Data Breach Today
Prevention. Response. Notification.
https://www.databreachtoday.com/

Cybercrime , Cybercrime as-a-service , Fraud Management & Cybercrime

The Evolution of a Nigerian Scammer

Report Illustrates Increasingly Sophisticated Tactics

Ishita Chigilli Palli (Ishita_CP) • March 18, 2020

Nigerian scammers have come a long way since the days of posing as a prince who needs help hiding his vast fortune, a new report illustrates.

See Also: Live Webinar | How to Identify & Address Risk with Attack Simulation

In a report released Tuesday by Check Point Research, analysts describe how one scammer became so proficient that over seven years he earned $100,000, or 14 times the national minimum wage in Nigeria and nearly three times the average yearly salary in the nation.

The report offers a look at how cybercrime has developed over the last several years as fraudsters rent the malicious tools that they need (see: *New Ransomware-as-a-Service Offered at Deep Discount: Report*).

The scammer portrayed in the report apparently started his career buying stolen credit cards and other payment data, and then began using off-the-shelf malware such as infostealers, exploits and keyloggers. Eventually, he hired more skilled developers to create remote access Trojans and other malware, according to the report.

The scammer's journey into cybercrime, the report states, "shows how even a relatively unskilled and undisciplined individual can profit handsomely from fraud and malicious online activity."

Other reports have also shown how Nigerian scams have grown more sophisticated thanks to cybercrime as a service. In May 2019, for instance, Palo Alto Networks' Unit 42 described the exploits of group called SilverTerrier that used about 20 types of commodity malware, including information stealers and RATs (see: *Nigerian BEC Scammers Use Malware to Up the Ante*).

Business email compromise scams have also proliferated with Nigerian gangs (see: *80 Indicted for Scams, Including Business Email Compromises*).

Tracking One Scammer

As part of the research, Check Point analysts tracked the movements of one scammer, who lives in Benin City, Nigeria, and has made a career as a cybercriminal under the alias "Bill Henry."

Starting around 2013, the scammer started out by spending about $13,000 for 1,000 stolen credit card credentials that he purchased from an online marketplace called the Ferrum Shop, according to the report. The scammer then make a series of charges on the stolen cards for about $550, the researchers note, adding that if the transactions did not go through, he would try a different merchant or buy another credit card.

"A back-of-the-envelope calculation shows that during the years 2013-2020, the $13,000 spent by this account were converted into about 1,000 credit cards, which were then fraudulently charged for a total easily exceeding $100,000 - probably several times that," the report says.

Buying stolen credit card information and having to constantly pay for it, however, was not as lucrative as the scammer hoped, so he moved to the next level and started stealing credentials himself, the researchers note. He started buying "leads" or email addresses for potential targets in bulk, the report says.

Following this, the scammer began spending money on malicious tools to help craft his own malware to starting spamming victims with phishing emails, according to Check Point.

Custom-Built RATs

The researchers also found that the scammer did not work alone, but instead reported to a manager, who in turn had another manager. The scammer got the capital required for his operations from these managers, who then demanded returns on their investments, the report notes.

"It's the cybercrime equivalent of a 'pyramid selling' or multi-level marketing scheme," the researchers note.

This pressure appears to have driven the scammer to venture out on his own and develop his own malware, which would not have a known signature and could bypass weaker security defenses, the report says.

To write the code he needed for the malware, the scammer hired a developer who goes by "RATs &exploits" after finding him on Discord, an online chat platform used mainly by gamers, according to the report. In turn, the scammer infected the developer's device with a different RAT in order to keep tabs on him and follow his progress, the report notes.

In another incident, the scammer worked with a different developer called "n0$f3ratu$" - Nosferatus - to buy a dataprotector that would help him pack his own malware binaries, according to the report. When not pleased with the results, the scammer reported that developer to Interpol, the analysts note.

The Check Point researchers note that the scammer is still operating in Nigeria. The analysts, however, have shared their research with police in Nigeria as well as other international law enforcement officials, they say.

About the Author

Ishita Chigilli Palli

Senior Correspondent, Global News Desk

As senior correspondent for Information Security Media Group's global news desk, Ishita covers news worldwide. She previously worked at Thomson Reuters, where she specialized in reporting breaking news stories on a variety of topics.