THREAT INTEL

Threat Intelligence

2022-11-14 Threat Intel Report

TLP: CLEAR

November 2022

updated: 11/14/22

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:

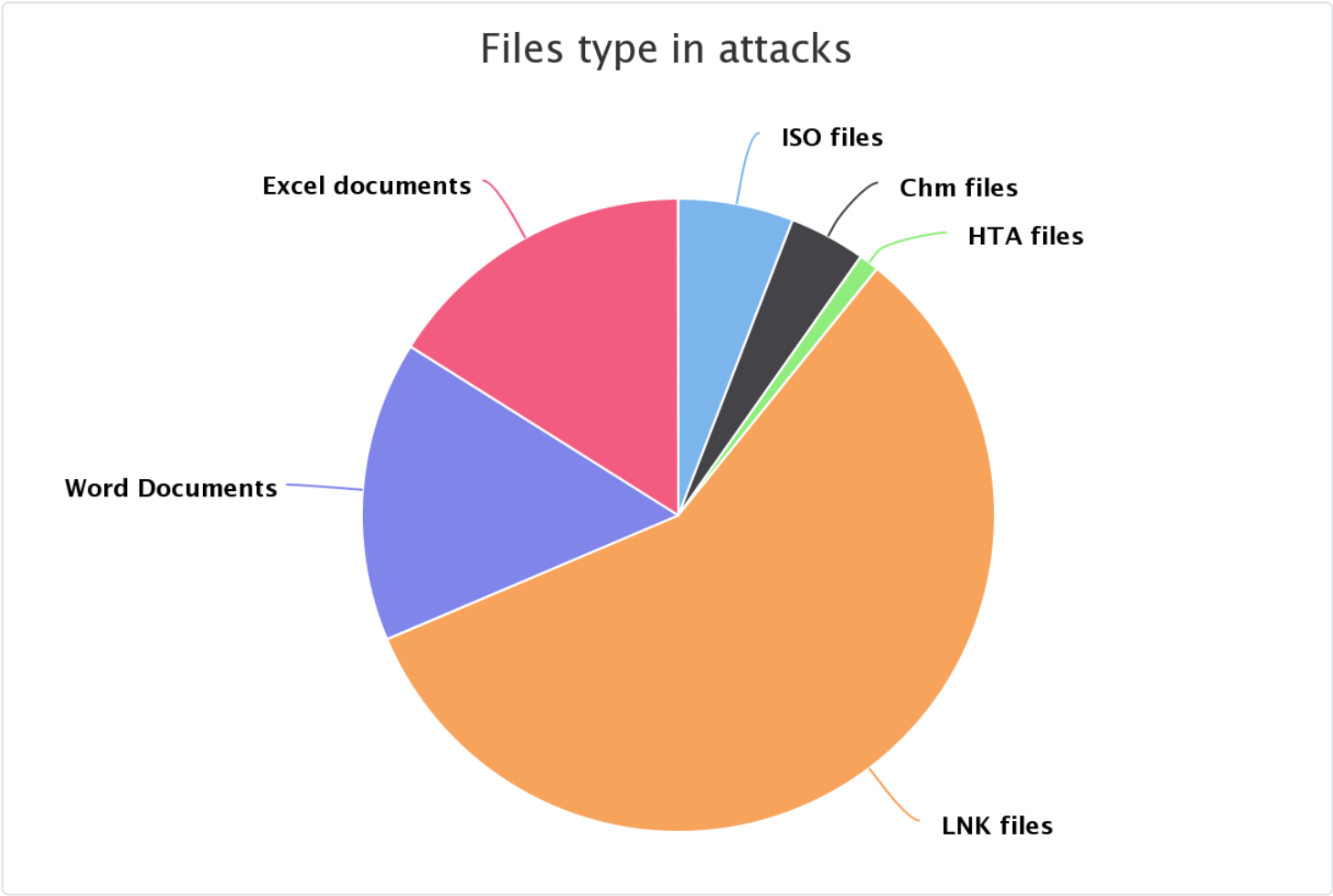
- Malspam
- Web
- Ransomware
- APTs
- Zero-days

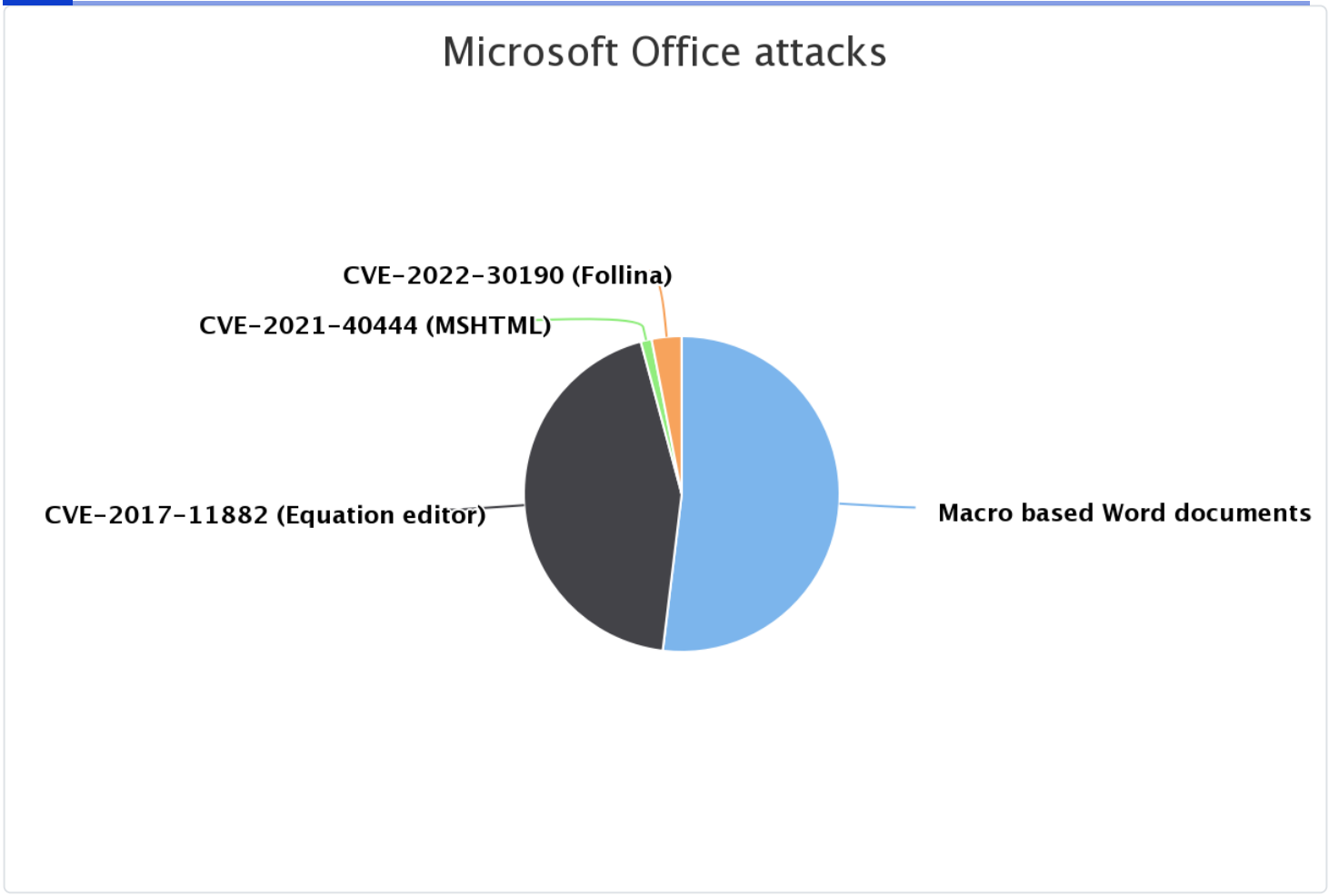
Each attack tracked and observed by our threat intelligence team is checked against Malwarebytes products to ensure our customers are continually protected.

