WSS:
The Essentials

+82 2 448 3435

4F FourMI2 Bldg. 84 Mabang-ro 2gil,
Seocho-Gu, Seoul, South Korea

umvwebsecurity.com

2024.04.19

SKT Hacked

Image Source: NewsWay

A web shell was implanted in an SK Telecom server in June 2022 and wasn't discovered until May 2025—nearly three years later.

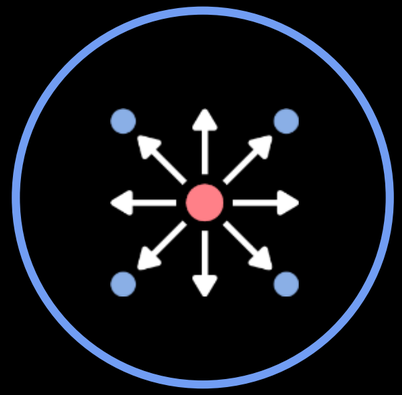
This web shell served as a gateway for 24 different types of BPFDoor malware, a sophisticated backdoor software.

Among the infected servers were ones storing user data, impacting approximately 25 million people.

SKT Hacking Process

Initial infiltration via phishing and/or web server vulnerabilities

After initial infiltration into web server, web shell uploaded to provide persistent access to the system



Gradual escalation of access privileges and movement into internal network

Final infiltration into HSS and data theft

Sources:The Elec
Sygnia
KBS

2024.07.26

WANTED BY THE FBI

RIM JONG HYOK

Conspiracy to Commit Computer Hacking; Conspiracy to Commit Promotion Money Laundering

DESCRIPTION

Alias: Rim Chong-Hyo'k

Sex: Male **Race:** Asian

Languages: English, Korean

REWARD

The Rewards For Justice Program, United States Department of State, is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act, to include Rim Jong Hyok.

REMARKS

Rim Jong Hyok is a North Korean citizen last known to be in North Korea.

CAUTION

Rim Jong Hyok, a member of the Andariel Unit of the North Korean Government's Reconnaissance General Bureau (RGB), a North Korean military intelligence agency, is wanted for allegedly conspiring to violate the Computer Fraud and Abuse Act. Acting on behalf of North Korea's RGB, Rim Jong Hyok allegedly conspired to use the Maui ransomware software to conduct computer intrusions against U.S. hospitals and healthcare companies, extort ransoms, launder the proceeds, and purchase additional internet servers to conduct cyber espionage hacks against government and technology victims in the United States, South Korea, and China.

On July 24, 2024, a federal arrest warrant was issued for Rim Jong Hyok in the United States District Court, District of Kansas, after he was charged with conspiracy to commit computer hacking and conspiracy to commit promotion money laundering.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: St. Louis

Image Source: Rewards for Justice

"How the U.S. State Department's Most Wanted North Korean Hacker Breached NASA..."

"Rim Jong Hyok has been accused of participating in attacks on 17 institutions across 11 states in the U.S., including an American health insurance company, NASA, and military bases. Additionally, he reportedly accessed computer systems of defense contractors in Michigan and California, as well as Air Force bases in Texas and Georgia.

Andariel, a state-backed hacking organization under the Third Bureau of North Korea's Reconnaissance General Bureau, operates out of Pyongyang and Sinuiju.

Andariel conducts widespread attacks on web servers by exploiting known vulnerabilities like Log4j. Through this, they distribute malicious script files known as "web shells," gaining access to critical information and applications to carry out further attacks.

Security authorities ... recommend protecting web servers from web shells, monitoring endpoints for malicious activities, and strengthening authentication and remote access security."

Source: Newsis (translated)

2023.06.02

Image Source: Phoenix Security

MOVEit Transfer Vulnerability Hacks

In late May 2023, the Cl0p ransomware group launched a sophisticated series of attacks by exploiting a zero-day SQL vulnerability in Progress MOVEit Transfer software.

