PRODAFT

Threat Intelligence Insights

VoipDialer

Automated Vishing Attack Targeting one of the Biggest US Banks

The PRODAFT Threat Intelligence (PTI) team has detected an autonomous version of fraudulent banking calls. *107'434 calls were made to customers of one of the largest U.S. banks that fell victim to a voice phishing attack ("vishing"),* created to automatically call the victims and record their credit card and personal information. The cybercriminal managed to steal more than thousands of credit cards. Up to now, it has been the most successful autonomous voice phishing attack in the USA, which raises concerns for the European financial sector as well. According to the FBI's Internet Crime Report, vishing is among the top 5 cyberattack trends in 2021.

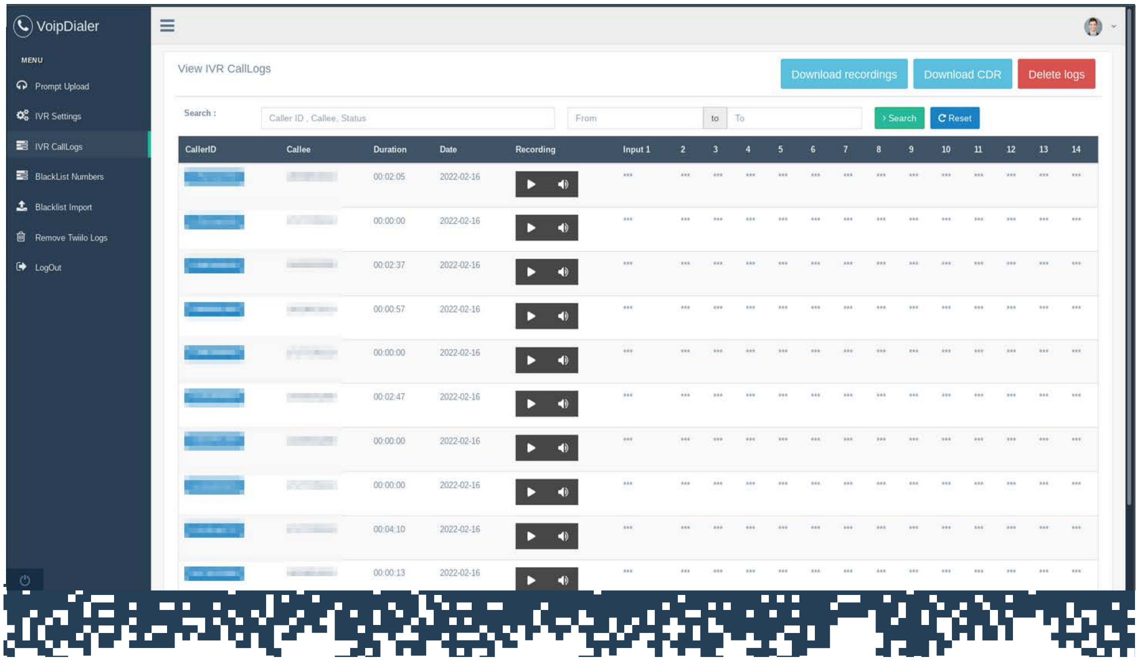
Attack Highlights

Threat Type:	Motivation:	Target country:	Total calls:
Voice Phishing	**Financial**	**USA**	**107'434**

Listen to one of the recorded conversation

The Strategy

Rather than calling the victims, the attacker built AI-powered conversational IVRs with Programmable Voice and Autopilot that recognize users' intent, collect data from users, answer frequently asked questions, record the call, and extract the information into a CSV file.



View IVR CallLogs

CallerID	Callee	Duration	Date	Recording	Input 1	2	3	4	5	6	7	8	9	10	11	12	13	14
[redacted]	[redacted]	00:02:05	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:00:00	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:02:37	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:00:57	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:00:00	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:02:47	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:00:00	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:00:00	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:04:10	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***
[redacted]	[redacted]	00:00:13	2022-02-16	▶ 🔊	***	***	***	***	***	***	***	***	***	***	***	***	***	***

