THREAT ADVISORY

July 11, 2024

FakeBat Loader Malware Spreading Rapidly

SUMMARY

FakeBat, a loader-as-a-service (LaaS) utilizes the drive-by download technique to download and execute payloads like IcedID, Lumma, RedLine, SmokeLoader, SectopRAT, and Ursnif.

TECHNICAL DETAILS

Drive-by attacks involve methods like search engine optimization (SEO) poisoning, malvertising, and injecting malicious code into compromised websites to trick users into downloading fake software installers or browser updates.

FakeBat (aka EugenLoader and PaykLoader) has been available as a loader-as-a-service (LaaS) on underground forums by a Russian-speaking threat actor named Eugenfest (aka Payk_34) since at least December 2022. FakeBat is designed to evade security controls and allows customers to generate trojanized builds of legitimate software. It includes an administration panel to monitor installations over time. FakeBat initially used an MSI format for its malware builds, transitioning to an MSIX format in 2023 that incorporates a digital signature with a valid certificate to bypass Microsoft SmartScreen protections.

List of software targeted by FakeBat malveritsing campaigns:

- 1Password
- Advanced SystemCare
- AnyDesk
- Bandicam
- Craavos
- Cisco Webex
- Epic Games
- Google Chrome
- Inkscape
- MS OneNote
- MS Teams
- Notion
- OBS Studio
- OpenProject
- Pay WGT Golf
- Python
- Shapr3D
- Todoist
- Trading View
- Trello
- VMware
- Webull
- WinRAR
- Zoom

The malware is priced at $1,000 per week or $2,500 per month for the MSI format, $1,500 per week or $4,000 per month for the MSIX format, and $1,800 per week or $5,000 per month for a combined MSI and signature package. According to reaserchers at Sekoia, different activity clusters have been detected disseminating FakeBat through three primary approaches: impersonating popular software via malicious Google ads, fake

web browser updates on compromised sites, and social engineering schemes on social networks. These campaigns are likely associated with groups such as FIN7, Nitrogen, and BATLOADER. Additionally, FakeBat's command-and-control servers likely filter traffic based on characteristics such as User-Agent value, IP address, and location.

INDICATORS OF COMPROMISE (IoCs)

FakeBat C2 servers:

- 0212top[.]online
- 0212top[.]site
- 0212top[.]top
- 0212top[.]xyz
- 0909kses[.]top
- 11234jkhfkujhs[.]online
- 11234jkhfkujhs[.]site
- 11234jkhfkujhs[.]top
- 11234jkhfkujhs[.]xyz
- 1212stars[.]online
- 1212stars[.]site
- 1212stars[.]top
- 1212stars[.]xyz
- 2311foreign[.]xyz
- 2311forget[.]online
- 2311forget[.]site
- 2311forget[.]xyz
- 2610asdkj[.]online
- 2610asdkj[.]site
- 2610asdkj[.]top
- 2610asdkj[.]xyz
- 2610kjhsda[.]online
- 2610kjhsda[.]site
- 2610kjhsda[.]top
- 2610kjhsda[.]xyz
- 3010cars[.]online
- 3010cars[.]site
- 3010cars[.]top
- 3010cars[.]xyz
- 3010offers[.]online
- 3010offers[.]site
- 3010offers[.]top
- 3010offers[.]xyz
- 343-ads-info[.]top
- 364klhjsfsl[.]top
- 465jsdlkd[.]top
- 756-ads-info[.]site
- 756-ads-info[.]top
- 756-ads-info[.]xyz
- 875jhrfks[.]top
- 98762341tdgi[.]online
- 98762341tdgi[.]site
- 98762341tdgi[.]top
- 98762341tdgi[.]xyz
- 999-ads-info[.]top
- ads-info[.]ru
- ads-info[.]site

- aipanelnew[.]ru
- aipanelnew[.]site
- cdn-ads[.]ru
- cdn-ads[.]site
- cdn-dwnld[.]ru
- cdn-dwnld[.]site
- cdn-new-dwnl[.]ru
- clk-brom[.]ru
- clk-brom[.]site
- clk-brood[.]online
- clk-brood[.]top
- clk-info[.]ru
- clk-info[.]site
- cornbascet[.]ru
- cornbascet[.]site
- dns-inform[.]top
- fresh-prok[.]ru
- fresh-prok[.]site
- ganalytics-api[.]com
- gotrustfear[.]ru
- gotrustfear[.]site
- infocdn-111[.]online
- infocdn-111[.]site
- infocdn-111[.]xyz
- new-prok[.]ru
- new-prok[.]site
- newtorpan[.]ru
- newtorpan[.]site
- prkl-ads[.]ru
- prkl-ads[.]site
- test-pn[.]ru
- test-pn[.]site
- topttr[.]com
- trust-flare[.]ru
- trust-flare[.]site
- trustdwnl[.]ru
- ads-analyze[.]online
- ads-analyze[.]site
- ads-analyze[.]top
- ads-analyze[.]xyz
- ads-change[.]online
- ads-change[.]site
- ads-change[.]top
- ads-change[.]xyz
- ads-creep[.]top
- ads-creep[.]xyz
- ads-eagle[.]top
- ads-eagle[.]xyz
- ads-forget[.]top
- ads-hoop[.]top
- ads-hoop[.]xyz
- ads-moon[.]top
- ads-moon[.]xyz
- ads-pill[.]top
- ads-pill[.]xyz
- ads-star[.]online