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

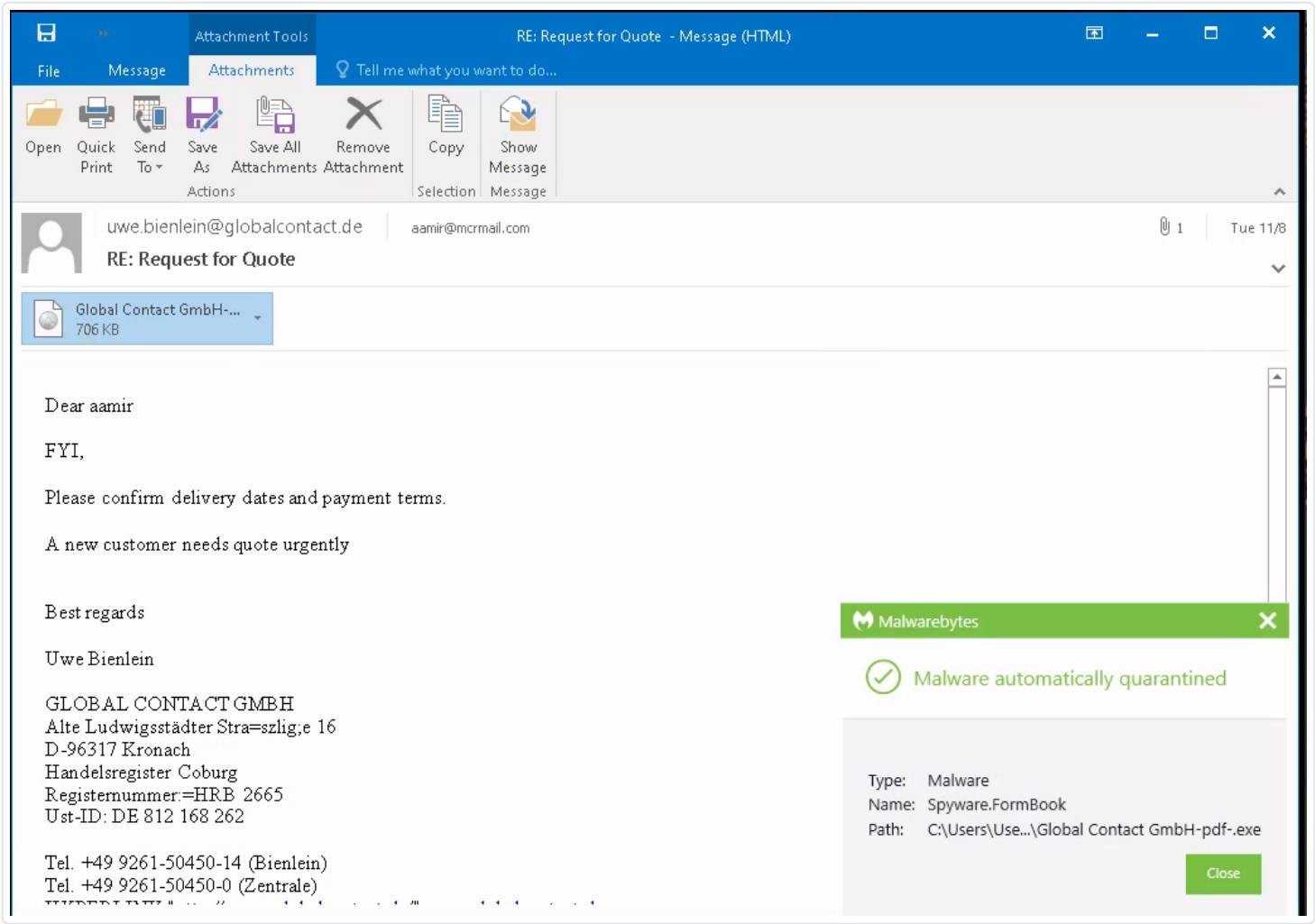




Note: Threat name descriptions are pulled from Malpedia .

