



THREAT INTEL

Threat Intelligence

2022-11-14 Threat Intel Report

TLP: CLEAR

Table of Contents

● Malspam threats	4
● Formbook	6
● Agent Tesla	7
● Emotet	8
● Remcos	9
● Web threats	10
● Magecart	10
● FakeUpdates/SocGholish	11
● Spammy Q&A redirects	12
● Ransomware	13
● Magniber	13
● Black Basta	14
● Royal ransomware	15
● Indicators of Compromise (IOCs)	16

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:

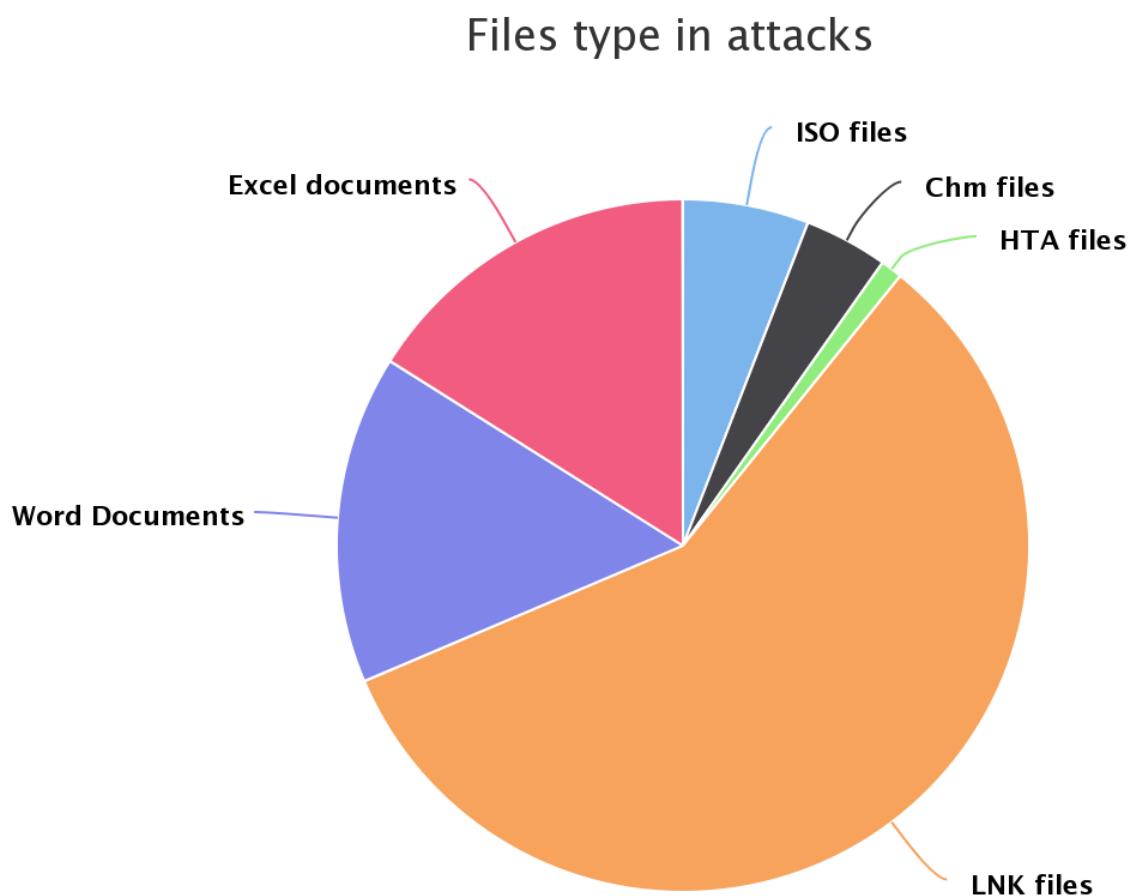
- Malspam
- Web
- Ransomware
- APTs
- Zero-days

