

SolarMarker: Hunt Insights and Findings

 hunt.io/blog/solarmarker-hunt-insight-and-findings

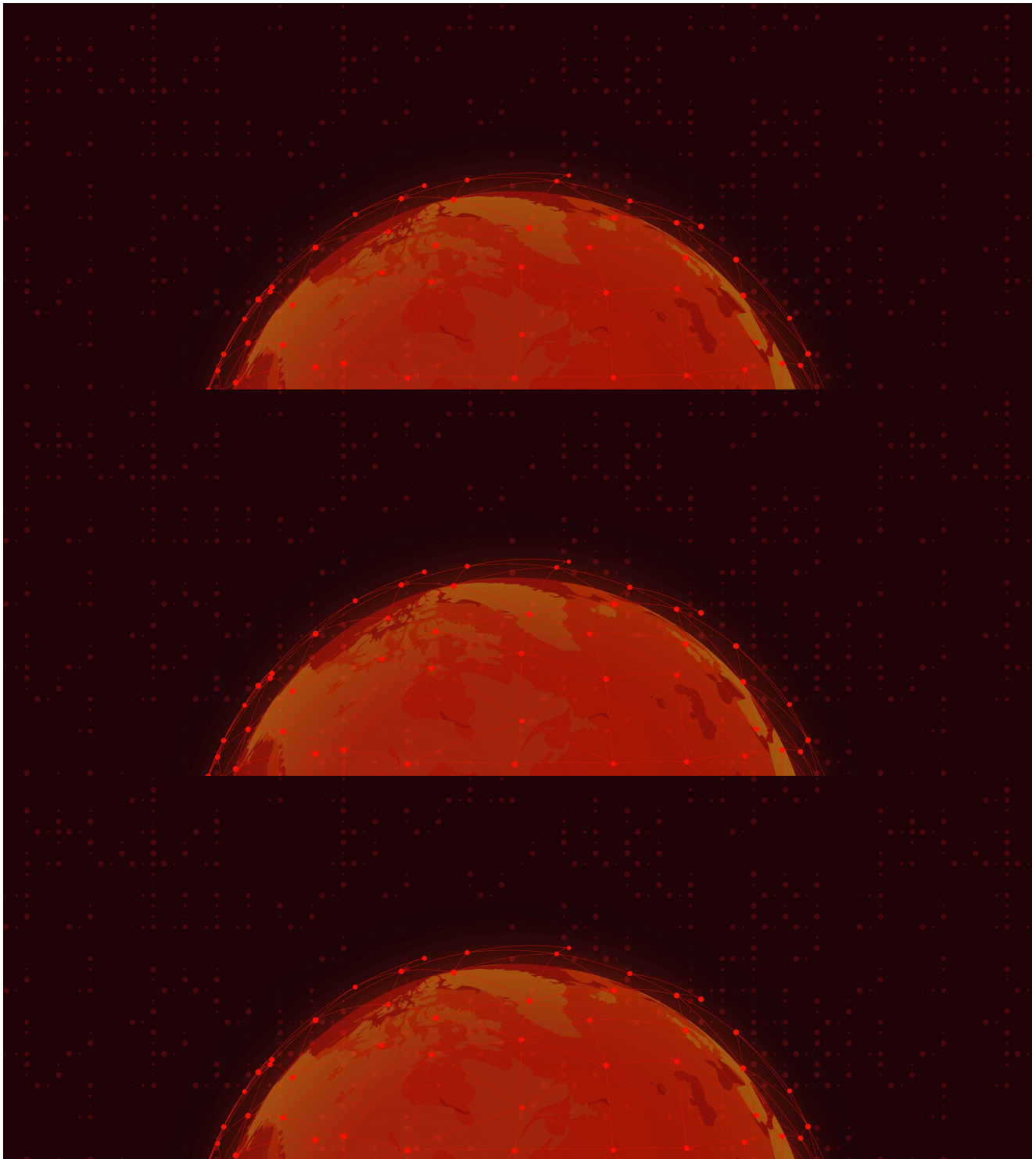


TABLE OF CONTENTS

Introduction

Following Recorded Future's (RF) report, "[Exploring the Depths of SolarMarker's Multi-tiered Infrastructure](#)," the Hunt Research Team leveraged the IOCs provided to discover a method of identifying clusters of SolarMarker servers in the wild.

Our scanning has uncovered 20 servers we believe with moderate confidence are associated with SolarMarker. While the RF report extensively covers SolarMarker's info-stealing capabilities, our focus here will be on the malware's infrastructure.

We will hold off on providing detection queries for SolarMarker servers for now. However, we will cover some observations, including the threat actor's choice of hosting providers, reused SSH keys associated with over 100 servers, and likely phishing domains consistent with SolarMarker targeting.

Overview of Infrastructure

Most of the servers we've identified align with the above report's configuration description for tier 1 servers (Nginx server, ports 22 & 80). One IP deviated from this pattern using port 443 and a Let's Encrypt TLS certificate.

The tier 1 servers are responsible for relaying victim data to higher-tier servers. The below image from the report provides an example of SolarMarkers [C2 infrastructure](#).

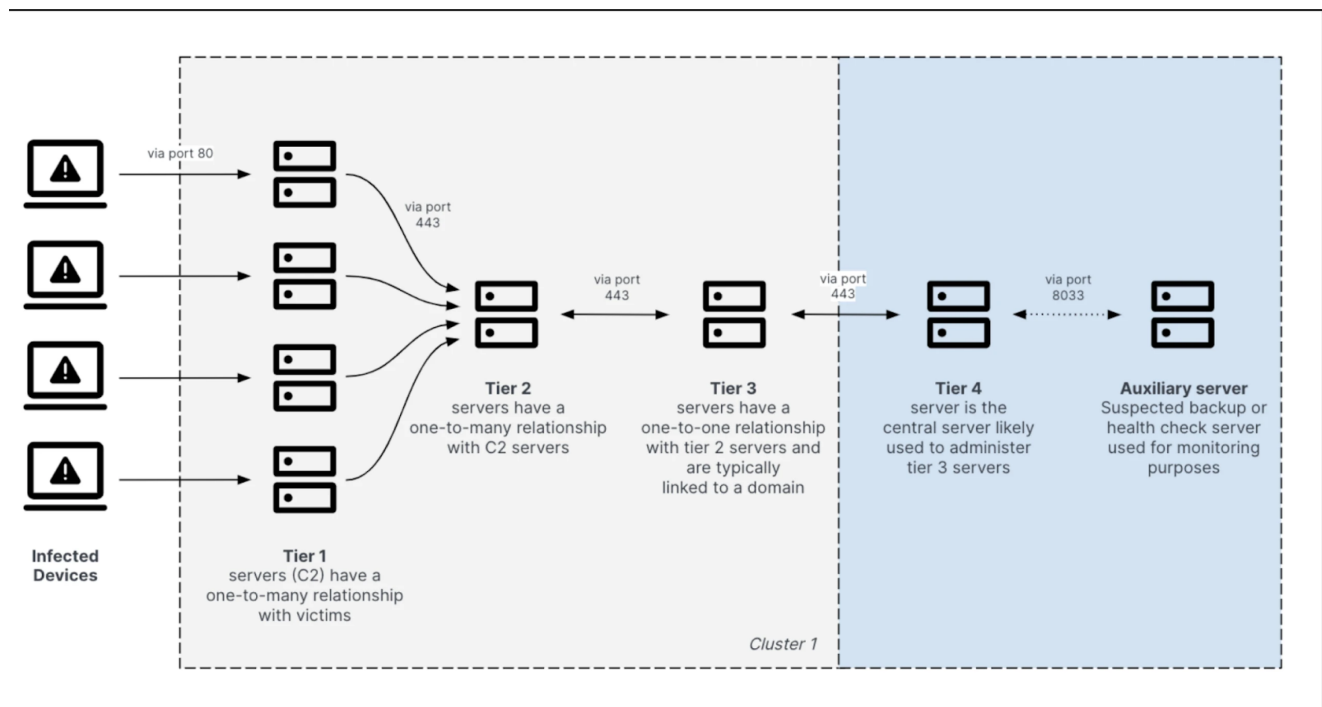


Image 1: SolarMarker's Tiered Infrastructure (Source: [Recorded Future](#), accessed 21 May 2024)

