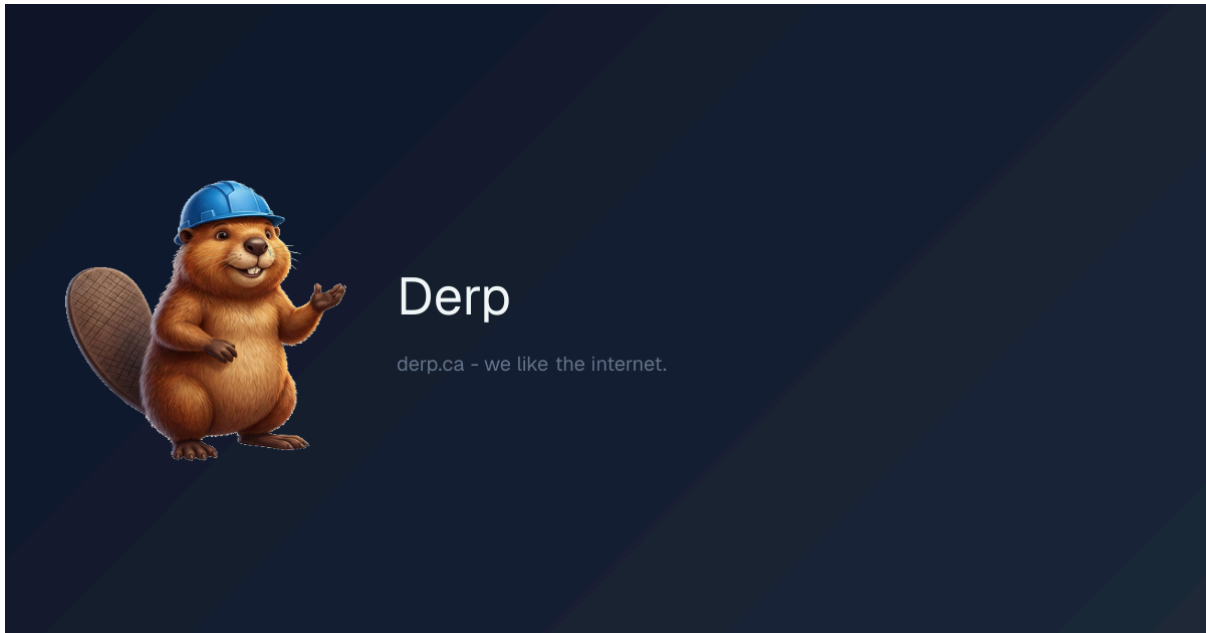


Urelas is old, weird, and still watching Korean card games

 derp.ca/research/urelas-korean-card-game-capture

Kirk

April 25, 2026



malware urelas reverse-engineering korea gaming screenshots

Urelas is boomer malware with a very specific hobby: Korean card games.

[Microsoft wrote up Urelas.C in 2012](#) as a trojan that watched card-game processes and sent screenshots plus host information to a remote server. The process list in that old writeup included [baduki.exe](#), [DuelPoker.exe](#), [highlow2.exe](#), [H00LA3.EXE](#), and [poker7.exe](#).

Fourteen years later, that same shape is still alive. A fresh Urelas sample from April 2026 drops a bit-flipped [MSMP](#) state file, watches Korean poker and badugi clients, and packages cropped game-window captures into JPEG/JFIF [6003](#) records. Its command-and-control path runs through Korean ISP space, including SK Broadband and DLIVE hosts.

This is not one dusty binary that happened to run. Across the current Urelas observations, the family appears in [3,166](#) sample rows and [3,142](#) unique SHA256s from March 13 to April 22, 2026. April alone accounts for [2,311](#) unique SHA256s through April 22.

That makes the old Urelas idea worth revisiting. It is not trying to be a modern stealer with a thousand features. It is closer to a game-table surveillance tool. Find the card-game client, capture the useful part of the window, compress it, and send it out.

If you operate a threat intelligence platform with API access and can provide a researcher account, please reach out to . Additional data sources directly increase the quality and coverage of the threat intel published here.

Sample overview

Artifact	SHA256	Role
Original sample	30d8dfd304a9f810e58facef95e8867cc9064fce96c9514e7b6660f46c888a4e	Parent sample
Intermediate executable	c2c2346d9586e4c85b705050827eac2cabcf9ff11f5fad2e4f2a71bd4635044d	Original file with a 50-byte run-specific tail
Dropped child	5149031bb8349fa8bae74cfac4964a4f5f589cb3d5d1ad9c1357dc2be572dd79	UPX-packed Urelas child
Unpacked child	d5149aea7c8264fb2f13435d8243331b1ce08f0bf53e12bb11bac01d11554ac7	Unpacked payload
golfinfo.ini	ec00df40306bf2c7c8bbf7256a976864bd286e7a190b9890a3c0fac7ab1d8adf	Bit-flipped MSMP state/config
Decoded MSMP config	34e5dad664c9ab2d8ca5f05efaf737916ef2ec29448e322a578d042f856ee628	Decoded config
Helper DLL	77e49b8b91127709ac2d32e0ea34a8e22813e6b7ea5ac93384cf4a6185b2af54	PECompact2 capture helper from ZIP resource

The original sample was collected from Triage submission [260419-mkg44agt3r](#). Controlled execution showed the parent writing an intermediate executable, writing [golfinfo.ini](#), launching the intermediate, and building socket targets for three command-and-control endpoints.

