

NETMANAGEIT

Intelligence Report

SNS Sender | Active

Campaigns Unleash

Messaging Spam Through

the Cloud

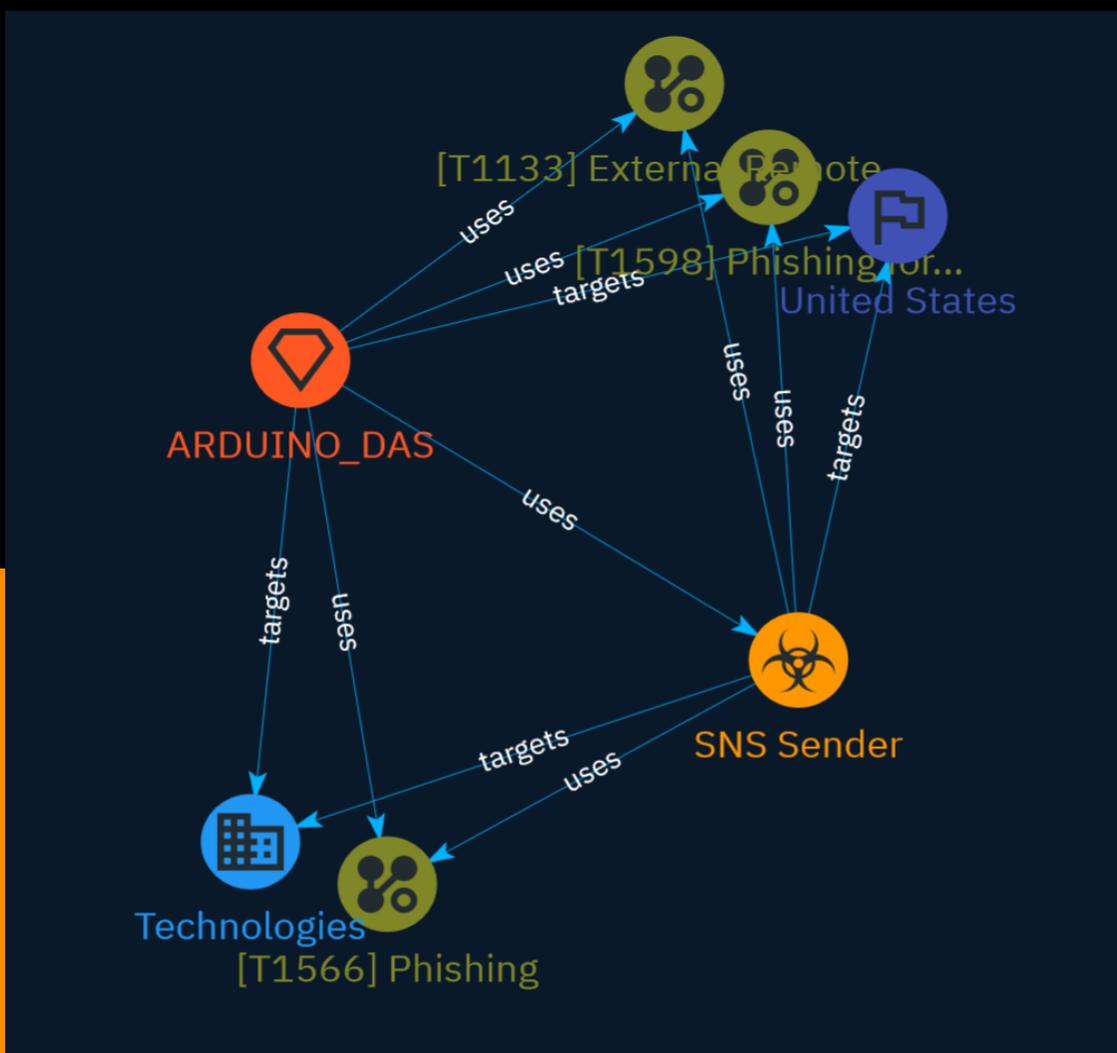


Table of contents

Overview

● Description	3
● Confidence	3
● Content	4

Entities

● Malware	5
● Intrusion-Set	6
● Attack-Pattern	7
● Country	10
● Sector	11

External References

● External References	12
-----------------------	----

Overview

Description

SNS Sender is a script that enables bulk SMS spamming using AWS SNS, a previously unseen technique in the context of cloud attack tools. The script author is known by the alias ARDUINO_DAS and is prolific in the phish kit scene. Links between this actor and phishing kits used to target victims' PII and payment card details were identified. The smishing scams often take the guise of a message from USPS regarding a missed package delivery.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Malware

Name

SNS Sender

Intrusion-Set

Name

ARDUINO_DAS

Attack-Pattern

Name

Phishing for Information

ID

T1598

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](<https://attack.mitre.org/techniques/T1566>) in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMicro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](<https://attack.mitre.org/techniques/T1585>) or [Compromise Accounts](<https://attack.mitre.org/techniques/T1586>)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce)

Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)). (Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (<https://attack.mitre.org/techniques/T1021/006>) and [VNC] (<https://attack.mitre.org/techniques/T1021/005>) can also be used externally. (Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts] (<https://attack.mitre.org/techniques/T1078>) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network. (Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard. (Citation: Trend Micro Exposed Docker Server) (Citation: Unit 42 Hildegard Malware)

Country

Name

United States

Sector

Name

Technologies

Description

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

External References

-
- <https://www.sentinelone.com/labs/sns-sender-active-campaigns-unleash-messaging-spam-through-the-cloud/>
-
- <https://otx.alienvault.com/pulse/65ce21bb10c3a109dcccdf71>