

ASTRA SECURITY



18 MINS TO COMPROMISE

Cybercriminals can now move from
initial access to lateral movement
inside enterprise systems in just 18
minutes.

THE FASTEST CASE: ONLY
6 MINUTES FROM VPN
BREACH TO INTERNAL
SPREAD.



WWW.GETASTRA.COM



Shrinking Breakout Time



Breakout Time = Initial Access → Lateral Movement

2019: often measured in days.

2022: dropped to under an hour.

2025: now just 18 minutes on average.

The faster the breakout, the smaller your detection & response window.

Security operations must adapt to this real-time threat speed.





How attackers are breaking in:

Attackers are relying on a mix of old and new techniques to get inside. Drive-by compromises, often through malicious websites or infected downloads, still account for more than a third of incidents. At the same time, USB-based malware is making a comeback, with strains like Gamarue hiding in DLL and shortcut files. More worryingly, attackers are poisoning search results to trick administrators into downloading trojanized versions of legitimate tools such as PuTTY. The message is clear: the front door is wide open in many different ways.



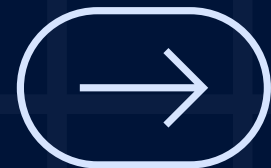
ASTRA SECURITY



Oyster Malware

A NEW MALWARE STRAIN, NICKNAMED OYSTER, ILLUSTRATES HOW SOPHISTICATED THESE ATTACKS HAVE BECOME. OYSTER SPECIFICALLY TARGETS IT ADMINISTRATORS, LURING THEM THROUGH FAKE SOFTWARE SITES. ONCE INSIDE, IT ABUSES TRUSTED SYSTEM BINARIES LIKE RUNDLL32.EXE TO RUN MALICIOUS DLLS, AND IT SETS UP HIDDEN SCHEDULED TASKS THAT LOOK LIKE ORDINARY SYSTEM UPDATES. IT EVEN DISGUISES ITS PAYLOADS WITH NAMES THAT MIMIC LEGITIMATE FILES, SUCH AS TWAIN_96.DLL. THIS MAKES IT EXTREMELY DIFFICULT FOR TRADITIONAL DEFENSES TO SPOT, AS IT BLENDS SEAMLESSLY INTO NORMAL SYSTEM BEHAVIOR.

WWW.GETASTRA.COM





Why It Matters

Enterprises now have just minutes to detect and respond. If attackers reach admin accounts, they can take over the entire network. With stealthy “living-off-the-land” techniques, traditional defenses often fail. The risk isn’t just technical — it’s about business continuity, revenue, and trust.





Defensive Priorities

To match attacker speed, defenses must evolve. Real-time monitoring and behavioral detection are essential. Admin privileges need strict control with MFA and least-privilege enforced. USB use should be restricted, and tools must be verified from trusted sources.