Family footprint

The March-April activity is much larger than the first short view suggested.

Scope	Sample rows	Unique SHA256	First seen	Last seen
March-April observations	3,166	3,142	2026-03-13 10:04:39Z	2026-04-22 00:39:27+01
March 2026	836	831	n/a	n/a

Scope	Sample rows	Unique SHA256	First seen	Last seen
April 2026 through April 22	2,330	2,311	n/a	n/a
Recent observations, April 17-24	554	545	2026-04-17 21:00:07Z	2026-04-24 22:46:24Z

The infrastructure is concentrated by ASN:

ASN / Org	Country	Endpoints	Sample IDs	Unique SHA256
AS9318 SK Broadband Co Ltd	KR	5	2,984	2,962
AS7684 SAKURA Internet Inc.	JP	1	831	827
AS10036 DLIVE	KR	2	171	170
AS4766 Korea Telecom	KR	3	87	86
AS3786 LG DACOM Corporation	KR	1	1	1

The sample below shows one branch of that activity: config, endpoint selection, game-window capture, and helper DLL behavior.

Why card games

Urelas makes more sense when you stop reading it as a generic remote-access trojan.

The target process list in this sample includes Korean poker, badugi, high-low, and launcher surfaces:

Process / Client	Why it matters
highlow2.exe	High-low card game target
poker7.exe / Poker.exe	Poker / 7 Poker target
Baduki.exe / Newbadugi.exe	Badugi / low badugi target
H00LA3.exe	Hoola-style card game target
DuelPoker.exe	Poker client target

Process / Client	Why it matters
PMLauncher.exe / _PMLauncher.exe	Game platform launcher surface

Those names are not random. They overlap heavily with the 2012 Microsoft process list and with the games still marketed by Korean card-game platforms. [Hangame Poker's Google Play listing](#) advertises Seven Poker, Low Badugi, Hold'em, and High Low. [Pmang Poker for Kakao](#) advertises 7 Poker, high-low, and low badugi, and the listing shows more than one million downloads.

These games are not valuable to Urelas because they are games in the Steam-library sense. They are valuable because the screen is the state. A capture can show the client, table view, game type, room context, cards, betting state, and account-side clues. That is why this malware keeps coming back to screenshots rather than browser cookies.

It is old, but the idea is not dumb. It is narrow.

Execution chain

This sample runs through three executables:

```
original sample
-> intermediate child
-> golfinfo.ini
-> UPX-packed second child
-> decoded MSMP state
-> Korean command-and-control endpoint loop
-> game-window capture path
-> JPEG/JFIF 6003 records
```

The first intermediate is unusual. The emitted file matches the original sample exactly, then adds a changing 50-byte tail. A second controlled run used different random names and produced a different 50-byte tail, but the chain stayed the same.

The next executable is cleaner. The dropped child is packed with stock UPX. Unpacking it gives a stable Windows executable:

```
d5149aea7c8264fb2f13435d8243331b1ce08f0bf53e12bb11bac01d11554ac7
```

That unpacked child contains the game-client strings, **MSMP** parser, socket helpers, record builder, capture path, and embedded helper DLL resource.

MSMP state

golfinfo.ini is not a normal INI file. It is a 512-byte state/config file where every stored byte has been bit-flipped.

The first four bytes are the obfuscated config marker:

b2 ac b2 af

The parser flips every bit in those bytes and expects to see **MSMP**:

4d 53 4d 50
MSMP

The parser at **fcn.00405910** reads 512 bytes, flips every bit, and accepts the result only when the decoded 32-bit value is **0x504d534d / MSMP**.

The decoded config contains:

Offset	Value	Role
0x00	MSMP	config marker
0x04	UTF-16 text 218.54.30.235	config host
0x84	16-bit value 0x51	second-child TCP port 81
0x86	UTF-16 text AAAA	state token, exact label unknown
0xa6	UTF-16 text 121.88.5.183	config host
0x126	16-bit value 0x2b70 / 11120	first-child port
0x188	UTF-16 text ab}a}}	dropped child file-name stem
0x1a8	UTF-16 text }aba}}	intermediate file-name stem
0x1c8	32-bit value 5	state/count value

The **MSMP** state matters because both child executables read it. The first child uses the decoded hosts **121.88.5.183** and **218.54.30.235**, then copies the **11120** port into its socket path. The second child also copies decoded host, port, and state fields before it starts its own network loop.

The .184 endpoint is not in the config

The active DLIVE/SK Broadband path for this sample has three endpoints:

Endpoint	Source
121.88.5.183:11120	decoded MSMP host + first-child port
121.88.5.184:11170	embedded first-child code path
218.54.30.235:11120	decoded MSMP host + first-child port

The middle endpoint is the easy one to get wrong. 121.88.5.184 and 11170 are not in the decoded golfinfo.ini config.