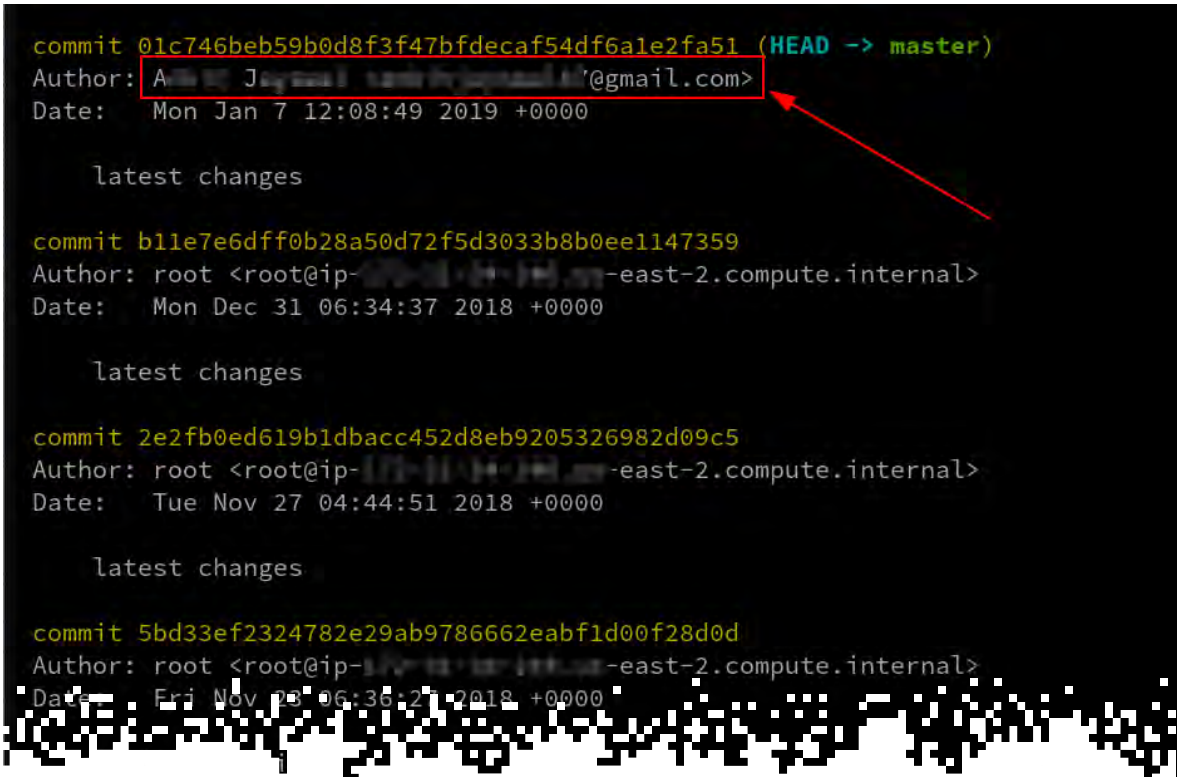
IVR (Interactive Voice Response) Call Logs Page

Twilio and Asterisk were among the different programs used to provide programmable communication tools for making and receiving phone calls, sending and receiving text messages, and performing other communication functions using its web service APIs.

Bankers or law enforcement were avoided with the added feature to import blacklist numbers. The complete automated process was intended to provide passive income to the attacker.

The Attacker

PRODAFT investigators discovered the attack on 16.02.2022. The attacker committed crucial mistakes leaving his credentials on GitHub. All this helped the PTI team to reveal his complete identity. The attacker was a web developer from Ahmedabad, Gujarat, India, whose origin server was in France. He was targeting regular customers of one of the biggest US banks.



```
commit 01c746beb59b0d8f3f47bfdecaf54df6a1e2fa51 (HEAD -> master)
Author: A[redacted] J[redacted]@gmail.com>
Date:   Mon Jan 7 12:08:49 2019 +0000

    latest changes

commit b11e7e6dff0b28a50d72f5d3033b8b0ee1147359
Author: root <root@ip-[redacted]-east-2.compute.internal>
Date:   Mon Dec 31 06:34:37 2018 +0000

    latest changes

commit 2e2fb0ed619b1dbacc452d8eb9205326982d09c5
Author: root <root@ip-[redacted]-east-2.compute.internal>
Date:   Tue Nov 27 04:44:51 2018 +0000

    latest changes

commit 5bd33ef2324782e29ab9786662eabf1d00f28d0d
Author: root <root@ip-[redacted]-east-2.compute.internal>
Date:   Fri Nov 23 06:36:27 2018 +0000
```

The trace of the attacker

Victim Data

Successful calls:	Stolen credit cards:	Age 50+:
25’184	**Thousands**	**75%**

The Findings

It was the first time the PTI team had encountered such a streamlined and automatic system for credit card fraud. PRODAFT's investigators gained visibility on the VoIP Dialer Panel and found ***25'184 sound files, which represents 23% of total calls.*** Each recorded audio was 5-6 minutes long, and the critical information was extracted into a CSV file. You can hear one of the audio recordings here.

The hacker stole thousands of credit cards. Audio calls were made to 107'434 customers of one of the biggest US banks, victims of the automated voice phishing attack.

Vishing and Credit Card Fraud Prevention

Notwithstanding that the targeted bank was from the US, the same type of attack could be easily adapted by cybercriminals to target other financial institutions in Europe as well.

Enterprise executives and their risk advisors need in-depth threat intelligence to mitigate these threats while minimizing the damage they cause. The work of our TI team is crucial toward understanding the cybercrime landscape.

Our TI platform relies on dozens of intelligence collection tools that monitor thousands of different sources and detect security issues earlier and faster to meet the challenges of today's complex cyberattacks. Proactive threat intelligence is key to identifying the factors contributing to cybercrime trends and preventing the threat actors from exploiting enterprise vulnerabilities.