Formbook

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



Email subject(s):

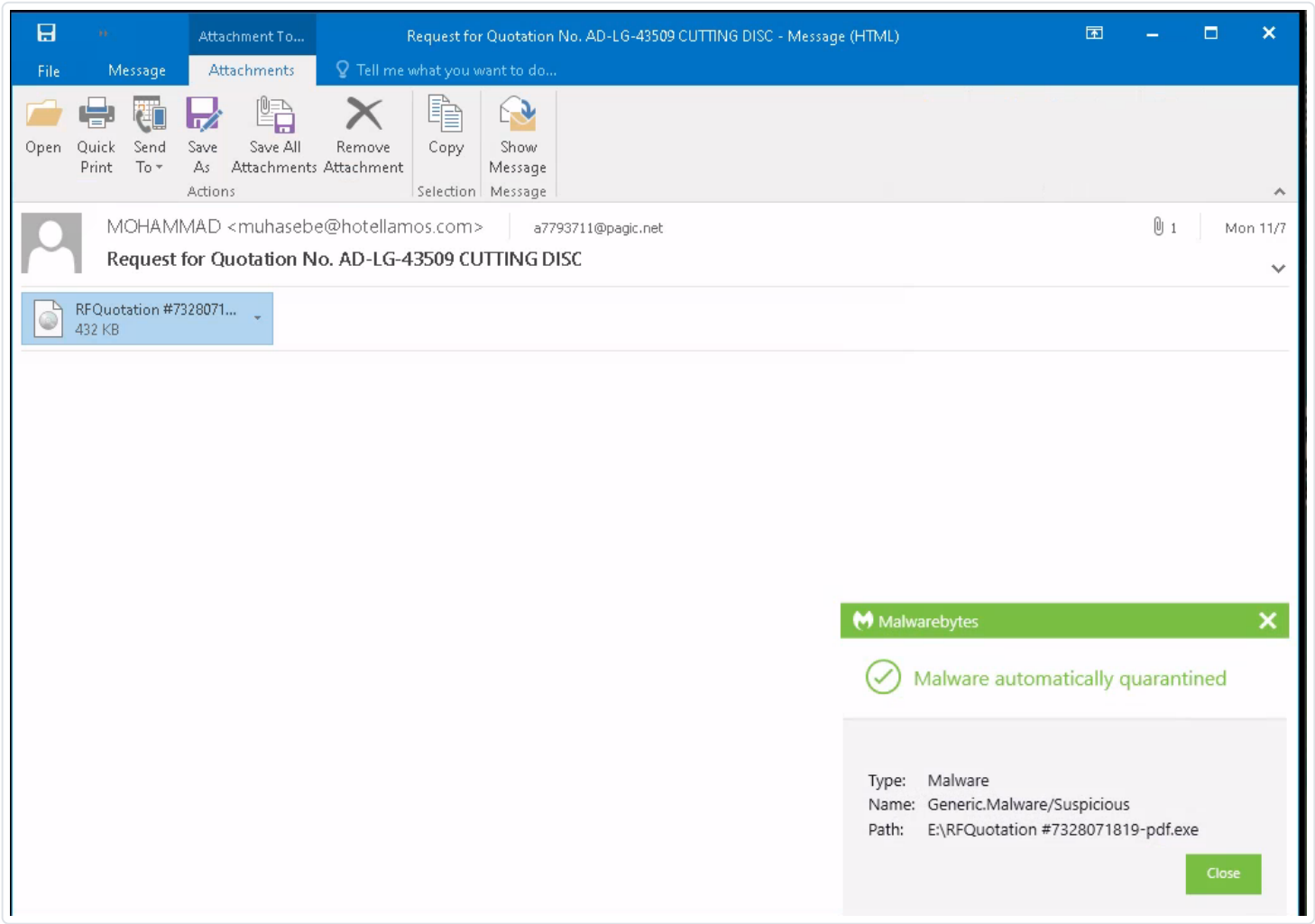
- RE: Request for Quote

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):

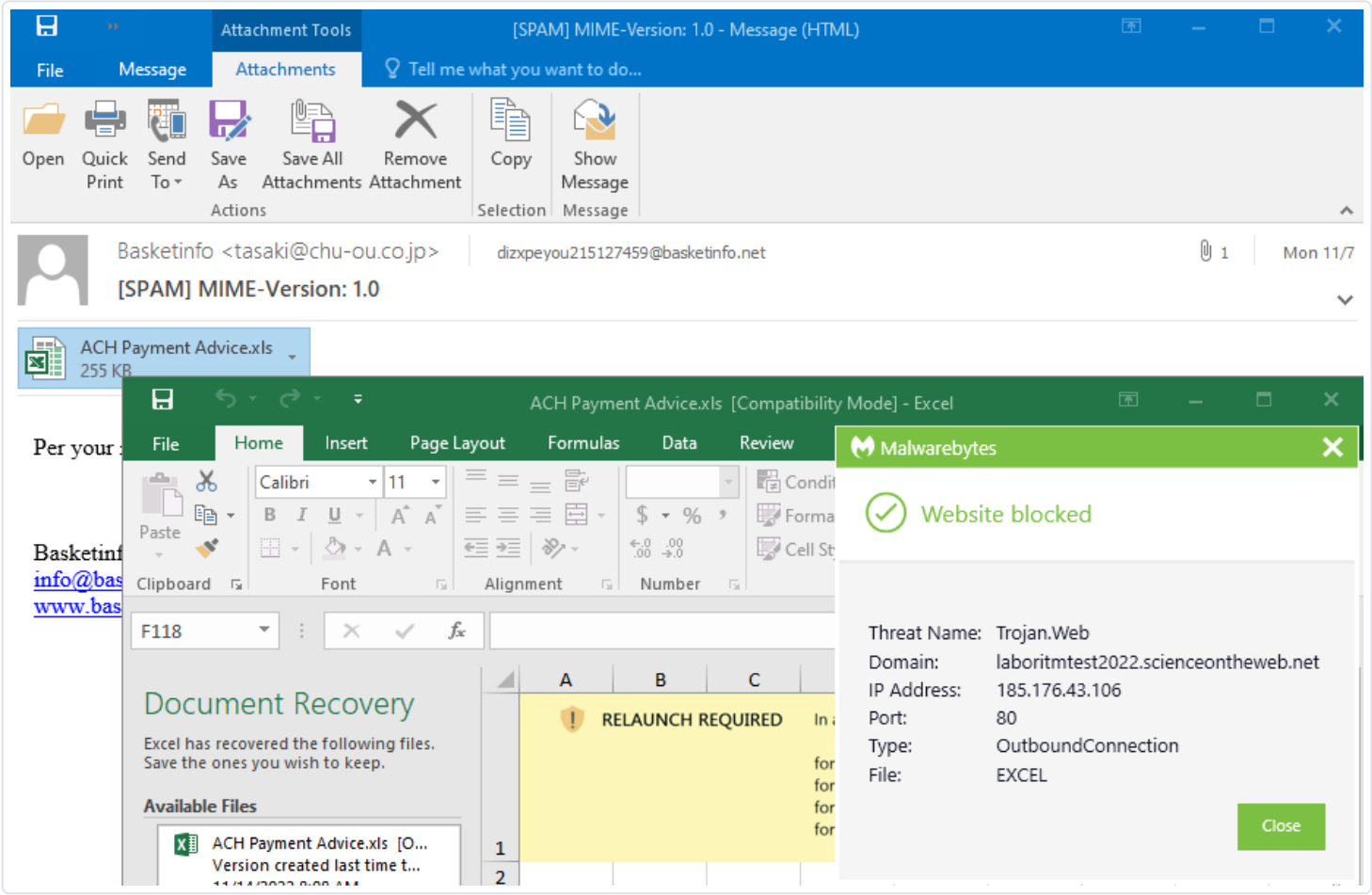
- FedEx Express AWB#5305323204643 - Information is required
- RE: Request for Quote
- COTIZACION ARTICULOS DE OFICINA PARA PRODUCCION.
- Pago de saldo/copias TT
- FB-108N & FB-108NK 詢價 - 田勤

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 atack.



