The evolution of a Mac trojan: UpdateAgent's progression

microsoft.com/security/blog/2022/02/02/the-evolution-of-a-mac-trojan-updateagents-progression/

February 2, 2022

Our discovery and analysis of a sophisticated Mac trojan in October exposed a year-long evolution of a malware family—and depicts the rising complexity of threats across platforms. The trojan, tracked as UpdateAgent, started as a relatively basic information-stealer but was observed distributing secondary payloads in the latest campaign, a capability that it added in one of its multiple iterations. Reminiscent of the progression of info-stealing trojans in other platforms, UpdateAgent may similarly become a vector for other threats to infiltrate target systems.

Since its first appearance in September 2020, the malware displayed an increasing progression of sophisticated capabilities, and while the latest two variants were sporting much more refined behavior compared with earlier versions, they show signs that the malware is still in the development stage and more updates are likely to come. The latest campaign saw the malware installing the evasive and persistent Adload adware, but UpdateAgent's ability to gain access to a device can theoretically be further leveraged to fetch other, potentially more dangerous payloads.

UpdateAgent lures its victims by impersonating legitimate software and can leverage Mac device functionalities to its benefit. One of the most advanced techniques found in UpdateAgent's latest toolbox is bypassing Gatekeeper controls, which are designed to ensure only trusted apps run on Mac devices. The trojan can leverage existing user permissions to quietly perform malicious activities before deleting the evidence to cover its tracks. UpdateAgent also misuses public cloud infrastructure, namely Amazon S3 and CloudFront services, to host its additional payloads. We shared our findings with the team at Amazon Web Services, and they have taken down the malicious URLs–another example of how intelligence sharing and collaboration results in better security for the broader community.

Threats like UpdateAgent are proof that, as environments continue to rely on a diverse range of devices and operating systems, organizations need security solutions that can provide protection across platforms and a complete picture of their security posture. Microsoft Defender for Endpoint delivers and coordinates threat defense across all major OS platforms including Windows, macOS, Linux, Android and iOS. On macOS devices, Microsoft Defender for Endpoint detects and exposes threats and vulnerabilities through its antivirus, endpoint detection and response (EDR), and threat and vulnerability management capabilities.

In this blog post, we share the evolving development of the UpdateAgent trojan targeting Mac users and detail the malware's recent campaign to compromise devices, steal sensitive information, and distribute adware as a secondary payload.

Progression of UpdateAgent

UpdateAgent is uniquely characterized by its gradual upgrading of persistence techniques, a key feature that indicates this trojan will likely continue to use more sophisticated techniques in future campaigns. Like many information-stealers found on other platforms, the malware attempts to

infiltrate macOS machines to steal data and it is associated with other types of malicious payloads, increasing the chances of multiple infections on a device.

The trojan is likely distributed via drive-by downloads or advertisement pop-ups, which impersonate legitimate software such as video applications and support agents. This action of impersonating or bundling itself with legitimate software increases the likelihood that users are tricked into installing the malware. Once installed, UpdateAgent starts to collect system information that is then sent to its command-and-control (C2) server.

Notably, the malware's developer has periodically updated the trojan over the last year to improve upon its initial functions and add new capabilities to the trojan's toolbox. The timeline below illustrates a series of techniques adopted by UpdateAgent from September 2020 through October 2021:

