



## IT threat evolution Q1 2023

07 JUN 2023 10 minute read



### Table of Contents

[IT threat evolution in Q1 2023](#)

[IT threat evolution in Q1 2023. Non-mobile statistics](#)

[IT threat evolution in Q1 2023. Mobile statistics](#)

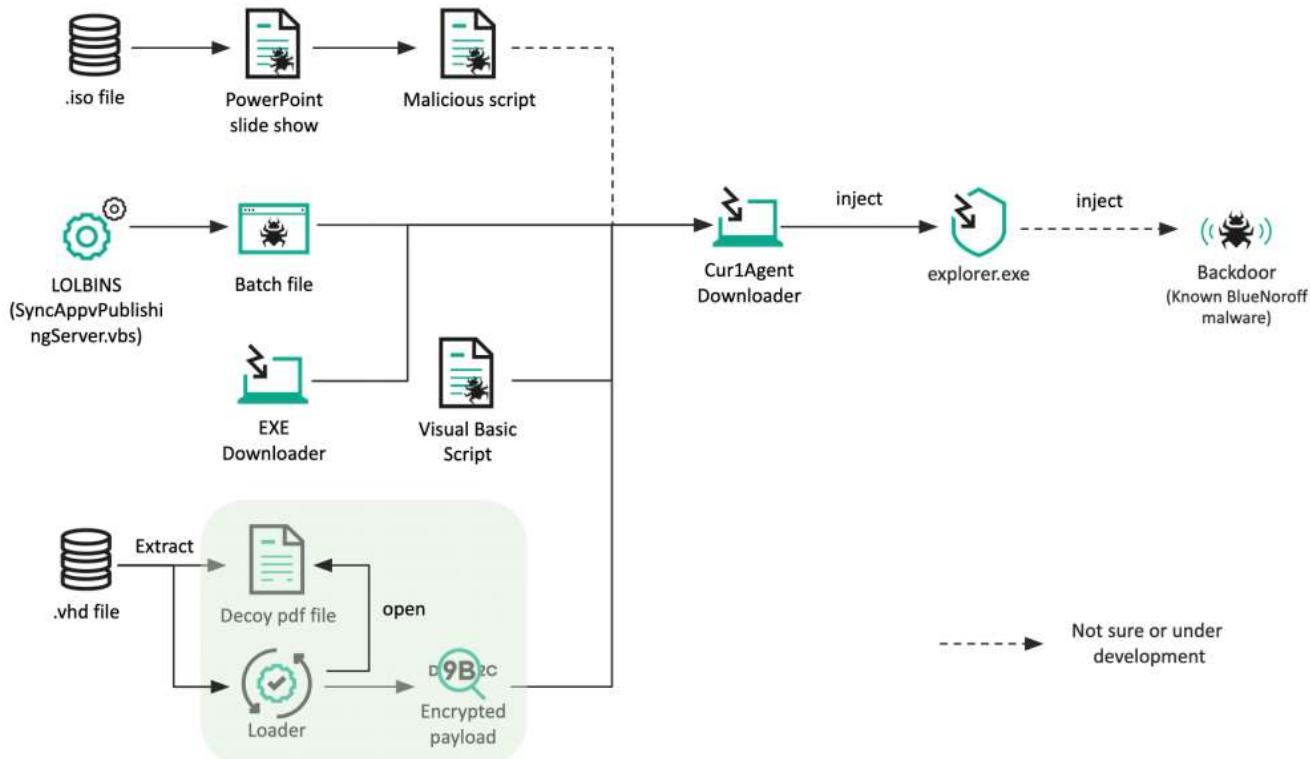
# Targeted attacks

## BlueNoroff introduces new methods bypassing MotW

At the close of 2022, we reported the [recent activities of BlueNoroff](#), a financially motivated threat actor known for stealing cryptocurrency. The threat actor typically exploits Word documents, using shortcut files for the initial intrusion. However, recently the group has adopted new methods to deliver its malware.

One of these, designed to evade the Mark-of-the-Web (MotW) flag, is the use of .ISO (optical disk image) and .VHD (virtual hard disk) file formats. MotW is a Windows security measure — the system displays a warning message when someone tries to open a file downloaded from the internet.

The threat actor also seems to be experimenting with new file types to deliver its malware. We observed a new Visual Basic script, a previously unseen Windows Batch file and a Windows executable.

