Threat Signal Report | FortiGuard Labs

Archived: 2026-04-02 10:59:45 UTC

FortiGuard Labs is aware of a report that APT group "Billbug" compromised a certificate authority (CA) as well as multiple government and defense organizations in Asia. Also known as Lotus Blossom and Thrip, the APT group reportedly has been active since 2009 and uses custom backdoor malware "Hannotog" and "Sagerunex" as well as available tools in compromised machines.

Why is this Significant?

This is significant because Billbug APT threat actor group targeted a certificate authority (CA). Should digital certificates be compromised, the attacker could use them to sign malware for detection evasion by security solutions and eavesdrop on HTTPS communications.

Also, the reports indicate that multiple organizations in government and defense sectors in Asia were compromised by Billbug APT.

What is Billbug APT?

Billbug, Lotus Blossom and Thrip, is a threat actor that has been reportedly active since at last 2009 and has interests in U.S. organizations as well as government, defense, and communications organizations in Southeast Asia. Their primary motive is thought to be information espionage.

Billbug APT employs living-off-the-land techniques and uses custom malware. The tools that were reportedly used by Billbug APT are the following:

- Hannotog backdoor
- Sagerunex backdoor
- AdFind
- Certutil
- LogMeIn
- Mimikatz
- NBTscan
- Ping
- Port Scanner
- PowerShell
- PsExec
- Route
- Tracert
- Winmail
- WinRAR
- WinSCP

What is the Status of Coverage?

FortiGuard Labs detects the files in the report with the following AV signatures:

- W32/Agent.QTP!tr
- W32/Elsentric.J!tr
- W32/Generic.A!tr
- W32/PossibleThreat
- W64/Agentb.F!tr
- W64/Agent.LF!tr
- W64/Elsentric.E!tr
- W64/Elsentric.G!tr
- Malicious_Behavior.SB
- PossibleThreat.PALLAS.H
- Riskware/Kryptik

No Telemetry data available at the moment.
