Agents raid home of Kansas man seeking info on botnet that infected DOD network

therecord.media/agents-raid-home-of-kansas-man-seeking-info-on-botnet-that-infected-dod-network/

May 12, 2021

US military investigators have raided the home of a Kansas man looking for information about a crypto-mining botnet that has infected US Air Force servers.

The raid is related to a November 2020 security breach that impacted the US Air Force Office of Special Investigations (OSI), the Air Force's internal law enforcement agency.

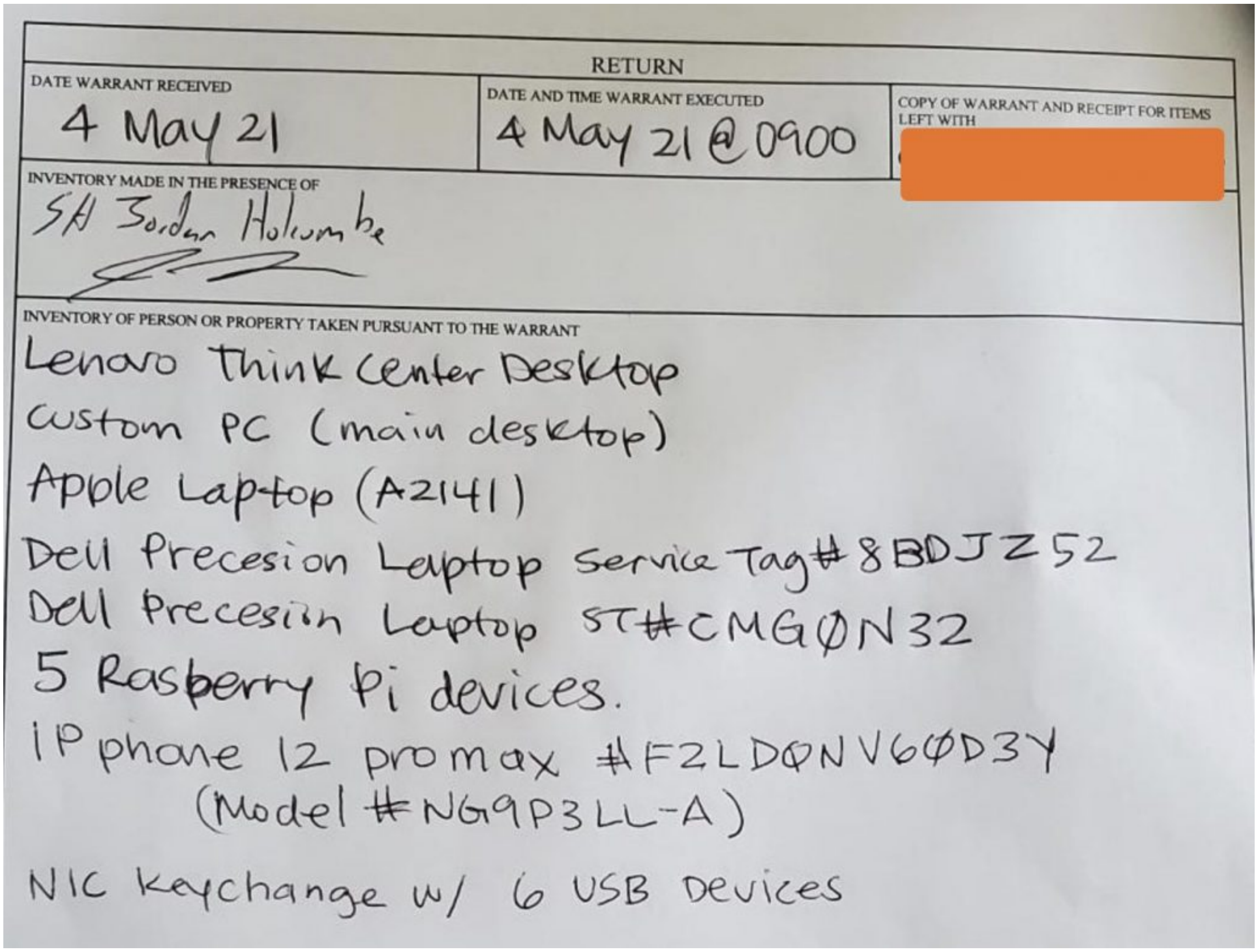
On November 16, 2020, OSI said one of its engineers found a cryptominer on one of its servers during a routine maintenance operation.

The crypto-mining malware, which was running at full capacity, had blocked the server altogether, which was failing to process valid requests.

OSI investigators identified the malware as a version of the Outlaw botnet [1, 2, 3], also known as PerlBot or ShellBot. They also tracked down an IP address that had attempted to connect to the OSI server 38 times in what Air Force investigators called an SSH brute-force attack.

Using a subpoena, OSI traced the IP address at the time of the attacks to a Raspberry Pi device running the Raspbian OS, on Google Fiber account, and a residential address in the city of Olathe, Kansas.

On May 4, law enforcement agents raided the Olathe home, from where they seized several computers, an iPhone, but also five Raspberry Pi devices.



RETURN

DATE WARRANT RECEIVED
4 May 21

DATE AND TIME WARRANT EXECUTED
4 May 21 @ 0900

COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
[redacted]

INVENTORY MADE IN THE PRESENCE OF
SA Jordan Holcumbe

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT
Lenovo Think Center Desktop
custom PC (main desktop)
Apple Laptop (A2141)
Dell Precesion Laptop Service Tag# 8BDJZ52
Dell Precesiin Laptop ST#CMGØN32
5 Rasberry Pi devices.
IP phone 12 promax #FZLDØNV6ØD3Y
(Model #NG9P3LL-A)
NIC keychange w/ 6 USB Devices

Image: The Record

While court documents shared by a source with *The Record* include the home owner's name, a DevOps engineer with government contractor NIC, we will not be naming the man for this article.

Due to how most crypto-mining botnets are designed today, it is unclear if the man was operating the botnet or if their device was merely infected with the Outlaw malware, which then abused the Raspberry Pi system to carry out brute-force attacks without the owner's knowledge, in attempts to find new systems to infect.

Air Force investigators are currently forensically searching the seized devices for evidence that the man was operating the botnet.

OSI officials have not filed formal charges against the Kansas man.

Second incident of its kind

The November 2020 incident is the second time that a cryptocurrency mining botnet has infected a part of the Department of Defense (DOD) network.

A first case was reported via the DOD's bug bounty program in February 2020. At the time, a bug hunter found that a crypto-miner botnet had used a misconfigured Jenkins automation server to plant its malicious scripts on Amazon web servers managed by the DOD.

Tags

- Air Force
- crypto-miner
- cryptomining
- DOD
- investigation
- Kansas
- legal
- Raspberry Pi

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.