Sep 07 2023

NETMANAGEIT

Intelligence Report

Active North Korean campaign targeting security researchers

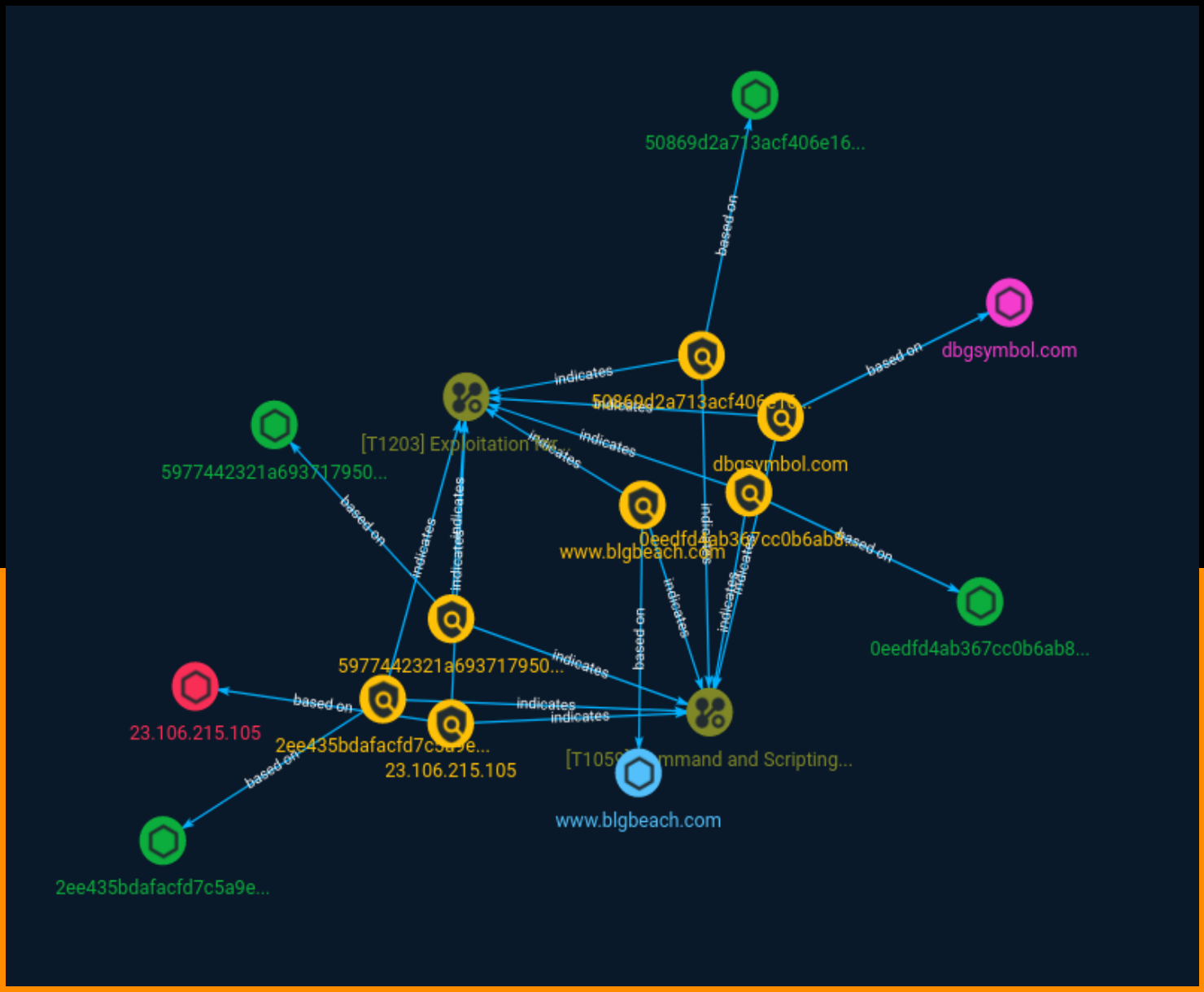

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new campaign from North Korean hackers is targeting security researchers, according to an analysis by security research group TAG, and is in the process of patching one of the most exploited 0-day exploits.

Confidence

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

15 / 100

Indicator

Name
dbgsymbol.com
Pattern Type
stix
Pattern
[domain-name:value = 'dbgsymbol.com']
Name
5977442321a693717950365446880058cc2585485ea582daa515719c1c21c5bd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5977442321a693717950365446880058cc2585485ea582daa515719c1c21c5bd']
Name

50869d2a713acf406e160d6cde3b442fafe7cfe1221f936f3f28c4b9650a66e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '50869d2a713acf406e160d6cde3b442fafe7cfe1221f936f3f28c4b9650a66e9']

Name

0eedfd4ab367cc0b6ab804184c315cc9ce2df5062cb2158338818f5fa8c0108e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0eedfd4ab367cc0b6ab804184c315cc9ce2df5062cb2158338818f5fa8c0108e']

Name

2ee435bdafacfd7c5a9ea7e5f95be9796c4d9f18643ae04dca4510448214c03c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ee435bdafacfd7c5a9ea7e5f95be9796c4d9f18643ae04dca4510448214c03c']

Name

www.blgbeach.com

Pattern Type

stix

Pattern

[hostname:value = 'www.blgbeach.com']

Name

23.106.215.105

Description

ISP: Leaseweb USA, Inc. **OS:** None ---------- Hostnames: - www.blgbeach.com - blgbeach.com ---------- Domains: - blgbeach.com ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Content-Type: text/html Server: Microsoft-IIS/10.0 Date: Tue, 05 Sep 2023 01:25:15 GMT Content-Length: 1233 ``` ---------- **443:** ``` HTTP/1.1 403 Forbidden Content-Type: text/html Server: Microsoft-IIS/10.0 Date: Wed, 06 Sep 2023 12:57:13 GMT Content-Length: 1233 ``` HEARTBLEED: 2023/09/06 12:57:20 23.106.215.105:443 - ERROR: write tcp 23.106.215.105:443: broken pipe ----------

Pattern Type

stix

Pattern

```
[ipv4-addr:value = '23.106.215.105']
```

Attack-Pattern

Name
Command and Scripting Interpreter
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

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Domain-Name

Value
dbgsymbol.com

StixFile

Value
5977442321a693717950365446880058cc2585485ea582daa515719c1c21c5bd
0eedfd4ab367cc0b6ab804184c315cc9ce2df5062cb2158338818f5fa8c0108e
2ee435bdafacfd7c5a9ea7e5f95be9796c4d9f18643ae04dca4510448214c03c
50869d2a713acf406e160d6cde3b442fafe7cfe1221f936f3f28c4b9650a66e9

Hostname

Value
www.blgbeach.com

IPv4-Addr

Value
23.106.215.105

External References

- https://otx.alienvault.com/pulse/64fa0325f88b5109856801c8
- https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/