THREAT INTEL

Threat Intelligence

2022-11-21 Threat Intel Report

TLP: CLEAR

November 2022

updated: 11/21/22

Table of Contents

This threat intelligence report has been prepared thanks to proprietary honeypot and OSINT data. The Malwarebytes threat intelligence team collects raw emails from several private and public sources and ingests them to generate metadata and track associated campaigns.

IT security practitioners, threat intel and malware analysts will find information about the threat landscape for the previous week. The categories covered include:

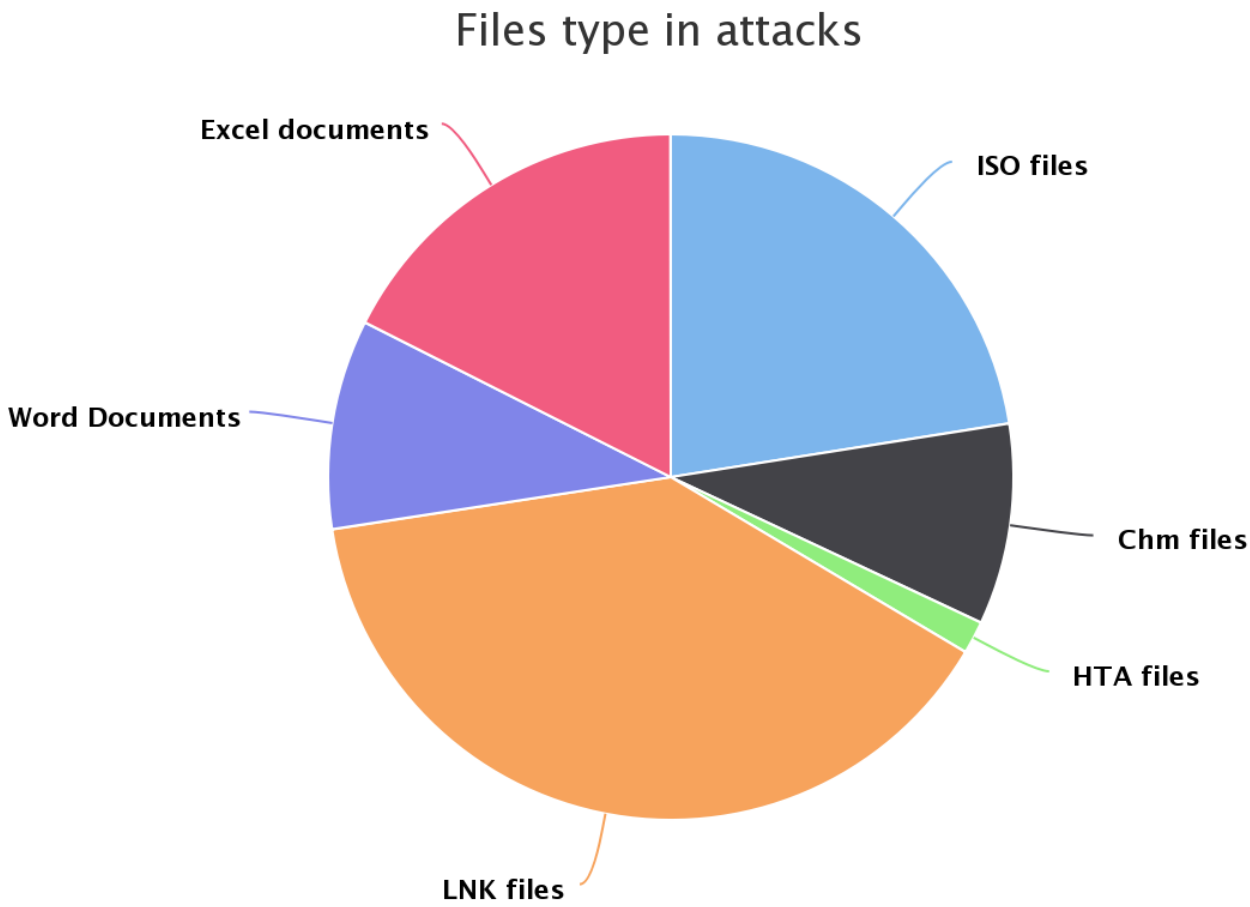
- Malspam
- Web
- Ransomware
- APTs
- Zero-days

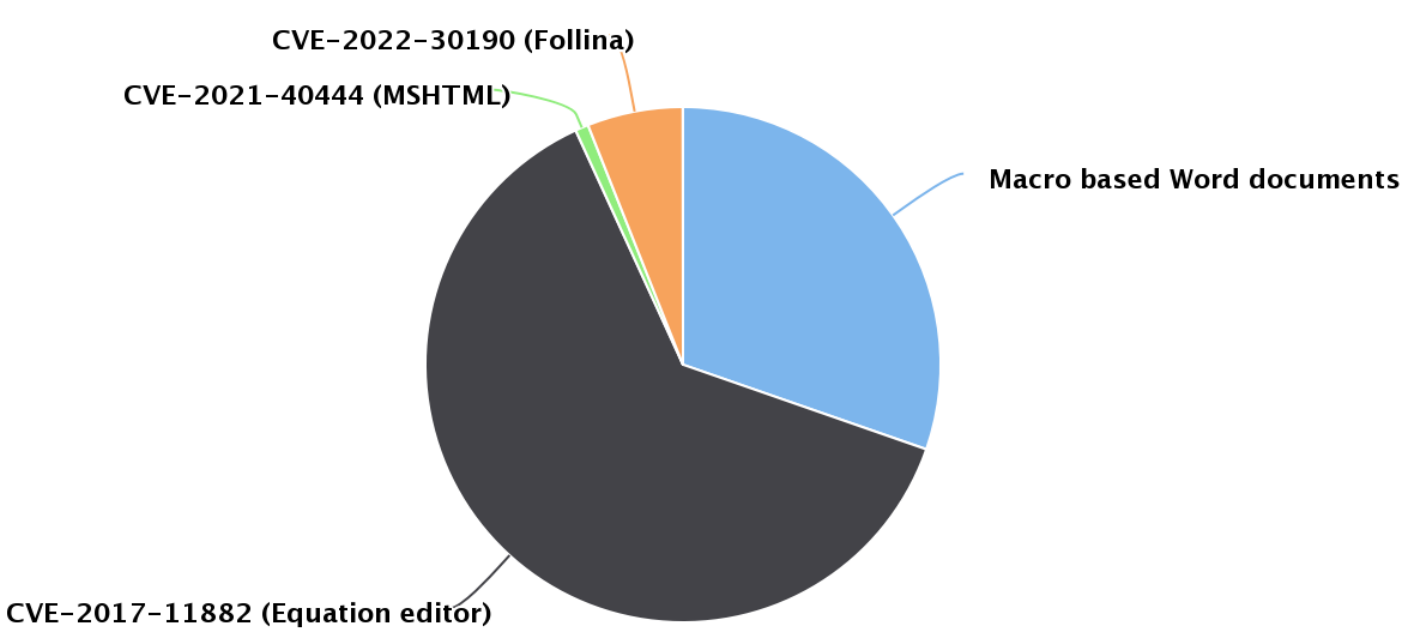
Each attack tracked and observed by our threat intelligence team is checked against Malwarebytes products to ensure our customers are continually protected.