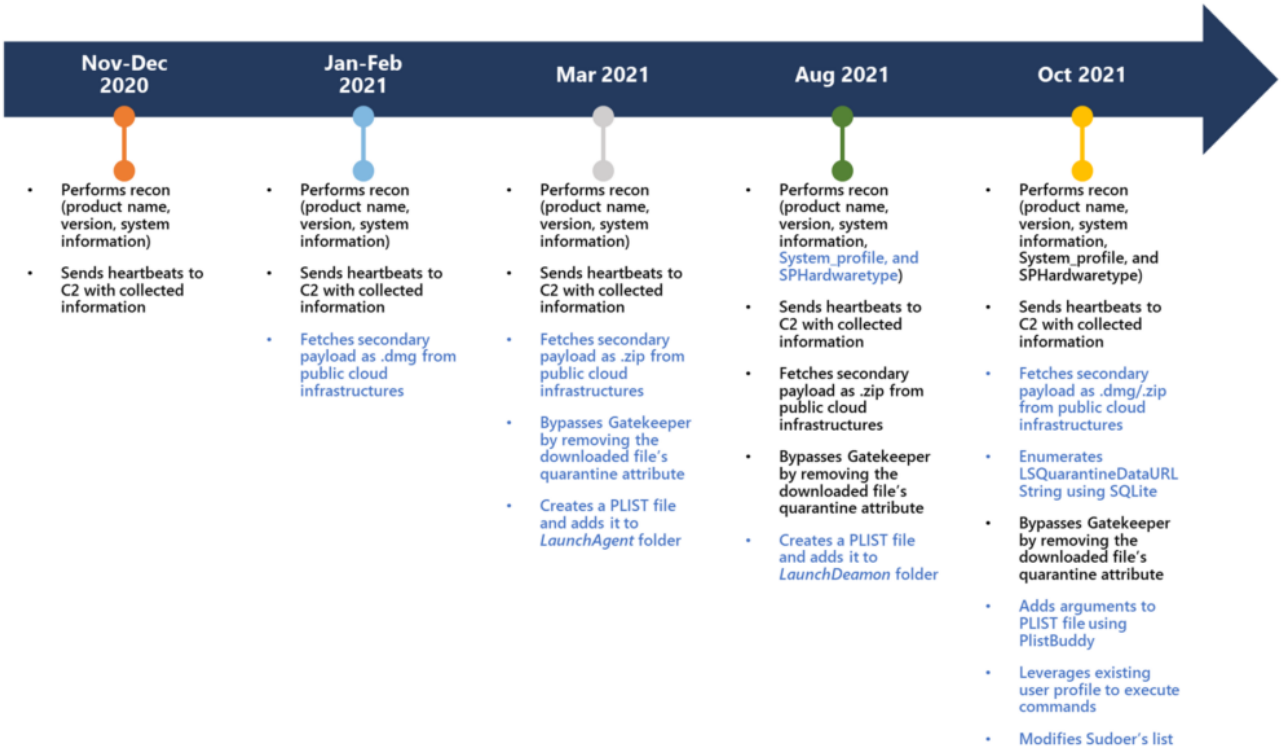

Figure 1. Tracking the evolution of UpdateAgent

September–December 2020: The initial version of UpdateAgent was considered to be a fairly basic information-stealer. At the time, the malware was only capable of performing reconnaissance to scan and collect system information such as product names and versions. Once gathered, the data was then sent as heartbeats to the malware's C2 server.

January–February 2021: Approximately two months later, UpdateAgent maintained its original capabilities and added a new one: the ability to fetch secondary payloads as *.dmg* files from public cloud infrastructure. DMG files are mountable disk images used to distribute software and apps to macOS, allowing the trojan to easily install additional programs on affected devices.

March 2021: Upon its third update, the malware altered one of its prior functions to fetch secondary payloads as *.zip* files instead of *.dmg* files. The malware's developer also included two new capabilities: the ability to bypass Gatekeeper by removing the downloaded file's quarantine attribute and the ability to create a PLIST file that is added to the *LaunchAgent* folder. The quarantine attribute forces Gatekeeper to block the launch of any file downloaded from the web or other unknown sources, and it also displays a pop-up warning that users cannot open the respective file as "it is from an unidentified developer". By removing the attribute, the malware both prevented the pop-up message warning users and allowed the files to launch without being blocked by Gatekeeper. Moreover, as the *LaunchAgent* folder specifies which apps and code automatically run each time a user signs into the machine, adding the malware's PLIST file allowed it to be included in these automatic launches for persistence upon users signing into the affected device.

August 2021: The malware's fourth update further altered some of its prior capabilities. For one, it expanded its reconnaissance function to scan and collect System_profile and SPHardwaretype information. Additionally, UpdateAgent was changed to create and add PLIST files to the *LaunchDaemon* folder instead of the *LaunchAgent* folder. While targeting the *LaunchDaemon* folder instead of the *LaunchAgent* folder required administrative privileges, it permitted the malware to inject persistent code that ran as root. This code generally takes the form of background processes that don't interact with users, thus it also improved the trojan's evasiveness.

October 2021: We detected the latest variants of UpdateAgent just over a year since its release into the wild. Sporting many of the updates found in the August 2021 variant, UpdateAgent still performed system reconnaissance, communicated with the C2 server as heartbeats, and bypassed Gatekeeper. Additionally, the October update expanded the malware's ability to fetch secondary payloads as both *.dmg* or *.zip* files from public cloud infrastructure, rather than choosing between filetypes. Among its new capabilities, UpdateAgent included the ability to enumerate LSQuarantineDataURLString using SQLite in order to validate whether the malware's downloaded app is within the Quarantine Events database where it would be assigned a quarantine attribute. The upgrade also allowed the malware to leverage existing user profiles to run commands requiring sudo access in addition to the ability to add arguments using PlistBuddy to create and edit PLIST files more easily. Lastly, the trojan included the ability to modify sudoers list, allowing the malware to bypass a prompt requiring high privilege user credentials while running UpdateAgent's downloaded app.

