PHP2Shell Weaponized After Japanese Real Estate Extortion

By ST SOCRadar Threat Research Unit (STRU)

Published: 2026-10-27 · Archived: 2026-11-28 02:00:18 UTC

SOCRadar Threat Research Unit identified an open directory on 96.126.130.81 that exposed the working files of an operator who ran an extortion campaign against Japanese real estate websites and **then turned to PHP2Shell**, the pair of unauthenticated PHP flaws tracked as CVE-2026-109618 and CVE-2026-109619. The server held more than 3,800 files, including **a weaponized copy of the PHP2Shell reproducer package**, scripts for web shell deployment and lateral movement, beacon logs, ransom pages and data stolen from victims. The ransom pages and contact addresses use the handle kkkkevin777.

The campaign focused on Japanese real estate and property-buying websites in October 2026. The intrusion resembled a supply chain attack. After compromising the website of a Japanese real estate services company, the operator used access material found in that environment to reach nearly 20 other sites on the same shared hosting infrastructure and to pull data on their customers.

The **PHP2Shell tooling only arrived on the server on October 21**, about ten days after this extortion wave, and the files show no link between PHP2Shell and these intrusions.

What This Report Does and Does Not Show

- **Initial access:** The server does not show how the operator first got into the real estate sites. The October 9-11 extortion wave did not rely on PHP2Shell
- **PHP2Shell timeline:** The PHP2Shell tooling reached the server on October 21, about ten days after the extortion wave
- **Current stage:** The operator was adapting the public reproducer, building exploit, probe and pipeline scripts around it. The files contain no record of a successful exploitation against a live target
- **Why it matters:** An operator who has already monetized shared-hosting access is now preparing PHP2Shell as a follow-on capability, likely for broader targeting

The stolen member data also creates third-party exposure. Customer records taken from the victims include email addresses on major Japanese telecom, mobile and ISP mail domains, which puts those end users at risk of phishing and credential stuffing well beyond the breached sites.

Key Takeaways

- An exposed staging server at 96.126.130.81 held a weaponized copy of the PHP2Shell reproducer package for CVE-2026-109618 and CVE-2026-109619, added on October 21, about ten days after the extortion wave
- The campaign started with one Japanese real estate services company and used it as a stepping stone to nearly 20 other Japanese websites, most of them real estate and property-buying businesses, between October 9 and 11, 2026

- Shared hosting accounts were reached with a stored SSH key and a database password reused across sites, which turned one compromise into many
- Ransom page templates and deployment scripts target public homepages with a fake maintenance notice and admin panels with a ransom note, with a negotiation deadline of October 11, 2026, 04:00 JST
- The operator turned the initial victim's customers into leverage, with a script built to mail its members in bulk and a drafted public forum post accusing the company of not reporting the breach
- Stolen data on the server includes 16,061 member records with plaintext passwords, income and savings details, plus five SQL Server database backups and 730 business emails from a Taiwanese company

Campaign at a Glance

Attribute	Details
Related CVEs	CVE-2026-109618, CVE-2026-109619 (PHP2Shell)
Affected component	PHP session upload progress handling
Staging server	96.126.130.81 (open directory on port 9999)
Confirmed victim	A Japanese real estate services company
Other affected sites	About 20 Japanese websites, mostly real estate and property buying, plus a Taiwanese company's Windows server
Activity window	Extortion wave October 9 to 11, 2026; PHP2Shell tooling added October 21, 2026
Impact	Web shells, data theft, defacement, extortion of the company and its customers
Motivation	Financial extortion

PHP2Shell on the Attacker's Server

The staging server held two copies of the PHP2Shell package. The packages include:

- Weaponization notes describing how the lab stages chain toward remote code execution
- Loop and single-child scripts for repeated exploitation attempts against live targets
- Helper and debugger scripts used during development
- A second build of the package with Docker files and its own tools folder

