Justice Department Announces Court-Authorized Seizure of Domain Names Used in Furtherance of Spear-Phishing Campaign Posing as U.S. Agency for International Development

justice.gov/opa/pr/justice-department-announces-court-authorized-seizure-domain-names-used-furtherance-spear

June 1, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, June 1, 2021

Domain Names Were in Part Used to Control a Cobalt Strike Software Tool that the Actors Implanted on Victim Networks

WASHINGTON – On May 28, pursuant to court orders issued in the Eastern District of Virginia, the United States seized two command-and-control (C2) and malware distribution domains used in recent spear-phishing activity that mimicked email communications from the U.S. Agency for International Development (USAID). This malicious activity was the subject of a May 27 Microsoft security alert, titled "New sophisticated email-based attack from Nobelium," and a May 28 FBI and Cybersecurity and Infrastructure Security Agency joint cybersecurity advisory.

The Department's seizure of the two domains was aimed at disrupting the malicious actors' follow-on exploitation of victims, as well as identifying compromised victims. However, the actors may have deployed additional backdoor accesses between the time of the initial compromises and last week's seizures.

“Last week’s action is a continued demonstration of the Department’s commitment to proactively disrupt hacking activity prior to the conclusion of a criminal investigation,” said Assistant Attorney General John C. Demers for the Justice Department’s National Security Division. “Law enforcement remains an integral part of the U.S. government’s broader disruption efforts against malicious cyber-enabled activities, even prior to arrest, and we will continue to evaluate all possible opportunities to use our unique authorities to act against such threats.”

“Cyber intrusions and spear-phishing email attacks can cause widespread damage throughout affected computer networks, and can result in significant harm to individual victims, government agencies, NGOs, and private businesses,” said Acting U.S. Attorney Raj Parekh for the Eastern District of Virginia. “As demonstrated by the court-authorized seizure of these malicious domains, we are committed to using all available tools to protect the public and our government from these worldwide hacking threats.”

“Friday’s court-authorized domain seizures reflect the FBI Washington Field Office’s continued commitment to cyber victims in our region,” said Assistant Director in Charge Steven M. D’Antuono of the FBI’s Washington Field Office. “These actions demonstrate our ability to quickly respond to malicious cyber activities by leveraging our unique authorities to disrupt our cyber adversaries.”

“The FBI remains committed to disrupting this type of malicious cyber activity targeting our federal agencies and the American public,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “We will continue to use all of the tools in our toolbelt and leverage our domestic and international partnerships to not only disrupt this type of hacking activity but to impose risk and consequences upon our adversaries to combat these threats.”

On or about May 25, malicious actors commenced a wide-scale spear-phishing campaign leveraging a compromised USAID account at an identified mass email marketing company. Specifically, the compromised account was used to send spear-phishing emails, purporting to be from USAID email accounts and containing a “special alert,” to thousands of email accounts at over one hundred entities.

Upon a recipient clicking on a spear-phishing email’s hyperlink, the victim computer was directed to download malware from a sub-domain of theyardservice[.]com. Using that initial foothold, the actors then downloaded the Cobalt Strike tool to maintain persistent presence and possibly deploy additional tools or malware to the victim’s network. The actors’ instance of the Cobalt Strike tool received C2 communications via other subdomains of theyardservice[.]com, as well as the domain worldhomeoutlet[.]com. It was those two domains that the Department seized pursuant to the court’s seizure order.

The National Security Division’s Counterintelligence and Export Control Section and the United States Attorney’s Office for the Eastern District of Virginia are investigating this matter in coordination with the FBI’s Cyber Division and Washington Field Office.