SolarMarker Infrastructure in Hunt

As detailed in various blog posts and vendor reports, SolarMarker not only engages in information stealing but is also capable of executing commands via a backdoor and utilizing hidden virtual network computing (hVNC).

Figure 1 illustrates the most popular ports, hosting companies, and hosting locations based on our scans.

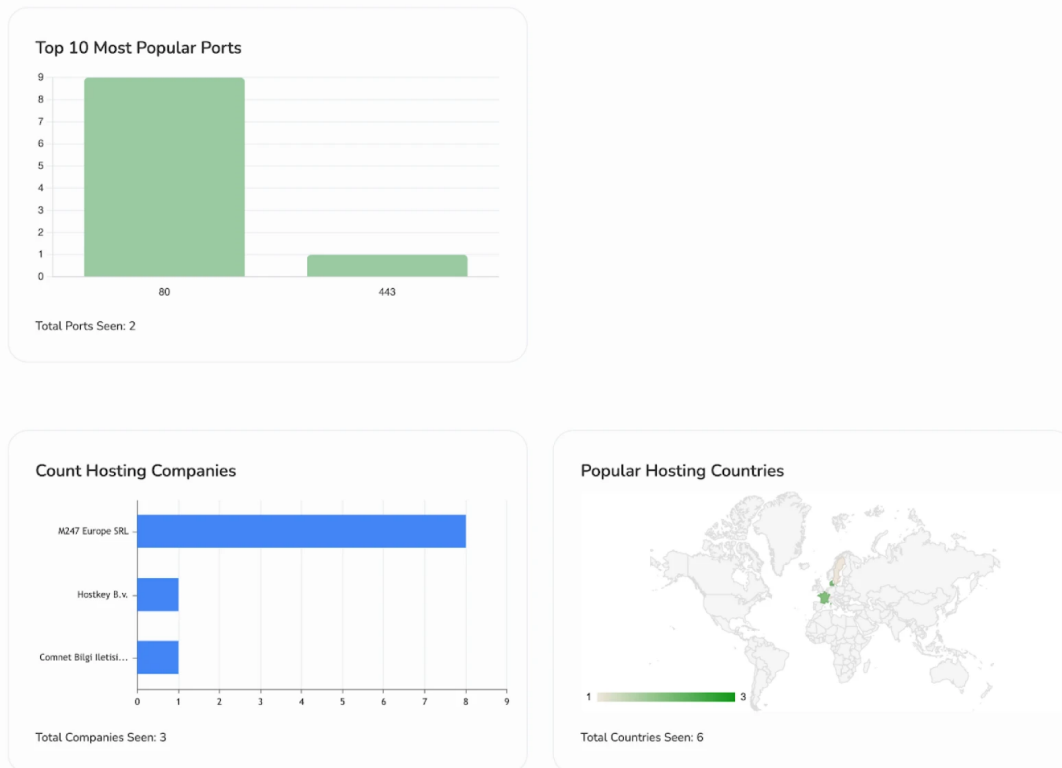


Figure 1: Distribution of Popular Ports, Hosting Companies, and Hosting Locations for SolarMarker IPs

It should come as no surprise that port 80 constitutes the bulk of SolarMarker detections. Infected devices communicate via HTTP POST requests on this port.

If you track malicious infrastructure, you are likely familiar with the M247 network. This ASN accounts for the majority of our findings across SolarMarker's infrastructure. Most of the malicious servers are located in Europe, with the U.S. following closely behind, which again aligns with threat reporting.

Figure 2 shows a snippet of the IPs readily available to Hunt users for deeper analysis.

The Insikt Group identified many of the servers shown in the image. However, we have also found a few that have not been publicly reported.

SolarMarker Detail

Records: 10 (10 Unique IPs)

IP Addresses	Domains	Ports	Admin Ports	Actor	Last Seen First Seen
78.135.73.176 Türkiye Comnet Bilgi İletisim Teknolojileri Ticaret A.s.	-	80		-	58 minutes ago 6 months ago
146.70.71.135 Zurich, Switzerland M247 Europe SRL	-	80		-	58 minutes ago 4 hours ago
193.29.104.25 Paris, France M247 Europe SRL	-	80		-	58 minutes ago 5 months ago
217.138.215.79 Amsterdam, The Netherlands M247 Europe SRL	-	80		-	58 minutes ago 4 hours ago
146.70.40.234 Paris, France M247 Europe SRL	-	443		-	58 minutes ago 4 hours ago
146.70.80.66 Copenhagen, Denmark M247 Europe SRL	-	80		-	58 minutes ago 4 hours ago
146.70.145.242 Stockholm, Sweden M247 Europe SRL	-	80		-	58 minutes ago 4 months ago

Figure 2: Snippet of SolarMarker Associated IP Addresses

Findings and Observations

Our first notable finding is that, although many servers operate on the M247 Europe SRL ASN, these servers are hosted on different subsidiaries, such as the one shown in Figure 3, hosted at M247 LTD Paris Infrastructure.

The threat actor's choice to use different M247 European subsidiaries, such as M247 Europe SRL, appears to be a strategic decision aligned with their targeting objectives. This approach could allow for targeting victims in specific regions by blending in so as not to raise the suspicions of network defenders.

Conversely, the preference for M247, a network known to host malicious content, may reflect the threat actor's tactic of leveraging a reliable and familiar infrastructure to maintain and expand their operations.

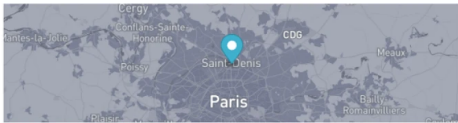
In either case, using various subsidiaries showcases a deliberate tactic in infrastructure management. This strategy potentially enhances the actor's ability to evade detection and sustain their malicious activities across multiple regions.

193.29.104.25 - Overview

Info Domains 0 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

193.29.104.25

M247 LTD Paris Infrastructure



Saint-Denis, Île-de-France, FR

DNS

Reverse DNS	Unused
Forward DNS	Not available
Tag	Not available

ASN

AS9009	193.29.104.0/24	M247 Europe SRL
--------	-----------------	-----------------

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
SSH	22	-	-	-	1 day ago	1 year ago
HTTP	80	-	-	-	6 hours ago	1 year ago

Figure 3: SolarMarker Servers Hosted on M247 Subsidiaries

Additional M247 locations were observed in Stockholm, Amsterdam, Copenhagen, and Zurich.