Both packages, and every file inside them, are dated October 21, 2026, about ten days after the extortion wave against Japanese real estate sites. Exploit, pipeline and probe scripts that build on the package appear on the server from that date onward, which marks PHP2Shell as the operator's next capability rather than the tool behind the

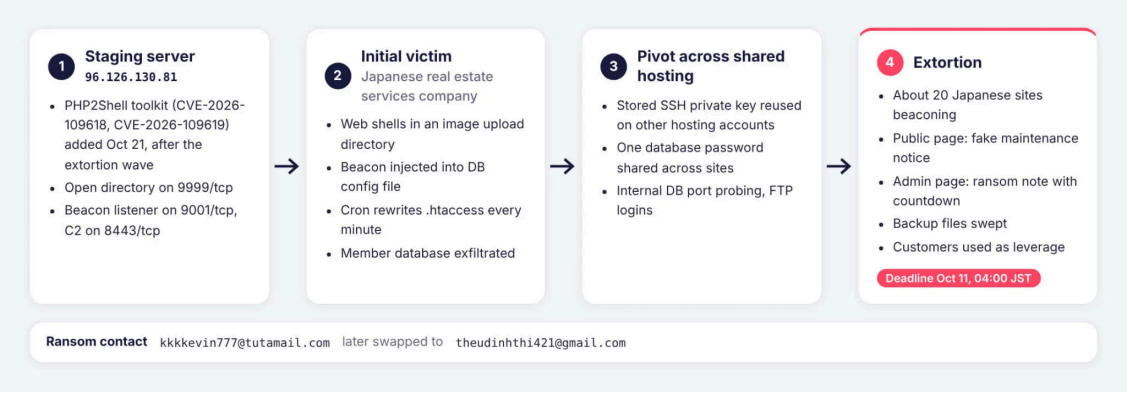
earlier intrusions. The files contain no saved output showing a successful PHP2Shell exploitation of a live site. Any PHP site running a vulnerable version should still be treated as exposed.

How the Exposed Server Was Found

The server at 96.126.130.81 exposed its working directory over an unauthenticated HTTP directory listing on port 9999. The listing included shell scripts, Python tools, PHP payloads, beacon and command-and-control (C2) logs, ransom page templates, an SSH private key and archives of stolen mail and databases.

File timestamps place most activity between October 8 and October 27, 2026, with peaks on October 10, October 15 and October 21 to 23. The server's SSH service had been moved to port 888 and fail2ban installed, a sign that the host was meant for long-term use.

From One Compromise to About 20 Victims



Attack flow of the campaign, from the staging server to extortion

Initial Victim

Scripts dated from October 9 show the attacker already holding web shell access to the initial victim's website. How that access was first obtained is not recorded on this server, and comments in the scripts say they were run from a separate machine. The attacker:

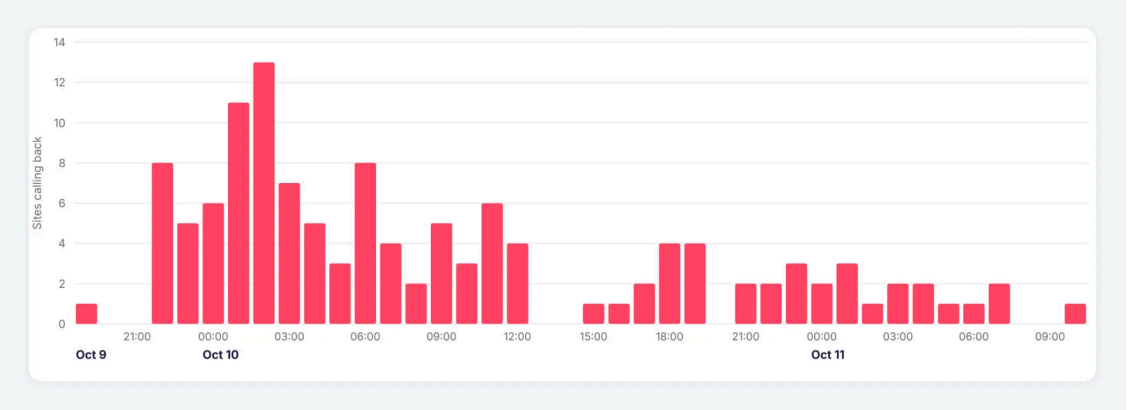
- Placed PHP web shells under an image upload directory, using random 32-character file names
- Injected a beacon into the site's database configuration file that called back to 96.126.130.81 on port 9001
- Seeded a self-propagating PHP hook across the web root
- Overrode the site owner's deny rules in .htaccess and installed a cron job that rewrote them every minute, so the owner's lockout attempts were reverted automatically
- Tested outbound mail from the company's info@ address to an external Gmail address

