A Cascade of Compromise: Unveiling Lazarus' Campaign Exploiting Software Company Products and its Intricate Connections with Other Campaigns

Seongsu Park
Kaspersky, GReAT

Seongsu Park

- Kaspersky, Global Research and Analysis Team
- Lead security researcher
- Tracking Korean-speaking actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

Who is Lazarus?

Adversary

- Lazarus
- a.k.a Diamond Sleet
- Published by Novetta in 2014

Victim

- Financial profit
- Cyber espionage
- Data theft

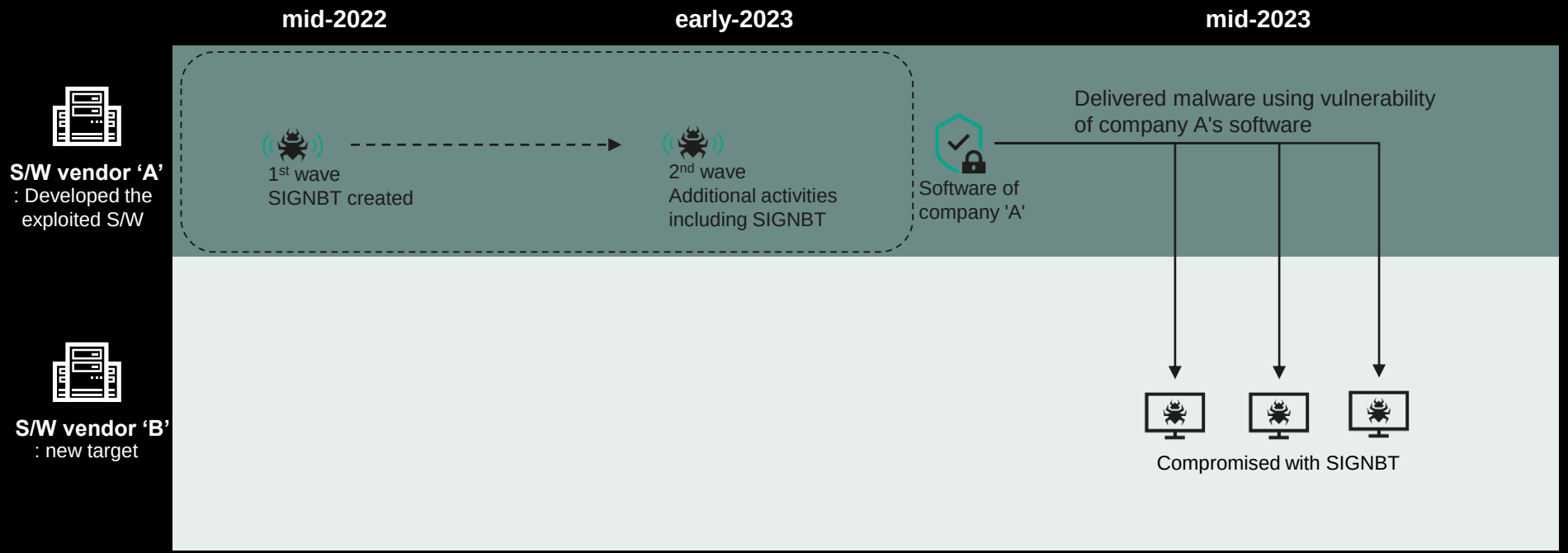
Capability

- Various infection vectors
- Multi-stage components
- Several malware clusters

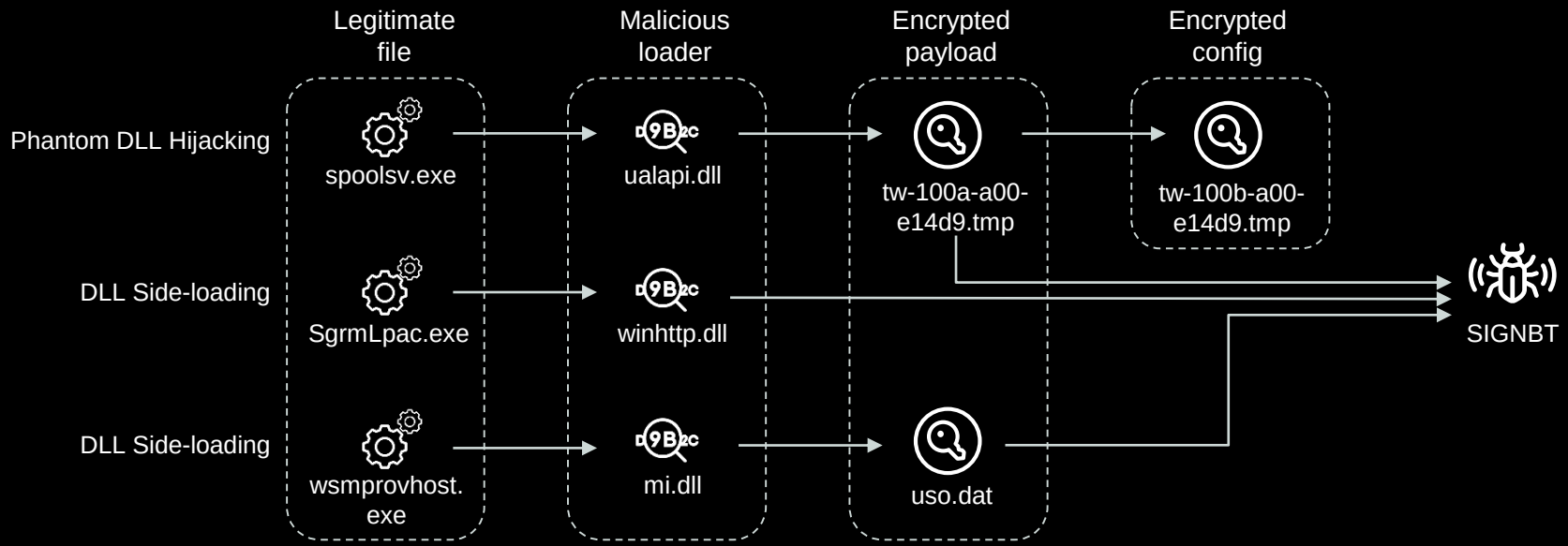
Infrastructure

- Compromised server
