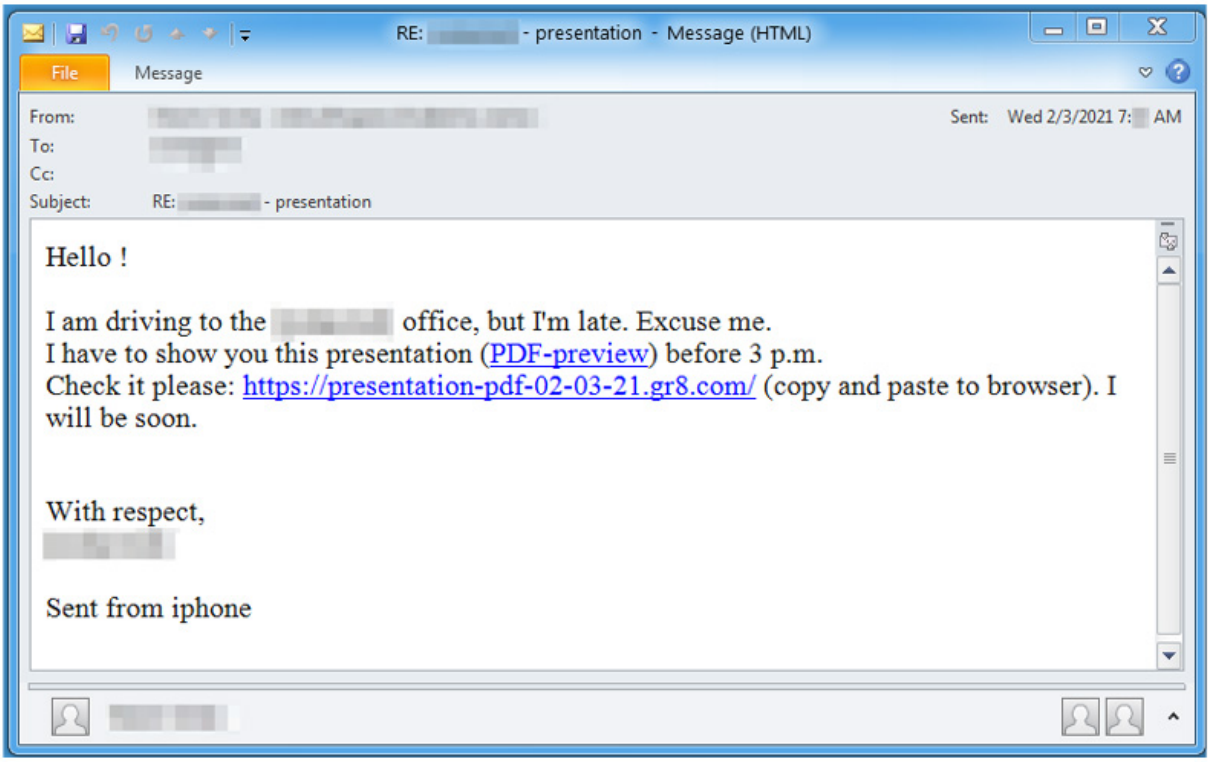
Spear-Phishing Campaign Distributes Nim-Based Malware

healthcareinfosecurity.com/spear-phishing-campaign-distributes-nim-based-malware-a-16176

Cybercrime , Fraud Management & Cybercrime , Fraud Risk Management

NimzaLoader Uses Nim Programming Language to Avoid Detection Prajeet Nair (@prajeetspeaks) • March 12, 2021



TA800 targets individuals with tailored phishing emails. (Source: Proofpoint)
An ongoing spear-phishing campaign by the threat group TA800 is distributing a new malware loader based on the Nim programming language that's designed to help avoid detection, according to the cybersecurity company Proofpoint.

See Also: OnDemand | Understanding Human Behavior: Tackling Retail's ATO & Fraud Prevention Challenge

“TA800 has predominantly used BazaLoader since April of 2020, but on February 3, 2021 they distributed this new malware we are calling NimzaLoader,” says Sherrod DeGrippo, senior director of Proofpoint's threat research and detection team. “This malware is exclusive to TA800, and we've only seen it distributed once. This could be a sign of more to come.”

Lewis Jones, threat intelligence analyst at cybersecurity company Talion, notes: "The use of Nim is uncommon for malware in the threat landscape. However we have recently seen a Nim-based downloader used by the Zebrocy threat group. It is likely that the threat actors are switching to Nim to avoid detection by defense teams who may not be familiar with the language."

Proofpoint researchers also found evidence suggesting NimzaLoader is being used to download and execute Cobalt Strike as its secondary payload.

NimzaLoader Malware

On Feb. 3, researchers discovered the Nim-based malware was being distributed via phishing. The messages are often designed to look as if they came from within the targeted company, DeGrippo says. “Lures have included hard-to-resist subjects, such as payments, meetings, termination, bonuses and complaints in the subject line or body of the email,” he says

The message contained links portrayed as a PDF preview that are actually links to a GetResponse (an email marketing service) landing page, Proofpoint discovered.

"The landing pages contained a link to the 'PDF' which was the NimzaLoader executable hosted on Slack and used a fake Adobe icon in an attempt to fool the user," the researchers note.

Nim-related strings used by the malware are encrypted when stored by using an XOR-based algorithm and a single key per string. One of those encrypted strings is a timestamp used as an expiration date for the malware, Proofpoint says.

"At the time of research, all known NimzaLoader C2s were down, but a public malware sandbox run seems to show it receiving a 'powershell' command that ultimately delivered a Cobalt Strike beacon," the researchers say. "We are unable to validate or confirm this finding, but it does align with past TA800 tactics, techniques and procedures."

Evolving Tactics

The switch to using Nim is a good example of how threat actors are constantly changing tactics to avoid detection, Jones says.

"The activity has so far been linked to TA800, who are a threat group that has targeted a wide range of industries infecting victims with banking Trojans and malware loaders," Jones says. "Previous activity by the group has often shown how the group has completed initial reconnaissance on targets to specifically target individuals with tailored phishing emails attempting to look more genuine and increasing success of the campaigns."

In the fourth quarter of last year, TA800 was responsible for a wave of attacks against the healthcare sector using a loader called BazaLoader DeGrippo says. “BazaLoader, under the control of a separate threat actor, subsequently installed a ransomware strain called Ryuk.”

DeGrippo says Proofpoint's analysis corroborates analysis by other researchers that NimzaLoader is not a BazaLoader variant. That's because NimzaLoader is written in a different programming language and does not use the same code-flattening obfuscator.