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

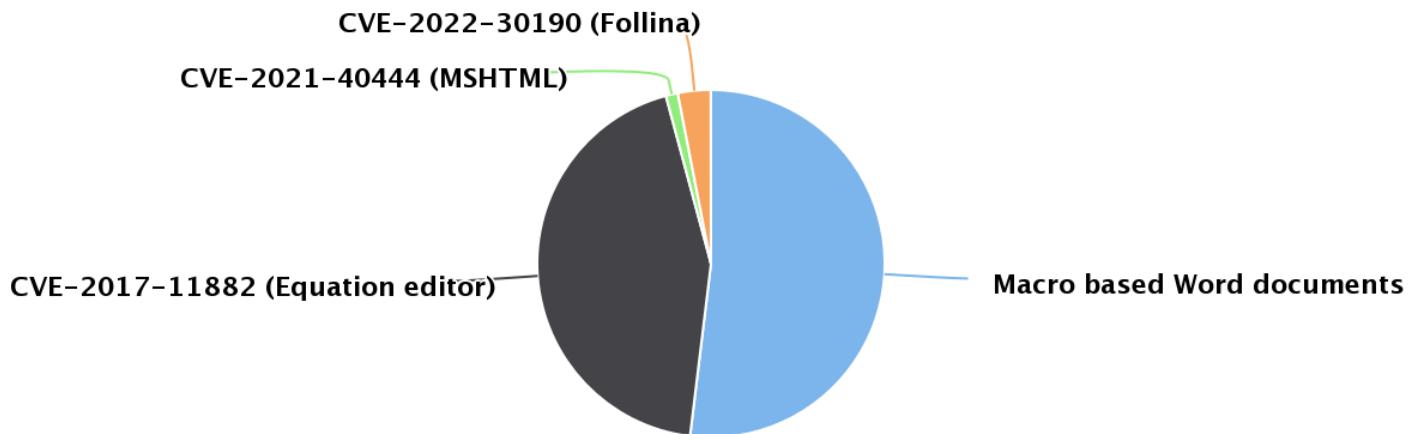
If you would like to provide any feedback, you are welcome to email us at intel@malwarebytes.com. You can follow our team on Twitter [@MBThreatIntel](#).

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



Microsoft Office attacks



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.

RE: Request for Quote - Message (HTML)

File Message Attachments Tell me what you want to do...

Open Quick Print Send To... Save As... Save All Remove Attachments Copy Selection Show Message Attachment Message

Actions

uwe.bienlein@globalcontact.de aamir@mcrmail.com

RE: Request for Quote

Global Contact GmbH.pdf... 706 KB

Dear aamir
FYI,
Please confirm delivery dates and payment terms.
A new customer needs quote urgently

Best regards
Uwe Bienlein
GLOBAL CONTACT GMBH
Alte Ludwigsstädter Straße 16
D-96317 Kronach
Handelsregister Coburg
Registernummer: HRB 2665
Ust-ID: DE 812 168 262

Tel. +49 9261-50450-14 (Bienlein)
Tel. +49 9261-50450-0 (Zentrale)

Malwarebytes

Malware automatically quarantined

Type: Malware
Name: Spyware.FormBook
Path: C:\Users\Use...\Global Contact GmbH-pdf-.exe

Close

Email subject(s):