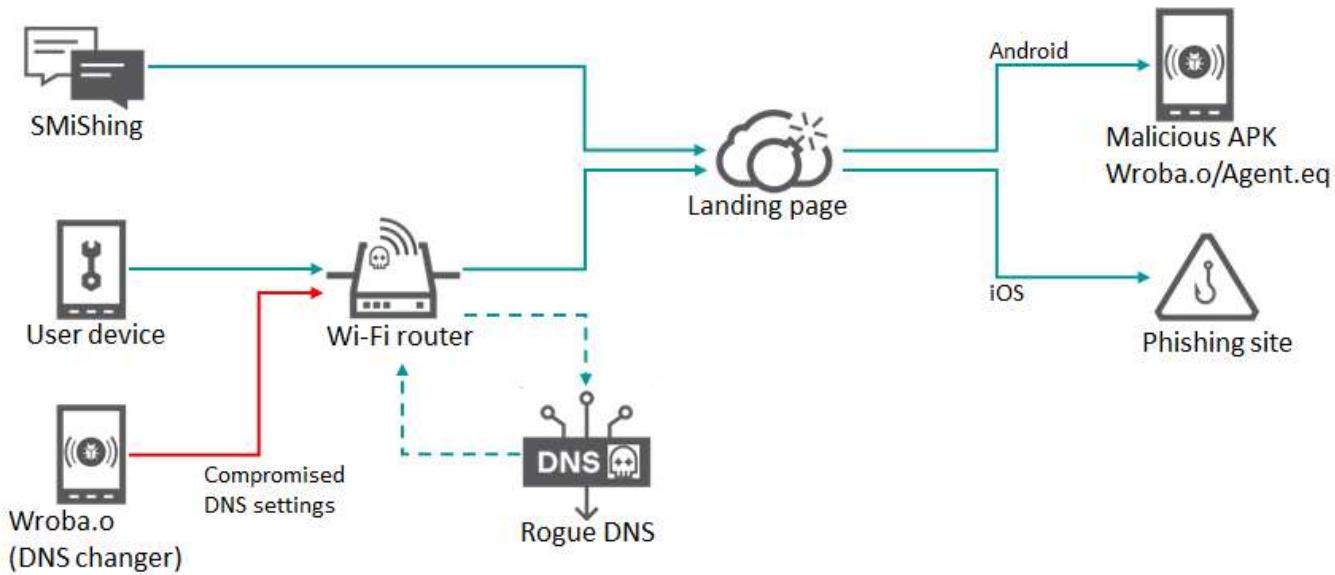


Our analysis revealed more than 70 domains used by this group, meaning that they were very active until recently. They also created numerous fake domains that look like venture capital and bank domains: most of these imitate Japanese venture capital companies, indicating that the group has an extensive interest in Japanese financial entities.

## Roaming Mantis implements new DNS changer

We continue to track the activities of Roaming Mantis (aka Shaoye), a well-established threat actor targeting countries in Asia. From 2019 to 2022, this threat actor mainly used ‘smishing’ to deliver a link to its landing page, with the aim of controlling infected Android devices and stealing device information, including user credentials.

However, in September 2022, we analyzed the new Wroba.o Android malware, used by Roaming Mantis, and [discovered a DNS changer function](#) that was implemented to target specific Wi-Fi routers used mainly in South Korea.



This can be used to manage all communications from devices using a compromised Wi-Fi router with the rogue DNS settings — for example, to redirect someone to malicious hosts and interfere with security product updates. People connect infected Android devices to free, public Wi-Fi in such places as cafes, bars, libraries, hotels, shopping malls, and airports. When connected to a targeted Wi-Fi model with vulnerable settings, the malware will compromise the router and affect other devices as well. As a result, it can spread widely in the targeted regions.

## BadMagic: new APT related to the Russo-Ukrainian conflict

Since the start of the Russo-Ukrainian conflict, we have identified a significant number of geo-political cyber-attacks, as outlined in our [overview of the cyber-attacks related to the conflict](#).

Last October, we identified an active infection of government, agriculture and transportation organizations located in Donetsk, Lugansk and Crimea. The initial vector of compromise is unclear, but the details of the next stage imply the use of spear-phishing or something similar. The targets navigated to a URL pointing to a ZIP archive hosted on a malicious web server. This archive contained two files: a decoy document (we discovered PDF, XLSX and DOCX versions) and a malicious LNK file with a double extension (e.g. PDF.LNK) which, when opened, results in infection.



ВИБОРЧА КОМІСІЯ  
РЕСПУБЛІКИ КРИМ

ИЗБИРАТЕЛЬНАЯ  
КОМИССИЯ  
РЕСПУБЛИКИ КРЫМ

КЪЫРЫМ  
ДЖУМХУРИЕТИНИНЬ  
САЙЛАВ КОМИССИЯСЫ

ул. Карла Маркса, 18, г. Симферополь, Республика Крым,  
Российская Федерация, 295000, тел/факс (3652) 27-61-84, e-mail: [ikrk2014@mail.ru](mailto:ikrk2014@mail.ru)

№ \_\_\_\_\_  
На № \_\_\_\_\_ от \_\_\_\_\_

Главному федеральному  
инспектору по Республике Крым

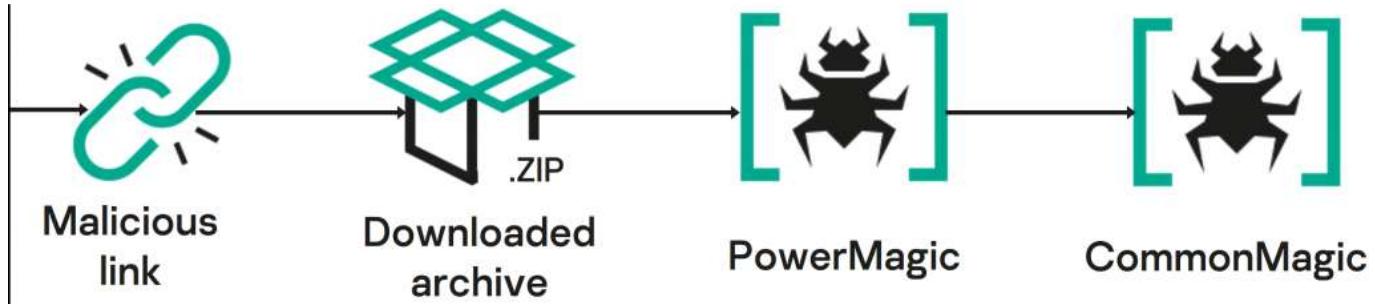
Уважаемый !