The Oddball

Out of the 20 results for SolarMarker infrastructure, our query found only one IP that did not use the standard port 80. The IP, 146.70.40_234, has a C2 configuration match on port 443 and has ports 22, 80, and 3306 open.

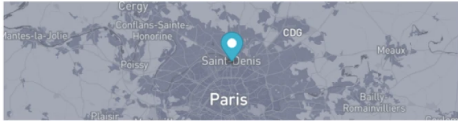
This IP hosts a Let's Encrypt TLS certificate with the domain barekaz[.]com as the issuer common name.

146.70.40.234 - Overview

Info Domains 1 History (Beta) Associations 199 SSL History SSH History JARM Port History Signals Activity 0

146.70.40.234

M247 LTD Paris Infrastructure



Saint-Denis, Île-de-France, FR

DNS

Reverse DNS: undefined

Forward DNS: barekaz.com... 1

Tag

ASN

AS9009 146.70.40.0/24 M247 Europe SRL

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
HTTP	80	nginx	1.14.2	-	4 days ago	1 year ago
TLS/HTTP	443	-	-	-	4 days ago	1 year ago
MYSQL	3306	-	-	-	4 days ago	1 year ago
SSH	22	-	-	-	1 day ago	1 year ago

Figure 4: Suspected SolarMarker Infrastructure on Port 443

Figure 5 shows data for the certificate, including the JA4X hash and fingerprints.

Home > Certificate

Certificate data

Certificate: C76116690A6190601F6C0C8458A6C4EAAF0E4E582C3FEB3093CCD63684B76A27 Collapse

General Details

Issued To

Common Name (CN)
barekaz.com

Organisation (O)
< Not part of certificate >

Organisational Unit (OU)
< Not part of certificate >

Issued By

Common Name (CN)
R3

Organisation (O)
Let's Encrypt

Organisational Unit (OU)
< Not part of certificate >

Validity Period

Issued On
Wednesday, 22 May, 2024 03:14:13

Expires On
Tuesday, 20 August, 2024 03:14:12

Fingerprints

SHA-256 Fingerprint
efbfb6116690a61efbfb601f6c0cefbbfbd58efbfb0e4e582c3fefbfb30efbfb36efbfb6a27

SHA-1 Fingerprint
efbfb2906316358566efbfbdd98befbfb406221137a4c

JA4X

JA4X
a373a9f63c6b_7022c563de38_821a8ec155c6 (11.516.482)

Figure 5: TLS Certificate for 146.70.40_234

Little information was available for the domain, and attempts to contact it resulted in an HTTP 404 Not Found error.

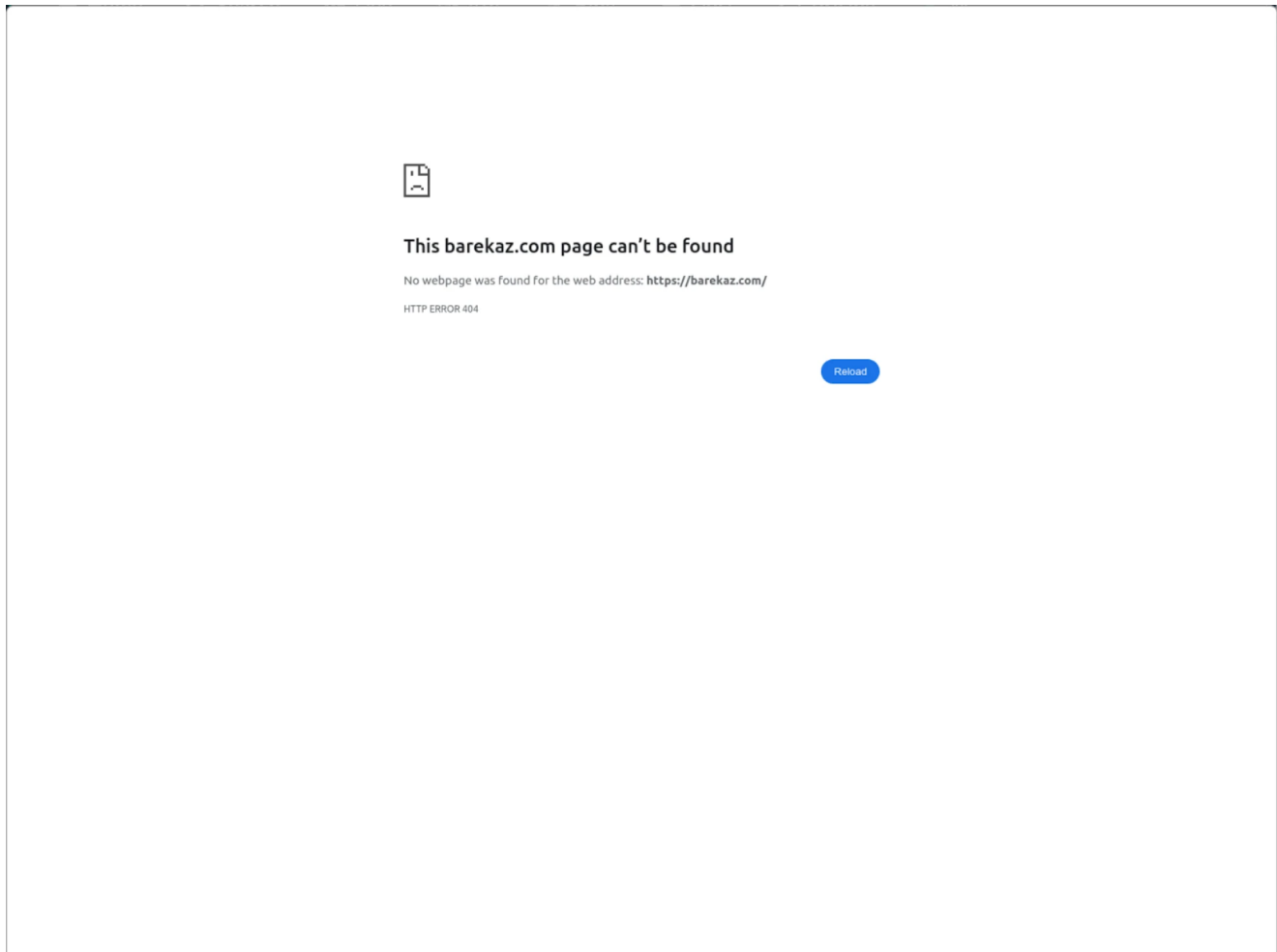


Figure 6: 404 Error For Certificate Domain

Shared SSH Keys

With an infrastructure of multiple tiers that handle various infection operations, a lone individual is unlikely to conduct server management.

The actor maintained solid operational security (OPSEC) by using separate SSH keys for many of the C2 servers, except for one instance. One of those servers, 217.138.215_79, hosted an SSH key that we pivoted on and found over 100 other servers using the same key.

The below view is an example of using the "Associations" tab in Hunt.

