Mar 27 2024

NETMANAGEIT

Intelligence Report

DarkGate Loader

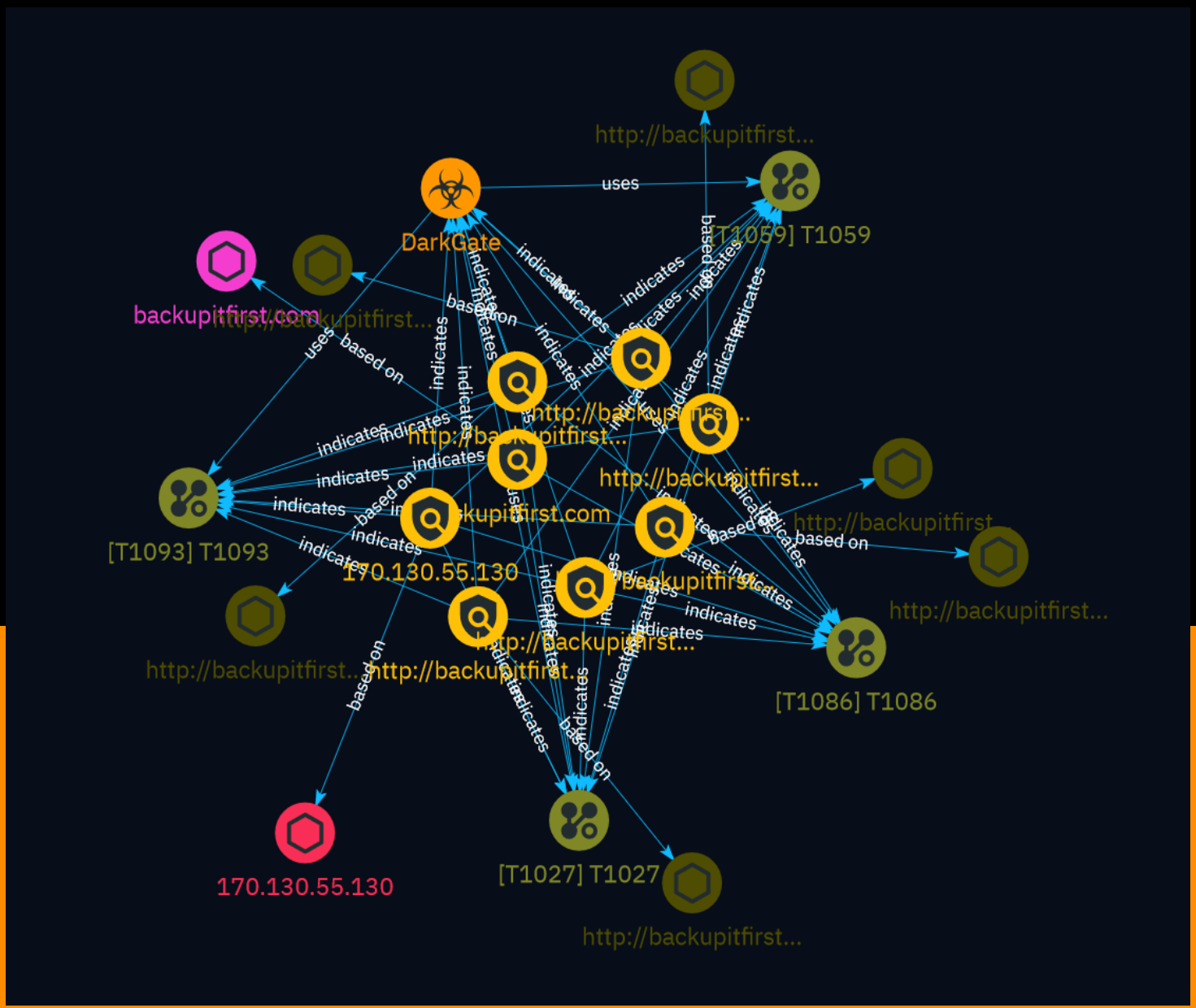

Table of contents

Overview

Entities

Observables

External References

Overview

Description

DarkGate IOCs from OSINT

Confidence

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

100 / 100

Content

N/A

Indicator

Name
backupitfirst.com
Pattern Type
stix
Pattern
[domain-name:value = 'backupitfirst.com']
Name
http://backupitfirst.com/wtabzuuxye
Pattern Type
stix
Pattern
[url:value = 'http://backupitfirst.com/wtabzuuxye']
Name
http://backupitfirst.com/vckpqpzn'

Pattern Type
stix
Pattern
[url:value = 'http://backupitfirst.com/vckpqpzn\'']
Name
http://backupitfirst.com/vckpqpzn
Pattern Type
stix
Pattern
[url:value = 'http://backupitfirst.com/vckpqpzn']
Name
http://backupitfirst.com/ltndniiq
Pattern Type
stix
Pattern
[url:value = 'http://backupitfirst.com/ltndniiq']
Name
http://backupitfirst.com/hcmjchqj

Pattern Type

stix

Pattern

[url:value = 'http://backupitfirst.com/hcmjchqj']

Name

http://backupitfirst.com/

Pattern Type

stix

Pattern

[url:value = 'http://backupitfirst.com/']

Name

170.130.55.130

Description

ISP: Eonix Corporation **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC2t0N9sfbnScj+ZtoHff9bAgLBlW0CmbKuXe1rbhKEXmCK jxdLaZw1A2DPT/t3I7PTn/IeRkf5QPma03pyTMDJ6rTZOKlS0bkezj3SLuq3PSaWXJAvGK+hdMXo k4vQLu3PMdQpxH7P1dNeapIikNHhED7w4VJR2ZhUP/WjvxJ9/LnsEo9vUpvu5d5J3gO3EiC3urpR wWoqsHMlMs6mYz1WHblvBhq8KHIdOwTcCsy5TH1b/ Zf+BPqD4kPlFtwK79NXnB3SRgOcxjn0gkU5 