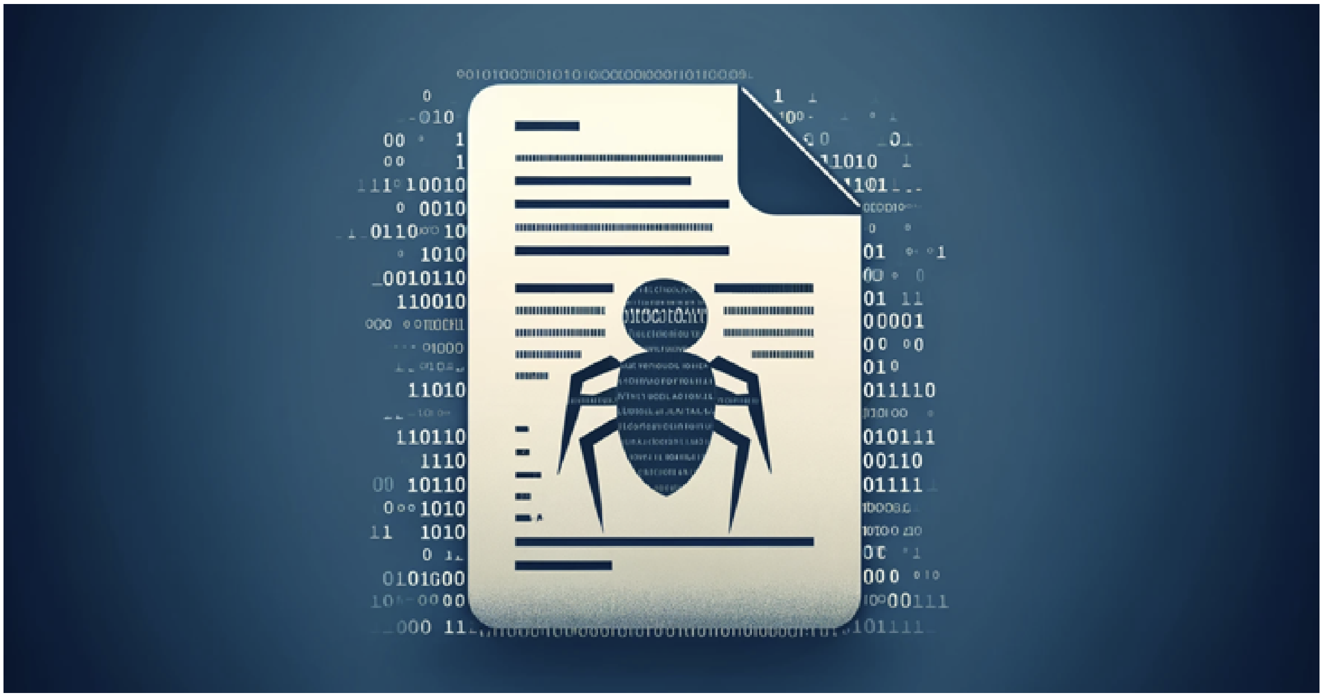
More_eggs Malware Disguised as Resumes Targets Recruiters in Phishing Attack

thehackernews.com/2024/06/moreeggs-malware-disguised-as-resumes.html

June 10, 2024



Cybersecurity researchers have spotted a phishing attack distributing the More_eggs malware by masquerading it as a resume, a technique originally detected more than two years ago.

The attack, which was unsuccessful, targeted an unnamed company in the industrial services industry in May 2024, Canadian cybersecurity firm eSentire disclosed last week.

"Specifically, the targeted individual was a recruiter that was deceived by the threat actor into thinking they were a job applicant and lured them to their website to download the loader," it said.

More_eggs, believed to be the work of a threat actor known as the Golden Chickens (aka Venom Spider), is a modular backdoor that's capable of harvesting sensitive information. It's offered to other criminal actors under a Malware-as-a-Service (MaaS) model.

Last year, eSentire unmasked the real-world identities of two individuals – Chuck from Montreal and Jack – who are said to be running the operation.

The latest attack chain entails the malicious actors responding to LinkedIn job postings with a link to a fake resume download site that results in the download of a malicious Windows Shortcut file (LNK).

Watch Now

That Phishy Feeling:
Learning to Spot Modern Phishing

HUNTRESS

It's worth noting that previous More_eggs activity has targeted professionals on LinkedIn with weaponized job offers to trick them into downloading the malware.

