Jul 11 2024

NETMANAGEIT

Intelligence Report

Persistent npm Campaign Shipping Trojanized jQuery

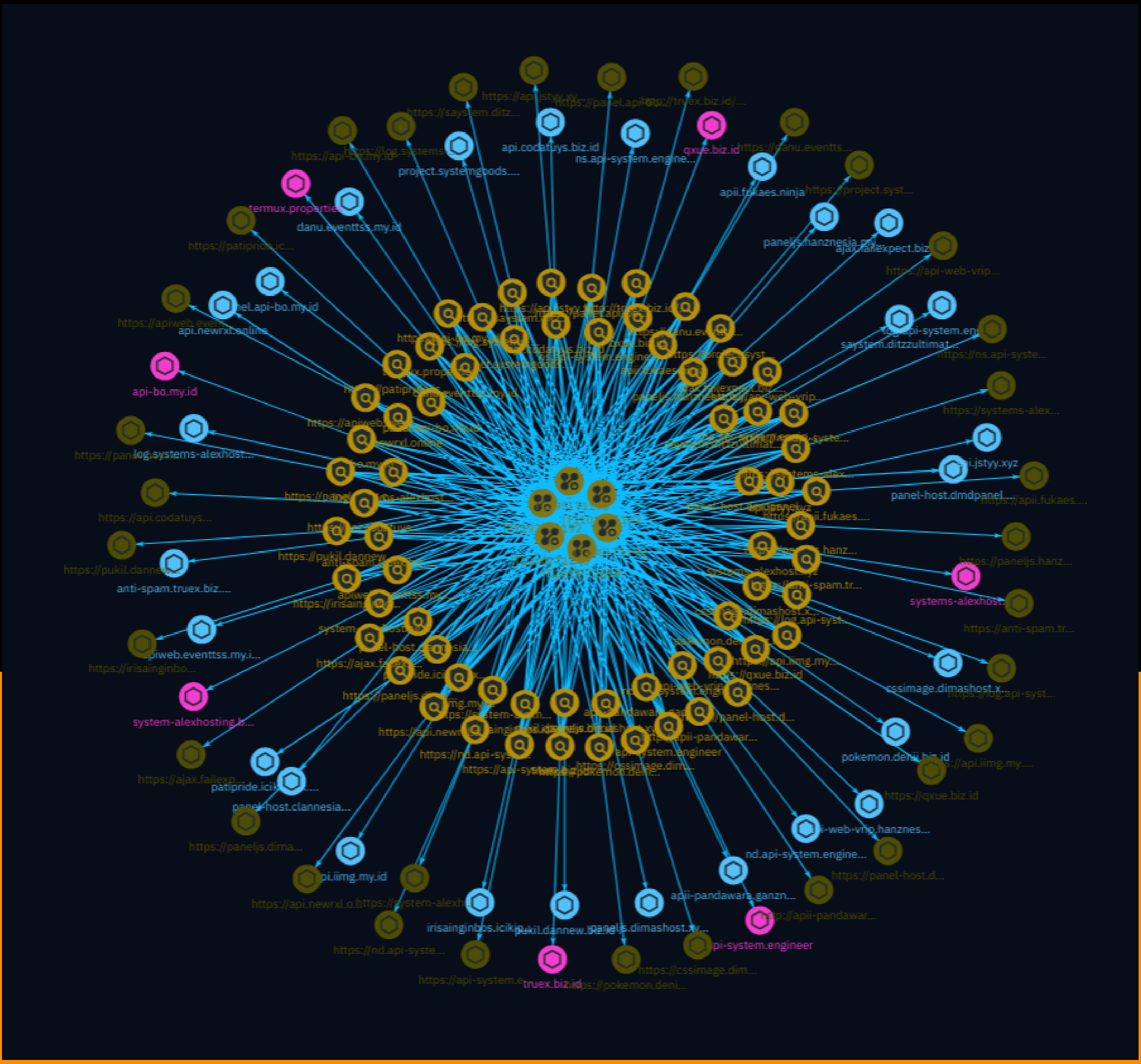

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The report describes a persistent supply chain attack involving the distribution of a trojanized version of jQuery through various platforms like npm and GitHub. The malicious jQuery variant, containing a modified 'end' function, exfiltrates website form data by sending it to remote URLs controlled by the attackers. The attack stands out due to its high variability across packages, including unique exfiltration URLs and usernames, as well as the inclusion of personal files in the published packages. This suggests a manual approach rather than an automated one. The report highlights the potential for widespread impact and demonstrates the increasing complexity of supply chain threats.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
T1192
ID
T1192
Description
Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Links may also direct users to malicious applications designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, in order to gain access to protected applications and information.(Citation: Trend Micro Pawn Storm OAuth 2017)
Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

