MALWARE

GuLoader: Malspam Campaign Installing NetWire RAT

6 min read

RELATED PRODUCTS

Advanced Threat Prevention

By: Brad Duncan

Published: April 3, 2020

Categories: Malware , Threat Research

Tags: Malspam , NetWire , NetWireRAT , Remote Access Trojan

Share

This post is also available in: 日本語 (Japanese)

Executive Summary

NetWire is a publicly-available RAT that has been used by criminal organizations and other malicious groups since 2012. NetWire is distributed through various campaigns, and we usually see it sent through malicious spam (malspam). GuLoader is a file downloader that was first discovered in December 2019, and it has been used to distribute a wide variety of remote administration tool (RAT) malware.

This blog reviews a recent distribution chain in March 2020 using Microsoft Word documents to distribute NetWire through GuLoader. We review the infection chain of events, examine the associated network traffic, and cover post-infection artifacts from an infected Windows host. This material is primarily helpful to Security Operations Center (SOC) personnel like front-line analysts and people who perform forensic investigations.

This blog covers the following areas:

- Chain of events
- Email lures
- Malicious Word documents
- The initial binary
- Infection traffic
- Forensics on an infected Windows host

TABLE OF CONTENTS

RELATED ARTICLES

Threat Assessment: North Korean Threat Groups

Accelerating Analysis When It Matters

Large-Scale StrelaStealer Campaign in Early 2024

Chain of Events

This chain of events kicks off with an email. The email contains a web link for a Microsoft Word document. The Word document has macro code that retrieves a Windows executable for GuLoader. The executable retrieves an encrypted data file used for NetWire. Then we see command and control (C2) traffic for NetWire RAT activity. See Figure 1 for a flow chart of this infection chain.

Figure 1. Chain of events for this NetWire RAT infection.

Email Lures

Malspam distributing NetWire typically uses attachments or links for the malware. Figure 2 shows one such **example from August 2019** with both an attachment and **a link** for the same **Word document** to kick off a NetWire RAT infection.

Figure 2. Malspam from August 2019 with both a link and an attachment for a Word document to kick off a NetWire RAT infection.

GuLoader is now widely used for RAT distribution in 2020 and we continue to see the same type of email lures for malspam pushing NetWIre RAT.

Malicious Word Documents

For an infection chain from March 2020, we clicked on an email link discovered through **AutoFocus** to retrieve a malicious Word document as shown in Figure 3.

Figure 3. Downloading a malicious Word document from the link in the malspam

Our research led us to two links that generated similar infection chains:

- `hxxp://www.artizaa[.]com/Andys_18US_Tax.doc`
- `hxxp://murthydigitals[.]com/PM_2019_Screen_18_Tax_File.doc`

Both links returned Word documents for the same type of NetWire RAT activity. Each document used a different template

Figure 4. Document from one of the links to start NetWire RAT infection

Figure 5. Document from another one of the links to start a NetWire RAT infection

The Initial Binary

Enabling macros for each of these Word documents generated an infection on a vulnerable Windows host. Each vulnerable host retrieved an initial binary for GuLoader and ran it from the infected users' `AppData\Local\Temp` directory. Figure 7 and Figure 8 show examples from each Word document.

Figure 7. Binary for GuLoader after enabling macros on Andys_18US_Tax.doc

Figure 8. Binary for GuLoader after enabling macros on PM_2019_Screen_18_Tax_File.doc

Infection Traffic

Pcaps of the infection traffic revealed the following:

- HTTP request that returned a malicious Word document
- HTTP request that returned a malicious Windows executable file (GuLoader)
- HTTP request that returned an encoded binary
- TCP traffic for NetWire RAT

See Figure 9 and Figure 10 for images of the traffic filtered in Wireshark.

Figure 9. NetWire RAT infection traffic associated with PM_2019_Screen_18_Tax_File.doc and GuLoader filtered in Wireshark

Figure 10. NetWire RAT infection traffic associated with Andys_18US_Tax.doc and GuLoader filtered in Wireshark

This March 2020 infection traffic follows the same concept for GuLoader to RAT activity discussed in **a previous analysis of GuLoader**.

Forensics on an Infected Windows Host

A copy of the initial EXE for GuLoader is made persistent, then the original is deleted from the infected user's `AppData\Local\Temp` directory where it was originally saved. The GuLoader EXE is persistent through the Windows Registry under the following key:

Figure 11. First example of GuLoader persistent through the Windows Registry.

Figure 12. Second example of GuLoader persistent through the Windows Registry

Because this is ultimately a NetWire RAT infection, we can also find a registry update at `HKCU\Software\NetWire` like the example shown in Figure 13.

Figure 13. Windows Registry update for NetWire

We can also find artifacts associated with a NetWire infection as shown in Figure 14 and Figure 15.

Figure 14. First example of file indicating data exfiltrated by NetWire RAT on 2020-03-25

Figure 15. Second example of file indicating data exfiltrated by NetWire RAT on March 25, 2020

Conclusion

These types of infections are not very effective against Windows 10 hosts using default security settings. Versions of Microsoft Office since 2013 have Protected View enabled by default that prevents users from enabling macros in Word documents downloaded from the Internet. Furthermore, Real-time protection and Tamper protection settings in Windows Defender were remarkably effective in preventing these infections within a Windows 10 test environment. Finally, within 24 hours of discovery, URLs serving the malware associated with these infections had been taken off-line.