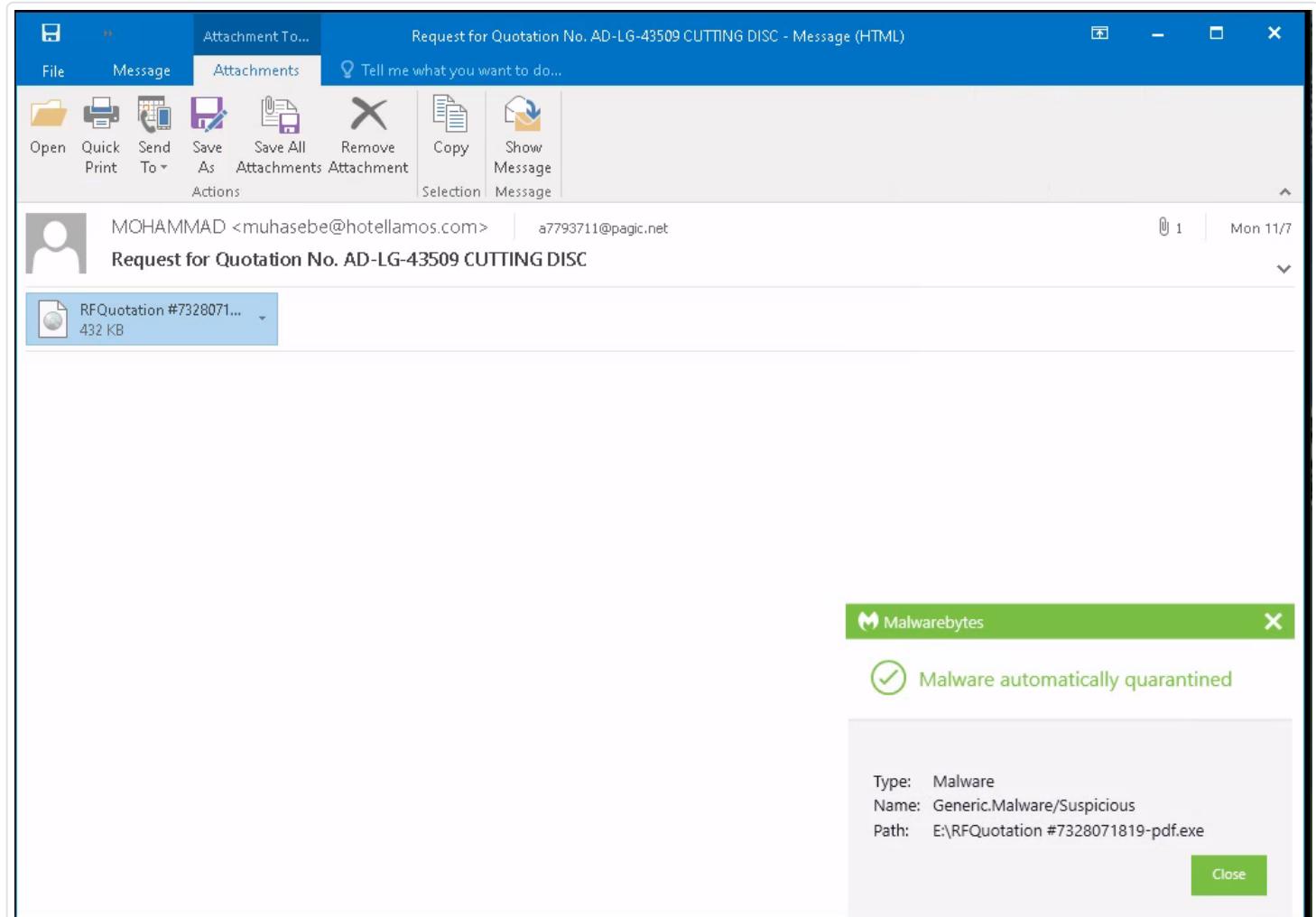
- RE: Request for Quote

Attachment name(s):

- Global Contact GmbH-pdf-.iso

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):

- FedEx Express AWB#5305323204643 - Information is required
- RE: Request for Quote
- COTIZACION ARTICULOS DE OFICINA PARA PRODUCCION.
- Pago de saldo/copias TT
- FB-108N & FB-108NK 詢價 - 田勤

Attachment name(s):

- shipping documents.iso
- Global Contact GmbH-pdf-.iso
- ##COTIZACION ARTICULOS DE OFICINA PARA PRODUCCION.xlsx
- Balance Payment.img
- FB-108N & FB-108NK - .IMG

Emotet

While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attack.

The screenshot shows an Outlook inbox with a single spam email from 'Basketinfo <tasaki@chu-ou.co.jp>'. The subject of the email is '[SPAM] MIME-Version: 1.0'. Below the message, there is an attachment named 'ACH Payment Advice.xls' (255 KB). An Excel window is open, showing the file 'ACH Payment Advice.xls [Compatibility Mode] - Excel'. The Microsoft Malwarebytes add-in is active, displaying a green banner with 'Website blocked' and a detailed threat report:

Threat Name:	Trojan.Web
Domain:	laboritmtest2022.scienceontheweb.net
IP Address:	185.176.43.106
Port:	80
Type:	OutboundConnection
File:	EXCEL

Email subject(s):

- [SPAM] MIME-Version: 1.0
- Fwd:
- Re: Csomagja_kézbesítésre_vár_!

Attachment name(s):

- ACH Payment Advice.xls
- Payment Status.xls
- Report - 2022-11-07_1313.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.

Request For Quotation - Message (HTML)

Patcharee <aye.hib@ibillcentre.com>

Request For Quotation

SKM-2639462946DF.iso
88 KB

Greetings from Schmersal (Thailand) Co. LTD=

hello,
In line with your company's good recommendation, we are Schmer=al (Thailand) Co. LTD.

- 1) We need your price for our end of year budget for 2022 (attachment).<=R>Send your quotation for our reference in or before November 18, 2022.
- 2) Send your price catalog for our reference.

If you have any questions, please contact me.

Thank you and regards
Patcharee

Schmersal (Thailand) Co. LTD.
No. 71, Soi Sukhumvit 52,
Bangchak S=district, Phra Khanong District, Bangkok - 10260
Thailand
Phone: +6= (0) 2-117-1723
GoGreen- Environmental Protection with Schmersal.