В соответствии с Вашим письмом от 13.09.2021 года № о предоставлении информации о ходе проведения на территории Республики Крым выборов, назначенных на 19 сентября 2021 года, Избирательная комиссия Республики Крым информирует об итогах выборов депутатов Государственной Думы Федерального Собрания Российской Федерации восьмого созыва.

1) Число протоколов № 2 окружных избирательных комиссий об итогах голосования по федеральному избирательному округу на соответствующих территориях, на основании которых составлен протокол избирательной комиссии субъекта Российской Федерации об итогах

In several cases, the contents of the decoy document were directly related to the name of the malicious LNK, to trick the user into activating it

The LNK file downloads and installs a PowerShell backdoor called "PowerMagic", which in turn deploys a sophisticated modular framework called "CommonMagic". We discovered CommonMagic plugins capable of stealing files from USB devices as well as taking screenshots and sending them to the threat actor.



During [our initial analysis](#), we were unable to find anything to connect the samples we found and the data used in the campaign to any previously known threat actor. However, our continuing investigations revealed more information about this threat, including links to other APT campaigns. You can find the details [here](#).

## Other malware

### Prilex targets contactless credit card transactions

Prilex has evolved from ATM-focused malware into [the most advanced PoS threat we have seen so far](#). The threat actor goes beyond the old memory scrapers seen in PoS attacks, to highly advanced malware that includes a unique cryptographic scheme, real-time patching of target software, forcing protocol downgrades, manipulating cryptograms, performing so-called “[GHOST transactions](#)” and credit card fraud – even on chip-and-PIN cards.

While investigating an incident, we discovered new Prilex samples, and one of the new features included the ability to [block contactless transactions](#). These transactions generate a unique identifier that’s valid for just one transaction, making them worthless to cybercriminals. By blocking the transaction, Prilex tries to force the customer to insert their card to make a chip-and-PIN transaction instead, allowing the cybercriminals to capture data from the card using their standard techniques.

With contactless card transactions increasing, this is a valuable technique that allows the Prilex threat actor to continue stealing card information.

The threat actor uses social engineering to infect a PoS terminal. They try to convince employees of a retail outlet that they urgently need to update the terminal’s software and to allow a “technical specialist” to visit the store, or at least provide remote access to the terminal. It’s important that retail organizations are alert to the signs of infection – including repeated failed contactless transactions – and [educate staff](#) about the methods used by cybercriminals to gain entry to their systems.

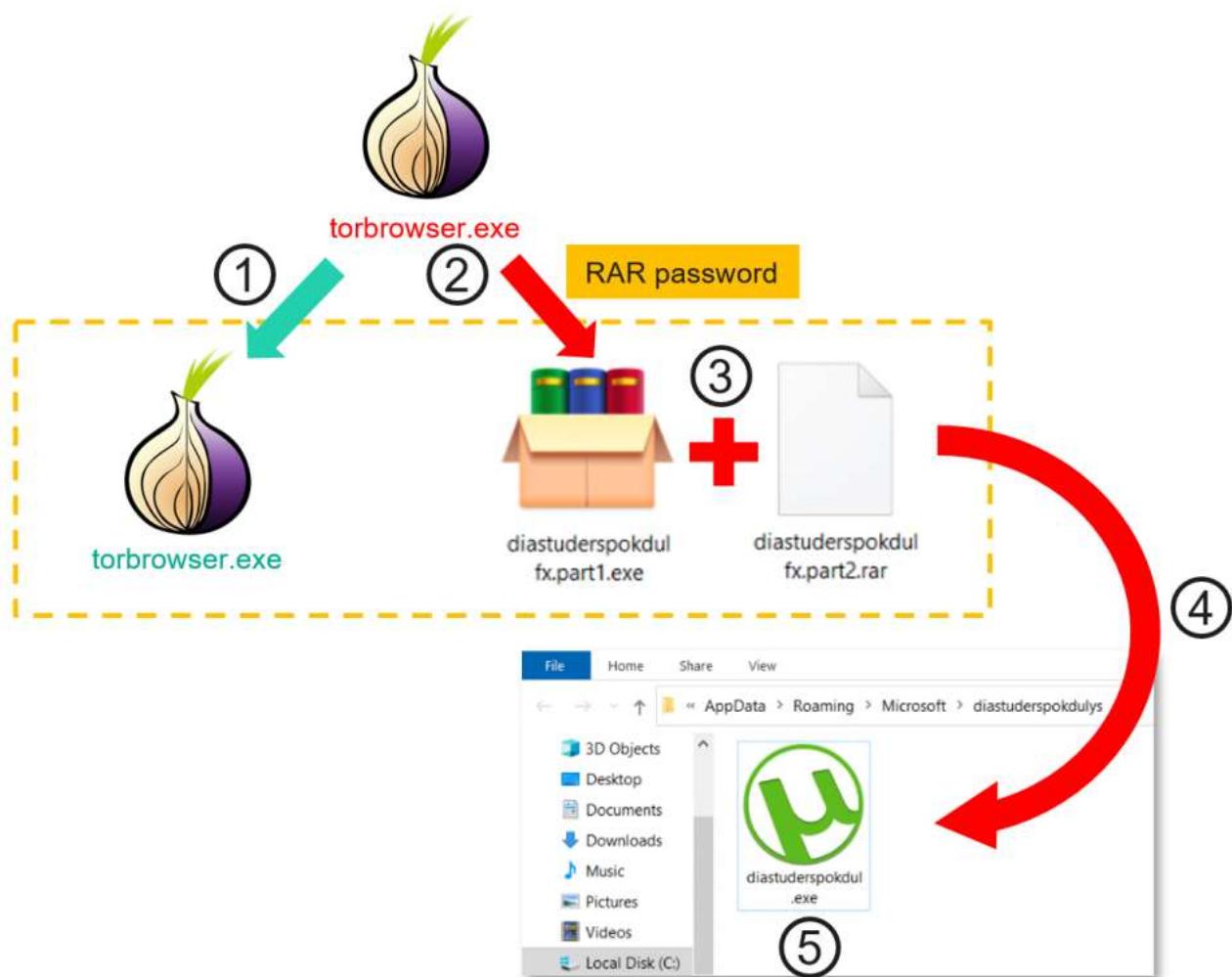
For retail companies (especially large networks with many branches), it’s important to develop internal regulations and explain to all employees exactly how technical support and/or maintenance crews should operate. This should at least prevent unauthorized access to POS-terminals. In