217.138.215.79 - Overview

Info Domains 0 History (Beta) Associations 310 SSL History SSH History JARM Port History Signals Activity 0

Public SSH Keys (116) IOCs (194) Malware configs (0) Certificates (0) Redirects (0)

Public SSH Keys

IP	SSH Fingerprint	First Seen	Last Seen
194.15.216.232 Artnet Sp. z o.o. Poland Artnet Sp. z o.o. 197155	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-04-12 05:14	2024-04-12 05:14
84.252.94.179 M247 LTD London Infrastructure United Kingdom M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 80944a6b5c020077411bc17f85f86c32ea13b0b735b090b309259f51772aaff7 a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-23 04:45	2024-05-20 02:54
146.70.106.174 M247 Europe - Amsterdam Infrastructure Netherlands M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-24 04:56	2024-05-15 04:42
84.247.51.183 M247 LTD Paris Infrastructure France M247 Europe SRL 9009	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e	2024-03-07 04:50	2024-03-07 04:50

Figure 7: Snippet of IPs Sharing the Same SSH Keys

Similarly, the SSH History tab provides detailed information, including the SSH version, first and last seen dates/times, and similar IPs.

This particular instance uses SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1.

217.138.215.79 - Overview

Info Domains 0 History (Beta) Associations 310 SSL History SSH History JARM Port History Signals Activity 0

Public SSH Keys (116) IOCs (194) Malware configs (0) Certificates (0) Redirects (0)

Public SSH Keys

IP	SSH Fingerprint	First Seen	Last Seen
194.15.216.232 Artnet Sp. z o.o. Poland Artnet Sp. z o.o. 197155	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-04-12 05:14	2024-04-12 05:14
84.252.94.179 M247 LTD London Infrastructure United Kingdom M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 80944a6b5c020077411bc17f85f86c32ea13b0b735b090b309259f51772aaff7 a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-23 04:45	2024-05-20 02:54
146.70.106.174 M247 Europe - Amsterdam Infrastructure Netherlands M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-24 04:56	2024-05-15 04:42
84.247.51.183 M247 LTD Paris Infrastructure France M247 Europe SRL 9009	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e	2024-03-07 04:50	2024-03-07 04:50

Figure 8: Screenshot of SSH History tab in Hunt

We won't cover all 100+ servers, but we will examine a few that caught my eye during the research and are still active as of this writing.

Sliver & Raccoon Stealer

IP addresses 185.17.40_153 and 146.70.106_171 hosted instances of the open-source adversary emulation framework Sliver (<https://github.com/BishopFox/sliver>) during the same period as the shared SSH key.

In early 2023, the IP ending in .171 also hosted Raccoon Stealer on port 80. We will use the History feature to examine the timeline of the ports and services to understand how they overlap.

*The SSH hash beginning with "354408..." is the shared key.

146.70.106.171 - Overview

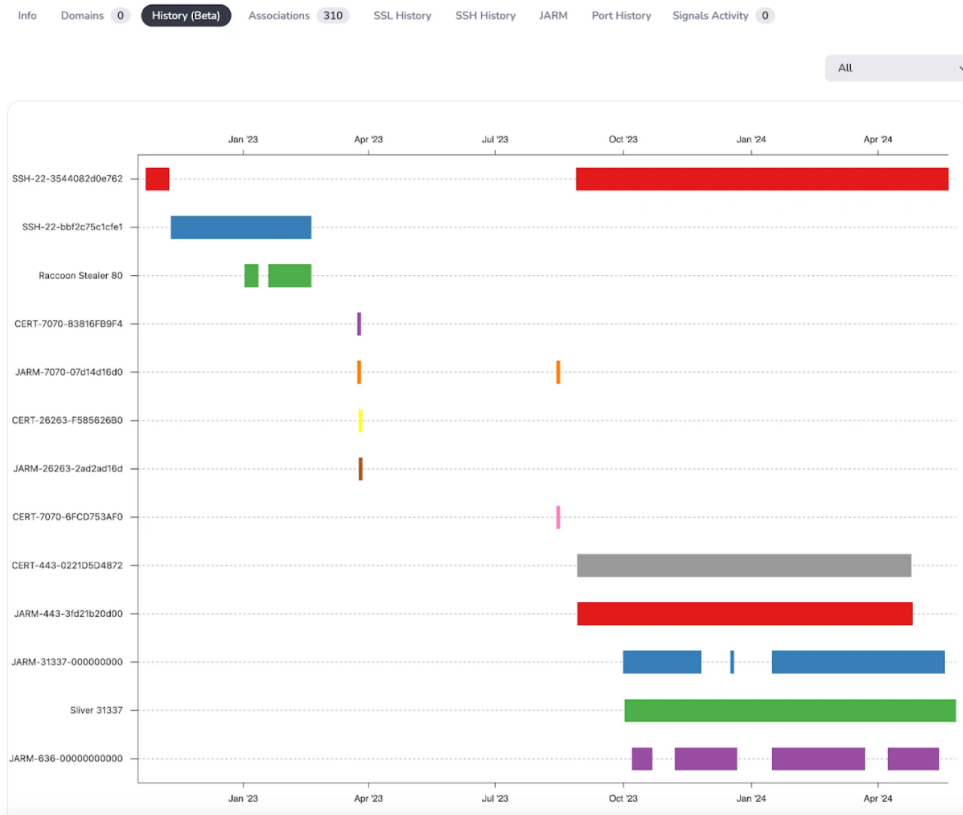


Figure 9: SSH Associated IP Hosting Sliver and Raccoon Stealer

185.17.40.153 - Overview





Figure 10: SSH Associated IP Hosting Sliver

Interesting Domains

89.238.185.16- Overview

Info **Domains 2** History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

1-2 of 2 results « Previous Next »

Hostname	Rank
 gigmbwin.com	-
 grvnews.live	-

1-2 of 2 results « Previous Next »

Figure 11: Domain previously Associated With Lycantrox Infrastructure


grvnews.live was previously identified as associated with Lycantrox infrastructure, as detailed in this SEKOIA blog post: <https://blog.sekoia.io/active-lycantrox-infrastructure-illumination/>.

Hunt first detected the SSH key on the server in July 2023, and according to PDNS records, the domain began resolving to the IP shortly after that in August.

It is important to clarify that this is not an attempt to link Lycantrox and SolarMarker but to highlight different actors' reuse of IP addresses.

Interac Spoofed Domain

188.116.34_204 currently hosts two domains, interac-financial[.]com and colminek[.]com. The former is likely an attempt to impersonate a legitimate Canadian company that facilitates electronic financial transactions between businesses and banks.



 Log Out

Home > Domains List 188.116.34.204

188.116.34.204- Overview

Info **Domains 2** History (Beta) Associations 472 SSL History SSH History JARM Port History Signals Activity 0

1-2 of 2 results « Previous Next »

Hostname	Rank
 colminek.com	-
 interac-financial.com	-

1-2 of 2 results « Previous Next »

Figure 12: IP Hosting Likely Phishing Domain

Similar to the previously mentioned domain, this domain also returns a 404 error.

E-Payment Provider Spoofed Domain




Three domains were found on IP address 2.58.15_58: mail.myfawry[.]net, myfawry[.]net, and [www.myfawry\[.\]net](http://www.myfawry[.]net). These domains are likely attempting to spoof Fawry, an e-payment and digital finance solutions provider in Egypt. In an ongoing theme, all three domains return a 404 error.