October 2021 Campaign

In the October 2021 campaign, UpdateAgent included a larger set of sophisticated techniques than ever previously observed. The attackers distributed the trojanized app in *.zip* or *.pkg* format, conforming with a campaign observed in early 2021:

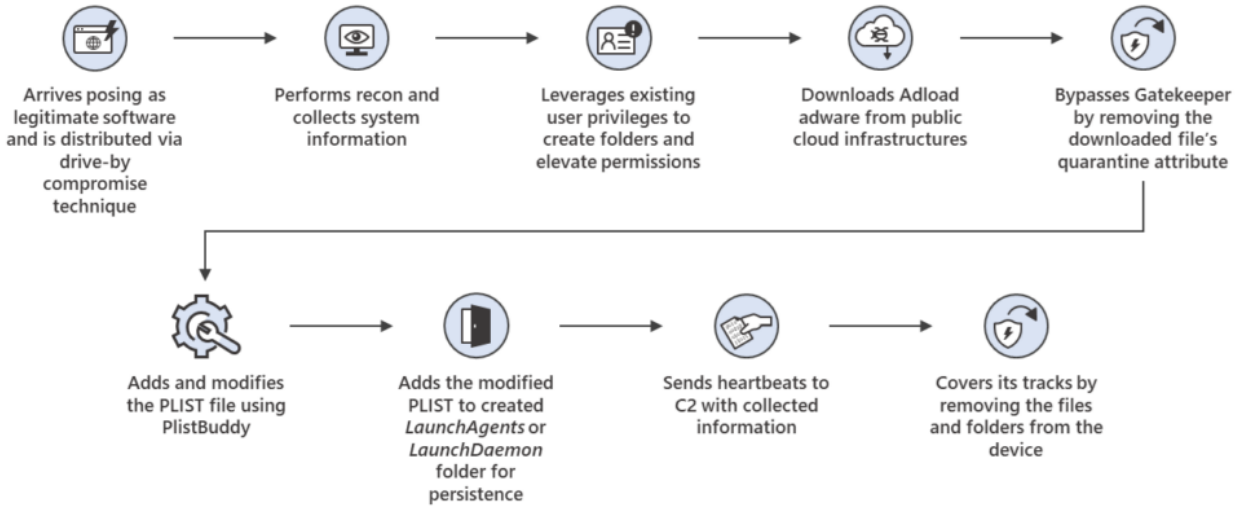

Figure 2. Attack chain of the latest UpdateAgent campaign

Upon analyzing UpdateAgent's infrastructure, we determined that the infrastructure used in the October 2021 campaign was created at the end of September 2021, and we also discovered additional domains with payloads. This indicates that the trojan is still in the developmental stage and is likely to add or modify its capabilities in future updates and continue its track of improving its overall level of sophistication.

We further observed two separate variants of the UpdateAgent trojan in its October 2021 campaign. Each variant leveraged different tactics to infect a device, as detailed below:

Variant 1

The first variant of UpdateAgent takes the following steps to infect a device:

1. A *.zip* file named *HelperModule.zip* downloads and installs UpdateAgent using a specific file path – */Library/Application Support/xxx/xxx.* This *.zip* file is installed in */Library/Application Support/Helper/HelperModule.*
2. UpdateAgent collects operating system and hardware information about the affected device. Once the compromised device connects to the C2 server, the trojan uses a *curl* request to send this data to the C2 server.
3. Upon successful connection, UpdateAgent requests a secondary payload, usually a *.dmg* or *.zip* file, which is hosted on a CloudFront instance.
4. Once the secondary payload downloads, UpdateAgent uses the *xattr* command – */usr/bin/xattr -rc /tmp/setup.dmg,* to remove the quarantine attribute of downloaded files and bypass Gatekeeper controls.
5. UpdateAgent then extracts the secondary payload (*.dmg* or *.zip).* Once the file is mounted, it unzips and copies the payload files to a temporary folder, assigning executable permissions, and launches these files. UpdateAgent also uses PlistBuddy to create PLIST files under the *LaunchAgent* folder to remain persistent through system restart.
6. UpdateAgent removes evidence by deleting the secondary payload, temporary folders, PLIST files, and all other downloaded artifacts.

