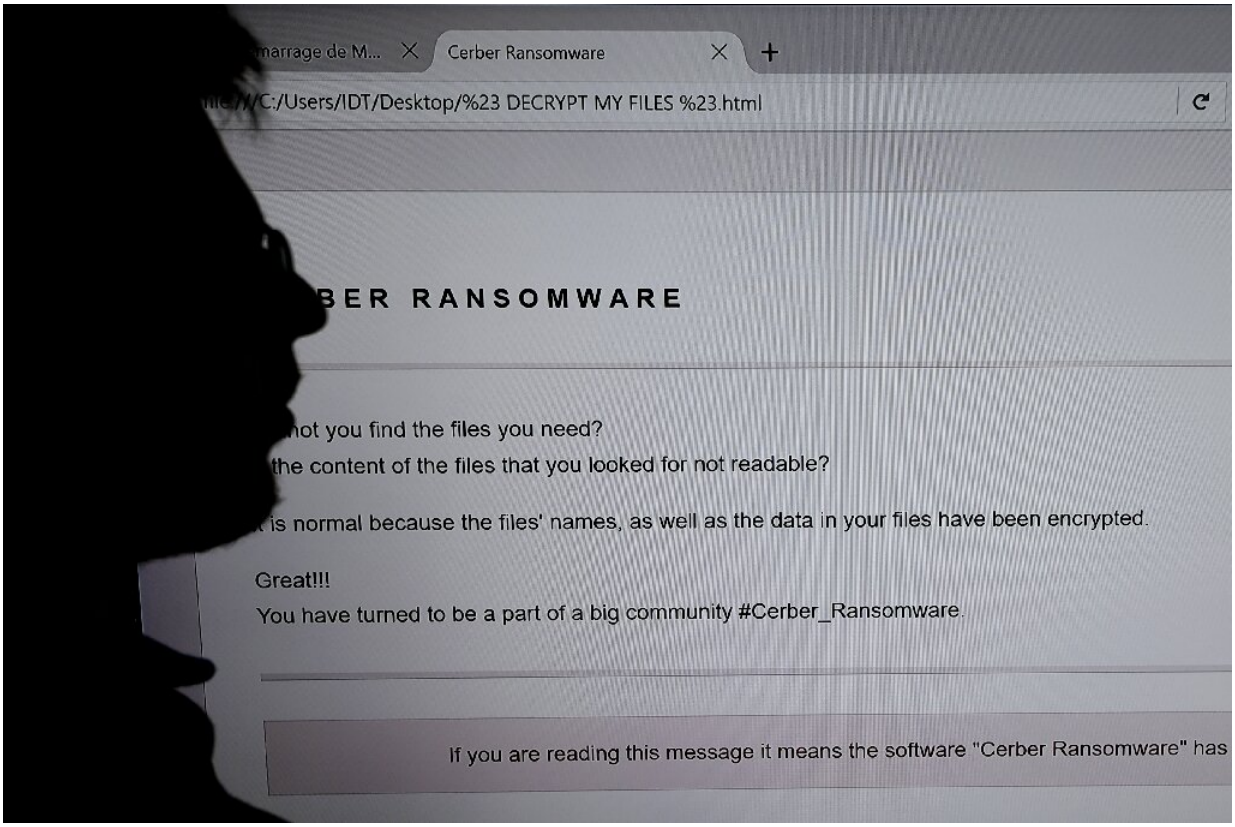
New ransomware strain exploits Microsoft Exchange security flaw

March 12 2021



A new ransomware strain which exploits vulnerabilities uncovered in Microsoft Exchange servers could lead to dire consequences, security researchers say

A new strain of ransomware has emerged which exploits a security flaw in Microsoft Exchange servers, signaling potentially damaging

consequences from a high-profile hack.

Microsoft and other security researchers said the new ransomware dubbed "DearCry" was showing up in servers affected by the breach attributed to a Chinese hacker group.

"We have detected and are now blocking a new family of ransomware being used after an initial compromise of unpatched on-premises Exchange Servers," said a tweet from Microsoft Security Intelligence.

Other researchers including Michael Gillespie, founder of the ID Ransomware service, noted the new strain of malware on Thursday, which could lead to a new wave of ransomware attacks that encrypt computer systems and seek to extract payments from operators.

This is the latest sign that the security flaw which became public this month could open the door to a variety of hackers, cybercriminals and cyberespionage operators.

"While patching to prevent compromises will be easy, remediating any systems that have already been compromised will not," said Brent Callow of the security firm Emsisoft.

"At this point, it's absolutely critical that governments quickly come up with a strategy to help organizations secure their Exchange servers and remediate any compromises before an already bad situation becomes even worse."

Earlier this week the FBI and Department of Homeland Security warned that the Exchange server vulnerability may be exploited for nefarious purposes.

A joint statement by the agencies said that "adversaries could exploit

these vulnerabilities to compromise networks, steal information, encrypt data for ransom, or even execute a destructive attack."

The DHS Cybersecurity and Infrastructure Security Agency has been pressing for patches to be applied to networks in both government and the private sector.

The potentially devastating hack, believed to have affected at least 30,000 Microsoft email servers, comes just months after revelations that Russia was probably behind the massive SolarWinds hack that shook the government and corporate security last year.

The two incidents add to pressure on the Biden administration as it weighs options for "hacking back" or other moves to protect cyberspace.