



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Malware Campaign- Nood RAT (Gh0st RAT) targeting Linux distributions

Tracking #:432315651

Date:26-02-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the Nood RAT (Gh0st RAT's Variant) Targeting Linux Systems.

TECHNICAL DETAILS:

A new variant of Gh0st RAT, known as Nood RAT, has been observed targeting Linux systems alongside its traditional focus on Windows platforms. This variant exhibits similar functionality to other RATs, allowing attackers to execute commands remotely, upload and download files, and establish proxies. It was first identified in 2018 and the malware leverages the open-source code of Gh0st RAT for malicious purposes. In the past, the discovery of Nood RAT was linked to exploit attempts against WebLogic servers (CVE-2017-10271) and its utilization by the Rocke group to deploy CoinMiners. Furthermore, it played a role in the Cloud Snooper APT campaign, highlighting its utility in complex attack scenarios.

Nood RAT is created using a builder program called "NoodMaker.exe." This program facilitates the creation of executables compatible with different system architectures, such as x86 or x64. This versatility ensures compatibility with a wide range of targeted systems.

更新说明

1. 针对“测试结果”的说明:
 - 针对Centos 6.6 + 32位系统测试正常,centos官网上下载的CentOS-6.8-i386-bin-DVD1.iso安装的,可以给出你们当时测试该系统的详细信息;
2. 控制端的监听端口完善:
 - 默认监听端口为8080,保存已经监听的成功的端口信息,下次启动程序时候自动监听;
3. 主机上线系统信息修正:
 - 修正系统信息和系统位数;
4. Shell功能中文乱码完善:
 - 处理完毕;
5. File功能:
 - 5.1 中文乱码处理完毕;
 - 5.2 upload功能添加直接拖拽方式上传文件,这个时候可以上传多个文件或目录;
 - 5.3 Delete功能完善:支持多个文件或目录同时删除;

现在运行程序后,自动改成后台运行

界面密码: hello!@#

이름	수정한 날짜	유형	크기
04-02-x86.bin	2021-04-02 오후 7:23	BIN 파일	63KB
64.bin	2021-04-02 오후 7:24	BIN 파일	82KB
config - 副本.ini	2018-12-25 오후 3:34	구성 설정	1KB
config.ini	2021-04-02 오후 7:23	구성 설정	1KB
Nood.exe	2016-10-25 오전 11:28	응용 프로그램	3,146KB
NoodMaker.exe	2016-10-24 오후 4:49	응용 프로그램	1,827KB
v1.0.2.zip	2018-10-16 오후 5:34	7zFM.exe file	3,057KB
更新说明.doc	2016-10-26 오전 12:24	Microsoft Word 97 - 2003 ...	15KB

Nood RAT builder (A Linux version of Gh0st RAT)

A key feature of Nood RAT is its ability to disguise itself as legitimate processes. It achieves this by using the RC4 algorithm to encrypt both process names and configuration data, employing unique strings as keys. Upon initialization, the malware relocates to a temporary directory to further conceal its presence. Encrypted configuration data includes command and control (C2) server addresses, activation schedules, and communication intervals – measures designed to evade detection. Initial communication with the C2 server transmits encrypted system information, using time-based keys to bypass packet inspection.

Nood RAT supports various functionalities like remote shell access, file management, proxying, and port forwarding. These capabilities enable comprehensive system control, data exfiltration, and facilitating lateral movement within compromised networks.

INDICATORS OF COMPROMISE(IoCs):

- Attached in Excel File 

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Regularly back up the data and store it in a secure location
- Ensure that all software, operating systems, and security applications are up to date with the latest patches and updates.
- Monitor the network for suspicious activity.
- Change the passwords regularly and Use strong passwords with multi-factor authentication (MFA).
- Educate employees about the risks of ransomware/malware, how to identify phishing attempts, and safe online behaviour.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. <https://asec.ahnlab.com/en/62144/>