



Remote Access Trojan Nanocore Poses Risk to HPH Sector

Executive Summary

Nanocore is a particularly sophisticated Remote Access Trojan (RAT) that has been used by criminals to gain complete control over victim's devices, including logging keystrokes and screen activity, manipulating private files and sensitive data, controlling surveillance systems like the webcam and microphone, and harvesting credentials that can be exploited by the criminal or resold. Nanocore is modular, meaning cybercriminals have developed a number of plug-ins and enhancements that are distributed either as part of the official malware kit or circulated amongst the networks of attackers that frequently use Nanocore. Recently, Nanocore has been used as part of coronavirus-themed malware campaigns.

While healthcare and public health (HPH) organizations are not uniquely vulnerable to RATs in general or Nanocore specifically, this malware poses substantial risks to the HPH sector as it provides attackers with broad access to the affected computer, any networks it has access to, and any data hosted on those networks. A successful Nanocore attack can place the data of patients, medical professionals, and staff, as well as the continuing function of a hospital or other medical facility, at risk.

Report

Nanocore was discovered in 2013 and since then, multiple versions have been leaked on underground forums, with the most recent leaked in 2015 with sales of the malware continuing to the present day. While there are legal uses for this type of technology—remote access technology can be used by businesses, IT departments, and schools exercising control over computers they issue—Nanocore has been used by criminals to gain complete control over victim's devices, including logging keystrokes and screen activity, manipulating private files and sensitive data, controlling surveillance systems like the webcam and microphone, and harvesting credentials that can be exploited by the criminal or resold. Although Nanocore is not a type of ransomware, some attacks using this malware have demanded victims pay ransoms to prevent the sale or leakage of sensitive or valuable data.

Tayler Huddleston, a.k.a. Aeonhacks, was sentenced to 33 years in prison for his role in creating and selling Nanocore malware to others from 2012 to 2016, primarily through the cybercriminal forum Hack Forums. Huddleston pled guilty, saying he "knowingly and intentionally aided and abetted thousands of unlawful computer intrusions" by selling the program and that he "acted with the purpose of furthering these unauthorized computer intrusions and causing them to occur." Although Huddleston posted on Hack Forums admonishing those who admitted they were using Nanocore as malware, saying he intended the software to be used for legitimate remote-access purposes, the software was widely distributed as malware both on this forum and elsewhere for as little as USD 25. While free "cracked" versions of the malware are also available for download, paid Nanocore "kits" can include the following features:

- Remote surveillance with desktop, webcam and audio feeds
- Reverse proxy connection capability
- Plugins
- 24/7 customer support

Nanocore is modular, meaning cybercriminals have developed a number of plug-ins and enhancements that are distributed either as part of the official malware kit or circulated amongst the networks of attackers that frequently use Nanocore, allowing even relatively unsophisticated actors to launch attacks. Nanocore intrusions are relatively



difficult to detect and often appear to be legitimate operations within devices and networks.

Nanocore has been used as part of coronavirus-themed malware campaigns. These campaigns use emails promising updates on the COVID-19 pandemic, details about conspiracy theories, or possible cures to entice users to click a link and enter their credentials. More sophisticated campaigns may disguise the emails as business communications in order to increase the urgency and importance assigned to the fake email, or use PowerPoint or International Organization for Standardization (ISO) files to disguise the malware, allowing it to bypass firewalls. Bad actors have used these campaigns to target a variety of industries, including the HPH sector.

To reduce the likelihood that an organization is affected, employees and staff should be trained to recognize and avoid the phishing techniques likely to spread Nanocore. Implementing role-based access control can prevent the takeover of a single user's device from affecting larger, more sensitive systems, while regular secure backups of sensitive data can reduce the impact of attacks that delete or change sensitive data.

References

"Bot Roundup: Avalanche, Kronos, NanoCore," February 27, 2018.

<https://krebsonsecurity.com/2018/02/bot-roundup-avalanche-kronos-nanocore/>.

"Nanocore: Malware Trends Tracker," May 28, 2020. <https://any.run/malware-trends/nanocore>.

Biasini, Nick, and Edmund Brumaghin. "Threat Actors Attempt to Capitalize on Coronavirus Outbreak," February 13, 2020. <https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html>.

Eddy, Nathan. "Coronavirus Outbreak Used by Hackers to Spread Malware," February 17, 2020.

<https://www.healthcareitnews.com/news/coronavirus-outbreak-used-hackers-spread-malware>.

Poulsen, Kevin. "FBI Arrests Hacker Who Hacked No One," March 31, 2017.

<https://www.thedailybeast.com/fbi-arrests-hacker-who-hacked-no-one>.

Wallen, Dave. "NanoCore RAT - Malware of the Month, May 2020," May 18, 2020.

<https://securityboulevard.com/2020/05/nanocore-rat-malware-of-the-month-may-2020/>.