The server also held a member database export from the site, containing customer names, contact details, addresses and passwords stored in plaintext.

Pivot Across Shared Hosting

The initial victim's environment gave the attacker what was needed to go further. An SSH private key stored on the staging server was used to log in to several other accounts on the same shared hosting provider. Scripts on the server also show one database password reused across multiple victim sites that share the same member table structure, which points to a common web platform or a common developer behind them.

The beacon log records callbacks from about 20 Japanese domains between October 9 and October 11, 2026. Most belong to real estate agencies, property-buying services and related local businesses. The attacker also probed internal database ports from inside the hosting network and tried FTP logins with harvested credentials on further accounts.



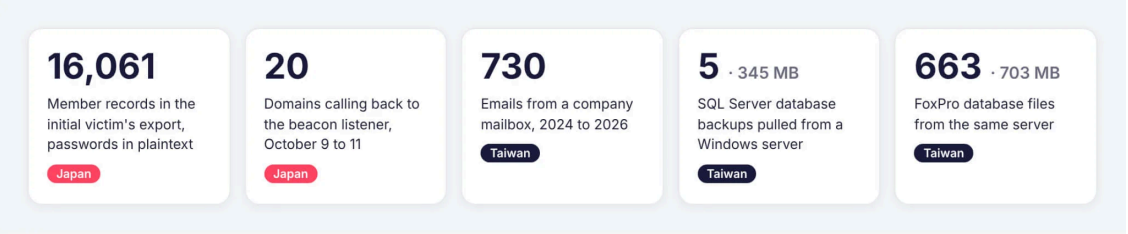
Distinct sites calling back to the beacon listener per hour, October 9 to 11, 2026 (server time)

Other Targets

Recon scripts and port lists also reference a Japanese food manufacturer's webmail, with no confirmed compromise. A Taiwanese company the operator researched through WHOIS lookups did not remain a reconnaissance target; its data appears on the server, as described below.

What Data Was Taken

The server holds the results of the operator's data theft, not only the tools. The haul spans Japan and Taiwan and covers customer records, internal databases and business email.

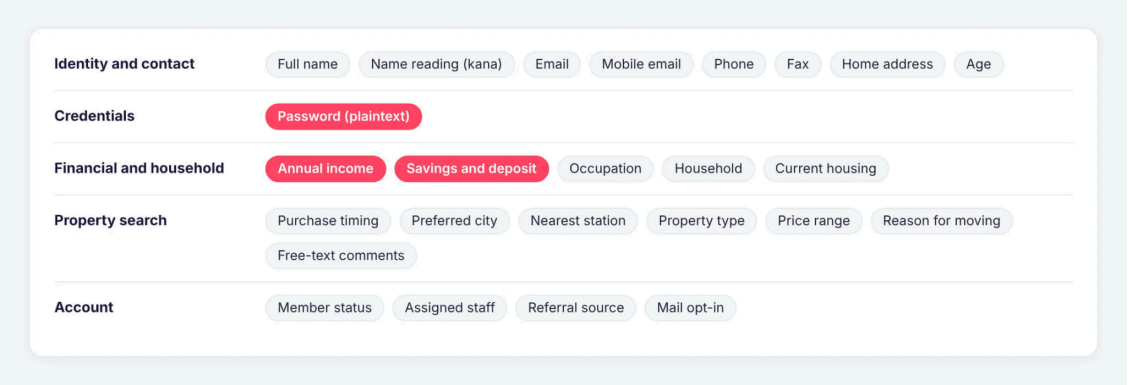


Data recovered from the operator's server

Customer Records From the Initial Victim

The initial victim's member export holds 16,061 records, and each one goes well beyond contact details. Alongside names, phone numbers, email addresses and home addresses, the export stores plaintext passwords, annual income, savings, occupation, household details and each member's property search, including budget,