Email subject(s):

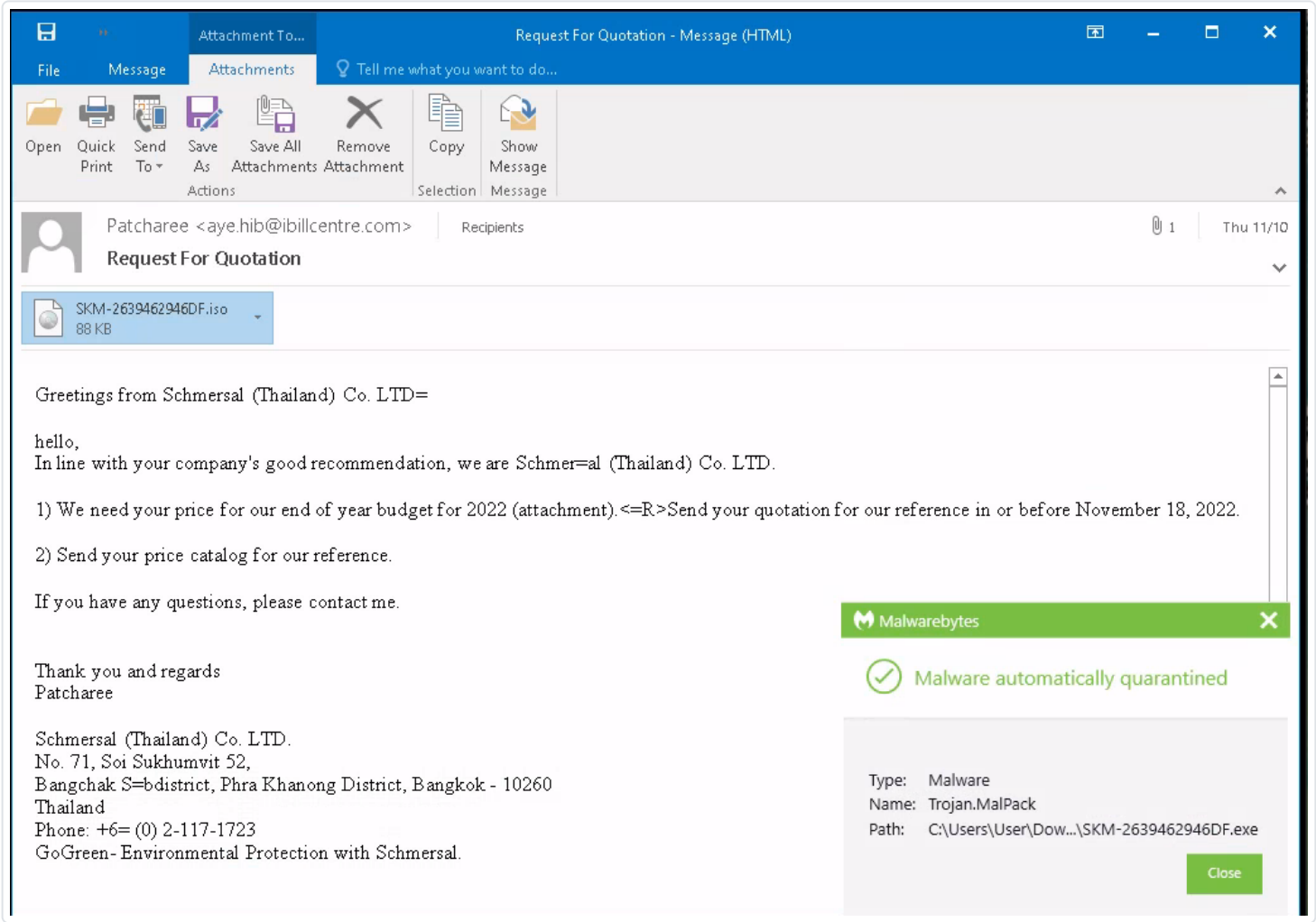
- [SPAM] MIME-Version: 1.0
- Fwd:
- Re: Csomagja_kézbesítésre_vár_!

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.



Email subject(s):

- Request For Quotation

Attachment name(s):

