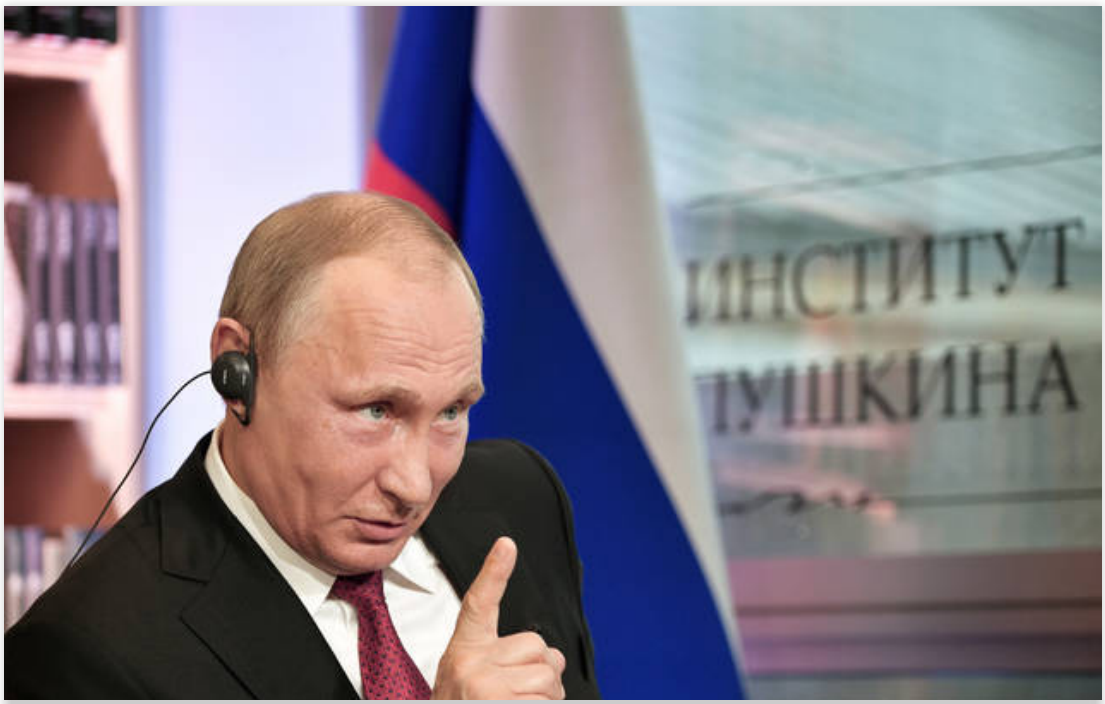
HONOLULU Star-Advertiser
December 4, 2017 | 78° | Check Traffic

TOP NEWS

Russian hackers pursued Putin foes, not just U.S. Democrats

Associated Press
Posted November 01, 2017
November 1, 2017

Updated November 2, 2017 2:26pm



ASSOCIATED PRESS

Russian President Vladimir Putin speaks during an interview in Paris, France.

WASHINGTON >> It wasn't just Hillary Clinton's emails they went after.

The hackers who disrupted the U.S. presidential election last year had ambitions that stretched across the globe, targeting the emails of Ukrainian officers, Russian

opposition figures, U.S. defense contractors and thousands of others of interest to the Kremlin, according to a previously unpublished digital hit list obtained by The Associated Press.

The list provides the most detailed forensic evidence yet of the close alignment between the hackers and the Russian government, exposing an operation that went back years and tried to break into the inboxes of 4,700 Gmail users — from the pope's representative in Kiev to the punk band Pussy Riot in Moscow. The targets were spread among 116 countries.

"It's a wish list of who you'd want to target to further Russian interests," said Keir Giles, director of the Conflict Studies Research Center in Cambridge, England, and one of five outside experts who reviewed the AP's findings. He said the data was "a master list of individuals whom Russia would like to spy on, embarrass, discredit or silence."

The AP findings draw on a database of 19,000 malicious links collected by cybersecurity firm Secureworks, dozens of rogue emails, and interviews with more than 100 hacking targets.

Secureworks stumbled upon the data after a hacking group known as Fancy Bear accidentally exposed part of its phishing operation to the internet. The list revealed a direct line between the hackers and the leaks that rocked the presidential contest in its final stages, most notably the private emails of Clinton campaign chairman John Podesta.

The issue of who hacked the Democrats is back in the national spotlight following the revelation Monday that a Donald Trump campaign official, George Papadopoulos, was briefed early last year that the Russians had "dirt" on Clinton, including "thousands of emails."

Kremlin spokesman Dmitry Peskov called the notion that Russia interfered "unfounded." But the list examined by AP provides powerful evidence that the Kremlin did just that.

"This is the Kremlin and the general staff," said Andras Racz, a specialist in Russian security policy at Pazmany Peter Catholic University in Hungary, as he examined the data.

"I have no doubts."

THE NEW EVIDENCE

Secureworks' list covers the period between March 2015 and May 2016. Most of the identified targets were in the United States, Ukraine, Russia, Georgia and Syria.

In the United States, which was Russia's Cold War rival, Fancy Bear tried to pry open at least 573 inboxes belonging to those in the top echelons of the country's diplomatic and security services: then-Secretary of State John Kerry, former Secretary of State Colin Powell, then-NATO Supreme Commander, U.S. Air Force Gen. Philip Breedlove, and one of his predecessors, U.S. Army Gen. Wesley Clark.

