old freelancer for the Clinton campaign. Lachlan Markay, a reporter for *The Washington Free Beacon*, found an audio clip buried deep in the cache. In the recording, which was made at a fundraiser in Virginia, Hillary Clinton could be heard describing Sanders supporters as "children of the Great Recession" who "are living in their parents' basement."

said.) Nevertheless, within a few days, Donald Trump was telling a roaring crowd in Pennsylvania, "Clinton thinks Bernie supporters are hopeless and ignorant basement dwellers."

n mid-August, when Guccifer and DC Leaks were making near-daily news, a third mysterious social-media account popped up out of nowhere. A group calling itself the Shadow Brokers announced that it had published "cyberweapons" that belonged to the NSA on file-sharing sites such as Github. The group said that it would soon hold an auction to sell off a second cache of tools. After a security researcher posted a link to a repository of the supposed NSA software, analysts flocked to the dump. Security researchers quickly discovered that the tools, a collection of malware designed to steal data from their targets, were the real thing. Crucially, The Intercept, a media outlet with access to the NSA files leaked by Edward Snowden, found a sixteen-character string ("ace02468bdf13579") in the Shadow Brokers' tools that was referenced in a top-secret, and previously unpublished, NSA manual. The connection proved the provenance of the Shadow Brokers' find.

ADVERTISEMENT - CONTINUE READING BELOW

Robbing the NSA, of course, is not easy. The agency's elite hacking unit, called Tailored Access Operations, has an internal network known as the "high side" that is physically segregated from the Internet (the "low side"). Data diodes, devices that allow data to flow one way only, like water from a faucet, make it nearly impossible to hack high-side computers from the low side. When TAO hackers want to attack an adversary, they move their tools from the high side to a server on the low side, navigate through a series of addresses that make their tracks

Shadow Brokers likely got lucky: Some analysts believe that an NSA operator mistakenly uploaded a whole set of tools to a staging computer the hackers were already watching. The alternative theory: an old-fashioned mole passed on the tools.

After going to all that trouble, why publish the results? A possible answer is suggested by a surprising discovery made by the U. S. intelligence community around the time Putin was addressing the journalists in St. Petersburg. American investigators had long known that the Russians were doing more than spear-phishing, but sometime around April they learned that the intruders were using commercial cloud services to "exfiltrate" data out of American corporations and political targets. Cozy Bear, the hacking group believed to be affiliated with the FSB, used some two hundred Microsoft OneDrive accounts to send data from its victims back to Moscow.



Getty

Using cloud services such as OneDrive was a clever but risky move—it was a little like taking the bus to make off with stolen goods from a burglary. Though the widespread use of the services by legitimate users offered a degree of cover for the hackers, data provided by Microsoft also helped America's elite digital spies identify the DNC intruders "with confidence"

30, an FSB press release announced that twenty government and defense organizations had been hit by high-powered spying tools.

Some intelligence analysts believe that the Shadow Brokers' publication of the NSA spy kit was a message from one group of professionals to another. "You see us?" the Russians seemed to be saying, perhaps in reference to ongoing U. S. efforts to investigate the DNC breach. "Fine, but we see you, too." Similarly, the announcement of an auction—all but certainly phony—was probably intended as a warning that the hackers were prepared to publish a key that would unlock an encrypted container holding a second batch of stolen tools. Like a severed ear in an envelope, the announcement told the Americans: Don't mess with us.

Like a severed ear in an envelope, the announcement told the Americans: Don't mess with us.

Meanwhile, the *kompromat* campaign proceeded apace. August and September each saw six data dumps, including files from the Democratic Congressional Campaign Committee, which had also been hacked. In October, as the presidential election drew near, Guccifer published a massive cache, more than twenty-one hundred files. Three days later, WikiLeaks began publishing thousands of emails stolen from John Podesta's account.

On the day WikiLeaks published the first batch of Podesta's emails, the U. S. government took the unprecedented step of announcing that it was "confident" Russia's "seniormost officials" had authorized the DNC hacks. So far U. S. investigators have not said publicly who was responsible for the Podesta hack, but the data harvested by SecureWorks makes it clear that Fancy Bear broke into the Clinton chairman's account as early as late March. The CIA briefed Trump about the origin of the *kompromat*, but he continued to cite the material, telling a Pennsylvania crowd, "I love WikiLeaks!"



n October 12, Putin appeared at another forum, this time with more than five hundred guests in Moscow. Sitting comfortably in front of a giant banner that said russia calling! he answered an audience question about the hacks.

"Everyone is talking about who did it," Putin said. "Is it so important?" The former KGB

Russia's interest, he said, was "hysteria" intended to distract Americans from what the hackers discovered: "the manipulation of public opinion." When the audience applauded, a smirk returned to Putin's face. "I think I answered your question," he said.

Thomas Rid (@RidT) *is a professor at King's College London and author of* Rise of the Machines.

MORE FROM ESQUIRE:

How Julian Assange Became a Conservative Heartthrob