PERISCOPE

July 13, 2022

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **bl33d**, **instruktor**, **mavr** and **parcal11** engaged in tax fraud and scams and the actors **edison**, **hdseo** and **Lebongolfeur** offered and sought insider services. Additionally, the actors **redpoint** and **Win_Ex** offered exploits for privilege escalation vulnerabilities, while the actors **barf**, **fckers47** and **t3ct0nic** targeted entities in India.

Threat actors engage in tax fraud, scams

- On July 2, 2022, the actor **parcal11** offered to sell photos of documents from Australia, the U.K. and the U.S. including address registration records, driver's licenses, identity cards, insurance documents, passports, Social Security numbers (SSNs), taxpayer identity documents and utility bills. The actor also offered a database containing selfies with Canadian documents, but the documents themselves were not available. The offer includes business and personal tax documents such as 1040 U.S. Individual Income Tax Return and W-2 Wage and Tax Statement forms.
- On July 3, 2022, the actor **bl33d** auctioned 1040, 1120 U.S. Corporation Income Tax Return and W-2 tax forms organized in four folders. The first allegedly includes files for more than 300 unique clients. The second has about 430 files with multiple forms including 1120-S, 1065 U.S. Return of Partnership Income and Schedule K-1 forms from 2021. The third has 140 tax documents from 2020. The fourth has more than 30 company-related documents including articles of incorporation and a few driver's licenses.
- On July 6, 2022, the actor **instruktor** offered to sell more than 100,000 W-2, 1040 and 1099 Miscellaneous Income tax forms collected between 2019 and 2021. The forms allegedly come with bank account and routing numbers, dates of birth (DOBs), email addresses, full information, phone numbers and SSNs. The actor specified all the files are in portable document format ([.]pdf) and suggested using the documents for automated clearing house (ACH) debit transactions or operations with checks.
- On July 6, 2022, the actor **mavr** auctioned 1,000 data sets including 1040 and W-2 tax forms from 2020 and 2021, bank account numbers and routing numbers, DOBs and SSNs. Some sets allegedly included 1098 Mortgage Interest Statement and 1099 tax forms.

Threat actors offer, seek insider services

- On July 2, 2022, the actor **hdseo** sought a France-based insider related to government, insurance, public health care system or national data. The actor claimed the data the insider provides will be used for "doxxing" or releasing personal information for malicious purposes.
- On July 2, 2022, the actor **Lebongolfeur** claimed to be an employee at an undisclosed bank with access to all customer data such as addresses, bank account numbers, current balances, DOBs, email addresses, names, phone numbers, security questions with answers and social insurance numbers. The actor admitted to having no hacking skills and expressed interest in partnering with someone from the forum to exploit the information.
- On July 6, 2022, the actor **edison** sought insiders working for large companies from a variety of industries. The actor claimed the insiders would have to run an allegedly malicious file the actor provides on the company's computer and added the reward might be five times the insider's annual income or higher.

Threat actors offer exploits for privilege escalation vulnerabilities

- On July 5, 2022, the actor **Win_Ex** offered to sell an exploit for a zero-day local privilege escalation (LPE) vulnerability in Windows operating system (OS) versions 8.1 through 11. The actor specified the vulnerability exists due to a race condition in the kernel image ntoskrnl[.]exe, which allegedly leads to use-after-free (UAF). The offer includes the source code written in the C programming language and a test example showing how the exploit operates. The actor noted the exploit only performs successfully at the medium integrity level but not low.
- On July 6, 2022, the actor **redpoint** offered to sell an exploit for the Windows common log file system driver elevation of privilege vulnerability tracked as CVE-2022-24521. The description claimed the exploit can bypass Windows Defender and remain fully undetectable (FUD) by other antivirus programs. The actor claimed the exploit would be provided in the dynamic-link library ([.]dll) or executable ([.]exe) file format.

Threat actors target entities in India

- On July 3, 2022, the actor **barf** auctioned unauthorized remote desktop protocol (RDP) access to an Indian iodine producer. The company allegedly has a revenue of 5 million in an unspecified currency and has 45 machines in its network according to the Advanced IP Scanner network scanning tool. The actor specified the partial IP address of the impacted host and claimed user privileges are available.
- On July 3, 2022, the actor **fckers47** advertised a data leak that allegedly impacts an India-based news and recommendations platform. The description claimed the leak contains a structured query language (SQL) database with information on more than 10,000 users including email addresses, names and phone numbers and application programming interfaces (APIs) of the impacted website. The actor shared a link to access the compromised data.
- On July 6, 2022, the actor **t3ct0nic** advertised a data set allegedly dumped from an India-based home finance company. The actor provided a link to an alleged sample of the compromised data and claimed the full data dump contains passports and other payment information.