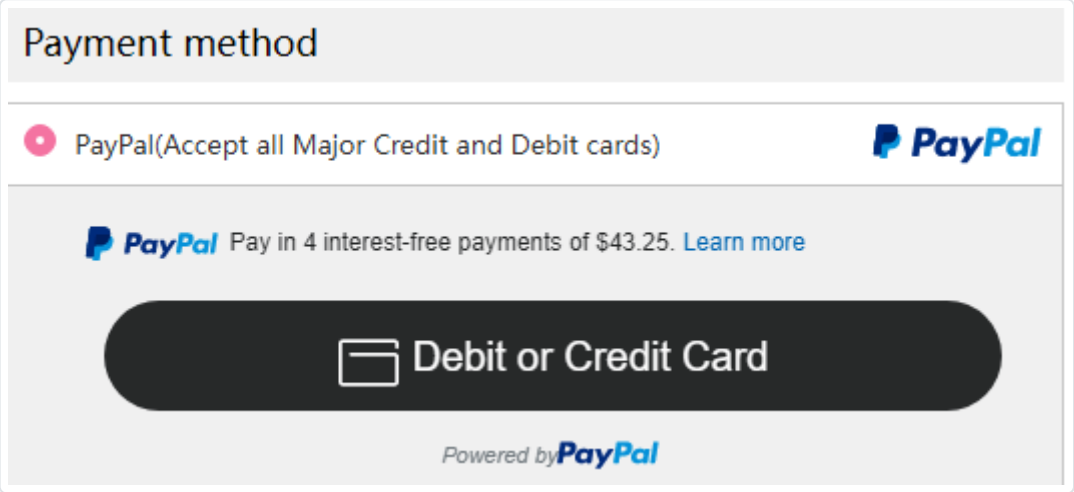
- SKM-2639462946DF.iso

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

Web threats

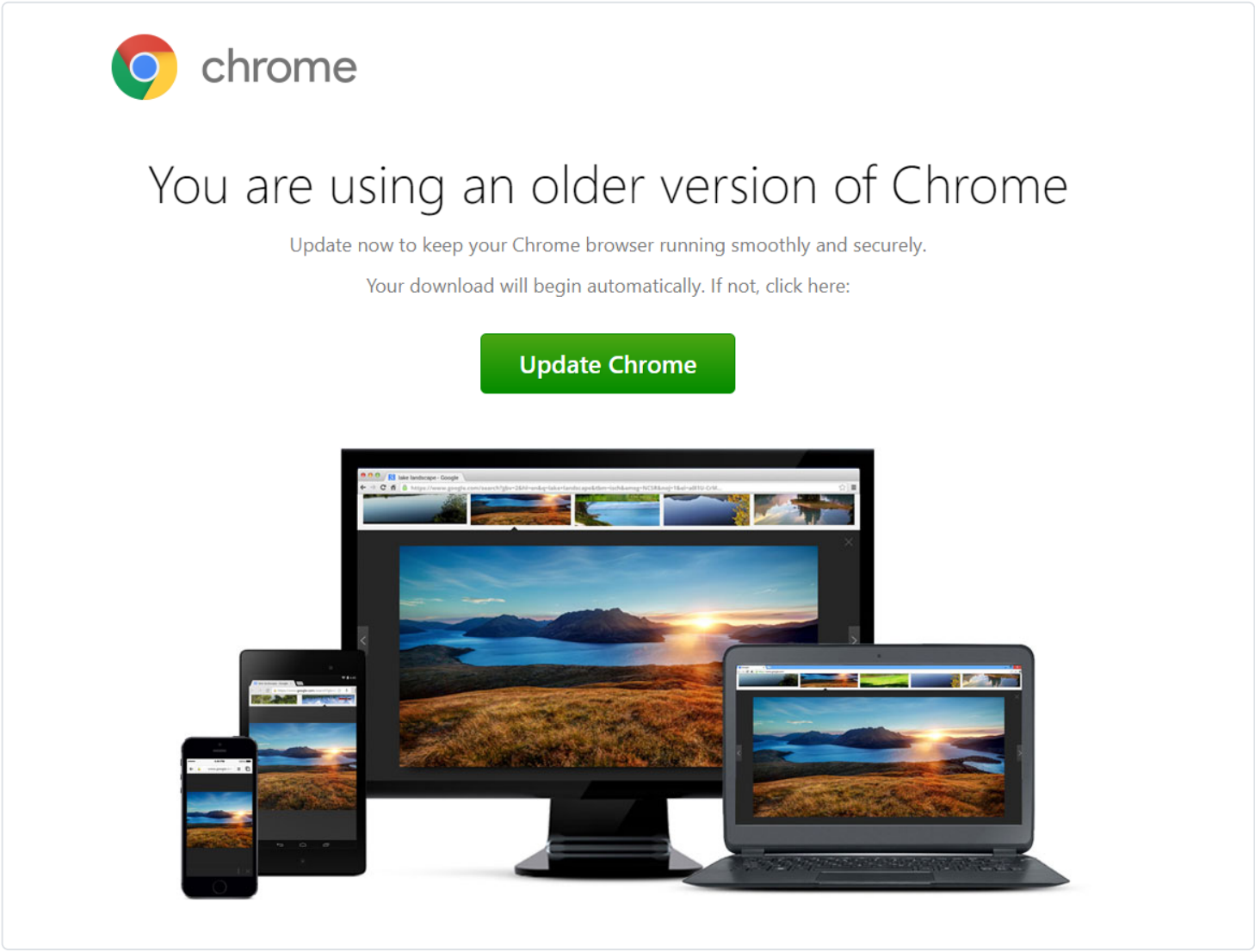
Magecart

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



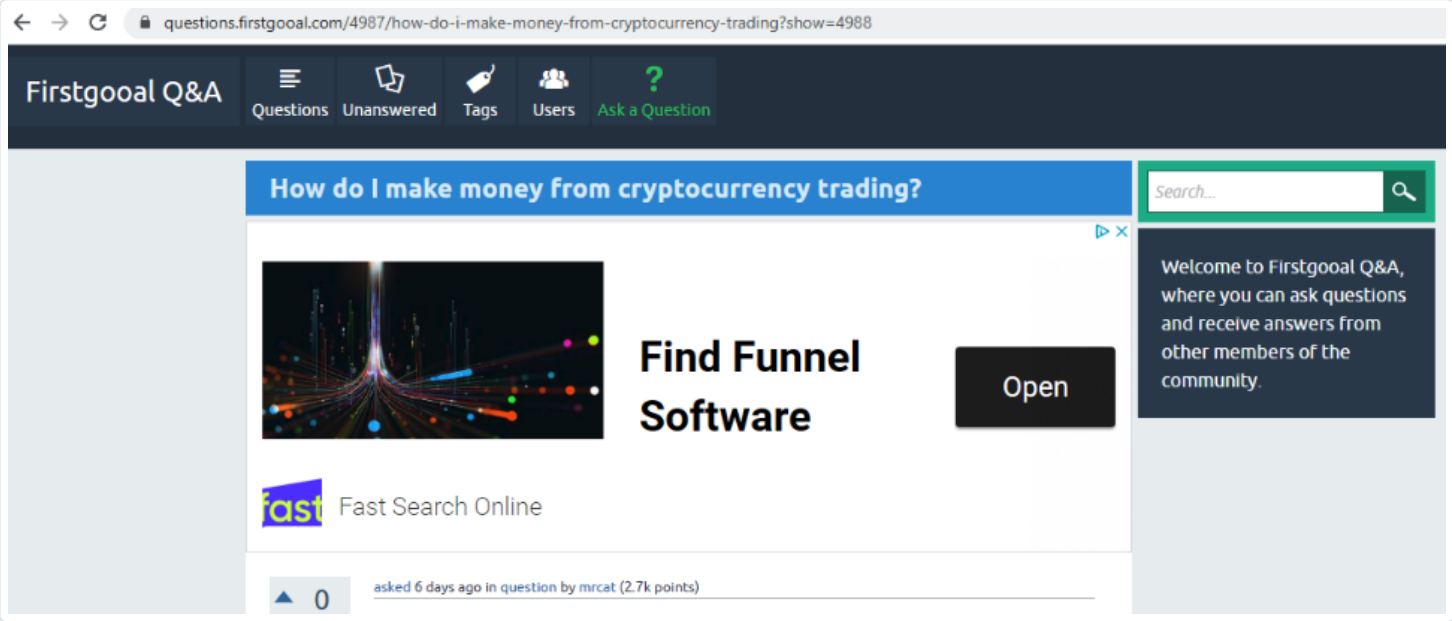
FakeUpdates/SocGholish

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