- Commercial hosting service

Cascading targeting attack against S/W vendors

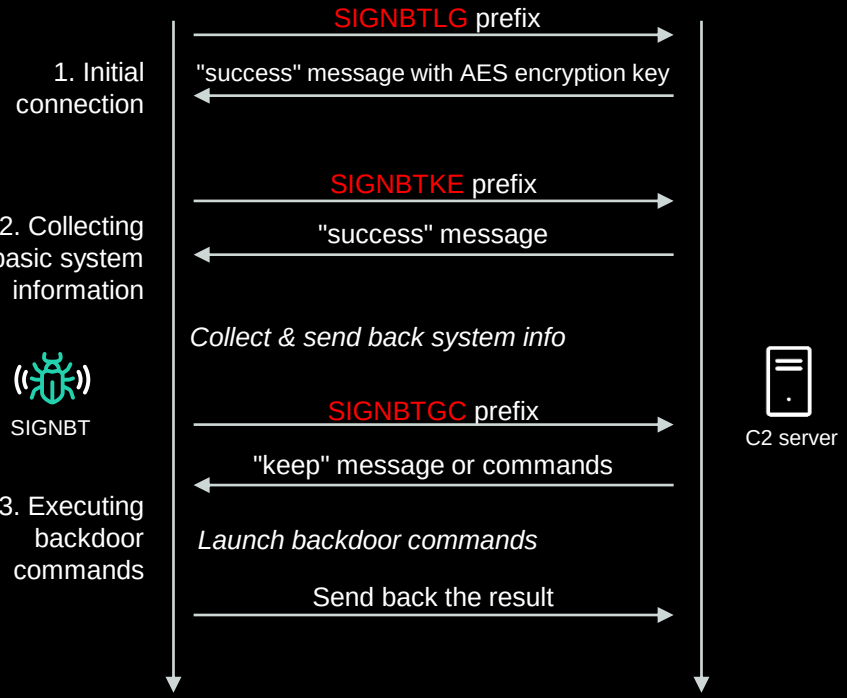


Infection chain of SIGNBT

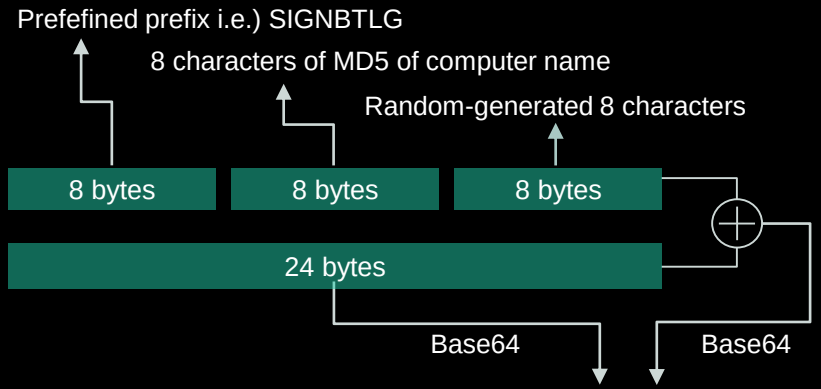


C2 communication of SIGNBT

C2 communication



Creating POST data

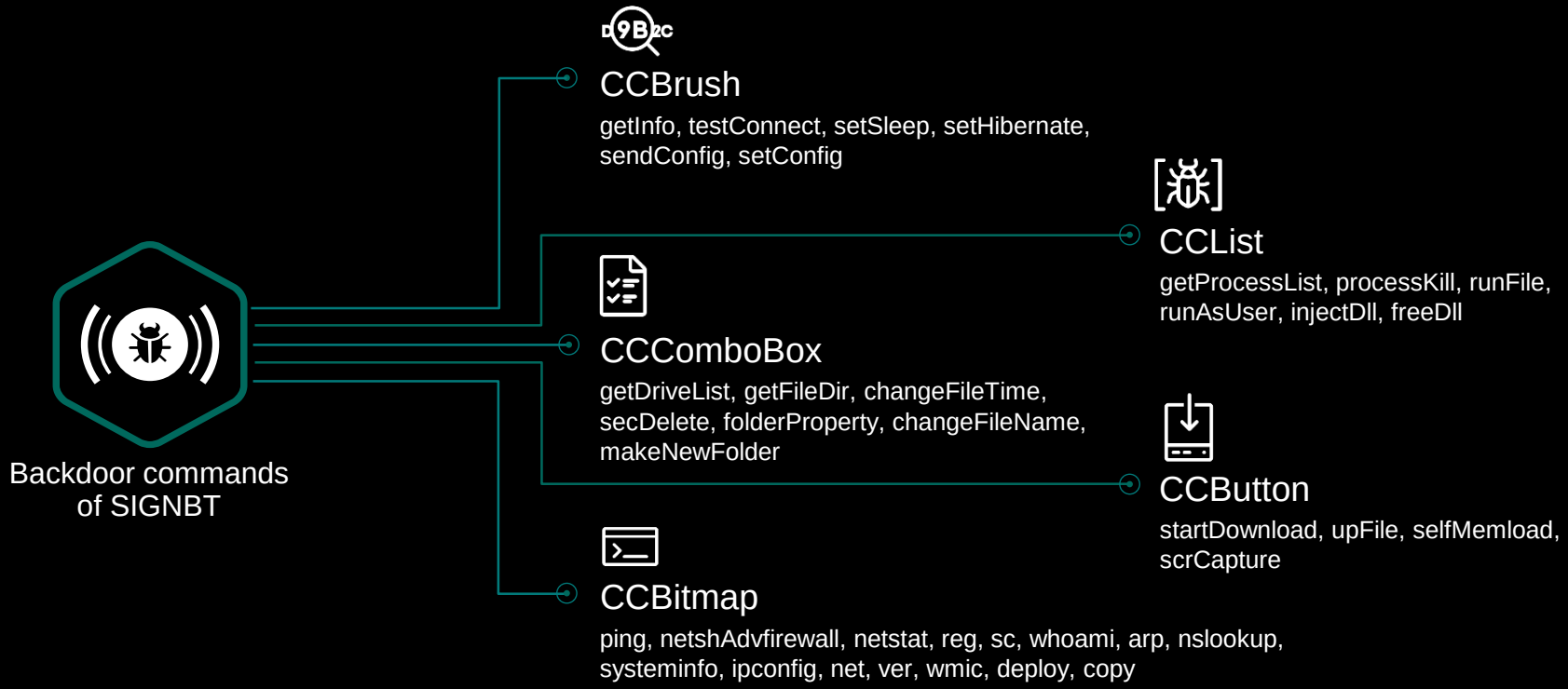


HTTP POST data: [random 3-7 characters]=%s %s