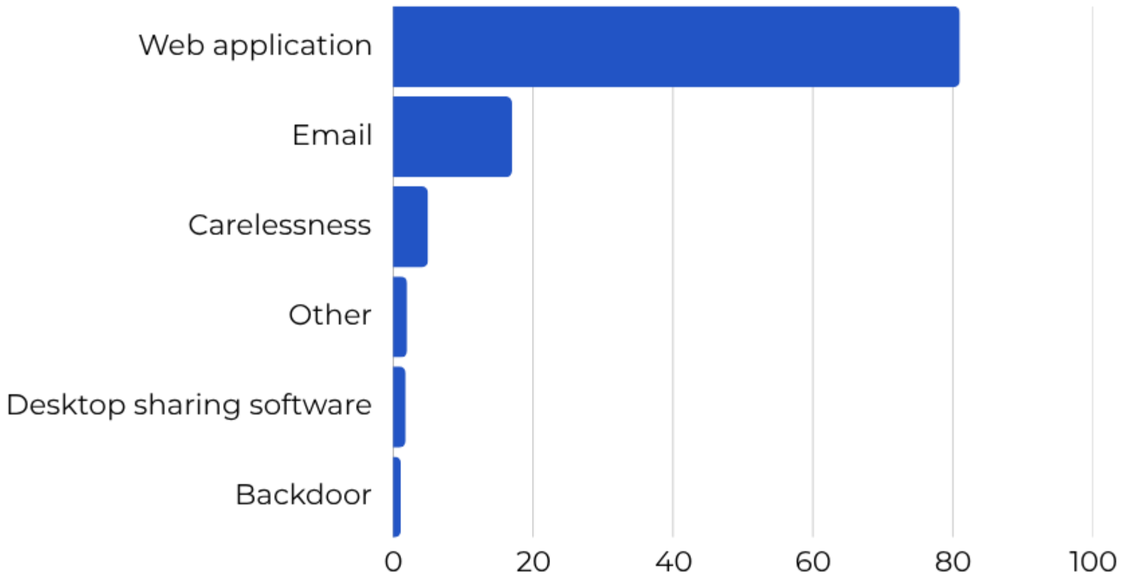
Leveraging their custom web shell, LEMURLOOT—camouflaged under an unassuming file name, “human2.aspx”—they exfiltrated sensitive data at astonishing speed, sometimes within minutes.

The devastating reach of this breach left 2,611 organizations compromised and over 5 million individuals exposed.

Even into November 2024, Amazon announced that its staff details had been leaked online as a ripple effect of the hack.

Source: KonBriefing
Mandiant
SecureWorld

Rising Web Server Hacking



"One year ago, we reported the steady increase in the use of web shells in attacks worldwide. The latest … data shows that this trend … accelerated: every month from August 2020 to January 2021 … an average of 140,000 encounters of these threats on servers, almost double the 77,000 monthly average we saw last year. [1]

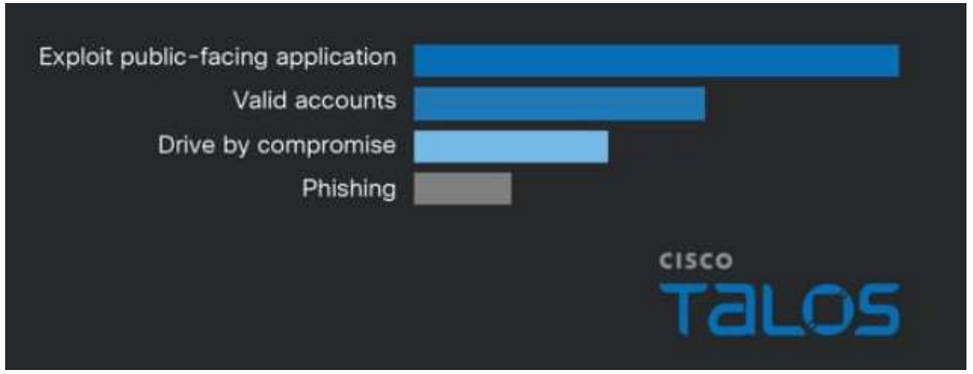
Additionally, around 80% of security incidents analyzed by Verizon in 2023 occurred through web applications. [2]

