Feb 09 2024

NETMANAGEIT

Intelligence Report

MoqHao Evolution: New variants start automatically right after installation

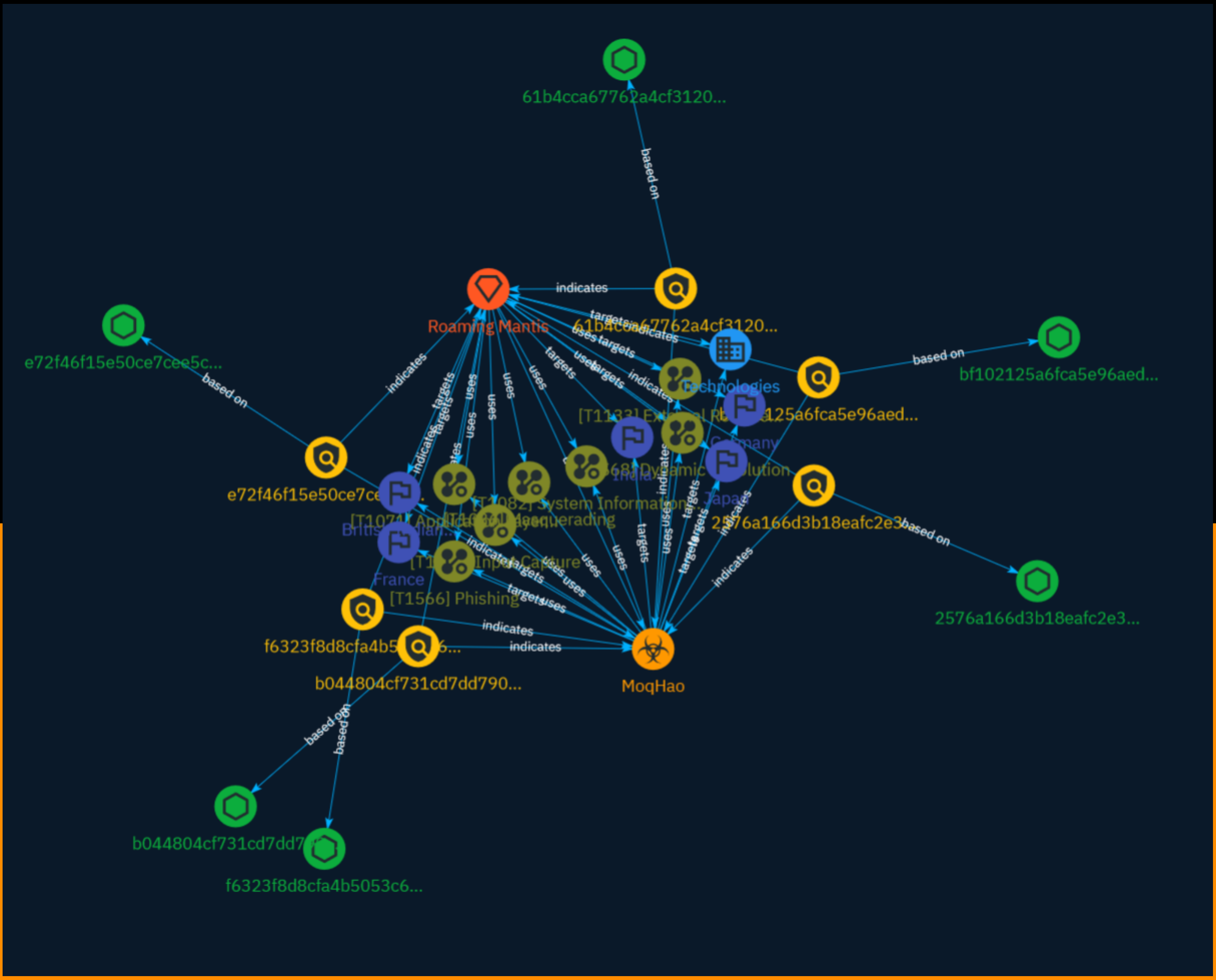

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 11
- Intrusion-Set 12
- Attack-Pattern 13
- Country 22
- Sector 24