Spammy Q&A redirects

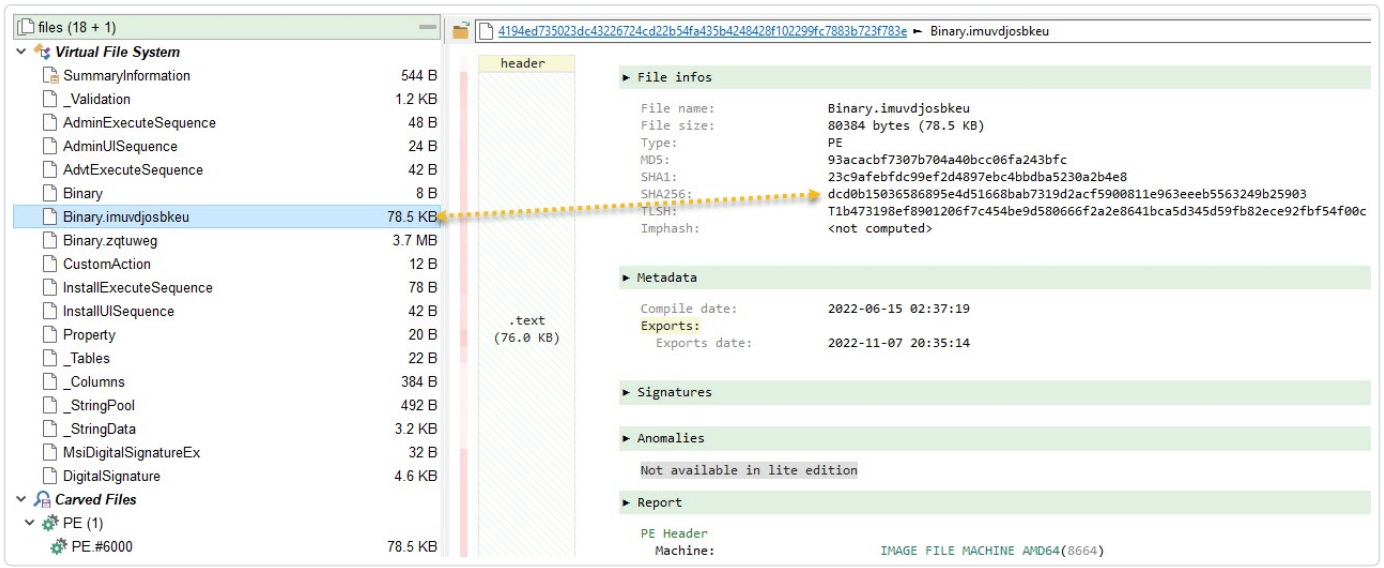
The folks at Sucuri published a **blog** about a large redirection campaign from compromised sites to various spammy Q&A pages. According to them, over 15 thousand websites have been hacked and redirecting users between September and October.



