“Million OK!!!!” and the Naver Facade: Tracking Recent Suspected Kimsuky Infrastructure

Published: 2024-12-10 · Archived: 2026-04-05 19:25:09 UTC

TABLE OF CONTENTS

In March 2024, a security researcher on Twitter/X observed a series of IP addresses and domains delivering an unusual HTTP response: '**Million OK!!!!**'. Subsequent analysis of the infrastructure and domains linked this activity to the North Korean threat group Kimsuky.

Hunt researchers recently observed additional activity involving recently registered domains returning the same response. These web pages use the favicon of Naver, a South Korean technology corporation, although they have no association with the company. Domain registration information suggests the group is actively maintaining and expanding its infrastructure.

Key observations:

- The reappearance of the 'Million OK!!!!' HTTP response.
- Continued reliance on top-level domains such as **p-e.kr**, **o-r.kr**, and **n-e.kr**, previously associated with Kimsuky.
- Use of Naver branding elements to enhance the credibility of malicious pages.

This post provides an overview of the newly observed domains and infrastructure.

Background: Targeting of Naver

North Korean threat actors, particularly Kimsuky, have repeatedly targeted South Korean platforms like Naver to steal credentials. These campaigns often employ phishing techniques, including counterfeit Naver login pages and tech-themed domain naming conventions.

In June 2023, South Korea's National Intelligence Service identified a phishing website replicating Naver's main page in real-time, aiming to harvest personal data from South Korean users. This past October, Hunt uncovered a phishing campaign targeting Naver users, utilizing exposed directories containing phishing pages designed to steal credentials.

The following section focuses on the domains, IPs, and infrastructure observed in the latest campaign.

Technical Details

This collection of "Million OK !!!!" infrastructure shares several notable traits. All observed IPs are hosted on the UCLOUD Information Technology (HK) Limited ASN, which is hosted in South Korea.

While the exact purpose of the above term remains unclear, it likely serves as a distinctive marker/placeholder for the group's malicious infrastructure to verify active servers.

Some of the distinct behaviors exhibited include:

1. **Direct IP Hosting**: Some IPs host a web server that presents the 'Million OK!!!' response, typically over port 80, without resolving to any domains.
2. **Domain Hosting**: Others host a small cluster of domains or TLS certificates issued by Sectigo, often linked to Kimsuky's phishing campaigns.
3. **Legacy Web Server Stack**: The server administrator installed outdated software versions of Apache Web Server (Win32), OpenSSL, and PHP. The commonly observed header across all instances was **Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30**.

The following screenshots show the response presented during our research and the favicon. The first example captures the domain `nidauth.r-e[.]kr`, which is likely meant to mimic Naver's sign-in page, while the other displays a direct request to an IP address.

Figure 1: Domain presenting the Million OK message and the Naver favicon.

Figure 2: Making an HTTP request to many IPs in this collection displays the above.

Searching for 'Million OK !!!!' in Hunt

Using HuntSQL™ Explorer, we queried the latest scan results to identify servers returning the distinctive text in their HTTP response bodies. This approach enabled us to pinpoint IPs relevant to our investigation efficiently.

The exact query used is shown below:

```
  SELECT ip, port, http.body FROM http WHERE http.body == 'Million OK !!!!' GROUP BY\
ip, port, http.body
```

Copy

This query retrieves the IP address, port, and HTTP response body from the dataset, focusing on entries where the body contains the exact text 'Million OK!!!!'. By grouping the results by IP, port, and response body, we isolate unique instances of this behavior, removing duplicates and streamlining our analysis.

