APT28 Hacker Group Targeting Europe, Americas, Asia in Widespread Phishing Scheme

thehackernews.com/2024/03/apt28-hacker-group-targeting-europe.html

March 18, 2024

The Russia-linked threat actor known as **APT28** has been linked to multiple ongoing phishing campaigns that employ lure documents imitating government and non-governmental organizations (NGOs) in Europe, the South Caucasus, Central Asia, and North and South America.

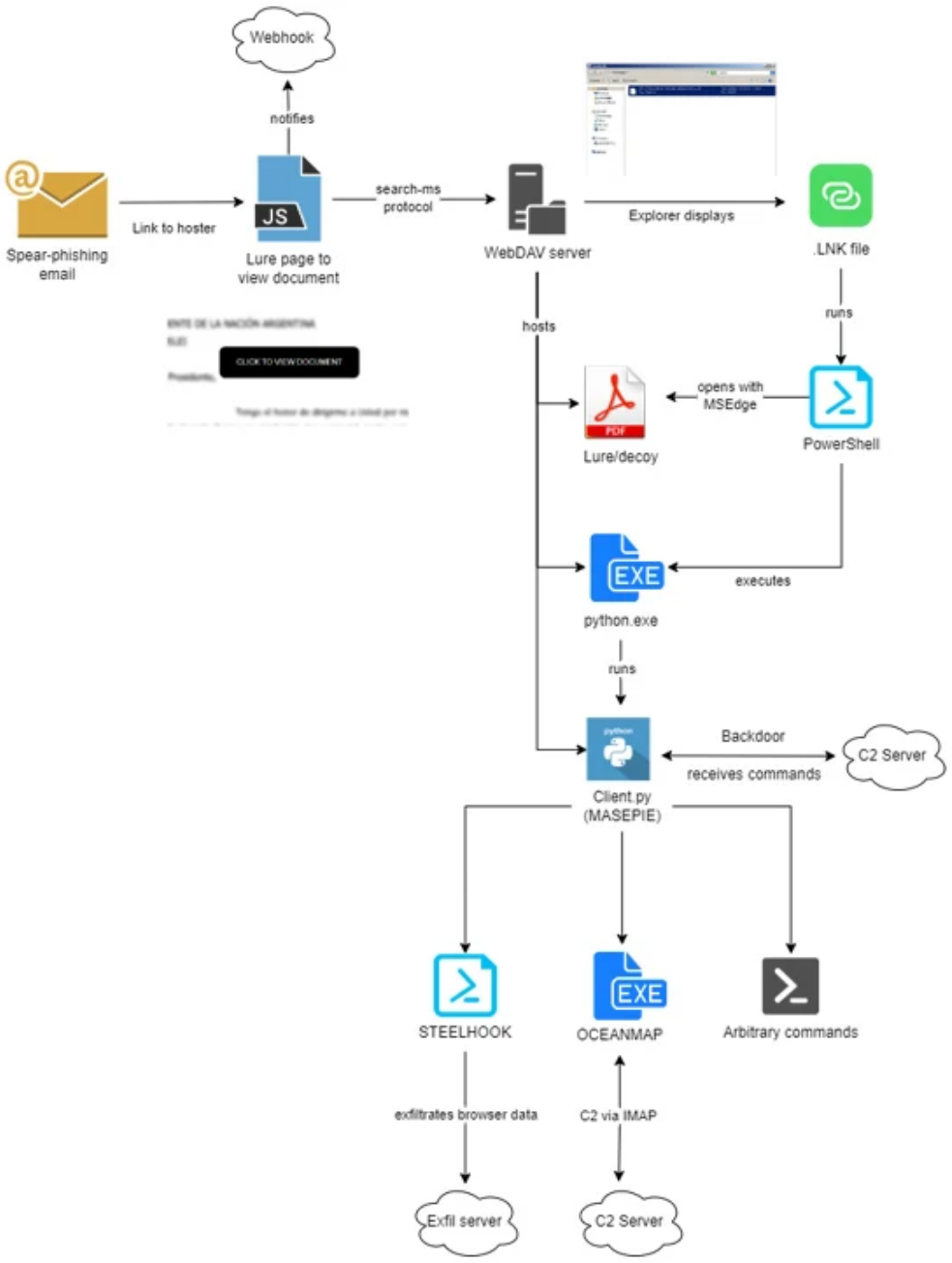
"The uncovered lures include a mixture of internal and publicly available documents, as well as possible actor-generated documents associated with finance, critical infrastructure, executive engagements, cyber security, maritime security, healthcare, business, and defense industrial production," IBM X-Force said in a report published last week.

The tech company is tracking the activity under the moniker ITG05, which is also known as Blue Athena, BlueDelta, Fancy Bear, Fighting Ursa, Forest Blizzard (formerly Strontium), FROZENLAKE, Iron Twilight, Pawn Storm, Sednit, Sofacy, TA422, and UAC-028.

The disclosure comes more than three months after the adversary was spotted using decoys related to the ongoing Israel-Hamas war to deliver a custom backdoor dubbed HeadLace.

APT28 has since also targeted Ukrainian government entities and Polish organizations with phishing messages designed to deploy bespoke implants and information stealers like MASEPIE, OCEANMAP, and STEELHOOK.

Other campaigns have entailed the exploitation of security flaws in Microsoft Outlook (CVE-2023-23397, CVSS score: 9.8) to plunder NT LAN Manager (NTLM) v2 hashes, raising the possibility that the threat actor may leverage other weaknesses to exfiltrate NTLMv2 hashes for use in relay attacks.



The latest campaigns observed by IBM X-Force between late November 2023 and February 2024 take advantage of the "search-ms:" URI protocol handler in Microsoft Windows to trick victims into downloading malware hosted on actor-controlled WebDAV servers.

There is evidence to suggest that both the WebDAV servers, as well as the MASEPIE C2 servers, may be hosted on compromised Ubiquiti routers, a botnet comprising which was taken down by the U.S. government last month.

The phishing attacks impersonate entities from several countries such as Argentina, Ukraine, Georgia, Belarus, Kazakhstan, Poland, Armenia, Azerbaijan, and the U.S., putting to use a mix of authentic publicly available government and non-government lure documents to activate the infection chains.

"In an update to their methodologies, ITG05 is utilizing the freely available hosting provider, firstcloudit[.]com to stage payloads to enable ongoing operations," security researchers Joe Fasulo, Claire Zaboeva, and Golo Mühr said.

The climax of APT28's elaborate scheme ends with the execution of MASEPIE, OCEANMAP, and STEELHOOK, which are designed to exfiltrate files, run arbitrary commands, and steal browser data. OCEANMAP has been characterized as a more capable version of CredoMap, another backdoor previously identified as used by the group.

"ITG05 remains adaptable to changes in opportunity by delivering new infection methodologies and leveraging commercially available infrastructure, while consistently evolving malware capabilities," the researchers concluded.