Aug 28 2023

NETMANAGEIT

Intelligence Report

Adversary On The Defense: ANTIBOT.PW

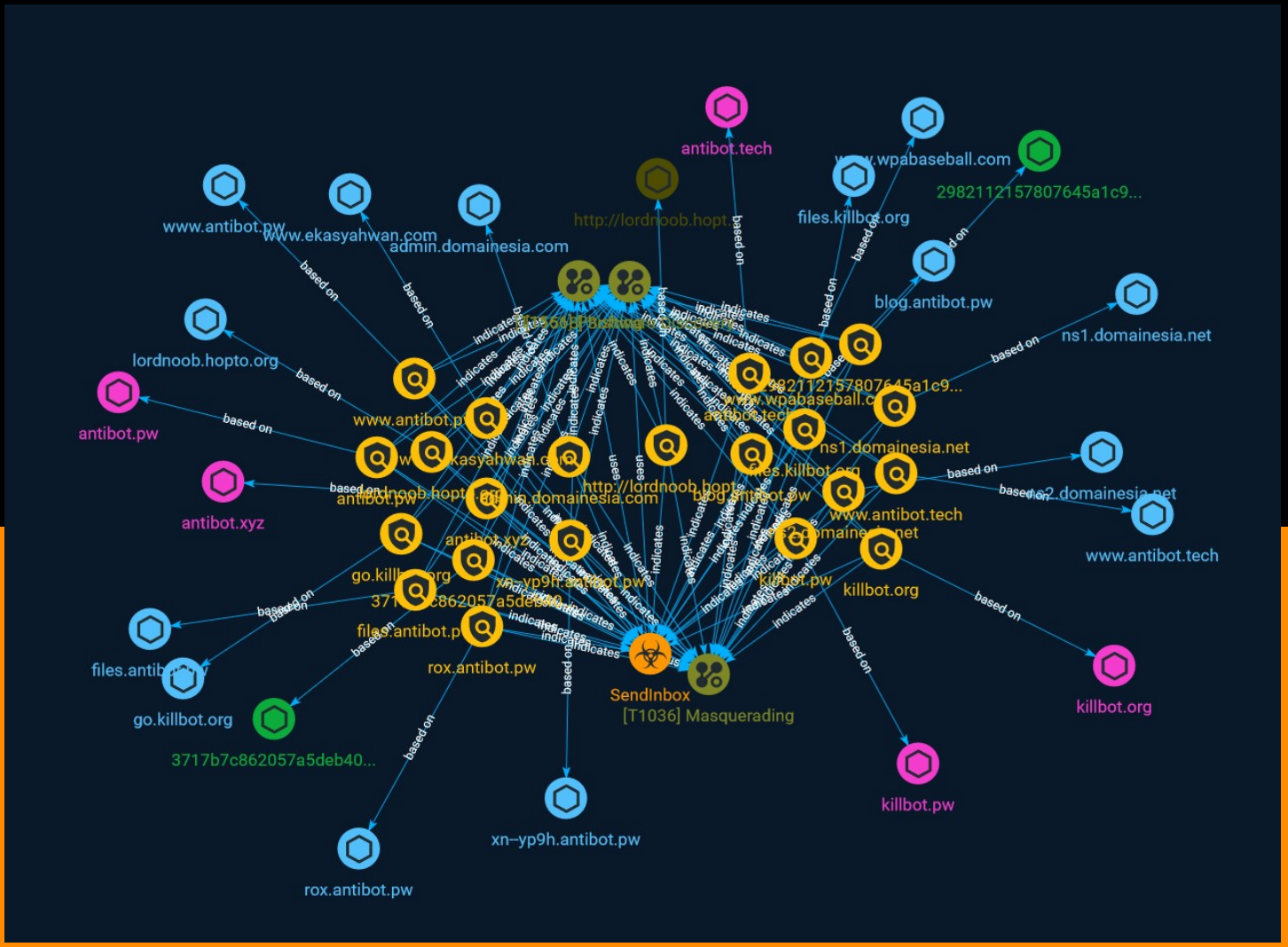

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A look at the use of web traffic filtering tools in the context of malware and phishing operations, as well as the development and development of a commercial platform offering for the service.