preferred area and purchase timing. That combination gives an attacker what is needed for credential stuffing, convincing real estate or financial phishing and targeted fraud.



Fields in the initial victim's member export, with no customer data shown

Proof of Access Across Nearly 20 Sites

The beacon listener on the staging server logged callbacks from 20 domains between October 9 and 11, 2026, each one a site carrying the operator's injected code. Scripts on the server also used the shared database password to query member tables on other victim sites.

beacon.log

```
1   09/Oct/2026 19:00:00   49.212.x.x     GET /b?h=[redacted].jp
2   09/Oct/2026 22:20:00   49.212.x.x     GET /b?h=[redacted].jp
3   09/Oct/2026 22:20:00   153.127.x.x    GET /b?h=[redacted].jp
4   09/Oct/2026 22:20:00   153.120.x.x    GET /b?h=[redacted].jp
5   09/Oct/2026 22:20:00   49.212.x.x     GET /b?h=[redacted].jp
6   09/Oct/2026 22:20:00   49.212.x.x     GET /b?h=[redacted].jp
7   09/Oct/2026 22:30:00   182.48.x.x     GET /b?h=[redacted].co.jp
8   09/Oct/2026 22:59:00   153.120.x.x    GET /b?h=[redacted].com
9   10/Oct/2026 00:59:00   153.120.x.x    GET /b?h=[redacted].jp
10  10/Oct/2026 01:58:12   49.212.x.x     GET /b?h=[redacted].jp
11  10/Oct/2026 01:58:18   49.212.x.x     GET /b?h=[redacted].jp
12  10/Oct/2026 01:58:21   49.212.x.x     GET /b?h=[redacted].jp
```

First callback from each site in the operator's beacon log, with hostnames redacted

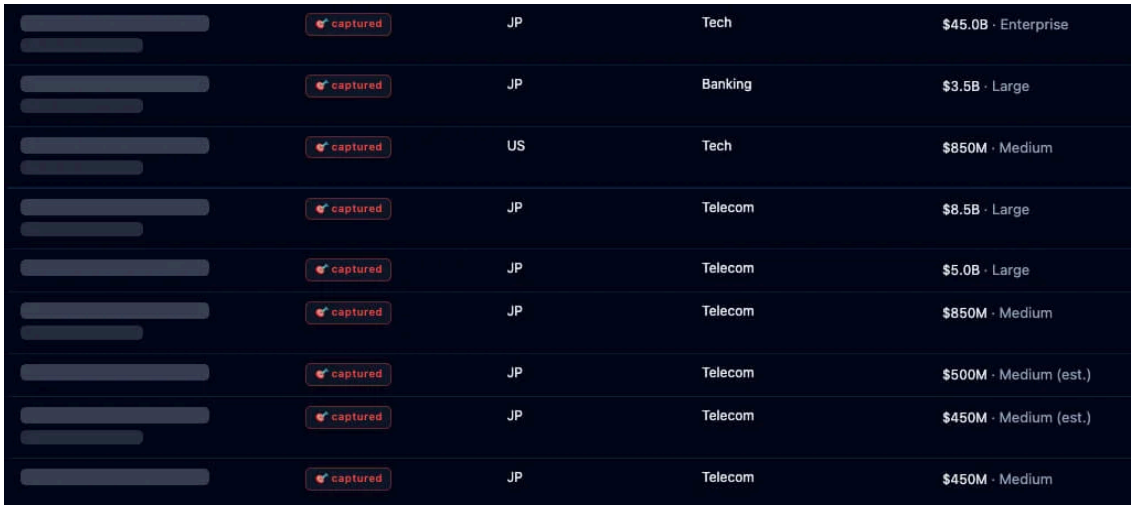
A Taiwanese Company's Databases and Mailbox

