Jun 19 2024

NETMANAGEIT

Intelligence Report

Bondnet Using High-Performance Bots For C2 Server

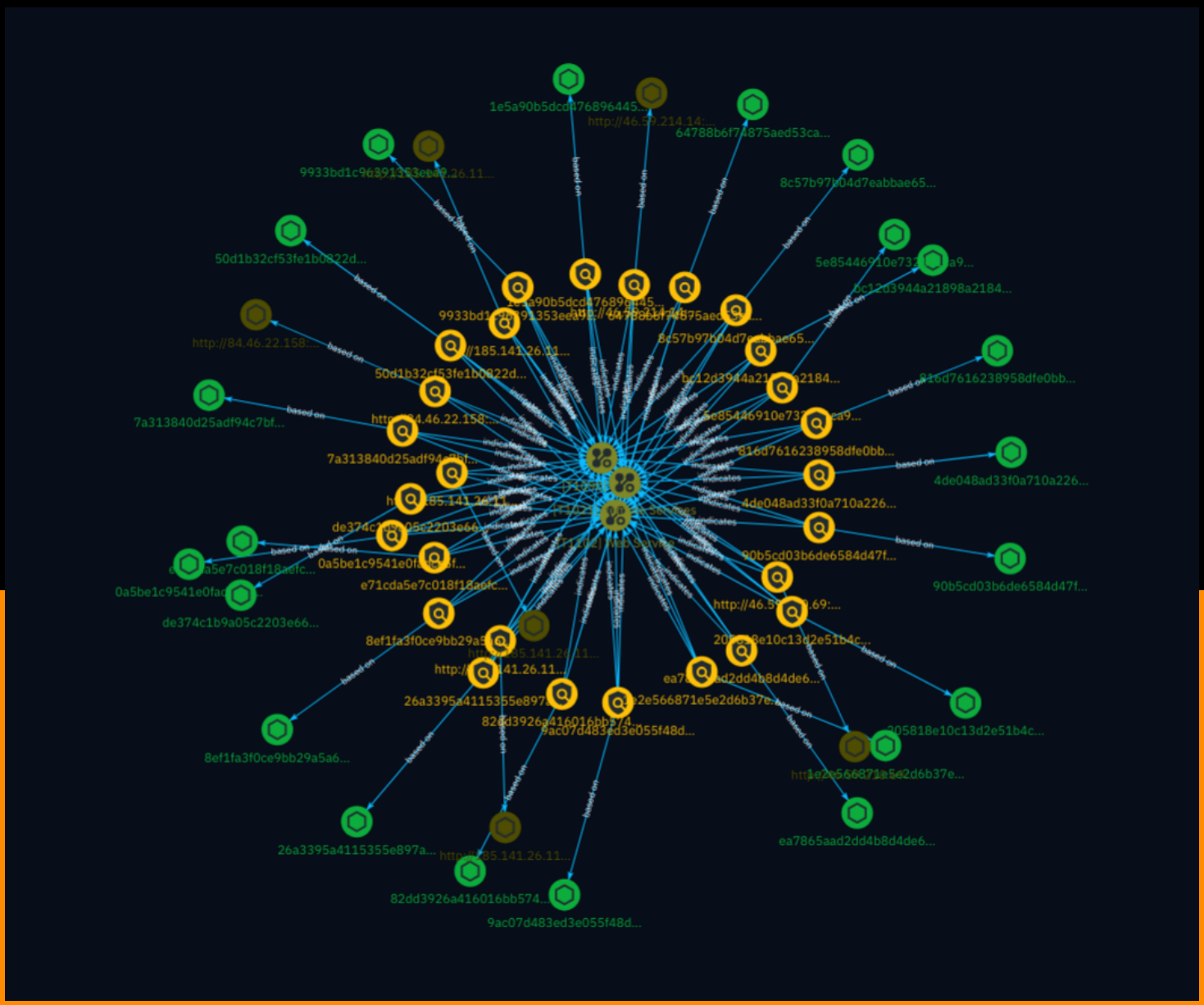

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Security researchers at ASEC have discovered that a threat actor is using high-performance bots to turn compromised systems into their central server (C2) servers, using tools such as the Cloudflare tunneling client.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
Proxy
ID
T1090
Description
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.
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

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop

commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Indicator

Name

816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019

Description

SHA256 of d28f0cfae377553fcb85918c29f4889b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019']

