Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

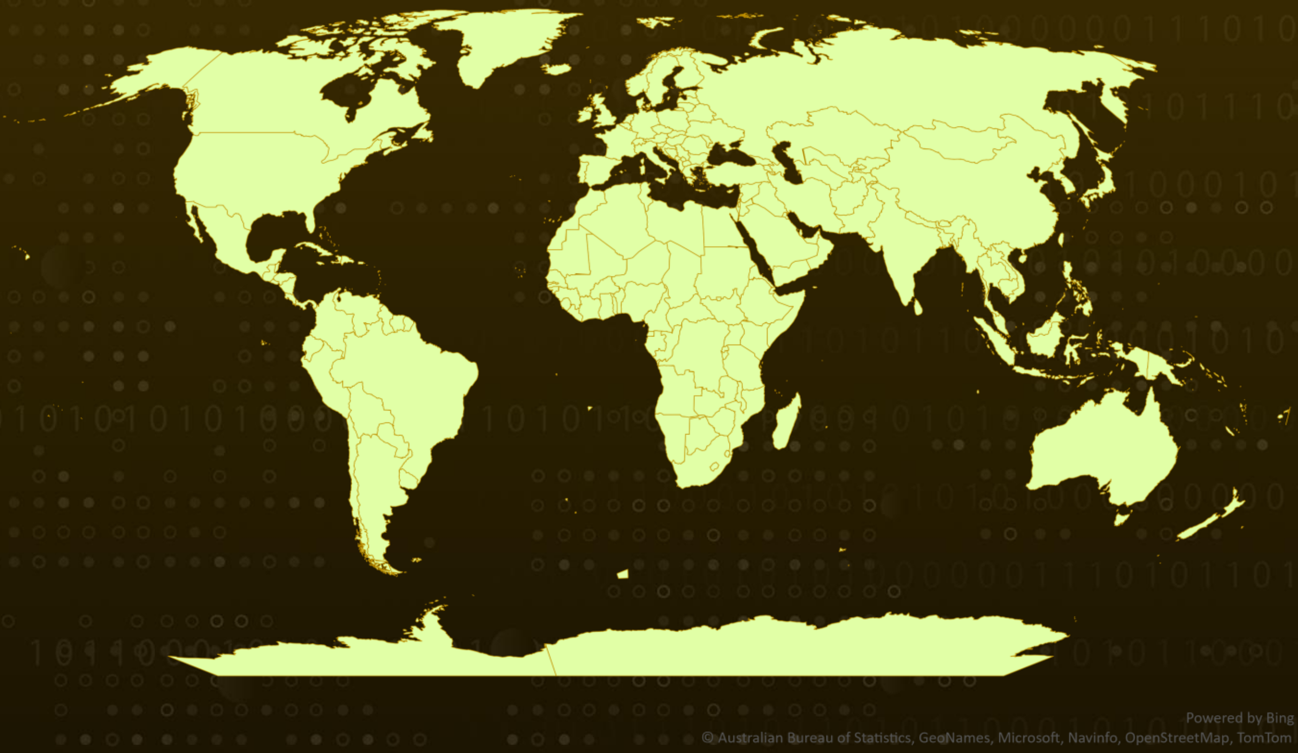
AdLoad Malware Persists on Mac Systems with New Proxy Payload

Date of Publication	Admiralty Code	TA Number
August 18, 2023	A1	TA2023336

Summary

First appeared: 2017
Attack Region: Worldwide
Malware: AdLoad
Affected Platforms: MacOS, and Windows
Attack: AdLoad malware persists on Mac systems with a new proxy application payload, converting infected devices into a proxy botnet. This scheme, involving thousands of IP addresses, points to a monetization strategy by a company offering proxy services, emphasizing the evolving nature of cyber threats.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

The AdLoad malware, discovered in 2017, remains a persistent threat to Mac systems, with new developments uncovered by AT&T Alien Labs. In the past year, over 150 instances of AdLoad have been detected in the wild, and its recent focus has been on a proxy application payload. This payload transforms infected Macs into a proxy botnet, with thousands of IP addresses acting as proxy exit nodes, suggesting a substantial number of compromised systems.