However, criminal distribution of RATs and other types of commodity malware are often a cat-and-mouse game against security vendors. After one wave of malware is distributed, the binaries are updated, and another wave is quickly released into the wild. These efforts rely on wide-scale distribution from the criminals and poor security practices among potential victims. Only a small percentage infection attempts need to be successful for these efforts to be cost-effective.

Palo Alto Networks customers are further protected through our **threat prevention** platform which is designed to detect and block such threats, and **AutoFocus** shows these binaries as malicious. As long as this type of malware distribution remains cost-effective, criminals will continue to pursue such methods of attack.

- 116.202.210[.]82 port 80 - murthydigitals[.]com - GET /PM_2019_Screen_18_Tax_File.doc
- 213.219.212[.]206 port 80 - ptgteft[.]com - GET /Exten/TY1920/TY30.exe
- 213.219.212[.]206 port 80 - matpincscr[.]com - GET /tec_encrypted_340BD0.bin
- 185.163.47[.]213 port 2121 - www.Novmintservices[.]com - NetWire RAT post-infection TCP traffic

Infection traffic - second run on 2020-03-25

- 104.27.138[.]31 port 80 - www.artizaa[.]com - GET /Andys_18US_Tax.doc
- 213.219.212[.]206 port 80 - saidialxo[.]com - GET /lp.exe
- 185.196.8[.]122 port 80 - www.rossogato[.]com - GET /ROSSO_encrypted_54E9BA0.bin
- 185.163.47[.]168 port 2020 - www.myamystills[.]com - NetWire RAT post-infection TCP traffic

Malware - first run

cc554633c0b734778211a6289e1d6d383d734a3e1a8edeb13d6d0fafc8a2f162

- Size: 117,204 bytes
- Location: hxxp://murthydigitals[.]com/PM_2019_Screen_18_Tax_File.doc
- Description: Word doc with malicious macro

4d373131b0d3254d72f1a06ea168267376b8cc8f805daa53963db5f051631967

- Size: 65,536 bytes
- Location: hxxp://ptgteft[.]com/Exten/TY1920/TY30.exe
- Description: GuLoader retrieved after enabling macros

aadc6031fed895de570214afb8b6cdc66f17d01f1df0407f4d57f1d04313ae2b

- Size: 130,624 bytes
- Location: hxxp://matpincscr[.]com/tec_encrypted_340BD0.bin
- Description: Encrypted binary retrieved by GuLoader for NetWire RAT

Malware - second run

c87e798118a539a136baa0bb9d2539a6e074b0ee640cf0a4ed1ef17936f69ebf

- Size: 150,534 bytes
- Location: hxxp://www.artizaa[.]com/Andys_18US_Tax.doc
- Description: Word doc with malicious macro

e895c525a99922beedf02ca7742c49f320448522185bec8f7d2a49d6cee9f24

- Size: 69,632 bytes
- Location: hxxp://saidialxo[.]com/lp.exe
- Description: GuLoader retrieved after enabling macros

661d9c0c23e9c17412eee8d72cc1bb66c1b4e5f73908c8cce48f89420f38b205

- Size: 130,624 bytes
- Location: hxxp://www.rossogato[.]com/ROSSO_encrypted_54E9BA0.bin
- Description: Encrypted binary retrieved by GuLoader for NetWire RAT

Back to top

TAGS

Related Malware Resources

C Ic THREAT RESEARCH

November 1, 2024

TA Phone Home: EDR Evasion Testing Reveals Extortion Actor's Toolkit

Extortion | Data exfiltration

Read now →

C Ic THREAT RESEARCH

October 9, 2024

Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Inst...

North Korea | Social engineering | Python

C Ic THREAT RESEARCH

October 1, 2024

Detecting Vulnerability Scanning Traffic From Underground Tools Using...

Machine Learning

Read now →

C Ic THREAT ACTOR GROUPS

September 26, 2024

Unraveling Sparkling Pisces's Tool Set: KLogEXE and FPSpy

MITRE | Keylogger | North Korea

Read now →

Newsletter

UNI 42 Sma Log Get updates from Unit 42

Peace of mind comes from staying ahead of threats. Contact us today.

Your Email

Subscribe for email updates to all Unit 42 threat research.
By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.

Subscribe Ri Ar

Products and services

Network Security Platform

CLOUD DELIVERED SECURITY SERVICES

Advanced Threat Prevention

DNS Security

Code to Cloud Platform

Prisma Cloud

Cloud-Native Application Protection Platform

Company

About Us

Careers

Contact Us

Corporate Responsibility

Customers

Popular links

Blog

Communities

Content Library

Cyberpedia

Event Center

Strata Cloud Manager

SECURE ACCESS SERVICE EDGE

Prisma Access

Prisma SD-WAN

Autonomous Digital Experience Management

Cloud Access Security Broker

Zero Trust Network Access

AI-Driven Security Operations Platform

Cortex XDR

Cortex XSOAR

Cortex Xpanse

Cortex XSIAM

External Attack Surface Protection

Security Automation

Threat Prevention, Detection & Response

Threat Intel and Incident Response Services

Proactive Assessments

Incident Response

Transform Your Security Strategy

Discover Threat Intelligence

Sitemap

Tech Docs

Unit 42

Do Not Sell or Share My Personal Information

Privacy Trust Center Terms of Use Documents

EN