Name

1e2e566871e5e2d6b37ed00747f8ecd4c7098d39a2fdc8f272b1ff2962122733

Description

stack_string SHA256 of 8cafdbb0a919a1de8e0e9e38f8aa19bd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e2e566871e5e2d6b37ed00747f8ecd4c7098d39a2fdc8f272b1ff2962122733']

Name

0a5be1c9541e0fadce5f1928d3bb95367baef9ce59d487688662b100e88aabf5

Description

Ransom:Win32/Phobos.PC!MTB SHA256 of 00fa7f88c54e4a7abf4863734a8f2017

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a5be1c9541e0fadce5f1928d3bb95367baef9ce59d487688662b100e88aabf5']

Name

8ef1fa3f0ce9bb29a5a676a0ca7af67dc554617a8595b1043d1eb9176c248934

Description

UPX SHA256 of e919edc79708666cd3822f469f1c3714

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8ef1fa3f0ce9bb29a5a676a0ca7af67dc554617a8595b1043d1eb9176c248934']

Name

64788b6f74875aed53ca80669b06f407e132d7be49586925dbb3dcde56cbca9c

Description

SHA256 of 35861f4ea9a8ecb6c357bdb91b7df804

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64788b6f74875aed53ca80669b06f407e132d7be49586925dbb3dcde56cbca9c']

Name

26a3395a4115355e897a7daf04551eba5e62da661d8dbae7c99205a2e74d24ba

Description

SHA256 of 782dd6152ab52361eba2bafd67771fa0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '26a3395a4115355e897a7daf04551eba5e62da661d8dbae7c99205a2e74d24ba']

Name

9933bd1c96391353eea9986844d283c066d290e3a57df8a4871b4ddc41408d76

Description

MS_Visual_Cpp_2008 SHA256 of 35ee8d4e45716871cb31a80555c3d33e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9933bd1c96391353eea9986844d283c066d290e3a57df8a4871b4ddc41408d76']

Name

http://185.141.26.116/winupdate.css

Pattern Type

stix

Pattern

[url:value = 'http://185.141.26.116/winupdate.css']

Name

5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6

Description

Win.Virus.Sality-6832741-0 SHA256 of 6121393a37c3178e7c82d1906ea16fd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6']

Name

bc12d3944a21898a2184c190b1ccf141aa38a2ec37f168ff9711e37296afe87c

Description

!UPX_1_20 SHA256 of 76b916f3eeb80d44915d8c01200d0a94

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc12d3944a21898a2184c190b1ccf141aa38a2ec37f168ff9711e37296afe87c']

Name

1e5a90b5dcd4768964454cdf659620f5939464c6073f1dfc5d9306a869b609d1

Description

Win.Coinminer.Generic-7151250-0 SHA256 of d6b2feea1f03314b21b7bb1ef2294b72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e5a90b5dcd4768964454cdf659620f5939464c6073f1dfc5d9306a869b609d1']

Name

http://46.59.214.14:7000

Pattern Type

stix

Pattern

[url:value = 'http://46.59.214.14:7000']

Name

http://84.46.22.158:7000

Pattern Type

stix

Pattern

[url:value = 'http://84.46.22.158:7000']

Name

e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b

Description

SHA256 of 7f31636f9b74ab93a268f5a473066053

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b']

Name

90b5cd03b6de6584d47f5ab2d9cbd3eed3ed68d7db4e806b1e327d59ec0a6cde

Description

stack_string SHA256 of e0db0bf8929ccaaf6c085431be676c45

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90b5cd03b6de6584d47f5ab2d9cbd3eed3ed68d7db4e806b1e327d59ec0a6cde']

Name

7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26

Description

Win.Trojan.Sality-126545 SHA256 of df218168bf83d26386dfd4ece7aef2d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26']

Name

8c57b97b04d7eabbae651c3400a5e6b897aea1ae8964507389340c44b99c523a

Description

HackTool:Win64/Mikatz!dha SHA256 of 5410539e34fb934133d6c689072ba49d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8c57b97b04d7eabbae651c3400a5e6b897aea1ae8964507389340c44b99c523a']

Name

http://46.59.210.69:7000

Pattern Type

stix

Pattern

[url:value = 'http://46.59.210.69:7000']