Variant 2

The second variant of UpdateAgent takes the following steps to infect a device:

1. A third-party WebVideoPlayer application (WebVideoPlayer.pkg) with a post-install script downloads additional apps or *.zip* files as */Applications/WebVideoPlayer.app/Contents/MacOS/WebVideoPlayer*. Notably, this application included a valid certificate that was later revoked by Apple in October 2021.
2. The application scans the user profile to identify existing user IDs and assigned groups.
3. The WebVideoPlayer application uses SQLite3 commands to determine if the *.pkg* file is within the Quarantine Events database, which contains URLs of downloaded files, mail addresses, and subjects for saved attachments.
4. The *.pkg* payload extracts and drops UpdateAgent in */Library/Application Support/WebVideoPlayer/WebVideoPlayerAgent*.
5. The WebVideoPlayer application also assigns executable permissions to UpdateAgent and attempts to remove the quarantine attribute of the file using the *xattr* command to bypass Gatekeeper controls.
6. The application then launches UpdateAgent and collects and sends the OS information to the attacker's C2 server. Like the first variant, the second variant sends *curl* requests that download additional payloads, such as adware, and removes evidence by deleting all files and folders that it created.

Adload adware

UpdateAgent is further characterized by its ability to fetch secondary payloads that can increase the chances of multiple infections on a device, with the latest campaign pushing adware. We first observed UpdateAgent distributing adware as a secondary payload in its October 2021 campaign, identified as part of the Adload adware family by Microsoft Defender Antivirus.

Similar to UpdateAgent, adware is often included in potentially unwanted or malicious software bundles that install the adware alongside impersonated or legitimate copies of free programs. In Adload's case, we previously observed the adware family targeting macOS users had spread via rogue installers often found on malicious websites.

Once adware is installed, it uses ad injection software and techniques to intercept a device's online communications and redirect users' traffic through the adware operators' servers, injecting advertisements and promotions into webpages and search results. More specifically, Adload leverages a Person-in-The-Middle (PiTM) attack by installing a web proxy to hijack search engine results and inject advertisements into webpages, thereby siphoning ad revenue from official website holders to the adware operators.

Adload is also an unusually persistent strain of adware. It is capable of opening a backdoor to download and install other adware and payloads in addition to harvesting system information that is sent to the attackers' C2 servers. Considering both UpdateAgent and Adload have the ability to install additional payloads, attackers can leverage either or both of these vectors to potentially deliver more dangerous threats to target systems in future campaigns.

Defending against macOS threats

UpdateAgent's evolution displays the increasing complexity of threats across platforms. Its developers steadily improved the trojan over the last year, turning a basic information-stealer into a persistent and more sophisticated piece of malware. This threat also exemplifies the trend of common malware increasingly harboring more dangerous threats, a pattern also observed in other platforms. UpdateAgent's ability to gain access to a device can theoretically be leveraged by attackers to introduce potentially more dangerous payloads, emphasizing the need to identify and block threats such as this.

Defenders can take the following mitigation steps to defend against this threat:

- Encourage the use of Microsoft Edge—available on macOS and various platforms—or other web browsers that support Microsoft Defender SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware.
- Restrict access to privileged resources, such as *LaunchDaemons* or *LaunchAgents* folders and sudoers files, through OSX enterprise management solutions. This helps to mitigate common persistence and privilege escalation techniques.
- Install apps from trusted sources only, such as a software platform's official app store. Third-party sources may have lax standards for the applications that they host, allowing malicious actors to upload and distribute malware.
- Run the latest version of your operating systems and applications. Deploy the latest security updates as soon as they become available.

As organizational environments are intricate and heterogenous, running multiple applications, clouds, and devices, they require solutions that can protect across platforms. Microsoft Defender for Endpoint offers cross-platform security and a unified investigation experience that gives customers visibility across all endpoints and enables them to detect, manage, respond, and remediate threats, such as the capability to detect UpdateAgent's anomalous use of PlistBuddy.

Microsoft Defender for Endpoint customers can apply the following mitigations to reduce the environmental attack surface and mitigate the impact of this threat and its payloads:

- Turn on cloud-delivered protection and automatic sample submission on Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- Enable potentially unwanted application (PUA) protection in block mode to automatically quarantine PUAs like adware. PUA blocking takes effect on endpoint clients after the next signature update or computer restart. PUA blocking takes effect on endpoint clients after the next signature update or computer restart.
- Turn on network protection to block connections to malicious domains and IP addresses.