addition, increasing [employee's awareness of the latest cyberthreats](#) is always a good idea: that way they'll be much less susceptible to new social engineering tricks.

## Stealing cryptocurrency using a fake Tor browser

We recently [discovered an ongoing cryptocurrency theft campaign](#) affecting more than 15,000 users across 52 countries. The attackers used a technique that has been around for more than a decade and was originally used by banking Trojans to replace bank account numbers. However, in the recent campaign, the attackers used a Trojanized version of the Tor Browser to steal cryptocurrency.

The target downloads the Trojanized version of the Tor Browser from a third-party resource containing a password protected RAR archive – the password is used to prevent it being detected by security solutions. Once the file is dropped onto the target's computer, it registers itself in the system's auto-start and masquerades as an icon for a popular application, such as uTorrent.



The malware waits until there is a wallet address in the clipboard and then replaces a portion of the entered clipboard contents with the cybercriminal's own wallet address.

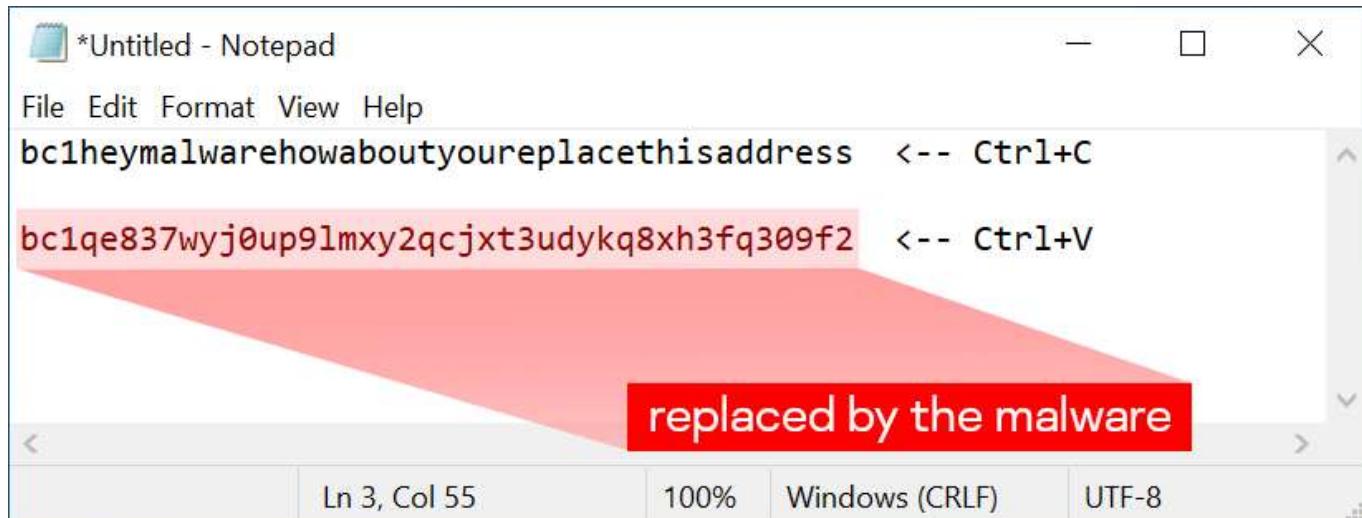
Our analysis of existing samples suggests that the estimated loss for those targeted in the campaign is at least \$400,000, but the actual amount stolen could be much greater, as our research focused only on Tor Browser abuse. Other campaigns may use different software and malware delivery methods, as well as other types of wallets.