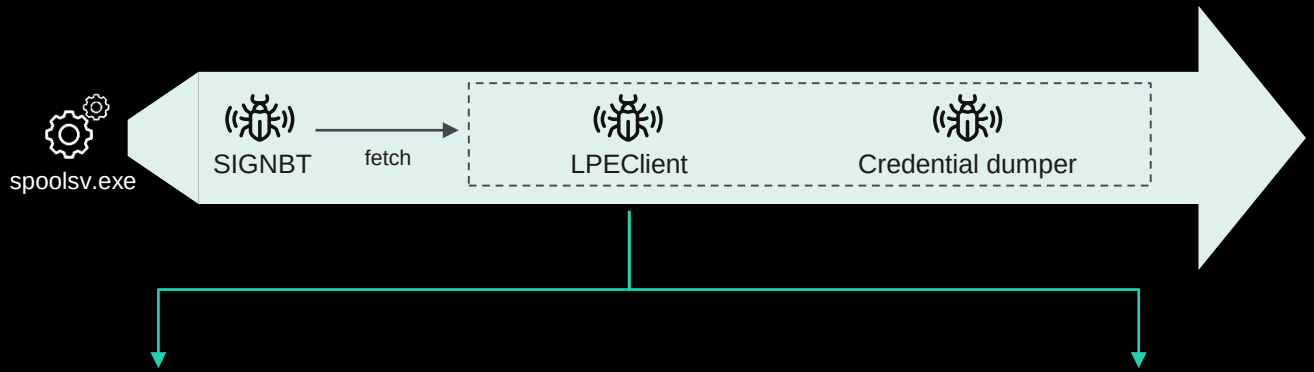
Delivered response data

```
<!DOCTYPE html><html><head></head><body marginwidth="0"
marginheight="0" style="background-color:transparent"><script>
[delivered data]
</script></body></html>
```

Backdoor commands of SIGNBT



Consecutive malware - LPEClient



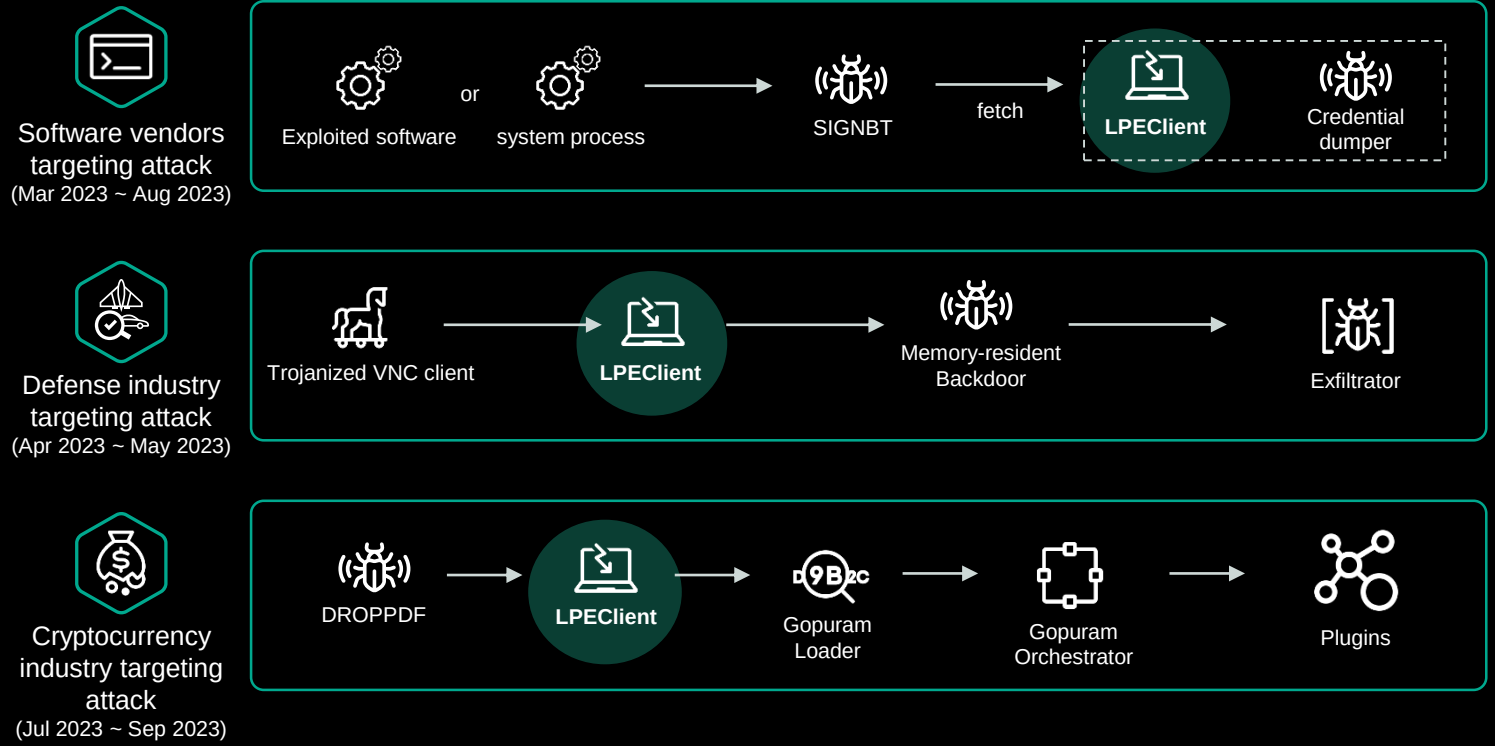
Basic functionalities:

- Utilized since 2020.
- Reporting victim's general info.
- Fetching additional payload.

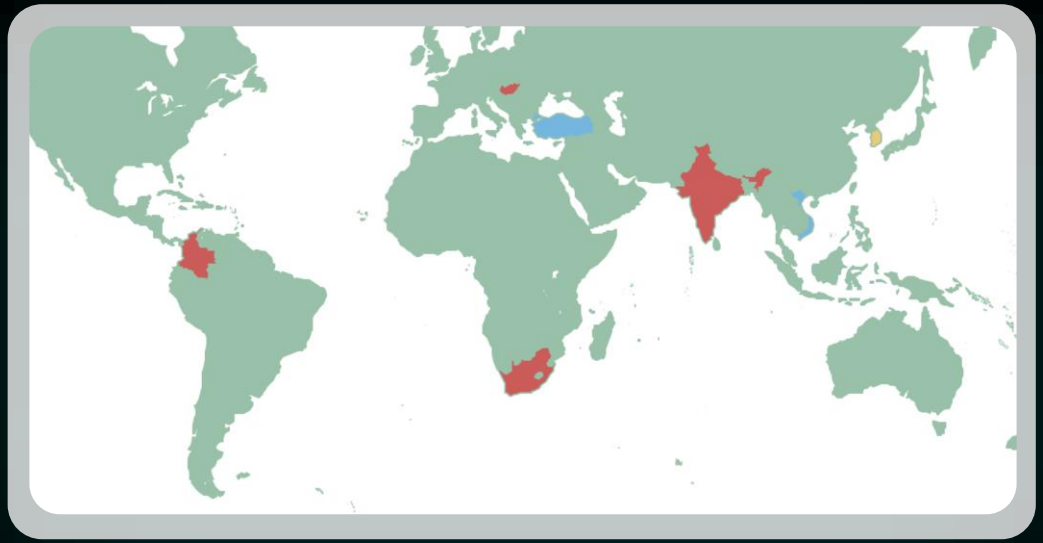
Keep evolving:

- Disable user-mode syscall hook
- Unhook essential system APIs
- Recovering original .text secion of system DLLs

Connection with other campaigns



One threat actor, but different campaigns



Target	Infection vector	Intention
S/W vendor	SWC with S/W exploit	Cyber espionage
Defense contractor	Social engineering with trojanized S/W	Stealing intellectual properties
Cryptocurrency industry	Unknown (3CX supply-chain)	Financial gathering

Takeaway

Persistent attack and increasing sophistication

- Continuously improve techniques to become more sophisticated
- Well-organized and well-resourced group
- Never slow-down

Full-context based defense is the key

- Hit-and-run style defense never works
- Need to understand full-context of threats
- Diversify defense points

Cooperation with other industry

- Each sector has different strength
- Cooperation is essential to cope with the latest cyber threats

#TheSAS2023

Let’s Talk?

Seongsu Park
Kaspersky