Defender for Endpoint's next-generation protection reinforces network security perimeters and includes antimalware capabilities to catch emerging threats, including UpdateAgent and its secondary payloads, C2 communications, and other malicious artifacts affiliated with the trojan's reconnaissance activities. Moreover, macOS antimalware detections provide insight into where a threat originated and how the malicious process or activity was created, providing security teams a comprehensive view of incidents and attack chains.

Finally, this research underscores the importance of understanding a macOS threat's progression to not only remedy its current abilities, but to prepare for increased capabilities and sophistication of the threat. As threats on other OS platforms continue to grow, our security solutions must secure users' computing experiences be it a Windows or non-Windows machine. By sharing our research and other forms of threat intelligence, collaboration across the larger security community can aid in enriching our protection technologies, regardless of the platform or device in use.

Detection details

Antivirus

Microsoft Defender Antivirus detects threat components and behavior as the following malware:

- Trojan:MacOS/UpdateAgent.B
- Trojan:MacOS/UpdateAgent.A
- Trojan:MacOS/Agent.A
- Adware:MacOS/Adload.A
- Behavior:MacOS/UpdateAgent.B

Endpoint detection and response (EDR)

Alerts with the following titles in the Microsoft 365 Security Center can indicate threat activity within your network:

- macOS Gatekeeper bypass
- Executable permission added to file or directory
- Suspicious database access
- Suspicious System Hardware Discovery
- Suspicious binary dropped and launched

Advanced hunting

To locate activity related to UpdateAgent, run the following advanced hunting queries in Microsoft 365 Defender or Microsoft Defender Security Center.

File quarantine attribute

Look for file quarantine attribute removal for the specific packages involved in the campaign.

```
DeviceProcessEvents
| where FileName has "xattr" and (ProcessCommandLine has "-rc Library/Application
Support/WebVideoPlayer/WebVideoPlayerAgent" or ProcessCommandLine has "-r -d
/Library/Application Support/Helper/HelperModule")
```

Quarantine Event database

Look for quarantine event database enumeration through *sqlite3* for the packages involved in the campaign.

```
DeviceProcessEvents
| where FileName has "sqlite3" and ProcessCommandLine has "WebVideoPlayer.pkg"
```

Curl request

Look for UpdateAgent's curl requests.

```
DeviceProcessEvents
| where FileName has "curl" and ProcessCommandLine has "--connect-timeout 900 -L"
```

Indicators

Files (SHA-256)