The first child contains embedded 121.88.5.184 strings. Its endpoint loop chooses that host from code and selects the port through an OS-version check. Instrumented execution confirms the socket arguments:

Host probe	Port probe	Resulting target
gethostbyname("121.88.5.183")	htons(0x2b70)	121.88.5.183:11120
gethostbyname("121.88.5.184")	htons(0x2ba2)	121.88.5.184:11170
gethostbyname("218.54.30.235")	htons(0x2b70)	218.54.30.235:11120

That distinction matters for detection and analysis. If you only decode golfinfo.ini, you miss one endpoint used during execution. If you only trust dynamic traffic, you miss why that endpoint appears.

Protocol records

The second child has its own protocol handler. The recovered code prepares several record types:

Record type	Role	Evidence
9000	initial client/game state record	record type plus 0x3c6-byte body copied from local UTF-16 text fields
6003	capture/image record	body produced by bitmap capture and JPEG/JFIF encoder path
6004	follow-up state record	same 0x3ca total record shape as 9000, field labels partial
4000	local/control update	updates host/state fields and forces reconnect

Record type	Role	Evidence
6001	capture/helper enable	updates capture-control values and calls helper <code>SetCommand(1)</code>
6002	capture/helper disable	calls helper <code>SetCommand(0)</code>

On the wire, each message starts with its length:

```
4-byte big-endian length
record body
```

The receive format and local/control parser are visible in the unpacked code.

Screenshots are the payload

The 6003 path is the clearest explanation of what this malware is for.

The unpacked child uses Windows screen and window capture APIs, including `GetWindowDC`, `CreateCompatibleBitmap`, `PrintWindow`, `BitBlt`, and `GetDIBits`. It then crops game-specific regions before encoding the result.

The encoder at `fcn.0040b380`:

- validates bitmap-like input
- limits the quality/control argument to `10..100`
- converts 32-bits-per-pixel rows to 24-bits-per-pixel
- writes to a memory buffer
- uses embedded JPEG/JFIF code paths
- returns the output length used by the prepared 6003 record

That ties the old Microsoft behavior to this sample. Urelas is still watching card-game windows and sending screenshots. The capture path is visible in the unpacked code and tied to the protocol record that sends the image.

HGDraw.dll helper

The second child also carries a helper resource. Resource 130, type `UNKNOWN (1144)`, language `LANG_KOREAN`, is a ZIP container. It contains:

```
CaptureDll_pe.dll
```

The child writes and loads this helper as `HGDraw.dll` when the selected game/process path needs it.

Helper property	Value
ZIP SHA256	f732d1c75d7aa387bb63f66b80a4247e7992cde1de02f2cf5110f520b1a939af
DLL SHA256	77e49b8b91127709ac2d32e0ea34a8e22813e6b7ea5ac93384cf4a6185b2af54
Format	PE32 DLL, PECompact2 compressed
Compile timestamp	2013-12-03 13:14:20
PDB path	D:\PMS\pms4\Project(20131120)\HanCapture_2005\bin\CaptureDll.pdb

Local helper execution reaches the helper code, resolves capture APIs, and enters the expected `Sleep(0xc8)` wait loop. The exports used by the parent are simple:

Export	Behavior
SetParentId	stores parent id
SetCommand	stores command flag; 6001 sets 1, 6002 sets 0
SetGameId	stores game/capture selector
GetDllDataLen	returns helper output length
GetDllData	copies helper output buffer to caller

The parent-facing behavior is clear: this DLL is a command-gated capture helper, and the second child can pull its output into the 6003 path.

Detection shape

The hunt is the combination, not one perfect indicator.

Signal	Why it matters
Urelas family with Korean ISP command-and-control hosts	March-April 2026 activity is concentrated in KR ISP space
golfinfo.ini with bit-flipped MSMP config	local state/config format

Signal	Why it matters
Korean card-game process names	target surface, not generic process noise
endpoints <code>121.88.5.183:11120</code> , <code>121.88.5.184:11170</code> , <code>218.54.30.235:11120</code>	this sample's command-and-control setup
<code>6003</code> records with JPEG/JFIF body	game-window capture path
ZIP resource containing PECompact2 <code>CaptureDll_pe.dll</code> / loaded <code>HGDraw.dll</code>	helper capture path
HKCU <code>Software\Microsoft\Windows NT\CurrentVersion\Windows</code> value <code>Run</code>	first-child persistence path

For this sample, the compact endpoint set is:

Type	Value
Command-and-control	<code>121.88.5.183:11120</code>
Command-and-control	<code>121.88.5.184:11170</code>
Command-and-control	<code>218.54.30.235:11120</code>
Config/state file	<code>golfinfo.ini</code>
Helper filename	<code>HGDraw.dll</code>
Capture record type	<code>6003</code>
Initial state record type	<code>9000</code>

The broader family footprint includes more infrastructure than those three IPs. The endpoint set above is the compact set for this sample.

Urelas is not dead, and it is not generic. In 2026, this old family is still doing the same narrow job it was doing in 2012: watching Korean card-game clients and sending the table view home.

Kirk

I like the internet. Want to get in touch?