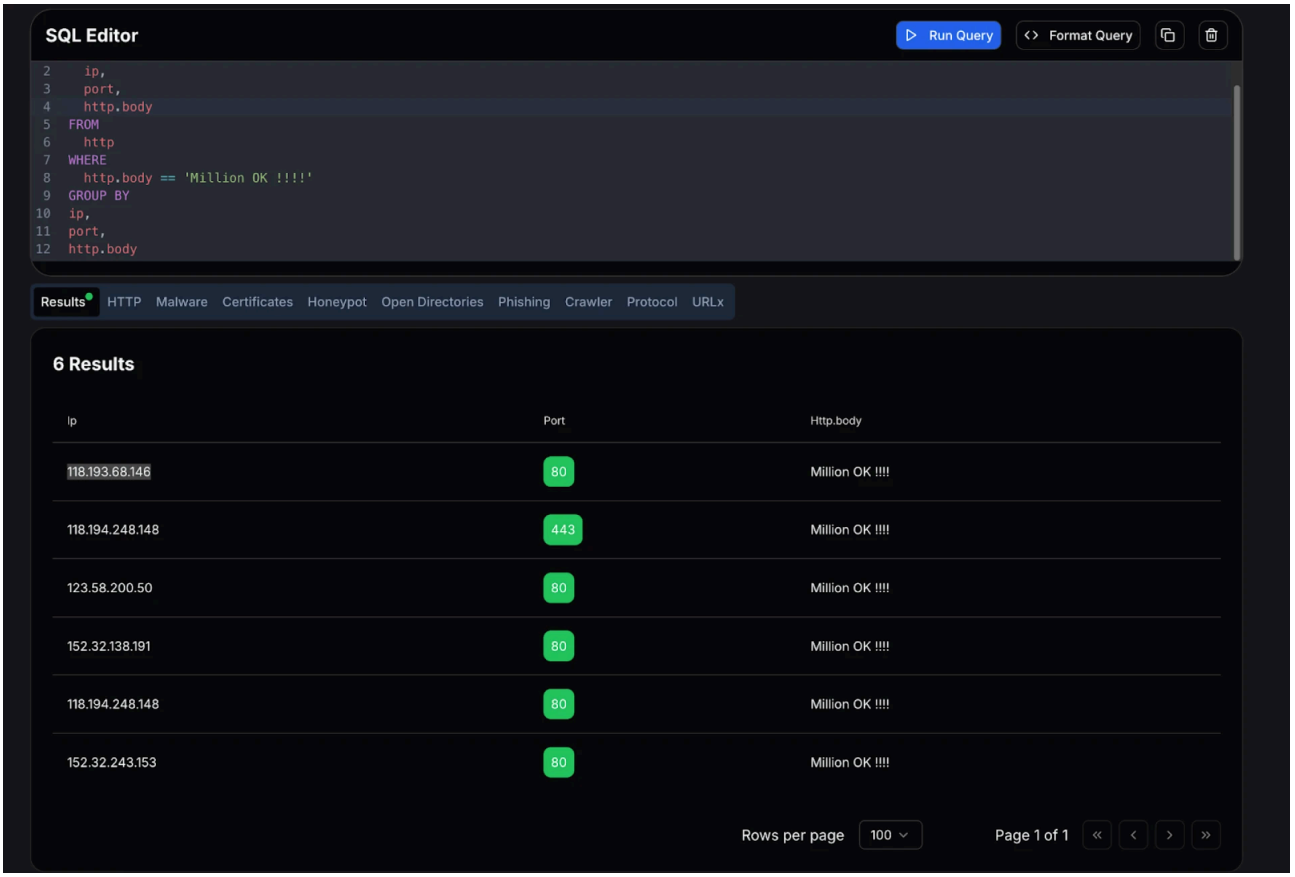

Figure 3: Screenshot of scan results using SQL Explorer in Hunt.

Latest Results

While most of our findings were observed on port 80, several IPs also had port 443 open. These instances mirrored the same HTTP response and favicon and included a TLS certificate. Additional details are displayed below.

IP Address	Resolving Domain(s)	TLS Certificate Org	Domain in Common Name of Certificate
118.193.68[.]146	N/A	Sectigo Limited	*.nidcheck.o-r[.]kr *.againcheck[.]site
118.194.248[.]148	N/A	N/A	N/A
123.58.200[.]50	N/A	N/A	N/A
152.32.138[.]191	N/A	N/A	N/A
152.32.243[.]153	N/A	Sectigo Limited	*.checkmail.kro[.]kr *.nidcorp[.]store *.checkagain[.]store

Historical Observations

IP Address	Resolving Domain(s)	TLS Certificate Org	Domain in Common Name of Certificate
118.193.69[.]248	ozszg[.]top mail.ozszg[.]top	N/A	N/A
123.58.200[.]13	N/A	N/A	N/A
152.32.243[.]184	nld.blog-view[.]o-r.kr	N/A	N/A
152.32.138[.]63	N/A	N/A	N/A

A Simple "Hello"

While analyzing servers displaying the Naver favicon, we found a web page hosted at IP address 101.36.114[.]153 that stood out. Instead of returning the previously observed text, the server responded with a simple 'Hello' message-a familiar sight for those accustomed to sifting through internet scan data.

What made this particular item interesting was that, in addition to the favicon, it also shares the same ASN, Sectigo-issued TLS certificate, and a similar Apache server configuration, though with different software versions.

Using Hunt's Port History tab from within the IP overview page, we can see the 'Hello' response captured along with the HTTP headers.

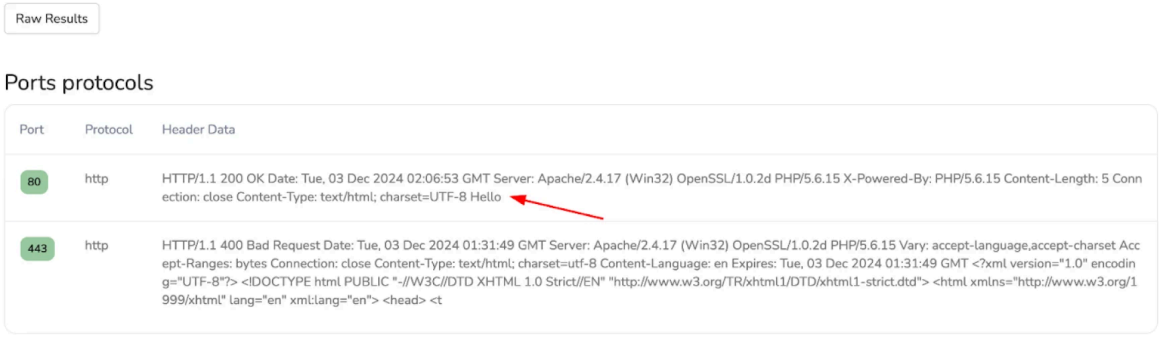

Figure 4: Port history showing the 'Hello' HTTP response (Hunt)

The TLS certificate associated with this server adds further context to its connection with the identified patterns. The certificate's Common Name (CN), `edoc-send.n-e[.]kr`, (SHA256: **3a6640efbfbd42efbfbd21d5bcefbfbd68023a74d19848efbfbd167b7aefbfbd0573efbfbd**) reflects the frequent use of the n-e.kr TLD in phishing and C2 infrastructure often tied to Kimsuky.