The list skewed toward workers for defense contractors such as Boeing, Raytheon and Lockheed Martin or senior intelligence figures, prominent Russia watchers and — especially — Democrats. More than 130 party workers, campaign staffers and supporters of the party were targeted, including Podesta and other members of Clinton's inner circle.

The AP also found a handful of Republican targets.

Podesta, Powell, Breedlove and more than a dozen Democratic targets besides Podesta would soon find their private correspondence dumped to the web. The AP has determined that all had been targeted by Fancy Bear, most of them three to seven months before the leaks.

"They got two years of email," Powell recently told AP. He said that while he couldn't know for sure who was responsible, "I always suspected some Russian connection."

In Ukraine, which is fighting a grinding war against Russia-backed separatists, Fancy Bear attempted to break into at least 545 accounts, including those of President Petro Poroshenko and his son Alexei, half a dozen current and former ministers such as Interior Minister Arsen Avakov and as many as two dozen current and former lawmakers.

The list includes Serhiy Leshchenko, an opposition parliamentarian who helped uncover the off-the-books payments allegedly made to Trump campaign chairman Paul Manafort — whose indictment was unsealed Monday in Washington.

In Russia, Fancy Bear focused on government opponents and dozens of journalists. Among the targets were oil tycoon-turned-Kremlin foe Mikhail Khodorkovsky, who spent a decade in prison and now lives in exile, and Pussy Riot's Maria Alekhina. Along

with them were 100 more civil society figures, including anti-corruption campaigner Alexei Navalny and his lieutenants.

“Everything on this list fits,” said Vasily Gatov, a Russian media analyst who was himself among the targets. He said Russian authorities would have been particularly interested in Navalny, one of the few opposition leaders with a national following.

Many of the targets have little in common except that they would have been crossing the Kremlin’s radar: an environmental activist in the remote Russian port city of Murmansk; a small political magazine in Armenia; the Vatican’s representative in Kiev; an adult education organization in Kazakhstan.

“It’s simply hard to see how any other country would be particularly interested in their activities,” said Michael Kofman, an expert on Russian military affairs at the Woodrow Wilson International Center in Washington. He was also on the list.

“If you’re not Russia,” he said, “hacking these people is a colossal waste of time.”

WORKING 9 TO 6 MOSCOW TIME

Allegations that Fancy Bear works for Russia aren’t new. But raw data has been hard to come by.

Researchers have been documenting the group’s activities for more than a decade and many have accused it of being an extension of Russia’s intelligence services. The “Fancy Bear” nickname is a none-too-subtle reference to Russia’s national symbol.

In the wake of the 2016 election, U.S. intelligence agencies publicly endorsed the consensus view, saying what American spooks had long alleged privately: Fancy Bear is a creature of the Kremlin.

But the U.S. intelligence community provided little proof, and even media-friendly cybersecurity companies typically publish only summaries of their data.

That makes the Secureworks’ database a key piece of public evidence — all the more remarkable because it’s the result of a careless mistake.

Secureworks effectively stumbled across it when a researcher began working backward from a server tied to one of Fancy Bear’s signature pieces of malicious software.

He found a hyperactive Bitly account that Fancy Bear (which Secureworks calls “Iron Twilight”) was using to sneak thousands of malicious links past Google’s spam filter. Because Fancy Bear forgot to set the account to private, Secureworks spent the next few months hovering over the group’s shoulder, quietly copying down the details of the thousands of emails it was targeting.

The AP obtained the data recently, boiling it down to 4,700 individual email addresses, and then connecting roughly half to account holders. The AP validated the list by running it against a sample of phishing emails obtained from people targeted and comparing it to similar rosters gathered independently by other cybersecurity companies, such as Tokyo-based Trend Micro and the Slovakian firm ESET .

The Secureworks data allowed reporters to determine that more than 95 percent of the malicious links were generated during Moscow office hours — between 9 a.m. and 6 p.m. Monday to Friday.

The AP's findings also track with a report that first brought Fancy Bear to the attention of American voters. In 2016, a cybersecurity company known as CrowdStrike said the Democratic National Committee had been compromised by Russian hackers, including Fancy Bear.

Secureworks' roster shows Fancy Bear making aggressive attempts to hack into DNC technical staffers' emails in early April 2016 — exactly when CrowdStrike says the hackers broke in.

And the raw data enabled the AP to speak directly to the people who were targeted, many of whom pointed the finger at the Kremlin.

"We have no doubts about who is behind these attacks," said Artem Torchinskiy, a project coordinator with Navalny's Anti-Corruption Fund who was targeted three times in 2015. "I am sure these are hackers controlled by Russian secret services."

THE MYTH OF THE 400-POUND MAN

Even if only a small fraction of the 4,700 Gmail accounts targeted by Fancy Bear were hacked successfully, the data drawn from them could run into terabytes — easily rivaling the biggest known leaks in journalistic history.

For the hackers to have made sense of that mountain of messages — in English, Ukrainian, Russian, Georgian, Arabic and many other languages — they would have needed a substantial team of analysts and translators. Merely identifying and sorting the targets took six AP reporters eight weeks of work.

The AP's effort offers "a little feel for how much labor went into this," said Thomas Rid, a professor of strategic studies at Johns Hopkins University's School of Advanced International Studies.

In response to the AP's investigation, the DNC issued a statement saying the evidence that Russia had interfered in the election was "irrefutable."

Rid said the investigation should put to rest any theories like the one then-candidate Donald Trump floated last year that the hacks could be the work of "someone sitting on their bed that weighs 400 pounds."

"The notion that it's just a lone hacker somewhere is utterly absurd," Rid said.