#2

AdLoad has a history of involvement in adware and bundleware campaigns, redirecting user traffic to insert ads into webpages. Its recent activity showcases a new payload involving proxy applications, further expanding its capabilities. The malware adjusts its payload based on factors like geolocation and operating system version. The proxy application payload is a part of a larger scheme involving a proxy service, where compromised systems are utilized for proxy purposes.

#3

The proxy application's cross-platform compatibility, working on macOS and Windows, is a notable aspect. Its communication involves a command and control server over port 7001, collecting system data and periodically checking for updates. This proxy scheme seems to be driven by monetization, as a company offers proxy services using the infected systems as exit nodes. The proxy application's stealthy installation, along with its ability to evade antivirus detection, underscores its efficacy.

#4

In sum, the ongoing presence of AdLoad underscores its resilience, and its recent shift towards proxy applications poses new challenges. The malware's ability to exploit infected systems for proxy services reflects a growing trend, highlighting the adaptability and evolving nature of cyber threats.

Recommendations

Software and System Updates: Regularly update operating systems, applications, and security software with the latest patches and updates. This helps to address vulnerabilities that malware can exploit.

Network Security Measures: Employ firewalls, intrusion detection systems, and network segmentation to monitor and control network traffic. These tools can help identify and contain malicious activities associated with the malware.

Application Whitelisting and Behavioral Analysis: Implement application whitelisting to only allow approved software to run. Additionally, use security solutions that employ behavioral analysis to detect abnormal activities indicative of malware infection.

Potential MITRE ATT&CK TTPs

TA0040 Impact	**TA0007** Discovery	**TA0005** Defense Evasion	**TA0011** Command and Control
TA0001 Initial Access	**TA0003** Persistence	**T1189** Drive-by Compromise	**T1543** Create or Modify System Process
T1543.001 Launch Agent	**T1140** Deobfuscate/Decode Files or Information	**T1497** Virtualization/Sandbox Evasion	**T1497.001** System Checks
T1222 File and Directory Permissions Modification	**T1222.002** Linux and Mac File and Directory Permissions Modification	**T1553** Subvert Trust Controls	**T1553.001** Gatekeeper Bypass
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1082** System Information Discovery	**T1090** Proxy
T1571 Non-Standard Port	**T1496** Resource Hijacking	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder
T1053 Scheduled Task/Job	**T1053.005** Scheduled Task		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b, 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472, 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc, 3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264, 2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709eff2fd6bd87, 7cb10a70fd25645a708c81f44bb1de2b6de39d583ae3a71df0913917ad1dffc3, 4a7c9829590e1230a448dd7a4272b9fbfbafccf7043441967c2f68f6082dde32, 68b6beb70bd547b75f2d36d70ca49f8b18542874480d39e33b09ee69eb1048b3, 1904b705105db4550371d678f8161826b98b1a9fca139fa41628214ed816d2f5, 2fb1d8e6454f43522f42675dcf415569e5df5d731e1d1390f793c282cce4a7aa, ee9ebdb1d9a7424cd64905d39820b343c5f76e29c9cd60c0cdd3bfe069fb7d51, c7721ab85bad163576c166a0a71c0dbe4cc491dda68c5a5907fd1d8cac50780d, 33585aed3e7c4387a3512b93612932718e9dff2358867ba8c4ad1e8073bbce31, 2b79d98043030645f27bd1b061ffa27eab19462dff356e6b4a89bb1d3c9bf02d, b0692f201e6dfdbe1b920849a31f2b9fb73db19779fdb77c660c28fa22b70a38, 424d35bc945ea2deda177b46978bbb45af74109a988450ea4ed5fe16c1f629f9, 518bc3b96a97a573c61934ff65cc284c3e5545c7823318918a7cb05cbb5518b1, 417cf3f959e1040ffe13fcf21691b05ea96da5849010b0a4d17c6cecbeaef621, 611ce42b0866c085d751c579f00b9e76c412a7d1e1ebcf998be6b666edc22416, 801ecf29bee98e3b942de85e08ec227373a15b0a253c9c3eb870af33709f3d8d, 7926a84dcb6ffbe93893477f7f3ad52516cfedf8def5c43686dd6737926146a7,