Ransomware

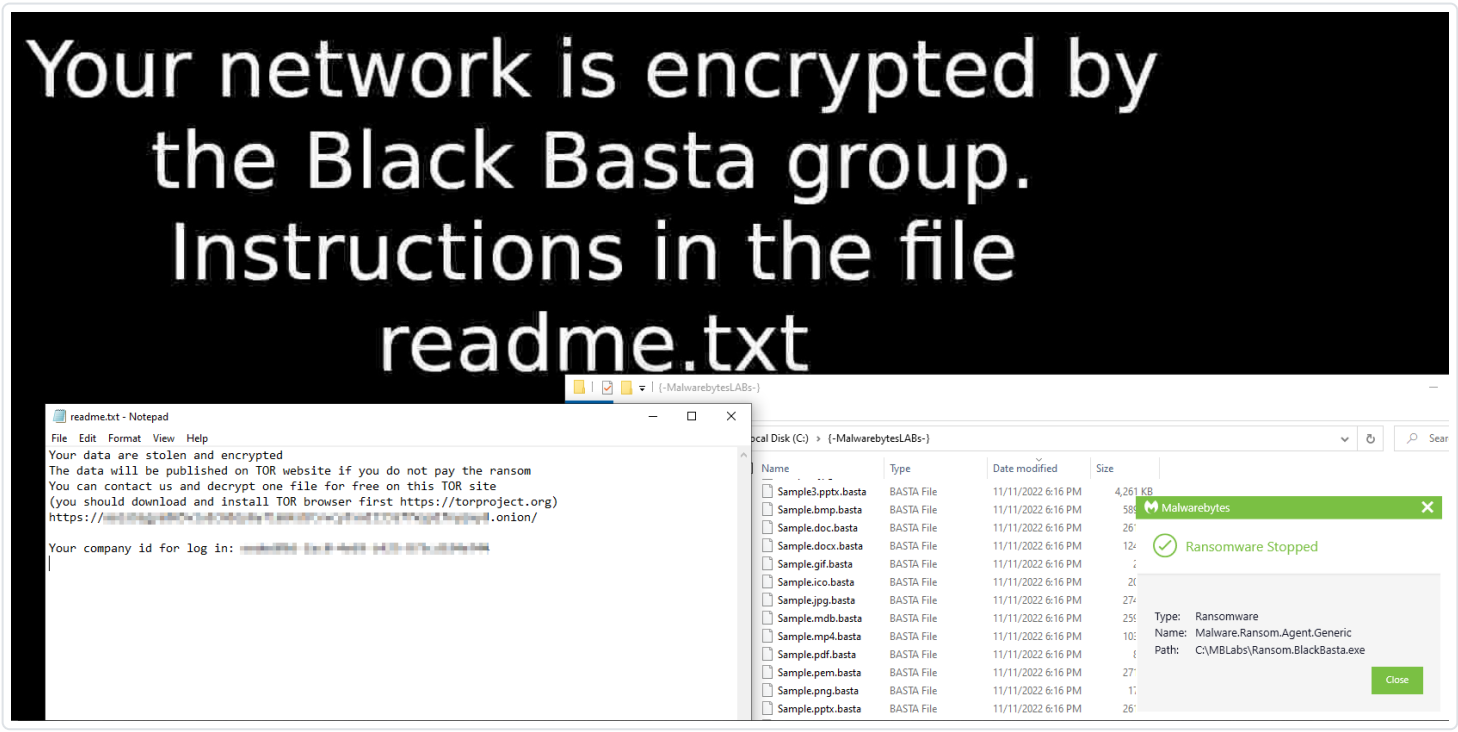
Magniber

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



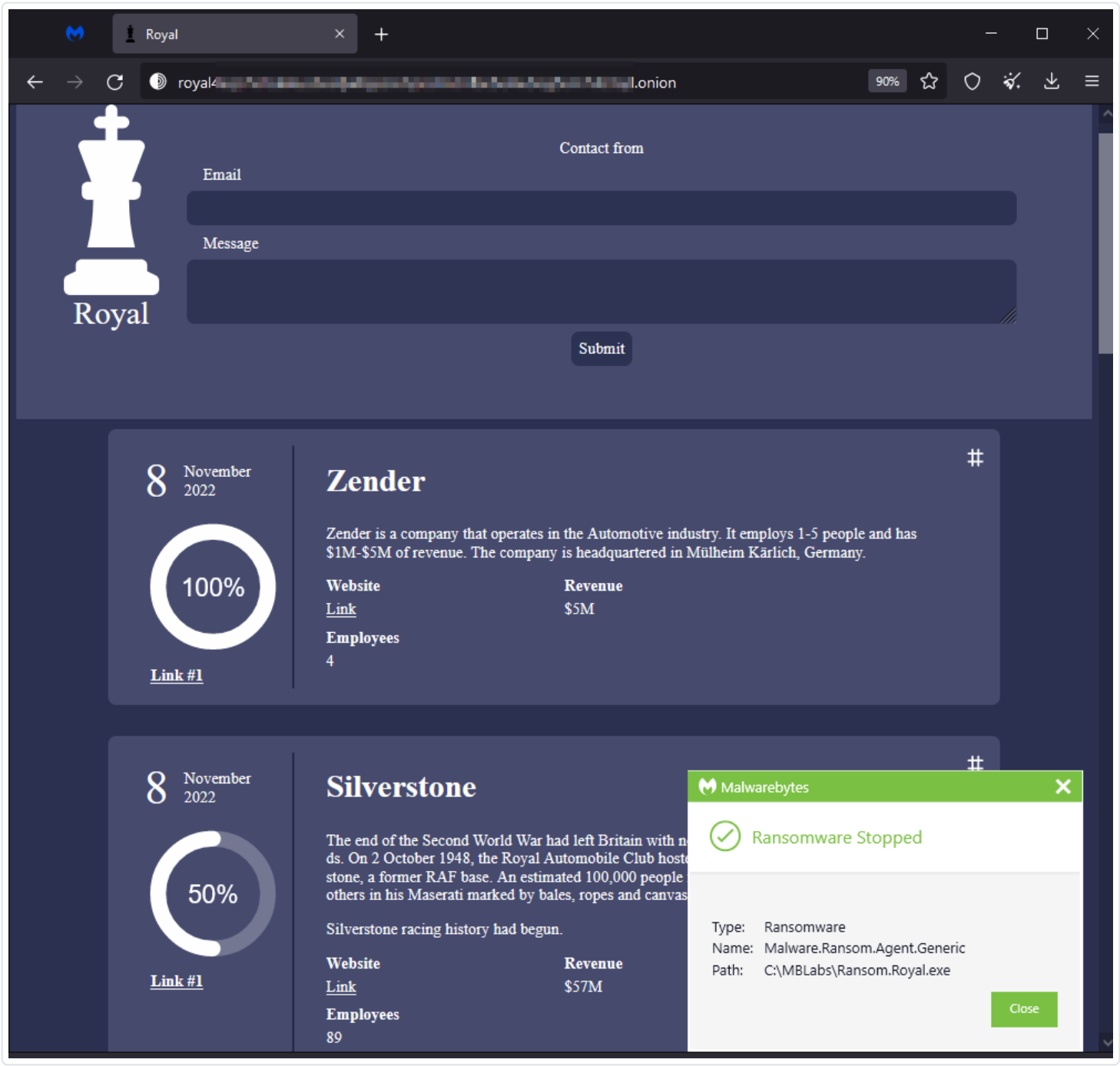
Black Basta

- Extension .basta
- Ransom note: readme.txt



Royal ransomware

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



Indicators of Compromise (IOCs)

Indicator	Type	Description
182[.]162[.]143[.]56	IP	Emotet
course[.]netpickstrading[.]com	Domain	SocGholish-DS
brontop[.]net	Domain	Magecart
fa554d4efb21948bc84493ac1a170406c4106e2e90f1b14e96f2064c3c1b7199	SHA256 Hash	Formbook
66[.]96[.]160[.]146	IP	Formbook
bridginglegal[.]com	Domain	Formbook
8ced3b47bed5c4a21219e9857f092343bfd2a66c53c18489aa0c0ecab733aebf	SHA256 Hash	Formbook
bf850e8ad84f2a75a68064fd21d0129d3e74ee2a7beaf22f2401a7f3ab60d4b0	SHA256 Hash	AgentTesla
bytesendesign[.]nl	Domain	Emotet
3b07c87e9306549b470fa6796c8994bca6ceb8266f638772b40482097bfc2ca6	SHA256 Hash	Emotet
blangkonstudio[.]com	Domain	Emotet
careofu[.]com	Domain	Emotet
laboritmtest2022[.]scienceontheweb[.]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
602de00f00c364c9549d313b9e0f941e6073c5320aa53ed6a8362ee5ceb6a19d	SHA256 Hash	Emotet
85ba4ce2eeeee9eca255d6da5e24c5fe1241966be579d07f2aee8b9058ec92c0	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[.]firstgooal[.]com	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
ca5bd5fdd79251b2fb4e274ff8cc219b66804d52e215863adab66ba3651bce42	SHA256 Hash	Magniber
b41a120d5a4a3ea9c6a6639fa0cdcaf14b383ec035890dc2e714a44a5e50ca9b	SHA256 Hash	Magniber
bc8f6149a6b6423c82dd7f51aff4756539577eacf27b7019c87e93823ff5e59d	SHA256 Hash	Magniber
d9751a0ed800334f8c7e1962e95d85ad9f32b7336e391a08db0b287ce093b8e2	SHA256 Hash	Magniber
e9bf93fe5599f2bda88d530e3ba7d5977dcf70111d2b623b77d80f8c0cb99cc1	SHA256 Hash	Magniber

