Ransomware Gang Masquerades as Real Company to Recruit Tech Talent; Group linked to Colonial Pipeline hack has made offers to potential employees in new ransomware expansion push, researchers say

McMillan, Robert . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]. 21 Oct 2021.

FULL TEXT

A criminal organization believed to have built the software that shut down a U.S. fuel pipeline has set up a fake company to recruit potential employees, according to researchers at the intelligence firm Recorded Future and Microsoft Corp.

The fake company is using the name Bastion Secure, according to the researchers. On a professional-looking website, the company says it sells cybersecurity services. But the site's operator is a well-known hacking group called Fin7, Recorded Future and Microsoft say.

Fin7 is believed to have hacked hundreds of businesses, stolen more than 20 million customer records and written the software used in a hack that disrupted gasoline delivery in parts of the Southeastern U.S., federal prosecutors and researchers say.

The Bastion Secure website, which uses the logo BS, has listed jobs that are technical in nature and appear similar to work that would be performed at any security company—programmers, system administrators and people who are good at finding bugs in software. Prospective hires will work nine-hour days on a predictable schedule: Monday to Friday, according to the company website. Lunch breaks are provided, the site says.

The attempt to impersonate a legitimate company for recruiting purposes represents a new development by purveyors of ransomware to grow and spread a scourge that has disrupted meat production, hospital care, education and hundreds of businesses. With hundreds of millions of dollars in illegal earnings, ransomware operators are increasingly operating like criminal startups with professionalized support staff, software development, cloud-computing services and media relations, security researchers say.

Recorded Future shared its findings with The Wall Street Journal and planned to publish them in a blog post Thursday. Microsoft officials gave a presentation on their discovery earlier this month at a conference hosted by the cybersecurity firm Mandiant.

Emails to an address listed on the Bastion Secure website went unanswered. A phone call to an Israeli number listed on the site was answered by a Russian-speaking man. "I'm just a person. I have nothing to do with any cybersecurity company," he said before hanging up.

The recruiting effort appears concentrated on Russian speakers, the researchers said. While criminals have traditionally operated in the shadows—recruiting partners in criminal forums—the demands of Fin7's growing business appear to have pushed it to recruit in the open, security researchers say.

"You can find more qualified people when you search more broadly," said Andrei Barysevich, the head of Gemini Advisory, a division of Recorded Future. "There's a lot of embedded law-enforcement agents on the dark web."

Information-technology jobs advertised by Bastion Secure offer salaries between $800 and $1,200 a month. That is decent pay in former Soviet countries such as Ukraine, but "a small fraction of a cybercriminal's portion of the

criminal profits from a successful ransomware extortion or large-scale payment-card-stealing operation," according to the Recorded Future report.

Fin7 has hacked thousands of computer systems and for years focused on stealing and selling credit-card information. The 70-person group caused more than $3 billion in damages to companies and individuals, federal prosecutors say.

The group has recently shifted from stealing card information to ransomware, and it now manages a ransomware service and conducts intrusions to deploy the file-encrypting software, said Nick Carr, a security analyst at Microsoft, while speaking at the Mandiant conference.

Microsoft believes Fin7 produced the software used in the hack that disrupted Colonial Pipeline Co.'s operations in the spring . The actual hack is believed to have been carried out by a criminal affiliate of Fin7, Mr. Carr said in his presentation. Fin7 marketed its ransomware business under the name DarkSide, but more recently has called it BlackMatter, researchers say.

On Monday, three federal agencies—the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation and the National Security Agency— published an alert , explaining how companies can protect themselves from BlackMatter and warning that in recent months, the ransomware "has targeted multiple U.S. critical infrastructure entities, including two U.S. Food and Agriculture Sector organizations."

Bastion Secure isn't the first fake company Fin7 has used to recruit employees. In August 2015 it used another fake cybersecurity company called Combi Security to recruit a Ukrainian man named Fedir Hladyr as a systems administrator, according to federal prosecutors.

Mr. Hladyr didn't realize that he was engaged in a criminal enterprise until many months after his hiring, according to his attorney, Arkady Bukh. He said Fin7 had compartmentalized its business to keep its different employees ignorant of the group's criminal activity. "At some stage, some would figure it out," the attorney said. "Sometimes not."

Mr. Hladyr maintained Fin7's communications servers as well as a world-wide network of servers used to launch and manage cyberattacks, according to federal prosecutors. After pleading guilty to hacking charges, he was sentenced to 10 years in prison in April.

With Bastion Secure, the company made offers to prospective recruits, the researchers say. The Microsoft researchers were able to find a copy of an employment agreement from Bastion Secure sent to a potential employee. "If you actually work there, you're not supposed to talk about it at speeches or media events," Mr. Carr said.

It didn't take long for one potential recruit—applying for an information-technology job—to spot red flags, said Mr. Barysevich, the researcher at Recorded Future whose firm said it spoke with the potential recruit. The first warning sign was that nobody with the company would meet face-to-face or talk via a voice call, the recruit told Mr. Barysevich. Instead, they would communicate only via the encrypted messaging software Telegram or Tox, according to Recorded Future.

Later, the recruit was sent software that Bastion Secure told him he would be using on the job, Mr. Barysevich said. He was asked to connect to what was described as a "client" network and collect information, but not told why or how it would be used. The software tools he was given were in fact hacking tools that a Recorded Future analysis linked to Fin7, Mr. Barysevich said.

Much of the text on the Bastion Secure website appears to have been lifted word-for-word from a legitimate U.K.-based cybersecurity company, Convergent Network Solutions Ltd, researchers say. A spokesman for Convergent said the company is treating the Bastion Secure site as a "malicious website" and is taking steps to get it removed, he said.

The website includes a quote that claims to be from Tom Deevy, described as a managing director of Bastion Secure. The Mr. Deevy quoted on the site couldn't be reached for comment. Another man named Tom Deevy is a managing director of a company called Bastion Security Products Ltd., a builder of panic rooms and other armored enclosures.

"It's completely fake," Mr. Deevy said of the quote. "We've never even dealt in the cybersecurity world."
Mr. Deevy added that a Gateshead, U.K., address listed by Bastion Secure as its U.K. business location was formerly occupied by his company. "That's an address that we held seven years ago," he said.
Valentina Ochirova contributed to this article.
Ransomware Gang Masquerades as Real Company to Recruit Tech Talent
Credit: By Robert McMillan

DETAILS

Subject:	Software; Researchers; Web sites; Computer security; Employees; Employment; Russian language; Ransomware; Pipelines; Public prosecutors
Business indexing term:	Subject: Employees Employment Ransomware
Location:	United States--US United Kingdom--UK
Company / organization:	Name: BlackMatter; NAICS: 511210
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2021
Publication date:	Oct 21, 2021
column:	Technology
Section:	Tech
Publisher:	Dow Jones &Company Inc
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	2583908432
Document URL:	https://www.proquest.com/newspapers/ransomware-gang-masquerades-as-real-company/docview/2583908432/se-2?accountid=44910
Copyright:	Copyright 2021 Dow Jones &Company, Inc. All Rights Reserved.

Last updated:	2021-10-21
Database:	U.S. Major Dailies