If you would like to provide any feedback, you are welcome to email us at **intel@malwarebytes.com** . You can follow our team on Twitter **@MBThreatIntel** .

The information shared within this report is about malicious activity and should be treated as such. Our Indicators of Compromise (IOCs) have been defanged to prevent accidental clicks.

Malspam threats

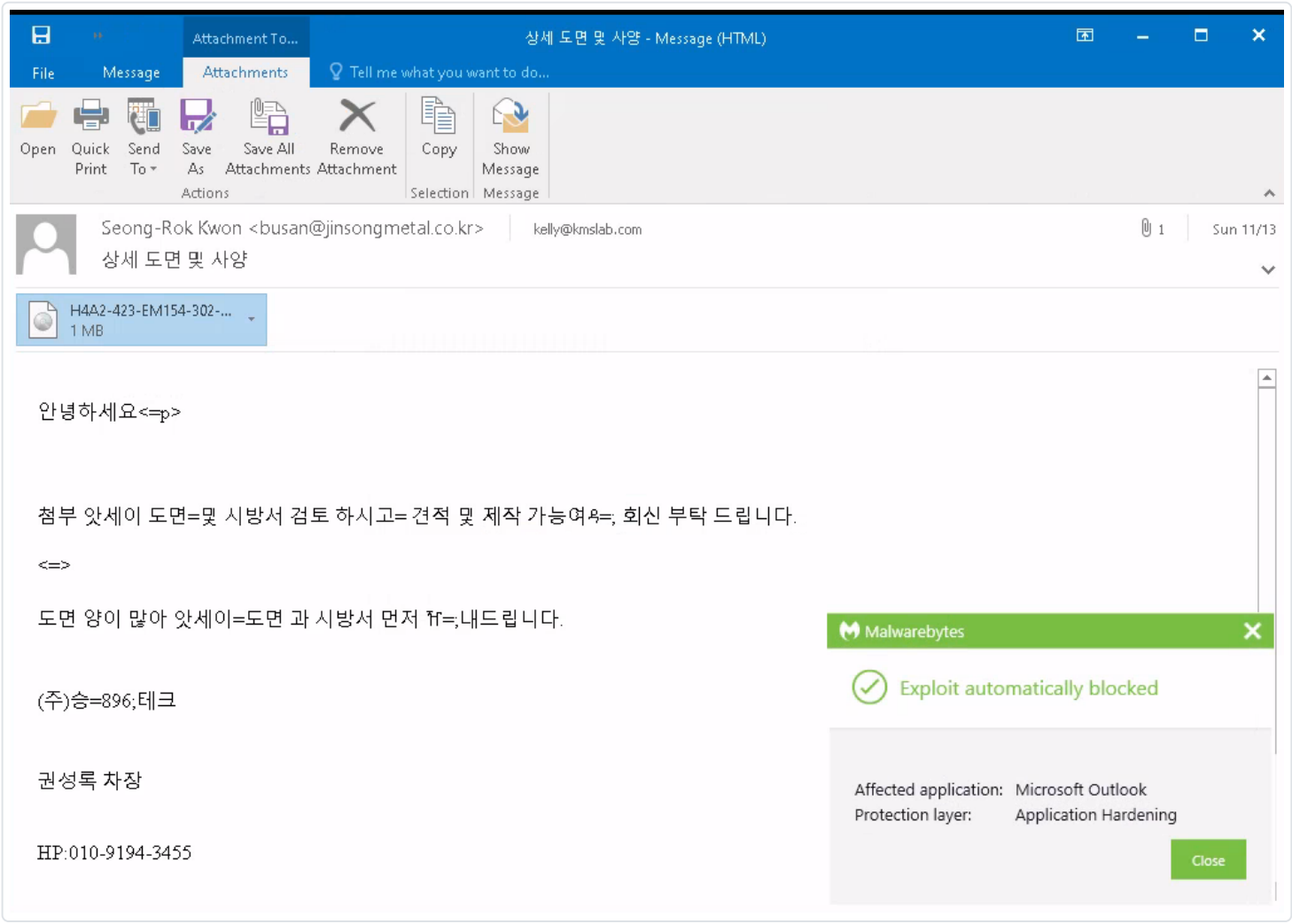




Note: Threat name descriptions are pulled from Malpedia .

Formbook

FormBook is a well-known commercial malware that steals information from victims' machines using keyloggers and form grabbers.



Email subject(s):