According to Cisco Talos' Q4 2024 Incident Report, web shells were used to exploit vulnerable web applications in 35% of security incidents. [3]

출처: [1] Microsoft Security Blog
[2] Verizon 2023 DBIR
[3] Cisco Talos Incident Response Trends

2025.01.30

“Web Shell Frenzy”



“Threat actors increasingly deployed web shells against vulnerable web applications and primarily exploited vulnerable or unpatched public-facing applications to gain initial access in Q4, a notable shift from previous quarters.

The functionality of the web shells and targeted web applications varied across incidents, highlighting the multitude of ways threat actors can leverage vulnerable web servers as a gateway into a victim’s environment.”

“In 35% of incidents in Q4 [2024], threat actors deployed a variety of open-source and publicly available web shells against vulnerable or unpatched web applications, a significant increase from less than 10% in the previous quarter.”

Source: Cisco Talos Incident Response Trends Q4 2024

Web Shells

Often mandated security tools like firewalls and IDS/IPS can't catch web shells effectively.

Coming in encoded, segmented, and disguised in normal traffic, web shells are notoriously hard to catch.

This makes web shells a go-to tool for threat actors, who know one successfully-implanted web shell will give them persistent and long-term backdoor access to a system.

It's the perfect launchpad for further damage and breach.

We all need more than just regulation security tools.

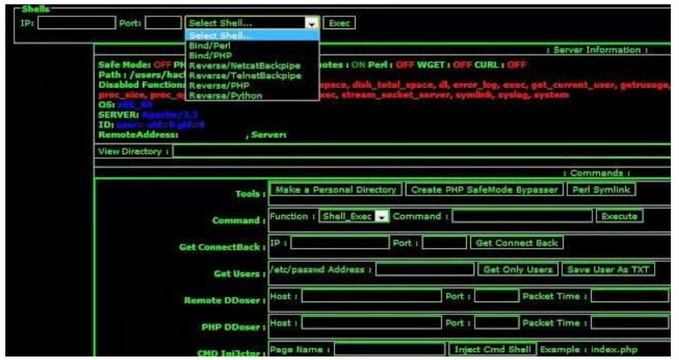


Image Source: Shreshta Blog

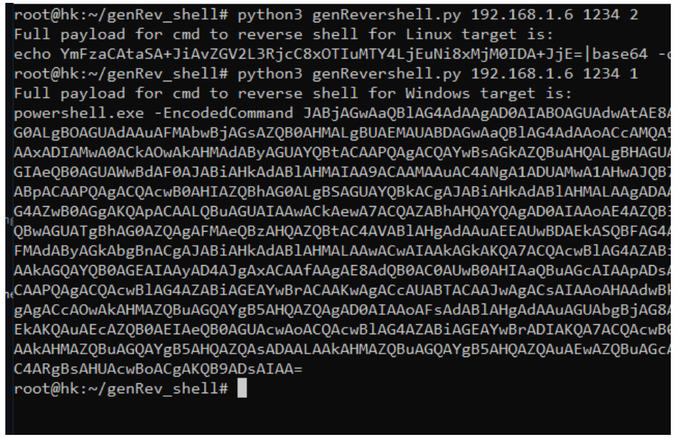


Image Source: GitHub

WSS

WSS stops web shells the instant they’re uploaded to a web server.

Real-Time DR

WSS combines FIM-like features with real-time quarantine to detect and isolate web shell scripts the moment they are uploaded to a web server.