Malwarebytes

Malware automatically quarantined

Type: Malware
Name: Trojan.MalPack
Path: C:\Users\User\Down...\\SKM-2639462946DF.exe

Close

Email subject(s):

- Request For Quotation

Attachment name(s):

- SKM-2639462946DF.iso

144[.]76[.]136[.]153

Web threats

Magecart

We discovered a new Magecart-related domain hosted as brontop[.]net

Payment method

PayPal(Accept all Major Credit and Debit cards) 

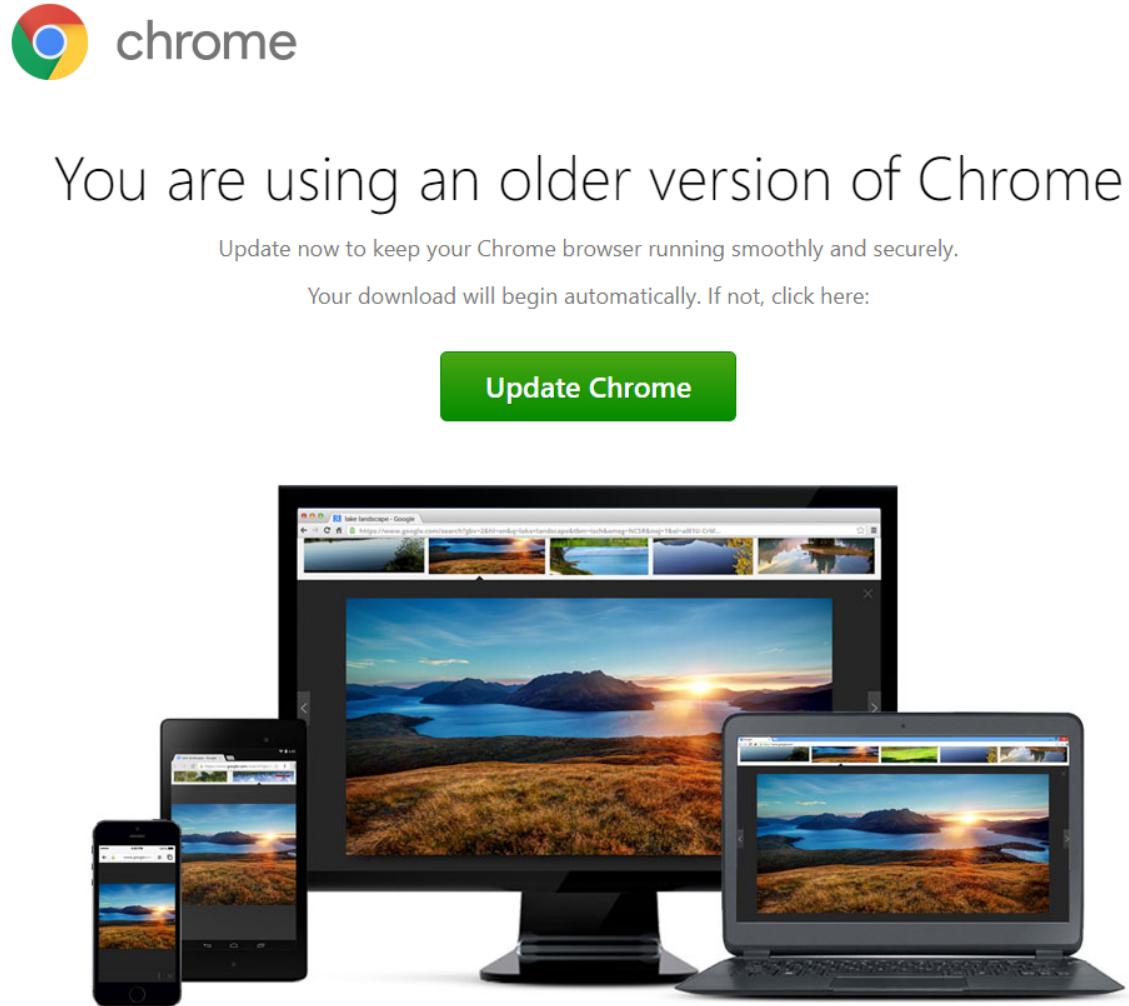
 **PayPal** Pay in 4 interest-free payments of \$43.25. [Learn more](#)

 Debit or Credit Card

Powered by **PayPal**

FakeUpdates/SocGholish

We saw new infrastructure for domain shadowing (course[.]netpickstrading[.]com) and C2 server (campaign[.]tworiversboat[.]com).



