Nov 27 2023

NETMANAGEIT

Intelligence Report

DPRK state-linked cyber actors conduct software supply chain attacks

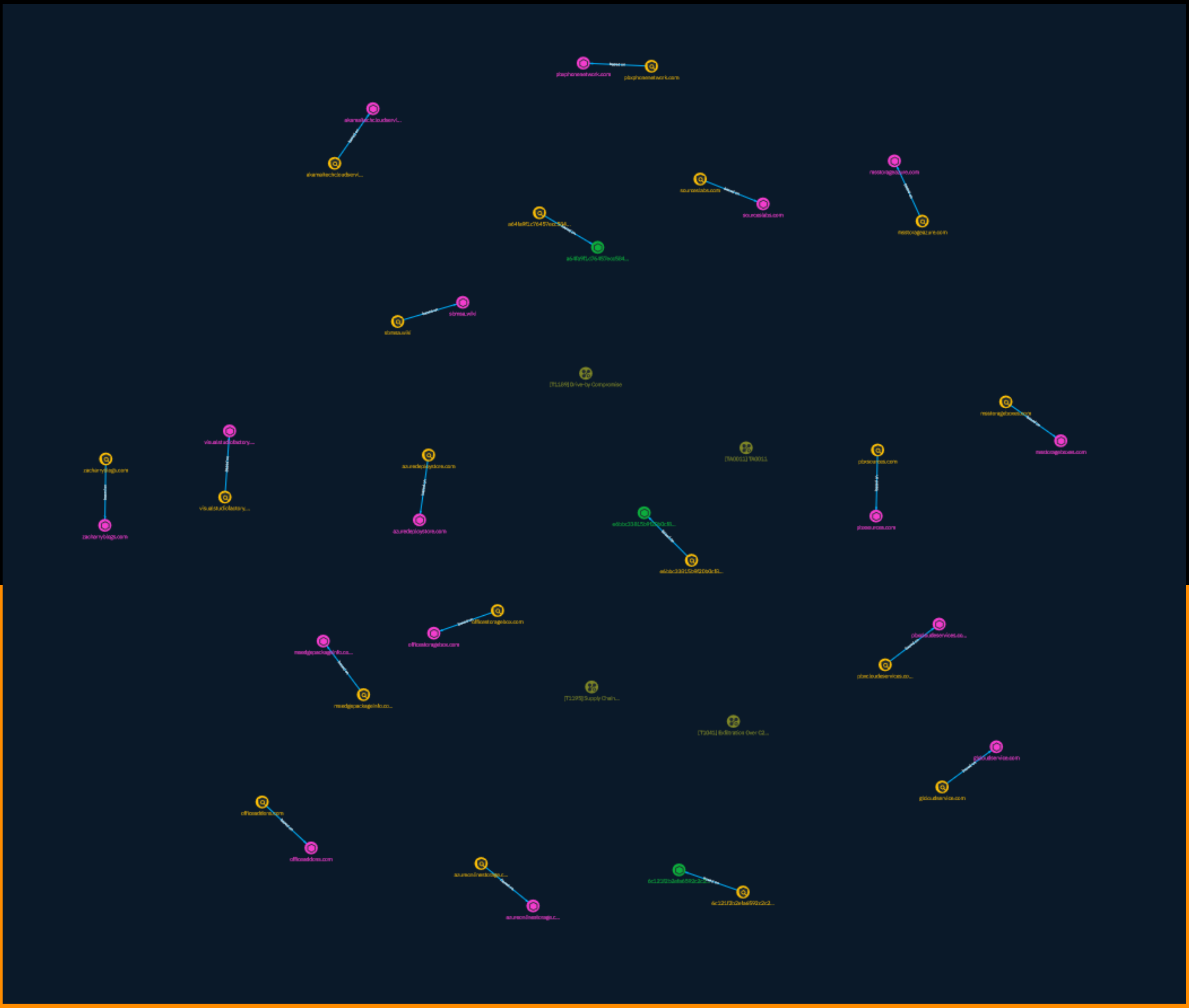

Table of contents

Overview

Entities

Observables

External References

Overview

Description

DPRK state-linked cyber actors conduct software supply chain attacks Overview The National Intelligence Service (NIS) of the Republic of Korea (ROK) and the National Cyber Security Centre (NCSC) of the United Kingdom (UK) have identified Democratic People's Republic of Korea (DPRK) state-linked cyber actors targeting software supply chain products, widely used by government organisations, financial institutions and defence industry companies globally.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name	TA0011
ID	TA0011
Name	Supply Chain Compromise
ID	T1195
Description	Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often

focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name

akamaitechcloudservices.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'akamaitechcloudservices.com']

Name

e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec']

Name

azureonlinestorage.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'azureonlinestorage.com']

Name

officestoragebox.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'officestoragebox.com']

Name

msedgepackageinfo.com

Description

UNC4736

Pattern Type

stix

Pattern

[domain-name:value = 'msedgepackageinfo.com']

Name

sourceslabs.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'sourceslabs.com']

Name

msstorageboxes.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'msstorageboxes.com']

Name

visualstudiofactory.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'visualstudiofactory.com']

Name

azuredeploystore.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'azuredeploystore.com']

Name

glcloudservice.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'glcloudservice.com']

Name

officeaddons.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'officeaddons.com']

Name

pbxphonenetwork.com

Description

UNC4736

Pattern Type

stix

Pattern

[domain-name:value = 'pbxphonenetwork.com']

Name

pbxcloudeservices.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'pbxcloudeservices.com']

Name

a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67']

Name

msstorageazure.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'msstorageazure.com']

Name

sbmsa.wiki

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'sbmsa.wiki']

Name

pbxsources.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'pbxsources.com']

Name

6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59']

Name

zacharryblogs.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'zacharryblogs.com']

Domain-Name

Value
pbxcloudeservices.com
azuredeploystore.com
akamaitechcloudservices.com
glcloudservice.com
zacharryblogs.com
sbmsa.wiki
azureonlinestorage.com
visualstudiofactory.com
msstorageboxes.com
officestoragebox.com
msstorageazure.com
pbxsources.com
msedgepackageinfo.com

sourceslabs.com
officeaddons.com
pbxphonenetwork.com

StixFile

Value
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec
a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67
6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59

External References

- https://otx.alienvault.com/pulse/6564c1dd6b56dfd223dd7d80
- https://www.documentcloud.org/documents/24174869-rok-uk-joint-cyber-security-advisoryeng