SEALED

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

June 2022 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. MAKSIM GALOCHKIN, aka "Bentley," Defendant.	Case No. '23 CR1166 LAB I N D I C T M E N T Title 18, U.S.C., Secs. 1030(a)(2)(C), 1030(a)(5)(A), 1030(a)(7)(C), 1030(c)(2)(B), 1030(c)(4)(B), 1030(c)(3)(A) – Damage to Protected Computers; Title 18, U.S.C., Sec. 2 – Aiding and Abetting; Title 18, U.S.C., Secs. 982(a)(2)(B), 982(b)(1), and 1030(i) and (j) – Criminal Forfeiture

The grand jury charges:

BACKGROUND

1. MAKSIM GALOCHKIN, aka "Bentley," and other persons known and unknown to the grand jury, conspired to attack businesses, nonprofits, and governments in the United States and around the world using malicious software known as "Conti," a type of ransomware.

2. In furtherance of the scheme, the conspirators hacked into victims' computer networks and copied the victims' data to the conspirators' own computers. The conspirators then encrypted the victims' data, which prevented the victims from accessing their own files. The conspirators typically then demanded a ransom to restore the victims' access to their files and to prevent the conspirators from publicly disclosing the hack and releasing the victims' stolen data to the internet.

JIS:nlv:San Diego:6/14/23

3. Different conspirators had different roles in the conspiracy, including: (1) developing Conti ransomware; (2) "crypting" Conti ransomware so that it would evade detection by anti-virus programs; (3) managing teams of hackers; (4) gaining initial access to victims' networks; (5) deploying Conti ransomware on victims' networks; and (6) negotiating with victims.

4. MAKSIM GALOCHKIN, aka "Bentley," and his co-conspirators have accessed without authorization and damaged the computers of more than nine hundred victims worldwide. Victims in approximately forty-seven states, the District of Columbia, Puerto Rico, and approximately thirty-one foreign countries reported Conti ransomware attacks. MAKSIM GALOCHKIN, aka "Bentley," and his co-conspirators attacked Scripps Health in the Southern District of California.

5. MAKSIM GALOCHKIN, aka "Bentley," was a so-called crypter who also managed other crypters. In that role, he scanned Conti's ransomware executable (i.e., a file that caused a computer to perform tasks or launch a software program when executed) to determine whether it would be detected by anti-virus programs and, if so, he modified the executable to ensure that it would evade detection. During his tenure in the Conti conspiracy, MAKSIM GALOCHKIN, aka "Bentley," used the moniker "Bentley," among others.

Count 1

(Access a Protected Computer Without Authorization)

6. On or about May 1, 2021, within the Southern District of California, and elsewhere, the defendant MAKSIM GALOCHKIN, aka "Bentley," did intentionally access a computer without authorization and thereby obtained information from a protected computer; to wit, defendant MAKSIM GALOCHKIN, aka "Bentley," aided and abetted the

intentional accessing of a computer used by Scripps Health without authorization, and thereby obtained information belonging to Scripps Health. The offense was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded $5,000.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B), and 2.

Count 2

(Damage a Protected Computer)

7. On or about May 1, 2021, within the Southern District of California, and elsewhere, defendant MAKSIM GALOCHKIN, aka "Bentley," did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer; to wit, defendant MAKSIM GALOCHKIN, aka "Bentley," knowingly caused the transmission of the Conti malware, and aided and abetted the same, and as a result of such conduct, caused damage without authorization to computers used by Scripps Health. The offense caused loss resulting from a related course of conduct affecting one or more protected computers aggregating at least $5,000 in value, the modification and impairment of the medical examination, diagnosis, treatment, and care of one or more individuals, a threat to public health and safety, and damage affecting 10 or more protected computers during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and 2.

//

//

//

Count 3

(Threatening to Damage a Protected Computer)

8. On or about May 1, 2021, within the Southern District of California, and elsewhere, defendant MAKSIM GALOCHKIN, aka "Bentley," with intent to extort from persons money and other things of value, transmitted in interstate and foreign commerce a communication containing a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion; to wit, defendant MAKSIM GALOCHKIN, aka "Bentley," aided and abetted the transmission of a ransom note to Scripps Health containing a demand and request for virtual currency in relation to Conti malware installed on the computers of Scripps Health. All in violation of Title 18, United States Code, Sections 1030(a)(7)(C), (c)(3)(A), and 2.

Criminal Forfeiture

9. Upon conviction of any of the offenses alleged in this indictment, defendant MAKSIM GALOCHKIN, aka "Bentley," shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting or derived from proceeds obtained directly or indirectly as a result of the offenses, and, pursuant to Title 18, United States Code, Section 1030(i) and (j), defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violations and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violations.

//

//

10. In the event that any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeit substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2).

All in violation of Title 18, United States Code, Sections 982(a)(2)(B), 982(b)(1), and 1030(i) and (j).

DATED: June 14, 2023.

[redacted]

RANDY S. GROSSMAN
United States Attorney

By: Jonathan I. Shapiro
JONATHAN I. SHAPIRO
KAREEM A. SALEM
Assistant U.S. Attorneys

I hereby attest and certify on 06/15/2023
That the foregoing document is a full, true and correct copy of the original on file in my office and in my legal custody.

CLERK U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

By M. Valle Deputy