Sep 13 2023

NETMANAGEIT

Intelligence Report

OriginBotnet Spreads via Malicious Word Document

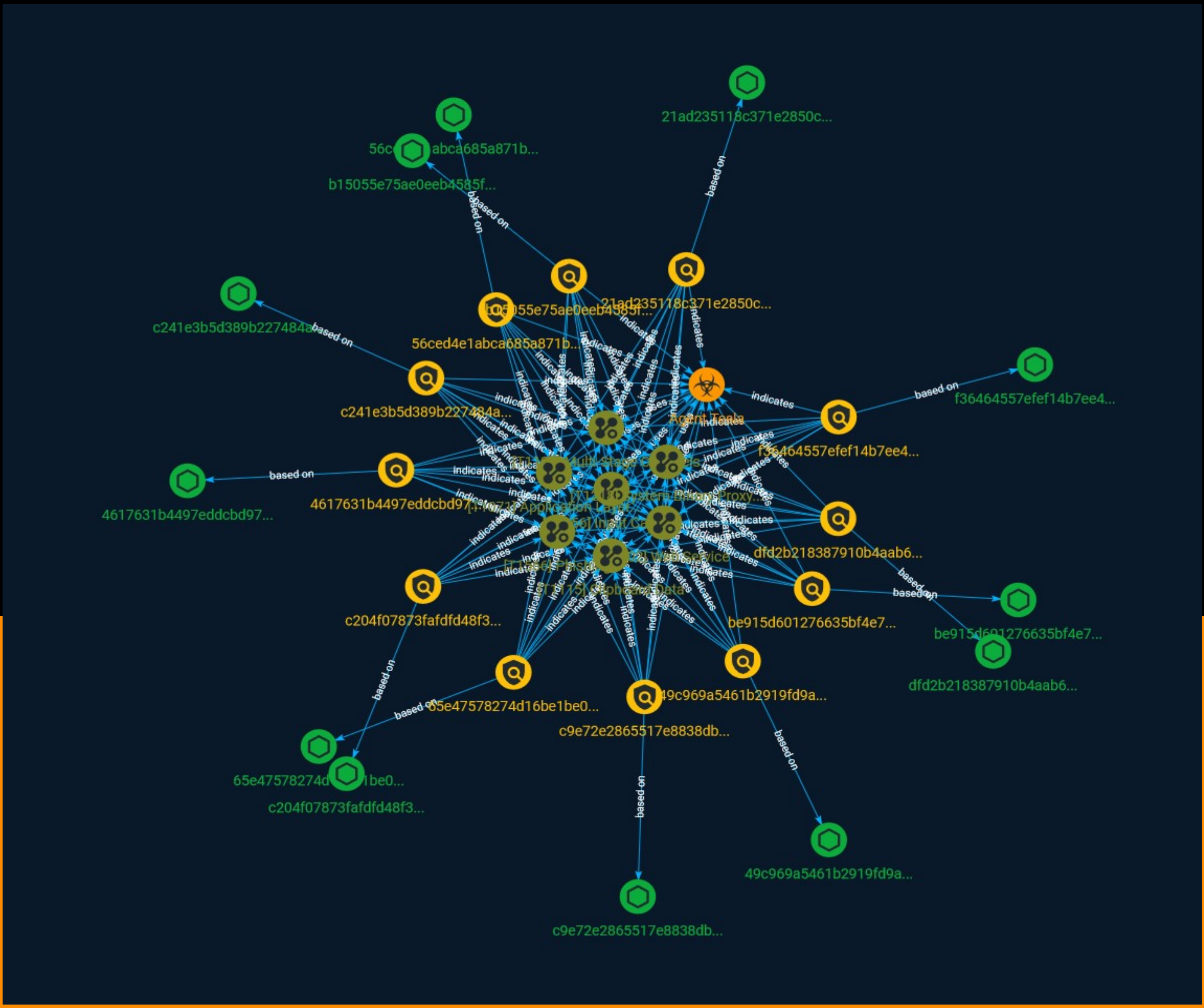

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A security firm, FortiGuard Labs, has published its analysis of OriginBotnet, a malicious web-based network that uses malware to steal credentials, passwords and other sensitive information from victims.