Confidence

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

15 / 100

Indicator

Name
antibot.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'antibot.xyz']
Name
admin.domainesia.com
Pattern Type
stix
Pattern
[hostname:value = 'admin.domainesia.com']
Name
www.antibot.tech

Pattern Type

stix

Pattern

[hostname:value = 'www.antibot.tech']

Name

3717b7c862057a5deb406cf747c4669e3f41d217ae66a22a80b0bfe225a731a5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3717b7c862057a5deb406cf747c4669e3f41d217ae66a22a80b0bfe225a731a5']

Name

blog.antibot.pw

Pattern Type

stix

Pattern

[hostname:value = 'blog.antibot.pw']

Name

2982112157807645a1c964e70a44d2a23021d4a62537ad2266445125c8783e5e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2982112157807645a1c964e70a44d2a23021d4a62537ad2266445125c8783e5e']

Name

antibot.pw

Pattern Type

stix

Pattern

[domain-name:value = 'antibot.pw']

Name

killbot.pw

Pattern Type

stix

Pattern

[domain-name:value = 'killbot.pw']

Name
www.wpabaseball.com
Pattern Type
stix
Pattern
[hostname:value = 'www.wpabaseball.com']
Name
go.killbot.org
Pattern Type
stix
Pattern
[hostname:value = 'go.killbot.org']
Name
antibot.tech
Pattern Type
stix
Pattern
[domain-name:value = 'antibot.tech']

Name
files.killbot.org
Pattern Type
stix
Pattern
[hostname:value = 'files.killbot.org']
Name
www.antibot.pw
Pattern Type
stix
Pattern
[hostname:value = 'www.antibot.pw']
Name
ns1.domainesia.net
Pattern Type
stix
Pattern
[hostname:value = 'ns1.domainesia.net']

Name

files.antibot.pw

Pattern Type

stix

Pattern

[hostname:value = 'files.antibot.pw']

Name

http://lordnoob.hopto.org/gx40/sendinbox-master.zip

Pattern Type

stix

Pattern

[url:value = 'http://lordnoob.hopto.org/gx40/sendinbox-master.zip']

Name

ns2.domainesia.net

Pattern Type

stix

Pattern

[hostname:value = 'ns2.domainesia.net']

Name
rox.antibot.pw
Pattern Type
stix
Pattern
[hostname:value = 'rox.antibot.pw']
Name
www.ekasyahwan.com
Pattern Type
stix
Pattern
[hostname:value = 'www.ekasyahwan.com']
Name
xn--yp9h.antibot.pw
Pattern Type
stix
Pattern
[hostname:value = 'xn--yp9h.antibot.pw']

Name
lordnoob.hopto.org
Pattern Type
stix
Pattern
[hostname:value = 'lordnoob.hopto.org']
Name
killbot.org
Pattern Type
stix
Pattern
[domain-name:value = 'killbot.org']

Malware

Name
SendInbox

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)
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

Software Discovery

ID

T1518

Description

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

Domain-Name

Value
antibot.pw
killbot.org
antibot.xyz
antibot.tech
killbot.pw

StixFile

Value
3717b7c862057a5deb406cf747c4669e3f41d217ae66a22a80b0bfe225a731a5
2982112157807645a1c964e70a44d2a23021d4a62537ad2266445125c8783e5e

Hostname

Value
www.wpabaseball.com
blog.antibot.pw
lordnoob.hopto.org
www.antibot.pw
www.antibot.tech
www.ekasyahwan.com
ns2.domainesia.net
xn--yp9h.antibot.pw
files.killbot.org
ns1.domainesia.net
go.killbot.org
admin.domainesia.com
rox.antibot.pw

files.antibot.pw

Url

Value
http://lordnoob.hopto.org/gx40/sendinbox-master.zip

External References

- https://otx.alienvault.com/pulse/64ecab3fdbfcb1bba0408571
- https://inquest.net/blog/adversary-on-the-defense-antibot-pw/