Spammy Q&A redirects

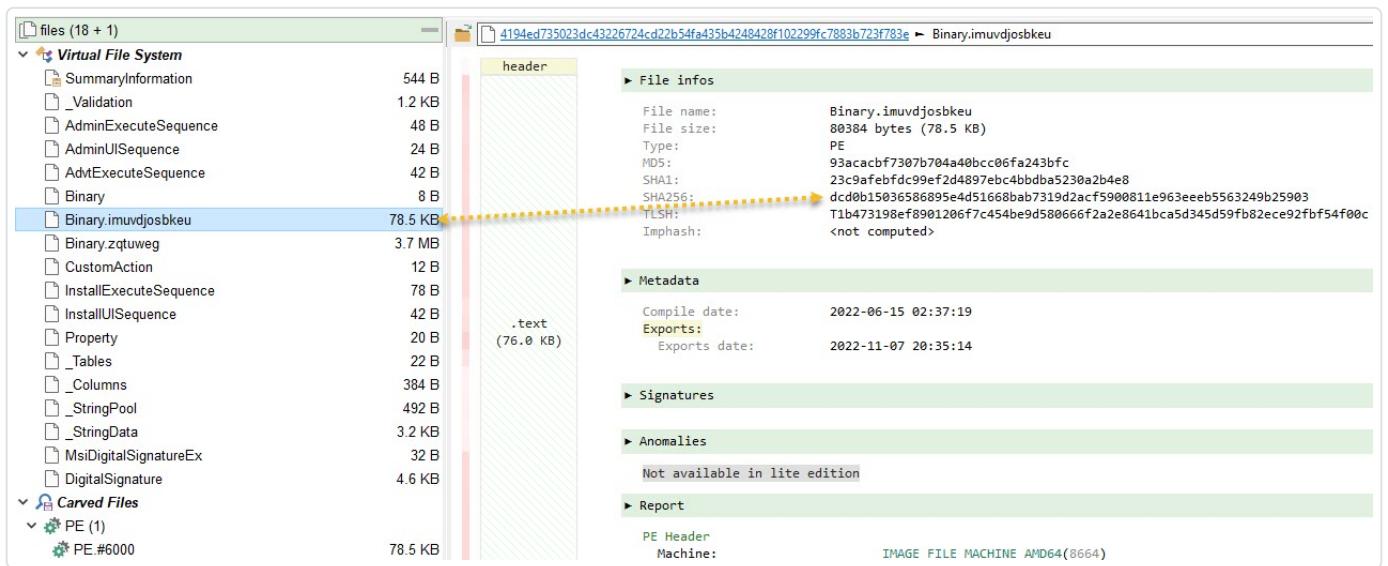
The folks at Sucuri published a [blog](#) about a large redirection campaign from compromised sites to various spammy Q&A pages. According to them, over 15 thousand websites have been hacked and redirecting users between September and October.

The screenshot shows a web browser window with the URL questions.firstgoool.com/4987/how-do-i-make-money-from-cryptocurrency-trading?show=4988. The page title is "How do I make money from cryptocurrency trading?". The main content area features a dark background with a colorful, abstract graphic of lines and dots. To the right of the graphic, there is an advertisement for "Find Funnel Software" with a "Open" button. Below the graphic, there is a logo for "fast" and the text "Fast Search Online". At the bottom of the page, there is a voting section with a "0" and an upvote arrow, and a timestamp "asked 6 days ago in question by mrcat (2.7k points)". The top navigation bar includes links for "Firstgoool Q&A", "Questions", "Unanswered", "Tags", "Users", and "Ask a Question". A search bar is located in the top right corner. A sidebar on the right side of the page says "Welcome to Firstgoool Q&A, where you can ask questions and receive answers from other members of the community."