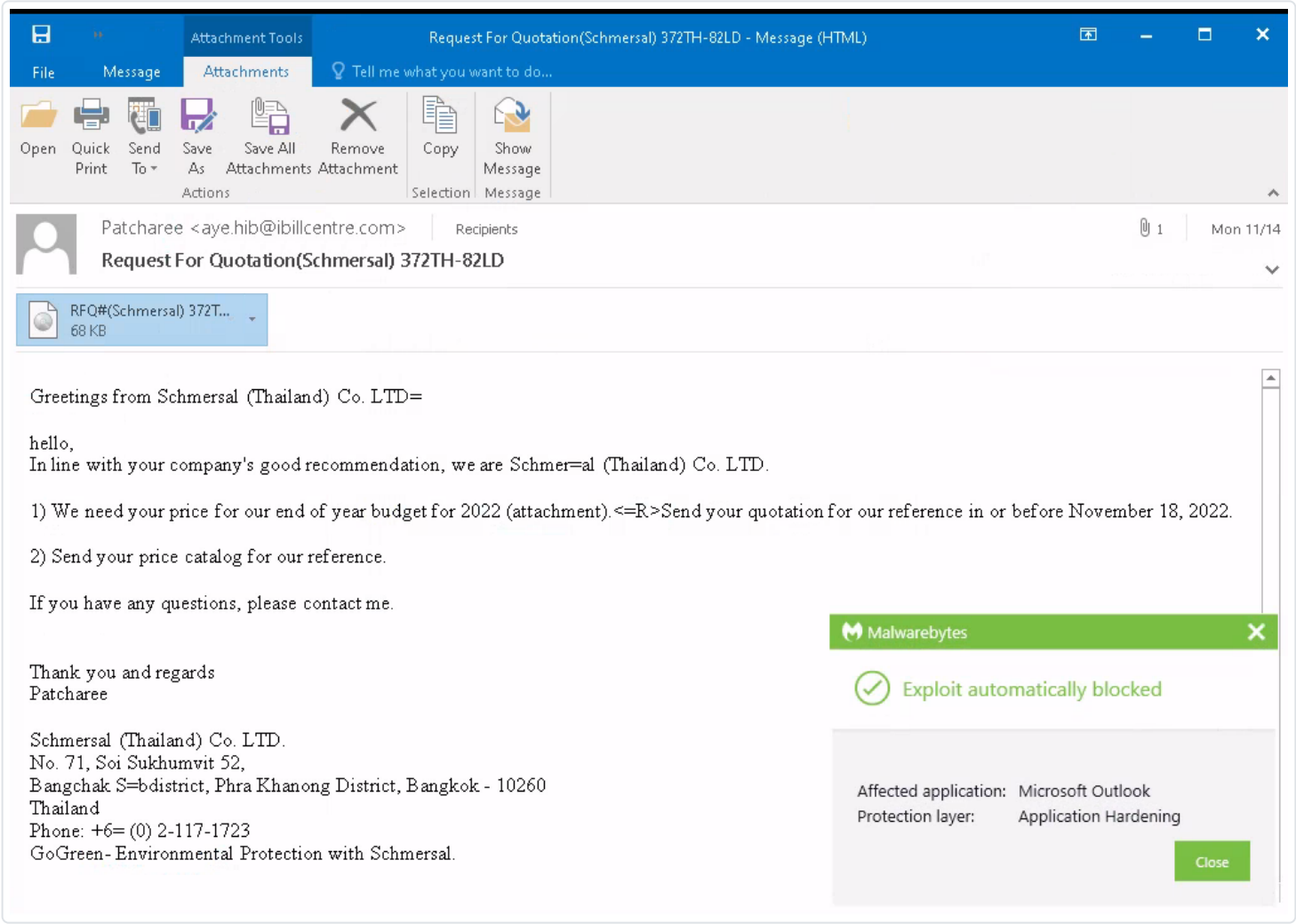
-
- Quotation Request

Attachment name(s):

- H4A2-423-EM154-302-20221114 JPG.ISO
- Quotation.xls

Remcos

Remcos (acronym of Remote Control & Surveillance Software) is a Remote Access Software used to remotely control computers. Once installed, opens a backdoor on the computer, granting full access to the remote user.



Email subject(s):

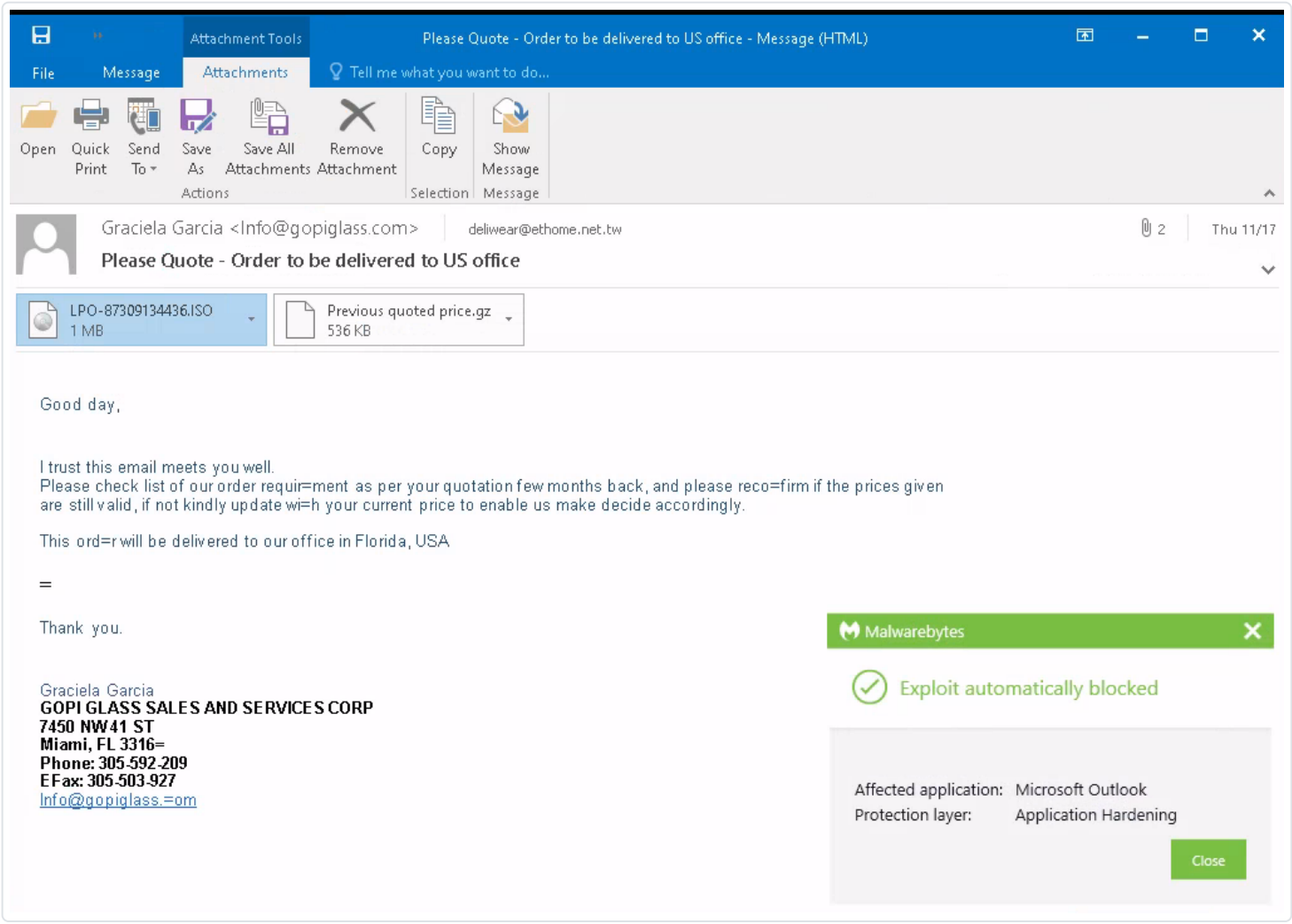
- Request For Quotation(Schmersal) 372TH-82LD
- Fwd: M/T BUENA LUNA - INQUIRY