TYPE	VALUE
SHA256	3aaaa01bdd20981fdc94d52c5ac0ed762a124b0a08c22d760ab7e43554ee84dd, 7a33d3f5ca81cdcfe5c38f9a4e5bbf3f900aa8f376693957261cdbe21832c110, 5a11065473b9a1e47d256d8737c2952da1293f858fc399157ab34bbaadff6cb8, de97da00ed54a1f021019852a23b50c82408ab7a71dc0f3e6fef3680ac884842, dad35cdd6213381cc350688f6c287f4f3e1192526f78b9b62779acc4b03495f9, 42ae669786b19556de65eeb1c45ec4685016b69384c21f3bbc30aaf2cddb2126, e79c37dc791d1bdb01524d158421efa29dcebde250f7571e9e30714496b3c06f, f22452a13635e4651b51c1491312a74891ca1dcd1b5072cbb978c06dc0a560ca, 6c3f24ff26c5d2f16ae6aa8842e97d402c2e203d0aa2798a40f4dc000554dbca, aad7a088f309c1e0671f327db2428a470c14d08d5f6489fcb628071d2361b6a7, 0e364d219192854032767476173c91c3d61230990597b52e5c36ebadd0fd96d8, 331cf0f8049fc0e68e8bd75f8efed629b41459425a971cbcec53485ba2bf4521, 0ca119c7be4ec67355b47d8d197361e730d93153a87d09e00a68ceda340fabb0, db115eff8d8b013e89f398b922294b248d5d6be51d7ab60cbde3b6ff2ff3f219, 1cff1d3a10cc36338803e37cc3c9e9121bdd8c5189ca4533d1c585715561bc4a, 530e59f9bd99b191b54ec18eb92d6b44005e56c1dd877b4e4ce0370d3d917fb4, 9a416904a4d942c77177770ea0680c48e5d5eddba793af3c434e4ff733daab56, aeeccab5b4712f4c7d75c0606fc4587f13df7a04aa4941bb6599f328ee67d950, 3ff5e3932ba4a438c12c253ec6b00416ac6ce250173bac6be0bb8d619cea47bd, a10d023b10b878a09697563155799bd088ed2f797aff489b732959f917414f97, 65a9895f5e49f8e18727fe16744c6631c0676e08499f4407b9d8c11634aae5e0, e07aa2d15520c6f0ab9bbbe049f48402e4b91fde59b22b5668daef2ec924a68b,

TYPE	VALUE
SHA256	cc3cbc8ad7f71223230a457aa2664d77b43b7f7a4988b42609ad707f0385aee3, cba34f77ca2a5d4dc56f4567ff1f0b2242105d532353d2868d7b2c42f1a37551, 153de6a7d78bcce8a0cec446cdc20ec4b18ee72b74f59e76780ec5c76efddc52, 8505c4c3d6406cc55a9492cf1a3285de9c0357691112b2ab787faa57d55d304b, c2029115292930520006fa6bc6a87c66bbd5621738190dbd75a5b3a150fed5c41, 550c4839f26bf81f480c5e4210be3ded43d4f8027d5d689a6fe8692c42235940, 5324f5aae565ddc8dc2a4b574bc690cba6b35bd4bf3f63e6df14d613b68ac769
Domains	bapp.digitalpulsedata[.]com
URLs	hxxp://m.skilledobject[.]com/a/rep, hxxp://m.browseractivity[.]com/a/rep, hxxp://m.enchantedreign[.]com/a/rep, hxxp://m.activitycache[.]com/a/rep, hxxp://m.activityinput[.]com/a/rep, hxxp://m.opticalupdater[.]com/a/rep, hxxp://m.connectioncache[.]com/a/rep, hxxp://m.analyzerstate[.]com/a/rep, hxxp://m.essencecuration[.]com/a/rep, hxxp://m.microrotator[.]com/a/rep, hxxp://m.articlesagile[.]com/a/rep, hxxp://m.progresshandler[.]com/a/rep, hxxp://m.originalrotator[.]com/a/rep, hxxp://m.productiveunit[.]com/a/rep, hxxp://api.toolenviroment[.]com/l, hxxp://api.inetfield[.]com/l, hxxp://api.operativeeng[.]com/l, hxxp://api.launchertasks[.]com/l, hxxp://api.launchelemnt[.]com/l, hxxp://api.validexplorer[.]com/l, hxxp://api.majorsprint[.]com/l, hxxp://api.essentialenumerator[.]com/l, hxxp://api.transactioneng[.]com/l, hxxp://api.macreationsapp[.]com/l, hxxp://api.commondevice[.]com/l, hxxp://api.compellingagent[.]com/l,