Observables

- StixFile 25

External References

● External References 26

Overview

Description

A recent variant of the Android malware MoqHao has been found to automatically execute itself upon installation without requiring user interaction. The malware is distributed via SMS phishing links and abuses legitimate services like URL shorteners and Pinterest. It targets users in Asia and Europe, collects device info, and contains many new command and control capabilities.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name
f6323f8d8cfa4b5053c65f8c1862a8e6844b35b260f61735b3cf8d19990fef42
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f6323f8d8cfa4b5053c65f8c1862a8e6844b35b260f61735b3cf8d19990fef42']
Name
e72f46f15e50ce7cee5c4c0c5a5277e8be4bb3dd23d08ea79e1deacb8f004136
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e72f46f15e50ce7cee5c4c0c5a5277e8be4bb3dd23d08ea79e1deacb8f004136']
Name

bf102125a6fca5e96aed855b45bbed9aa0bc964198ce207f2e63a71487ad793a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'bf102125a6fca5e96aed855b45bbed9aa0bc964198ce207f2e63a71487ad793a']

Name

b044804cf731cd7dd79000b7c6abce7b642402b275c1eb25712607fc1e5e3d2b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'b044804cf731cd7dd79000b7c6abce7b642402b275c1eb25712607fc1e5e3d2b']

Name

61b4cca67762a4cf31209056ea17b6fb212e175ca330015d804122ee6481688e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61b4cca67762a4cf31209056ea17b6fb212e175ca330015d804122ee6481688e']

Name

2576a166d3b18eafc2e35a7de3e5549419d10ce62e0eeb24bad5a1daaa257528

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2576a166d3b18eafc2e35a7de3e5549419d10ce62e0eeb24bad5a1daaa257528']

Name

f6323f8d8cfa4b5053c65f8c1862a8e6844b35b260f61735b3cf8d19990fef42

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6323f8d8cfa4b5053c65f8c1862a8e6844b35b260f61735b3cf8d19990fef42']

Name

e72f46f15e50ce7cee5c4c0c5a5277e8be4bb3dd23d08ea79e1deacb8f004136

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e72f46f15e50ce7cee5c4c0c5a5277e8be4bb3dd23d08ea79e1deacb8f004136']

Name

bf102125a6fca5e96aed855b45bbed9aa0bc964198ce207f2e63a71487ad793a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf102125a6fca5e96aed855b45bbed9aa0bc964198ce207f2e63a71487ad793a']

Name

b044804cf731cd7dd79000b7c6abce7b642402b275c1eb25712607fc1e5e3d2b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b044804cf731cd7dd79000b7c6abce7b642402b275c1eb25712607fc1e5e3d2b']

Name

61b4cca67762a4cf31209056ea17b6fb212e175ca330015d804122ee6481688e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'61b4cca67762a4cf31209056ea17b6fb212e175ca330015d804122ee6481688e']

Name

2576a166d3b18eafc2e35a7de3e5549419d10ce62e0eeb24bad5a1daaa257528

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'2576a166d3b18eafc2e35a7de3e5549419d10ce62e0eeb24bad5a1daaa257528']

Malware

Name
MoqHao

Name
MoqHao

Intrusion-Set

Name
Roaming Mantis

Name
Roaming Mantis

Attack-Pattern

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn’t require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Country

Name
Germany
Name
France
Name
India
Name
Japan
Name
British Indian Ocean Territory
Name
Germany
Name
France

Name
India

Name
Japan

Name
British Indian Ocean Territory

Sector

Name	Description
Technologies	Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Technologies	Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

StixFile

Value
f6323f8d8cfa4b5053c65f8c1862a8e6844b35b260f61735b3cf8d19990fef42
e72f46f15e50ce7cee5c4c0c5a5277e8be4bb3dd23d08ea79e1deacb8f004136
bf102125a6fca5e96aed855b45bbed9aa0bc964198ce207f2e63a71487ad793a
b044804cf731cd7dd79000b7c6abce7b642402b275c1eb25712607fc1e5e3d2b
61b4cca67762a4cf31209056ea17b6fb212e175ca330015d804122ee6481688e
2576a166d3b18eafc2e35a7de3e5549419d10ce62e0eeb24bad5a1daaa257528
f6323f8d8cfa4b5053c65f8c1862a8e6844b35b260f61735b3cf8d19990fef42
e72f46f15e50ce7cee5c4c0c5a5277e8be4bb3dd23d08ea79e1deacb8f004136
bf102125a6fca5e96aed855b45bbed9aa0bc964198ce207f2e63a71487ad793a
b044804cf731cd7dd79000b7c6abce7b642402b275c1eb25712607fc1e5e3d2b
61b4cca67762a4cf31209056ea17b6fb212e175ca330015d804122ee6481688e
2576a166d3b18eafc2e35a7de3e5549419d10ce62e0eeb24bad5a1daaa257528

External References

- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-evolution-new-variants-start-automatically-right-after-installation/
- https://otx.alienvault.com/pulse/65c6368f806499197ff51125