Mar 05 2024

NETMANAGEIT

Intelligence Report

DDoSia project: 2024 updates and behavioural shifts

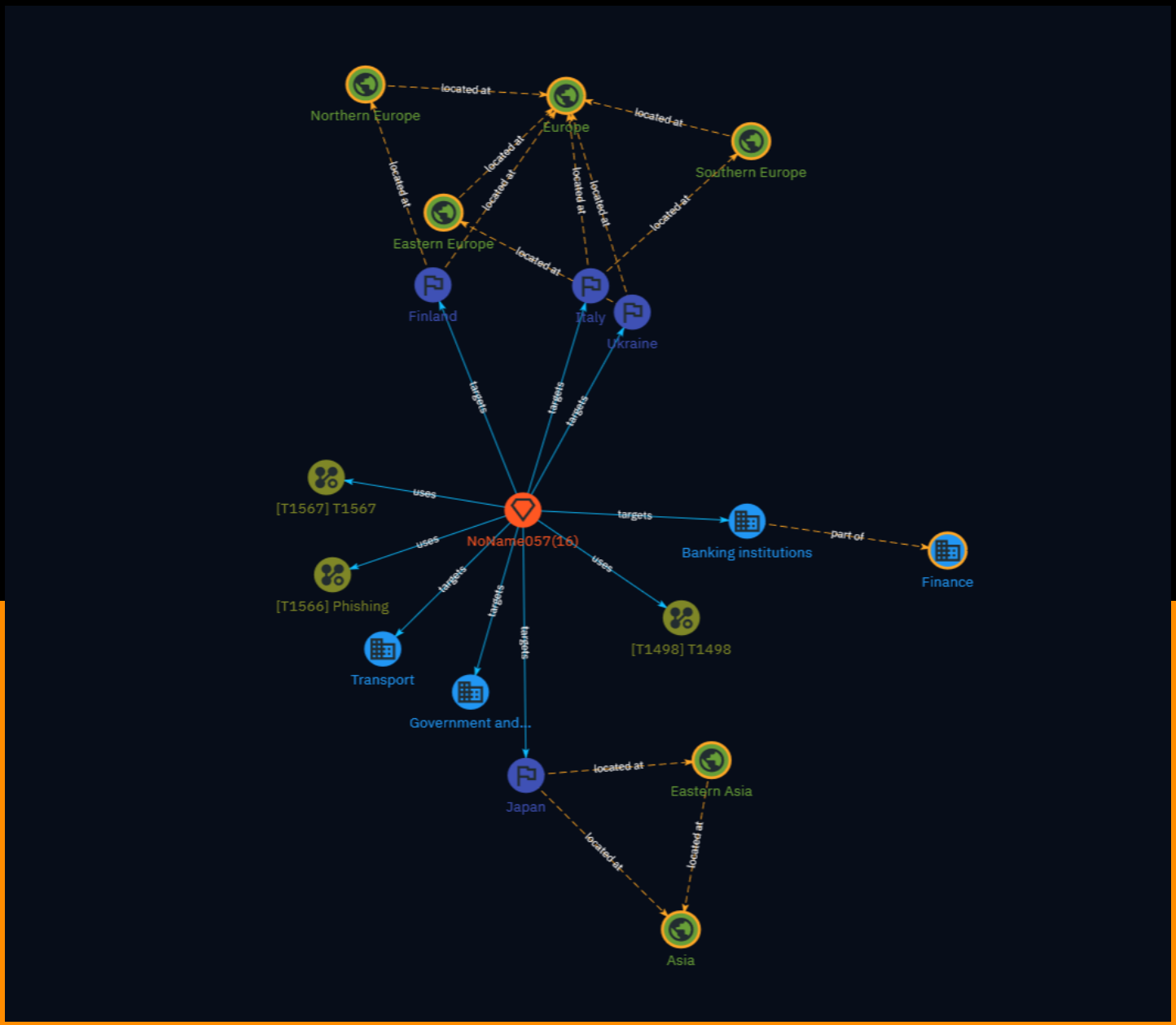

Table of contents

Overview

Entities

External References

Overview

Description

This report details an overview of the changes made by the pro-Russian hacktivist group NoName057(16) in their DDoSia project, from the perspective of the software shared to generate attacks and the evolution of command and control servers. It discusses increased sophistication in data transmission mechanisms, frequent C2 changes indicating disruption efforts, and victimology showing European countries supporting Ukraine remain prime targets, especially impacting government entities. The report concludes that despite infrastructure instability, NoName057(16) persists in daily attacks, likely to continue software updates and expand cooperation with other groups.

Confidence

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

100 / 100

Content

N/A

Intrusion-Set

Name
NoName057(16)

Attack-Pattern

Name
T1498
ID
T1498
Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion. (Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.
Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

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

T1567

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Country

Name
Italy
Name
Finland
Name
Ukraine
Name
Japan

Region

Name
Southern Europe
Name
Northern Europe
Name
Eastern Europe
Name
Europe
Name
Eastern Asia
Name
Asia

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Banking institutions
Description
Credit institutions whose business consists in receiving repayable funds from the public and granting credit. As the bank of banks, central banks are included in this scope.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Name
Transport
Description
All entities involved in the movement of people or goods from one place to another.

External References

- https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts
- https://otx.alienvault.com/pulse/65e5f71435f30008955f046f