The New York Times | http://nyti.ms/2eiuaxz

U.S.

Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools

By SCOTT SHANE, MATT APUZZO and JO BECKER OCT. 19, 2016

WASHINGTON — Investigators pursuing what they believe to be the largest case of mishandling classified documents in United States history have found that the huge trove of stolen documents in the possession of a National Security Agency contractor included top-secret N.S.A. hacking tools that two months ago were offered for sale on the internet.

They have been hunting for electronic clues that could link those cybertools — computer code posted online for auction by an anonymous group calling itself the Shadow Brokers — to the home computers of the contractor, Harold T. Martin III, who was arrested in late August on charges of theft of government property and mishandling of classified information.

But so far, the investigators have been frustrated in their attempt to prove that Mr. Martin deliberately leaked or sold the hacking tools to the Shadow Brokers or, alternatively, that someone hacked into his computer or otherwise took them without his knowledge. While they have found some forensic clues that he might be the source, the evidence is not conclusive, according to a dozen officials who have been involved in or have been briefed on the investigation.

All spoke on condition of anonymity because they were not authorized to discuss it publicly.

Mr. Martin, an enigmatic loner who according to acquaintances frequently expressed his excitement about his role in the growing realm of cyberwarfare, has

insisted that he got in the habit of taking material home so he could improve his skills and be better at his job, according to these officials. He has explained how he took the classified material but denied having knowingly passed it to anyone else.

“As a contractor, he gets to see a slice of the overall picture,” said one person familiar with the exchanges, summarizing Mr. Martin’s explanation. “He wanted to see the overall picture so that he could be more effective.”

The material the F.B.I. found in his possession added up to “many terabytes” of information, according to court papers, which would make it by far the largest unauthorized leak of classified material from the classified sector. That volume dwarfs the hundreds of thousands of N.S.A. documents taken by Edward J. Snowden in 2013 and exceeds even the more voluminous Panama Papers, leaked records of offshore companies obtained by a German newspaper in 2015, which totaled 2.6 terabytes. One terabyte of data is equal to the contents of about one million books.

F.B.I. agents on the case, advised by N.S.A. technical experts, do not believe Mr. Martin is fully cooperating, the officials say. He has spoken mainly through his lawyers, James Wyda and Deborah Boardman of the federal public defender’s office in Baltimore. They declined to comment before a detention hearing set for Friday in federal court.

In interviews, officials described how the Martin case has deeply shaken the secret world of intelligence, from the N.S.A.’s sprawling campus at Fort Meade, Md., to the White House. They expressed astonishment that Mr. Martin managed to take home such a vast collection of classified material over at least 16 years, undetected by security officers at his workplaces, including the N.S.A., the Office of the Director of National Intelligence and Pentagon offices. And they are deeply concerned that some of the mountain of material may, by whatever route, have reached hackers or hostile intelligence services.

Investigators discovered the hacking tools, consisting of computer code and instructions on how to use it, in the thousands of pages and dozens of computers and data storage devices that the F.B.I. seized during an Aug. 27 raid on Mr. Martin’s modest house in suburban Glen Burnie, Md. More secret material was found in a shed in his yard and in his car, officials said.

The search came after the Shadow Brokers leak set off a panicked hunt at the N.S.A. Mr. Martin attracted the F.B.I.’s attention by posting something on the internet that was brought to the attention of the N.S.A. Whatever it was — officials are

not saying exactly what — it finally set off an alarm.

The release of the N.S.A.'s hacking tools, even though they dated to 2013, is extraordinarily damaging, said Dave Aitel, a former agency employee who now runs Immunity Inc., an information security company.

"The damage from this release is huge, both to our ability to protect ourselves on the internet and our ability to provide intelligence to policy makers and the military," Mr. Aitel said.