On October 22 and 23, 2026, the operator pulled data from a Windows server hosted in Taiwan through a web shell: five SQL Server database backups totaling about 345 MB, 663 FoxPro database files totaling about 703 MB and 730 emails from a company mailbox dated 2024 to 2026. A script on the server was written to crack a

password-protected archive from the same haul. How the operator first got into that server is not recorded in the files.

Large Organizations in the Blast Radius

SOCRadar's analysis of the stolen customer data found email addresses on domains belonging to major Japanese banking, telecommunications and technology organizations, including companies with annual revenues ranging from hundreds of millions to tens of billions of dollars. Most of these are consumer mail services, so the exposed people are subscribers who were customers of the victim sites. A smaller number are corporate domains, which puts those organizations' employees within reach of targeted phishing. None of these organizations was breached in this campaign.



Organizations whose email domains appear in the stolen customer data, with names redacted

The Extortion Playbook

The server holds two page templates and the scripts that deploy them:

- **Public site:** Overwrites the homepage with a Japanese "system maintenance" notice listing a contact address
- **Admin panel:** Overwrites the management page with a warning that names the same address as the negotiation contact and shows a countdown to October 11, 2026, 04:00 JST



Fake maintenance notice built for victims' public homepages, rendered from the attacker's template



Ransom note built for victims' admin panels, rendered from the attacker's template after the deadline expired

The scripts back up the original index pages before overwriting them. Repeated "relock" scripts, along with a saved copy of a site owner's own lockout rules, indicate that owners were removing the pages and the operator kept restoring them. Scripts also ran database processing jobs on several victim accounts and swept victims' home directories for backup files, which would reduce their options for recovery.

A later script searched victims' web roots for the original Tutamail contact address and replaced it with a Gmail address, the same address targeted by a test message sent from the initial victim's mail server. Whether the second address belongs to the same person, a partner or a buyer of access is not established in the files.

em_swap_box.sh

```
#!/bin/sh
F=$(grep -rl 'kkkkevin777@tutamail.com' $HOME/www 2>/dev/null)
echo "FILES: $F"
if [ -n "$F" ]; then echo "$F" | xargs sed -i '' 's/kkkkevin777@tutamail.com/theudinhthi421@gmail.com/g'; echo SWAPPED; fi
```

relock_box.sh

```
#!/bin/sh
W=$HOME/www
[ -f $W/index.php ] && cp $W/index.php $W/index.php.orig20261010
base64 -d < $HOME/relock_u.b64 > $W/index.php
mkdir -p $W/manage
[ -f $W/manage/index.php ] && cp $W/manage/index.php $W/manage/index.php.orig20261010
base64 -d < $HOME/relock_m.b64 > $W/manage/index.php
rm -f $HOME/relock_u.b64 $HOME/relock_m.b64
echo RELOCKED
```

Scripts that swap the ransom contact address and restore the ransom pages on victim sites

Pressure on Customers

The operator also turned the initial victim's customers into leverage. A script on the server, staged on October 10, was built to send pre-written messages in bulk through sendmail, with progress tracking and a kill switch. A drafted public forum post claims that notices went out from the initial victim's official mail server to every member, each containing the recipient's own details and those of 49 other members, and that data on 167,000 members was taken. These figures are the operator's claims; the server itself holds a member export of more than 16,000 records from the initial victim.

Direct Threats and Public Exposure

Victims were contacted outside the ransom pages as well. A "final warning" email drafted for staff at one victim company states that ignoring LINE messages or taking the site offline would not let them escape, and demands an immediate reply. On October 11, the operator drafted a thread for the 5ch newsplus board accusing the initial victim of failing to report the breach to Japan's Personal Information Protection Commission. The saved responses stop at the board's confirmation page, so publication is not confirmed.

