What are Potato attacks?

Potato attacks are a family of Windows privilege-escalation techniques (JuicyPotato, RoguePotato, PrintSpoofer, GodPotato and others) that turn the SeImpersonatePrivilege held by service accounts into SYSTEM. They work by coercing a high-privilege Windows process to authenticate to the attacker, then using the impersonation privilege to steal its token. They are the go-to Windows escalation once an attacker lands as an IIS or SQL service account. The defence centres on patching and least-privilege service accounts.

HOW IT WORKS

01 The abuse and payload

The attacker confirms SeImpersonate, then runs the variant that fits the target:

- Confirm: `whoami /priv` shows SeImpersonatePrivilege enabled.
- Run, for example: `PrintSpoofer.exe -i -c cmd` or `GodPotato -cmd "cmd /c whoami"`
- The tool coerces a SYSTEM process to authenticate, impersonates its token, and spawns a shell as NT AUTHORITY\SYSTEM.

Which variant works depends on the Windows version and patch level. Documented techniques shown for defenders.

> THEY ALL NEED SEIMPERSONATE
>
> *Every Potato variant depends on SeImpersonatePrivilege. If a service account does not hold it, the whole family fails, which is why least-privilege service accounts matter.*

HOW TO DEFEND

- Patch promptly, since specific Potato variants rely on bugs Microsoft has addressed over time.
- Remove SeImpersonatePrivilege from accounts that do not need it, and use least-privilege managed service accounts.
- Harden and limit the print spooler and DCOM where feasible (PrintSpoofer abuses the spooler).
- Segment so a compromised web or database service cannot easily reach more.
- Detect the named-pipe and token-impersonation patterns these tools produce.

SOURCES

[1] MITRE ATT&CK: Privilege Escalation (TA0004)

[2] Microsoft: Privilege Constants (Windows)

[3] NIST SP 800-115 Technical Guide to Security Testing

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-are-potato-attacks

Open online