- ads-star[.]site
- ads-star[.]top
- ads-star[.]xyz
- ads-strong[.]online
- ads-strong[.]site
- ads-strong[.]top
- ads-strong[.]xyz
- ads-tooth[.]top
- ads-tooth[.]xyz
- ads-work[.]site
- ads-work[.]top
- ads-work[.]xyz
- cdn-inform[.]com
- udr-offdips[.]com
- urd-apdaps[.]com
- usm-pontic[.]com
- utd-corts[.]com
- utd-forts[.]com
- utd-gochisu[.]com
- utd-horipsy[.]com
- utm-adrooz[.]com
- utm-adschuk[.]com
- utm-adsgoogle[.]com
- utm-adsname[.]com
- utm-advrez[.]com
- utm-drmka[.]com
- utm-fukap[.]com
- utm-msh[.]com
- utr-gavlup[.]com
- utr-jopass[.]com
- utr-krubz[.]com
- utr-provit[.]com
- amydlesk[.]com
- notilon[.]co
- notliion[.]com
- notlon[.]top
- notlilon[.]co
- notion.findreaders[.]com
- findreaders[.]com
- notion.ilusofficial[.]com

Fake web browser updates:

- brow-ser-update[.]top
- hxxps://brow-ser-update[.]top/download/dwnl.php
- hxxps://brow-ser-update[.]top/GoogleChrome-x86.msix
- photoshop-adobe[.]shop
- hxxps://photoshop-adobe[.]shop/download/dwnl.php
- c336d98d8d4810666ee4693e8c3a2a34191bad864d6b46e468a7eed36e7085f4 (GoogleChrome[1]x86.msix)
- b5ed2f42359e809bf171183a444457c378355d07b414f5828e1e4f7b35bb505f (boci.ps1)

Social engineering schemes on social networks:

- app.getmess[.]io
- hxxps://app.getmess[.]io/

- hxxps://app.getmess[.]io/download/dwnl.php
- hxxps://getmess[.]download/Getmess.msix
- utd-corts[.]com • hxxp://utd-corts[.]com/buy/
- 12ea41f2dfa89ad86f082fdf80ca57f14cd8a8f27280aca4f18111758de96d15 (Getmess.msix)
- 72a1f6e7979daae38d8e0e14893db4c182b8362acc5d721141ed328ed02c7e28 (ynwje.ps1)

Hashes:

- c336d98d8d4810666ee4693e8c3a2a34191bad864d6b46e468a7eed36e7085f4
- 7265ffdbe31dd96d6e6c8ead5a56817c905ff012418546e2233b7dce22372630
- 9aa39f017b50dcc2214ce472d3967721c676a7826030c2e34cb95c495dba4960
- 1bb51d62457f606e947a4e7ce86198e9956ae1fe4e51e4e945370cc25fe6bfff
- 400277618bd2591efb2eb22ac0041c1c5561d96c479a60924ef799de3e2d290c
- f3ebb23bdcc7ac016d958c1a057152636bc2372b3a059bf49675882f64105068
- 12ea41f2dfa89ad86f082fdf80ca57f14cd8a8f27280aca4f18111758de96d15
- 3bd95eadb44349c7d88ea989501590fb3652ae27eded15ab5d12b17e2708969f
- 67663233f9e3763171afd3a44b769dc67a8a61d4a159f205003c5fdb150e2ca1
- f0e0aea32962a8a4aecd0c4b0329dc7e901fa5b103f0b03563cf9705d751bbe1
- 8f88a86d57b93cd7f63dfdf3cb8cc398cdce358e683fb04e19b0d0ed73dd50ee
- 3d3a9cd140972b7b8a01dde2e4cd9707913f2eba09a3742c72016fd073004951
- 96bd6abb1c8ec2ede22b915a11b97c0cd44c1f5ed1cda8bee0acfee290f8f580
- f1d72a27147c42a4f4baf3e10a6f03988c70546bb174a1025553a8319717ba95
- 806d08e6169569eb1649b2d1f770ad30a01ff55beedfe93aebccac2bc24533c0
- 763bdd0b5413bb2e0e3c4a68a7542586bbd638665b7ca250dbd9c7558216e427
- 9a2268162982113c12d163b1377dc4e72c93f91e26bd511d16c1b705262ca03c
- e5b94c001fc3c1c1aa35c71a3d1e9909124339e0ade09f897b918fe0729c12e1
- 9e800a05e65efe923a35815157129652980f03cbcf95cf0d64676f6da73471de
- f312e59be5ddbf857d92de506d55ae267800b0cbc2b82665ce63c889a7ae9414
- 7c7dc62ed7af2f90aeafdd5c3af5284c5539aeded7d642d39f5fd5f187d33c87
- 409a2a2a4e442017e6d647524fdec11507515a9f58a314e74307e67059bd8149
- 1d5d671bf680d739ded1e25e78970b38d00e8182816171a7c6a186504a79eeee
- aa998fde06a6a6ab37593c054333e192ce4706a14d210d8fc6c0de3fd2d74ce2
- 767dd301dc5297828a35eaba81f84bd0f50d61fe1a9208b8d89b5eaba064d65e
- 7d0aaf734f73c1cf93e53703e648125bba43e023203be9a938f270dfe3492718
- 6e0179344ca0bbc42dce77027f5a6a049844daf34595fd184d9f094e8c74325c
- 49a7668d60e8df9d0a57ba9e0e736c1eb48700da19711cc0ec0f3c94a56ce507
- 2e8a82f07de254848615f81272f08e0cf9af474d1c20f67d9ddbdf439f1d8fde
- f0f77c85c7da4391e34d106c4b5f671eb606ba695dc11401a6ee8ae53e337cbe
- d1da457b0891b68df16ce86e2a48a799b9528c1631bccc379623551f873c0eed
- 175fcb7495c0814a5c18afa6244d467f0daeb0f02ad93c0ab4d3af8cbbacb537
- 7316ed0cb0fdbede33a0b6d05d0be1fe3c616ef7c1098dfcc9a2339c793e7020
- 90641a72a4ea6f1fca57ec5e5daec4319ec95bec53dd2bf0fa58d1f9ade42ad4
- 6fb502d83b7b5181abcb53784270239cc3e4143344e1f64101537aa3848c8c95
- 2b033fc28ad12cb57c7c691bd40911ca47dd2a8e495a2d253557d2c6bcd40c5e
- 4029e194864e2557786e169c7f2c101b9972164de7b4f1ffadf89382317cf96c
- 020cd2e4ec27185550bf736b490d8ace0d244fe09315f9f7e18362de659bc7ad
- b5ed2f42359e809bf171183a444457c378355d07b414f5828e1e4f7b35bb505f
- 5ee273180702a54f32520be02c170ad154588893b63eefe2062cdb34ad83712c
- 1c5cadde01f10a730cd8f55633c967c3a7259f4906f961477b7e095e7db326b7
- 72a1f6e7979daae38d8e0e14893db4c182b8362acc5d721141ed328ed02c7e28
- 00e7e8a0e8495189bb7feca21864fbd6c61a5aa680462186504de02536e0c2f9
- 088ed84658a7c3bef4401601ef67a6953492fb0200a3b580bfabb21cd3ac8236
- b7aa4697e16bbafe0df02ab3b8d0be8ec6e4abf6e6ca7d787d3d3684ca8f4b63
- f138728ce2cc87201a51c9250fa87cbab20354012a8f566e1b2cd776cc1a66af
- 0c4cef985c90ed764f041c2ccab6820fdbe38edaaddebe01a5b8d31d93204b88
- f8ab48848ab915d1b23e3ee51dd20a2699bd4f277bde218a727d7a55a572d174

- 07a0986ab43f717e181a32d6742b11f788403ce582ad5fcbb9d20d0bd40d410b
- 5e5c134cea48e57da9604981c0a7fd6ef1704c4151b540f29de685e0017fa730
- e3f18df1d8f5e27a41221246cc63236487c56354ba0c926a3fdaea70db901adb
- 4e39fa74e49be2bf26fbfbbcea12d1374fa2f1607ff7fa2a0c8c323e697959ad
- d069437eda843bd7a675a1cca7fd4922803833f39265d951fa01e7ad8e662c60
- 904ce1b1ffa601f9aeb0a6d68bc83532c5e76b958029bd1c889937fa7cf1867f
- 00ea5d43f2779a705856a824a3f8133cb100101e043cb670e49b163534b0c525
- cea1c4f2229e7aa0167c07e22a3809f42ec931332da7cc28f7d14b9e702af66b
- ae641dda420f2cf63ac29804f7009ba1c248c702679fbccef35e4d9319d77d2d

RECOMMENDATIONS

- Ensure that all software and systems are kept up to date with the latest security patches.
- Implement comprehensive security solutions that include anti-malware, anti-phishing, and firewall protection.
- Use MFA for accessing sensitive systems and data to add an extra layer of security.
- Conduct regular training sessions on recognizing phishing and social engineering attacks.
- Continuously monitor network traffic for unusual activity and signs of malicious behavior.
- Implement URL filtering to block access to known malicious websites.
- Allow only approved applications to run on your systems.

REFERENCES

- https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
- https://thehackernews.com/2024/07/fakebat-loader-malware-spreads-widely.html