Home > Domains List 2.58.15.58

2.58.15.58- Overview

Info Domains (3) History (Beta) Associations (80) SSL History SSH History JARM Port History Signals Activity (0)

1-3 of 3 results « Previous Next »

Hostname	Rank
 mail.myfawry.net	-
 myfawry.net	-
 www.myfawry.net	-

1-3 of 3 results « Previous Next »

Figure 13: SSH Key Linked IP Hosting Suspicious Domains

We have some work to do with so many IPs to pivot on for the shared SSH key. If we find anything significant, we'll consider an additional blog post or post on X to keep the community informed.

Please follow our X/Twitter account, [@Huntio](https://twitter.com/Huntio), to stay updated on our findings and future blogs.

Wrap-Up

In this blog post, we explored SolarMarker's infrastructure, uncovering key IP addresses, domains, and server configurations associated with the malware. Our findings revealed intriguing patterns, such as the reuse of IP addresses and SSH keys by different threat actors and the strategic use of various hosting providers.

Join us in uncovering more links to SolarMarker

Apply for an account today and gain access to our comprehensive tools and scan data to detect and mitigate the threat SolarMarker poses.

[Apply Now](#)

Indicators

SolarMarker IP Addresses

2.58.14_183

2.58.15_58

2.58.15_214

23.29.115_186

45.86.163_163

46.17.96_139

46.30.188_221

68.233.238_123

78.135.73_176

146.70.40_234

146.70.71_135

146.70.80_66

146.70.80_83

146.70.145_242

185.243.115_88

193.29.104_25

212_237.217_133

217.138.215_79

217.138.215_105

SSH Key SHA-256 Fingerprint

Vkftcw/Kyybnc6sIHBv3WSdmVZzb3/4QFfxUUfPCEQ4=

TLS Cert SHA-256 Fingerprint

efbfd6116690a61efbfd601f6c0cefbfd58efbfd0e4e582c3fefbfd30efbfd36efbfd6a27

Introduction

Following Recorded Future's (RF) report, "[Exploring the Depths of SolarMarker's Multi-tiered Infrastructure](#)," the Hunt Research Team leveraged the IOCs provided to discover a method of identifying clusters of SolarMarker servers in the wild.

Our scanning has uncovered 20 servers we believe with moderate confidence are associated with SolarMarker. While the RF report extensively covers SolarMarker's info-stealing capabilities, our focus here will be on the malware's infrastructure.

We will hold off on providing detection queries for SolarMarker servers for now. However, we will cover some observations, including the threat actor's choice of hosting providers, reused SSH keys associated with over 100 servers, and likely phishing domains consistent with SolarMarker targeting.

Overview of Infrastructure

Most of the servers we've identified align with the above report's configuration description for tier 1 servers (Nginx server, ports 22 & 80). One IP deviated from this pattern using port 443 and a Let's Encrypt TLS certificate.

The tier 1 servers are responsible for relaying victim data to higher-tier servers. The below image from the report provides an example of SolarMarkers [C2 infrastructure](#).

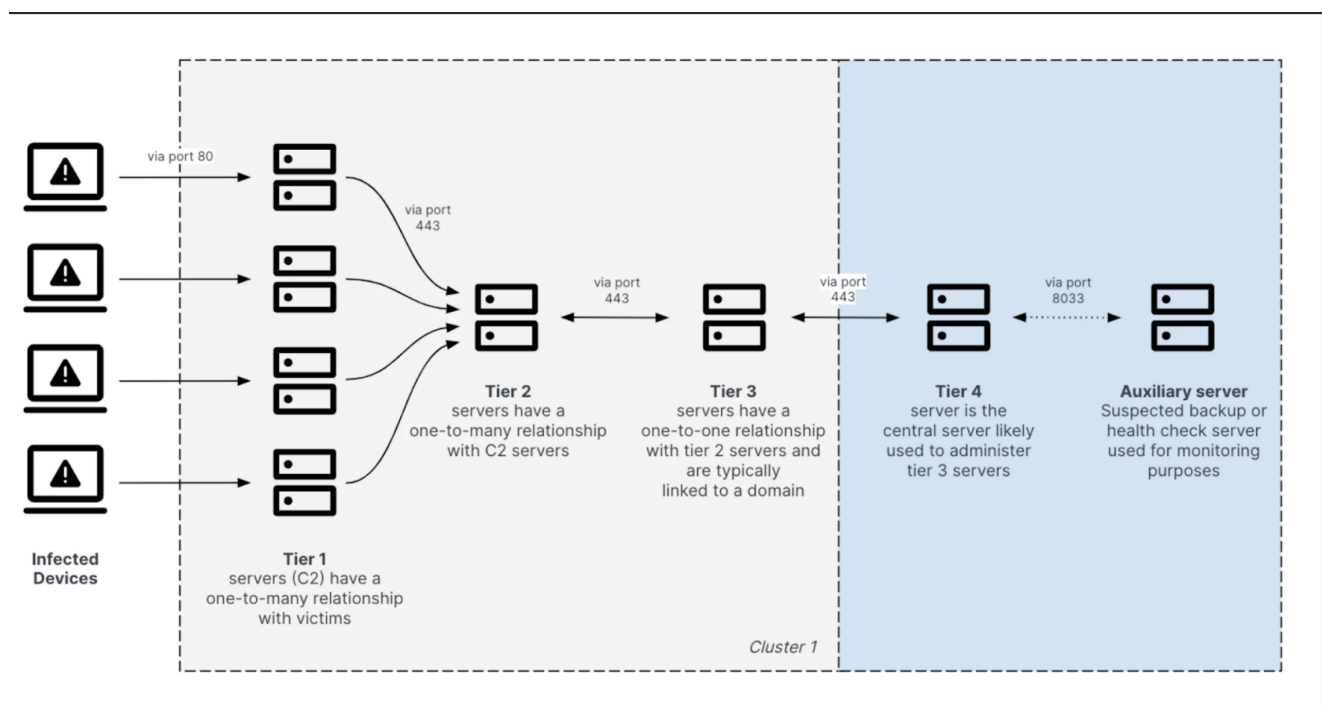


Image 1: SolarMarker's Tiered Infrastructure (Source: [Recorded Future](#), accessed 21 May 2024)

SolarMarker Infrastructure in Hunt

As detailed in various blog posts and vendor reports, SolarMarker not only engages in information stealing but is also capable of executing commands via a backdoor and utilizing hidden virtual network computing (hVNC).

Figure 1 illustrates the most popular ports, hosting companies, and hosting locations based on our scans.

