Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

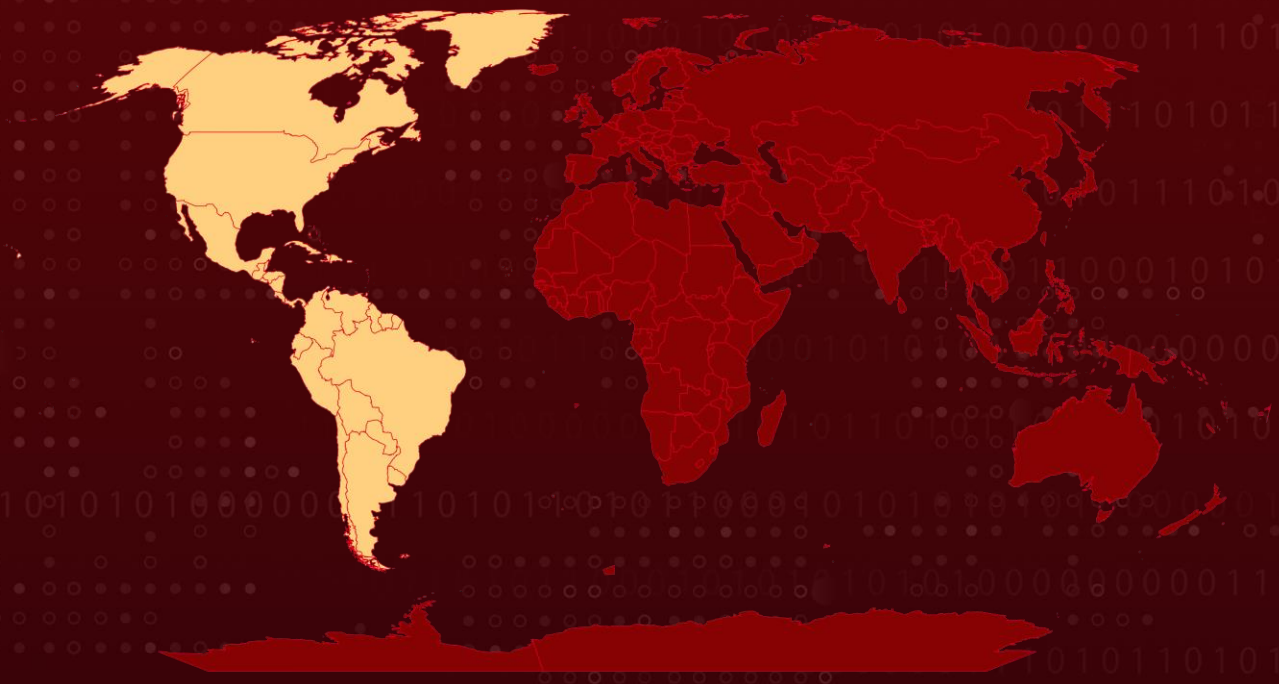
# Metamorfo Banking Trojan Targets the Americas

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| May 20, 2024 | A1 | TA2024195 |

# Summary

**Active Since:** 2018
**Malware:** Metamorfo Banking Trojan (aka Mekotio, Casbaneiro)
**Attack Region:** North and South America
**Attack:** Metamorfo, also referred to as Mekotio or Casbaneiro, is an advanced banking Trojan disseminated through malspam campaigns, primarily targeting users in North and South America. Active since 2018, this malware is designed to pilfer financial information and banking credentials.

## Attack Regions



# Attack Details

**#1** Metamorfo, also known as Mekotio or Casbaneiro, is a sophisticated banking Trojan that spreads through malspam campaigns. This malware primarily targets users in North and South America, aiming to steal financial information and banking credentials.

**#2** Active since 2018, Metamorfo has been highly effective at exfiltrating banking information and other sensitive data to its command-and-control (C2) server. Metamorfo entices users into clicking on HTML attachments, initiating a complex sequence of actions designed to harvest system metadata.

**#3** The infection chain employs advanced obfuscation techniques, URL evasion strategies, and the downloading of malicious payloads. Once activated, the malware connects to remote servers, collects sensitive data, disables security measures such as antivirus software, and alters system registry settings.