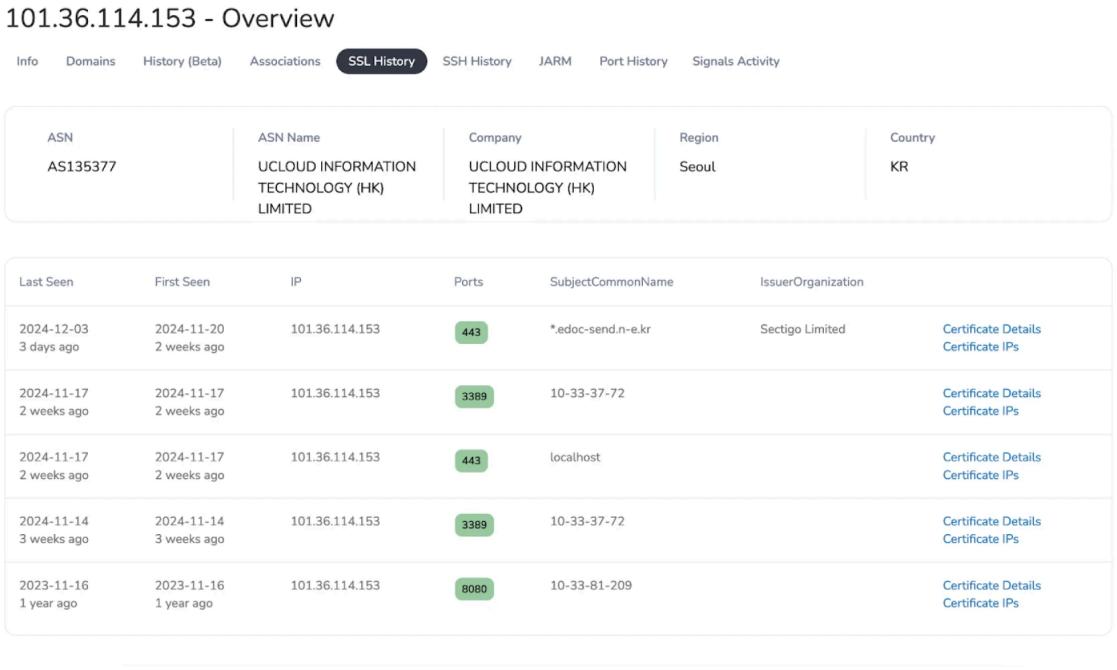

Figure 5: Screenshot of the historical TLS records for 101.36.114[.]153 (Hunt).

Further examination of the certificate's domain revealed a registrant email address of **cfa4a551515dc742s@gmail[.]com**. As reported in September by Unit 42, this email is tied to two domains used by malware families, KLogEXE and FPSpy.

Figure 1. Infrastructure layout showing the connection between the malware.

Figure 6: Screenshot showing registrant email links (Source: Unit 42).

For additional details, see the original blog post, "Unraveling Sparkling Pisces's Tool Set: KLogEXE and FPSpy."

Conclusion

Consistent patterns emerged across the infrastructure discussed in this blog, including Sectigo-issued TLS certificates, Apache server configurations, specific TLD use, and a focus on Naver-related targeting.

A distinct HTTP response at 101.36.114[.]153 led to the discovery of a wildcard domain in the certificate's Common Name, which was tied to a registrant email address previously reported by Unit42.

SQL Explorer enable analysts to identify and monitor suspicious infrastructure without relying on malware samples or active phishing pages. Outlining these recurring patterns and infrastructure traits offers defenders valuable context to monitor adversary activity and understand their operational methods.

Certificate Hashes

- *.nidcheck.o-r[.]kr - 393CBD41F14B1C55BDE92A32E10B5D65384E33A97C77F352BD90FDB8FD5D73AE
- *.againcheck[.]site - 5F2C65E695D85395634E7AB561242425E6EF281CE2E14A0D5C1704ED593CFA5F
- *.checkmail.kro[.]kr - 98C85EF91E05593CD470FFE8698AA6D97B36E8B885200BE87080B8C2A135FB9C
- *.nidcorp[.]store - D8A8DDDA6CC12C5533268B20E48E1B636CE9173E9F9B5BB4C832FE00F1B26841
- *.checkagain[.]store - 974E386F8FACFF325EC2F3EBB7439A9A1E4E4C88944D5BEB5C341923DC993556