- 1966d64e9a324428dec7b41aca852034cbe615be1179ccb256cf54a3e3e242ee
- ef23a1870d84e164a4234074251205190a5dfda9f465c8eee6c7e0d6878c2b05
- 519339e67b1d421d51a0f096e80a57083892bac8bb16c7e4db360bb0fda3cb11
- cc2f246dda46b17e9302242879788aa114ee64327c8de43ef2b9ab56e8fb57b2
- 5c1704367332a659f6e10d55d08a3e0ab1bd26aa97654365dc82575356c80502
- c60e210f73d5335f57f367bd7e166ff4c17f1073fd331370eb63342ab1c82238
- f01dec606db8f66489660615c777113f9b1180a09db2f5d19fb5bca7ba3c28c7
- 4f1399e81571a1fa1dc822b468453122f89ac323e489f57487f6b174940e9c2e
- 9863bc1917af1622fdeebb3bcde3f7bebabcb6ef13eae7b571c8a8784d708d57
- a1fba0bb0f52f25267c38257545834a70b82dbc98863aee01865a2661f814723
- 81cfa53222fa473d91e2a7d3a9591470480d17535d49d91a1d4a7836ec943d3a
- 78b4478cd3f91c42333561abb9b09730a88154084947182b2ec969995b25ad78
- 91824c6a36ef60881b4f502102b0c068c8a3acd4bceb86eb4ffd1043f7990763
- 86b45b861a8f0855c97cc38d2be341cc76b4bc1854c0b42bdca573b39da026ac
- 84ff961552abd742cc2393dde20b7b3b7b2cfb0019c80a02ac24de6d5fcc0db4
- 0ee6c8fd43c03e8dc7ea081dfa428f22209ed658f4ae358b867de02030cfc69b
- 443b6173ddfbcc3f19d69f60a1e5d72d68d28b7323fe2953d051b32b4171aa9a
- 409f1b4aeb598d701f6f0ed3b49378422c860871536425f7835ed671ba4dd908
- 77f084b5fc81c9c885a9b1683a12224642072f884df9e235b78941a1ad69b80d
- cbabbbb270350d07444984aa0ce1bb47078370603229a3f03a431d6b7a815820
- 053fbb833ac1287d21ae96b91d9f5a9cfdd553bc41f9929521d4043e91e96a98
- 29e3d46867caddde8bb429ca578dd04e5d7112dd730cd69448e5fb54017a2e30
- 356d429187716b9d5562fe6eee35ea60b252f1845724b0a7b740fbddec73350f
- a98ecd8f482617670aaa7a5fd892caac2cfd7c3d2abb8e5c93d74c344fc5879c
- c94760fe237da5786464ec250eadf6f7f687a3e7d1a47e0407811a586c6cb0fc
- eb71d15308bfcc00f1b80bedbe1c73f1d9e96fd55c86cf420f1f4147f1604f67
- 0c08992841d5a97e617e72ade0c992f8e8f0abc9265bdca6e09e4a3cb7cb4754
- 738822e109f1b14413ee4af8d3d5b2219293ea1a387790f207d937ca11590a14
- 0d9f861fe4910af8299ac3cb109646677049fa9f3188f52065a47e268438b107
- a586ef06ab8dd6ad1df77b940028becd336a5764caf097103333975a637c51fa
- 73a465170feed88048dbc0519fbd880aca6809659e011a5a171afd31fa05dc0b
- d5c808926000bacb67ad2ccc4958b2896ea562f27c0e4fc4d592c5550e39a741
- 7067e6a69a8f5fdbabfb00d03320cfc2f3584a83304cbeeca7e8edc3d57bbbd4
- 939cebc99a50989ffbdbb2a6727b914fc9b2382589b4075a9fd3857e99a8c92a
- c5017798275f054ae96c69f5dd0b378924c6504a70c399279bbf7f33d990d45b
- 57d46205a5a1a5d6818ecd470b61a44aba0d935f256265f5a26d3ce791038fb4
- e8d4be891c518898dd3ccdff4809895ed21558d90d415cee868bebdab2da7397

- 9f1989a04936cd8de9f5f4cb1f5f573c1871b63737b42d18ac4fa337b089cbdc
- b55c806367946a70d619f25e836b6883a36c9ad22d694a173866b57dfe8b29c9
- e46b09b270552c7de1311a8b24e3fcc32c8db220c03ca0d8db05e08c76e536f1
- f9842e31ed16fe0173875c38a41ed3a766041350b4efcd09da62718557ca3033
- bad5dc1dd6ff19f9fb1af853a8989c1b0fdfeaa4c588443607de03fccf0e21c9

Download URLs

- hxxps://d35ep4bg5x8d5j[.]cloudfront[.]net/pkg
- hxxps://d7rp2fva69arq[.]cloudfront[.]net/pkg
- hxxps://daqi268hfl8ov[.]cloudfront[.]net/pkg
- hxxps://events[.]optimizerservices[.]com/pkg
- hxxps://ekogidekinvgwyzmeydw[.]s3[.]amazonaws[.]com/OptimizerProcotolStatus[.]zip
- hxxps://lnzjvpeyarvvvtljxsws[.]s3[.]amazonaws[.]com/ConsoleSoftwareUpdateAgent[.]zip
- hxxps://qqirhvehhnvuemxezfxc[.]s3[.]amazonaws[.]com/ModuleAgent[.]zip
- hxxps://dpqsxofvslaxjaiyjdok[.]s3[.]amazonaws[.]com/ProtocolStatus[.]zip
- hxxps://oldbrlauserz[.]s3[.]amazonaws[.]com/setup[.]zip
- hxxps://grxqorfazgqbmzeetpus[.]s3[.]amazonaws[.]com/SetupUpdateAgent[.]zip
- hxxps://phdhrhdsp[.]s3[.]amazonaws[.]com/setup[.]zip
- hxxps://xyxeaxtugahkwrcvbzsw[.]s3[.]amazonaws[.]com/BundleAgent[.]zip
- [.]s3[.]amazonaws[.]com/GuideServices[.]zip
- hxxps://tnkdcxekehzpnpvimdwquzwzgpehlnwgizrlmzev[.]s3[.]amazonaws[.]com/HelperModule[.]zip
- hxxps://svapnilpkasjmwtygfstkhsdfrraa[.]s3[.]amazonaws[.]com/WizardUpdate[.]zip