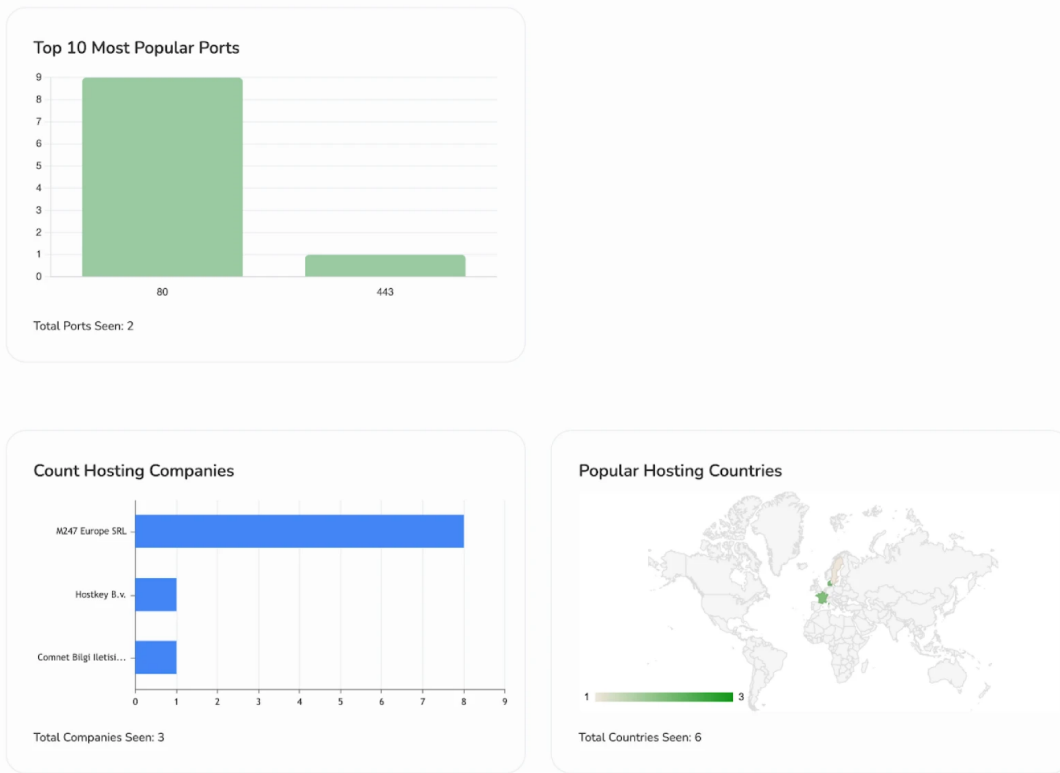


Figure 1: Distribution of Popular Ports, Hosting Companies, and Hosting Locations for SolarMarker IPs

It should come as no surprise that port 80 constitutes the bulk of SolarMarker detections. Infected devices communicate via HTTP POST requests on this port.

If you track malicious infrastructure, you are likely familiar with the M247 network. This ASN accounts for the majority of our findings across SolarMarker's infrastructure. Most of the malicious servers are located in Europe, with the U.S. following closely behind, which again aligns with threat reporting.

Figure 2 shows a snippet of the IPs readily available to Hunt users for deeper analysis.

The Insikt Group identified many of the servers shown in the image. However, we have also found a few that have not been publicly reported.

SolarMarker Detail

Records: 10 (10 Unique IPs)

IP Addresses	Domains	Ports	Admin Ports	Actor	Last Seen First Seen
78.135.73.176 Türkiye Comnet Bilgi İletisim Teknolojileri Ticaret A.s.	-	80		-	58 minutes ago 6 months ago
146.70.71.135 Zurich, Switzerland M247 Europe SRL	-	80		-	58 minutes ago 4 hours ago
193.29.104.25 Paris, France M247 Europe SRL	-	80		-	58 minutes ago 5 months ago
217.138.215.79 Amsterdam, The Netherlands M247 Europe SRL	-	80		-	58 minutes ago 4 hours ago
146.70.40.234 Paris, France M247 Europe SRL	-	443		-	58 minutes ago 4 hours ago
146.70.80.66 Copenhagen, Denmark M247 Europe SRL	-	80		-	58 minutes ago 4 hours ago
146.70.145.242 Stockholm, Sweden M247 Europe SRL	-	80		-	58 minutes ago 4 months ago

Figure 2: Snippet of SolarMarker Associated IP Addresses

Findings and Observations

Our first notable finding is that, although many servers operate on the M247 Europe SRL ASN, these servers are hosted on different subsidiaries, such as the one shown in Figure 3, hosted at M247 LTD Paris Infrastructure.

The threat actor's choice to use different M247 European subsidiaries, such as M247 Europe SRL, appears to be a strategic decision aligned with their targeting objectives. This approach could allow for targeting victims in specific regions by blending in so as not to raise the suspicions of network defenders.

Conversely, the preference for M247, a network known to host malicious content, may reflect the threat actor's tactic of leveraging a reliable and familiar infrastructure to maintain and expand their operations.

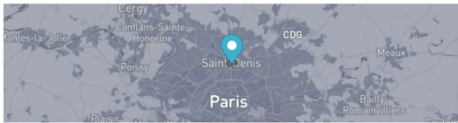
In either case, using various subsidiaries showcases a deliberate tactic in infrastructure management. This strategy potentially enhances the actor's ability to evade detection and sustain their malicious activities across multiple regions.

193.29.104.25 - Overview

Info Domains 0 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

193.29.104.25

M247 LTD Paris Infrastructure



Saint-Denis, Île-de-France, FR

DNS

Reverse DNS	Unused
Forward DNS	Not available
Tag	Not available

ASN

AS9009	193.29.104.0/24	M247 Europe SRL
--------	-----------------	-----------------

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
SSH	22	-	-	-	1 day ago	1 year ago
HTTP	80	-	-	-	6 hours ago	1 year ago

Figure 3: SolarMarker Servers Hosted on M247 Subsidiaries

Additional M247 locations were observed in Stockholm, Amsterdam, Copenhagen, and Zurich.

The Oddball

Out of the 20 results for SolarMarker infrastructure, our query found only one IP that did not use the standard port 80. The IP, 146.70.40_234, has a C2 configuration match on port 443 and has ports 22, 80, and 3306 open.

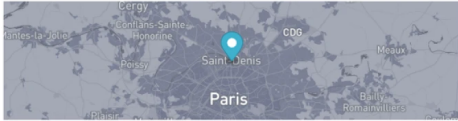
This IP hosts a Let's Encrypt TLS certificate with the domain barekaz[.]com as the issuer common name.

146.70.40.234 - Overview

Info Domains 1 History (Beta) Associations 199 SSL History SSH History JARM Port History Signals Activity 0

146.70.40.234

M247 LTD Paris Infrastructure



Saint-Denis, Île-de-France, FR

DNS

Reverse DNS: undefined

Forward DNS: barekaz.com... 1

Tag

ASN

AS9009 146.70.40.0/24 M247 Europe SRL

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
HTTP	80	nginx	1.14.2	-	4 days ago 1 year ago	🔍
TLS/HTTP	443	-	-	-	4 days ago 1 year ago	🔍 🚫
MYSQL	3306	-	-	-	4 days ago 1 year ago	🔍
SSH	22	-	-	-	1 day ago 1 year ago	🔍

Figure 4: Suspected SolarMarker Infrastructure on Port 443

Figure 5 shows data for the certificate, including the JA4X hash and fingerprints.

Home > Certificate

Certificate data

Certificate: C76116690A6190601F6C0C8458A6C4EAAF0E4E582C3FEB3093CCD63684B76A27 [Collapse](#)

General Details

Issued To

Common Name (CN)
barekaz.com

Organisation (O)
< Not part of certificate >

Organisational Unit (OU)
< Not part of certificate >

Issued By

Common Name (CN)
R3

Organisation (O)
Let's Encrypt

Organisational Unit (OU)
< Not part of certificate >

Validity Period

Issued On
Wednesday, 22 May, 2024 03:14:13

Expires On
Tuesday, 20 August, 2024 03:14:12

Fingerprints

SHA-256 Fingerprint
efbfb6116690a61efbfb601f6c0cefbbfbd58efbfb0e4e582c3fefbfb30efbfb36efbfb6a27

SHA-1 Fingerprint
efbfb2906316358566efbfbdd98befbfb406221137a4c

JA4X

JA4X
a373a9f83c6b 7022c563da38 821a8ec155c6 (11.516.482)

Figure 5: TLS Certificate for 146.70.40_234

Little information was available for the domain, and attempts to contact it resulted in an HTTP 404 Not Found error.