Ransomware

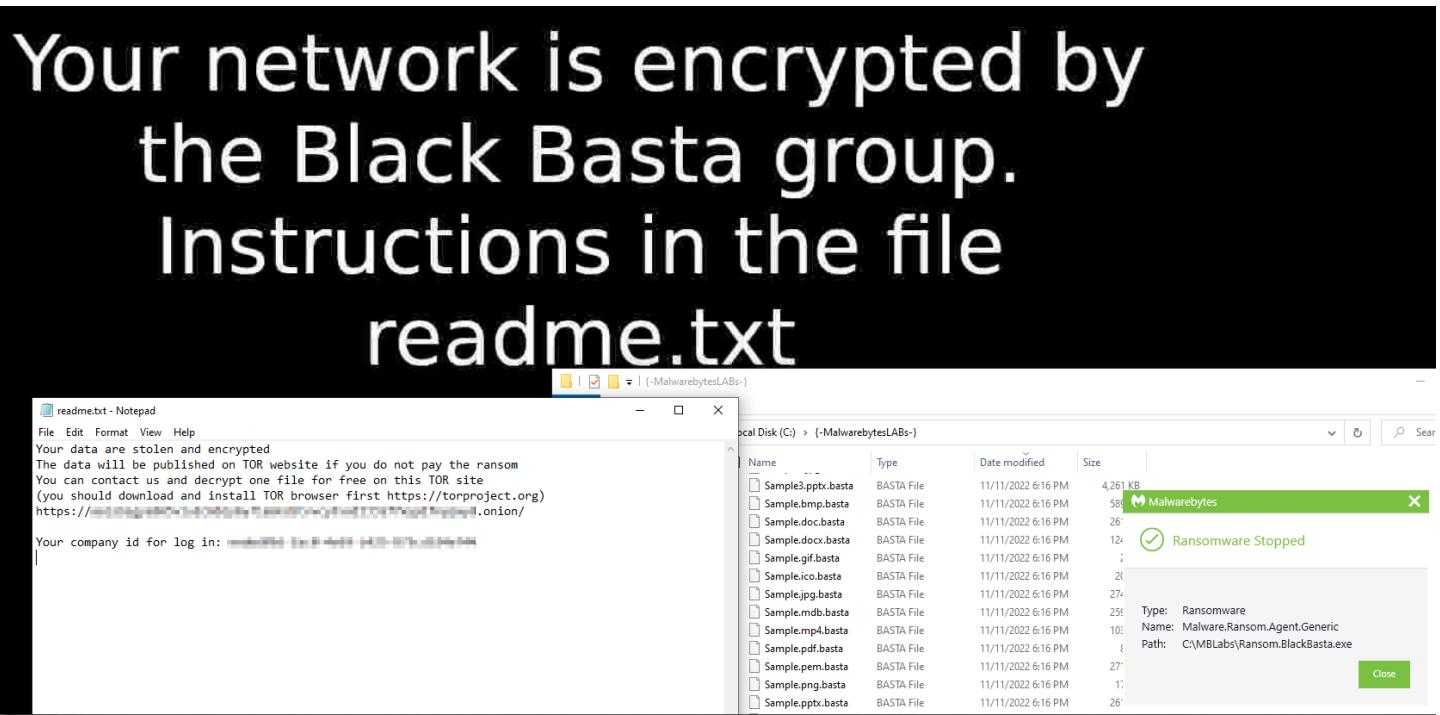
Magniber

1. ZIP: af8ebdec2fd2d20d91a02ead72a4292fef36a271fe33510efa0e6aaca5f0ebcd
2. MSI: 4194ed735023dc43226724cd22b54fa435b4248428f102299fc7883b723f783e
3. DLL: dcd0b15036586895e4d51668bab7319d2acf5900811e963eeeb5563249b25903



Black Basta

- Extension .basta
- Ransom note: readme.txt



Royal ransomware

- Extension: .royal
- Ransom note: README.TXT

Screenshot of a web browser showing a contact form for "Royal". The URL is "royal4[REDACTED].onion".

Contact from

Email: [REDACTED]

Message: [REDACTED]

Submit

Zender

8 November 2022

Website: [Link](#) **Revenue**: \$5M

Employees: 4

[Link #1](#)

Silverstone

8 November 2022

Website: [Link](#) **Revenue**: \$57M

Employees: 89

The end of the Second World War had left Britain with no racing circuits. On 2 October 1948, the Royal Automobile Club hosted the first race at Silverstone, a former RAF base. An estimated 100,000 people attended. Sir Stirling Moss was the first driver to set a lap record, driving his Maserati marked by bales, ropes and canvas.

Silverstone racing history had begun.

Malwarebytes

Ransomware Stopped

Type: Ransomware
Name: Malware.Ransom.Agent.Generic
Path: C:\MBLabs\Ransom.Royal.exe

Close

Indicators of Compromise (IOCs)

Indicator	Type	Description
182[.]162[.]143[.]56	IP	Emotet
course[.]netpickstrading[.]com	Domain	SocGholish-DS
brontop[.]net	Domain	Magecart
fa554d4efb21948bc84493 ac1a170406c4106e2e90f1b 14e96f2064c3c1b7199	SHA256 Hash	Formbook
66[.]96[.]160[.]146	IP	Formbook
bridginglegal[.]com	Domain	Formbook
8ced3b47bed5c4a21219e9 857f092343bfd2a66c53c18 489aa0c0ecab733aebf	SHA256 Hash	Formbook
bf850e8ad84f2a75a68064 fd21d0129d3e74ee2a7beaf 22f2401a7f3ab60d4b0	SHA256 Hash	AgentTesla
bytesendesign[.]nl	Domain	Emotet
3b07c87e9306549b470fa6 796c8994bca6ceb8266f63 8772b40482097bfc2ca6	SHA256 Hash	Emotet
blangkonstudio[.]com	Domain	Emotet
careofu[.]com	Domain	Emotet
laboritmtest2022[.]science ontheweb[.]net	Domain	Emotet