Windows C2 and a Second Operation

The server also ran a small Python C2 on port 8443 paired with a PowerShell agent that polls for commands every 30 seconds and posts results back. Comments in both files label it as a beacon for a separate "finance line" operation, which indicates the operator was set up to run commands on Windows machines outside the real estate campaign. Results folders for this C2 were empty at the time of collection.

Who Is Behind the Campaign?

The ransom pages, contact addresses and scripts point to an operator using the handle kkkkevin777. Script comments and working notes are written in Simplified Chinese, while every victim-facing message is written in Japanese, and SSH keys authorized on the server carry the comment administrator@chenzicccc.

The files show no affiliate program, data leak site or ransomware-as-a-service panel. Each step, from web shell access to customer pressure, is scripted by hand. After the Japanese wave, the operator compiled 3,913 Hong Kong and Taiwan IP ranges and ran mass scans against them on October 21, 2026, the same day the PHP2Shell tooling arrived, and the separate "finance line" C2 points to more than one operation running in parallel. These are investigative leads drawn from the operator's own files, not a confirmed identity.

Third-Party Exposure From the Stolen Member Data

The stolen member databases hold the personal data of the victim sites' customers. Analysis of the email domains in this data shows heavy concentration on major Japanese telecom, mobile carrier and ISP mail services, alongside a smaller number of corporate domains.

Those customers were not breached through their own providers. Their names, contact details and home addresses are now in the attacker's hands, along with plaintext passwords for the initial victim's members, which makes them likely targets for phishing, extortion follow-ups and credential stuffing against other services where the same password was reused.

MITRE ATT&CK Techniques

Tactic	Technique	ID
Initial Access	Exploit Public-Facing Application	T1190
Persistence	Server Software Component: Web Shell	T1505.003
Persistence	Scheduled Task/Job: Cron	T1053.003
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
Credential Access	Unsecured Credentials: Private Keys	T1552.004
Lateral Movement	Remote Services: SSH	T1021.004
Defense Evasion	Valid Accounts	T1078
Collection	Email Collection	T1114
Command and Control	Application Layer Protocol: Web Protocols	T1071.001
Impact	Defacement: External Defacement	T1491.002
Impact	Inhibit System Recovery	T1490

Indicators of Compromise

Network:

- 96.126.130.81 (staging server; open directory on 9999/tcp, SSH on 888/tcp)
- 96.126.130.81:9001 (PHP beacon listener)
- 96.126.130.81:8443 (PowerShell C2)

Beacon URI patterns:

- /b?h=<hostname>

- /h?h=<hostname>&t=bk_hook
- /c?h=<hostname>
- /c and /d on port 8443

Email addresses:

- kkkkevin777@tutamail.com
- theudinhthi421@gmail.com

Files and artifacts on victim hosts:

- .whk.php in the web root
- index.php.orig20261010 and manage/index.php.orig20261010 (backups of overwritten pages)
- htaccess.their20261010 (backup of the owner's .htaccess)
- A cron entry rewriting .htaccess to "Require all granted" every minute
- PHP files with 32-character hexadecimal names in image or upload directories
- Calls to file_get_contents pointing to 96.126.130.81:9001 inside index.php or database configuration files

SSH key comment:

- administrator@chenzicccc

How to Check Whether Your Site Was Compromised

- Search web roots for the string 96.126.130.81 and for the email addresses above
- Look for .whk.php, *.orig20261010 files and PHP files with random hexadecimal names in upload or image directories
- Review the hosting account's crontab for entries that rewrite .htaccess
- Check web server logs for multipart requests with unusually long filenames that return HTTP 500, a pattern associated with PHP2Shell exploitation attempts
- Audit authorized_keys files and SSH login history on shared hosting accounts
- Compare database table contents against recent backups to confirm whether data was altered