Attachment name(s):

- RFQ#(Schmersal) 372TH-82LD.iso
- BUL_Requisition.img

Agent Tesla

A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.



Email subject(s):

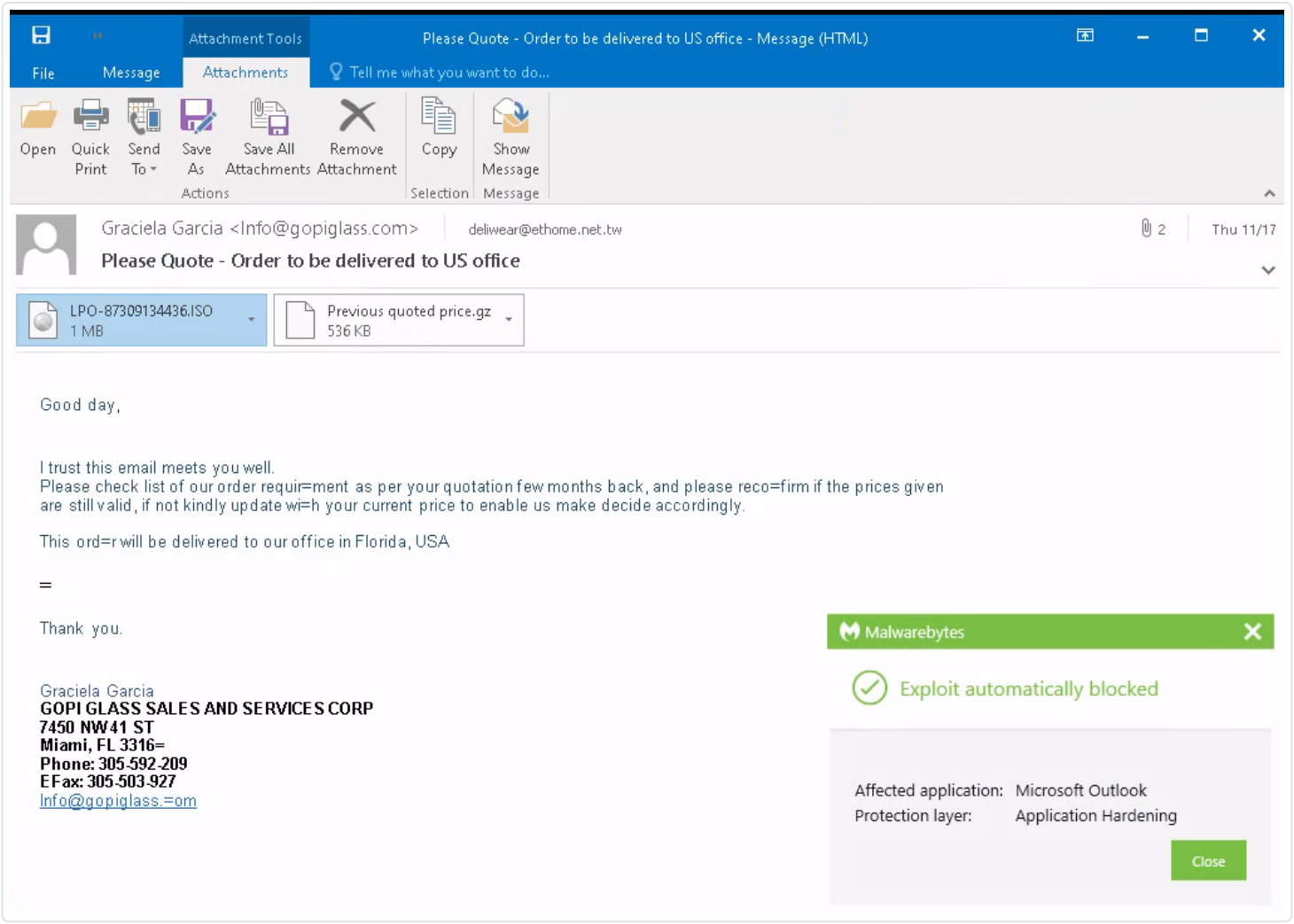
-
- Quotation Request
- Please Quote - Order to be delivered to US office
- DHL Shipping Document

Attachment name(s):

- H4A2-423-EM154-302-20221114 JPG.ISO
- Quotation.xls
- LPO-87309134436.ISO
- waybill number #8318869311.doc

Snake Keylogger

Snake is a common info stealer primarily delivered via malicious documents attached to spam emails. In addition to logging keystrokes, it can also record the contents of the clipboard and capture screenshots. It has the capability to exfiltrate the collected data via email, FTP, SMTP, Pastebin, and the messaging app Telegram.