Confidence

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

15 / 100

Attack-Pattern

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

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

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Name

Clipboard Data

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Indicator

Name
c9e72e2865517e8838dbad0ce41561b2bd75c399b7599c1711350f9408189b9b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c9e72e2865517e8838dbad0ce41561b2bd75c399b7599c1711350f9408189b9b']
Name
56ced4e1abca685a871b77fab998766cbddfb3edf719311316082b6e05986d67
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '56ced4e1abca685a871b77fab998766cbddfb3edf719311316082b6e05986d67']
Name

dfd2b218387910b4aab6e5ee431acab864b255832eddd0fc7780db9d5844520a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfd2b218387910b4aab6e5ee431acab864b255832eddd0fc7780db9d5844520a']

Name

c204f07873fafdfd48f37e7e659e3be1e4202c8f62db8c00866c8af40a9a82c5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c204f07873fafdfd48f37e7e659e3be1e4202c8f62db8c00866c8af40a9a82c5']

Name

21ad235118c371e2850c539040b6dcdd88196c021245440155fe80aacf6ccc7e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21ad235118c371e2850c539040b6dcdd88196c021245440155fe80aacf6ccc7e']

Name

49c969a5461b2919fd9a7dc7f76dd84101b2acc429b341f8eeee248998e9da32

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '49c969a5461b2919fd9a7dc7f76dd84101b2acc429b341f8eeee248998e9da32']

Name

c241e3b5d389b227484a8baec303e6c3e262d7f7bf7909e36e312dea9fb82798

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c241e3b5d389b227484a8baec303e6c3e262d7f7bf7909e36e312dea9fb82798']

Name

f36464557efef14b7ee4cebadcc0e45af46f5c06b67c5351da15391b03a19c4c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f36464557efef14b7ee4cebadcc0e45af46f5c06b67c5351da15391b03a19c4c']

Name

65e47578274d16be1be0f50767bad0af16930df43556dd23d7ad5e4adc2bcbe3

Description

ALF:Trojan:MSIL/AgentTesla.KM

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'65e47578274d16be1be0f50767bad0af16930df43556dd23d7ad5e4adc2bcbe3']

Name

b15055e75ae0eeb4585f9323ef041fa25ed9b6bf2896b6ea45d871d49a1c72b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b15055e75ae0eeb4585f9323ef041fa25ed9b6bf2896b6ea45d871d49a1c72b8']

Name

be915d601276635bf4e77ce6b84feeec254a900c0d0c229b0d00f2c0bca1bec7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'be915d601276635bf4e77ce6b84feeec254a900c0d0c229b0d00f2c0bca1bec7']

Name

4617631b4497eddcbd97538f6712e06fabdb53af3181d6c1801247338bffaad3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4617631b4497eddcbd97538f6712e06fabdb53af3181d6c1801247338bffaad3']

Malware

Name
Agent Tesla

Description
[Agent Tesla](https://attack.mitre.org/software/S0331) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citation: Fortinet Agent Tesla April 2018)(Citation: Bitdefender Agent Tesla April 2020)(Citation: Malwarebytes Agent Tesla April 2020)

StixFile

Value
65e47578274d16be1be0f50767bad0af16930df43556dd23d7ad5e4adc2bcbe3
be915d601276635bf4e77ce6b84feeec254a900c0d0c229b0d00f2c0bca1bec7
c9e72e2865517e8838dbad0ce41561b2bd75c399b7599c1711350f9408189b9b
56ced4e1abca685a871b77fab998766cbddfb3edf719311316082b6e05986d67
b15055e75ae0eeb4585f9323ef041fa25ed9b6bf2896b6ea45d871d49a1c72b8
4617631b4497eddcbd97538f6712e06fabdb53af3181d6c1801247338bffaad3
c204f07873fafdfd48f37e7e659e3be1e4202c8f62db8c00866c8af40a9a82c5
49c969a5461b2919fd9a7dc7f76dd84101b2acc429b341f8eeee248998e9da32
c241e3b5d389b227484a8baec303e6c3e262d7f7bf7909e36e312dea9fb82798
f36464557efef14b7ee4cebadcc0e45af46f5c06b67c5351da15391b03a19c4c
dfd2b218387910b4aab6e5ee431acab864b255832eddd0fc7780db9d5844520a
21ad235118c371e2850c539040b6dcdd88196c021245440155fe80aacf6ccc7e

External References

- https://otx.alienvault.com/pulse/6501cd70169b9b54bab0217b
- https://www.fortinet.com/blog/threat-research/originbotnet-spreads-via-malicious-word-document