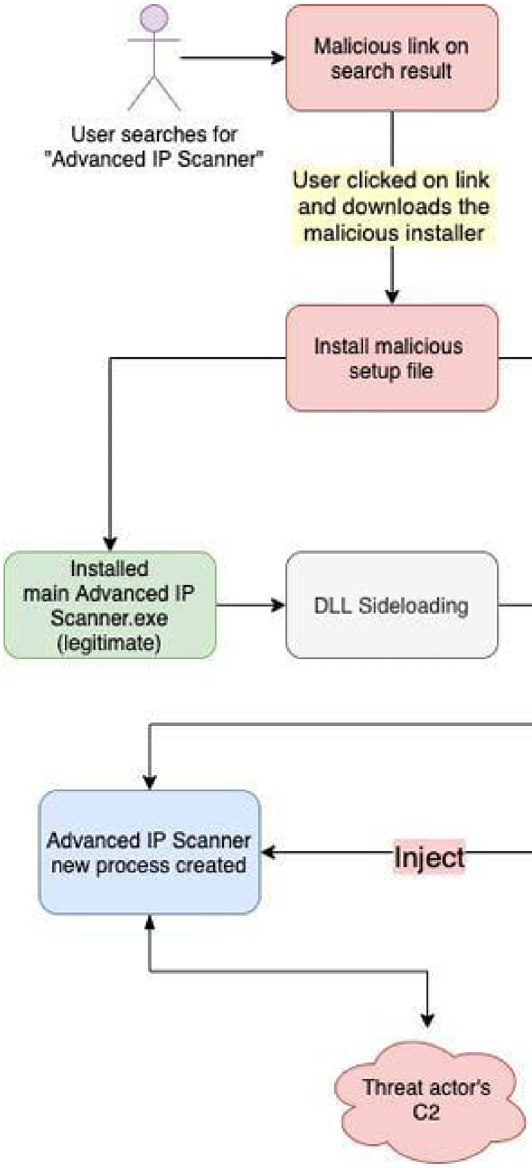
"Navigating to the same URL days later results in the individual's resume in plain HTML, with no indication of a redirect or download," eSentire noted.

The LNK file is then used to retrieve a malicious DLL by leveraging a legitimate Microsoft program called ie4uinit.exe, after which the library is executed using regsvr32.exe to establish persistence, gather data about the infected host, and drop additional payloads, including the JavaScript-based More_eggs backdoor.

"More_eggs campaigns are still active and their operators continue to use social engineering tactics such as posing to be job applicants who are looking to apply for a particular role, and luring victims (specifically recruiters) to download their malware," eSentire said.

"Additionally, campaigns like more_eggs, which use the MaaS offering appear to be sparse and selective in comparison to typical malspam distribution networks."

The development comes as the cybersecurity firm also revealed details of a drive-by download campaign that employs fake websites for the KMSPico Windows activator tool to distribute Vidar Stealer.


User searches for "Advanced IP Scanner"
Malicious link on search result
User clicked on link and downloads the malicious installer
Install malicious setup file
Installed main Advanced IP Scanner.exe (legitimate)
DLL Sideloading
Installed malicious pcre.dll
Decrypt blob
Advanced IP Scanner new process created
Inject
CobaltStrike Beacon
Threat actor's C2

"The kmspico[.]ws site is hosted behind Cloudflare Turnstile and requires human input (entering a code) to download the final ZIP package," eSentire noted. "These steps are unusual for a legitimate application download page and are done to hide the page and final payload from automated web crawlers."

Similar social engineering campaigns have also set up lookalike sites impersonating legitimate software like Advanced IP Scanner to deploy Cobalt Strike, Trustwave SpiderLabs said last week.

It also follows the emergence of a new phishing kit called V3B that has been put to use to single out banking customers in the European Union with the goal of stealing credentials and one-time passwords (OTPs).

CIS SecureSuite®

The kit, offered for $130-$450 per month through a Phishing-as-a-Service (PhaaS) model on the dark web and a dedicated Telegram channel, is said to have been active since March 2023. It's designed to support over 54 banks located in Austria, Belgium, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, and the Netherlands.

The most important aspect of V3B is that it features customized and localized templates to mimic various authentication and verification processes common to online banking and e-commerce systems in the region.

It also comes with advanced capabilities to interact with victims in real-time and get their OTP and PhotoTAN codes, as well as execute a QR code login jacking (aka QRLJacking) attack on services such as WhatsApp that allow sign-in via QR codes.

"They have since built a client base focused on targeting European financial institutions," Resecurity said. "Currently, it is estimated that hundreds of cybercriminals are using this kit to commit fraud, leaving victims with empty bank accounts."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

SHARE
SHARE