Email subject(s):

- RFQ D78GHK
- NEW INQUIRY
- ORDER

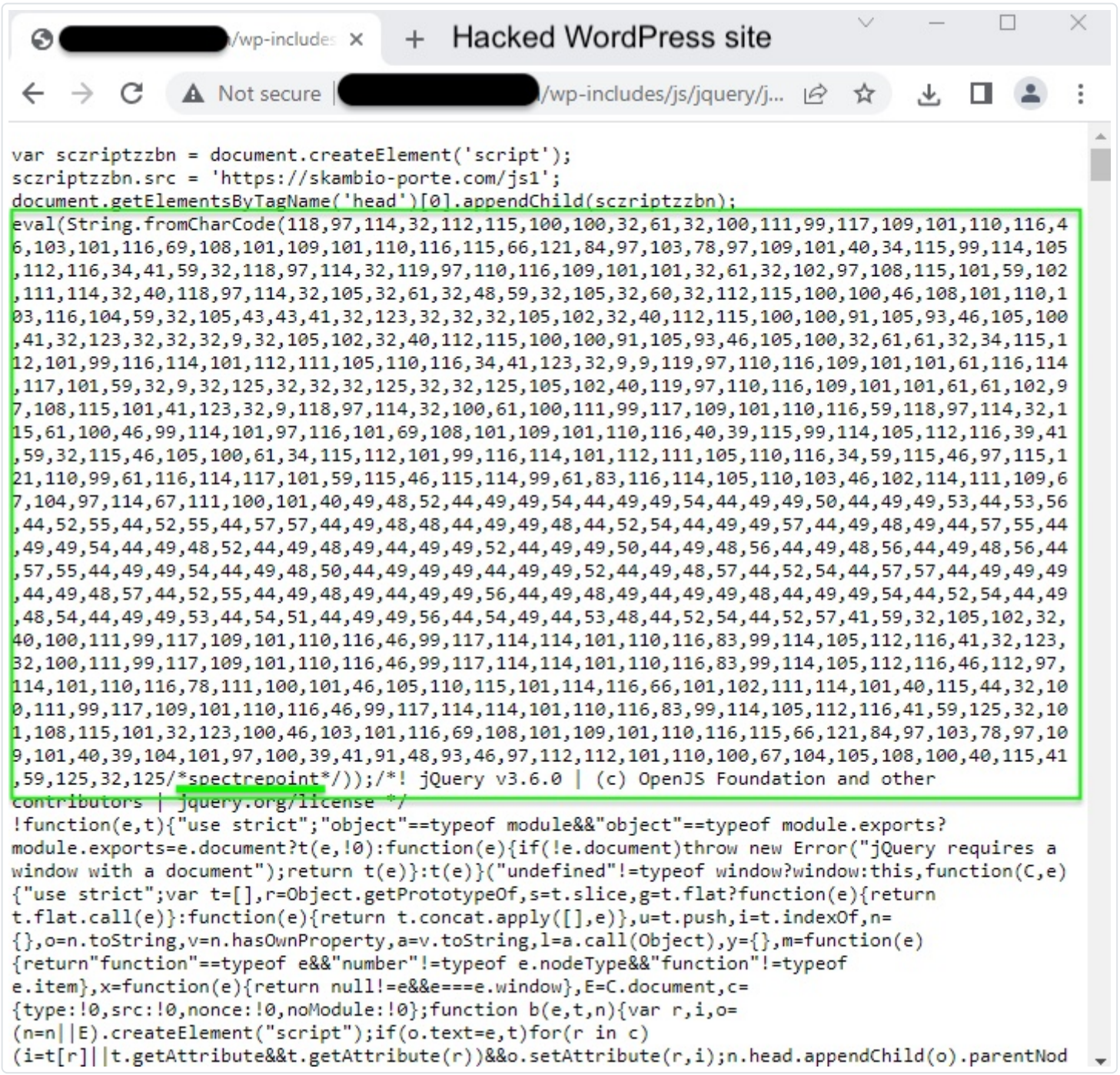
Attachment name(s):

- D112SRL.doc
- NEW INQUIRY.doc
- RFQ.doc

Web threats

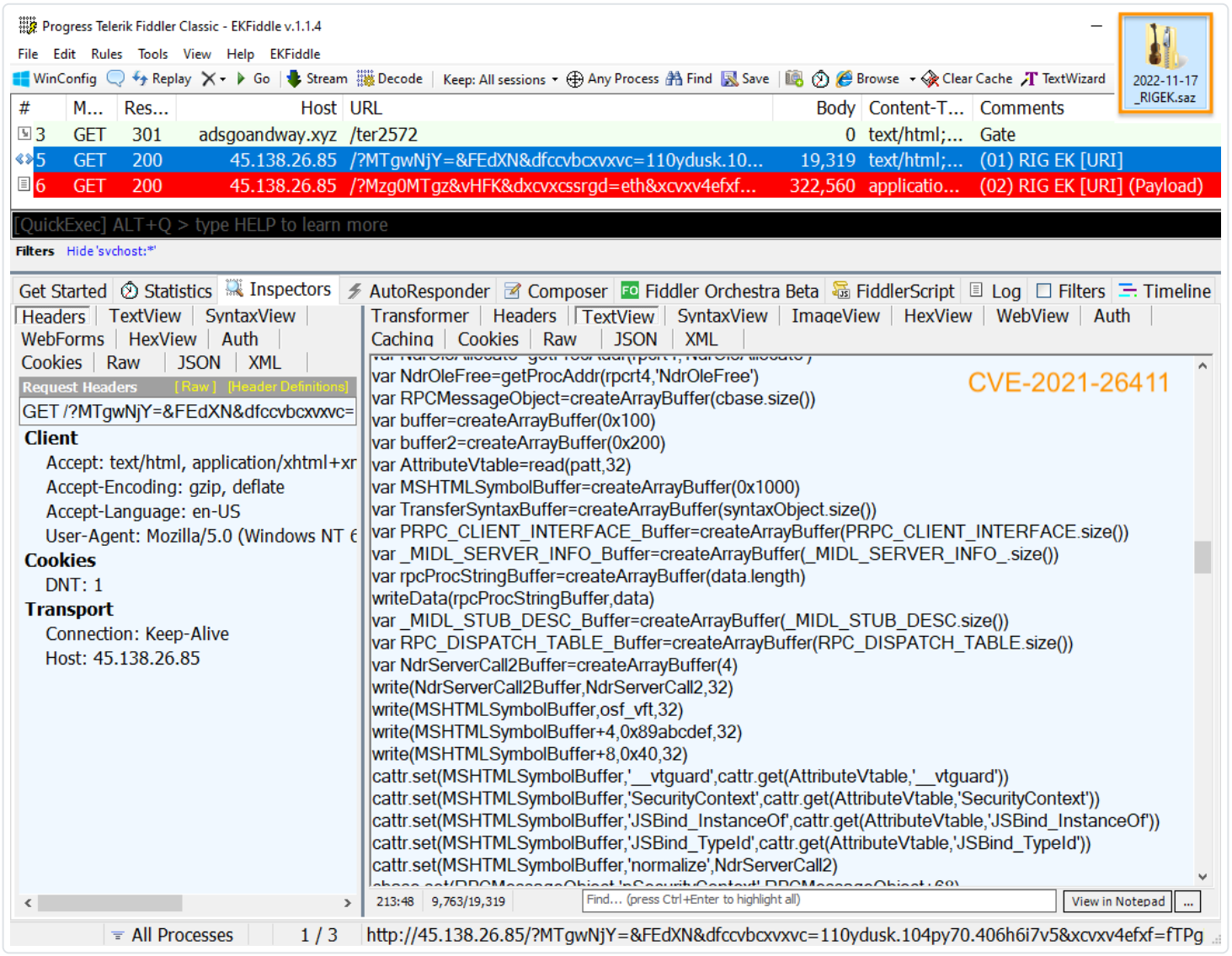
Spectrepoint campaign

The ' **spectrepoint** ' malware is part of an **old WordPress injection campaign** . Its goal is to redirect traffic from legitimate but compromised sites to a number of scams including browser push notifications.