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

T1195

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

T1102

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

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Indicator

Name

panel-host.clannesia.com

Pattern Type

stix

Pattern

[hostname:value = 'panel-host.clannesia.com']

Name

anti-spam.truex.biz.id

Pattern Type

stix

Pattern

[hostname:value = 'anti-spam.truex.biz.id']

Name

https://qxue.biz.id

Pattern Type

stix

Pattern

[url:value = 'https://qxue.biz.id']

Name

https://api.jstyy.xyz

Pattern Type

stix

Pattern

[url:value = 'https://api.jstyy.xyz']

Name

https://project.systemgoods.me

Pattern Type

stix

Pattern

[url:value = 'https://project.systemgoods.me']

Name

https://log.api-system.engineer

Pattern Type
stix
Pattern
[url:value = 'https://log.api-system.engineer']
Name
http://truex.biz.id/halo/?cat=
Pattern Type
stix
Pattern
[url:value = 'http://truex.biz.id/halo/?cat=']
Name
truex.biz.id
Pattern Type
stix
Pattern
[domain-name:value = 'truex.biz.id']
Name
https://ajax.failexpect.biz.id

Pattern Type

stix

Pattern

[url:value = 'https://ajax.failexpect.biz.id']

Name

https://apiweb.eventtss.my.id

Pattern Type

stix

Pattern

[url:value = 'https://apiweb.eventtss.my.id']

Name

api.jstyy.xyz

Pattern Type

stix

Pattern

[hostname:value = 'api.jstyy.xyz']

Name

panel-host.dmdpanel.my.id

Pattern Type

stix

Pattern

[hostname:value = 'panel-host.dmdpanel.my.id']

Name

api.codatuys.biz.id

Pattern Type

stix

Pattern

[hostname:value = 'api.codatuys.biz.id']

Name

pukil.dannew.biz.id

Pattern Type

stix

Pattern

[hostname:value = 'pukil.dannew.biz.id']

Name

panel.api-bo.my.id

Pattern Type

stix

Pattern

[hostname:value = 'panel.api-bo.my.id']

Name

https://ns.api-system.engineer

Pattern Type

stix

Pattern

[url:value = 'https://ns.api-system.engineer']

Name

systems-alexhost.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'systems-alexhost.xyz']

Name

patipride.icikipoxx.pw

Pattern Type

stix

Pattern

[hostname:value = 'patipride.icikipoxx.pw']

Name

paneljs.hanznesia.my.id

Pattern Type

stix

Pattern

[hostname:value = 'paneljs.hanznesia.my.id']

Name

api-bo.my.id

Pattern Type

stix

Pattern

[domain-name:value = 'api-bo.my.id']

Name

https://log.systems-alexhost.xyz

Pattern Type

stix

Pattern

[url:value = 'https://log.systems-alexhost.xyz']

Name

https://panel-host.clannesia.com

Pattern Type

stix

Pattern

[url:value = 'https://panel-host.clannesia.com']

Name

apiweb.eventtss.my.id

Pattern Type

stix

Pattern

[hostname:value = 'apiweb.eventtss.my.id']

Name

http://apii-pandawara.ganznesia.my.id

Pattern Type
stix
Pattern
[url:value = 'http://apii-pandawara.ganznesia.my.id']
Name
https://nd.api-system.engineer
Pattern Type
stix
Pattern
[url:value = 'https://nd.api-system.engineer']
Name
api.newrxl.online
Pattern Type
stix
Pattern
[hostname:value = 'api.newrxl.online']
Name
https://api.iimg.my.id

Pattern Type
stix

Pattern
[url:value = 'https://api.iimg.my.id']

Name
https://pokemon.denii.biz.id

Pattern Type
stix

Pattern
[url:value = 'https://pokemon.denii.biz.id']

Name
ajax.failexpect.biz.id

Pattern Type
stix

Pattern
[hostname:value = 'ajax.failexpect.biz.id']

Name
saystem.ditzzultimate.xyz

Pattern Type

stix

Pattern

[hostname:value = 'saystem.ditzzultimate.xyz']

Name

project.systemgoods.me

Pattern Type

stix

Pattern

[hostname:value = 'project.systemgoods.me']

Name

pokemon.denii.biz.id

Pattern Type

stix

Pattern

[hostname:value = 'pokemon.denii.biz.id']

Name

https://api.codatuys.biz.id

Pattern Type

stix

Pattern

[url:value = 'https://api.codatuys.biz.id']

Name

https://api.newrxl.online

Pattern Type

stix

Pattern

[url:value = 'https://api.newrxl.online']

Name

system-alexhosting.biz.id

Pattern Type

stix

Pattern

[domain-name:value = 'system-alexhosting.biz.id']

