MALWARE ANALYSIS

NetWire malware: What it is, how it works and how to prevent it | Malware spotlight

November 25, 2020 by Pedro Tavares

NetWire is a remote access Trojan focused on password stealing and keylogging, as well as including remote control capabilities. This threat has been used by malicious groups since 2012 and distributed through various social engineering campaigns (malspam). Recently, NetWire has been distributed as a second payload using Microsoft Word documents via GuLoader phishing waves.

This article will deliver details, tactics and the operation mode of NetWire malware as well as preventions measures that can be used to stop this threat.

NetWire 2020 overview

The NetWire RAT is malicious software that emerged in the wild in 2012. This multi-platform malware has since undergone several upgrades and was identified in different types of attacks that range from Nigerian scammers to advanced persistent threat (APT) attacks.

According to Spamhaus Botnet Threat Update - Q2 2020, NetWire RAT has been observed during 2020 as one of the most active botnets. In this threat report, it

In this Series

NetWire malware: What it is, how it works and how to prevent it | Malware spotlight

How AsyncRAT is escaping security defenses

Chrome extensions used to steal users' secrets

Luna ransomware encrypts Windows, Linux and ESXi systems

Bahamut Android malware and its new features

LockBit 3.0 ransomware analysis

AstraLocker releases the

Figure 1: Malware families associated with botnets C&C — Q2 2020 (**Spamhaus**) — #15 NetWire

The threat spreads essentially through COVID-19 themed attacks, according to the Group-IB report. As you can see in Figure 2, NetWire was one of the malware families most exploited in COVID-19 phishing campaigns between February and April 2020.

Figure 2: Malware families most actively exploited in COVID-19 phishing campaigns from February to April 2020 (Group-IB)

NetWire's modus operandi

These days, NetWire is often launched via social engineering campaigns or as a later payload of another malware chain. Criminals send emails with malicious the victim’s computer. The shared files often used by crooks are PDF, Word and IMG files.

Figure 3: NetWire phishing templates

As a result, after clicking on the shared URL, the next stage is downloaded onto the victim’s computer. At this moment, the downloaded file can be a ZIP file containing a PE file inside (see Figure 4), or a DOC file that contains a malicious macro that will download the binary file from the C2 server (Figure 5).

Figure 4: ZIP file containing the NetWire binary inside

Figure 5: Word file with a malicious macro that will download the NetWire binary from the C2 server

After being executed on the victim’s side, several anti-analysis techniques to protect it from being analyzed are executed. In detail, it dynamically extracts the malicious code into the memory and executes it in order to bypass AV detection.

Another interesting detail is the mouse moves detection (Figure 6). No mouse moves mean the target device can be a sandboxing system. With these tricks in place, NetWire pretends to protect itself against automated malware analysis.

NetWire creates a log folder (%AppData%\Logs) to store the log files with the data it collects from the victim's system during its execution. The malware gets all of the victim's keyboard actions and times, as well as the titles of what the victim is typing on. The recorded data is encoded and stored in the log file and sent later onto the C2 server online.

Figure 7: Encoded keylogger log file and its decoded content

As a persistence technique, NetWire creates a home key (HKCU\SOFTWARE\Netwire) as well as adding it into the auto-run group in the victim's registry. With this approach, it executes every time the infected system starts. Based on other analyzed samples, a VBS file is also created on the Windows startup folder (defender.vbs) to make it persistent.

Figure 8: NetWire persistence techniques

Network campaigns target users and companies via social engineering schemas. In general, these kinds of waves could be prevented by taking the following precautions:

- Train users frequently to be aware of potential phishing schemas and how to handle them in the right way
- Be wary of emails from unfamiliar sends or unknown sources and with suspicious attachments related to financial or delivery correspondence, documents and URLs
- Verify the source via alternative means — for instance, by phone or in person — before opening or downloading the content
- Use anti-malware software such as antivirus or any endpoint protection software
- Keep updated all the installed software and the operating system

And finally, be proactive and start taking malware protection seriously!

Sources

- Spamhaus Botnet Threat Update, Spamhaus
- CERT-GIB: Phishers prefer Tesla, top 3 malware strains in COVID-19 phishing campaigns, and pandemic-related dilemmas faced by hacker underground, Group IB
- New NetWire RAT Campaigns Use IMG Attachments to Deliver Malware Targeting Enterprise Users, SecurityIntelligence
- New NetWire RAT Variant Being Spread Via Phishing, Fortinet
- GuLoader: Malspam Campaign Installing NetWire RAT, Unit 42

Posted: November 25, 2020

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker, Malware Analyst and a Security Evangelist. He is also Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years, he has invested in the field of information security, exploring and analyzing a wide range of topics, such as malware, reverse engineering, pentesting (Kali Linux), hacking/red teaming, mobile, cryptography, IoT, and security in computer networks. He is also a Freelance Writer.

Linkedin

MALWARE ANALYSIS

How AsyncRAT is escaping security defenses

January 10, 2023

Pedro Tavares

MALWARE ANALYSIS

Chrome extensions used to steal users' secrets

October 19, 2022

Pedro Tavares

MALWARE ANALYSIS

Luna ransomware encrypts Windows, Linux and ESXi systems

September 28, 2022

Pedro Tavares

MALWARE ANALYSIS

Bahamut Android malware and its new features

September 21, 2022

Pedro Tavares

INFOSEC

Products

Infosec IQ

Security awareness, culture & phishing simulator

Infosec Skills

Hands-on skill development & boot camps

Resources

Blog

Cyber Work Podcast

Events & webcasts

Company

Contact us

About Infosec

Careers

Newsroom

Partners

Newsletter

Get the latest news, updates and offers straight to your inbox.

Email address...

Subscribe

For information about how Cengage uses personal information, see our privacy policy.

Privacy Terms of Use Regulatory Information