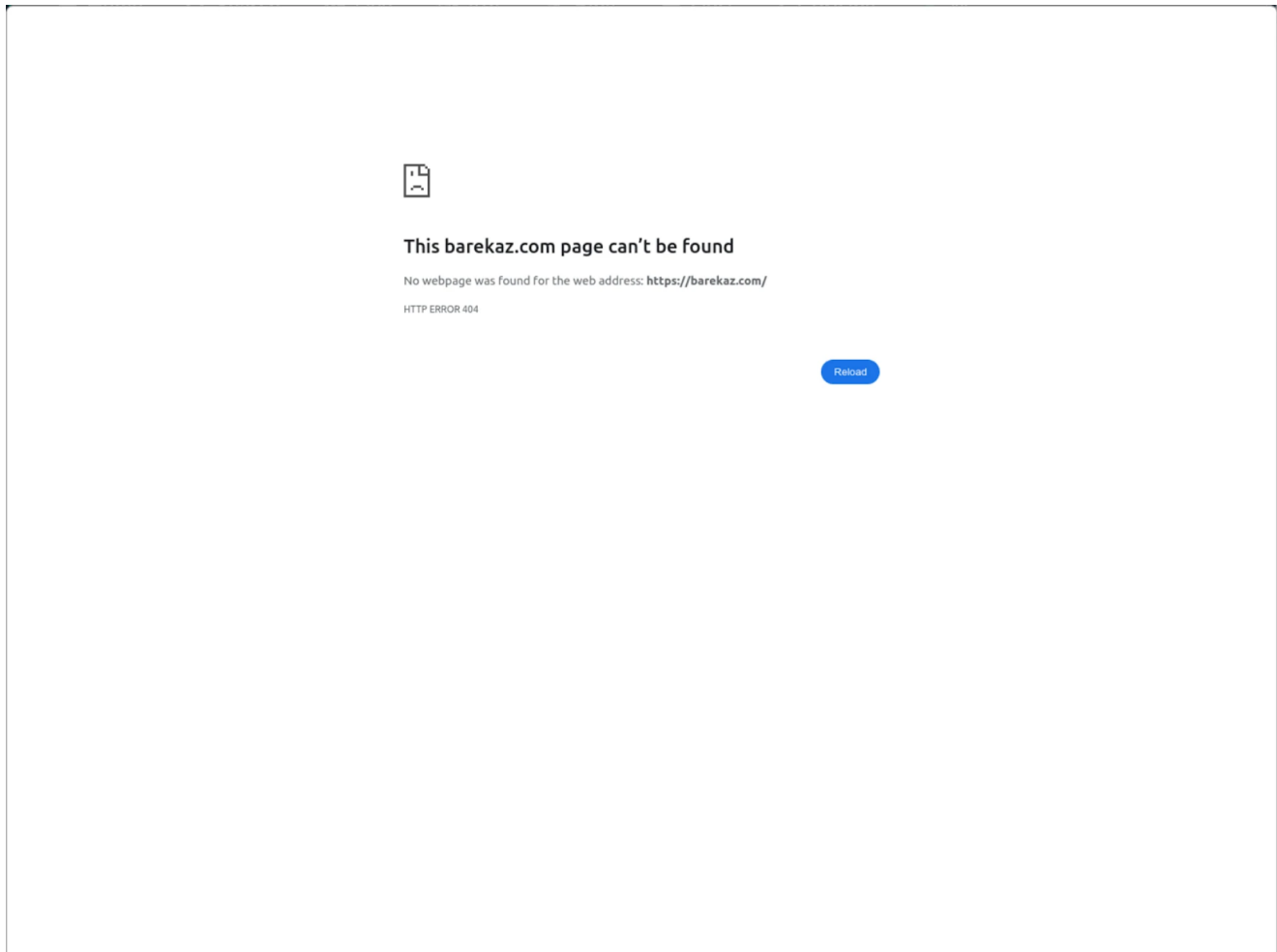


Figure 6: 404 Error For Certificate Domain

Shared SSH Keys

With an infrastructure of multiple tiers that handle various infection operations, a lone individual is unlikely to conduct server management.

The actor maintained solid operational security (OPSEC) by using separate SSH keys for many of the C2 servers, except for one instance. One of those servers, 217.138.215_79, hosted an SSH key that we pivoted on and found over 100 other servers using the same key.

The below view is an example of using the "Associations" tab in Hunt.

217.138.215.79 - Overview

Info Domains 0 History (Beta) Associations 310 SSL History SSH History JARM Port History Signals Activity 0

Public SSH Keys (116) IOCs (194) Malware configs (0) Certificates (0) Redirects (0)

Public SSH Keys

IP	SSH Fingerprint	First Seen	Last Seen
194.15.216.232 Artnet Sp. z o.o. Poland Artnet Sp. z o.o. 197155	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-04-12 05:14	2024-04-12 05:14
84.252.94.179 M247 LTD London Infrastructure United Kingdom M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 80944a6b5c020077411bc17f85f86c32ea13b0b735b090b309259f51772aaff7 a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-23 04:45	2024-05-20 02:54
146.70.106.174 M247 Europe - Amsterdam Infrastructure Netherlands M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-24 04:56	2024-05-15 04:42
84.247.51.183 M247 LTD Paris Infrastructure France M247 Europe SRL 9009	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e	2024-03-07 04:50	2024-03-07 04:50

Figure 7: Snippet of IPs Sharing the Same SSH Keys

Similarly, the SSH History tab provides detailed information, including the SSH version, first and last seen dates/times, and similar IPs.

This particular instance uses SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1.

217.138.215.79 - Overview

Info Domains 0 History (Beta) Associations 310 SSL History SSH History JARM Port History Signals Activity 0

Public SSH Keys (116) IOCs (194) Malware configs (0) Certificates (0) Redirects (0)

Public SSH Keys

IP	SSH Fingerprint	First Seen	Last Seen
194.15.216.232 Artnet Sp. z o.o. Poland Artnet Sp. z o.o. 197155	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-04-12 05:14	2024-04-12 05:14
84.252.94.179 M247 LTD London Infrastructure United Kingdom M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 80944a6b5c020077411bc17f85f86c32ea13b0b735b090b309259f51772aaff7 a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-23 04:45	2024-05-20 02:54
146.70.106.174 M247 Europe - Amsterdam Infrastructure Netherlands M247 Europe SRL 9009	4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e a64e23960ee8963b5638cba67da4caf0b14a488db23fa17d078d2a631969f5e5	2024-02-24 04:56	2024-05-15 04:42
84.247.51.183 M247 LTD Paris Infrastructure France M247 Europe SRL 9009	b44395cad82cc87a080896364b8a8759a867f9691ff8ca391ad13a8c3c3be0db 4b8b3898c9034b14386799434c23ecfaba1fa96ba5051fcbd46344f380b15c2e	2024-03-07 04:50	2024-03-07 04:50

Figure 8: Screenshot of SSH History tab in Hunt

We won't cover all 100+ servers, but we will examine a few that caught my eye during the research and are still active as of this writing.