Name

http://185.141.26.116/stats.php

Pattern Type

stix

Pattern

[url:value = 'http://185.141.26.116/stats.php']

Name

ea7865aad2dd4b8d4de6711699a79b3faf32b8019eb7b01bd7359df589bb73a2

Description

MS_Visual_Cpp_2008 SHA256 of 057d5c5e6b3f3d366e72195b0954283b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea7865aad2dd4b8d4de6711699a79b3faf32b8019eb7b01bd7359df589bb73a2']

Name

http://185.141.26.116/hotfixl.ico

Pattern Type

stix

Pattern

[url:value = 'http://185.141.26.116/hotfixl.ico']

Name

de374c1b9a05c2203e66917202c42d11eac4368f635ccaaadf02346035e82562

Description

UPX SHA256 of 0753cab27f143e009012053208b7f63e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de374c1b9a05c2203e66917202c42d11eac4368f635ccaaadf02346035e82562']

Name

4de048ad33f0a710a226d193f92f20417da5ba3628f79b0e25cbe83b0c979fc0

Description

Virus:Win32/Neshta.A SHA256 of dc8a0d509e84b92fbf7e794fbbe6625b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4de048ad33f0a710a226d193f92f20417da5ba3628f79b0e25cbe83b0c979fc0']

Name

9ac07d483ed3e055f48dbf031889e51e055bddf16058abb0239af1f0a9cb15dd

Description

SHA256 of 9b7be5271731cffc51ebdf9e419fa7c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ac07d483ed3e055f48dbf031889e51e055bddf16058abb0239af1f0a9cb15dd']

Name

82dd3926a416016bb5747eab624285c5013ce8ea5a8ae017027bd5c8181d3174

Description

MS_Visual_Cpp_2008 SHA256 of 0fc84b8b2bd57e1cf90d8d972a147503

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '82dd3926a416016bb5747eab624285c5013ce8ea5a8ae017027bd5c8181d3174']

Name

205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964

Description

HackTool:Win32/Passview!MSR SHA256 of 44bd492dfb54107ebfe063fcbfbddff5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964']

Name

50d1b32cf53fe1b0822d2606aa397743d6069785ba0b03a3cad52e63f84c90a8

Description

SHA256 of 2513eb59c3db32a2d5efbede6136a75d

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '50d1b32cf53fe1b0822d2606aa397743d6069785ba0b03a3cad52e63f84c90a8']

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name

based-on

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name

StixFile

Value
1e2e566871e5e2d6b37ed00747f8ecd4c7098d39a2fdc8f272b1ff2962122733
de374c1b9a05c2203e66917202c42d11eac4368f635ccaaadf02346035e82562
50d1b32cf53fe1b0822d2606aa397743d6069785ba0b03a3cad52e63f84c90a8
0a5be1c9541e0fadce5f1928d3bb95367baef9ce59d487688662b100e88aabf5
8ef1fa3f0ce9bb29a5a676a0ca7af67dc554617a8595b1043d1eb9176c248934
4de048ad33f0a710a226d193f92f20417da5ba3628f79b0e25cbe83b0c979fc0
82dd3926a416016bb5747eab624285c5013ce8ea5a8ae017027bd5c8181d3174
205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964
1e5a90b5dcd4768964454cdf659620f5939464c6073f1dfc5d9306a869b609d1
9933bd1c96391353eea9986844d283c066d290e3a57df8a4871b4ddc41408d76
8c57b97b04d7eabbae651c3400a5e6b897aea1ae8964507389340c44b99c523a
e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b
26a3395a4115355e897a7daf04551eba5e62da661d8dbae7c99205a2e74d24ba

64788b6f74875aed53ca80669b06f407e132d7be49586925dbb3dcde56cbca9c

bc12d3944a21898a2184c190b1ccf141aa38a2ec37f168ff9711e37296afe87c

816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019

ea7865aad2dd4b8d4de6711699a79b3faf32b8019eb7b01bd7359df589bb73a2

90b5cd03b6de6584d47f5ab2d9cbd3eed3ed68d7db4e806b1e327d59ec0a6cde

9ac07d483ed3e055f48dbf031889e51e055bddf16058abb0239af1f0a9cb15dd

5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6

7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26

External References

- https://cybersecuritynews.com/bondnet-high-performance-bots-c2-server/
- https://otx.alienvault.com/pulse/6670c9ec24067e93485c2b73