TYPE	VALUE
URLs	hxxp://api.lookupindex[.]com/l, hxxp://api.practicalsync[.]com/l, hxxp://api.accessiblelist[.]com/l, hxxp://api.functionconfig[.]com/l, hxxps://vpnservices[.]live, hxxps:// upgrader[.]live, hxxp://bapp.pictureworld[.]co

References

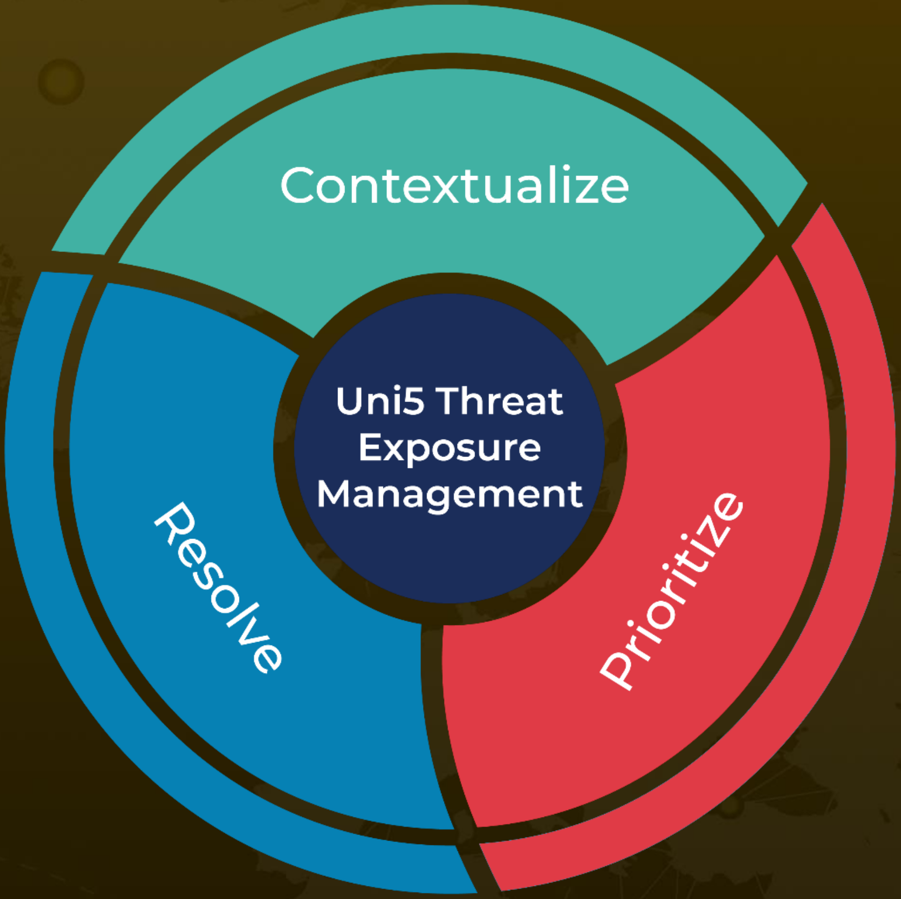
https://cybersecurity.att.com/blogs/labs-research/mac-systems-turned-into-proxy-exit-nodes-by-adload

https://cybersecurity.att.com/blogs/labs-research/proxynation-the-dark-nexus-between-proxy-apps-and-malware

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 18, 2023 • 6:40 AM

More at www.hivepro.com