We haven't been able to identify a single web site that hosts the installer, so it is probably distributed either via torrent downloads or some other software downloader. The installers coming from the official Tor Project are digitally signed and didn't contain any signs of such malware. So, to stay safe, you should download software only from reliable and trusted sources. Even where someone has downloaded the Trojanized version, a good anti-virus product should be able to detect it.

There is also a way to check if your system is compromised with malware of the same class. Put the following "Bitcoin address" into Notepad:

**bc1hey malware how about you replace this address**

Now press Ctrl+C and Ctrl+V. If the address changes to something else — the system is probably compromised by clipboard-injector malware and is dangerous to use.



We would recommend that you scan your system with security software. If you want to have full confidence that no hidden backdoors remain, once a system has been compromised, you should not trust it until it has been rebuilt.

## **It seems that everyone's chatting about ChatGPT**

Since OpenAI opened up its large [GPT-3](#) language model to the general public through [ChatGPT](#), interest in the project has soared, as people rushed to explore its possibilities, including writing poetry, engaging in dialogue, providing information, creating content for web sites and more.

There has also been a good deal of discussion about the [potential impact of ChatGPT on the threat landscape](#).

Given ChatGPT's ability to mimic human interaction, it's likely that automated spear-phishing attacks using ChatGPT are already taking place. ChatGPT allows attackers to generate persuasive, personalized e-mails on an industrial scale. Moreover, any responses from the target of the phishing message can easily be fed into the chatbot's model, producing a compelling follow-up in seconds. That said, while ChatGPT may make it easier for cybercriminals to churn out phishing messages, it doesn't change the nature of this form of attack.

Cybercriminals have also reported on underground hacker forums how they have used ChatGPT to create new Trojans. Since the chatbot is able to write code, if someone describes a desired function (for example, "save all passwords in file X and send via HTTP POST to server Y"), they can create a simple info-stealer without having any programming skills. However, such Trojans are likely to be primitive and could contain bugs that make it less effective. For now, at least, chatbots can only compete with novice malware writers.

We also uncovered a [malicious campaign](#) that sought to exploit the growing popularity of ChatGPT. Fraudsters created social network groups that mimicked communities of enthusiasts. These groups also contained fake credentials for pre-created accounts that purported to provide access to ChatGPT. The groups contained a plausible link inviting people to download a fake version of ChatGPT for Windows.

Introducing ChatGPT research release [Try](#) [Learn more](#)

[OpenAI](#)

[API](#) [RESEARCH](#) [BLOG](#) [ABOUT](#)

## ChatGPT: Optimizing Language Models for Dialogue

We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests. ChatGPT is a sibling model to InstructGPT, which is trained to follow an instruction in a prompt and provide a detailed response.

[DOWNLOAD FOR WINDOWS](#)

November 30, 2022  
13 minute read

The malicious link installs a Trojan that steals account credentials stored in Chrome, Edge, Firefox, Brave and other browsers.

Since security researchers frequently publish reports about threat actors, including TTPs (Tactics, Techniques and Procedures) and other indicators, we decided to try to find out [what ChatGPT](#)

already knows about threat research and whether it can help common malicious tools and IoCs (Indicators of Compromise), such as malicious hashes and domains.

The responses for host-based artifacts looked promising, so we instructed ChatGPT to write some code to extract various metadata from a test Windows system and then to ask itself whether the metadata was an IoC:

SE

Write PowerShell script to download Sysinternals Autoruns, upload it via WinRM to remote system, run it remotely and for each line of output extract LaunchString column and ask ChatGPT API if it is an indicator of compromise



Here is a PowerShell script that downloads Sysinternals Autoruns, uploads it via WinRM to a remote system, runs it remotely, and for each line of output, extracts the "LaunchString" column and asks the OpenAI ChatGPT API if it is an indicator of compromise:

Copy code

```
# Download Sysinternals Autoruns
Invoke-WebRequest -Uri "https://download.sysinternals.com/files/Autoruns.zip" -OutFile "Autoruns.zip"
Expand-Archive -Path "Autoruns.zip" -DestinationPath "C:\temp"

# Upload the file to remote system via WinRM
$session = New-PSSession -ComputerName "REMOTE_HOST"
Copy-Item -Path "C:\temp\Autoruns.exe" -Destination "C:\temp" -ToSession
$session

# Run Autoruns remotely and capture the output
$output = Invoke-Command -Session $session -ScriptBlock { C:\temp\Autoruns.exe -a }

# Split the output into rows
$rows = $output -split "`n"

# For each row, extract the LaunchString column
foreach ($row in $rows) {
```

Since certain code snippets were handier than others, we continued developing this proof of concept manually: we filtered the output for events where the ChatGPT response contained a "yes" statement regarding the presence of an IoC, added exception handlers and CSV reports, fixed small bugs and converted the snippets into individual cmdlets, which produced a simple IoC scanner, HuntWithChatGPT.psm1, capable of scanning a remote system via WinRM.

While the exact implementation of IoC scanning may not currently be a very cost-effective solution at \$15 to £20 per host for the OpenAI API, it shows interesting interim results, and reveals opportunities for future research and testing.