Detection Accuracy

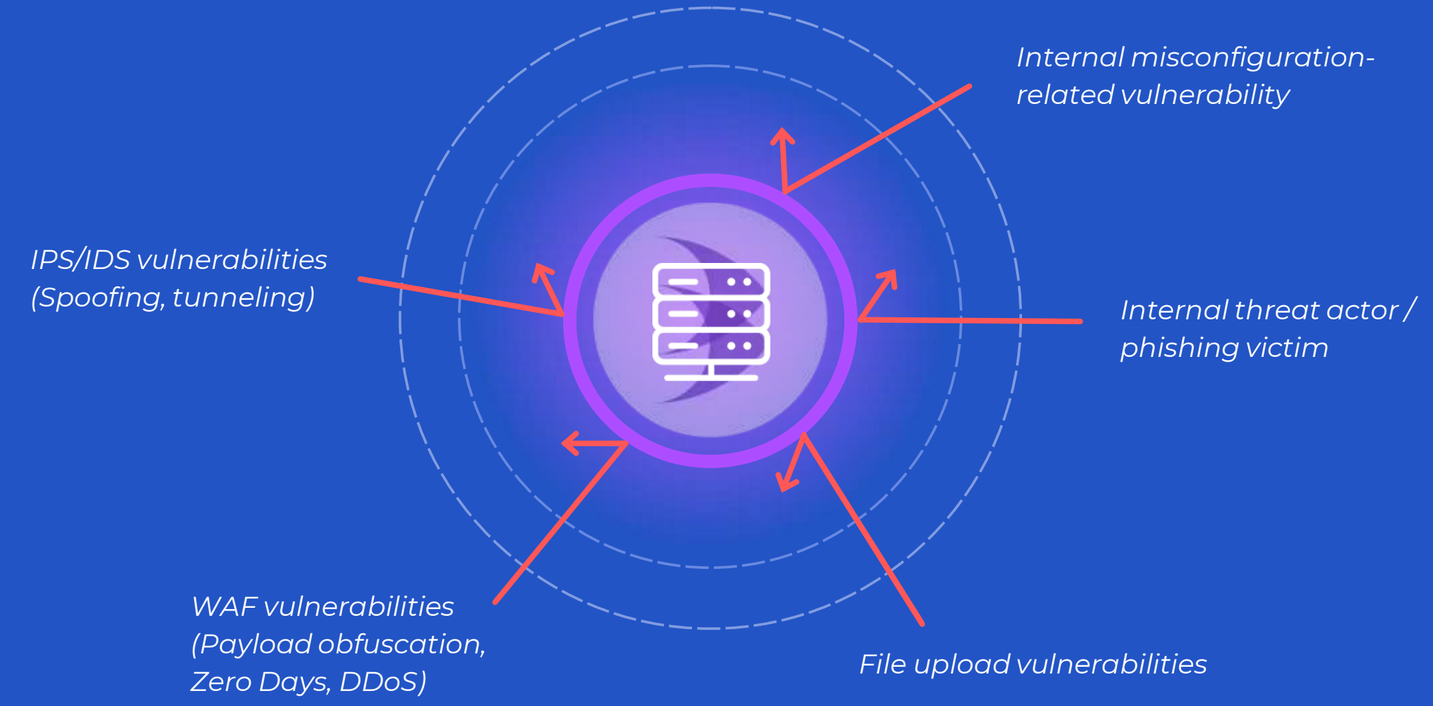
Detection based on patterns, hash values, signatures, and algorithms improves detection rates and accuracy.

Your Final Defense

The concept is simple:
Servers are assets in 95% of data breach incidents, and web applications are a target in ~43% of credential abuse and vulnerability exploitation cases.*

Catching malware at the web server is an effective way to combat most infiltrative cyber attacks.

WSS does this, providing you with a final layer of defense before a breach can truly begin.



*Source: Verizon 2025 DBIR

What about WAFs?

Web Shell Detection Rates

A WAF is an important piece of regulation security that inspects traffic.

While many WAFs include a web-shell detection function, detection rates are low due to script encoding and segmentation.

Several high-profile web shell-enabled data breaches (e.g. SKT, Andariel, MOVEit exploits, etc,) despite the presence of firewalls.

*Detection rates and specs may vary by product

What about Server EDR?

Server EDRs use data collection and behavior/anomaly-based detection to detect suspicious activity on servers, PCs, and other endpoints.