The N.S.A.'s hacking into other countries' networks can be for defensive purposes: By identifying rivals' own hacking methods, the agency can recognize and defend against them, he said. And other countries, with some of the N.S.A.'s tools now in hand, can study past hacks and identify the attacker as the N.S.A., learn how to block similar intrusions, or even decide to retaliate, Mr. Aitel said.

Mr. Martin, 51, a Navy veteran who was completing a Ph.D. in information systems at the University of Maryland, Baltimore County, has worked for several of the contracting companies that help staff the nation's security establishment. After stints at the Computer Sciences Corporation and Tenacity Solutions, where he was assigned to the Office of the Director of National Intelligence, he joined Booz Allen Hamilton in 2009. He worked on that firm's N.S.A. contract until 2015, when he was moved to a different Pentagon contract in the area of offensive cyberwarfare.

He has long held a high-level clearance and for a time worked with the N.S.A.'s premiere hacking unit, called Tailored Access Operations, which breaks into the computer networks of foreign countries and which developed the hacking tools later obtained by the Shadow Brokers. According to one person briefed on the investigation, Mr. Martin was able to obtain some of the hacking tools by accessing a digital library of such material at the N.S.A.

One possibility investigators are considering is that Mr. Martin did not knowingly share the Shadow Brokers material but that it was physically stolen from him — conceivable given the descriptions of the chaos of his house, shed and car — or more likely, grabbed by hackers. But the forensic examination of Mr. Martin's computers has so far turned up no evidence that he was hacked, officials say.

At the core of the investigation, if Mr. Martin deliberately shared the secret N.S.A. tools, is the mystery of his motive. People who know him call him deeply patriotic and say they do not believe he would have given classified information to another country. They also say he has never been interested in politics, making unlikely a politically motivated leak like that of Mr. Snowden, who thought the N.S.A. was violating Americans' privacy.

The F.B.I. is considering whether he might have sold the hacking tools or other materials for money. His annual salary in recent years has exceeded $100,000 and he owns his house without a mortgage. But he has long bought expensive suits and Rolex watches, according to an old acquaintance, and a person familiar with his finances says he has struggled with debt. Court records show one past lien, an $8,997 state tax bill imposed in 2000 and not paid off until 2014.

Some people who know Mr. Martin favor a psychological motive for taking the documents home — one that echoes what he is himself telling investigators: a drive to distinguish himself and prove that his computer knowledge was equal to that of the N.S.A.'s top operators.

"He always thought of himself like a James Bond-type person, wanting to save the world from computer evil," said a person who knows him well but would not speak about him on the record for fear of being pulled into the criminal case.

Last year, commenting online on an article on the future of computer warfare, Mr. Martin struck a martial and patriotic tone.

"The battles ahead will require a special breed of warrior," he wrote. "It's really a calling, and something the individual has to want to do as a profession, due to the sacrifices required to be top flight in this new, electronic, version of the great game."

Mr. Martin's tone of confidence reflected his comfort in the world of computer experts. Mr. Aitel, who runs a popular email list on computer security called Daily Dave, said Mr. Martin regularly emailed the list and him privately, usually expressing his enthusiasm for a technical achievement: "Outstanding! You rock!" he wrote about one exploit, Mr. Aitel said.

But Mr. Martin's online self-assurance, people who know him say, masked a timid, introverted personality. Though he could be warm and generous, he had few friends, was socially awkward and often seemed lost in his work and doctoral studies, these people said.

For years, Mr. Martin struggled with obesity, and then had gastric bypass surgery and lost a lot of weight, according to acquaintances who did not want to be named because they also did not want to drawn into the investigation. But within a decade, he had gained most of it back, they said.

Not long before his arrest, Mr. Martin exchanged emails with Mr. Aitel about attending Mr. Aitel's annual security conference, called Infiltrate, scheduled for April in Miami.

"He sounded completely normal," Mr. Aitel said. "Making plans for the future."

Adam Goldman contributed reporting.

Follow The New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on October 20, 2016, on page A1 of the New York edition with the headline: Hacking Tools Are Among Data Stolen From U.S.