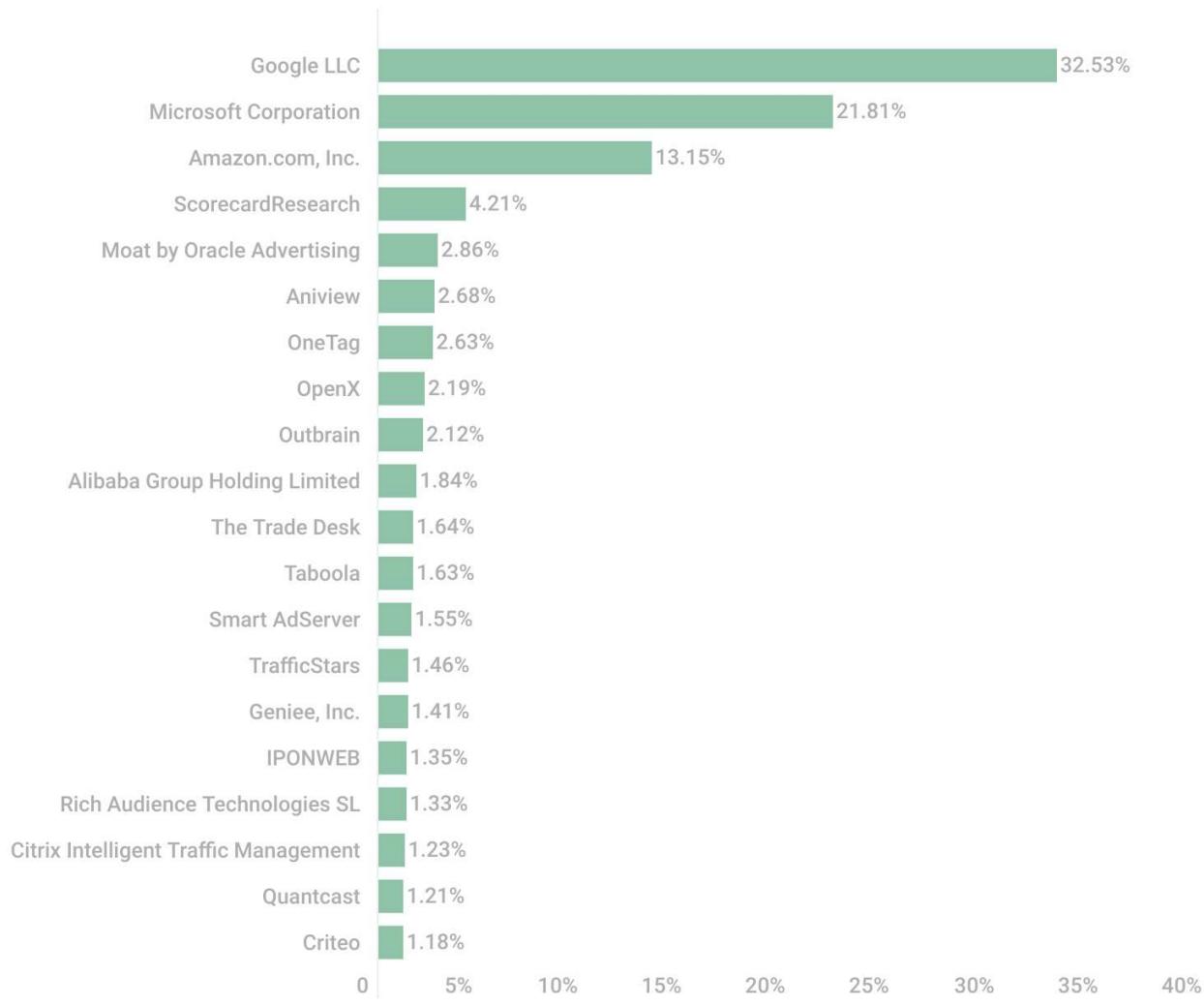
The impact of AI on our lives will extend far beyond the current capabilities of ChatGPT and other current machine learning projects. Ivan Kwiatkowski, a researcher in our Global Research and Analysis Team, recently [explored the likely scope of the changes we can expect](#) in the long term. These perspectives not only include the productivity gains offered by AI, but the social, economic and political implications of the changes it is likely to usher in.

## Tracking our digital footprints

We've become used to service providers, marketing agencies and analytical companies tracking our mouse clicks, social media posts and browser and streaming services history. Companies do this for a number of reasons. They want to understand our preferences better, and suggest products and services that we're more likely to buy. They do it to find out which images or text we focus on most. They also sell on our online behavior and preferences to third parties.