Indicator	Type	Description
4194ed735023dc43226724cd22b54fa435b4248428f102299fc7883b723f783e	SHA256 Hash	Magniber
9b58afa73eecbfebb9da733eeade27930270864596adf8789a104f38892808eb	SHA256 Hash	Magniber
4341336f045c2debc740eecae45406642ebe7d7ecde9e3c9073fcf61c17bf2b3	SHA256 Hash	Magniber
52f14b4a6c1087b4505133497aafdb3d628d333168f680b59d9ed88ec78ef989	SHA256 Hash	Magniber
d8fdc881b9017c49c2665a5af0662ca0021825980cf9e3523d0b3288e8064e5e	SHA256 Hash	Magniber
71b17fa931c1227f1a07fc76c39249b5af28db728fea43ede63489022b016118	SHA256 Hash	Magniber
24aa96e1888c5f7ca567326d3d36afc0b3295fd33c7393c94542d4d7a73a0690	SHA256 Hash	Magniber
532cd9f4204de4ea6af9d89bea4f2ab1fecc0ad62e4a8a8b83f3315cb8885876	SHA256 Hash	Magniber
c49ce435bd4e308de2d3000f799ae7e240e52e5534e5d3543bf9adeb737642ca	SHA256 Hash	Magniber
	SHA256 Hash	Magniber

Indicator	Type	Description
ddb4ca46c2be3e0feadb37b26043c79c5bc533a9b8dd349d87673a8157e7c29f		
59186e296cffbd438b0a462ab1a57c517a7c7225fb16702a5395f9e6ace28615	SHA256 Hash	Magniber
b9931f91a07ec9571d6866786f71d5255427b8f772b330c475cd5d35b2afd758	SHA256 Hash	Magniber
f31a2b06d00ebb691dd1cb400ef3a4e2e959f04a1e84065a8936f1165bdb9253	SHA256 Hash	Magniber
63cc2e25fb2729e11ce69d48f993b7795f1be3a1cc16988e956efe041eb25ebe	SHA256 Hash	Magniber
a1141be7c8d3c0f8e40fa708ba5a009af5875cd66a042accfb8e297d22763155	SHA256 Hash	Magniber
dcd0b15036586895e4d51668bab7319d2acf5900811e963eeeb5563249b25903	SHA256 Hash	Magniber
c948d66cb4fcd5a4322ed952b198326b5cb22b33cb2cf0c7997761c704251209	SHA256 Hash	Magniber
ef76c3ad1730670a22b5e306f07d3f8f4cf3ce429a64386c09346e50df3bbd0c	SHA256 Hash	Magniber
04d971099443a580da388b717c769dbdacc0d35eb7cd9cc0115753dc8e7a2365	SHA256 Hash	Magniber

Indicator	Type	Description
af4eb3dc93f1472826c737bd2804528fb3cbe543f3a6f671b578abba459aa832	SHA256 Hash	Magniber
c1e9353487796fb7763f5c41e8703e4bdad290fd6ec491418001171345d80962	SHA256 Hash	Magniber
6171a0ff4855654b140c27bb1d2ab9b6e33cd33f37496dd7db6c90bc555c1a39	SHA256 Hash	Magniber
c99d824b9ae74c7e3faef1bf4e13e52bb12778cd0059ffcaa6dbcaff2859ad61	SHA256 Hash	Magniber
c24c59c8f4e7a581a5d45ee181151ec0a3f0b59af987eacf9b363577087c9746	SHA256 Hash	Ransom.Royal
5fda381a9884f7be2d57b8a290f389578a9d2f63e2ecb98bd773248a7eb99fa2	SHA256 Hash	Ransom.Royal
9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926	SHA256 Hash	Ransom.Royal
f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429	SHA256 Hash	Ransom.Royal
2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f	SHA256 Hash	Ransom.Royal
	SHA256 Hash	Ransom.Royal

Indicator	Type	Description
312f34ee8c7b2199a3e78b4a52bd87700cc8f3aa01aa641e5d899501cb720775		
491c2b32095174b9de2fd799732a6f84878c2e23b9bb560cd3155cbdc65e2b80	SHA256 Hash	Ransom.Royal
7cbfea0bff4b373a175327d6cc395f6c176dab1cedf9075e7130508bec4d5393	SHA256 Hash	Ransom.Royal
cc00d17f132719a7f942e259a2766d901401beab9cf33d667c78ff471243de8c	SHA256 Hash	Emotet
5863e46a1393b316cda81ed67d154b7cf1b241bc71bf1070ad4affc39e869573	SHA256 Hash	Emotet
20[.]106[.]255[.]48	IP	AgentTesla
141db01f957472533d9791c5fb883b442d25d557497c0b6b94961fb64330a57f	SHA256 Hash	AgentTesla
195[.]178[.]120[.]24	IP	AgentTesla
e7552675d7930f3259d3afc5fc2ebc23224906a2379e5917f0632e9137cd88ff	SHA256 Hash	Remcos
bdfa49ba459255ece9528e133fab8a0f858b60f6d6253c52d3f3b0bb1f59bdc0	SHA256 Hash	Remcos
obologs[.]work[.]gd	Domain	Remcos
144[.]76[.]136[.]153	IP	Remcos

Indicator	Type	Description
79213f7a11227ebd73c0ad8eeff1960cd8f8cf901a0fdabe319eec1c1ef0ee39	SHA256 Hash	AgentTesla
195eef0d5de283dbe0d5e9c9d549bf97277d9154385a019b750caba13c038659	SHA256 Hash	AgentTesla
automatic[.]tworiversboats[.]com	Domain	SocGholish-DS
15560b1e35a3a8612a7ba91d00dea6b8dd6e4f3f857399c22c0c75377c9b31a2	SHA256 Hash	BlackBasta
1bb7e645d4ff753157bbdd78829276356cb6660a767ab7158fc7dec3fe8b0e2f	SHA256 Hash	BlackBasta