Jul 26 2023

NETMANAGEIT

Intelligence Report

Mysterious Decoy Dog malware toolkit still lurks in DNS shadows

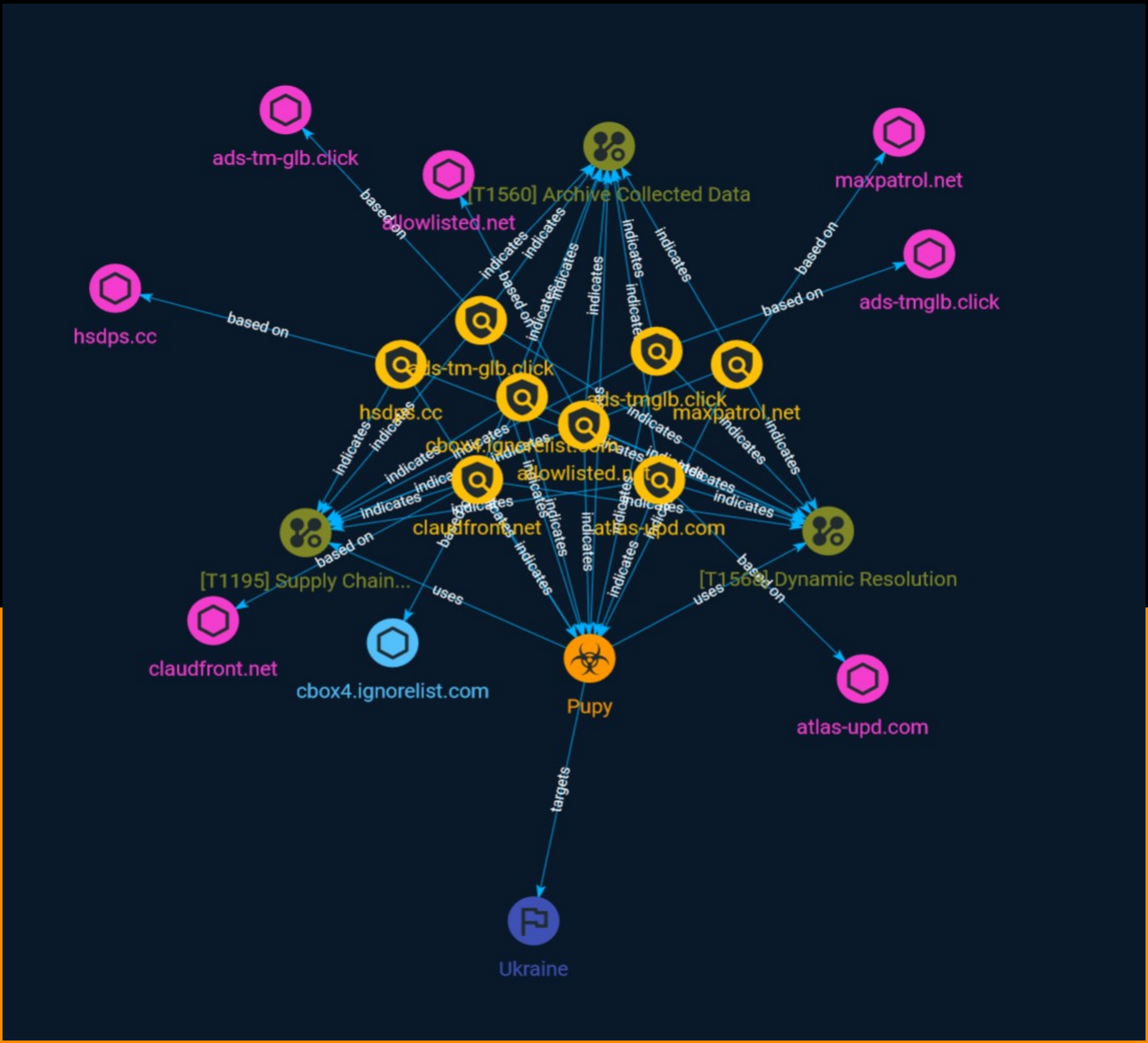

Table of contents

Overview

Entities

Observables

External References

Overview

Description

New details have emerged about Decoy Dog, a largely undetected sophisticated toolkit likely used for at least a year in cyber intelligence operations, relying on the domain name system (DNS) for command and control activity.

Confidence

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

15 / 100

Indicator

Name	ads-tmglb.click
Pattern Type	stix
Pattern	[domain-name:value = 'ads-tmglb.click']
Name	claudfront.net
Pattern Type	stix
Pattern	[domain-name:value = 'claudfront.net']
Name	cbox4.ignorelist.com

Pattern Type

stix

Pattern

[hostname:value = 'cbox4.ignorelist.com']

Name

atlas-upd.com

Pattern Type

stix

Pattern

[domain-name:value = 'atlas-upd.com']

Name

hsdps.cc

Pattern Type

stix

Pattern

[domain-name:value = 'hsdps.cc']

Name

maxpatrol.net

Pattern Type
stix
Pattern
[domain-name:value = 'maxpatrol.net']
Name
allowlisted.net
Pattern Type
stix
Pattern
[domain-name:value = 'allowlisted.net']
Name
ads-tm-glb.click
Pattern Type
stix
Pattern
[domain-name:value = 'ads-tm-glb.click']

Malware

Name
Pupy

Attack-Pattern

Name
Dynamic Resolution
ID
T1568
Description
Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)
Name
Supply Chain Compromise
ID
T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Country

Name
Ukraine

Domain-Name

Value
ads-tm-glb.click
ads-tmglb.click
claudfront.net
allowlisted.net
atlas-upd.com
hsdps.cc
maxpatrol.net

Hostname

Value
cbox4.ignorelist.com

External References

- https://otx.alienvault.com/pulse/64c12c7ccbf6b2e988374eda
- https://www.bleepingcomputer.com/news/security/mysterious-decoy-dog-malware-toolkit-still-lurks-in-dns-shadows/