Mitigation and Recommendations

- **Patch PHP:** Update to a PHP release that fixes CVE-2026-109618 and CVE-2026-109619 and review the vendor's guidance on session upload progress settings
- **Rotate credentials:** Replace every SSH key, database password and FTP password used on affected hosting accounts, especially where the same credentials serve multiple sites
- **Separate customer environments:** Web developers and agencies managing several client sites should stop reusing keys and database passwords across clients
- **Reset customer passwords:** Victim sites should force password resets, move to hashed password storage and notify affected customers
- **Keep offline backups:** Store backups outside the web hosting account so an attacker with account access cannot find or remove them

- **Block the infrastructure:** Deny traffic to and from 96.126.130.81 at the network and hosting level
- **Do not pay:** Verify the actual state of databases before engaging with any ransom demand, since the attacker already copied the data off the servers

Frequently Asked Questions

What Is PHP2Shell?

PHP2Shell refers to CVE-2026-109618 and CVE-2026-109619, two unauthenticated memory corruption flaws in PHP's session upload progress handling. A reproducer package shows how the flaws can lead to remote code execution. The operator's staging server held a weaponized copy of that package, added after the real estate extortion wave.

Is PHP2Shell Being Exploited in the Wild?

A weaponized PHP2Shell toolkit and follow-on exploit and probe scripts were found on the server of an active extortion operator, added after the operator's attacks on Japanese real estate sites. The files contain no saved output confirming a successful exploitation of a live target, but the tooling was prepared for use against internet-facing PHP hosts.

Which Organizations Were Affected?

The initial victim is a Japanese real estate services company. From its environment, the attacker reached nearly 20 other Japanese websites, mostly real estate agencies and property-buying services, through shared hosting access. A Taiwanese company's Windows server was also accessed later in October, and its databases and email were pulled. Customers of the victim sites are affected too, because their member records were stolen. Email addresses at major banking, telecom and technology organizations appear in that customer data, but those organizations were not breached in this campaign.

Who Is Behind the Attacks?

The ransom pages and contact addresses use the handle kkkkevin777, and the operator's scripts carry Simplified Chinese comments. The files point to a hands-on, financially motivated extortion operator with no sign of a ransomware affiliate program. These are leads from the operator's own files, not a confirmed identity.

What Data Was Stolen?

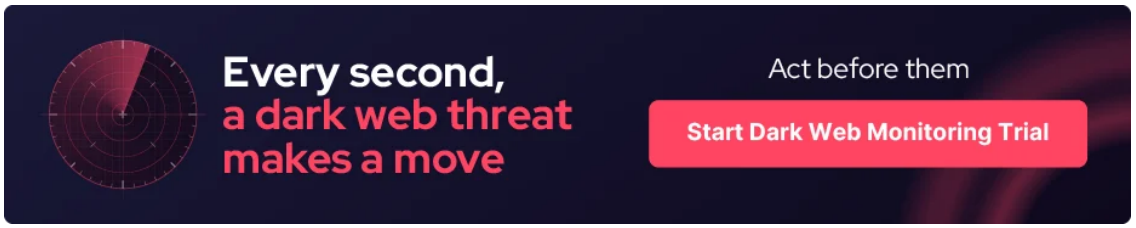
The server held member databases with customer names, contact details and home addresses; the initial victim's export of 16,061 records also includes plaintext passwords, annual income, savings and property search details. From a Taiwanese company, the operator pulled five SQL Server database backups, 663 FoxPro database files and 730 emails. The operator then used that data to pressure victims through their own customers.

Is Patching PHP Enough?

No. Patching closes the PHP2Shell flaws, but the real estate intrusions described here were not traced to PHP2Shell. Affected sites also need to remove web shells and cron entries, rotate every SSH key and database password, and restore clean pages and data. Sites that shared credentials with a compromised site should be treated as compromised even if PHP was patched.

Should Victims Pay the Ransom?

Victims should first verify the actual state of their databases and whether clean backups exist. The attacker copied data off the servers before making the demand, so payment does not guarantee –it never does– the data will be deleted or kept private.



Source: https://socradar.io/blog/php2shell-weaponized-japanese-real-estate-extortion/