Sliver & Raccoon Stealer

IP addresses 185.17.40_153 and 146.70.106_171 hosted instances of the open-source adversary emulation framework Sliver (<https://github.com/BishopFox/sliver>) during the same period as the shared SSH key.

In early 2023, the IP ending in .171 also hosted Raccoon Stealer on port 80. We will use the History feature to examine the timeline of the ports and services to understand how they overlap.

*The SSH hash beginning with "354408..." is the shared key.

146.70.106.171 - Overview

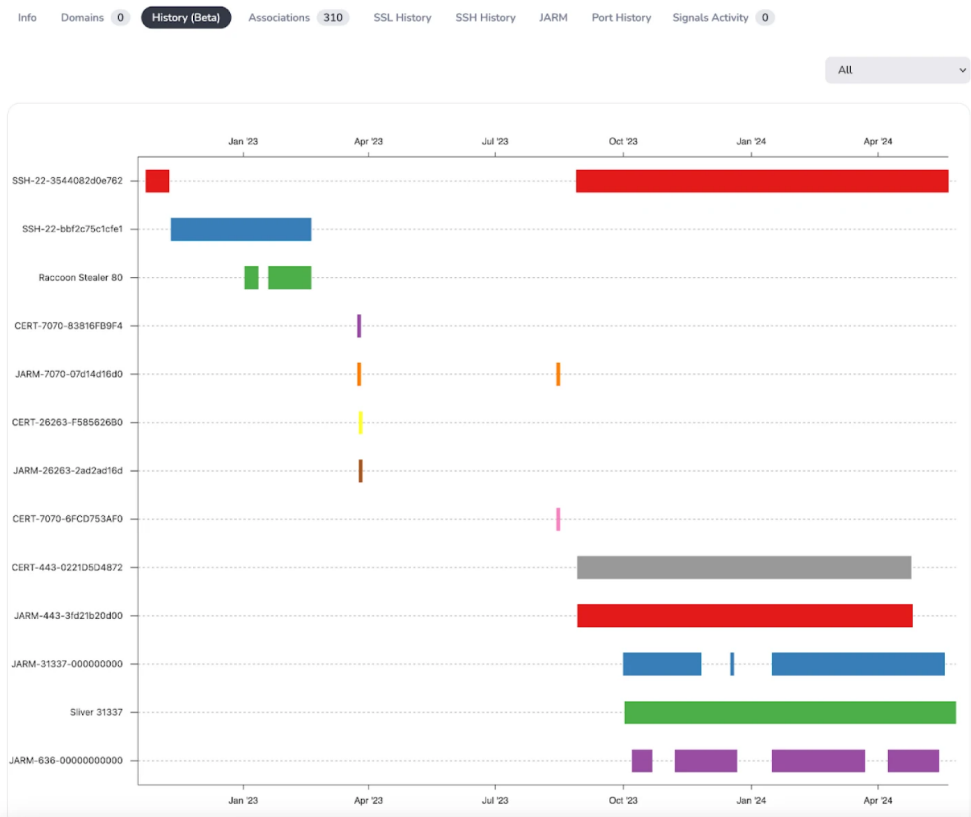


Figure 9: SSH Associated IP Hosting Sliver and Raccoon Stealer

185.17.40.153 - Overview





Figure 10: SSH Associated IP Hosting Sliver

Interesting Domains

89.238.185.16- Overview

Info **Domains 2** History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

1-2 of 2 results « Previous Next »

Hostname	Rank
 gigmbwin.com	-
 grvnews.live	-

1-2 of 2 results « Previous Next »

Figure 11: Domain previously Associated With Lycantrox Infrastructure


grvnews.live was previously identified as associated with Lycantrox infrastructure, as detailed in this SEKOIA blog post: <https://blog.sekoia.io/active-lycantrox-infrastructure-illumination/>.

Hunt first detected the SSH key on the server in July 2023, and according to PDNS records, the domain began resolving to the IP shortly after that in August.

It is important to clarify that this is not an attempt to link Lycantrox and SolarMarker but to highlight different actors' reuse of IP addresses.

Interac Spoofed Domain

188.116.34_204 currently hosts two domains, interac-financial[.]com and colminek[.]com. The former is likely an attempt to impersonate a legitimate Canadian company that facilitates electronic financial transactions between businesses and banks.



 Log Out

Home > Domains List 188.116.34.204

188.116.34.204- Overview

Info **Domains 2** History (Beta) Associations 472 SSL History SSH History JARM Port History Signals Activity 0

1-2 of 2 results « Previous Next »

Hostname	Rank
 colminek.com	-
 interac-financial.com	-

1-2 of 2 results « Previous Next »

Figure 12: IP Hosting Likely Phishing Domain

Similar to the previously mentioned domain, this domain also returns a 404 error.

E-Payment Provider Spoofed Domain




Three domains were found on IP address 2.58.15_58: mail.myfawry[.]net, myfawry[.]net, and [www.myfawry\[.\]net](http://www.myfawry[.]net). These domains are likely attempting to spoof Fawry, an e-payment and digital finance solutions provider in Egypt. In an ongoing theme, all three domains return a 404 error.

Home > Domains List 2.58.15.58

2.58.15.58- Overview

Info **Domains 3** History (Beta) Associations **80** SSL History SSH History JARM Port History Signals Activity **0**

1-3 of 3 results « Previous Next »

Hostname	Rank
 mail.myfawry.net	-
 myfawry.net	-
 www.myfawry.net	-

1-3 of 3 results « Previous Next »

Figure 13: SSH Key Linked IP Hosting Suspicious Domains

We have some work to do with so many IPs to pivot on for the shared SSH key. If we find anything significant, we'll consider an additional blog post or post on X to keep the community informed.

Please follow our X/Twitter account, [@Huntio](https://twitter.com/Huntio), to stay updated on our findings and future blogs.

Wrap-Up

In this blog post, we explored SolarMarker's infrastructure, uncovering key IP addresses, domains, and server configurations associated with the malware. Our findings revealed intriguing patterns, such as the reuse of IP addresses and SSH keys by different threat actors and the strategic use of various hosting providers.

Join us in uncovering more links to SolarMarker

Apply for an account today and gain access to our comprehensive tools and scan data to detect and mitigate the threat SolarMarker poses.

[Apply Now](#)

Indicators

SolarMarker IP Addresses

2.58.14_183

2.58.15_58

2.58.15_214

23.29.115_186

45.86.163_163

46.17.96_139

46.30.188_221

68.233.238_123

78.135.73_176

146.70.40_234

146.70.71_135

146.70.80_66

146.70.80_83

146.70.145_242

185.243.115_88

193.29.104_25

212_237.217_133

217.138.215_79

217.138.215_105

SSH Key SHA-256 Fingerprint

Vkftcw/Kyybnc6sIHBv3WSdmVZzb3/4QFfxUUfPCEQ4=

TLS Cert SHA-256 Fingerprint

efbfd6116690a61efbfd601f6c0cefbfd58efbfd0e4e582c3fefbfd30efbfd36efbfd6a27