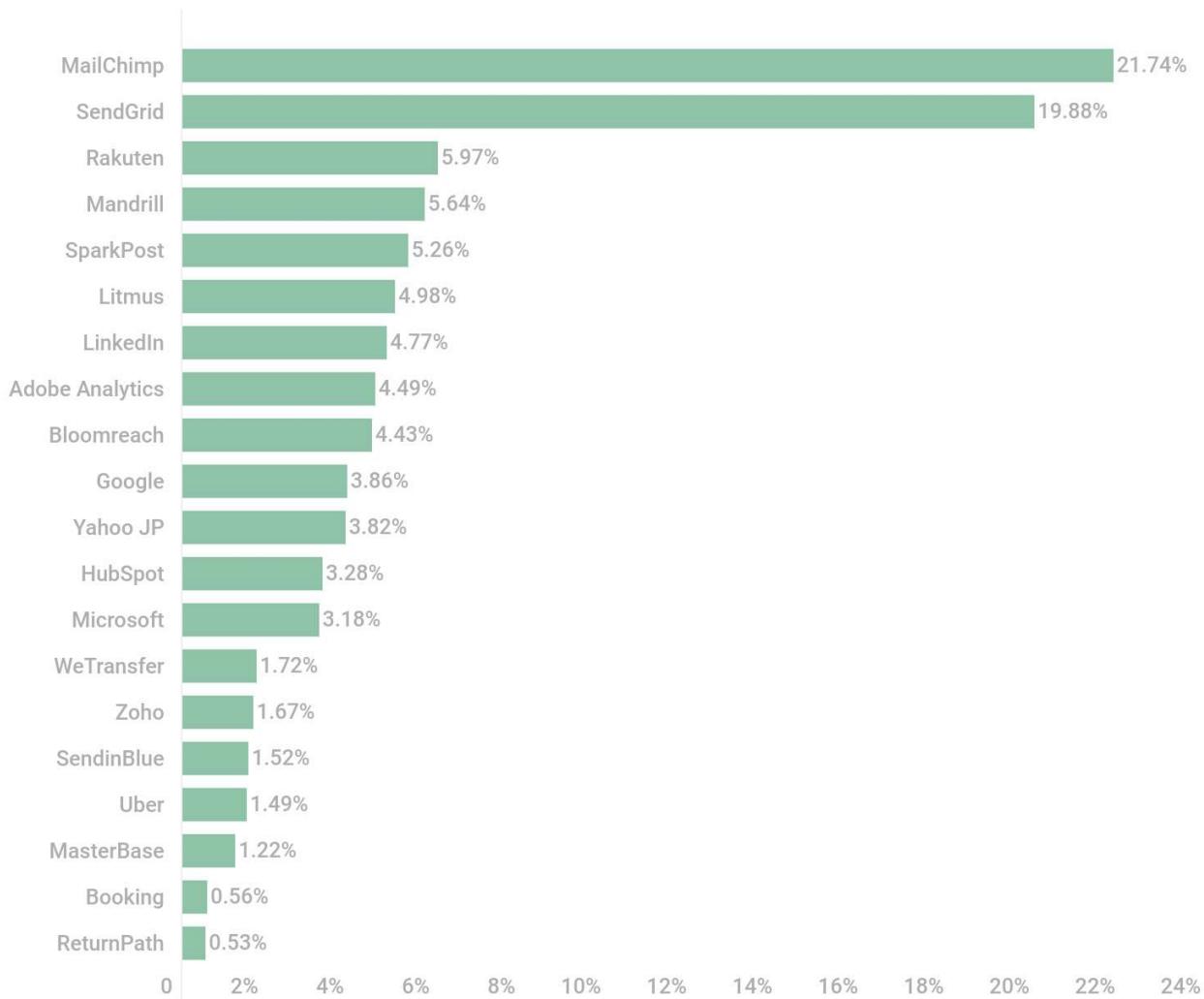
The tracking is done using web beacons (aka tracker pixels and spy pixels). The most popular tracking technique is to insert a tiny image –1x1 or even 0x0 pixels in size – into an e-mail, application, or web page. The e-mail client or browser makes a request to download the image from the server by transmitting information about you, which the server records. This includes the time, device, operating system, browser, and the page from which the pixel was downloaded. This is how the operator of the beacon learns that you opened the e-mail or web page, and how. Often a small piece of JavaScript inside the web page, which can collect even more detailed information, is used instead of a pixel. These beacons, placed on every page or application screen, make it possible for companies to follow you wherever you go on the web.

In our [recent report on web trackers](#), we listed the 20 most common beacons found on web sites and in e-mail. The data for web beacons is based on anonymous statistics from the Do Not Track (DNT) component of Kaspersky consumer products, which blocks the loading of web site trackers. Most of the companies have at least some connection to digital advertising and marketing, including tech giants such as Google, Microsoft, Amazon and Oracle.



**kaspersky**

The data for e-mail beacons is from anonymized anti-spam detection data from Kaspersky mail products. The companies in the list are either e-mail service providers (ESP) or customer relationship management (CRM) companies.

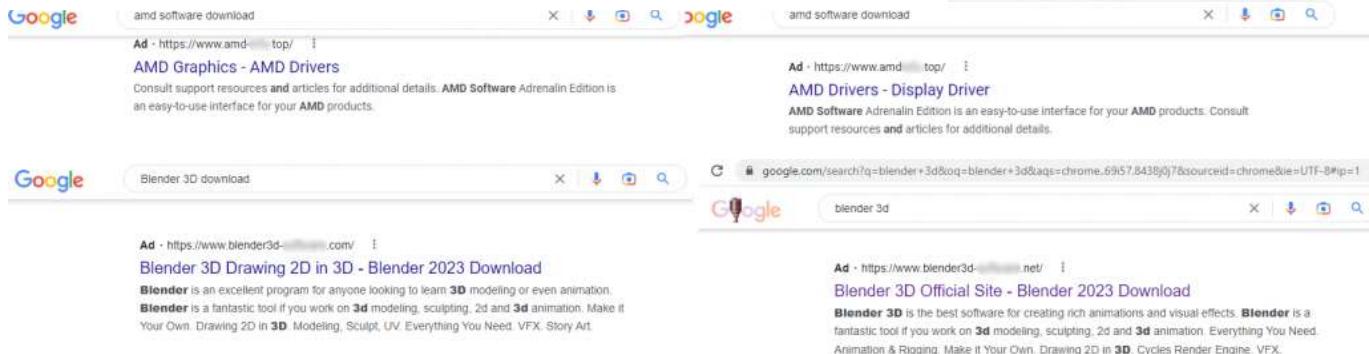


**kaspersky**

The information collected using trackers is of value not just to legitimate companies, but also to cybercriminals. If they are able to obtain such information — for example, as result of a data leak — they can use it to hack online accounts or send fake e-mails. In addition, attackers make use of web beacons too. You can find information on how to protect yourself from tracking [here](#).

