Mar 25 2024

NETMANAGEIT

Intelligence Report

Sign1 Malware: Analysis, Campaign History & Indicators of Compromise

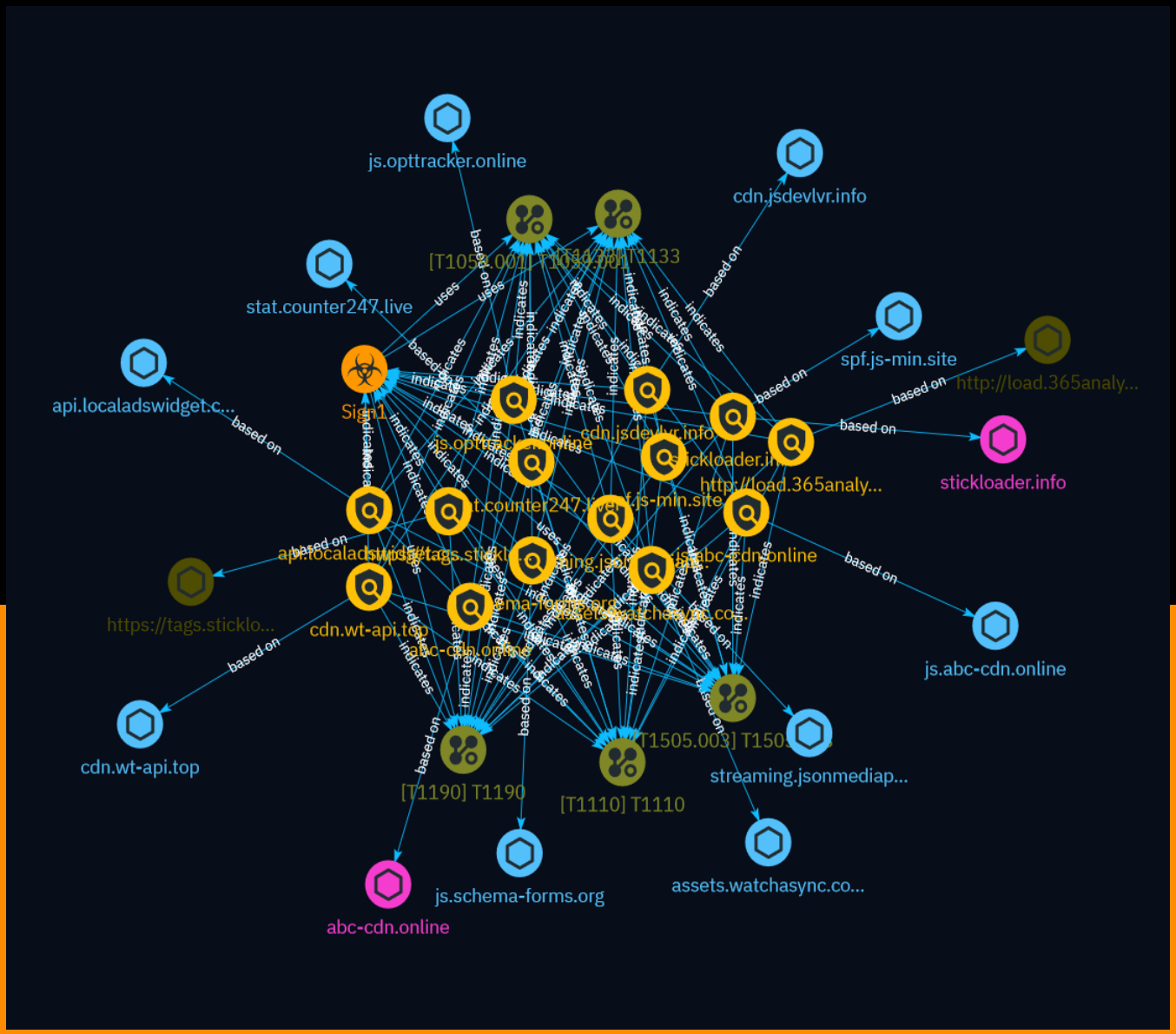

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report analyzes a JavaScript injection related to a massive malware campaign called Sign1, which has infected over 39,000 sites. It documents Sign1's campaign history, obfuscation techniques, use of time-based randomization and XOR encoding, dynamically changing URLs, waves of injections via WordPress plugins, and recommendations for protection.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
streaming.jsonmediapacks.com
Pattern Type
stix
Pattern
[hostname:value = 'streaming.jsonmediapacks.com']
Name
stat.counter247.live
Pattern Type
stix
Pattern
[hostname:value = 'stat.counter247.live']
Name
spf.js-min.site

Pattern Type
stix
Pattern
[hostname:value = 'spf.js-min.site']
Name
js.schema-forms.org
Pattern Type
stix
Pattern
[hostname:value = 'js.schema-forms.org']
Name
js.opttracker.online
Pattern Type
stix
Pattern
[hostname:value = 'js.opttracker.online']
Name
js.abc-cdn.online

Pattern Type
stix
Pattern
[hostname:value = 'js.abc-cdn.online']
Name
cdn.wt-api.top
Pattern Type
stix
Pattern
[hostname:value = 'cdn.wt-api.top']
Name
cdn.jsdevlvr.info
Pattern Type
stix
Pattern
[hostname:value = 'cdn.jsdevlvr.info']
Name
assets.watchasync.com

Pattern Type
stix
Pattern
[hostname:value = 'assets.watchasync.com']
Name
api.localadswidget.com
Pattern Type
stix
Pattern
[hostname:value = 'api.localadswidget.com']
Name
stickloader.info
Pattern Type
stix
Pattern
[domain-name:value = 'stickloader.info']
Name
abc-cdn.online

Pattern Type
stix
Pattern
[domain-name:value = 'abc-cdn.online']
Name
https://tags.stickloader.info/my/pack.js
Pattern Type
stix
Pattern
[url:value = 'https://tags.stickloader.info/my/pack.js']
Name
http://load.365analytics.xyz/my.counter.1710313200.js?ver=65f15aa8
Pattern Type
stix
Pattern
[url:value = 'http://load.365analytics.xyz/my.counter.1710313200.js?ver=65f15aa8']

Malware

Name
Sign1

Attack-Pattern

Name
T1110
ID
T1110
Description
Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.
Name
T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1505.003

ID

T1505.003

Description

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.(Citation: volexity_0day_sophos_FW) In addition to a server-side

script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper](https://attack.mitre.org/software/S0020) Web shell client). (Citation: Lee 2013)

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). 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

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Hostname

Value
streaming.jsonmediapacks.com
stat.counter247.live
spf.js-min.site
js.schema-forms.org
js.opttracker.online
js.abc-cdn.online
cdn.wt-api.top
cdn.jsdevlvr.info
assets.watchasync.com
api.localadswidget.com

Domain-Name

Value
stickloader.info
abc-cdn.online

Url

Value
http://load.365analytics.xyz/my.counter.1710313200.js?ver=65f15aa8
https://tags.stickloader.info/my/pack.js

External References

- https://blog.sucuri.net/2024/03/sign1-malware-analysis-campaign-history-indicators-of-compromise.html
- https://otx.alienvault.com/pulse/66017516c12e72eb68aef003