WvmLNiUxqgDZ32G9GOu524cs6hIcIXJkoQYGBT7k7XY2w7uHD6VSJigADR4r5wdRwZejHXvz4QuK DBjCunrK9M/ PheTyD8xtbSWPwGrpnXeCSp0FNsYmA3AVRkwgSwbydi2GOrZbFcvUB5Bl5MvU0UIq u6evvkSD4niAXQpKXu9VaTd7VPdICZs0NH/pzTwYG1jkKDFkkKR3WhhODXudFTiXPQ00y6y9rQzv

0jNWpBG3LqE= Fingerprint: 71:5f:b0:55:54:30:73:ed:1e:f2:5e:53:56:15:68:0b Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 27 Feb 2024 02:20:55 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Thu, 18 Jan 2024 14:02:16 GMT ETag: "29af-60f38cfa7d44c" Accept-Ranges: bytes Content-Length: 10671 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **445:** ``` SMB Status: Authentication: disabled SMB Version: 2 Capabilities: raw-mode Shares Name Type Comments ---------- share Disk IPC$ IPC IPC Service (Samba 4.13.13-Debian) ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '170.130.55.130']

Attack-Pattern

Name
T1086
ID
T1086
Name
T1093
ID
T1093
Name
T1059
ID
T1059
Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer

systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly

benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Malware

Name
DarkGate

Domain-Name

Value
backupitfirst.com

Url

Value
http://backupitfirst.com/wtabzuuxye
http://backupitfirst.com/vckpqpzn'
http://backupitfirst.com/vckpqpzn
http://backupitfirst.com/ltndniiq
http://backupitfirst.com/hcmjchqj
http://backupitfirst.com/

IPv4-Addr

Value
170.130.55.130

External References

- https://otx.alienvault.com/pulse/660436548f3e11479243bb8c