Server EDRs provide wide detection coverage, but are consequently resource-heavy and expensive.

Behavior-based detection is not always accurate, and necessarily occurs after damaging activity has already begun.

Lightweight Performance

WSS minimizes resource consumption (can operate on ≤1% CPU) to ensure optimal and stable web server performance.

Real-Time Detection

WSS detects web shell scripts the instant they're discovered in a web server's file system, and quarantines them in real-time before damage can begin.

Why choose WSS?

Lightweight

WSS can operate on limited resources (e.g. ≤1% CPU), ensuring minimal impact on server performance

Automated

WSS automatically quarantines web shells and automatically finds home directories for detection

Efficient

WSS offers streamlined management and focused web shell detection

Case Studies

Hyundai Card

In April 2011, 420,000 customers' (~24%) personal information was leaked in a breach (~2 months). ~100,000 USD was lost directly to the hacker; 13,000 clients' passwords were stolen.

Hyundai Capital reached out to UMV immediately, and by June 2011 had purchased a WSS On-Premise site license.

They now have ~200 Agents in operation, and their servers have been running WSS smoothly for 15+ years.

kobaco
한국방송광고진흥공사

Due to receiving an insufficient rating in the file protection category in a NIS audit, this organization decided to adopt a web shell detection solution.

After conducting a comparison among competitors, WSS was selected and implemented.

In a subsequent audit, the organization achieved compliance for file protection.

Case Studies

Hana Financial Group

Due to maintenance and detection performance issues with a leading competitor's product, a competitive review led to the adoption of WSS.

WSS was selected based on its product performance, installation speed, and maintenance capabilities.

Post-implementation, WSS received praise for its responsiveness, improved maintenance, and superior performance compared to the previous system.

SUPREME COURT OF KOREA 대법원

In 2023, after a two-year undetected breach by North Korea's Lazarus group stole 1,000GB of sensitive data, the Supreme Court discreetly implemented WSS.

WSS enhanced real-time monitoring, AI-assisted anomaly detection, and automated incident response.

The solution improved detection speed, reduced manual workload, and strengthened forensic capabilities, earning praise for restoring trust with minimal operational impact.

References

Web Server Safeguard (WSS) has been trusted by enterprises and public institutions spanning diverse sectors for 15+ years.

300+
Customers

30K+
Agents
in Operation

10+
Patents &
Certifications

PUBLIC

Ministry of National Defense, Republic of Korea
SEOUL METROPOLITAN GOVERNMENT
Ministry of Foreign Affairs, Republic of Korea
KORAIL
CHEONG WA DAE
Kdata, Korea Data Agency

FINANCE

LOTTECARD
SK securities
SAMSUNG CARD
Hyundai Capital
BC CARD
NH Bank
Hana Financial Group

ENTERPRISE

SAMSUNG SDS
cafe24
Gmarket
S-OIL Corporation
CJ CHEILJEDANG
SHINSEGAE
GS
dun & bradstreet
ebay
Prudential
AhnLab
TOYOTA
Deloitte.
Hanwha
gabia.

Locations

Founded in 2008 in Seoul, South Korea,
UMV has expanded its corporate presence to Europe and Central Asia
with the hope of enhancing web security across the globe

Headquarters

Seoul, South Korea

4F FourMI2 Bldg. 84 Mabang-ro 2gil, Seocho-Gu,
Seoul, South Korea

+82 2 448 3435

Local Corporation

İstanbul, Türkiye

Polat İs Merkezi, Mecidiyekoy Mah., Cemal Sahir Sok.,
No:29/32, Sisli, İstanbul, Türkiye

+90 212 266 21 88

Local Corporation

Almaty, Kazakhstan

630, 6th Floor, Prospekt Zhibek Zholy, 50/1 Medeuskij
rajon, Almaty, Kazakhstan

+7 700 980 7428

Contact

The security chain is only as strong as its weakest link

Contact us to learn more

sales@umvglobal.com

umvwebsecurity.com