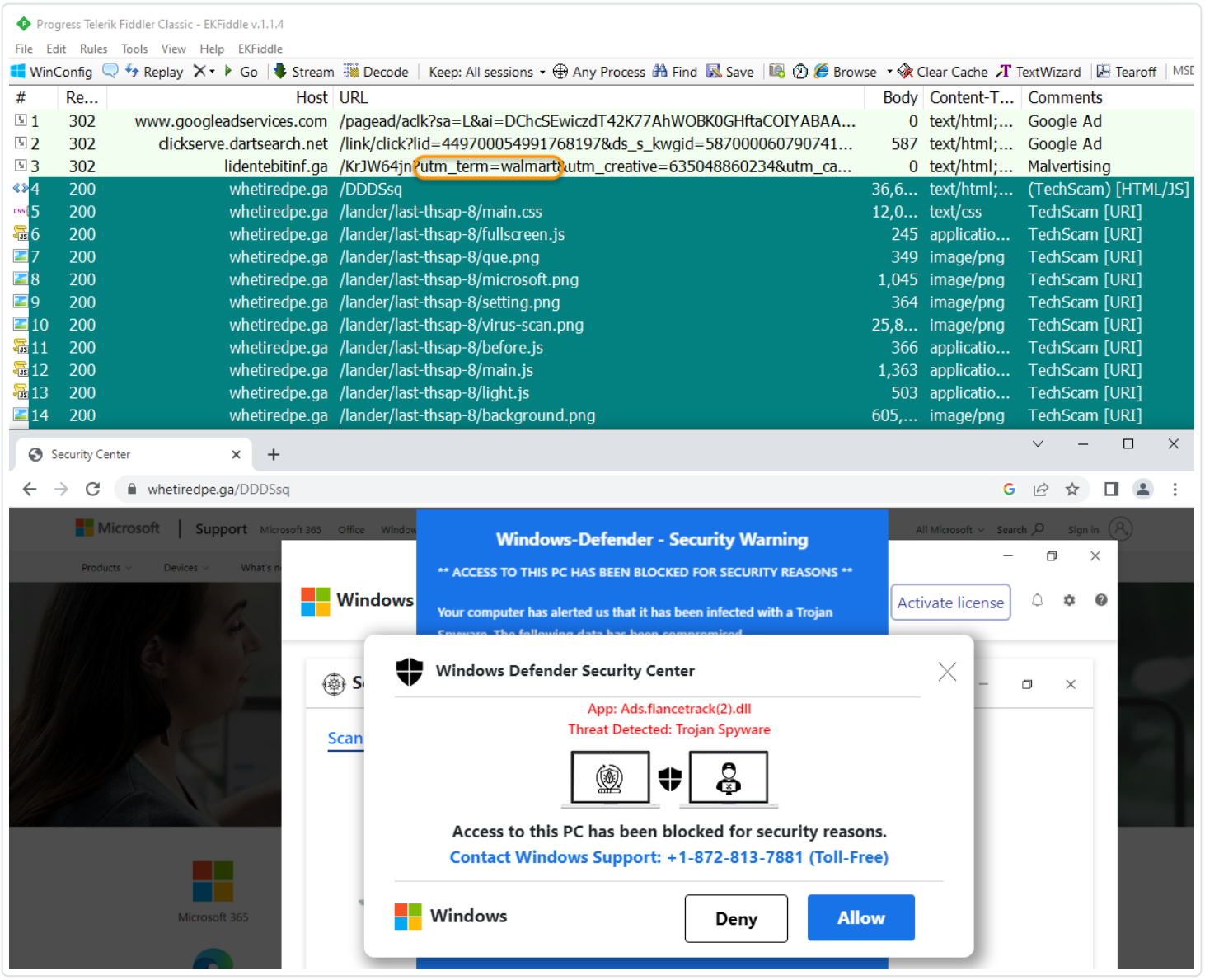
RIGEK

The RIG exploit continues to be used in very limited malvertising campaign. Here, we got it dropping Redline Stealer.



Google Ads malvertising

We saw a malvertising campaign abusing Google ads for popular keyword searches such as 'walmart'. The fraudsters are redirecting victims to tech support scam pages.