Name

https://system-alexhosting.biz.id

Pattern Type
stix
Pattern
[url:value = 'https://system-alexhosting.biz.id']
Name
https://paneljs.hanznesia.my.id
Pattern Type
stix
Pattern
[url:value = 'https://paneljs.hanznesia.my.id']
Name
https://saystem.ditzzultimate.xyz
Pattern Type
stix
Pattern
[url:value = 'https://saystem.ditzzultimate.xyz']
Name
ns.api-system.engineer

Pattern Type

stix

Pattern

[hostname:value = 'ns.api-system.engineer']

Name

https://cssimage.dimashost.xyz

Pattern Type

stix

Pattern

[url:value = 'https://cssimage.dimashost.xyz']

Name

api.iimg.my.id

Pattern Type

stix

Pattern

[hostname:value = 'api.iimg.my.id']

Name

https://paneljs.dimashost.xyz

Pattern Type

stix

Pattern

[url:value = 'https://paneljs.dimashost.xyz']

Name

https://panel.api-bo.my.id

Pattern Type

stix

Pattern

[url:value = 'https://panel.api-bo.my.id']

Name

irisainginbos.icikipoxx.pw

Pattern Type

stix

Pattern

[hostname:value = 'irisainginbos.icikipoxx.pw']

Name

https://anti-spam.truex.biz.id

Pattern Type

stix

Pattern

[url:value = 'https://anti-spam.truex.biz.id']

Name

https://patipride.icikipoxx.pw

Pattern Type

stix

Pattern

[url:value = 'https://patipride.icikipoxx.pw']

Name

https://pukil.dannew.biz.id

Pattern Type

stix

Pattern

[url:value = 'https://pukil.dannew.biz.id']

Name

https://api-bo.my.id

Pattern Type

stix

Pattern

[url:value = 'https://api-bo.my.id']

Name

paneljs.dimashost.xyz

Pattern Type

stix

Pattern

[hostname:value = 'paneljs.dimashost.xyz']

Name

apii.fukaes.ninja

Pattern Type

stix

Pattern

[hostname:value = 'apii.fukaes.ninja']

Name

https://api-web-vrip.hanznesia.my.id

Pattern Type

stix

Pattern

[url:value = 'https://api-web-vrip.hanznesia.my.id']

Name

https://panel-host.dmdpanel.my.id

Pattern Type

stix

Pattern

[url:value = 'https://panel-host.dmdpanel.my.id']

Name

https://api-system.engineer

Pattern Type

stix

Pattern

[url:value = 'https://api-system.engineer']

Name

termux.properties

Pattern Type

stix

Pattern

[domain-name:value = 'termux.properties']

Name

apii-pandawara.ganznesia.my.id

Pattern Type

stix

Pattern

[hostname:value = 'apii-pandawara.ganznesia.my.id']

Name

api-system.engineer

Pattern Type

stix

Pattern

[domain-name:value = 'api-system.engineer']

Name

https://danu.eventtss.my.id

Pattern Type

stix

Pattern

[url:value = 'https://danu.eventtss.my.id']

Name

log.systems-alexhost.xyz

Pattern Type

stix

Pattern

[hostname:value = 'log.systems-alexhost.xyz']

Name

https://apii.fukaes.ninja

Pattern Type

stix

Pattern

[url:value = 'https://apii.fukaes.ninja']

Name

api-web-vrip.hanznesia.my.id

Pattern Type
stix

Pattern
[hostname:value = 'api-web-vrip.hanznesia.my.id']

Domain-Name

Value
qxue.biz.id
truex.biz.id
api-bo.my.id
termux.properties
system-alexhosting.biz.id
systems-alexhost.xyz
api-system.engineer

Hostname

Value
danu.eventtss.my.id
paneljs.hanznesia.my.id
log.api-system.engineer
project.systemgoods.me
pokemon.denii.biz.id
apii.fukaes.ninja
paneljs.dimashost.xyz
api.newrxl.online
api.jstyy.xyz
panel-host.dmdpanel.my.id
cssimage.dimashost.xyz
api.iimg.my.id
panel-host.clannesia.com

apii-pandawara.ganznesia.my.id
api-web-vrip.hanznesia.my.id
log.systems-alexhost.xyz
apiweb.eventtss.my.id
ajax.failexpect.biz.id
patipride.icikipoxx.pw
saystem.ditzzultimate.xyz
anti-spam.truex.biz.id
nd.api-system.engineer
api.codatuys.biz.id
panel.api-bo.my.id
ns.api-system.engineer
irisainginbos.icikipoxx.pw
pukil.dannew.biz.id

External References

- https://blog.phylum.io/persistent-npm-campaign-shipping-trojanized-jquery/
- https://otx.alienvault.com/pulse/668e56193194da7c0afb3c8c