Indicator	Type	Description
t2022	MITRE ATT&CK Technique	None
185[.]176[.]43[.]106	IP	Emotet
203[.]161[.]184[.]7	IP	Emotet
185[.]182[.]57[.]100	IP	Emotet
175[.]98[.]167[.]163	IP	Emotet
602de00f00c364c9549d3 13b9e0f941e6073c5320aa 53ed6a8362ee5ceb6a19d	SHA256 Hash	Emotet
85ba4ce2eeee9eca255d6 da5e24c5fe1241966be579d 07f2aee8b9058ec92c0	SHA256 Hash	Emotet
campaign[.]tworiversboat[.]com	Domain	SocGholishC2
ois[.]is	Domain	TDS
en[.]w4ksa[.]com	Domain	SpamContent
peace[.]yomeat[.]com	Domain	SpamContent
qa[.]bb7r[.]com	Domain	SpamContent
en[.]ajeel[.]store	Domain	SpamContent
qa[.]istisharaat[.]com	Domain	SpamContent
en[.]photolovegirl[.]com	Domain	SpamContent
en[.]poxnel[.]com	Domain	SpamContent
qa[.]tadalafilhot[.]com	Domain	SpamContent
questions[.]rawafedpor[.]com	Domain	SpamContent

Indicator	Type	Description
qa[.]elbwaba[.]com	Domain	SpamContent
questions[.]firstgoool[.]co m	Domain	SpamContent
qa[.]cr-halal[.]com	Domain	SpamContent
qa[.]aly2um[.]com	Domain	SpamContent
chabapos[.]com	Domain	TSS
chirpypossum[.]com	Domain	TSS
delphitoken[.]com	Domain	TSS
dicksnearme[.]com	Domain	TSS
grsly[.]org	Domain	TSS
stancel[.]com	Domain	TSS
ca5bd5fdd79251b2fb4e274 ff8cc219b66804d52e21586 3adab66ba3651bce42	SHA256 Hash	Magniber
b41a120d5a4a3ea9c6a663 9fa0cdcaf14b383ec03589 0dc2e714a44a5e50ca9b	SHA256 Hash	Magniber
bc8f6149a6b6423c82dd7f 51aff4756539577eacf27b70 19c87e93823ff5e59d	SHA256 Hash	Magniber
d9751a0ed800334f8c7e19 62e95d85ad9f32b7336e39 1a08db0b287ce093b8e2	SHA256 Hash	Magniber
e9bf93fe5599f2bda88d53 0e3ba7d5977dcf70111d2b6 23b77d80f8c0cb99cc1	SHA256 Hash	Magniber

Indicator	Type	Description
4194ed735023dc43226724		
cd22b54fa435b4248428f1	SHA256 Hash	Magniber
02299fc7883b723f783e		
9b58afa73eecbfedb9da73		
3eeade27930270864596a	SHA256 Hash	Magniber
df8789a104f38892808eb		
4341336f045c2debc740ee		
cae45406642ebe7d7ecde	SHA256 Hash	Magniber
9e3c9073fcf61c17bf2b3		
52f14b4a6c1087b45051334		
97aafdb3d628d333168f68	SHA256 Hash	Magniber
0b59d9ed88ec78ef989		
d8fdc881b9017c49c2665a		
5af0662ca0021825980cf9	SHA256 Hash	Magniber
e3523d0b3288e8064e5e		
71b17fa931c1227f1a07fc76c		
39249b5af28db728fea43e	SHA256 Hash	Magniber
de63489022b016118		
24aa96e1888c5f7ca567326		
d3d36afc0b3295fd33c739	SHA256 Hash	Magniber
3c94542d4d7a73a0690		
532cd9f4204de4ea6af9d8		
9bea4f2ab1fecc0ad62e4a	SHA256 Hash	Magniber
8a8b83f3315cb8885876		
c49ce435bd4e308de2d30		
00f799ae7e240e52e5534e	SHA256 Hash	Magniber
5d3543bf9adeb737642ca		
	SHA256 Hash	Magniber