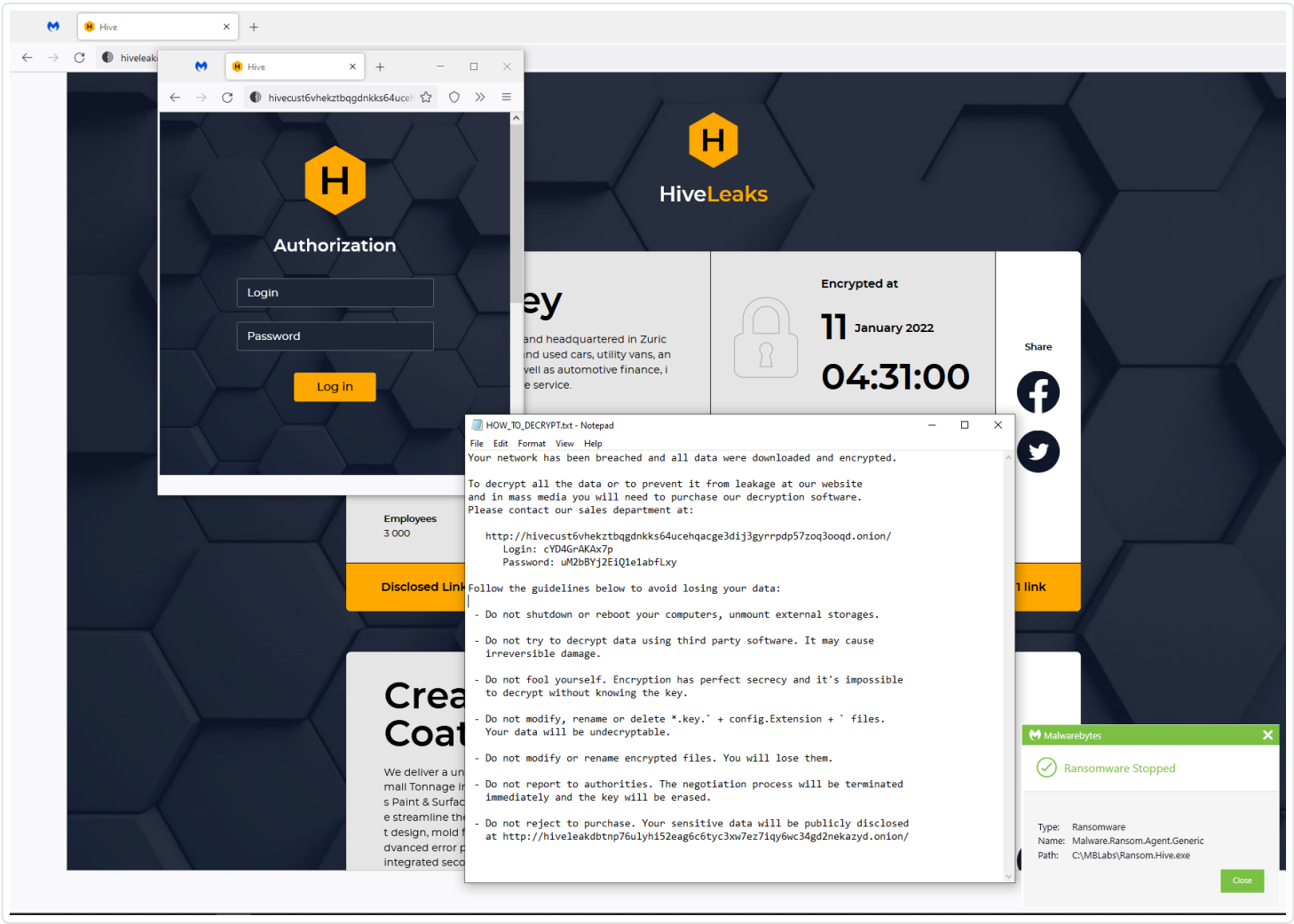


Ransomware

Hive

Hive ransomware follows the ransomware-as-a-service (RaaS) model in which developers create, maintain, and update the malware, and affiliates conduct the ransomware attacks. From June 2021 through at least November 2022, threat actors have used Hive ransomware to target a wide range of businesses and critical infrastructure sectors, including Government Facilities, Communications, Critical Manufacturing, Information Technology, and especially Healthcare and Public Health (HPH).

As of November 2022, Hive ransomware actors have victimized over 1,300 companies worldwide, receiving approximately US$100 million in ransom payments, according to **FBI information** .



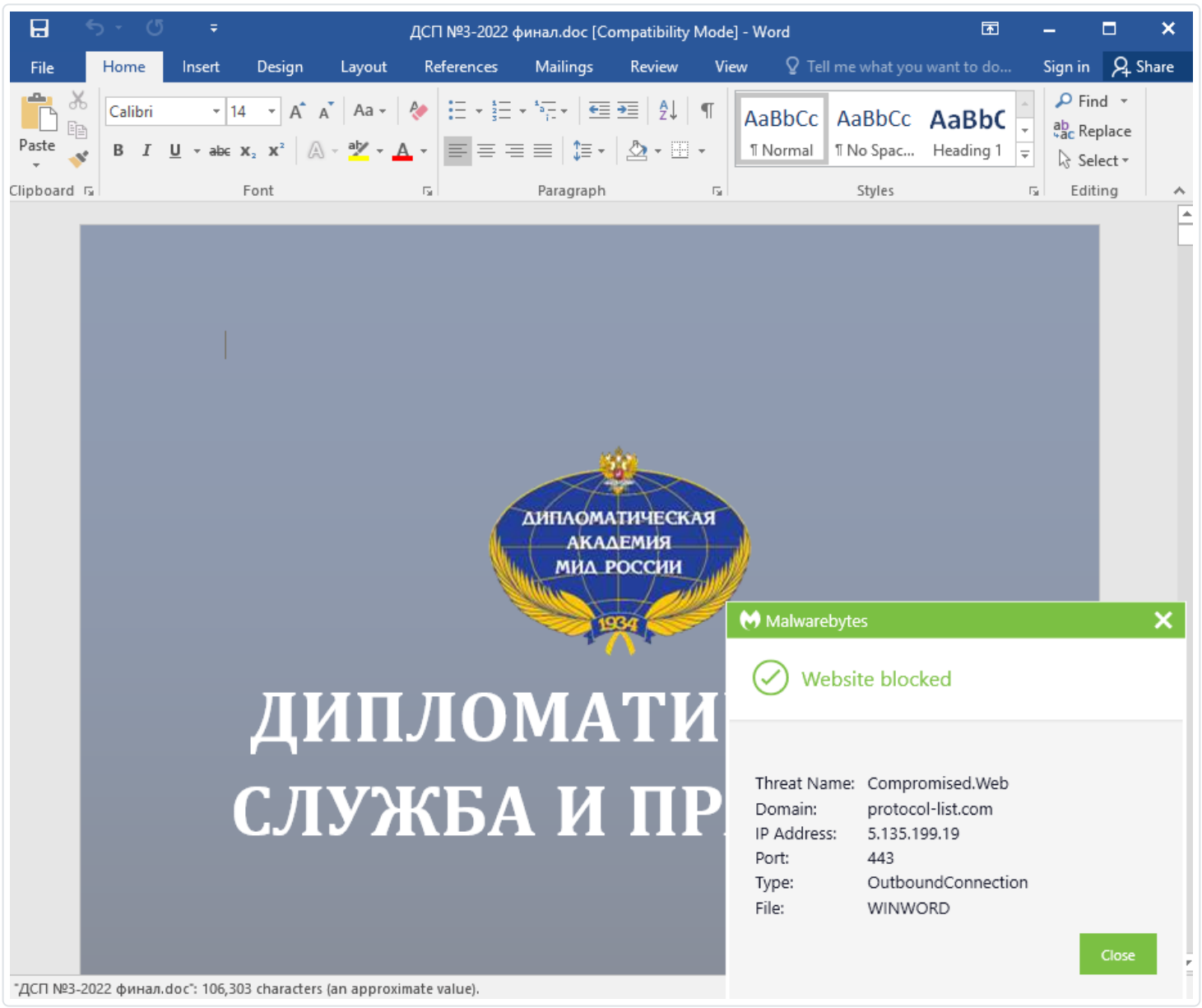
Hive actors have also gained initial access to victim networks by distributing phishing emails with malicious attachments and by exploiting the following vulnerabilities against Microsoft Exchange servers:

- **CVE-2021-31207** - Microsoft Exchange Server Security Feature Bypass Vulnerability
- **CVE-2021-34473** - Microsoft Exchange Server Remote Code Execution Vulnerability
- **CVE-2021-34523** - Microsoft Exchange Server Privilege Escalation Vulnerability

APTs

CloudAtlas

Our research Hossein Jazi identified an email and documents that may be related to the CloudAtlas APT targeting Russia. The document named ДСП №3-2022 финал.doc downloads a remote template which attempts to exploit the Microsoft Equation Editor vulnerability.



References

1. https://www.malwarebytes.com/blog/threat-intelligence/2022/11/spectrepoint
2. https://blog.sucuri.net/2017/09/old-themes-abandoned-scripts-pitfalls-cleaning-serialized-data.html
3. https://twitter.com/h2jazi/status/1592158351475240962

Indicators of Compromise (IOCs)

Indicator	Type	Description
208[.]67[.]105[.]179	IP	AgentTesla
obologs[.]work[.]gd	Domain	Remcos
community[.]backpacktrader[.]com	Domain	SocGholish-DS
rate[.]coinangel[.]online	Domain	None
assetsclick[.]com	Domain	Magecart
founder[.]carflower[.]pics	Domain	SocGholish-DS
54[.]31[.]50[.]94	IP	Formbook
207[.]244[.]245[.]189	IP	Formbook
192[.]64[.]116[.]149	IP	Formbook
103[.]91[.]8[.]90	IP	Formbook
50[.]31[.]188[.]71	IP	Formbook
aceadora[.]shop	Domain	Formbook
bandmarket[.]live	Domain	Formbook
carlyle55[.]com	Domain	Formbook
t1fbrc[.]com	Domain	Formbook
pinturaalhorno[.]com	Domain	Formbook
7e72ff51060dd585714ecc9ca539d13aae29d97f037d3586995a0068f7a8f4b3	SHA256 Hash	Formbook

Indicator	Type	Description
d58435f674ace7aef5c2f22a53d64892c4a65d38370615505dbb4e496a4d68e6	SHA256 Hash	Remcos
a41dfb5ce97b44a76609417808670b569e2d9a6aeba5d3fa13c49872134424de	SHA256 Hash	Remcos
194[.]55[.]186[.]82	IP	Remcos
212604b13ca215693db01f642c18e800aeb394f53d1f559b939b39fae9708d87	SHA256 Hash	Formbook
103[.]145[.]253[.]70	IP	Formbook
b8d1741d826709951f5f4500548053319997c7da5703fb6172b1ab3146ad84ea	SHA256 Hash	Formbook
193[.]47[.]61[.]170	IP	Remcos
brremcoz1[.]ddns[.]net	Domain	Remcos
f4856be3e8adf500b82f1ee5605521796b4ff8aef1e54235378239f7a7a39493	SHA256 Hash	Remcos
775922a73a2385cf43b9707a1ef3e35665a07713b1245900860f586687dfa752	SHA256 Hash	Remcos
ec69450ffb674fb751914a0336e7c68d7f21b62f94f452c5dc6e8aed0cb265f9	SHA256 Hash	AgentTesla
68[.]65[.]122[.]214	IP	AgentTesla
104[.]168[.]45[.]102	IP	AgentTesla

Indicator	Type	Description
host39[.]registrar-servers[.]com	Domain	AgentTesla
aaf20b9370f24df82c97b0273f52e6bd40f90df8fb8911bb10a70d57a77e775e	SHA256 Hash	AgentTesla
192[.]168[.]100[.]2	IP	AgentTesla
904e50e24012be4d9046305f4f745df1375753d87bb70726017dbd2a3d5874bd	SHA256 Hash	AgentTesla
b7815624a43bf6975106243171dac5a1d632deec30ea12a5ad30ec5cb780b5a9	SHA256 Hash	AgentTesla
8e48f49e936e2d55130911c24ce3ac4577b8e7235be829c0df51084a3be11a1e	SHA256 Hash	AgentTesla
6580a9592020f97cfcb114a99b3ada9bb7e4320af463226c1de4a30628be1736	SHA256 Hash	AgentTesla
edb1d5994dd210d662eeaf3ecc611f3b6a3804b67e337731485793b327932161	SHA256 Hash	AgentTesla
121b89503cd42346a4cd62a7b55662edf52ec1cf39544ea8d55b583de4ee09af	SHA256 Hash	SnakeKeylogger
91[.]235[.]128[.]141	IP	SnakeKeylogger
fe0acab9e7af19546f5b9092a35045fab873846ea0d53083e07f7a563dad7f01	SHA256 Hash	SnakeKeylogger

Indicator	Type	Description
cp5ua[.]hyperhost[.]ua	Domain	SnakeKeylogger
f750ed5a3a35107886675b34757848dd7092b4cbc77453b39e342eac5a71d251	SHA256 Hash	SnakeKeylogger
8cff398b16e8e2a230d61b4a8a3a9bff3180c52d42917808bde8dc3cc13baa33	SHA256 Hash	SnakeKeylogger
d313021c2d82399a673f8aee4debe06a81254e56a2225ba7e8ceda85d6d950bb	SHA256 Hash	None
i-io[.]io	Domain	Malvertising
weatherplllatform[.]com	Domain	None
lidentebitinf[.]ga	Domain	Malvertising
koffie[.]life	Domain	Malvertising
furns[.]shop	Domain	Malvertising
friscomusicgroup[.]com	Domain	Malvertising