## Malvertising through search engines

In recent months, we have observed an increase in the number of malicious campaigns that use Google Advertising as a means of distributing and delivering malware. At least two different stealers, Rhadamanthys and RedLine, [abused](#) the search engine promotion plan in order to deliver malicious payloads to victims' computers.



They seem to be using the same technique of mimicking a web site associated with well-known software, such as Notepad++ and Blender 3D. The threat actors create copies of legitimate software web sites and use “typosquatting” (using incorrectly spelled brands or company names as URLs) or “combosquatting” (as above, but adding arbitrary words as URLs) to make the sites look legitimate. They then pay to promote the site in the search engine in order to push it to the top of search results – a technique known as “malvertising”.

Fully Featured

Whether you do animation, modeling, VFX, games, you name it. Blender's got you covered.

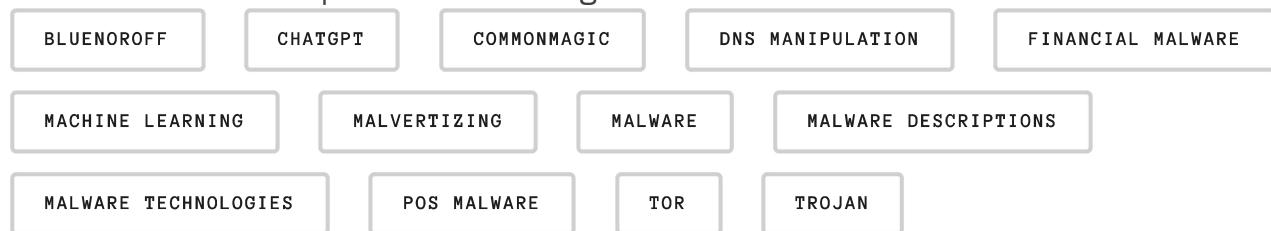
Free & Open Source

Free to Use. Free to Share. Free to Change. Free to Sell Your Work. Blender is Free Software.

Be Part of It

Blender's main strength is its huge community. Made by hundreds of contributors from around the world.

The distribution of malware that we have seen suggests that threat actors are targeting victims, both individual and corporate, across the globe.



## Authors

DAVID EMM

## IT threat evolution Q1 2023

Your email address will not be published. Required fields are marked \*

Name \*

Email \*

## Comment

## // LATEST POSTS

## **Windows CLFS and five exploits used by ransomware operators (Exploit #4 – CVE-2023-23376)**

BORIS LARIN

## **Windows CLFS and five exploits used by ransomware operators (Exploit #3 – October 2022)**

BORIS LARIN

## **Windows CLFS and five exploits used by ransomware operators (Exploit #2 – September 2022)**

BORIS LARIN

## // LATEST WEBINARS



## TECHNOLOGIES AND SERVICES

11 DEC 2023, 4:00PM

## The Future of AI in cybersecurity: what to expect in 2024

Vladimir Dashchenko, Victor Sergeev,  
Vladislav Tushkanov, Dennis Kipker

# 2024 Advanced persistent threat predictions

kaspersky

CYBERTHREAT TALKS

14 NOV 2023, 4:00PM

## 2024 Advanced persistent threat predictions

IGOR KUZNETSOV, DAVID EMM, MARC RIVERO, DAN DEMETER,

## **Windows CLFS and five exploits used by ransomware operators (Exploit #1 – CVE-2022-24521)**

BORIS LARIN



## THREAT INTELLIGENCE AND TR

30 NOV 2023, 4:00PM 70 MIN

## Responding to a data breach: a step-by-step guide

ANNA PAVLOVSKAYA

The image features the Kaspersky logo at the bottom left. To its right is a dark green rectangular banner with white text that reads "2024 Advanced persistent threat predictions". The background of the slide is a dark green gradient. On the right side, there is a 3D rendering of a black server rack unit with several glowing blue lights on its front panel. A bright red beam of light originates from the top of the server and points towards the text on the banner.

# Modern car: compromise techniques and methods of protection



CYBERTHREAT TALKS

09 NOV 2023, 5:00PM

## **Overview of modern car compromise techniques and methods of protection**

## // REPORTS

### HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

### Modern Asian APT groups' tactics, techniques and procedures (TTPs)

### A cascade of compromise: unveiling Lazarus' new campaign

### How to catch a wild triangle



## // SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

### Threats

### Categories

Archive

Webinars

Statistics

Threats descriptions

All tags

APT Logbook

Encyclopedia

KSB 2023

© 2024 AO Kaspersky Lab. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

[Privacy Policy](#)   [License Agreement](#)   [Cookies](#)