Indicator	Type	Description
ddb4ca46c2be3e0feadb37		
b26043c79c5bc533a9b8d		
d349d87673a8157e7c29f		
59186e296cffbd438b0a46		
2ab1a57c517a7c7225fb1670	SHA256 Hash	Magniber
2a5395f9e6ace28615		
b9931f91a07ec9571d68667		
86f71d5255427b8f772b330	SHA256 Hash	Magniber
c475cd5d35b2afd758		
f31a2b06d00ebb691dd1cb		
400ef3a4e2e959f04a1e84	SHA256 Hash	Magniber
065a8936f1165bdb9253		
63cc2e25fb2729e11ce69d4		
8f993b7795f1be3a1cc1698	SHA256 Hash	Magniber
8e956efe041eb25ebe		
a1141be7c8d3c0f8e40fa70		
8ba5a009af5875cd66a04	SHA256 Hash	Magniber
2accfb8e297d22763155		
dcd0b15036586895e4d51		
668bab7319d2acf5900811	SHA256 Hash	Magniber
e963eeeb5563249b25903		
c948d66cb4fcd5a4322ed		
952b198326b5cb22b33cb2	SHA256 Hash	Magniber
cf0c7997761c704251209		
ef76c3ad1730670a22b5e3		
06f07d3f8f4cf3ce429a643	SHA256 Hash	Magniber
86c09346e50df3bbd0c		
04d971099443a580da388		
b717c769dbdacc0d35eb7c	SHA256 Hash	Magniber
d9cc0115753dc8e7a2365		

Indicator	Type	Description
af4eb3dc93f1472826c737b d2804528fb3fbe543f3a6f 671b578abba459aa832	SHA256 Hash	Magniber
c1e9353487796fb7763f5c4 1e8703e4bdad290fd6ec49 1418001171345d80962	SHA256 Hash	Magniber
6171a0ff4855654b140c27b b1d2ab9b6e33cd33f37496 dd7db6c90bc555c1a39	SHA256 Hash	Magniber
c99d824b9ae74c7e3faef1b f4e13e52bb12778cd0059ff caa6dbcaff2859ad61	SHA256 Hash	Magniber
c24c59c8f4e7a581a5d45e e181151ec0a3f0b59af987ea cf9b363577087c9746	SHA256 Hash	Ransom.Royal
5fda381a9884f7be2d57b8a 290f389578a9d2f63e2ecb 98bd773248a7eb99fa2	SHA256 Hash	Ransom.Royal
9db958bc5b4a21340ceee b8c36873aa6bd02a460e6 88de56ccbba945384b192 6	SHA256 Hash	Ransom.Royal
f484f919ba6e36ff33e4fb3 91b8859a94d89c172a4659 64f99d6113b55ced429	SHA256 Hash	Ransom.Royal
2598e8adb87976abe48f0e ba4bbb9a7cb69439e0c13 3b21aee3845dfccf3fb8f	SHA256 Hash	Ransom.Royal
	SHA256 Hash	Ransom.Royal

Indicator	Type	Description
312f34ee8c7b2199a3e78b4		
a52bd87700cc8f3aa01aa6		
41e5d899501cb720775		
491c2b32095174b9de2fd7		
99732a6f84878c2e23b9bb	SHA256 Hash	Ransom.Royal
560cd3155cbdc65e2b80		
7cbfea0bff4b373a175327d		
6cc395f6c176dab1cedf907	SHA256 Hash	Ransom.Royal
5e7130508bec4d5393		
cc00d17f132719a7f942e25		
9a2766d901401beab9cf33	SHA256 Hash	Emotet
d667c78ff471243de8c		
5863e46a1393b316cda81e		
d67d154b7cf1b241bc71bf10	SHA256 Hash	Emotet
70ad4affc39e869573		
20[.]106[.]255[.]48	IP	AgentTesla
141db01f957472533d9791c		
5fb883b442d25d557497c0	SHA256 Hash	AgentTesla
b6b94961fb64330a57f		
195[.]178[.]120[.]24	IP	AgentTesla
e7552675d7930f3259d3af		
c5fc2ebc23224906a2379e	SHA256 Hash	Remcos
5917f0632e9137cd88ff		
bdfa49ba459255ece9528e		
133fab8a0f858b60f6d625	SHA256 Hash	Remcos
3c52d3f3b0bb1f59bdc0		
obologs[.]work[.]gd	Domain	Remcos
144[.]76[.]136[.]153	IP	Remcos

Indicator	Type	Description
79213f7a11227ebd73c0ad8 eef1960cd8f8cf901a0fdab e319eec1c1ef0ee39	SHA256 Hash	AgentTesla
195eef0d5de283dbe0d5e9 c9d549bf97277d9154385a 019b750cab13c038659	SHA256 Hash	AgentTesla
automatic[.]tworiversboats [.]com	Domain	SocGholish-DS
15560b1e35a3a8612a7ba91 d00dea6b8dd6e4f3f85739 9c22c0c75377c9b31a2	SHA256 Hash	BlackBasta
1bb7e645d4ff753157bbdd7 8829276356cb6660a767a b7158fc7dec3fe8b0e2f	SHA256 Hash	BlackBasta