**#4** Further, a PowerShell script executes to create multiple shortcuts and batch files in various locations, including AppData and the StartUp folder. These actions ensure the malware's persistence on the compromised system.

# Recommendations

**User Education and Awareness:** Educate users about the dangers of opening suspicious documents or files received via email or other channels. Encourage them to be cautious and vigilant when interacting with unknown or unexpected content.

**Zero Trust Architecture:** Adopting a zero-trust security model can help organizations mitigate the risk of insider threats and unauthorized access. Implementing strict access controls, multi-factor authentication (MFA), and continuous monitoring can prevent unauthorized users from compromising AI systems and data.

**Anomaly Detection:** Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

**Network Segmentation:** Implement network segmentation to isolate critical systems and sensitive data from less secure areas of your network. This can help contain the spread of malware like Metamorfo.

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0005<br>Defense Evasion |
| TA0004<br>Privilege Escalation | TA0006<br>Credential Access | TA0007<br>Discovery | TA0009<br>Collection |
| TA0011<br>Command and Control | TA0010<br>Exfiltration | TA0040<br>Impact | T1566.001<br>Spearphishing Attachment |
| T1566<br>Phishing | T1059<br>Command and Scripting Interpreter | T1059.001<br>PowerShell | T1204<br>User Execution |
| T1204.001<br>Malicious Link | T1547.001<br>Registry Run Keys / Startup Folder | T1543<br>Create or Modify System Process | T1068<br>Exploitation for Privilege Escalation |
| T1055<br>Process Injection | T1140<br>Deobfuscate/Decode Files or Information | T1212<br>Exploitation for Credential Access | T1083<br>File and Directory Discovery |
| T1518.001<br>Security Software Discovery | T1082<br>System Information Discovery | T1005<br>Data from Local System | T1071<br>Application Layer Protocol |
| T1041<br>Exfiltration Over C2 Channel | T1657<br>Financial Theft | T1566.002<br>Spearphishing Link | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 54[.]39[.]10[.]87,<br>20[.]206[.]126[.]228,<br>89[.]116[.]236[.]122,<br>158[.]69[.]110[.]217,<br>89[.]117[.]37[.]61,<br>185[.]185[.]87[.]45,<br>172[.]105[.]111[.]154, |

| TYPE | VALUE |
| --- | --- |
| IPv4 | 51[.]38[.]235[.]152,<br>192[.]46[.]216[.]151,<br>86[.]38[.]217[.]167,<br>38[.]54[.]20[.]37,<br>154[.]223[.]16[.]114,<br>139[.]177[.]193[.]74,<br>149[.]100[.]158[.]179,<br>20[.]92[.]164[.]32,<br>212[.]46[.]38[.]43,<br>216[.]238[.]70[.]224,<br>185[.]45[.]195[.]226,<br>80[.]211[.]249[.]77,<br>18[.]184[.]132[.]208 |
| Domains | vqz8[.]gotdns[.]ch,<br>nhoquemassa[.]com,<br>09dfwss6g1v73sya[.]online,<br>cevda3jvv5oz1t37[.]online,<br>4yw2twoy438df9qt[.]online,<br>albumdepremios[.]com[.]br,<br>chooseanother[.]com,<br>yuphsa6qwtg5[.]online,<br>6c48ax07dy25hvu0hub[.]online,<br>z5im1ou9o480se02pro[.]online,<br>x50zbqev4po5[.]online,<br>newlife2020[.]club,<br>k6ue95v1ca2r[.]online,<br>jkue[.]myftp[.]biz,<br>2xo0uaqv4cqds331mart[.]online,<br>zfi8ny6yi30s[.]website,<br>mpy8n37wvwu2now[.]online,<br>l155vcram2hl6ws0[.]online,<br>x6vl9710f400g7alstar[.]online,<br>baza[.]alta-bars[.]ru |
| URLs | hxxp://86.38.217[.]167/13/index[.]php,<br>hxxp://86.38.217[.]167/ps1/index[.]php,<br>hxxp://86.38.217[.]167/ld/index[.]php,<br>hxxp://86.38.217[.]167/vth/vth,<br>hxxp://86.38.217[.]167/ps/index[.]php,<br>hxxp://adbd[.]tech/26/index[.]php,<br>hxxp://86.38.217[.]167/07/index[.]php,<br>hxxp://86.38.217[.]167/21/index[.]php,<br>hxxp://ad2.gotdns[.]ch/22/22,<br>hxxp://38.54.20[.]37/29/index[.]php,<br>hxxp://38.54.20[.]37/nv/index[.]php,<br>hxxp://38.54.20[.]37/17/17, |

| TYPE | VALUE |
| --- | --- |
| URLs | hxxp://a.3utilities[.]com/17/, hxxp://38.54.20[.]37/04/04, hxxp://avs.myftp[.]biz/04/, hxxp://38.54.20[.]37/19/index[.]php, hxxp://38.54.20[.]37/29/29, hxxp://avs.myftp[.]biz/29/, hxxp://38.54.20[.]37/08/08, hxxp://jan.viewdns[.]net/08/ |
| SHA1 | 428fe9b7608cd82303e27103c3058ecd61bd58a6, bbf3387c82a600053e2fdfef6491cc20d099dd0a, 5844edfe712db9ba8f50ae767089c6430cb2a3ff, 7fd7c43a1237c2c4245ac987fbbac54fdad3ba06, 0a590eece111062573082c248d722c428134db66, 8cc2248e33c3e9521f97965706ce374530d971cb, 45f8c91f0299012a8dcb40d9a2fb5ce7962b887a, a9e9df6762418bbed030e825099282da59278db0, e2218b08b6dd53fa115ad50b70f41d0f0a080ce6, 2bd4acea5c3bf107cc6615af65d1617c847814cc, 4b5b7cf403ac7d6e3dd787104e3e6bd088743815 |

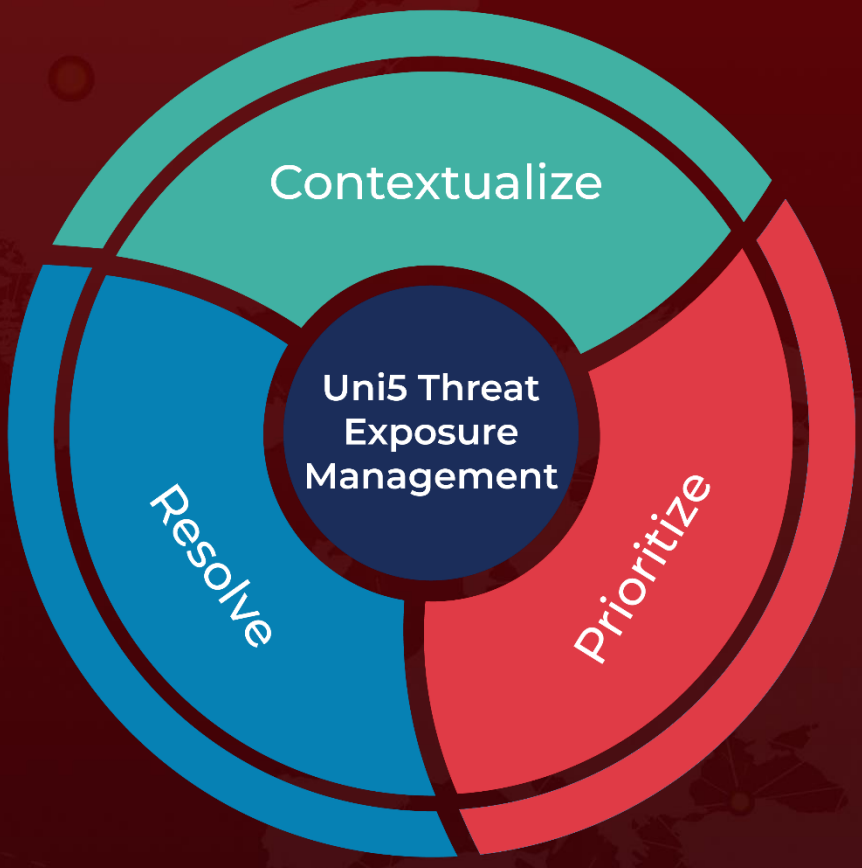
## References

https://www.forcepoint.com/blog/x-labs/exploring-metamorfo-banking-malware

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**May 20, 2024 • 6:00 AM**



More at www.hivepro.com